International Journal of Development Mathematics Vol 2 Issue 3 Page No. 094 - 102

INTERNATIONAL JOURNAL OF DEVELOPMENT MATHEMATICS

ISSN: 3026-8656 (Print) | 3026-8699 (Online)

journal homepage: https://ijdm.org.ng/index.php/Journals

# The Equivalence of the Identities: $p(q \cdot pr) = (pq \cdot p)r$ and $pq \cdot rp = p(qr \cdot p)$

Garba G. Zaku[a]* and Lois A. Ademola[a]

[a]*Department of Mathematics, University of Jos, Jos, Nigeria.*

**ARTICLE INFO**

***Article history:***
Received 10 July 2025
Received in revised form 10 September 2025
Accepted 20 September 2025

**Keywords:**
Moufang loop, identity

**MSC 2020 Subject classification:**
**20N05**

**ABSTRACT**

Moufang loop ⟨L , ·⟩ is defined as a loop that satisfies any one of the identities: pq · rp = (p · qr)p, pq · rp = p(qr · p), (pq · r)q = p(q · rq) or p(q · pr) = (pq · p)r. This definition assumes the equivalence of these identities. We had earlier provided the proof of the equivalence of two of these identities: pq · rp = (p · qr)p and (pq · r)q = p(q · rq) in [5], using simple algebraic method and manipulation. In this paper we continue with our style of proof by providing the proof of the equivalence of another two of these identities: p(q · pr) = (pq · p)r and p(qr · p) = pq · rp

## 1. Introduction

The Moufang loops were introduced by the German mathematician Ruth Moufang in her paper (Moufang, 1935). She proved the equivalence of the identities: $pq \cdot rp = (p \cdot qr)p$, $(pq \cdot r)q = p(q \cdot rq)$, $p(q \cdot pr) = (pq \cdot p)r$ and $pq \cdot rp = p(qr \cdot p)$. Bruck (1971) was the first to prove that all the four identities were equivalent. These identities were later referred to as the Moufang Identities. Thus, loops that satisfied any one of these identities are referred to as Moufang loops.

Bruck (1971); Pflugfelder (1990) and Drapal (2010), all proved the equivalence of these identities using the concept of autotopism. Autotopism is a difficult concept to understand, especially by the new generation mathematics students. So, just as we did in Zaku and Jelten (2023), we here provide an alternative proof for two of these identities: $p(q \cdot pr) = (pq \cdot p)r$ and $p(qr \cdot p) = pq \cdot rp$ using purely basic properties of quasigroups and loops in a straightforward algebraic manner which is easy to follow and understand.

* Corresponding author. Tel.: +2348036020165
E-mail address: garbazaku@gmail.com (Garba Gambo ZAKU)
https://doi.org/10.62054/ijdm/0203.06

We first provide (below) some basic definitions of terms and concepts that we will be used in the work.

## 2. Preliminaries

**Definition 2.1.** Bruck (1971)

Let $L$ be a non-empty set. A function from $L \times L$ to $L$ is defined as a binary operation on $L$. If "$\cdot$" is a binary operation on $L$then $\langle L , \cdot \rangle$ is defined as binary system. In addition, if "$\cdot$" maps $(p, q) \in L \times L$to $r \in L$, then we write $p \cdot q = r$ or sometimes, merely as $pq = r$ where the binary operation used is already obvious and clear.

**Definition 2.2.** Bruck (1971)

A binary system $\langle L , \cdot \rangle$ is said to have:

(a) a left identity element $e_L \in L$ if $e_L \cdot p = p, \forall\, p \in L$;

(b) a right identity element $e_R \in L$ if $p \cdot e_R = p, \forall\, p \in L$;

(c) an identity element $e \in L$ if $e \cdot p = p \cdot e = p, \ \forall\, p \in L$.

**Definition 2.3.** Bruck (1971) Let $\langle L , \cdot \rangle$ be a binary system with an identity element $e$. An element $q \in L$ is said to be an inverse of the element $p \in L$ if $p \cdot q = q \cdot p = e$. If $p \in L$ has a unique inverse, then the inverse element is denoted as $p^{-1}$.

**Definition 2.4.** Bruck (1971) Let $\langle L , \cdot \rangle$ be a binary system and $a , b \in L$. Then $\langle L , \cdot \rangle$ is defined as a quasigroup if there exist unique elements $p , q \in L$ such that $a \cdot p = b$ and $q \cdot a = b$.

