THE MOUFANG LAWS, GLOBAL AND LOCAL

J. D. PHILLIPS

ABSTRACT. There are many possible ways to define *Moufang element*. We show that the traditional definition is not the most felicitious—for instance, the set of all Moufang elements in an arbitrary loop, qua the traditional definition, need not form a subloop. We offer a new definition of Moufang element that ensures that the set of all Moufang elements in an arbitrary loop is a subloop. Moreover, this definition is "maximally algebraic" with respect to autotopisms. We also give an application of this new definition by showing that a flexible A-element in an inverse property loop is, in fact, a Moufang element, thus sharpening a well-known result of Kinyon, Kunen, and the present author [6]. Finally, we prove that divisible, Moufang groupoids are Moufang loops, thus sharpening a result of Kunen [9], one of the first computer-generated proofs in loop theory.

1. Introduction

A *groupoid* is a set with a single binary operation. A *quasigroup* is a groupoid such that in $x \cdot y = z$, knowledge of any two of x, y, and z specifies the third uniquely. This definition can also be expressed in the language of universal algebra: a *quasigroup* is a set with three binary operations $\cdot$, $/$, $\backslash$ that satisfy the following four identities:

$$x \cdot (x\backslash y) = y, \quad (y/x) \cdot x = y, \quad x\backslash(x \cdot y) = y, \quad (y \cdot x)/x = y.$$

A *loop* is a quasigroup with a unique two-sided identity element, denoted by 1. We usually write xy instead of $x \cdot y$, and reserve $\cdot$ to have lower priority than juxtaposition among factors to be multiplied, for instance, $x \cdot yz$ stands for $x \cdot (y \cdot z)$. Given a loop L with binary operation denoted by $\cdot$, the *opposite loop* of L is the loop whose underlying set is L and with binary operation given by $x + y = y \cdot x$.

One can consider global or local identities in groupoids. For instance, the familiar commutative and associative laws can be thought of as global laws, since they are universally quantified, e.g., $\forall x, y, xy = yx$ (commutativity); $\forall x, y, z, xy \cdot z = x \cdot yz$ (associativity).

Their localized versions (*i.e.*, given in terms of fixed constants that satisfy these laws) yield the commutant and the four nuclei: the *commutant* is defined by $\mathrm{C}(L) = \{a : ax = xa, \forall x \in L\}$, the *left nucleus* by $\mathrm{N}_\lambda(L) = \{a : a \cdot xy = ax \cdot y, \forall x, y \in L\}$, the *middle nucleus* by $\mathrm{N}_\mu(L) = \{a : x \cdot ay = xa \cdot$

1991 *Mathematics Subject Classification.* 20N05.
Key words and phrases. loop, Moufang, A-loop.

$y, \forall x, y \in L\}$, the *right nucleus* by $\mathrm{N}_\rho(L) = \{a : x{\cdot}ya = xy{\cdot}a, \forall x, y \in L\}$, and the *nucleus* by $\mathrm{N}(L) = \mathrm{N}_\lambda(L) \cap \mathrm{N}_\mu(L) \cap \mathrm{N}_\rho(L)$. In the balance of the paper, all occurrences of x, y, and z are understood to be universally quantified, and hence, we omit the symbol $\forall$; for instance, we write $\{a : x \cdot ay = xa \cdot y\}$ as shorthand for $\{a : x \cdot ay = xa \cdot y, \forall x, y \in L\}$.

If L is a loop, $\mathrm{C}(L)$ need not be a subloop [7]. But in some varieties, e.g., groups, Moufang loops (definition to follow), they are. All four nuclei are subloops [12].

We use the standard notation for the right and left translations: $xR(y) = yL(x) = xy$. The *multiplication group*, $\mathrm{Mlt}(L)$, of a loop L is the subgroup of the group of all bijections on L generated by right and left translations. Clearly $\mathrm{Mlt}(L)$ acts as a permutation group on L. The subgroup of $\mathrm{Mlt}(L)$ which fixes $1 \in L$ is called the *inner mapping group* and is generated by the following three families of mappings [1]:

$$\begin{aligned} T(x) &= L(x)^{-1}R(x) \\ R(x, y) &= R(x)R(y)R(xy)^{-1} \\ L(x, y) &= L(x)L(y)L(yx)^{-1}. \end{aligned}$$

A loop is an *inverse property* loop if it satisfies the two identies $x^{-1}{\cdot}xy = y$ and $yx{\cdot}x^{-1} = y$, where x^{-1} is the unique element given by $x^{-1}x = 1 = xx^{-1}$. A loop is *flexible* if it satisfies the identity $x{\cdot}yx = xy{\cdot}x$. A loop is *alternative* if it satisfies the two identities $x \cdot xy = xx \cdot y$ and $y \cdot xx = yx \cdot x$. A triple of bijections, (f, g, h) on a loop L is called an *autotopism* if $xf \cdot yg = (x \cdot y)h$.

