Pseudoautomorphisms of Bruck loops and their generalizations

Mark Greer, Michael Kinyon

Abstract. We show that in a weak commutative inverse property loop, such as a Bruck loop, if α is a right [left] pseudoautomorphism with companion c, then c [c^2] must lie in the left nucleus. In particular, for any such loop with trivial left nucleus, every right pseudoautomorphism is an automorphism and if the squaring map is a permutation, then every left pseudoautomorphism is an automorphism as well. We also show that every pseudoautomorphism of a commutative inverse property loop is an automorphism, generalizing a well-known result of Bruck.

Keywords: pseudoautomorphism, Bruck loop, weak commutative inverse property

Classification: 20N05

A *loop* $(Q, \cdot)$ consists of a set Q with a binary operation $\cdot : Q \times Q \to Q$ such that (i) for all $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$, and (ii) there exists $1 \in Q$ such that $1x = x1 = x$ for all $x \in Q$. We denote these unique solutions by $x = a\backslash b$ and $y = b/a$, respectively. For $x \in Q$, define the *right* and *left translations* by x by, respectively, $yR_x = yx$ and $yL_x = xy$ for all $y \in Q$. That these mappings are permutations of Q is essentially part of the definition of loop. Standard reference in loop theory are [7], [13].

A triple (α, β, γ) of permutations of a loop Q is an *autotopism* if for all $x, y \in Q$, $x\alpha \cdot y\beta = (xy)\gamma$. The set $\mathrm{Atp}(Q)$ of all autotopisms of Q is a group under composition. Of particular interest here are the three subgroups

$$\begin{aligned}
\mathrm{Atp}_\lambda(Q) &= \{(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \mid 1\beta = 1\},\\
\mathrm{Atp}_\mu(Q) &= \{(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \mid 1\gamma = 1\},\\
\mathrm{Atp}_\rho(Q) &= \{(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \mid 1\alpha = 1\}.
\end{aligned}$$

For instance, say, $(\alpha, \beta, \gamma) \in \mathrm{Atp}_\lambda(Q)$. For all $x \in Q$, $x\alpha = x\alpha \cdot 1 = x\alpha \cdot 1\beta = (x1)\gamma = x\gamma$. Thus $\alpha = \gamma$. Set $a = 1\alpha$. For all $x \in Q$, $x\alpha = (1x)\alpha = 1\alpha \cdot x\beta = a \cdot x\beta$ Thus $\alpha = \beta L_a$, and so every element of $\mathrm{Atp}_\lambda(Q)$ has the form $(\beta L_a, \beta, \beta L_a)$ for some $a \in Q$. Conversely, it is easy to see that if a triple of permutations of that form is an autotopism, then $1\beta = 1$.

By similar arguments for the other two cases, we have the following characterizations:

$$\begin{aligned}\mathrm{Atp}_\lambda(Q) &= \mathrm{Atp}(Q) \cap \{(\beta L_a, \beta, \beta L_a) \mid \beta \in \mathrm{Sym}(Q), a \in Q\},\\ \mathrm{Atp}_\mu(Q) &= \mathrm{Atp}(Q) \cap \{(\gamma R_{c\backslash 1}^{-1}, \gamma L_c^{-1}, \gamma) \mid \gamma \in \mathrm{Sym}(Q), c \in Q\},\\ \mathrm{Atp}_\rho(Q) &= \mathrm{Atp}(Q) \cap \{(\alpha, \alpha R_b, \alpha R_b) \mid \alpha \in \mathrm{Sym}(Q), b \in Q\}.\end{aligned}$$

Since these special types of autotopisms are entirely determined by a single permutation and an element of the loop, it is customary to focus on those instead of on the autotopisms themselves. This motivates the following definitions.

