Journal of the Nigerian Association of Mathematical Physics
Volume 55 **(February *2020 Issue*), pp1 – 6**

THE EQUIVALENCE OF THE MOUFANG IDENTITIES: A SIMPLIFIED PROOF

G. G. Zaku and L.A. Ademola

Department of Mathematics, University of Jos, Jos, Nigeria.

Abstract

A Moufang loop $\langle M, \cdot \rangle$ ***is defined as a loop that satisfies any one of identities:*** $xy \cdot zx = (x \cdot yz)x$, $xy \cdot zx = x(yz \cdot x)$, $(xy \cdot z)y = x(y \cdot zy)$ ***or*** $x(y \cdot xz) = (xy \cdot x)z$. ***This definition assumes the equivalence of these identities. The known proofs of the equivalence are cumbersome as they require additional knowledge about autotopism and hence additional definitions about mappings come into play. In this paper we provide an elegant alternative proof of the equivalence-a proof that mainly uses clever manipulation of the Moufang identities as well as the basic definitions of quasigroups, loops and the identity element.***

Keywords: Moufang, loop, identity

1. Introduction and Definitions

Moufang loops were first introduced by the German mathematician Ruth Moufang in her paper [1]. She originally presented loops that satisfied the identity $(x \cdot yx)z = x(y \cdot xz)$. She also wrote about loops that satisfied the identities: $xy \cdot zx = x(yz \cdot x), (xy \cdot x)z = x(y \cdot xz)$ and $(xy \cdot z)y = x(y \cdot zy)$; and proved the equivalence of three of these identities. However, she gave a separate definition for loops that satisfy the identity $xy \cdot zx = x(yz \cdot x)$. Bruck, R. H. [2] however proved that all of these identities were equivalent. These identities were later referred to as the Moufang Identities. Hence the loops that satisfied any one of these (equivalent) identities could be simply called Moufang loops.

Original definition of Moufang loops talk about quasigroups and loops but the proof of the equivalency of the Moufang identities provided by Bruck brought in additional concepts such as autotopism. To study Moufang loops one needs to have a proper grasp of these identities and the fact that they are all equivalent. Hence, the need to also be at home with the proof of their equivalence. We tried reading the works of others who have also proved the equivalence of these identities and noticed that each of them also made use of autotopism. For example, Pflugfelder, H. O. in her book [3] also provided the proof for the equivalence of these Moufang's identities but by still using autotopism [see page 90, line 19]. Also, Drapal, A. in his work [4] again provided proof for the equivalence of the Moufang identities. But going through the work one discovers that it made use of the traditional style of using autotopism to prove it [see page 97, line 34].

Thus, from available literatures on this topic, the proofs for the equivalence of these Moufang identities use autotopism. On the one hand the study of autotopism can produce many new results about loops but the concept itself can be daunting to a novice. Now, given the fact that these identities and the proof of their equivalence serves as a gate way into the study of Moufang loops, we decided to find a proof that is more direct, easy to understand and devoid of autotopism; making use of only basic properties of quasigroups and loops. Thus, it is our goal to make the study of Moufang loops more attractive and appealing to young mathematicians right from the entrance.

Hence, the purpose of this work is to show that the proof can be done in a straightforward algebraic manner which is easy to follow and understand.

We begin by giving some basic definitions of terms and concepts that we will be using in the work.

Definition 1.1. Let M be a non-empty set. A function from $M \times M$ to M is defined as a binary operation on M .If "$\cdot$" is a binary operation on M then $\langle M, \cdot \rangle$ is defined as binary system. Moreover, if "$\cdot$" maps $(x, y) \in M \times M$ to $z \in M$, then we write $x \cdot y = z$ or sometimes, merely as $xy = z$ if the binary operation used is already obvious and clear.