Our investigations were aided by the automated reasoning tool Prover9 and by the finite model builder Mace4 [10] . It is common practice to publish untranslated Prover9 (and its predecessor, Otter) proofs [11]. This is mathematically sound since the program can be made to output a simple *proof object*, which can be independently verified by a short `lisp` program. Since Prover9 proofs can be a bit difficult to parse, especially for the uninitiated, we have opted not to include them, here. We have, though, posted them on the author's website:

`http://persweb.wabash.edu/facstaff/phillipj/research.html`.

Finally, we note that we have included all relevant distinguishing examples not simply for the sake of completeness, but also because some of them are fairly difficult to find (*i.e.*, it takes a finite model builder—in our case, Mace 4—over a week to find a few of them).

2. Local Moufang Laws

Consider the following four (global) groupoid identities:

$$\begin{aligned} (A):&\quad z(xy \cdot z) = zx \cdot yz &\qquad (C):&\quad z(x \cdot zy) = (zx \cdot z)y \\ (B):&\quad (z \cdot xy)z = zx \cdot yz &\qquad (D):&\quad (xz \cdot y)z = x(z \cdot yz) \end{aligned}$$

In each of these four equations we use z as the variable that appears twice on each side of the equal sign, and we use x and y, in alphabetical order, as the two variables that appear once on each side of the equal sign. This standard notation will prove useful, as we shall see.

In loops, each of $(A), (B), (C)$, and (D) is equivalent to the other three [12]. In fact, the same is true in quasigroups, and in this case, they are loops [9]. They are known as the four *Moufang identities.*

Now, given an element a in a groupoid G, consider all possible local versions of the Moufang identities:

$$\begin{array}{rlrl} (A2): & a(xy \cdot a) = ax \cdot ya & (C2): & a(x \cdot ay) = (ax \cdot a)y \\ (A1x): & z(ay \cdot z) = za \cdot yz & (C1x): & z(a \cdot zy) = (za \cdot z)y \\ (A1y): & z(xa \cdot z) = zx \cdot az & (C1y): & z(x \cdot za) = (zx \cdot z)a \end{array}$$

$$\begin{array}{rlrl} (B2): & (a \cdot xy)a = ax \cdot ya & (D2): & (xa \cdot y)a = x(a \cdot ya) \\ (B1x): & (z \cdot ay)z = za \cdot yz & (D1x): & (az \cdot y)z = a(z \cdot yz) \\ (B1y): & (z \cdot xa)z = zx \cdot az & (D1y): & (xz \cdot a)z = x(z \cdot az) \end{array}$$

The labels are meant to be suggestive. For instance, $(A2)$ indicates that in the Moufang identity (A), the constant a is substituted for the variable z (which appears twice on each side of the equal sign); $(B1x)$ indicates that in the Moufang identity (B), the constant a is substituted for the variable x (which appears once on each side of the equal sign); $(C1y)$ indicates that in the Moufang identity (C), the constant a is substituted for the variable y (which appears once on each side of the equal sign); and so on.

Definition 2.1. An element a in a groupoid L is a called a *flexible element* if $a \cdot xa = ax \cdot a$.

Lemma 2.2. *In a groupoid with two-sided identity element, if a satisfies any one of* $(A2), (B2), (C2)$ *or* $(D2)$*, then a is a flexible element. In particular,* $(A2)$ *and* $(B2)$ *are equivalent in groupoids with two-sided identity elements.*

Proof. Let e be the two-sided identity element. Assume that a is an $(A2)$ element. Then $a \cdot xa = a(xe \cdot a) = ax \cdot ea = ax \cdot a$. The other implications are similarly trivial to prove. □

Remark 2.3. Note that in the proof, we showed that $a \cdot xa = ax \cdot a$. In other words, in a groupoid with 2-sided identity element, $(A2)$ elements are flexible. We use this fact freely in the balance of the paper.

We will thus use $(A2)$, and omit $(B2)$ from the balance of the this paper. No one of these eleven identities implies any of the other ten, as the following eleven examples show. Each example is of minimal order.

Example 2.4. In this loop, 1 is an $(A2)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	1	4	0	2
4	2	5	1	3	0
5	3	4	0	2	1

Example 2.5. In this loop, 1 is an $(A1x)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	5	7	6	0	1	3	2
5	6	4	7	1	3	2	0
6	7	5	4	3	2	0	1
7	4	6	5	2	0	1	3

Example 2.6. In the opposite loop of the loop in the previous example, 1 is a $(B1y)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

Example 2.7. In this loop, 1 is an $(A1y)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

0	1	2	3	4	5	6	7	8	9	10	11
1	2	0	4	5	3	7	8	6	10	11	9
2	0	1	5	3	4	8	6	7	11	9	10
3	5	4	0	2	1	9	10	11	6	7	8
4	3	5	1	0	2	10	11	9	8	6	7
5	4	3	2	1	0	11	9	10	7	8	6
6	7	8	9	10	11	0	1	2	3	5	4
7	8	6	10	11	9	1	2	0	4	3	5
8	6	7	11	9	10	2	0	1	5	4	3
9	11	10	8	7	6	3	4	5	0	2	1
10	9	11	6	8	7	5	3	4	1	0	2
11	10	9	7	6	8	4	5	3	2	1	0

Example 2.8. In the opposite loop of the loop in the previous example, 1 is a $(B1x)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