**Definition 2.5.** Bruck (1971) A quasigroup $\langle L , \cdot \rangle$, that has an identity element is called a loop.

**Definition 2.6.** Bruck (1971) A Moufang loop is a loop $\langle L , \cdot \rangle$ that satisfies the identity $xy \cdot zx = (x \cdot yz)x$ for all$p, q, r \in L$. For the purpose of 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, $p \cdot (q \cdot (p \cdot r))$ will be written as $p(q \cdot pr)$ and this means first compute $pr$, then multiply$q$ on its left, and again multiply $p$ on the left of the element $q \cdot pr$.

## 3. Methodology

From available literatures on this topic, the proofs for the equivalence of these Moufang identities use autotopism, a concept that is daunting to a novice. Thus, the methodology we adopt here in this work is to make use of only basic properties of quasigroups and loops in an algebraic manner.

## 4. Results

Our objective is to prove the equivalence of the two Moufang identities: $p(q \cdot pr) = (pq \cdot p)r$ and $p(qr \cdot p) = pq \cdot rp$ using purely algebraic methods. Thus the proof involves establishing several other well-known properties of Moufang loops. These properties include, left and right cancellation laws, associativity between any two elements; existence of a unique inverse element for every element and the inverse property.

We shall be referring to these two identities (below) in the statements of Lemmas 3.3, 3.4, 3.5, 3.6 and Theorem 3.7:

$$p(q \cdot pr) = (pq \cdot p)r \quad (1)$$

$$p(qr \cdot p) = pq \cdot rp \quad (2).$$

**Lemma 3.1 (Left and right cancellation laws):** Let $\langle L\ , \cdot \rangle$ be a quasigroup and $p, q, r \in L$. Then $\langle L\ , \cdot \rangle$ satisfies the left and right cancellation laws, that is, $p \cdot q = p \cdot r \Rightarrow\ q = r$ (LCL); and $p \cdot q = r \cdot q \ \Rightarrow\ p = r$ (RCL) respectively.

Proof: This proof follows as a result of the definition of a quasigroup.

**Lemma 3.2.** 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: We proof this lemma by merely using Definition 2.2 (a) and (b), $e_R = e_L \cdot e_R = e_L$ ; thus $\Rightarrow\ e = e_L = e_R$ by (c).

**Lemma 3.3 (Associativity of two elements):**

Let $\langle L\ ,\ \cdot\rangle$ be a loop. Suppose $L$ satisfies any one of the two Moufang identities (1) or (2). Then for any two elements $p, q \in L$:

(a) $p \cdot qp = pq \cdot p$

(b) $p \cdot pq = pp \cdot q$

(c) $q \cdot pp = qp \cdot p$

[NOTE: The identity in (a) is called the flexible identity; in (b), the left alternative identity; and (c), the right alternative identity. See (Bruck, 1971).

Proof:

Case 1: Suppose (1) holds, that is, $p(q \cdot pr) = (pq \cdot p)r \quad \forall\ p, q, r \in L$ .

$\Rightarrow p(q \cdot p1) = (pq \cdot p)1$ by (1) and $\Rightarrow p \cdot qp = pq \cdot p$. This proves (a).

Also $p(1 \cdot pq) = (p1 \cdot p)q$ by (1) since $p,\ 1, q \in L$ . $\Rightarrow \quad p \cdot pq = pp \cdot q$

which proves (b).

Again $p(q \cdot pp) = (pq \cdot p)p$ by (1)

$= (p \cdot qp)p$ by (a)

$= p(qp \cdot p)$ by (a)

By LCL, $q \cdot pp = qp \cdot p$ which proves (c).

Case 2: Suppose (2) holds, that is,

Given $p, q, 1 \in L, pq \cdot 1p = p(q1 \cdot p)$ by (2).

$\Rightarrow\ pq \cdot p = p \cdot qp$, this proves (a).

Given $p, q \in L$, by the quasigroup property, $\exists\ \ u \in L$ such that $up = q$.

So $pp \cdot up = p(pu \cdot p)$ by (2)

$= p(p \cdot up)$ by (a)

$\Rightarrow \ pp \cdot q = p \cdot pq$ this proves (b).

Similarly, for $p, q \in L$, $\exists \ \ v \in L$ such that $pv = q$.

Now $pv \cdot pp = p(vp \cdot p)$ by (2)

$= (p \cdot vp)p$ by (a)

$= (pv \cdot p)p$ by (a) again.

