

J. I. Hall

On Mikheev's construction of enveloping groups

Commentationes Mathematicae Universitatis Carolinae, Vol. 51 (2010), No. 2, 245--252

Persistent URL: <http://dml.cz/dmlcz/140102>

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 2010

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

On Mikheev’s construction of enveloping groups

J.I. HALL

Abstract. Mikheev, starting from a Moufang loop, constructed a groupoid and reported that this groupoid is in fact a group which, in an appropriate sense, is universal with respect to enveloping the Moufang loop. Later Grishkov and Zavarnitsine gave a complete proof of Mikheev’s results. Here we give a direct and self-contained proof that Mikheev’s groupoid is a group, in the process extending the result from Moufang loops to Bol loops.

Keywords: Bol loop, Moufang loop, autotopism group, group with triality

Classification: 20N05

1. Introduction

A *groupoid* (Q, \circ) is a set Q endowed with a binary product $\circ : Q \times Q \longrightarrow Q$. The groupoid is a *quasigroup* if, for each $x \in Q$, the right translation map $R_x : Q \longrightarrow Q$ and left translation map $L_x : Q \longrightarrow Q$ given by

$$aR_x = a \circ x \quad \text{and} \quad aL_x = x \circ a$$

are both permutations of Q .

The groupoid (Q, \circ) is a *groupoid with identity* if it has a two-sided identity element:

$$1 \circ x = x = x \circ 1, \quad \text{for all } x \in Q.$$

That is, R_1 and L_1 are Id_Q , the identity permutation of Q . A quasigroup with identity is a *loop*.

The loop (Q, \circ) is a (*right*) *Bol* loop if it identically has the right Bol property:

$$\text{for all } a, b, x \in Q, \quad a((xb)x) = ((ax)b)x.$$

(We often abuse notation by writing pq in place of $p \circ q$.) The loop is a *Moufang* loop if it has the Moufang property:

$$\text{for all } a, b, x \in Q, \quad a(x(bx)) = ((ax)b)x.$$

Finally the loop is a *group* if it has the associative property:

$$\text{for all } a, b, x \in Q, \quad a(xb) = (ax)b.$$

Partial support provided by the National Science Foundation, USA.

The Moufang property is clearly a weakened form of the associative property. Furthermore, with $a = 1$ the Moufang property gives $x(bx) = (xb)x$ identically; so the Bol property is a consequence of the Moufang property. Thus every group is a Moufang loop and every Moufang loop is a Bol loop. The reverse implications do not hold in general; see [6, Examples IV.1.1 and IV.6.2].

A (right) pseudo-automorphism of the groupoid with identity (Q, \circ) is a permutation A of Q equipped with an element $a \in Q$, a companion of A , for which R_a is a permutation (always true for (Q, \circ) a loop) and such that

$$xA \circ (yA \circ a) = (xy)A \circ a$$

for all $x, y \in Q$. We shall abuse this terminology by referring to the pair (A, a) as a pseudo-automorphism. The set of all pseudo-automorphisms (A, a) is then denoted $\text{PsAut}(Q, \circ)$ and admits the group operation

$$(A, a)(D, d) = (AD, aD \circ d),$$

as we shall verify in Proposition 2.1 below.

In the research report [5] Mikheev, starting from a Moufang loop (Q, \circ) , constructed a groupoid on the set $\text{PsAut}(Q, \circ) \times Q$. The main results reported by Mikheev are that this groupoid is in fact a group and that, in an appropriate sense, it is universal with respect to “enveloping” the Moufang loop (Q, \circ) .

In [3] Grishkov and Zavarnitsine gave a complete proof of Mikheev’s results (and a great deal more). Concerning Mikheev’s construction they proved:

Theorem 1.1. *Let (Q, \circ) be a Moufang loop.*

(a) *The groupoid $(\text{PsAut}(Q, \circ) \times Q, \star)$ given by*

$$\begin{aligned} & \{(A, a), x\} \star \{(B, b), y\} = \{(A, a)(B, b)(C, c), (xB)y\} \quad \text{with} \\ \text{(Mk)} \quad & (C, c) = \left(R_{xB, b}^{-1}, (((xB)b)^{-1}b)xB \right) \left(R_{xB, y}, ((xB)^{-1}y^{-1})((xB)y) \right) \end{aligned}$$

is a group $\mathcal{W}(Q, \circ)$.

