

# Commutative automorphic $p$ -loops

Přemysl Jedlička<sup>1</sup>, Michael K. Kinyon<sup>2</sup>, Petr Vojtěchovský<sup>2</sup>

<sup>1</sup>Department of Mathematics  
Faculty of Engineering (former Technical Faculty)  
Czech University of Life Sciences (former Czech University of Agriculture), Prague

<sup>2</sup>Department of Mathematics  
University of Denver



AAA 80, Będlewo  
2<sup>nd</sup> June 2010



# Quasigroups

## Definition

Let  $(G, \cdot)$  be a groupoid. The mapping  $L_x : a \mapsto xa$  is called the *left translation* and the mapping  $R_x : a \mapsto ax$  the *right translation*.

## Definition (Combinatorial)

A groupoid  $(Q, \cdot)$  is called a *quasigroup* if the mappings  $L_x$  and  $R_x$  are bijections, for each  $x \in Q$ .

## Definition (Universal algebraic)

The algebra  $(Q, \cdot, /, \backslash)$  is called a *quasigroup* if it satisfies the following identities:

$$x \backslash (x \cdot y) = y$$

$$(x \cdot y) / y = x$$

$$x \cdot (x \backslash y) = y$$

$$(x / y) \cdot y = x$$

# Quasigroups

## Definition

Let  $(G, \cdot)$  be a groupoid. The mapping  $L_x : a \mapsto xa$  is called the *left translation* and the mapping  $R_x : a \mapsto ax$  the *right translation*.

## Definition (Combinatorial)

A groupoid  $(Q, \cdot)$  is called a *quasigroup* if the mappings  $L_x$  and  $R_x$  are bijections, for each  $x \in Q$ .

## Definition (Universal algebraic)

The algebra  $(Q, \cdot, /, \backslash)$  is called a *quasigroup* if it satisfies the following identities:

$$x \backslash (x \cdot y) = y$$

$$(x \cdot y) / y = x$$

$$x \cdot (x \backslash y) = y$$

$$(x / y) \cdot y = x$$

# Loops

## Definition

A quasigroup  $Q$  is called a *loop* if it contains the identity element.

## Example (A minimal nonassociative loop)

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

# Multiplication Groups

## Definitions

Let  $Q$  be a loop.

- The group generated by  $L_x$  and  $R_x$ , for all  $x \in Q$ , is called *the multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ .
- The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called *the inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ .

## Fact

*An inner mapping of a loop needs not to be an automorphism.*

## Definition

A loop  $Q$  is called an *automorphic loop* (or an *A-loop*) if  $\text{Inn}(Q) \leq \text{Aut}(Q)$ .

# Multiplication Groups

## Definitions

Let  $Q$  be a loop.

- The group generated by  $L_x$  and  $R_x$ , for all  $x \in Q$ , is called *the multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ .
- The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called *the inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ .

## Fact

*An inner mapping of a loop needs not to be an automorphism.*

## Definition

A loop  $Q$  is called an *automorphic loop* (or an *A-loop*) if  $\text{Inn}(Q) \leq \text{Aut}(Q)$ .

# Multiplication Groups

## Definitions

Let  $Q$  be a loop.

- The group generated by  $L_x$  and  $R_x$ , for all  $x \in Q$ , is called *the multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ .
- The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called *the inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ .

## Fact

*An inner mapping of a loop needs not to be an automorphism.*

## Definition

A loop  $Q$  is called an *automorphic loop* (or an *A-loop*) if  $\text{Inn}(Q) \leq \text{Aut}(Q)$ .

# Multiplication Groups

## Definitions

Let  $Q$  be a loop.

- The group generated by  $L_x$  and  $R_x$ , for all  $x \in Q$ , is called *the multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ .
- The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called *the inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ .

## Fact

*An inner mapping of a loop needs not to be an automorphism.*

## Definition

A loop  $Q$  is called an *automorphic loop* (or an *A-loop*) if  $\text{Inn}(Q) \leq \text{Aut}(Q)$ .



# Multiplication Groups

## Definitions

Let  $Q$  be a loop.

- The group generated by  $L_x$  and  $R_x$ , for all  $x \in Q$ , is called *the multiplication group* of  $Q$  and it is denoted by  $\text{Mlt}(Q)$ .
- The subgroup of  $\text{Mlt}(Q)$  stabilizing the neutral element of  $Q$  is called *the inner mapping group* of  $Q$  and it is denoted by  $\text{Inn}(Q)$ .

