Right division in Moufang loops

Maria de Lourdes M. Giuliani, Kenneth W. Johnson

Abstract. If $(G, \cdot)$ is a group, and the operation $(*)$ is defined by $x * y = x \cdot y^{-1}$ then by direct verification $(G, *)$ is a quasigroup which satisfies the identity $(x * y) * (z * y) = x * z$. Conversely, if one starts with a quasigroup satisfying the latter identity the group $(G, \cdot)$ can be constructed, so that in effect $(G, \cdot)$ is determined by its right division operation. Here the analogous situation is examined for a Moufang loop. Subtleties arise which are not present in the group case since there is a choice of defining identities and the identities produced by replacing loop multiplication by right division give identities in which loop inverses appear. However, it is possible with further work to obtain an identity in terms of $(*)$ alone. The construction of the Moufang loop from a quasigroup satisfying this identity is significantly more difficult than in the group case, and it was first carried out using the software Prover9. Subsequently a purely algebraic proof of the construction was obtained.

Keywords: Moufang loop, Prover9

Classification: Primary 20N05; Secondary 20-04

1. Introduction

The operation of right division in a group first appeared implicitly in the work of Frobenius on group matrices and the group determinant, which gave rise to group representation theory. This operation has been studied algebraically by several authors (see [2]). If $(G, \cdot)$ is a group, and the operation $(*)$ is defined by $x * y = x \cdot y^{-1}$, then, as mentioned above, it is easy to show that $(G, *)$ satisfies the identity

$$(x * y) * (z * y) = x * z. \tag{1}$$

This identity has appeared under several names, one of which is the Ward identity. Conversely, if $(Q, *)$ is a quasigroup which satisfies (1), then an operation $(\circ)$ can be defined such that $(Q, \circ)$ is a group, and if $(Q, *)$ arises as above from a group $(G, \cdot)$ then $(G, \circ)$ is isomorphic to $(G, \cdot)$ (see, for example, [2] and the references provided there). Thus (1) provides a way of characterizing groups by

The first author wishes to thank the University of Santa Maria and the Pennsylvania State University for providing support while the work on this paper was carried out. Thanks are also due to the University of Denver which partially funded a visit by both authors during which we were introduced to the Prover9 software.

right division. We address below the question of whether a similar identity exists for right division in Moufang loops.

If one starts with a Moufang loop $(M, \cdot)$ and defines $(*)$ by $x * y = x \cdot y^{-1}$ then the Moufang identity

$$x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z \tag{2}$$

translates to

$$x * ((z^{-1} * x) * y) = ((x * y^{-1}) * x^{-1}) * z^{-1}, \tag{3}$$

where here the inverse operation is that in the loop $(M, \cdot)$. Work is needed to replace the inverses in order to obtain an identity in terms of $(*)$ alone, (10) below. If one assumes that $(Q, *)$ is a quasigroup satisfying (10) it is much more difficult than in the group case to construct a Moufang loop. We first found such a construction using the automatic software Prover9. An analysis of the long proof which Prover9 produced showing that the construction did produce the required Moufang loop enabled us to produce an entirely algebraic proof which is given below. It is significantly more involved than in the group case.

2. Moufang loops under right division

We first give the appropriate definitions. A quasigroup $(Q, \cdot)$ is a set Q together with a binary operation such that $x \cdot y = z$ has a unique solution for any x, y or z whenever the other 2 variables are given. In the finite case this is equivalent to the multiplication table of $(Q, \cdot)$ being a latin square. In a quasigroup we have the operations of left and right division which are denoted by $(\backslash)$ and $(/)$:

$$a \backslash b = x \quad \text{where} \quad a \cdot x = b \quad \text{and} \quad a/b = y \quad \text{where} \quad a = y \cdot b.$$

It is clear that

$$a \cdot (a \backslash b) = b \quad \text{and} \quad a \backslash (a \cdot b) = b.$$

A loop $(L, \cdot)$ is a quasigroup with a two-sided identity element e. A Moufang loop is a loop $(M, \cdot)$ satisfying the identity

$$x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z. \tag{4}$$

We now consider a Moufang loop $(M, \cdot)$ and define the operation $*$ by

$$x * y = x \cdot y^{-1}. \tag{5}$$

This operation is well-defined since every element in a Moufang loop has a unique two-sided inverse.