(b) *The group $\mathcal{W}(Q, \circ)$ admits a group of triality automorphisms and is universal (in an appropriate sense) among all the groups admitting triality that envelope the Moufang loop (Q, \circ) .*

Here for each p, q in an arbitrary loop (Q, \circ) we have set $R_{p,q} = R_p R_q R_{pq}^{-1}$.

The expression (Mk) can be simplified somewhat. By Moufang’s Theorem ([1, p. 117] and [6, Cor. IV.2.9]) Moufang loops generated by two elements are groups, so within (Q, \circ) commutators

$$[p, q] = p^{-1}q^{-1}pq = (qp)^{-1}pq$$

are well-defined, as seen in Mikheev’s original formulation [5]. Also in Moufang loops we have $R_{p,q}^{-1} = R_{q,p}$ by [1, Lemma VII.5.4]. Therefore Grishkov and Zavarnitsine could give (Mk) in the pleasing form

$$(C, c) = (R_{b,xB}, [b, xB]) (R_{xB,y}, [xB, y]).$$

Grishkov and Zavarnitsine [3, Corollary 1] verify Mikheev’s construction by first constructing from (Q, \circ) a particular group admitting triality and then showing that Mikheev’s groupoid is a quotient of that group and especially is itself a group. Their construction displays universal properties for the two groups admitting triality and so also for Mikheev’s enveloping group. (Grishkov and Zavarnitsine also correct several small misprints from [5].)

In this short note we take a different approach. In particular we give a direct and self-contained proof that Mikheev’s groupoid is a group. In the process we extend the result from Moufang loops to Bol loops, and we see that the groupoid has a natural life as a group.

An *autotopism* (A, B, C) of the groupoid (Q, \circ) is a triple of permutations of Q such that

$$xA \circ yB = (x \circ y)C$$

for all $x, y \in Q$. Clearly the set $\text{Atop}(Q, \circ)$ of all autotopisms of (Q, \circ) forms a group under composition.

We then have

Theorem 1.2. *Let (Q, \circ) be a Bol loop. The groupoid $(\text{PsAut}(Q, \circ) \times Q, \star)$ with product given by (Mk) is isomorphic to the autotopism group $\text{Atop}(Q, \circ)$. In particular $(\text{PsAut}(Q, \circ) \times Q, \star)$ is a group.*

Theorem 1.2 gives Theorem 1.1(a) immediately, and 1.1(b) directly follows. Indeed following Doro [2], the group G admits triality if G admits the symmetric group of degree three, $\text{Sym}(3) = S$, as a group of automorphism such that, for σ of order 2 and τ of order 3 in S , the identity $[g, \sigma][g, \sigma]^\tau [g, \sigma]^{\tau^2} = 1$ holds for all $g \in G$. Doro proved that the set $\{ [g, \sigma] \mid g \in G \}$ naturally carries the structure of a Moufang loop (Q, \circ) ; we say that G envelopes (Q, \circ) . Many nonisomorphic groups admitting triality envelope Moufang loops isomorphic to (Q, \circ) . Among these the autotopism group $A = \text{Atop}(Q, \circ)$ is the largest that is additionally faithful, which is to say that the centralizer of S^A within $A \times S$ is the identity. That is, for every group G admitting triality that is faithful and envelopes (Q, \circ) there is an S -injection of G into A . This is the universal property examined by Mikheev, Grishkov, and Zavarnitsine. See [4, §10.3] for further details.

The general references for this note are the excellent books [1] and [6]. Several of the results given here are related to ones from [6] — both as exact versions (“see”) and as variants or extensions (“compare”).

2. Autotopisms of groupoids

Proposition 2.1. *Let (Q, \circ) be a groupoid with identity 1. The map*

$$\psi: (A, a) \mapsto (A, AR_a, AR_a)$$

gives a bijection of $\text{PsAut}(Q, \circ)$ with the subgroup of $\text{Atop}(Q, \circ)$ consisting of all autotopisms (A, B, C) for which $1A = 1$. For such an autotopism we have

$$\psi^{-1}(A, B, C) = (A, 1C).$$

In particular $\text{PsAut}(Q, \circ)$ is a group under the composition

$$(A, a)(D, d) = (AD, aD \circ d).$$

PROOF: (Compare [6, III.4.14].) If (A, a) is a pseudo-automorphism then (A, AR_a, AR_a) is an autotopism by definition. In particular for every $x \in Q$ we have $1A \circ xAR_a = (1 \circ x)AR_a = xAR_a$. As AR_a is a permutation of Q , there is an x with $1 = xAR_a$. Thus $1A = 1A \circ 1 = 1$.