## Fact

*An inner mapping of a loop needs not to be an automorphism.*

## Definition

A loop  $Q$  is called an *automorphic loop* (or an *A-loop*) if  $\text{Inn}(Q) \leq \text{Aut}(Q)$ .

# Basic properties of A-loops

## Fact

*Any characteristic subloop of an A-loop is normal.*

Theorem (R. H. Bruck, J. L. Paige)

*Every monogenerated subloop of an A-loop is a group.*

## Notation

We write  $x^3$  instead of  $x \cdot (x \cdot x)$  or  $(x \cdot x) \cdot x$ .

We write  $x^{-1}$  instead of  $1/x$  or  $x \setminus 1$ .

# Basic properties of A-loops

## Fact

*Any characteristic subloop of an A-loop is normal.*

## Theorem (R. H. Bruck, J. L. Paige)

*Every monogenerated subloop of an A-loop is a group.*

## Notation

We write  $x^3$  instead of  $x \cdot (x \cdot x)$  or  $(x \cdot x) \cdot x$ .

We write  $x^{-1}$  instead of  $1/x$  or  $x \setminus 1$ .

# Basic properties of A-loops

## Fact

*Any characteristic subloop of an A-loop is normal.*

## Theorem (R. H. Bruck, J. L. Paige)

*Every monogenerated subloop of an A-loop is a group.*

## Notation

We write  $x^3$  instead of  $x \cdot (x \cdot x)$  or  $(x \cdot x) \cdot x$ .

We write  $x^{-1}$  instead of  $1/x$  or  $x \setminus 1$ .

# Variety of A-loops

## Fact

Let  $Q$  be a loop. The inner mapping group of  $Q$  is generated by the mappings

$$L_{xy}^{-1}L_xL_y, \quad R_{xy}^{-1}R_xR_y \quad \text{and} \quad L_x^{-1}R_x,$$

where  $x, y \in Q$ .

## Corollary

A loop is an A-loop iff it satisfies the following three identities:

$$\begin{aligned} (xy) \setminus (x(y \cdot uv)) &= ((xy) \setminus (x \cdot yu)) \cdot ((xy) \setminus (x \cdot yv)), \\ ((uv \cdot x)y) / (xy) &= ((ux \cdot y) / (xy)) \cdot ((vx \cdot y) / (xy)), \\ x \setminus (uv \cdot x) &= (x \setminus (ux)) \cdot (x \setminus (vx)). \end{aligned}$$

# Variety of A-loops

## Fact

Let  $Q$  be a loop. The inner mapping group of  $Q$  is generated by the mappings

$$L_{xy}^{-1}L_xL_y, \quad R_{xy}^{-1}R_xR_y \quad \text{and} \quad L_x^{-1}R_x,$$

where  $x, y \in Q$ .

## Corollary

A loop is an A-loop iff it satisfies the following three identities:

$$\begin{aligned} (xy) \setminus (x(y \cdot uv)) &= ((xy) \setminus (x \cdot yu)) \cdot ((xy) \setminus (x \cdot yv)), \\ ((uv \cdot x)y) / (xy) &= ((ux \cdot y) / (xy)) \cdot ((vx \cdot y) / (xy)), \\ x \setminus (uv \cdot x) &= (x \setminus (ux)) \cdot (x \setminus (vx)). \end{aligned}$$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$



# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Uniquely 2-divisible loops

## Definition

A loop  $Q$  is called *uniquely 2-divisible* if the map  $x \mapsto x^2$  is a bijection.

## Lemma

Let  $Q$  be a finite commutative loop with both-sided inverses. Then  $Q$  is uniquely 2-divisible if and only if  $|Q|$  is odd.

## Proof.

" $\Rightarrow$ ": If  $Q$  is uniquely 2-divisible then it contains no element of order 2. Hence the bijection  $x \mapsto x^{-1}$  has only one fixed point and the number of nonidentity elements of  $Q$  is even.

" $\Leftarrow$ ": Fix  $c \in Q$ . The set  $\{(x, y); xy = c\}$  has size  $|Q|$ , that means an odd size. By commutativity, the set  $\{(x, y); xy = c \text{ \& } x \neq y\}$  is of an even size. Hence there exists  $x \in Q$  such that  $x^2 = c$ .  $\square$

# Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

Corollary

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.

# Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

Corollary

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.

# Commutatives A-loops of odd orders

**Proposition (P. J., M. K., P. V.)**

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

**Corollary**

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.



# Commutatives A-loops of odd orders

**Proposition** (P. J., M. K., P. V.)

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

**Corollary**

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.

