Commutative Automorphic Loops Arising from Groups

Lee Raney
(joint work with Mark Greer)

Department of Mathematics
University of North Alabama

Loops 2019
Budapest University of Technology and Economics, Hungary
8 July, 2019

Theorem (Thompson, 1964)

Let p be an odd prime and let A be the semidirect product of a p-subgroup P with a normal p'-subgroup Q. Suppose that A acts on a p-group G such that

$$C_G(P) \leq C_G(Q).$$

Then Q acts trivially on G.

A proof due to Bender (1967) makes use of the following binary operation.

Definition (Baer, 1957)

Let G be a uniquely 2-divisible group. For $x, y \in G$, define

$$x \circ y = xy[y, x]^{1/2},$$

where $[y, x]$ is the commutator $y^{-1}x^{-1}yx$, and $z^{1/2}$ is the unique element $u \in P$ such that $u^2 = z$.

Observations about $\circ$

- $x \circ y = y \circ x$
- $1 \circ x = x$
- (Greer, 2014) If $x \circ a = b$, then $x = a \backslash b = (a^{-1}ba^{-1}b^{-1})^{1/2}b$.

Thus, $(G, \circ)$ is a commutative loop.

- If G is abelian, then $(G, \circ) = G$.
- G has nilpotency class at most 2 (i.e. $G' = [G, G] \leq Z(G)$) if and only if $(G, \circ)$ is an abelian group.

In general, what can be said about the loop structure of $(G, \circ)$?

Definition

A loop Q is *Moufang* if Q satisfies any of the (equivalent) identities

- $z(x(zy)) = ((zx)z)y$
- $x(z(yz)) = ((xz)y)z$
- $(zx)(yz) = (z(xy))z$
- $(zx)(yz) = z((xy)z)$,

known as the *Moufang identities*, for all $x, y, z \in Q$.

Definition

A group G is *2-Engel* (or *Levi*) if $[[x, y], x] = 1$ for all $x, y \in G$.

Proposition (Greer)

Let G be a uniquely 2-divisible group. Then $(G, \circ)$ is Moufang if and only if G is 2-Engel.

Definition (Greer, 2014)

A loop Q is a Γ-*loop* if each of the following is satisfied:

1. Q is commutative.
2. Q has the *automorphic inverse property*: for all $x, y \in Q$, $(xy)^{-1} = x^{-1}y^{-1}$.
3. For all $x \in Q$, $L_x L_{x^{-1}} = L_{x^{-1}} L_x$ (where $zL_x = xz$).
4. For all $x, y \in Q$, $P_x P_y P_x = P_{yP_x}$ (where $zP_x = x^{-1}\backslash(zx)$)

Theorem (Greer, 2014)

Let G be a uniquely 2-divisible group. Then $(G, \circ)$ is a Γ-loop.

Definition

A *(left) Bruck loop* is a loop Q which satisfies each of the following identities:

1. $(x(yx))z = x(y(xz))$
2. $(xy)^{-1} = x^{-1}y^{-1}$

Theorem (Glauberman, 1964)

Let G be a uniquely 2-divisible group. Then $(G, \oplus)$, where

$$x \oplus y = (xy^2x)^{1/2},$$

is a Bruck loop.

Theorem (Greer, 2014)

The categories $\mathbf{BrLp_o}$ *of Bruck loops of odd order and* $\mathbf{\Gamma Lp_o}$ *of* Γ*-loops of odd order are isomorphic.*

In particular, the functor $\mathcal{G} : \mathbf{BrLp_o} \to \mathbf{\Gamma Lp_o}$ given by $Q \mapsto (L_Q, \circ)$ is an isomorphism, where L_Q is a particular *twisted subgroup* of $\mathrm{Mlt}_\lambda(Q) = \langle L_x \mid x \in Q \rangle$, the left multiplication group of Q. This correspondence can be used to study multiplication groups of Bruck loops.

Definition (Aschbacher, 1998)

A *twisted subgroup* of a group G is a subset T of G such that $1 \in T$ and for all $x, y \in T$, $x^{-1} \in T$ and $xyx \in T$.

Definition

Let Q be a loop. The *inner mapping group*, $\mathrm{Inn}(Q)$ is the stabilizer of 1 in the multiplication group of Q.

Theorem (Bruck?)