Let Q be a loop. If $\beta \in \mathrm{Sym}(Q)$ and $a \in Q$ satisfy

$$a \cdot (xy)\beta = (a \cdot x\beta)(y\beta) \tag{1}$$

for all $x, y \in Q$, then β is called a *left pseudoautomorphism* with *companion a*. If $\gamma \in \mathrm{Sym}(Q)$ and $c \in Q$ satisfy

$$(xy)\gamma = [(x\gamma)/(c\backslash 1)][c\backslash(y\gamma)] \tag{2}$$

for all $x, y \in Q$, then γ is called a *middle pseudoautomorphism* with *companion c*. Finally, if $\alpha \in \mathrm{Sym}(Q)$ and $b \in Q$ satisfy

$$(xy)\alpha \cdot b = (x\alpha)(y\alpha \cdot b) \tag{3}$$

for all $x, y \in Q$, then α is called a *right pseudoautomorphism* with *companion b*.

Pseudoautomorphisms can also be viewed as isomorphisms between loop isotopes where the isotopy is determined by the companion. Since this perspective will not play a role in what follows, we leave the details to the literature [7].

There are some specializations of the notion of pseudoautomorphism worth mentioning explicitly. First, recall that the *left*, *middle* and *right nucleus* of a loop Q are the sets

$$\begin{aligned}N_\lambda(Q) &= \{a \in Q \mid ax \cdot y = a \cdot xy,\ \forall x, y \in Q\},\\ N_\mu(Q) &= \{c \in Q \mid xc \cdot y = x \cdot cy,\ \forall x, y \in Q\},\\ N_\rho(Q) &= \{b \in Q \mid xy \cdot b = x \cdot yb,\ \forall x, y \in Q\},\end{aligned}$$

respectively.

We denote the identity mapping on Q by ι.

Lemma 1. *Let Q be a loop. The nuclei are characterized as follows:*

$$\begin{aligned}
N_\lambda(Q) &= \{a \in Q \mid (\iota L_a, \iota, \iota L_a) \in \mathrm{Atp}(Q)\} \\
&= \{a \in Q \mid \iota \text{ is a left pseudoautomorphism with companion } a\}, \\
N_\mu(Q) &= \{c \in Q \mid (\iota R_c, \iota L_c^{-1}, \iota) \in \mathrm{Atp}(Q)\} \\
&= \{c \in Q \mid \iota \text{ is a middle pseudoautomorphism with companion } c\}, \\
N_\rho(Q) &= \{b \in Q \mid (\iota, \iota R_b, \iota R_b) \in \mathrm{Atp}(Q)\} \\
&= \{b \in Q \mid \iota \text{ is a right pseudoautomorphism with companion } b\}.
\end{aligned}$$

Proof: Perhaps the only claim which is not immediately obvious is the characterization of the middle nucleus. Suppose ι is a middle pseudoautomorphism with companion c. Then for all $x, y \in Q$, $xy = [x/(c\backslash 1)][c\backslash y]$. Replace y with cy to get $x \cdot cy = [x/(c\backslash 1)]y$. Set $y = 1$ so that $xc = x/(c\backslash 1)$. Thus $x \cdot cy = xc \cdot y$, that is, $c \in N_\mu(Q)$. The reverse inclusion is similarly straightforward. □

Note that all three of the nuclei are subloops. This can be proved directly from their definitions, but perhaps the easiest proof uses the autotopic characterization of Lemma 1.

A permutation σ of a loop Q is an *automorphism* of Q if $(xy)\sigma = (x\sigma)(y\sigma)$ for all $x, y \in Q$. Observe that a permutation σ is an automorphism if and only if it is a pseudoautomorphism of any of the three types with companion 1. The following is also clear from Lemma 1.

Lemma 2. *Let Q be a loop. If $\sigma \in \mathrm{Sym}(Q)$ is a left [middle, right] pseudoautomorphism with companion $c \in Q$ then σ is an automorphism if and only if $c \in N_\lambda(Q)$ [$N_\mu(Q)$, $N_\rho(Q)$].*

A loop Q is said to be a (right) *Bruck loop* if it satisfies the *Bol identity* $[(xy)z]y = x[(yz)y]$ for all $x, y, z \in Q$ and the *automorphic inverse property* (AIP):

$$\text{(AIP)} \qquad (xy)^{-1} = x^{-1}y^{-1}$$

for all $x, y \in Q$. (Bruck loops have also been called "K-loops" [10] or "gyrocommutative gyrogroups" [14]. Note that much of the literature works with the dual notion of *left* Bruck loop.) In a Bruck loop Q, inverses are two-sided, that is, $1/x = x\backslash 1 = x^{-1}$, and the *right inverse property* (RIP) holds:

$$\text{(RIP)} \qquad xy \cdot y^{-1} = x \qquad \text{or equivalently} \qquad R_y^{-1} = R_{y^{-1}}$$

for all $x, y \in Q$. Bruck loops have been intensively studied in recent years [1], [2], [3], [4], [5], [8], [10], [12].

