



The Equivalence Of The Identities: $pq \cdot rp = (p \cdot qr) p$ and $(pq \cdot r)q = p(q \cdot rq)$

Garba Gambo ZAKU (Ph.D) & Naphtali Bashi JELTEN (Ph.D)

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

E-mail: garbazaku@gmail.com ; jeltenn@unijos.edu.ng
+2348036020165; +2348163166586

ABSTRACT

A Moufang loop $\langle L, \cdot \rangle$ is defined as a loop that satisfies any one of the identities: $pq \cdot rp = (p \cdot qr) p$, $pq \cdot rp = p(qr \cdot p)$, $(pq \cdot r)q = p(q \cdot rq)$ or $p(q \cdot pr) = (pq \cdot p)r$. The definition assumes the equivalence of these identities. In this paper we provide a proof of the equivalence of two of these identities: $pq \cdot rp = (p \cdot qr) p$ and $(pq \cdot r)q = p(q \cdot rq)$, using simple algebraic method and manipulation.

Keywords: Moufang, loop, identity

1. INTRODUCTION AND DEFINITIONS

Moufang loops were first introduced by the German mathematician Ruth Moufang in her paper [1], where she proved the equivalence of the identities: $pq \cdot rp = (p \cdot qr) p$, $(pq \cdot r)q = p(q \cdot rq)$ and $p(q \cdot pr) = (pq \cdot p)r$; and later the identity: $pq \cdot rp = p(qr \cdot p)$. Bruck, R. H. [2] was the one that first proved that all the four identities were equivalent. These identities were later referred to as the Moufang Identities. Thus, the loops that satisfied any one of these identities could be simply called Moufang loops.

Bruck and other authors such as Pflugfelder, H. O. [3] and Drapal, A [4], who also proved the equivalence of these identities made use of the concept of autotopism. The concept of autotopism is a difficult concept to understand, especially by modern day mathematics students. So, we provide an alternative proof for two of these identities: $pq \cdot rp = (p \cdot qr) p$ and $(pq \cdot r)q = p(q \cdot rq)$ using purely basic properties of quasigroups and loops in a manner that is easy to understand and straightforward.

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

Definition 1.1. 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 1.2. 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 1.3. 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 1.4. 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 1.5. A quasigroup $\langle L, \cdot \rangle$, that has an identity element is called a loop.

Definition 1.6. A Moufang loop is a loop $\langle L, \cdot \rangle$ that satisfies the identity $pq \cdot rp = (p \cdot qr) p$ 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 $q \cdot pr$.

2. RESULTS

Our main objective is to prove the equivalence of the two Moufang identities: $pq \cdot rp = (p \cdot qr) p$ and $(pq \cdot r) q = p(q \cdot rq)$ by using purely algebraic methods, so the proof involves establishing several other well-known properties of Moufang loops as well. The 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.

In the statement of Lemmas 2.3, 2.4, 2.5, 2.6 and Theorem 2.7, we shall be referring to the two identities as:

$$pq \cdot rp = (p \cdot qr) p \tag{1}$$

$$(pq \cdot r) q = p(q \cdot rq) \tag{2}.$$

Lemma 2.1 (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: The proof is as a result of the definition of a quasigroup.

Lemma 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 lemma is by merely using Definition 1.2 (a) and (b), $e_R = e_L \cdot e_R = e_L$; thus $\Rightarrow e = e_L = e_R$ by (c).

Lemma 2.3 (Associativity of two elements):

Let $\langle L, \cdot \rangle$ be a loop. Assume 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.]

Proof:

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

Since $p, q, 1 \in L$, $p1 \cdot qp = (p \cdot 1q) p$ by (1).

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

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

Now $pu \cdot pp = (p \cdot up) p$ by (1)

$= (pu \cdot p) p$ by (a).

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

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

Now $pp \cdot vp = (p \cdot pv) p$ by (1)

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

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

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

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

Then $(1p \cdot q) p = 1(p \cdot qp)$ by (2) since $1, p, q \in L$. So $pq \cdot p = p \cdot qp$ which proves (a).

Now $(pp \cdot q) p = p(p \cdot qp)$ by (2)

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

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

By RCL, we get $pp \cdot q = p \cdot pq$. This proves (b).

Similarly, $(qp \cdot 1)p = q(p \cdot 1p)$ by (2) and this implies that $qp \cdot p = q \cdot pp$ which proves (c).

This completes the proof of Lemma 2.3.

Lemma 2.4 (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. Since L is a quasigroup, there exist unique elements $u, v \in L$ such that:

$$u\ell = 1 \tag{4}$$

and

$$\ell v = 1 \tag{5}.$$

We prove this lemma 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: Assume (1) is true, that is, $pq \cdot rp = (p \cdot qr)p \quad \forall p, q, r \in L$.

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

$$\begin{aligned} v \cdot \ell v &= v\ell \cdot v && \text{by Lemma 2.3(a)} \\ &= v\ell \cdot 1v \\ &= v\ell(u\ell \cdot v) && \text{by (4)} \\ &= [v(\ell u \cdot \ell)]v && \text{by (1) \& Lemma 2.3(a)} \\ &= (v \cdot \ell u)(\ell v) && \text{by (1)} \\ &= (v \cdot \ell u)1 = v \cdot \ell u && \text{by (5).} \end{aligned}$$

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) is true, that is, $(pq \cdot r)q = p(q \cdot rq) \quad \forall p, q, r \in L$.

$$\begin{aligned} \text{Now: } v\ell &= (1 \cdot v)\ell = (u\ell \cdot v)\ell && \text{by (4)} \\ &= u(\ell \cdot v\ell) && \text{by (2)} \\ &= u(\ell v \cdot \ell) && \text{by Lemma 2.3(a)} \\ &= u(1 \cdot \ell) = u\ell && \text{by (5).} \end{aligned}$$

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

This completes the proof of Lemma 2.4.