Lemma 1. *If $(M, \cdot)$ is a Moufang loop then $(M, *)$ is a quasigroup satisfying*

$$x * [(z * x) * y] = [x * (((x * x) * x) * y)] * z. \tag{6}$$

Proof: We remark that a Moufang loop satisfies the Inverse Property:

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$

Expressing the left hand side of (4) in terms of $(*)$ we obtain

$$\begin{aligned} x \cdot (y \cdot (x \cdot z)) &= x * (y \cdot (x \cdot z))^{-1} \\ &= x * ((z^{-1} \cdot x^{-1}) \cdot y^{-1}) \\ &= x * ((z^{-1} * x) * y). \end{aligned}$$

The right hand side of (4) is:

$$((x \cdot y) \cdot x) \cdot z = ((x * y^{-1}) * x^{-1}) * z^{-1}.$$

Therefore a consequence of (4) is

$$x * ((z^{-1} * x) * y) = ((x * y^{-1}) * x^{-1}) * z^{-1}.$$

On replacing z^{-1} by z we obtain the identity:

(7) $$x * ((z * x) * y) = ((x * y^{-1}) * x^{-1}) * z.$$

We emphasise that x^{-1} is the inverse element with respect to the operation $(\cdot)$. It is well known that in a Moufang loop $x \cdot (y \cdot x) = (x \cdot y) \cdot x$ [1]. This in turn translates into

(8) $$x * (x^{-1} * y) = (x * y^{-1}) * x^{-1}.$$

Using (8) in the right hand side of (7) we get

(9) $$x * ((z * x) * y) = (x * (x^{-1} * y)) * z.$$

In order to obtain an identity in terms of $(*)$ we need to replace x^{-1} by a suitable word. We can do this because for any $x \in M$, $(x * x) = e$ and $e * x = e \cdot x^{-1} = x^{-1}$. Therefore $x^{-1} = (x * x) * x$. On inserting this expression for x^{-1} in (9) the lemma follows. $\square$

The *Fundamental Identity* $(\mathcal{FI})$ is defined to be:

(10) $$x * [(z * x) * y] = [x * (((x * x) * x) * y)] * z.$$

From now on we assume that $(Q, *)$ is a quasigroup satisfying the identity (10). Let the operation $(\circ)$ be defined on Q by

(11) $$x \circ y = x * ((y * y) * y).$$

Lemma 2. *For any $x, y \in (Q, *)$, $x * x = y * y$.*

Proof: In the right hand side of $(\mathcal{FI})$ we replace $(x*x)*x$ by u to obtain

$$[x*(((x*x)*x)*y)]*z=[x*(u*y)]*z. \tag{12}$$

Substitute $t=u*y$ in (12)

$$[x*(((x*x)*x)*y)]*z=[x*t]*z.$$

Since we can replace y by $u\setminus t$, the left hand side of $(\mathcal{FI})$ becomes

$$x*((z*x)*(u\setminus t)).$$

Thus we have

$$(x*t)*z=x*((z*x)*(u\setminus t)). \tag{13}$$

Now replace t by y in (13)

$$(x*y)*z=x*((z*x)*(u\setminus y)). \tag{14}$$

A further replacement of z by $x*x$ produces

$$(x*y)*(x*x)=x*(((x*x)*x)*(u\setminus y)). \tag{15}$$

Since $(x*x)*x=u$, the right hand side of (15) becomes

$$x*(u*(u\setminus y))=x*y \tag{16}$$

and therefore

$$(x*y)*(x*x)=x*y.$$

Since x,y are arbitrary it follows that $x*x=y*y$ for any $x,y\in Q$. □

Corollary 1. $z*(x*x)=z\ \forall\, z,x\in Q$.

Theorem 1. *For any* $x,y,z\in Q$

$$((x\circ y)\circ x)\circ z=x\circ(y\circ(x\circ z)). \tag{17}$$

The proof of this theorem was initially obtained using Prover9 [3]. The following is a proof which is computer independent. We begin by some technical lemmas.

Lemma 3. *For any* $x,y,z\in(Q,*)$,

(i) $(x*y)*z=x*[(z*x)*(((x*x)*x)\setminus y)]$;
(ii) $(z*x)*y=x\setminus[(x*(((x*x)*x)*y))*z]$.

Proof: (i) Is a restatement of (14).
(ii) Apply left division by x to both sides of $(\mathcal{FI})$ to obtain

$$x\setminus[x*((z*x)*y)]=x\setminus[(x*(((x*x)*x)*y))*z]. \tag{18}$$

The left hand side reduces to $(z*x)*y$ and the lemma is proved. □

Now for all $x \in Q$ we define $x' = (x * x) * x$. Then the $(\mathcal{FI})$ may be restated as

(19) $$x * [(z * x) * y] = [x * (x' * y)] * z.$$

We note that for any $x, y \in Q$

(20) $$y' = (x * x) * y.$$

Lemma 4. *For any $x, y \in (Q, *)$, $(x * y') * x' = x * (x' * y)$.*

Proof: We first show that

(21) $$x * (x' * y) = [(x * (x' * y)) * x] * x'.$$

Now

$$[(x * (x' * y)) * x] * x' = (u * x) * x'$$

where $u = x * (x' * y)$. Applying Lemma 3(ii)

$$(u * x) * x' = x \setminus ((x * (x' * x')) * u) = x \setminus (x * u) = u = x * (x' * y),$$

showing (21). Now, replacing z by x in (19) we obtain:

(22) $$x * [(x * x) * y] = [x * (x' * y)] * x.$$

The left hand side of (22) reduces to $x * y'$. Therefore

$$(x * y') * x' = [(x * (x' * y)) * x] * x',$$

and the lemma is proved. □

Lemma 5. *For any $x, y \in (Q, *)$,*

(i) $(x * y) * y' = x$,
(ii) $(x * y) \setminus x = y'$,
(iii) $x'' = x$,
(iv) $(x * y') * y = x$.