The interest in Bruck loops is partly because they are a naturally occurring class. As an example, consider the set $S_n^+(\mathbb{R})$ of all $n \times n$ positive definite, symmetric matrices. By the polar decomposition, the product AB of two such matrices decomposes uniquely as $AB = UP$ where U is an orthogonal matrix and

$P \in S_n^+(\mathbb{R})$. Define $A \odot B = P$. Then it is straightforward to show that $(S_n^+(\mathbb{R}), \odot)$ is a Bruck loop (see, *e.g.*, [10]).

Bruck loops are the motivation for our main result below, but we will state and prove it in much more generality (hence the generalizations mentioned in the title). The class of loops we will consider are those with two-sided inverses such that the following identity holds:

$$(xy)^{-1}y = x^{-1} \tag{WCIP}$$

for all x, y. These were introduced by Johnson and Sharma [9] who called them *weak commutative inverse property loops* (WCIP loops). It is clear that any loop with the RIP and AIP satisfies WCIP. This applies in particular to Bruck loops or even to the more general class of Kikkawa loops [10]. In fact, it is evident that any two of the properties RIP, AIP and WCIP imply the third.

Lemma 3. *A loop Q has the WCIP if and only if for all $x, y \in Q$,*

$$y^{-1} \backslash x^{-1} = x \backslash y. \tag{WCIP2}$$

Proof: Replacing y in (WCIP) with $x\backslash y$ and rearranging, we obtain (WCIP2). Replacing y in (WCIP2) with xy and rearranging, we obtain (WCIP). $\square$

In particular, Lemma 3 shows that a loop Q has the WCIP if and only if the isotrophic loop [13] $(Q, \circ)$ defined by $x \circ y = x^{-1} \backslash y$ is commutative.

Before turning to our main result, we will show that in the present setting we can dispense with the notion of middle pseudoautomorphism. In a loop Q with two-sided inverses, we will denote the inversion map by $J : Q \to Q; x \mapsto x^{-1}$.

Lemma 4. *Let Q be loop with WCIP. If $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$, then $(J\gamma J, \beta, J\alpha J) \in \mathrm{Atp}(Q)$.*

Proof: Since $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$, we have $x\alpha \cdot y\beta = (xy)\gamma$ for all $x, y \in Q$. Thus $(xy)\gamma J \cdot y\beta = (x\alpha \cdot y\beta)J \cdot y\beta = x\alpha J$ using the WCIP. Replace x with $(xy)^{-1}$ and use the WCIP again to get $xJ\gamma J \cdot y\beta = (xy)J\alpha J$ for all $x, y \in Q$. Thus $(J\gamma J, \beta, J\alpha J) \in \mathrm{Atp}(Q)$. $\square$

Lemma 5. *Let Q be a loop with WCIP and let $\sigma \in \mathrm{Sym}(Q)$. Then σ is a middle pseudoautomorphism with companion c if and only if $J\sigma J$ is a right pseudoautomorphism with companion c^{-1}.*

Proof: Suppose σ is a middle pseudoautomorphism with companion c so that $(\sigma R_{c^{-1}}^{-1}, \sigma L_c^{-1}, \sigma)$ is an autotopism. By Lemma 4, $(J\sigma J, \sigma L_c^{-1}, J\sigma R_{c^{-1}}^{-1} J) \in \mathrm{Atp}(Q)$. Since the first component fixes 1, this autotopism lies in $\mathrm{Atp}_\rho(Q)$, and so the second and third components coincide and have the form $J\sigma J R_d$ for some d. To determine d, we compute $d = 1J\sigma R_{c^{-1}}^{-1} J = c^{-1}$. Thus $(J\sigma J, J\sigma J R_c, J\sigma J R_c) \in \mathrm{Atp}_\rho(Q)$, that is, σ is a right pseudoautomorphism with companion c^{-1}. The converse is similar. $\square$