Example 2.9. In this loop, 1 is a $(C2)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

0	1	2	3	4	5
1	2	0	4	5	3
2	0	1	5	3	4
3	5	4	0	2	1
4	3	5	2	1	0
5	4	3	1	0	2

Example 2.10. In the opposite loop of the loop in the previous example, 1 is a $(D2)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

Example 2.11. In this loop, 1 is a $(C1x)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	7	5	6	0	3	1	2
5	4	6	7	2	0	3	1
6	5	7	4	1	2	0	3
7	6	4	5	3	1	2	0

Example 2.12. In the opposite loop of the loop in the previous example, 1 is a $(D1y)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

Example 2.13. In this loop, 1 is a $(C1y)$ element, but 1 does not satisfy any of the other 10 local Moufang identities. This example is of minimal order.

0	1	2	3	4	5	6	7	8	9
1	2	3	4	0	6	8	5	9	7
2	3	4	0	1	7	5	9	6	8
3	4	0	1	2	8	9	6	7	5
4	0	1	2	3	9	7	8	5	6
5	7	9	8	6	0	4	1	2	3
6	5	7	9	8	1	0	3	4	2
7	9	8	6	5	4	2	0	3	1
8	6	5	7	9	3	1	2	0	4
9	8	6	5	7	2	3	4	1	0

Example 2.14. In the opposite loop of the loop in the previous example, 1 is a $(D1x)$ element, but 1 does not satisfy any of the other 10 local Moufang identities.

The following lemma will prove useful.

Lemma 2.15. *If an element a of a loop L satisfies any one of (A2), (A1x), (A1y), (B2), (B1x), (B1y), (C2), (C1x), (C1y), (D2), (D1x) or (D1y), then $1/a = a\backslash 1$, so that a has a two-sided inverse, a^{-1}.*

Proof. We prove this for ($A2$), and leave the other cases for the reader. In this case we have

$$(a[(x/a)\cdot a])/a = ([a\cdot(x/a)]a)/a = a\cdot x/a\ . \tag{1}$$

Let $x = 1$ in (1) to obtain

$$1 = (a\cdot 1)/a = (a[(1/a)\cdot a])/a = a\cdot 1/a\ . \tag{2}$$

Left division of (2) by a , gives $a\backslash 1 = 1/a$. □

3. Moufang Elements

The examples in the previous section show that there are eleven possible basic definitions of "Moufang element". Traditionally, ($A2$) has been used as the definition of Moufang element. Explicitly, an element a in a loop L has traditionally been called a *Moufang element* if it satisfies $a(xy\cdot a) = ax\cdot ya$. Why has ($A2$) been so privileged? One reason is that in a left (or right) inverse property loop, the set of Moufang elements, qua the traditional definition, forms a subloop [4], while the set of Moufang elements in an arbitrary loop need not be a subloop. For example, in the following loop, 1 and 2 are Moufang elements (again, qua the traditional ($A2$) definition), but $1\cdot 2$ is not, since $(1\cdot 2)\cdot((6\cdot 6)\cdot(1\cdot 2)) = 4 \neq 3 = ((1\cdot 2)\cdot 6)\cdot(6\cdot(1\cdot 2))$. We believe that this is the first such example in the literature. We shall revisit this theme in section 5.

Example 3.1.

0	1	2	3	4	5	6	7	8	9	10	11
1	0	3	2	5	4	7	6	10	11	8	9
2	4	0	5	1	3	8	9	6	7	11	10
3	5	1	4	0	2	9	8	11	10	6	7
4	2	5	0	3	1	10	11	7	6	9	8
5	3	4	1	2	0	11	10	9	8	7	6
6	7	8	10	9	11	0	1	2	3	4	5
7	6	9	11	8	10	1	0	3	2	5	4
8	10	6	7	11	9	2	4	0	5	1	3
9	11	7	6	10	8	4	2	5	0	3	1
10	8	11	9	6	7	3	5	1	4	0	2
11	9	10	8	7	6	5	3	4	1	2	0

Another reason that ($A2$) has been so privileged is that the intersection of all ($A2$) elements with the commutant forms a subloop [13]. This is an interesting example of two sets, neither of which is necessarily a subloop, whose intersection is a subloop.

Yet another reason that $(A2)$ has been so privileged is that it can be expressed via an autotopism. But in fact, exactly four of the twelve local Moufang laws can be given via autotopisms (here we include $(B2)$ for symmetry):

$$\begin{array}{llll} (A2): & (L_a, R_a, R_aL_a) & \qquad (C2): & (L_aR_a, L_a^{-1}, L_a) \\ (B2): & (L_a, R_a, L_aR_a) & \qquad (D2): & (R_a^{-1}, R_aL_a, R_a) \end{array}$$

Thus, since $(A2)$ and $(B2)$ are equivalent, we see that there are three algebraically appealing possible definitions of Moufang element (including the traditional one), at least insofar as they are expressible via an autotopism. We give each of them in the following definition (note the obvious analog with the left, middle, and right nuclei).