$\mathrm{Inn}(Q)$ *is generated by the following transformations* $Q \to Q$*:*

- $L_{x,y} = L_x L_y L_{yx}^{-1}$
- $R_{x,y} = R_x R_y R_{xy}^{-1}$
- $T_x = L_x^{-1} R_x$,

where L_x *and* R_x *and the maps* $z \mapsto xz$ *and* $z \mapsto zx$*, resp.*

Definition

A loop Q is said to be an *automorphic loop* (or *A-loop*) if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

Theorem (Greer, 2014)

Commutative automorphic loops are Γ*-loops.*

Conjecture (Greer-Kinyon)

A Γ-loop is automorphic if and only if the (left) multiplication group of the corresponding Bruck loop is metabelian.

Recall that a group G is *metabelian* if there is an abelian normal subgroup A of G such that G/A is also abelian; equivalently, G' is abelian.

We approach this problem with a similar conjecture.

Conjecture

Let G be a finite group of odd order. Then $(G, \circ)$ is automorphic if and only if G is metabelian.

Now, for the duration, let G be the semidirect product of a normal abelian subgroup H of odd order acted on (as automorphisms) by an abelian group F of odd order. Then

$$G = H \rtimes F$$

and

$$(h_1, f_1)(h_2, f_2) = (h_1 f_1(h_2), f_1 f_2).$$

Note that G is metabelian (we call such groups *split metabelian*).

Lemma

Suppose H is an abelian group of odd order, and $\alpha, \beta \in \mathrm{Aut}(H)$ are commuting automorphisms of odd order. Then the map $h \mapsto \alpha(h)\beta(h)$ is an automorphism of H.

In particular, for any $f \in F$, the map $\phi_f : H \to H$ given by $\phi_f(h) = hf(h)$ is an automorphism of H which commutes with each automorphism in F.

Lemma

Let $u = (h, f), x = (h_1, f_2), y = (h_2, f_2) \in G$. Then

- $x \circ y = ((\phi_{f_1}(h_2)\phi_{f_2}(h_1))^{1/2}, f_1 f_2)$
- $uL_{x,y} = \left(\phi_{f_1 f_2}^{-1}\left(\phi_{f_1}\phi_{f_2}(h)\phi_{ff_1}(h_2)f(h_2)^{-1}f_1(h_2)^{-1}\right)^{1/2}, f\right)$

Note that since $(G, \circ)$ is commutative, $L_{x,y} = R_{x,y}$ and $T_x = id_G$.

Theorem

Let G be a split metabelian group of odd order. Then $(G, \circ)$ is automorphic.

Corollary

If $|G|$ is any one of the following (for distinct odd primes p and q), then $(G, \circ)$ is automorphic.

- pq *(where p divides $q - 1$)*
- p^2q
- p^2q^2

Note that if $|G| = p$, pq (where $p \nmid q - 1$), p^2, or p^3, then G has class at most 2, and hence $(G, \circ)$ is an abelian group.

Corollary

Let p and q be distinct odd primes with p dividing $q - 1$. Then there is exactly one nonassociative, commutative, automorphic loop of order pq.

This result follows since there is a unique nonassociative Bruck loop of order pq above [Kinyon-Nagy-Vojtěchovský, 2017].

Suppose $|G| = p^4$ (odd prime). Then G is metabelian. There are 15 such groups. All but one of them are split.

- If $|G| = 3^4$, then $(G, \circ)$ is automorphic.
- For $p > 3$, the non-split metabelian group of order p^4 is $(\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p) \rtimes \mathbb{Z}_p$.

Groups of order p^5 are metabelian.

Connection to quandles/food for thought:

- Due to [Kikkawa-Robinson, 1973/1979], there is a one-to-one correspondence between involutory latin quandles and Bruck loops of odd order.
- Does there exist a class of quandles corresponding in a similar manner to Γ-loops such that the following diagram commutes?

$$\begin{array}{ccc} \Gamma\text{-loops} & \longrightarrow & \text{Bruck loops} \\ \downarrow & & \downarrow \\ \text{??-quandles} & \longrightarrow & \text{inv. latin quandles} \end{array}$$

- What properties of ??-quandles/involutory latin quandles corresponds to commutative automorphic loop/metabelian left multiplication group?

Thank you!