As an aside, we mention that a similar result holds for loops with the right inverse property: σ is a middle pseudoautomorphism with companion c if and only if σ is a right pseudoautomorphism with companion c. In place of Lemma 4, the argument uses the fact that in RIP loops, $(\alpha,\beta,\gamma)\in \mathrm{Atp}(Q)$ implies $(\gamma, J\beta J,\alpha)\in \mathrm{Atp}(Q)$ [10].

As a corollary of Lemmas 1 and 5, we re-obtain a fact from [9].

Corollary 6. *In a loop Q with WCIP, $N_\mu(Q)=N_\rho(Q)$.*

Our main result is the following.

Theorem 7. *Let Q be a WCIP loop, let σ be a permutation of Q and let $c\in Q$.*

(1) *If σ is a right pseudoautomorphism of Q with companion c, then $c\in N_\lambda(Q)$.*
(2) *If σ is a left pseudoautomorphism of Q with companion c, then c^{-1} is also a companion of σ and $c^2\in N_\lambda(Q)$.*

Proof: (1) Since $1=yy^{-1}=y\cdot x(x\backslash y^{-1})$, we have

$$c=1\sigma\cdot c=y\sigma\cdot((x(x\backslash y^{-1}))\sigma\cdot c)=y\sigma\cdot[x\sigma\cdot((x\backslash y^{-1})\sigma\cdot c)].$$

Thus

$$x\sigma\backslash(y\sigma\backslash c)=(x\backslash y^{-1})\sigma\cdot c. \tag{4}$$

Exchanging the roles of x and y, we also have

$$y\sigma\backslash(x\sigma\backslash c)=(y\backslash x^{-1})\sigma\cdot c. \tag{5}$$

By (WCIP2), the right sides of (4) and (5) are equal, and so

$$x\sigma\backslash(y\sigma\backslash c)=y\sigma\backslash(x\sigma\backslash c). \tag{6}$$

Replacing x with $x\sigma^{-1}$ and y with $y\sigma^{-1}$ in (6), we have $x\backslash(y\backslash c)=y\backslash(x\backslash c)$, and so

$$x(y\backslash(x\backslash c))=y\backslash c. \tag{7}$$

Setting $x=c$ in (7), we obtain

$$y\backslash c=cy^{-1}. \tag{8}$$

Using (8) in (7), we have

$$x(y\backslash(cx^{-1}))=cy^{-1}. \tag{9}$$

Taking $y=cx^{-1}$ in (9), we get

$$c(cx^{-1})^{-1}=x. \tag{10}$$

Now in (9), replace x with cx^{-1} and use (10) and (WCIP2) to obtain

$$cx^{-1} \cdot (x^{-1} \backslash y^{-1}) = cy^{-1}. \tag{11}$$

Finally, in (11), replace x with x^{-1} and y with y^{-1}, and then replace y with xy to get

$$cx \cdot y = c \cdot xy,$$

which shows $c \in N_\lambda(Q)$, as claimed.

(2) Since $(\sigma L_c, \sigma, \sigma L_c) \in \mathrm{Atp}(Q)$, we have $(J\sigma L_c J, \sigma, J\sigma L_c J) \in \mathrm{Atp}(Q)$ by Lemma 3. Since $1\sigma = 1$, this autotopism lies in $\mathrm{Atp}_\lambda(Q)$. Thus $J\sigma L_c J = \sigma L_d$ where $d = 1J\sigma L_c J = c^{-1}$. Hence $(\sigma L_{c^{-1}}, \sigma, \sigma L_{c^{-1}}) \in \mathrm{Atp}(Q)$, which shows that σ has c^{-1} as a companion. We have

$$(L_{c^{-1}}^{-1}\sigma^{-1}, \sigma^{-1}, L_{c^{-1}}^{-1}\sigma^{-1})(\sigma L_c, \sigma, \sigma L_c) = (L_{c^{-1}}^{-1} L_c, \iota, L_{c^{-1}}^{-1} L_c) \in \mathrm{Atp}(Q).$$