Definition 3.2. An element a in a loop L is called

1. a *left Moufang element* if (L_aR_a, L_a^{-1}, L_a) is an autotopism, *i.e.*, if $a(x \cdot ay) = (ax \cdot a)y$, *i.e.*, if a is (C2),
2. a *middle Moufang element* if (L_a, R_a, R_aL_a) is an autotopism, *i.e.*, if $a(xy \cdot a) = ax \cdot ya$, *i.e.*, if a is (A2), *i.e.*, the traditional definition of Moufang element,
3. a *right Moufang element* if (R_a^{-1}, R_aL_a, R_a) is an autotopism, *i.e.*, if $(xa \cdot y)a = x(a \cdot ya)$, *i.e.*, if a is (D2).

Proposition 3.3. *For an element a of a loop L, any two of the following imply the third: (i) a is a middle Moufang element, (ii) a is a left Moufang element, (iii) a is a right Moufang element.*

Proof. Each of the three conditions implies a is a flexible element, that is, $L_aR_a = R_aL_a$. Using this, observe that

$$(L_a, R_a, R_aL_a)^{-1}(L_aR_a, L_a^{-1}, L_a)(R_a^{-1}, R_aL_a, R_a) = (\mathrm{id}_L, \mathrm{id}_L, \mathrm{id}_L)\,.$$

Thus if any two of these triples is an autotopism, so is the third. □

We denote the set of all left Moufang elements $\mathrm{M}_\lambda(L)$; $\mathrm{M}_\mu(L)$ and $\mathrm{M}_\rho(L)$ are defined analogously. None of these is necessarily a subloop, as we shall see in section 5. We are now ready to give a new definition of Moufang element.

Definition 3.4. An element a in a loop L is called a *Moufang element* if it is a left, a middle, and a right Moufang element. We call the set of all Moufang elements of L the *Moufang core of L*, and we denote it by $\mathrm{M}(L)$; that is, $\mathrm{M}(L) = \mathrm{M}_\lambda(L) \cap \mathrm{M}_\mu(L) \cap \mathrm{M}_\rho(L)$; *cf.* the definition of nucleus. We call $\mathrm{M}_\lambda(L)$ the *left Moufang core*, $\mathrm{M}_\mu(L)$ the *middle Moufang core*, and $\mathrm{M}_\rho(L)$ the *right Moufang core*.

The next theorem, together with the facts that this definition is expressible entirely via autotopisms, and moreover, that it uses *all* autotopisms of this form, suggests that ours is the right definition of Moufang element.

Theorem 3.5. *Let L be an arbitrary loop; then* $\mathrm{M}(L)$ *is a subloop.*

Proof. We show that $\mathrm{M}(L)$ is closed under multiplication. Fix $a, b \in \mathrm{M}(L)$. We freely use the fact that a,b are flexible in what follows.

$$\begin{aligned}
[a(bx \cdot ab) \cdot y]b &= [(a \cdot bx \cdot a)b \cdot y]b \\
&= (a \cdot bx \cdot a) \cdot byb \\
&= a[bx \cdot (a \cdot byb)] \\
&= a[bx \cdot (ab \cdot y)b] \\
&= a[b \cdot x(ab \cdot y) \cdot b] \\
&= (ab \cdot x(ab \cdot y))b\,.
\end{aligned}$$

Canceling b's, we have

$$a(bx \cdot ab) \cdot y = ab \cdot x(ab \cdot y)\,. \tag{3}$$

Set $y = 1$ to get

$$a(bx \cdot ab) = ab \cdot (x \cdot ab)\,. \tag{4}$$

Apply (4) to (3) to obtain

$$[ab \cdot (x \cdot ab)] \cdot y = ab \cdot x(ab \cdot y)\,,$$

i.e., ab is a left Moufang element.

Next, starting with (4), we have

$$\begin{aligned}
ab \cdot (xy \cdot ab) &= a[(b \cdot xy) \cdot ab] \\
&= a[b(xy \cdot a)b] \\
&= a[b\,\{((x/a)a \cdot y)a\}\,b] \\
&= a[b\,\{(x/a) \cdot aya\}\,b] \\
&= a[b(x/a) \cdot (aya \cdot b)] \\
&= a[b(x/a) \cdot a(y \cdot ab)] \\
&= (a \cdot b(x/a) \cdot a)(y \cdot ab) \\
&= (ab \cdot (x/a)a)(y \cdot ab) \\
&= (ab \cdot x)(y \cdot ab)\,.
\end{aligned}$$

Thus, ab is a middle Moufang element. Finally, by Proposition 3.3, ab is also a right Moufang element, and so $\mathrm{M}(L)$ is closed under multiplication.

Now, assume a is in $\mathrm{M}(L)$. By Lemma 2.15, a has a two-sided inverse, a^{-1}. Finally, it is easy to show that a^{-1} is in $\mathrm{M}(L)$. Thus, by Theorem 4.2 in [14], $\mathrm{M}(L)$ is a subloop. □

Next, we prove a useful technical lemma.