$\Rightarrow \ q \cdot pp = qp \cdot p$, which proves (c).

Hence, the proof of Lemma 3.3 is complete.

**Lemma 3.4 (Inverse Element):** Let $\langle L \ , \cdot \rangle$ be a loop that satisfies any one of the two Moufang identities (1) or (2). Then every element in $L$ has a unique inverse element in the loop.

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

$$u\ell = 1 \qquad (3)$$

and

$$\ell v = 1 \qquad (4)$$

This lemma is prove by showing the existence of a unique left and right inverse element for any element in $L$, and then show that these two are equal.

Case 1: Suppose (1) is true, that is, $p(q \cdot pr) = (pq \cdot p)r \quad \forall \ p, q, r \in L$.

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

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

$= (\ell \cdot u\ell)v$ by Lemma 3.3(a)

$= (\ell \cdot 1)v = \ell v$ by (3).

That is $\ell u = \ell v$. By LCL, $u = v$. So $u = v = \ell^{-1}$.

Case 2: Suppose (2) is true, that is, $pq \cdot rp = p(qr \cdot p) \quad \forall\ p, q, r \in L$ .

Thus, since $u, \ell, v \in L$:

$v \cdot \ell v = v\ell \cdot v$ by Lemma 3.3(a)

$= v\ell \cdot 1v$

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

$= v[(lu \cdot l)v]$ by (2) and Lemma 3.3(a)

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

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

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

Hence, the proof of Lemma 3.4 is complete.

**Lemma 3.5 (Inverse Property):** A loop $\langle L\ , \cdot\rangle$that satisfies any one of the two Moufang identities (1) or (2) has the following properties:

(a) $q^{-1} \cdot qp = p$ (left inverse property) and

(b) $pq \cdot q^{-1} = p$ (right inverse property) for every $p, q \in L$.

Proof: Let $\ell \in L$. By Lemma 3.4, there exists a unique element $\ell^{-1} \in L$ such that

$$\ell \cdot \ell^{-1} = \ell^{-1} \cdot \ell = 1 \qquad (5)$$

Case 1: Suppose $L$ satisfies (1), that is, $p(q \cdot pr) = (pq \cdot p)r \quad \forall\ p, q, r \in L$.

So: $q(q^{-1} \cdot qp) = (qq^{-1} \cdot q)p$ by (3)

$= (1 \cdot q)p = qp$ by (5).

By LCL, $q^{-1} \cdot qp = p$. This proves (a).

Again for $p, q \in L$, there exist $v \in L$ such that $qv = p$.Then we have:

$(qv \cdot q)q^{-1} = q(v \cdot qq^{-1})$ by (3)

$= q(v \cdot 1) = qv$ by (5).

$\Rightarrow\ pq \cdot q^{-1} = p$, which proves (b).

Case 2: Suppose (2) holds, that is, $pq \cdot rp = p(qr \cdot p) \quad \forall\ p, q, r \in L$ .

So: $(q \cdot q^{-1}p)q = q(q^{-1}p \cdot q)$ by Lemma 2.3(a)

$= qq^{-1} \cdot pq$ by (2)

$= 1 \cdot pq = pq$ by (5)

That is, $(q \cdot q^{-1}p)q = pq$. Thus, by RCL, $q \cdot q^{-1}p = p$. This proves (a).

Similarly:

$q(pq^{-1} \cdot q) = qp \cdot q^{-1}q$ by (2)

$= qp \cdot 1 = qp$ by (5)

Thus, $q(pq^{-1} \cdot q) = qp$. By LCL, $pq^{-1} \cdot q = p$ , which proves (b).

This completes the proof of Lemma 3.5.

**Lemma 3.6:** Let $\langle L\ ,\ \cdot \rangle$ be a loop that satisfies any one of the two Moufang identities (1) or (2). Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: $(ab)^{-1} = (ab)^{-1}a \cdot a^{-1}$ by Lemma 3.5(b)

$[(ab)^{-1}(ab \cdot b^{-1})]a^{-1}$ by Lemma 3.5(b) again

$= b^{-1}a^{-1}$ by Lemma 3.5(a)

**Theorem 3.7:** The two Moufang identities (1) and (2) are equivalent identities for any loop.

Proof: Let $\langle L\ ,\ \cdot\rangle$ be a loop. We prove the equivalence by showing that (1) ⇒ (2) ⇒ (1).