Therefore $L_{c^{-1}}^{-1} L_c = L_e$ where $e = 1L_{c^{-1}}^{-1} L_c = c^2$. Thus $(L_{c^2}, \iota, L_{c^2}) \in \mathrm{Atp}(Q)$, that is, $c^2 \in N_\lambda(Q)$. □

Corollary 8. *Let Q be a WCIP loop with trivial left nucleus. Then every right pseudoautomorphism is an automorphism. If, in addition, every element of Q has a unique square root, then every left pseudoautomorphism is an automorphism.*

Example 9. The *relativistic Bruck loop* (or relativistic gyrocommutative gyrogroup) is the set of relativistic velocity vectors with Einstein's velocity addition as the operation [14]. This is isomorphic to the natural Bruck loop structure on the set of positive definite symmetric Lorentz transformations [10, Chapter 10]. The left nucleus is trivial, because it is precisely the set of fixed points of the action of the special orthogonal group. In addition, every element of the loop has a unique square root. Thus we obtain: *In the relativistic Bruck loop, every pseudoautomorphism is an automorphism.*

Finally, we generalize a well-known result of Bruck [6], who proved the following for commutative Moufang loops.

Corollary 10. *Every pseudoautomorphism of a commutative, inverse property loop is an automorphism.*

Proof: In an inverse property loop, all nuclei coincide, so by Theorem 7 and its left/right dual, the companion of any pseudoautomorphism lies in the nucleus of Q. By Lemma 2, we have the desired result. □

Acknowledgment. Our investigations were aided by the automated deduction tool Prover9 developed by McCune [11]. The problem of the existence of pseudoautomorphisms of the relativistic Bruck loop which are not automorphisms was suggested to the second author several years ago by Anton Greil.

References

[1] Aschbacher M., *Bol loops of exponent* 2, J. Algebra **288** (2005), 99–136.

[2] Aschbacher M., Kinyon M.K., Phillips J.D., *Finite Bruck loops*, Trans. Amer. Math. Soc. **358** (2006), 3061–3075.

[3] Baumeister B., Stein A., *Self-invariant* 1*-factorizations of complete graphs and finite Bol loops of exponent* 2, Beiträge Algebra Geom. **51** (2010), 117–135.

[4] Baumeister B., Stroth G., Stein A., *On Bruck loops of* 2*-power exponent*, J. Algebra **327** (2011), 316–336.

[5] Baumeister B., Stein A., *The finite Bruck loops*, J. Algebra **330** (2011), 206–220.

[6] Bruck R.H., *Pseudo-automorphisms and Moufang loops*, Proc. Amer. Math. Soc. **3** (1952), 66–72.

[7] Bruck R.H., *A Survey of Binary Systems*, Springer, Berlin, 1971

[8] Glauberman G., *On loops of odd order I*, J. Algebra **1** (1964), 374–396.

[9] Johnson K.W., Sharma B.L., *A variety of loops*, Ann. Soc. Sci. Bruxelles Sér. I **92** (1978), 25–41.

[10] Kiechle H., *Theory of K-loops*, Lecture Notes in Mathematics, 1778, Springer, Berlin, 2002.

[11] McCune W.W., *Prover9,* version 2009-11A, `http://www.cs.unm.edu/~mccune/prover9/`

[12] Nagy G.P., *A class of finite simple Bol loops of exponent* 2, Trans. Amer. Math. Soc. **361** (2009), 5331–5343.

[13] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math., 7, Heldermann, Berlin, 1990.

[14] Ungar A.A., *Beyond the Einstein addition law and its gyroscopic Thomas precession: The theory of gyrogroups and gyrovector spaces*, Fundamental Theories of Physics, 117, Kluwer, Dordrecht, 2001.

Department of Mathematics, 2360 S Gaylord St, University of Denver, Denver, CO 80208, USA

E-mail: mark.greer@du.edu
mkinyon@du.edu

(*Received* April 10, 2012, *revised* April 24, 2012)