Lemma 3.6. *If a is a left, middle or right Moufang element in a loop L, then a is an inverse property element, that is, $L_a^{-1} = L_{a^{-1}}$ and $R_a^{-1} = L_{a^{-1}}$.*

Proof. By Lemma 2.15 we have

$$a^{-1} \cdot ya \cdot a^{-1} = a^{-1}y \cdot aa^{-1} = a^{-1}y \ .$$

Canceling a^{-1}'s we have $ya \cdot a^{-1} = y$. The left inverse property is proved similarly. □

The next theorem is important especially insofar as it encompasses Flora's result, mentioned above, about $(A2)$ elements in inverse property loops (we state this explicitly in the corollary).

Theorem 3.7. *In a left inverse property loop or a right inverse property loop* L*,* $\mathrm{M}_\mu(L) = \mathrm{M}_\lambda(L) = \mathrm{M}_\rho(L)$.

Proof. Let L be a left inverse property loop. If (f, g, h) is an autotopism, then so is (f^J, h, g) where $J : L \to L; x \to x^{-1}$ is the inversion mapping. So if a is a middle Moufang element, then (L_a^J, R_aL_a, R_a) is an autotopism. Thus, for all $x \in L$, $xL_a^J \cdot a^{-1}R_aL_a = (xa^{-1})R_a$, that is, $xL_a^J \cdot a = xa^{-1} \cdot a$, and so $xL_a^J = xR_{a^{-1}}$. This, together with the preceding lemma assures us that (R_a^{-1}, R_aL_a, R_a) is an autotopism, and so a is a right Moufang element. The reverse inclusion is proved similarly, and so $\mathrm{M}_\mu(L) = \mathrm{M}_\rho(L)$. The rest follows from Proposition 3.3. The proof for right inverse property loops is dual. □

Corollary 3.8. *In a left inverse property loop or a right inverse property loop, the set of* $(A2)$ *elements forms a subloop.*

Proof. Combine Theorem 3.5 and Theorem 3.7. □

The Moufang core is a genuine generalization of the nucleus, as the next example shows.

Example 3.9. In this loop, 1 is in $\mathrm{M}(L)$, but 1 is not nuclear, since $1\cdot(2\cdot2) = 5 \neq 6 = (1 \cdot 2) \cdot 2$. Since the smallest nonassociative Moufang loop has order 12 [3], $\mathrm{M}(L)$ in this example is associative.

0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	4	5	6	7	0	1
3	2	6	7	0	1	5	4
4	6	5	0	7	2	1	3
5	7	0	6	1	3	4	2
6	4	7	1	2	0	3	5
7	5	1	4	3	6	2	0

Example 3.10. The smallest loop, L, in which $\mathrm{M}(L)$ is not associative, has order 36. In this loop, $\mathrm{M}(L)$ is the twelve element nonassociative Moufang loop. Moreover, $\mathrm{M}(L)$ is not normal in L. We note further that L has the inverse property, it is not alternative, nor is it flexible, and all three of its nuclei, as well as its commutant, are trivial. Its multiplication table may be found here [13].

For a further discussion of Moufang elements and related topics, see [5] and [8].

4. Divisible Moufang Groupoids

Recall that a *quasigroup* is a set with three binary operations $\cdot$, $/$, $\backslash$ that satisfy the following four identities:

$$x \cdot (x \backslash y) = y, \quad (y/x) \cdot x = y, \quad x \backslash (x \cdot y) = y, \quad (y \cdot x)/x = y.$$

A groupoid satisfying the last two of these four identities is called a *cancellative* groupoid, since its multiplication is both right and left cancellative. A groupoid that satisfies the first two of these four identities is called a *divisible* groupoid, since each element is expressible as a product.

In [9] Kunen showed that a quasigroup satisfying any one of $(A), (B), (C)$, or (D), is a Moufang loop. We offer a global generalization of this result in the following theorem.

Theorem 4.1. *A divisible groupoid satisfying any one of (A), (B), (C), or (D), is a Moufang loop.*

Proof. [13]. □

Problem 4.2. *Find a (necessarily infinite) example that shows the analogous result for cancellative groupoids does not hold.*

Now consider Kunen's result recast in a slightly different form: *a quasigroup satisfying any one of* $(A), (B), (C)$, *or* (D), *has a 2-sided identity element.* We offer a local generalization of Kunen's result. By way of preparation, we give the following definition.

Definition 4.3. An element a in a groupoid L is called an *(A)-Moufang element* if it satisfies all three (A) identies, e.g., $(A2), (A1x)$, and $(A1y)$. *(B)-Moufang, (C)-Moufang*, and *(D)-Moufang* elements are defined analogously.

Theorem 4.4. *Let L be a groupoid containing an element a that is either:*

1. *(A)-Moufang and such that L_a bijects and R_a is either onto or 1-1, or*
2. *(C)-Moufang and such that L_a and R_a are both onto and such that $L_a L_a = L_{a^2}$.*

Then L has a two-sided identity element. (There are, of course, mirror statements for (B) and (D)).

Proof. [13]. □

Lest the left alternative condition in part (2) of the previous theorem appear superfluous, we note that in the following example, which does not have a two-sided inverse, 1 is a (C)-Moufang element, and both R_1 and L_1 are onto, but $L_1 L_1 \neq L_{1^2}$.

