Constructions of commutative A-loops

Přemysl Jedlička[1], Michael K. Kinyon[2], Petr Vojtěchovský[2]

[1]Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture), Prague

[2]Department of Mathematics
University of Denver

2nd Mile High
Denver, June 22, 2009

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:

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

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

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:

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

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 $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

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

Definition

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

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 $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

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

Definition

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

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 $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

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

Definition

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

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 $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

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

Definition

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

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 $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

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

Definition

A loop Q is called an *A-loop* if $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$.

Characteristic subloops

Fact

Any characteristic subloop of an A-loop is normal.

Definition

Let Q be a loop. An element $a \in Q$ belongs to the *center* of Q if $ax = xa$, $a \cdot xy = ax \cdot y$, $x \cdot ay = xa \cdot y$, and $x \cdot ya = xy \cdot a$, for all $x, y \in Q$.

Definition

Let Q be a loop. We define the *left*, *right* and *middle nuclei* as

$$N_\lambda = \{a \in Q;\ a \cdot xy = ax \cdot y\ \forall x, y \in Q\};$$
$$N_\mu = \{a \in Q;\ x \cdot ay = xa \cdot y\ \forall x, y \in Q\};$$
$$N_\rho = \{a \in Q;\ x \cdot ya = xy \cdot a\ \forall x, y \in Q\}.$$

Characteristic subloops

Fact

Any characteristic subloop of an A-loop is normal.

Definition

Let Q be a loop. An element $a \in Q$ belongs to the *center* of Q if $ax = xa$, $a \cdot xy = ax \cdot y$, $x \cdot ay = xa \cdot y$, and $x \cdot ya = xy \cdot a$, for all $x, y \in Q$.

Definition

Let Q be a loop. We define the *left*, *right* and *middle nuclei* as

$$N_\lambda = \{a \in Q;\ a \cdot xy = ax \cdot y\ \forall x, y \in Q\};$$
$$N_\mu = \{a \in Q;\ x \cdot ay = xa \cdot y\ \forall x, y \in Q\};$$
$$N_\rho = \{a \in Q;\ x \cdot ya = xy \cdot a\ \forall x, y \in Q\}.$$

Characteristic subloops

Fact

Any characteristic subloop of an A-loop is normal.

Definition

Let Q be a loop. An element $a \in Q$ belongs to the *center* of Q if $ax = xa,\ a \cdot xy = ax \cdot y,\ x \cdot ay = xa \cdot y,$ and $x \cdot ya = xy \cdot a,$ for all $x, y \in Q$.

Definition

Let Q be a loop. We define the *left*, *right* and *middle nuclei* as

$$N_\lambda = \{a \in Q;\ a \cdot xy = ax \cdot y\ \forall x, y \in Q\};$$
$$N_\mu = \{a \in Q;\ x \cdot ay = xa \cdot y\ \forall x, y \in Q\};$$
$$N_\rho = \{a \in Q;\ x \cdot ya = xy \cdot a\ \forall x, y \in Q\}.$$

Variety of A-loops

Fact

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

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

where $x, y \in Q$.

Corollary

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

$$(xy)\backslash(x(y \cdot uv)) = ((xy)\backslash(x \cdot yu)) \cdot ((xy)\backslash(x \cdot yv)),$$
$$((uv \cdot x)y)/(xy) = ((ux \cdot y)/(xy)) \cdot ((vx \cdot y)/(xy)),$$
$$x\backslash(uv \cdot x) = (x\backslash(ux)) \cdot (x\backslash(vx)).$$

Variety of A-loops

Fact

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

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

where $x, y \in Q$.

Corollary

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

$$(xy)\backslash(x(y \cdot uv)) = ((xy)\backslash(x \cdot yu)) \cdot ((xy)\backslash(x \cdot yv)),$$
$$((uv \cdot x)y)/(xy) = ((ux \cdot y)/(xy)) \cdot ((vx \cdot y)/(xy)),$$
$$x\backslash(uv \cdot x) = (x\backslash(ux)) \cdot (x\backslash(vx)).$$

Examples of Commutative A-loops

Examples

Examples of commutative A-loops

- Commutative Moufang loops
- ? ? ?