If (A, a) and (B, b) are pseudo-automorphisms with (A, AR_a, AR_a) equal to (B, BR_b, BR_b) , then $A = B$ and $a = 1AR_a = 1BR_b = b$; so ψ is an injection of $\text{PsAut}(Q, \circ)$ into the described subgroup of $\text{Atop}(Q, \circ)$.

Now suppose that (A, B, C) is an autotopism with $1A = 1$. Always $1 \circ x = x$, so

$$xB = 1A \circ xB = (1 \circ x)C = xC,$$

giving $B = C$.

Again $x \circ 1 = x$ and

$$xA \circ 1C = (x \circ 1)C = xC.$$

That is $B = C = AR_{1C}$, and in particular R_{1C} is a permutation. Therefore $(A, B, C) = (A, AR_a, AR_a)$, the image of the pseudo-automorphism (A, a) for $a = 1C$. The map ψ is indeed a bijection.

Those autotopisms with $1A=1$ clearly form a subgroup, so ψ^{-1} gives $\text{PsAut}(Q, \circ)$ a natural group structure. We find

$$\begin{aligned} \psi(A, a)\psi(D, d) &= (A, AR_a, AR_a)(D, DR_d, DR_d) \\ &= (AD, AR_aDR_d, AR_aDR_d) \\ &= \psi(AD, e) \end{aligned}$$

for some e with $AR_aDR_d = ADR_e$. Indeed $e = 1ADR_e = 1AR_aDR_d = aD \circ d$. Therefore multiplication in $\text{PsAut}(Q, \circ)$ is given by

$$(A, a)(D, d) = (AD, aD \circ d),$$

as stated here and above. □

From now on we identify $\text{PsAut}(Q, \circ)$ with its isomorphic image under ψ in $\text{Atop}(Q, \circ)$.

- Corollary 2.2.** (a) *Let (A, B, C) and (D, E, F) be autotopisms of the groupoid with identity (Q, \circ) . Then we have $(A, B, C) = (D, E, F)$ if and only if $A = D$ and $1C = 1F$.*
 (b) *Let (A, B, C) and (D, E, F) be autotopisms of the loop (Q, \circ) . Then we have $(A, B, C) = (D, E, F)$ if and only if $A = D$ and there is an $x \in Q$ with $xC = xF$.*

PROOF: (Compare [6, III.3.1].) One direction is clear.

Now suppose that $A = D$.

$$\begin{aligned} (X, Y, Z) &= (A, B, C)(D, E, F)^{-1} \\ &= (AD^{-1}, BE^{-1}, CF^{-1}) \\ &= (\text{Id}_Q, BE^{-1}, CF^{-1}) \\ &= (\text{Id}_Q, \text{Id}_Q R_e, \text{Id}_Q R_e) \\ &= (\text{Id}_Q, R_e, R_e) \end{aligned}$$

for $e = 1CF^{-1}$ by the proposition.

For any x with $xC = xF$ we then have

$$x \circ 1 = x = xCF^{-1} = xZ = x \circ e,$$

so in both parts of the corollary we find $e = 1$. Therefore (X, Y, Z) is equal to $(\text{Id}_Q, \text{Id}_Q, \text{Id}_Q)$, the identity of $\text{Atop}(Q, \circ)$. □

A particular consequence of the corollary is that we may (if we wish) denote the autotopism (A, B, C) by $(A, *, C)$, since A and C determine B uniquely.

3. Autotopisms of Bol loops

Recall that a Bol loop (Q, \circ) is a loop with

$$\text{for all } a, b, x \in Q, \quad a((xb)x) = ((ax)b)x.$$

- Lemma 3.1.** (a) *The loop (Q, \circ) is a Bol loop if and only if $(R_x^{-1}, L_x R_x, R_x)$ is an autotopism for all $x \in Q$.*
 (b) *The Bol loop (Q, \circ) is a right inverse property loop. That is, for x^{-1} defined by $xx^{-1} = 1$ we have $(x^{-1})^{-1} = x$ and $(ax)x^{-1} = a$, for all $a, x \in Q$. In particular $R_x^{-1} = R_{x^{-1}}$ for all x .*

PROOF: (a) (See [6, Theorem IV.6.7].) For a fixed $x \in Q$ we have $a((xb)x) = ((ax)b)x$ for all $a, b \in Q$ if and only if $(cR_x^{-1})(bL_x R_x) = (cb)R_x$ for all $c (= ax)$, $b \in Q$ if and only if $(R_x^{-1}, L_x R_x, R_x)$ is an autotopism.