Example 4.5.

$$\begin{matrix} 0 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{matrix}$$

5. Miscellanea

Our new definition requires that a Moufang element satisfy the four conditions $(A2), (B2), (C2)$, and $(D2)$. It's natural to ask about elements that satisfy all 12 conditions.

Lemma 5.1. *A loop L containing an element a that satisfies (A2), (A1x), (A1y), (B2), (B1x), (B1y), (C2), (C1x), (C1y), (D2), (D1x), and (D1y) must be flexible and alternative.*

Proof.

$$\begin{aligned} xy \cdot x &= x[a \cdot (a\backslash y)] \cdot x \\ &= xa \cdot [(a\backslash y) \cdot x] \\ &= x \cdot [a \cdot (a\backslash y)]x \\ &= x \cdot yx \end{aligned}$$

Thus, L is flexible. (Note, we used only $(A1x)$ and $(B1x)$, as well as the fact that $y = a \cdot (a\backslash y)$, to establish flexibility.)

For left alternativity, we first note that by Lemma 2.15 we have

$$a^{-1} \cdot ya \cdot a^{-1} = a^{-1}y \cdot aa^{-1} = a^{-1} \cdot y\ .$$

Canceling a^{-1}'s we have $ya \cdot a^{-1} = y$. Now, let $y = x/a$ to obtain

$$xa^{-1} = x/a\ . \tag{5}$$

Next, note that

$$\begin{aligned} (x \cdot [x/a])a &= a\backslash[a \cdot (x[x/a]) \cdot a] \\ &= a\backslash[ax \cdot (x/a)a] \\ &= a\backslash[ax \cdot x] \\ &= a\backslash[(a \cdot (x/a) \cdot a)x] \\ &= a\backslash[a(x/a \cdot ax)] \\ &= x/a \cdot ax \\ &= xa^{-1} \cdot ax \\ &= x[a^{-1}a \cdot x] \\ &= xx \end{aligned}$$

where the seventh equality comes from (5). We have thus derived

$$xx = (x \cdot [x/a])a\ . \tag{6}$$

Now, note that

$$\begin{aligned}(x \cdot xy)a &= [(x/a) \cdot a \cdot xy]a \\ &= (x/a) \cdot a(xy \cdot a) \\ &= (x/a) \cdot (ax \cdot ya) \\ &= (x/a) \cdot (a[(x/a) \cdot a] \cdot ya) \\ &= (x/a) \cdot (a \cdot [(x/a) \cdot (a \cdot ya)]) \\ &= ([(x/a) \cdot a) \cdot (x/a)) \cdot (a \cdot ya) \\ &= (x \cdot [x/a]) \cdot (a \cdot ya) \\ &= ([x \cdot (x/a)]a \cdot y)a \\ &= (xx \cdot y)a\end{aligned}$$

where the last equality is obtained by (6). Now cancel a's to get the left alternative law. The right alternative law is proved similarly. □

In flexible, alternative loops, the first three of these conditions imply the others:

Lemma 5.2. *If an element a in a flexible, alternative loop is an (A)-Moufang element, then it is also satisfies (B2), (B1x), (B1y), (C2), (C1x), (C1y), (D2), (D1x), and (D1y).*

Proof. [13]. □

In section 2, we gave an example of minimal order that showed that the set of all elements satisfying $(A2)$—and recall again that $(A2)$ is the traditional definition of Moufang element—in an arbitrary loop need not form a subloop (recall that the loop had order 12). Here, we complete this analysis for the remaining 10 local Moufang laws.

Example 5.3. Here is an example of a loop of minimal order in which the set of all $(A1x)$ elements does not form a subloop. In this example, 1 and 2 are $(A1x)$ elements but $1{\cdot}2$ is not, since $5{\cdot}(((1{\cdot}2){\cdot}0){\cdot}5) = 4 \neq 3 = (5{\cdot}(1{\cdot}2)){\cdot}(0{\cdot}5)$.

0	1	2	3	4	5	6	7	8	9
1	2	3	4	0	6	7	8	9	5
2	3	4	0	1	7	8	9	5	6
3	4	0	1	2	8	9	5	6	7
4	0	1	2	3	9	5	6	7	8
5	6	7	9	8	0	1	2	4	3
6	7	8	5	9	1	2	4	3	0
7	8	9	6	5	2	4	3	0	1
8	9	5	7	6	4	3	0	1	2
9	5	6	8	7	3	0	1	2	4

Example 5.4. Here is an example of a loop of minimal order in which the set of all $(A1y)$ elements does not form a subloop. In this example, 1 and 2 are $(A1y)$ elements but $1{\cdot}2$ is not, since $4{\cdot}((4{\cdot}(1{\cdot}2)){\cdot}4) = 6 \neq 5 = (4{\cdot}4){\cdot}((1{\cdot}2){\cdot}4)$.