Examples of Commutative A-loops

Examples

Examples of commutative A-loops

- Commutative Moufang loops
- ? ? ?

Examples of Commutative A-loops

Examples

Examples of commutative A-loops

- Commutative Moufang loops
- ? ? ?

Smallest Moufang Loop

Construction by O. Chein:

1	2	3	4	5	6	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
2	1	4	3	6	5	$\bar{2}$	$\bar{1}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$
3	6	5	2	1	4	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{1}$	$\bar{2}$
4	5	6	1	2	3	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{5}$	$\bar{6}$
5	4	1	6	3	2	$\bar{5}$	$\bar{6}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
6	3	2	5	4	1	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	1	2	3	4	5	6
$\bar{2}$	$\bar{1}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	2	1	4	3	6	5
$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{1}$	$\bar{2}$	3	6	5	2	1	4
$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{5}$	$\bar{6}$	4	5	6	1	2	3
$\bar{5}$	$\bar{6}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	5	4	1	6	3	2
$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	6	3	2	5	4	1

Smallest Conjugacy Closed Loop

Construction by A. Drápal:
We take a group $G(+)$, an automorphism $f \in \mathrm{Aut}(G)$ and $t \in G$ satisfying $f^2(x) = t^{-1}xt$ and $f(t) \neq t$. We construct

$$x * y = \begin{array}{c|c} x + y & \overline{f(x) + y} \\ \hline \overline{x + y} & f(x) + y + t \end{array}$$

Example

1	2	3	$\bar{1}$	$\bar{2}$	$\bar{3}$
2	3	1	$\bar{3}$	$\bar{1}$	$\bar{2}$
3	1	2	$\bar{2}$	$\bar{3}$	$\bar{1}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	2	3	1
$\bar{2}$	$\bar{3}$	$\bar{1}$	1	2	3
$\bar{3}$	$\bar{1}$	$\bar{2}$	3	1	2

Smallest A-loop

Example

1	2	3	$\bar{1}$	$\bar{2}$	$\bar{3}$
2	3	1	$\bar{2}$	$\bar{3}$	$\bar{1}$
3	1	2	$\bar{3}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{3}$	$\bar{2}$	1	3	2
$\bar{3}$	$\bar{2}$	$\bar{1}$	3	2	1
$\bar{2}$	$\bar{1}$	$\bar{3}$	2	1	3

Construction by R. H. Bruck & L. J. Paige:
We take a group G and a nontrivial automorphism $f \in \mathrm{Aut}(G)$. We construct

$$x * y = \frac{x+y}{f(x+y)} \quad \frac{\overline{x+y}}{f^{-1}(x+y)}$$

Smallest A-loop

Example

1	2	3	$\bar{1}$	$\bar{2}$	$\bar{3}$
2	3	1	$\bar{2}$	$\bar{3}$	$\bar{1}$
3	1	2	$\bar{3}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{3}$	$\bar{2}$	1	3	2
$\bar{3}$	$\bar{2}$	$\bar{1}$	3	2	1
$\bar{2}$	$\bar{1}$	$\bar{3}$	2	1	3

Construction by R. H. Bruck & L. J. Paige:
We take a group G and a nontrivial automorphism $f \in \mathrm{Aut}(G)$. We construct

$$x * y = \begin{array}{cc} x+y & \overline{x+y} \\ \hline f(x+y) & f^{-1}(x+y) \end{array}$$

Commutative A-loops of Order 8

1	2	3	4	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
2	3	4	1	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$
3	4	1	2	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
4	1	2	3	$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	1	4	3	2
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	4	3	2	1
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	3	2	1	4
$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	2	1	4	3

1	2	3	4	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
2	1	4	3	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$
3	4	1	2	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
4	3	2	1	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	1	3	4	2
$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	3	1	2	4
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	4	2	1	3
$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	2	4	3	1