(b) (See [6, Theorem IV.6.3].) In the identity $a((xb)x) = ((ax)b)x$ set $b = x^{-1}$ to find $ax = a((xx^{-1})x) = ((ax)x^{-1})x$. That is, $aR_x = (ax)x^{-1}R_x$ and so

$a = (ax)x^{-1}$. Further set $a = x^{-1}$ in this identity, giving

$$1R_{x^{-1}} = x^{-1} = (x^{-1}x)x^{-1} = (x^{-1}x)R_{x^{-1}},$$

whence $1 = x^{-1}x$ and $(x^{-1})^{-1} = x$. □

Throughout the balance of this section let (Q, \circ) be a Bol loop.

For all p in the Bol loop (Q, \circ) set

$$r_p = (R_{p^{-1}}^{-1}, L_{p^{-1}}R_{p^{-1}}, R_{p^{-1}}) = (R_p, L_{p^{-1}}R_{p^{-1}}, R_{p^{-1}}),$$

and set $r_{p,q} = r_p r_q r_{pq}^{-1}$ for all p, q . By the lemma, each r_p and $r_{p,q}$ is an autotopism of (Q, \circ) .

Lemma 3.2. (a) $r_p^{-1} = r_{p^{-1}}$.

(b) $r_{p,q} = (R_{p,q}, (p^{-1}q^{-1})(pq))$.

(c) $r_{p,q}^{-1} = (R_{p,q}^{-1}, ((pq)^{-1}q)p)$.

PROOF: By Lemma 3.1

$$r_p^{-1} = (R_p^{-1}, *, R_{p^{-1}}) = (R_p^{-1}, *, R_p) = (R_{p^{-1}}, *, R_p) = r_{p^{-1}},$$

as in (a). Therefore

$$r_{p,q} = r_p r_q r_{pq}^{-1} = (R_p R_q R_{pq}^{-1}, *, R_{p^{-1}} R_{q^{-1}} R_{pq}) = (R_{p,q}, *, R_{p^{-1}} R_{q^{-1}} R_{pq})$$

and

$$r_{p,q}^{-1} = (R_{p,q}, *, R_{p^{-1}} R_{q^{-1}} R_{pq})^{-1} = (R_{p,q}^{-1}, *, R_{(pq)^{-1}} R_q R_p).$$

Here

$$1 R_p R_q R_{pq}^{-1} = (pq)(pq)^{-1} = 1;$$

$$1 R_{p^{-1}} R_{q^{-1}} R_{pq} = (p^{-1}q^{-1})(pq);$$

$$1 R_{(pq)^{-1}} R_q R_p = ((pq)^{-1}q)p.$$

The first calculation tells us that $r_{p,q}$ (and $r_{p,q}^{-1}$) are in $\text{PsAut}(Q, \circ)$. The second, together with Proposition 2.1, then gives (b) and the third (c). □

Proposition 3.3. *Let (X, Y, Z) be in $\text{Atop}(Q, \circ)$. Set $x = 1X$, $A = XR_x^{-1}$, and $a = 1Z \circ x$. Then*

$$(X, Y, Z) = (A, a)r_x.$$

In particular $\{r_x \mid x \in Q\}$ is a set of right coset representatives for the subgroup $\text{PsAut}(Q, \circ)$ in $\text{Atop}(Q, \circ)$.

PROOF: (Compare [6, III.4.16, IV.6.8].)

$$\begin{aligned} (X, Y, Z) &= (X, Y, Z)r_x^{-1}r_x \\ &= (XR_x^{-1}, YR_{x^{-1}}^{-1}L_{x^{-1}}^{-1}, ZR_{x^{-1}}^{-1})r_x \\ &= (XR_{x^{-1}}, *, ZR_x)r_x. \end{aligned}$$

For $A = XR_x^{-1} = XR_{x^{-1}}$ we have $1A = 1XR_{x^{-1}} = x \circ x^{-1} = 1$. Furthermore $1ZR_x = 1Z \circ x = a$, so by Proposition 2.1 we have $(X, Y, Z) = (A, a)r_x$. \square