# Commutatives A-loops of odd orders

**Proposition** (P. J., M. K., P. V.)

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

**Corollary**

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.

# Commutatives A-loops of odd orders

## Proposition (P. J., M. K., P. V.)

Let  $(Q, \cdot)$  be a uniquely 2-divisible commutative A-loop. We associate to  $Q$  an operation  $\circ$  defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then  $Q$  is a Bruck loop. Moreover, the powers in  $(Q, \cdot)$  coincide with the powers in  $(Q, \circ)$

## Corollary

- Lagrange theorem,
- If  $p \mid |Q|$ , for  $p$  prime, then there exists  $x \in Q$  of order  $p$ ,
- Existence of Sylow  $p$ -subloops,
- Solvability.

# Nilpotency of loops

## Definition

Let  $Q$  be a loop. The *center* of  $Q$  is the set

$$Z(Q) = \{a \in Q; \varphi(a) = a \forall \varphi \in \text{Inn}(Q)\}$$

## Definition

Let  $Q$  be a loop. The *upper central series* of  $Q$  is

$$Z_0(Q) \leq Z_1(Q) \leq Z_2(Q) \leq \cdots \leq Z_n(Q) \leq \cdots \leq Q,$$

where  $Z_0(Q) = \{1\}$  and  $Z_i(Q)$  is the preimage of  $Z(Q/Z_{i-1}(Q))$ .  
If there exists some  $n$  such that  $Z_n(Q) = Q$  then  $Q$  is said to be  
(centrally) *nilpotent of class  $n$* .

# Nilpotency of loops

## Definition

Let  $Q$  be a loop. The *center* of  $Q$  is the set

$$Z(Q) = \{a \in Q; \varphi(a) = a \forall \varphi \in \text{Inn}(Q)\}$$

## Definition

Let  $Q$  be a loop. The *upper central series* of  $Q$  is

$$Z_0(Q) \leq Z_1(Q) \leq Z_2(Q) \leq \cdots \leq Z_n(Q) \leq \cdots \leq Q,$$

where  $Z_0(Q) = \{1\}$  and  $Z_i(Q)$  is the preimage of  $Z(Q/Z_{i-1}(Q))$ .

If there exists some  $n$  such that  $Z_n(Q) = Q$  then  $Q$  is said to be (*centrally*) *nilpotent of class  $n$* .

# Nilpotency of loops

## Definition

Let  $Q$  be a loop. The *center* of  $Q$  is the set

$$Z(Q) = \{a \in Q; \varphi(a) = a \forall \varphi \in \text{Inn}(Q)\}$$

## Definition

Let  $Q$  be a loop. The *upper central series* of  $Q$  is

$$Z_0(Q) \leq Z_1(Q) \leq Z_2(Q) \leq \cdots \leq Z_n(Q) \leq \cdots \leq Q,$$

where  $Z_0(Q) = \{1\}$  and  $Z_i(Q)$  is the preimage of  $Z(Q/Z_{i-1}(Q))$ .  
If there exists some  $n$  such that  $Z_n(Q) = Q$  then  $Q$  is said to be  
(centrally) *nilpotent of class  $n$* .

# Drápal's Construction

## Theorem (A. Drápal, refined by P. Jedlička & D. Simon)

Let  $K$  be the  $q$ -element finite field,  $\text{char}(K) \neq 2$ . Let  $k$  be an odd divisor either of  $q - 1$  or of  $q + 1$ . Take  $\xi$ , a  $k$ -th primitive root of unity. We define an operation  $*$  on the set  $Q = K \times \mathbb{Z}_k$  as follows:

$$(a, i) * (b, j) = \left( (a + b) \cdot \frac{(\xi^i + 1) \cdot (\xi^j + 1)}{2 \cdot (\xi^{i+j} + 1)}, i + j \right).$$

Then  $(Q, *)$  is a commutative automorphic loop,  $|Q|$  is odd and  $Z(Q) = 1$ .

# $p$ -loops

## Definition

Let  $Q$  be a loop where each element generates a cyclic subgroup and let  $p$  be a prime. The loop is called a  $p$ -loop if, for each  $x \in Q$ , there exists  $k$ , such that  $x^{p^k} = 1$ .