0	1	2	3	4	5	6	7
1	3	0	2	5	7	4	6
2	0	3	1	6	4	7	5
3	2	1	0	7	6	5	4
4	6	5	7	1	3	0	2
5	4	7	6	0	1	2	3
6	7	4	5	3	2	1	0
7	5	6	4	2	0	3	1

Example 5.5. Here is an example of a loop of minimal order in which the set of all $(C2)$ elements does not form a subloop. In this example, 1 and 2 are $(C2)$ elements but $1 \cdot 2$ is not, since $(1 \cdot 2) \cdot (0 \cdot (((1 \cdot 2) \cdot) \cdot 4)) = 5 \neq 4 = (((1 \cdot 2) \cdot 0) \cdot ((1 \cdot 2) \cdot)) \cdot 4$.

0	1	2	3	4	5	6	7	8	9	10	11
1	0	3	2	5	4	8	9	6	7	11	10
2	3	0	1	6	8	4	10	5	11	7	9
3	2	1	0	7	9	10	5	11	4	8	6
4	5	6	8	9	7	11	1	10	0	3	2
5	4	7	9	8	6	0	11	1	10	2	3
6	7	4	10	11	1	9	2	3	8	0	5
7	6	5	11	10	0	3	4	9	2	1	8
8	9	10	4	1	11	7	3	2	5	6	0
9	8	11	5	0	10	2	6	7	3	4	1
10	11	8	6	2	3	5	0	4	1	9	7
11	10	9	7	3	2	1	8	0	6	5	4

Example 5.6. Here is an example of a loop of minimal order in which the set of all $(C1x)$ elements does not form a subloop. In this example, 1 and 2 are $(C1x)$ elements but $1{\cdot}2$ is not, since $6{\cdot}((1{\cdot}2){\cdot}(6{\cdot}0)) = 3 \neq 4 = ((6{\cdot}(1{\cdot}2)){\cdot}6){\cdot}0$.

0	1	2	3	4	5	6	7	8	9	10	11
1	0	3	2	5	4	7	6	9	8	11	10
2	4	0	5	1	3	8	11	6	10	9	7
3	5	1	4	0	2	9	10	7	11	8	6
4	2	5	0	3	1	11	8	10	6	7	9
5	3	4	1	2	0	10	9	11	7	6	8
6	7	8	9	11	10	0	1	2	3	5	4
7	6	11	10	8	9	1	0	4	5	3	2
8	9	6	7	10	11	2	3	0	1	4	5
9	8	10	11	6	7	4	5	1	0	2	3
10	11	9	8	7	6	5	4	3	2	0	1
11	10	7	6	9	8	3	2	5	4	1	0

Example 5.7. Here is an example of a loop of minimal order in which the set of all $(C1y)$ elements does not form a subloop. In this example, 1 and 2 are $(C1y)$ elements but $1{\cdot}2$ is not, since $6{\cdot}(0{\cdot}(6{\cdot}(1{\cdot}2))) = 2 \neq 1 = ((6{\cdot}0){\cdot}6){\cdot}(1{\cdot}2)$.

0	1	2	3	4	5	6	7	8	9	10	11
1	4	3	0	5	2	7	11	6	8	9	10
2	3	4	5	0	1	9	8	10	11	7	6
3	0	5	2	1	4	8	6	9	10	11	7
4	5	0	1	2	3	11	10	7	6	8	9
5	2	1	4	3	0	10	9	11	7	6	8
6	7	9	8	11	10	4	5	2	0	3	1
7	11	8	6	10	9	0	2	4	1	5	3
8	6	10	9	7	11	1	3	0	4	2	5
9	8	11	10	6	7	5	1	3	2	0	4
10	9	7	11	8	6	3	0	1	5	4	2
11	10	6	7	9	8	2	4	5	3	1	0

The (B)'s are mirrors of the (A)'s, and the (D)'s are mirrors of the $(C)'s$, so the remaining six (five, if we omit (B2)) minimal models are the opposite loops of these six.

Problem 5.8. *Are there any loops of odd order such that the set of (A2) elements does not form a subloop? Of course, there is the same question for (A1x), (A1y), etc.*

We recall a classic result about nuclei in quasigroups; see [13] for a proof.

Theorem 5.9. *If the middle nucleus of a quasigroup is nonempty, then the quaisgroup is a loop.*

It is natural, then, to wonder if quasigroups with nontrivial middle Moufang core are loops.

Example 5.10. Here is an example of quasigroup, Q, that is not a loop and with nontrivial middle Moufang core. In this example, 0 is in $\mathrm{M}_\mu(Q)$. This example is of minimal order.

2	3	4	5	0	1	7	8	6
3	2	6	8	7	0	5	1	4
4	6	0	7	2	3	8	5	1
6	8	7	0	3	2	1	4	5
0	1	2	3	4	5	6	7	8
7	5	3	1	6	8	4	0	2
1	0	8	2	5	4	3	6	7
8	7	5	4	1	6	0	2	3
5	4	1	6	8	7	2	3	0

For the sake of completeness, and in preparation for the next theorem, we note that the same is true of quasigroups with nontrivial left or right Moufang cores, as the next example shows.

Example 5.11. Here is an example of quasigroup, Q, that is not a loop and with nontrivial left Moufang core. In this example, 0 is in $\mathrm{M}_\lambda(Q)$. Of course, in the opposite quasigroup, 0 is in the right Moufang core. Both examples are of minimal order.

$$\begin{matrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{matrix}$$

On the other hand, we do have the following analog of the classic result mentioned above (Theorem 5.9).