1	2	3	4	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
2	1	4	3	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$
3	4	1	2	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
4	3	2	1	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	1	2	4	3
$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	2	1	3	4
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	4	3	1	2
$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	3	4	2	1

1	2	3	4	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
2	1	4	3	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$
3	4	1	2	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
4	3	2	1	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	2	1	3	4
$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	1	2	4	3
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	3	4	2	1
$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	4	3	1	2

Construction of the Smallest Commutative A-loops

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

Let $(G,+)$ be an abelian group, f an automorphism of G and t a fixed point of f. We define an operation $*$ on $Q = G \cup \bar{G}$ as follows:

$$x * y = x + y, \qquad \bar{x} * y = \overline{x + y},$$
$$x * \bar{y} = \overline{x + y}, \qquad \bar{x} * \bar{y} = f(x + y) + t.$$

Then Q is a loop and

- *Q is associative if and only if f is trivial;*
- *if f is not trivial then $N_\mu = G$ and $Z(Q) = \{x \in G;\ f(x) = x\}$;*
- *Q is an A-loop if and only if $f(2x) = 2x$, for all $x \in G$.*

Moreover, if a commutative A-loop Q has $[Q : N_\mu] = 2$ then Q can be obtained via this construction with $G = N_\mu$.

Construction of the Smallest Commutative A-loops

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

Let $(G,+)$ be an abelian group, f an automorphism of G and t a fixed point of f. We define an operation $*$ on $Q = G \cup \bar{G}$ as follows:

$$x * y = x + y, \qquad \bar{x} * y = \overline{x + y},$$
$$x * \bar{y} = \overline{x + y}, \qquad \bar{x} * \bar{y} = f(x + y) + t.$$

Then Q is a loop and

- *Q is associative if and only if f is trivial;*
- *if f is not trivial then $N_\mu = G$ and $Z(Q) = \{x \in G;\ f(x) = x\}$;*
- *Q is an A-loop if and only if $f(2x) = 2x$, for all $x \in G$.*

Moreover, if a commutative A-loop Q has $[Q : N_\mu] = 2$ then Q can be obtained via this construction with $G = N_\mu$.

Construction of the Smallest Commutative A-loops

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

Let $(G,+)$ be an abelian group, f an automorphism of G and t a fixed point of f. We define an operation $*$ on $Q = G \cup \bar{G}$ as follows:

$$x * y = x + y, \qquad \bar{x} * y = \overline{x + y},$$
$$x * \bar{y} = \overline{x + y}, \qquad \bar{x} * \bar{y} = f(x+y) + t.$$

Then Q is a loop and

- *Q is associative if and only if f is trivial;*
- *if f is not trivial then $N_\mu = G$ and $Z(Q) = \{x \in G;\ f(x) = x\}$;*
- *Q is an A-loop if and only if $f(2x) = 2x$, for all $x \in G$.*

Moreover, if a commutative A-loop Q has $[Q : N_\mu] = 2$ then Q can be obtained via this construction with $G = N_\mu$.

Construction of the Smallest Commutative A-loops

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

Let $(G, +)$ be an abelian group, f an automorphism of G and t a fixed point of f. We define an operation $*$ on $Q = G \cup \bar{G}$ as follows:

$$x * y = x + y, \qquad \bar{x} * y = \overline{x + y},$$
$$x * \bar{y} = \overline{x + y}, \qquad \bar{x} * \bar{y} = f(x + y) + t.$$

Then Q is a loop and

- *Q is associative if and only if f is trivial;*
- *if f is not trivial then $N_\mu = G$ and $Z(Q) = \{x \in G;\ f(x) = x\}$;*
- *Q is an A-loop if and only if $f(2x) = 2x$, for all $x \in G$.*

Moreover, if a commutative A-loop Q has $[Q : N_\mu] = 2$ then Q can be obtained via this construction with $G = N_\mu$.