## Theorem (P. J., M. K., P. V.)

*Let  $Q$  be a finite commutative automorphic loop and let  $p$  be a prime. Then  $Q$  is a  $p$ -loop if and only if  $|Q| = p^k$  for some  $k$ .*



# $p$ -loops

## Definition

Let  $Q$  be a loop where each element generates a cyclic subgroup and let  $p$  be a prime. The loop is called a  $p$ -loop if, for each  $x \in Q$ , there exists  $k$ , such that  $x^{p^k} = 1$ .

## Theorem (P. J., M. K., P. V.)

*Let  $Q$  be a finite commutative automorphic loop and let  $p$  be a prime. Then  $Q$  is a  $p$ -loop if and only if  $|Q| = p^k$  for some  $k$ .*

# Nilpotency of commutative automorphic $p$ -loops

Theorem (P. J., M. K., P. V.)

Let  $Q(\cdot)$  be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop  $Q(\circ)$ . Then, for each non-negative integer  $n$ ,

$$Z_n(Q, \circ) = Z_n(Q, \cdot)$$

Corollary

Commutative automorphic  $p$ -loops are nilpotent, for each odd prime  $p$ .

# Nilpotency of commutative automorphic $p$ -loops

Theorem (P. J., M. K., P. V.)

Let  $Q(\cdot)$  be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop  $Q(\circ)$ . Then, for each non-negative integer  $n$ ,

$$Z_n(Q, \circ) = Z_n(Q, \cdot)$$

Corollary

Commutative automorphic  $p$ -loops are nilpotent, for each odd prime  $p$ .

# Commutative automorphic 2-loops with trivial center

## Proposition (P. J., M. K., P. V.)

Let  $G$  be a vector space over  $\mathbb{F}_2$  and let  $f$  be an automorphism of  $V$ . We construct an operation  $*$  on  $Q = V \times \mathbb{F}_2$  as follows:

$$(\vec{v}, i) * (\vec{w}, j) = (f^{i \cdot j}(\vec{v} + \vec{w}), i + j).$$

Then  $Q$  is a commutative automorphic loop of exponent 2.

If  $f$  is identical then  $Q$  is a group, otherwise

$$Z(Q) = \{\vec{u} \in V; f(\vec{u}) = \vec{u}\} \times 0.$$

## Corollary

There exist commutative automorphic 2-loops with trivial center.

# Commutative automorphic 2-loops with trivial center

## Proposition (P. J., M. K., P. V.)

Let  $G$  be a vector space over  $\mathbb{F}_2$  and let  $f$  be an automorphism of  $V$ . We construct an operation  $*$  on  $Q = V \times \mathbb{F}_2$  as follows:

$$(\vec{v}, i) * (\vec{w}, j) = (f^{i \cdot j}(\vec{v} + \vec{w}), i + j).$$

Then  $Q$  is a commutative automorphic loop of exponent 2.

If  $f$  is identical then  $Q$  is a group, otherwise

$$Z(Q) = \{\vec{u} \in V; f(\vec{u}) = \vec{u}\} \times 0.$$

## Corollary

There exist commutative automorphic 2-loops with trivial center.

# Commutative automorphic loops of order $p^3$

Proposition (P. J., M. K., P. V.)

For  $n \geq 1$  and  $a, b \in \mathbb{Z}_n$ , define  $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$  on  $\mathbb{Z}_n^3$  as

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = (x_1 + y_1 + (x_2 + y_2)x_3y_3 + \\ + a(x_2, y_2)_n + b(x_3, y_3)_n, x_2 + y_2, x_3 + y_3),$$

where

$$(x, y)_n = \begin{cases} 0 & \text{if } x + y < n, \\ 1 & \text{if } x + y \geq n. \end{cases}$$

The loop  $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$  is a commutative automorphic loop with  $Z(\mathcal{Q}_{a,b}(\mathbb{Z}_n)) = \mathbb{Z}_n \times 0 \times 0$ .

# References



R. H. Bruck, J. L. Paige:

Loops whose inner mappings are automorphisms,  
The Annals of Math., 2nd Series, **63**, no. 2, (1956), 308–323



A. Drápal: A class of comm. loops with metacyclic inner mapping groups, Comment. Math. Univ. Carolin. **49**,3 (2008) 357–382.



P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Constructions of commutative automorphic loops, to appear in Comm. in Alg.



P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Structure of commutative automorphic loops, to appear in Trans. of AMS



P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Commutative automorphic loops of odd prime power order (preprint)



P. Jedlička, D. Simon: Commutative A-loops of order  $pq$  (preprint)



M. K. Kinyon, K. Kunen, J. D. Phillips: Every diassociative A-loop is Moufang, Proc. Amer. Math. Soc. **130** (2002), 619–624