Theorem 5.12. *In a quasigroup L, if any of $\mathrm{M}_\mu(L) \cap \mathrm{M}_\lambda(L)$, $\mathrm{M}_\mu(L) \cap \mathrm{M}_\rho(L)$ or $\mathrm{M}_\lambda(L) \cap \mathrm{M}_\rho(L)$ are nonempty, then L is a loop.*

Proof. [13]. □

6. An Application: A-elements

A loop is called an *A-loop* if all of its inner mappings are automorphisms. The most prominent examples of A-loops are groups and commutative Moufang loops [2]. In a series of papers from the 1950's, beginning with [2], R.H. Bruck and L.J. Paige developed a provocative line of research detailing the similarities between two important clases of loops: the inverse property A-loops and the Moufang loops. Though they did not publish any classification theorems, in 1958, Bruck's colleague, J.M. Osborn, managed to show that diassociative, commutative A-loops are Moufang [15]. The general problem, though, remained open until 2002, when Kinyon, Kunen, and the present author showed that inverse proprety A-loops are Moufang [6]. Here, we offer a local generalization of this result.

Definition 6.1. We will call an element a in a loop L an *A-element* if, for each x in L the following are automorphisms: $L(x, a), L(a, x), R(a, x), R(x, a)$, and $T(a)$.

Theorem 6.2. *If a is an A-element in an inverse property loop, then a is a Moufang element.*

Proof. [13]. □

The proof of the previous theorem is simplified by the following lemma.

Lemma 6.3. *An element a in an inverse property loop L is an A-element if $T(a)$ is an automorphism, and if any one of the following four is an automorphism (for all x, of course): $L(x, a), L(a, x), R(a, x), R(x, a)$.*

Proof. [13]. □

We end with an example that shows that the previous theorem is a genuine generalization of the main result in [6].

Example 6.4. In this inverse property loop, 1 is a flexible, A-element, but the loop is not an A-loop, since $R(2,4)$ is not an automorphism (for instance, $(2\cdot 4)R(2,4) = 7 \neq 6 = 2\cdot 4 = 2R(2,4)\cdot 4R(2,4)$). This example is of minimal order.

0	1	2	3	4	5	6	7	8	9	10	11
1	0	3	2	5	4	7	6	9	8	11	10
2	3	0	1	6	7	4	5	10	11	8	9
3	2	1	0	7	6	5	4	11	10	9	8
4	5	6	7	8	9	11	10	0	1	2	3
5	4	7	6	9	8	10	11	1	0	3	2
6	7	4	5	11	10	9	8	2	3	0	1
7	6	5	4	10	11	8	9	3	2	1	0
8	9	10	11	0	1	2	3	4	5	7	6
9	8	11	10	1	0	3	2	5	4	6	7
10	11	8	9	2	3	0	1	7	6	5	4
11	10	9	8	3	2	1	0	6	7	5	4

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.

[2] R.H. Bruck and L.J. Paige, Loops whose inner mappings are automorphisms, *Ann. Math.* **63**(2) (1956) 308–232.

[3] O. Chein, Moufang Loops of Small Order I, *Trans. Amer. Math. Soc.* **188** (1974), 31–51.

[4] I.A. Florja, Loops with one-sided invertibility. (Russian. Moldavian summary) *Bul. Akad. Štiince RSS Moldoven.* 1965 no. 7, 68–79.

[5] M.K. Kinyon and K. Kunen, Power-associative, conjugacy closed loops *J. of Algebra* 304 (2006), 679–711.

[6] M.K. Kinyon, K. Kunen, and J.D. Phillips, Every diassociative A-loop is Moufang *Proc. Amer. Math. Soc.* 17 130 (2002), 619624.

[7] M.K. Kinyon and J.D. Phillips, Commutants of Bol loops of odd order, *Proc. Amer. Math. Soc.*, **132** (2004), 617–619.

[8] M.K. Kinyon and P. Vojtěchovský, Primary decompositions in varieties of commutative diassociative loops, *Communications in Algebra*, to appear.

[9] K. Kunen, Moufang quasigroups *Journal of Algebra*, **183** (1996) no. 1, 231–234.

[10] W. W. McCune, *Prover9*, automated reasoning software, and *Mace4*, finite model builder, Argonne National Laboratory, 2005. `http://www.prover9.org`

[11] W.W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag, 1996.

[12] H. Pflugfelder, *Quasigroups and Loops, Introduction*, Helderman-Verlag, 1990.

[13] J.D. Phillips, `http://persweb.wabash.edu/facstaff/phillipj/research.html`

[14] J.D. Phillips and P. Vojtěchovský, A scoop from groups: new equational foundations for loops, *Commentationes Mathematicae Universitatis Carolinae*, **49 (3)**, (2008), 279–290.

[15] J.M. Osborn, A theorem on A-loops, *Proc. Amer. Math. Soc.* **9** (1959) 347–349.

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, Indiana 47933, U.S.A.

E-mail address: `phillipj@wabash.edu`