*Case 1[(1) ⇒ (2)].*

Assume (1) holds, that is, $p(q\cdot pr)=(pq\cdot p)r\ \forall\ p,q,r\in L$. Note that by Lemma 3.4, $\forall\ p,q,r\in L\ \exists\ p^{-1},q^{-1},r^{-1}\in L$. Also $(p^{-1})^{-1}=p\ \forall\ p^{-1}\in L$ since $p\cdot p^{-1}=p^{-1}\cdot p=1$ by (5). Hence, $\forall\ p,q,r\in L$ we can also express (1) as $p^{-1}(q^{-1}\cdot p^{-1}r^{-1})=(p^{-1}q^{-1}\cdot p^{-1})r^{-1}$.

Thus, we can proceed to show that (1) ⇒ (2) as follows:

$p(qr\cdot p)=p\{[(qp^{-1}\cdot p)r]p\}$ by Lemma 3.5(b)

$=\{[p^{-1}[r^{-1}(p^{-1}\cdot pq^{-1})]]p^{-1}\}^{-1}$ by Lemma 3.6

$=\{[(p^{-1}r^{-1}\cdot p^{-1})\cdot pq^{-1}]p^{-1}\}^{-1}$ by (1)

$=p[(p^{-1}r^{-1}\cdot p^{-1})\cdot pq^{-1}]^{-1}$ by Lemma 3.6

$=p[qp^{-1}\cdot(p\cdot rp)]$ by Lemma 3.6

$=[(p\cdot qp^{-1})p]\cdot rp$ by (1)

$=[p(qp^{-1}\cdot p)]\cdot rp$ by Lemma 3.3(a)

$=pq\cdot rp$ by Lemma 3.5(b).

Therefore (1) ⇒ (2).

*Case 2 [(2) ⇒ (1)].*

Assume (2) is true, that is, $pq\cdot rp=p(qr\cdot p)\quad\forall\ p,q,r\in L$ .

Now $p(q\cdot pr)=p\{[(q\cdot pr)q]q^{-1}\}$ by Lemma 3.5(b)

$=p\{[q(pr\cdot q)]q^{-1}\}$ by Lemma 3.3(a)

$=(q^{-1}\cdot qp)[(qp\cdot rq)q^{-1})$ by (2) and Lemma 3.5(a)

$= q^{-1}\{[(qp)^2 \cdot rq]q^{-1}\}$ by (2) and Lemma 3.3(b)

$= [q^{-1}(qp)^2](rq \cdot q^{-1})$ by (2)

$= [(q^{-1} \cdot qp)(qp)]r$ by Lemma 3.5(b) and Lemma 3.3(c)

$= (p \cdot qp)r = (pq \cdot p)r$ by Lemma 3.5(a) and Lemma 3.3(a).

Therefore (2) ⇒ (1). This concludes the proof of the theorem.

## 5. Conclusion

We have successfully proved the equivalence of the two Moufang identities: $p(q \cdot pr) = (pq \cdot p)r$ and $p(qr \cdot p) = pq \cdot rp$, using algebraic methods that are devoid of the concept of "autotopism" (which was the only way used by mathematicians in this area to prove the equivalence of these identities).

**Benefits:** Indeed, this method, which involves the use of purely basic properties of quasigroups and loops, is easy to understand and straightforward to follow. We believe that this will be exciting to modern-day mathematicians and students alike.

**Acknowledgement:** We wish to acknowledge the great works of Bruck R. H., which we used substantially in this work. Also worthy of mention are Moufang R., Pflugfelder H. O. and Drapal A.

### References

Bruck R. H. (1971). *A Survey of Binary Systems*, Springer-Verlag, New York.

Drapal A. (2010). A Simplified Proof of Moufang's Theorem, *Proceedings of the American Mathematical Society*, **139(1)**, 93-98.

Moufang R. (1935). *Zur Struktur von Alternativkörpern, Math. Ann.* **110**, 416-430.

Pflugfelder H. O. (1990). *Quasigroups and Loops: Introduction, Sigma Series in Pure Mathematics 7*, Heldermann Verlag Berlin.

Zaku, G. G. and Jelten, N. B. (2023). The Equivalence of the Identities: pq · rp = (p · qr)p amd (pq · r)q = p(q · rq). *International Journal of Innovative Mathematics, Statistics & Energy Policies*, 11(1) 36-42.