Proof: (i) On replacing x, y, z by y, y', x respectively in right hand side of Lemma 3(ii),

(23) $$(x * y) * y' = y \setminus [(y * (((y * y) * y) * y') * x)] = y \setminus [(y * (y' * y')) * x],$$

but by Corollary 1, $y * (y' * y') = y * (y * y) = y$. Thus

(24) $$y \setminus [(y * (y' * y')) * x] = y \setminus (y * x) = x.$$

(ii) Suppose $(x*y) \setminus x = u$. It follows that $x = (x*y)*u$. But from (i) $x = (x*y)*y'$ and therefore $u = y'$.
Remark: On replacing y by x in (ii) we obtain

(25) $$(x * x) \setminus x = x'.$$

(iii) Let $u = x'' = (x')'$. Then $u = (x' * x') * x' = (x * x) * x'$. Therefore $(x * x) \setminus u = x'$ which implies that $(u * u) \setminus u = x'$. But by (25) $(u * u) \setminus u = u'$ and (iii) follows.
(iv) This follows immediately, from (i), since $y'' = y$. □

Lemma 6. *For any $y, z \in (Q, *)$, $(y * z)' = z * y$.*

Proof: By (20) $(y * z)' = (x * x) * (y * z)$. Now $z * y = ((x * x) * z') * y$. From Lemma 3(i) we have

$$(x * y) * z = x * [(z * x) * (x' \setminus y)]. \tag{26}$$

On replacing x, y, z respectively by $(x * x), z', y$ in (26), we obtain

$$((x * x) * z') * y = (x * x) * [(y * (x * x)) * ((x * x)' \setminus z')]. \tag{27}$$

The left hand side of (27) is equal to $z * y$ and using Corollary 1 and (20) the right hand side reduces to

$$(x * x) * (y * z) = (y * z)'.$$

The lemma follows. □

We can now express $(\circ)$ as

$$x \circ y = x * y'. \tag{28}$$

Lemma 7. $(Q, \circ)$ *is a loop.*

Proof: We show that $(Q, \circ)$ has the two-sided identity element $e = x * x$. It is clear that e is well-defined by Lemma 2. Then by Corollary 1, $x * e = x$ for all x in Q. Since $e' = (x * x)' = (x * x) = e$ it follows that $x \circ e = x * e' = x$. Now $e \circ x = (x * x) \circ x = (x * x) * x' = x'' = x$. The lemma is proved. □

Proof of Theorem 1: Applying (28) to the left hand side of (17) we obtain

$$((x \circ y) \circ x) \circ z = ((x * y') * x') * z'.$$

With repeated use of Lemma 6 the right hand side of (17) becomes

$$x * (y * (x * z')')' = x * ((x * z')' * y) = x * ((z' * x) * y). \tag{29}$$

Using (4) the right hand side of (29) becomes

$$(x * (x' * y)) * z'.$$

Then from Lemma 4

$$x * (x' * y) = (x * y') * x',$$

and hence

$$(x * (x' * y)) * z = ((x * y') * x') * z'.$$

We have shown that (17) holds and therefore $(Q, \circ)$ is a Moufang loop. $\square$

It is clear that if the quasigroup $(M, *)$ is constructed from the Moufang loop by right division, then the loop $(M, \circ)$ is isomorphic to $(M, \cdot)$.

References

[1] Zhevlakov K.A., Slin'ko A.M., Shestakov I.P., Shirshov A.I., *Rings That Are Nearly Associative*, Pure and Applied Mathematics, 104, Academic Press, New York-London, 1982.
[2] Johnson K.W., Vojtěchovský P., *Right division in groups, Dedekind-Frobenius group matrices, and Ward quasigroups*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 121–136.
[3] McCune W.W., *Prover9, automated reasoning software, and Mace4, finite model builder*, Argonne National Laboratory, 2005, `http://www.prover9.org`.

Universidade Federal do ABC, Rua Santa Adélia, 166, Santo André, SP, Brazil, 09210-170

E-mail: maria.giuliani@ufabc.edu.br

Abington College, The Pennsylvania State University, 1600 Woodland Road, Abington, PA 19001, USA

E-mail: kwj1@psu.edu

(*Received* September 24, 2009, *revised* January 12, 2010)