Proposition 3.4. $r_x(B, b) = (B, b)r_{(xB)b}r_b^{-1}$

PROOF: We have

$$\begin{aligned} r_x(B, b) &= (R_x, L_{x^{-1}}R_{x^{-1}}, R_{x^{-1}})(B, BR_b, BR_b) \\ &= (R_x B, *, R_{x^{-1}}BR_b) \end{aligned}$$

and

$$\begin{aligned} (B, b)r_{(xB)b}r_b^{-1} &= (B, BR_b, BR_b)(R_{(xB)b}, *, R_{((xB)b)^{-1}})(R_b^{-1}, *, R_b) \\ &= (BR_{(xB)b}R_b^{-1}, *, BR_bR_{((xB)b)^{-1}}R_b). \end{aligned}$$

First we observe that $xR_{x^{-1}}BR_b = 1BR_b = b$ and

$$xBR_bR_{((xB)b)^{-1}}R_b = ((xB)b)R_{((xB)b)^{-1}}R_b = 1R_b = b.$$

Therefore by Corollary 2.2 we need only verify $R_x B = BR_{(xB)b}R_b^{-1}$ to prove the proposition.

As (B, b) is a pseudo-automorphism

$$\begin{aligned} pR_x BR_b &= (px)BR_b \\ &= (px)B \circ b \\ &= pB \circ (xB \circ b) \\ &= pBR_{(xB)b} \end{aligned}$$

for every $p \in Q$. Therefore $R_x BR_b = BR_{(xB)b}$ and $R_x B = BR_{(xB)b}R_b^{-1}$ as desired. \square

Corollary 3.5. $(A, a)r_x(B, b)r_y = (A, a)(B, b)r_{xB, b}^{-1}r_{xB, y}r_{(xB)y}$.

PROOF:

$$\begin{aligned}
 (A, a)r_x(B, b)r_y &= (A, a)(r_x(B, b))r_y \\
 &= (A, a)((B, b)r_{(xB)b}r_b^{-1})r_y \\
 &= (A, a)(B, b)r_{(xB)b}r_b^{-1}(r_{xB}^{-1}r_{xB})r_y(r_{(xB)y}^{-1}r_{(xB)y}) \\
 &= (A, a)(B, b)(r_{(xB)b}r_b^{-1}r_{xB}^{-1})(r_{xB}r_yr_{(xB)y}^{-1})r_{(xB)y} \\
 &= (A, a)(B, b)r_{xB, b}^{-1}r_{xB, y}r_{(xB)y}.
 \end{aligned}$$

□

Theorem 3.6. For the Bol loop (Q, \circ) the map

$$\varphi: \{(A, a), x\} \mapsto (A, a)r_x$$

gives an isomorphism of Mikheev's groupoid $(\text{PsAut}(Q, \circ) \times Q, \star)$ and the autotopism group $\text{Atop}(Q, \circ)$. In particular $(\text{PsAut}(Q, \circ) \times Q, \star)$ is a group.

PROOF: By Proposition 3.3 the map φ is a bijection of $\text{PsAut}(Q, \circ) \times Q$ and $\text{Atop}(Q, \circ)$. By Lemma 3.2 and Corollary 3.5

$$\varphi(\{(A, a), x\} \star \{(B, b), y\}) = \varphi(\{(A, a), x\}) \varphi(\{(B, b), y\}).$$

Thus $(\text{PsAut}(Q, \circ) \times Q, \star)$ and $\text{Atop}(Q, \circ)$ are isomorphic as groupoids. Furthermore since $\text{Atop}(Q, \circ)$ is itself a group, so is $(\text{PsAut}(Q, \circ) \times Q, \star)$. □

Theorem 1.2 is an immediate consequence.

REFERENCES

- [1] Bruck R.H., *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer, Berlin-Göttingen-Heidelberg, 1958.
- [2] Doro S., *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **83** (1978), 377–392.
- [3] Grishkov A.N., Zavarnitsine A.V., *Groups with triality*, J. Algebra Appl. **5** (2006), 441–463.
- [4] Hall J.I., *Moufang loops and groups with triality are essentially the same thing*, submitted.
- [5] Mikheev P.O., *Enveloping groups of Moufang loops*, Uspekhi Mat. Nauk **48** (1993), 191–192; translation in Russian Math. Surveys **48** (1993), 195–196.
- [6] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics, **7**, Heldermann, Berlin, 1990.

DEPARTMENT OF MATHEMATICS, MICHIGAN STATE UNIVERSITY, EAST LANSING, MICHIGAN 48824, U.S.A.

E-mail: jhall@math.msu.edu

(Received September 6, 2009, revised December 17, 2009)