Definition 1.2.A binary system $\langle M, \cdot \rangle$ is said to have:

Corresponding Author**:** Zaku G.G., Email: garbazaku@gmail.com, Tel: +2348036020165, +2348163833611 (LAA)

(a) a left identity element $e_L \in M$ if $e_L \cdot x = x, \forall\, x \in M$;
(b) a right identity element $e_R \in M$ if $x \cdot e_R = x, \forall\, x \in M$;
(c) an identity element $e \in M$ if $e \cdot x = x \cdot e = x, \forall\, x \in M$.

Definition 1.3. Let $\langle M, \cdot \rangle$ be a binary system with an identity element e. An element $y \in M$ is said to be an inverse of the element $x \in M$ if $x \cdot y = y \cdot x = e$. If $x \in M$ has a unique inverse, we can denote the inverse element as x^{-1}.

Definition 1.4. Let $\langle M, \cdot \rangle$ be a binary system and $a, b \in M$. Then $\langle M, \cdot \rangle$ is defined as a quasigroup if there exist unique (not necessarily distinct) elements $x, y \in M$ such that $a \cdot x = b$ and $y \cdot a = b$. Note: It is common to denote $x = a \backslash b$ and $y = b / a$, where " \ " and " / " are called the left and right divisions respectively and in fact are also binary operations on M. So, we can also denote a quasigroup as $\langle M, \cdot, \backslash, / \rangle$, that is, a non-empty set M with the three binary operations.

Definition 1.5.A quasigroup $\langle M, \cdot, \backslash, / \rangle$, that has an identity element is called a loop. However, we shall merely use the notation $\langle M, \cdot \rangle$ for a loop.

Definition 1.6.A Moufang loop is a loop $\langle M, \cdot \rangle$ that satisfies the identity $xy \cdot zx = (x \cdot yz)x$ for all $x, y, z \in M$.Note that for brevity, while writing the product of many elements, we shall omit writing the binary operation and parentheses if no confusion arises and accept that juxtaposition precedes ' $\cdot$ ' which then precedes parentheses. For example, $x \cdot (y \cdot (x \cdot z))$ will be written as $x(y \cdot xz)$ and this means first compute xz, then multiply y on its left, and again multiply x on the left of the element $y \cdot xz$.

2. Results

Though our main objective is to prove the equivalence of the Moufang identities by using purely algebraic methods, the proof involves establishing several other (well-known) properties of Moufang loops as well. This includes the property of left and right cancellation laws, associativity between any two elements; existence of a (unique) inverse element for every element and the inverse property. In proving these properties, we stick to our first objective of proving them using simple and direct algebraic methods. This ensures that our work is as self-contained as possible.

In the following theorems, various properties of loops that satisfy any one of the following (Moufang) identities are obtained. So, in the statement of Lemmas 2.3, 2.4, 2.5, 2.6 and Theorem 2.7, these are the identities that are referred to:

$$xy \cdot zx = (x \cdot yz)x \quad (1)$$

$$(xy \cdot z)y = x(y \cdot zy) \quad (2)$$

$$x(y \cdot xz) = (xy \cdot x)z \quad (3)$$

Lemma 2.1(Left and right cancellation laws): Let $\langle M, \cdot \rangle$ be a quasigroup and $x, y, z \in M$. Then $\langle M, \cdot \rangle$ satisfies the left and right cancellation laws, that is, $x \cdot y = x \cdot z \Rightarrow y = z$ (LCL); and $x \cdot y = z \cdot y \Rightarrow x = z$ (RCL) respectively.

Proof: The proof is a direct consequence of the definition of a quasigroup.

Proposition 2.2. A binary system that contains both left and right identities contains a unique identity element which is the unique left identity and right identity element of the system.

Proof: The proof of this proposition is extremely simple-merely using Definition 1.2, $e_R = e_L \cdot e_R = e_L$ by (a) and (b) $\Rightarrow e = e_L = e_R$ by (c).