Lemma 2.5 (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 2.4, there exists a unique element $\ell^{-1} \in L$ such that

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

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

$$\text{So: } (q \cdot q^{-1}p)q = qq^{-1} \cdot pq \tag{1}$$

$$= 1 \cdot pq = pq \tag{6}.$$

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

Similarly:

$$q(pq^{-1} \cdot q) = (q \cdot pq^{-1})q \tag{1}$$

$$= qp \cdot q^{-1}q \tag{1}$$

$$= qp \cdot 1 = qp \tag{6}.$$

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

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

$$\text{So: } (pq \cdot q^{-1})q = p(q \cdot q^{-1}q) \tag{2}$$

$$= p(q \cdot 1) = pq \tag{6}.$$

By RCL, $pq \cdot q^{-1} = p$. This proves (b).

For $p, q \in L$, there exist $u \in L$ such that $uq = p$. Then we have:

$$q^{-1}(q \cdot uq) = (q^{-1}q \cdot u)q \tag{2}$$

$$= (1 \cdot u)q = uq \tag{6}.$$

Thus, $q^{-1}(q \cdot p) = p$, this proves (a).

This completes the proof of Lemma 2.5.

Lemma 2.6: 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 2.5(b)

$$[(ab)^{-1}(ab \cdot b^{-1})]a^{-1} \tag{1} \tag{6} \tag{2.5(b)}$$

$$= b^{-1}a^{-1} \tag{2.5(a)}$$

Theorem 2.7: 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 $(1) \Rightarrow (2) \Rightarrow (1)$.

Case 1 [(1) \Rightarrow (2)].

Assume (1) is true, that is, $pq \cdot rp = (p \cdot qr) p \quad \forall p, q, r \in L$.

$$\begin{aligned}
 \text{Now } (pq \cdot r)q &= \{r^{-1}[r(pq \cdot r)]\}q && \text{by Lemma 2.5(a)} \\
 &= \{r^{-1}[(r \cdot pq)r]\}q && \text{by Lemma 2.3(a)} \\
 &= [r^{-1}(rp \cdot qr)](qr \cdot r^{-1}) && \text{by (1) \& Lemma 2.5(b)} \\
 &= \{r^{-1}[rp \cdot (qr)^2]\}r^{-1} && \text{by (1) \& Lemma 2.3(c)} \\
 &= (r^{-1} \cdot rp)[(qp)^2 r^{-1}] && \text{by (1)} \\
 &= p[(qr)(qr \cdot r^{-1})] && \text{by Lemma 2.5(a)\&Lemma 2.3(b)} \\
 &= p(qr \cdot q) = p(q \cdot rq) && \text{by Lemma 2.5(b)\&Lemma 2.3(a).}
 \end{aligned}$$

Therefore (1) \Rightarrow (2).

Case 2 [(2) \Rightarrow (1)].

Suppose (2) holds, that is, $(pq \cdot r)q = p(q \cdot rq) \quad \forall p, q, r \in L$. By Lemma 2.4, $\exists p^{-1}, q^{-1}, r^{-1} \in L \quad \forall p, q, r \in L$. Also $(p^{-1})^{-1} = p \quad \forall p^{-1} \in L$ since $p \cdot p^{-1} = p^{-1} \cdot p = 1$ by (6).

So with this we can proceed to show that (2) \Rightarrow (1) as follows:

$$\begin{aligned}
 (p \cdot qr)p &= [p[q(p \cdot p^{-1}r)]]p && \text{by Lemma 2.5(a)} \\
 &= \{p^{-1}[[r^{-1}p \cdot p^{-1}]q^{-1}]p^{-1}\}^{-1} && \text{by Lemma 2.6} \\
 &= \{p^{-1}[r^{-1}p(p^{-1} \cdot q^{-1}p^{-1})]\}^{-1} && \text{by (2)} \\
 &= [r^{-1}p(p^{-1} \cdot q^{-1}p^{-1})]^{-1}p && \text{by Lemma 2.6} \\
 &= [(pq \cdot p) \cdot p^{-1}r]p && \text{by Lemma 2.6} \\
 &= pq \cdot [p(p^{-1}r \cdot p)] && \text{by (2)} \\
 &= pq \cdot [(p \cdot p^{-1}r)p] && \text{by Lemma 2.3(a)} \\
 &= pq \cdot rp && \text{by Lemma 2.5(a).}
 \end{aligned}$$

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

CONCLUSION

We have succeeded in proving the equivalence of the two Moufang identities: $pq \cdot rp = (p \cdot qr) p$ and $(pq \cdot r)q = p(q \cdot rq)$, using purely algebraic methods devoid of the concept of ‘‘autotopism’’ (which was the only way used by earlier mathematicians in this area to prove the equivalence of these identities). We have shown that 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.

REFERENCES

1. Moufang R. (1935). Zur Struktur von Alternativkörpern, Math. Ann. **110**, 416-430.
2. Bruck R. H. (1971). A Survey of Binary Systems, Springer-Verlag, New York.
3. Pflugfelder H. O. (1990). Quasigroups and Loops: Introduction, Sigma Series in Pure Mathematics 7, Heldermann Verlag Berlin.
4. Drapal A. (2010). A Simplified Proof of Moufang's Theorem, Proceedings of the American Mathematical Society, **139(1)**, p93-98.