Lemma 2.3 (Associativity of two elements):

Let $\langle M, \cdot \rangle$ be a loop. Suppose M satisfies any one ofthe three Moufang identities (1), (2) or (3).Then for any two elements $x, y \in M$:

(a) $x \cdot yx = xy \cdot x$

(b) $x \cdot xy = xx \cdot y$

(c) $y \cdot xx = yx \cdot x$

[NOTE: The identity in (a) is called the flexible identity; in (b), the left alternative identity; and (c), the right alternative identity.]

Proof:

Case 1: Suppose (1) holds, that is, $xy \cdot zx = (x \cdot yz)x \quad \forall\, x, y, z \in M$.

Since $x, y, 1 \in M$, $x1 \cdot yx = (x \cdot 1y)x$ by (1).

$\Rightarrow \quad x \cdot yx = xy \cdot x$, which proves(a).

Since $x, y \in M$, by the quasigroup property, $\exists\ u \in M$ such that $xu = y$.

Now $xu \cdot xx = (x \cdot ux)x$ by (1)

$= (xu \cdot x)x$ by (a).

$\Rightarrow \quad y \cdot xx = yx \cdot x$ which proves (c).

Similarly, for $x, y \in M$, $\exists\ v \in M$ such that $vx = y$.

Now $xx \cdot vx = (x \cdot xv)x$ by (1)

$= x(xv \cdot x)$ by (a)

$= x(x \cdot vx)$ by (a) again.

$\Rightarrow \quad xx \cdot y = x \cdot xy$, which proves (b).

Case 2: Suppose (2.2) holds, that is, $(xy \cdot z)y = x(y \cdot zy) \quad \forall\ x, y, z \in M$.

Then $(1x \cdot y)x = 1(x \cdot yx)$ by (2) since $1, x, y \in M$. So $xy \cdot x = x \cdot yx$ which proves (a).

Now $(xx \cdot y)x = x(x \cdot yx)$ by (2)

$= x(xy \cdot x)$ by (a)

$= (x \cdot xy)x$ by (a) again.

By RCL, we get $xx \cdot y = x \cdot xy$ .This proves(b).

Similarly, $(yx \cdot 1)x = y(x \cdot 1x)$ by (2.2) and this implies that $yx \cdot x = y \cdot xx$ which proves(c).

Case 3: Suppose (3) holds, that is, $x(y \cdot xz) = (xy \cdot x)z \quad \forall\ x, y, z \in M$.

$\Rightarrow x(y \cdot x1) = (xy \cdot x)1$ by (3) and $\Rightarrow x \cdot yx = xy \cdot x$. This proves (a).

Also $x(1 \cdot xy) = (x1 \cdot x)y$ by (3) since $x, 1, y \in M$. $\Rightarrow\ x \cdot xy = xx \cdot y$

which proves (b).

Again $x(y \cdot xx) = (xy \cdot x)x$ by (3)

$= (x \cdot yx)x$ by(a)

$= x(yx \cdot x)$ by (a).

By LCL, $y \cdot xx = yx \cdot x$ which proves (c). This completes the proof of Lemma 2.3.

Lemma 2.4 (Inverse Element): Let M be a loop that satisfies any one of the three Moufang identities(1), (2) or (3).Then every element in M has a (unique) inverse element in the loop.

Proof: Let $\ell \in M$. By the definition of loops, M contains 1, a unique identity element. Since M is a quasigroup, there exist unique elements $u, v \in M$ such that:

$u\ell = 1$ (4)

and

$\ell v = 1$ (5).

We prove this lemma by showing that there exist a unique left and right inverse element for any element in M, and then proving that these two are equal.

Case 1: Suppose (1) holds, that is, $xy \cdot zx = (x \cdot yz)x \quad \forall\ x, y, z \in M$.

Now, since $u, \ell, v \in M$,

$v \cdot \ell v = v\ell \cdot v$ by Lemma 2.3(a)

$= v\ell \cdot 1v$

$= v\ell(u\ell \cdot v)$ by (4)

$= [v(\ell u \cdot \ell)]v$ by (1)& Lemma 2.3(a)

$= (v \cdot \ell u)(\ell v)$ by (1)

$= (v \cdot \ell u)1 = v \cdot \ell u$ by (5).

So $v \cdot \ell v = v \cdot \ell u$.

Using the LCL twice, we get $v = u$. So $u = v = \ell^{-1}$.

Case 2: Assume (2.2) holds, that is, $(xy \cdot z)y = x(y \cdot zy) \quad \forall\, x, y, z \in M$.

Now: $v\ell = (1 \cdot v)\ell = (u\ell \cdot v)\ell$ by (4)

$= u(\ell \cdot v\ell)$ by (2)

$= u(\ell v \cdot \ell)$ by Lemma 2.3(a)

$= u(1 \cdot \ell) = u\ell$ by (5).

Thus $v\ell = u\ell$. By RCL, $v = u$. Thus $u = v = \ell^{-1}$.

Case 3: Suppose (2.3) holds, that is, $x(y \cdot xz) = (xy \cdot x)z \quad \forall\, x, y, z \in M$.

Now: $\ell u = \ell(u \cdot 1) = \ell(u \cdot \ell v)$ by (5)

$= (\ell u \cdot \ell)v$ by (3)

$= (\ell \cdot u\ell)v$ by Lemma 2.3(a)

$= (\ell \cdot 1)v = \ell v$ by (4).

That is $\ell u = \ell v$. By LCL, $u = v$. Thus $u = v = \ell^{-1}$.This completes the proof of Lemma 2.4.

Lemma 2.5 (Inverse Property):A loop *M* that satisfies any one of the three Moufang identities(1), (2) or (3)has the following properties:

(a) $y^{-1} \cdot yx = x$ (left inverse property) and

(b) $xy \cdot y^{-1} = x$ (right inverse property) for every $x, y \in M$.

Proof: Let $\ell \in M$. By Lemma 2.4, there exists a unique element $\ell^{-1} \in M$ such that

$\ell \cdot \ell^{-1} = \ell^{-1} \cdot \ell = 1$ (6).

Case 1: Suppose M satisfies (1), that is, $xy \cdot zx = (x \cdot yz)x \quad \forall\, x, y, z \in M$.

Now: $(y \cdot y^{-1}x)y = yy^{-1} \cdot xy$ by (1)

$= 1 \cdot xy = xy$ by (6).

Thus $(y \cdot y^{-1}x)y = xy$. By RCL, $y \cdot y^{-1}x = x$. This proves (a).

Similarly:

$y(xy^{-1} \cdot y) = (y \cdot xy^{-1})y$ by Lemma 2.3(a)

$= yx \cdot y^{-1}y$ by (1)

$= yx \cdot 1 = yx$ by (6).

So $y(xy^{-1} \cdot y) = yx$ .By LCL, $xy^{-1} \cdot y = x$, which proves (b).

Case 2: Assume (2) is true, that is, $(xy \cdot z)y = x(y \cdot zy) \quad \forall\, x, y, z \in M$.

So: $(xy \cdot y^{-1})y = x(y \cdot y^{-1}y)$ by (2)

$= x(y \cdot 1) = xy$ by (6).

By RCL, $xy \cdot y^{-1} = x$. This proves (b).

For $x, y \in M$, there exist $u \in M$ such that $uy = x$. Then we have:

$y^{-1}(y \cdot uy) = (y^{-1}y \cdot u)y$ by (2)

$= (1 \cdot u)y = uy$ by (6).

That is $y^{-1}(y \cdot x) = x$, which proves (a).

Case 3: Suppose (3) holds, that is, $x(y\cdot xz)=(xy\cdot x)z \quad \forall\ x,y,z\in M$.

Now: $y(y^{-1}\cdot yx)=(yy^{-1}\cdot y)x$ by (3)

$=(1\cdot y)x=yx$ by (6).

By LCL, $y^{-1}\cdot yx=x$. This proves (a).

Again for $x,y\in M$, there exist $v\in M$ such that $yv=x$ .Then we have:

$(yv\cdot y)y^{-1}=y(v\cdot yy^{-1})$ by (3)

$=y(v\cdot 1)=yv$ by (6).

$\Rightarrow \quad (x\cdot y)y^{-1}=x$, which proves (b).This completes the proof of Lemma 2.5.

Lemma 2.6: Let M be a loop that satisfies any one of the three Moufang identities (1), (2) or (3). Then $(xy)^{-1}=y^{-1}x^{-1} \quad \forall\ x,y\in M$.

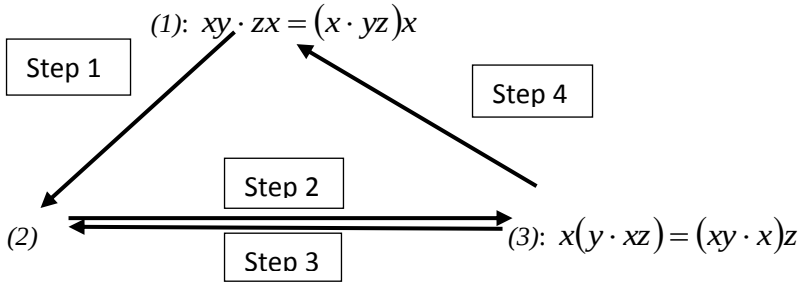
Proof: $(xy)^{-1}=(xy)^{-1}x\cdot x^{-1}$ by Lemma 2.5(b)

$=[(xy)^{-1}(xy\cdot y^{-1})]x^{-1}$ by Lemma 2.5(b) again

$=y^{-1}x^{-1}$ by Lemma 2.5(a).

Theorem 2.7: The threeMoufang identities (1), (2) and (3) are equivalent identities for any loop.

Proof:Let $\langle M,\cdot\rangle$ be a loop. We can prove the equivalence by showing that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). However,to prove that(3) $\Rightarrow$ (1), we need to also use (2). So, we prove in addition that (3) $\Rightarrow$ (2) as well. Hence, our cycle of proof is as shown in the following diagram:



Step 1 [(1) $\Rightarrow$ *(2)]*.

Suppose (1) is true, that is, $xy\cdot zx=(x\cdot yz)x \quad \forall\ x,y,z\in M$.

Now $(xy\cdot z)y=\{z^{-1}[z(xy\cdot z)]\}y$ by Lemma 2.5(a)

$=\{z^{-1}[(z\cdot xy)z]\}y$ by Lemma 2.3(a)

$=[z^{-1}(zx\cdot yz)](yz\cdot z^{-1})$ by (1)&Lemma 2.5(b)

$=z^{-1}[zx\cdot(yz)^2]z^{-1}$ by (1)&Lemma2.3(c)

$=(z^{-1}\cdot zx)[(yz)^2z^{-1}]$ by (1)

$=x[(yz)(yz\cdot z^{-1})]$ by Lemma 2.5(a)&Lemma 2.3(b)

$=x(yz\cdot y)=x(y\cdot zy)$ by Lemma 2.5(b)&Lemma 2.3(a).

Therefore (1) $\Rightarrow$ (2).

Step 2 [(2) $\Rightarrow$ *(3)]*.

Assume (2) is true, that is, $(xy\cdot z)y=x(y\cdot zy) \quad \forall\ x,y,z\in M$. By Lemma 2.4, $\exists\ x^{-1},y^{-1},z^{-1}\in M \quad \forall\ x,y,z\in M$ .Also $(x^{-1})^{-1}=x \quad \forall\ x^{-1}\in M$ since $x\cdot x^{-1}=x^{-1}\cdot x=1$ by (6).

Then $(z^{-1}x^{-1}\cdot y^{-1})x^{-1}=z^{-1}(x^{-1}\cdot y^{-1}x^{-1})$ by (2). (7)

Taking the inverse on both sides of (7)and applying Lemma2.6 we have:

$[(z^{-1}x^{-1}\cdot y^{-1})x^{-1}]^{-1}=[z^{-1}(x^{-1}\cdot y^{-1}x^{-1})]^{-1}$

$\Rightarrow\ x(y\cdot xz)=(xy\cdot x)z$, which is (3). Hence (2) $\Rightarrow$ (3).

*Step 3 [(3) $\Rightarrow$ (2)].*Suppose (3) holds, that is, $x(y\cdot xz)=(xy\cdot x)z \quad \forall\, x,y,z\in M$. By a repeat of the same argument we had in step2 above, we now have:

$y^{-1}(z^{-1}\cdot y^{-1}x^{-1})=(y^{-1}z^{-1}\cdot y^{-1})x^{-1}$ by (3). (8)

Taking the inverse on both sides of (8) and again applying Lemma2.6gives us:

$[y^{-1}(z^{-1}\cdot y^{-1}x^{-1})]^{-1}=[(y^{-1}z^{-1}\cdot y^{-1})x^{-1}]^{-1}$

$\Rightarrow (xy\cdot z)y=x(y\cdot zy)$. And this proves that (3) $\Rightarrow$ (2).

Step 4 [(3)$\Rightarrow$(1)].

$(x\cdot yz)x=[x[y(x\cdot x^{-1}z)]]x$ by Lemma 2.5(a)

$=[(xy\cdot x)\cdot x^{-1}z]x$ by (3)

$=xy\cdot[x(x^{-1}z\cdot x)]$ by (2)

$=xy\cdot[(x\cdot x^{-1}z)x]$ by Lemma 2.3(a)

$=xy\cdot zx$ by Lemma 2.5(a).

Therefore (3) $\Rightarrow$ (1).And this concludes the proof of the theorem.

Corollary 2.8:

All the four Moufang Identities are equivalent. That is

(a) $xy\cdot zx=(x\cdot yz)x$,

(b) $xy\cdot zx=x(yz\cdot x)$,

(c) $(xy\cdot z)y=x(y\cdot zy)$ and

(d) $x(y\cdot xz)=(xy\cdot x)z$ are equivalent identities.

Note that we can call (a) the right middle Moufang identity whereas (b) can be called the left middle Moufang identity; while (c) and (d) are usually called the right and left Moufang identities respectively.

Proof: Let $\langle M,\cdot\rangle$ be a loop that satisfies any of the four Moufang identities. We only need to prove that (a) $\Rightarrow$ (b) and (b) $\Rightarrow$ (a), since by Theorem 2.7; (a), (c) and (d) are equivalent identities.

First suppose M satisfies (a), that is, $xy\cdot zx=(x\cdot yz)x$. Then by Lemma 2.3(a), $(x\cdot yz)x=x(yz\cdot x)$. Hence (a) $\Rightarrow$ (b).

Now suppose M satisfies (b), that is, $xy\cdot zx=x(yz\cdot x)$. Then $xy\cdot 1x=x(y1\cdot x)\Rightarrow xy\cdot x=x\cdot yx$, $\forall\, x,y\in M$. This implies $(x\cdot yz)x=x(yz\cdot x)$ since $x,yz\in M$.Thus $(x\cdot yz)x=x(yz\cdot x)=xy\cdot zx$ by (b). Therefore (b) $\Rightarrow$ (a). Hence the result is complete.

References:

[1] R. Moufang, ZurStruktur von Alternativkörpern, Math. Ann. **110** (1935), 416-430.

[2] R. H. Bruck, A Survey of Binary Systems, Springer-Verlag, New York, 1971.

[3] H. O. Pflugfelder, Quasigroups and Loops: Introduction, Sigma Series in Pure Mathematics 7, Heldermann Verlag Berlin, 1990.

[4] A. Drapal, A Simplified Proof of Moufang's Theorem, Proceedings of the American Mathematical Society, **139(1)** (2010), p93-98.