Construction of the Smallest Commutative A-loops

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

Let $(G,+)$ be an abelian group, f an automorphism of G and t a fixed point of f. We define an operation $*$ on $Q = G \cup \bar{G}$ as follows:

$$x * y = x + y, \qquad \bar{x} * y = \overline{x+y},$$
$$x * \bar{y} = \overline{x+y}, \qquad \bar{x} * \bar{y} = f(x+y) + t.$$

Then Q is a loop and

- *Q is associative if and only if f is trivial;*
- *if f is not trivial then $N_\mu = G$ and $Z(Q) = \{x \in G;\ f(x) = x\}$;*
- *Q is an A-loop if and only if $f(2x) = 2x$, for all $x \in G$.*

Moreover, if a commutative A-loop Q has $[Q : N_\mu] = 2$ then Q can be obtained via this construction with $G = N_\mu$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Commutative A-loops of Order 8 — Constructions

Examples

The commutative A-loops of order 8 are

1. $G = \mathbb{Z}_4$, $f : x \mapsto 3x$ and $t = 0$ or 2;
2. $G = \mathbb{Z}_2^2$, f of order 2 and t neutral;
3. $G = \mathbb{Z}_2^2$, f of order 2 and t not neutral.
4. $G = \mathbb{Z}_2^2$, f of order 3 and t neutral;

Corollary

There exist commutative A-loops with trivial center for any size 2^k with $k > 2$.

Cocycles in Groups

Definition

Let G be a group and V an abelian group. A mapping $\theta : G^2 \to V$ is called a *group cocycle* if, for all g, h, k in G,

$$\theta(g, 1) = \theta(1, g) = 0,$$

$$\theta(g, hk) + \theta(h, k) = \theta(g, h)^k + \theta(gh, k).$$

Theorem

Ler G be a group and V an abelian group. The set $G \times V$ with the operation

$$(g, u) \cdot (h, v) = (gh, \theta(g, h) + u + v)$$

is a group denoted by $E(\theta, G, V)$.
On the other hand, every group E, with a normal abelian subgroup V is isomorphic to $E(\theta, E/V, V)$, for some cocycle θ.

Cocycles in Groups

Definition

Let G be a group and V an abelian group. A mapping $\theta : G^2 \to V$ is called a *group cocycle* if, for all g, h, k in G,

$$\theta(g,1) = \theta(1,g) = 0,$$
$$\theta(g,hk) + \theta(h,k) = \theta(g,h)^k + \theta(gh,k).$$

Theorem

Ler G be a group and V an abelian group. The set $G \times V$ with the operation

$$(g,u) \cdot (h,v) = (gh, \theta(g,h) + u + v)$$

is a group denoted by $E(\theta, G, V)$.
On the other hand, every group E, with a normal abelian subgroup V is isomorphic to $E(\theta, E/V, V)$, for some cocycle θ.

Cocycle Extensions of A-loops

Theorem (R. H. Bruck & L. J. Paige, special version)

Let Z be an elementary abelian 2-group and K a commutative A-loop of exponent 2. Let $\theta : K \times K \to Z$ be a loop cocycle satisfying $\theta(x,y) = \theta(y,x)$, for every $x,y \in K$, $\theta(x,x) = 1$, for every $x \in K$, and

$$\theta(x,y)\theta(x',y)\theta(xx',y)\theta(x,x')\theta(xy,z)\theta(x'y,z)\theta(y,z)\theta((xx')y,z) = \\ \theta(R(y,z)x,yz)\theta(R(y,z)x',yz)\theta(R(y,z)(xx'),yz) \\ \theta(R(y,z)x,R(y,z)x,R(y,z)x')$$

for every $x,y,z,x' \in K$, where $R(y,z) = R_yR_zR_{yz}^{-1}$. Then $K \ltimes_\theta R$ is a commutative A-loop of exponent 2.
Conversely, every commutative A-loop of exponent two that is a central extension of Z by K can be represented in this manner.

Cocycles from Trilinear Forms

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

Let $Z = \mathbb{F}_2$ and let V be a vector space over $\mathbb{F}_2$. Let $g : V^3 \to \mathbb{F}_2$ be a trilinear form such that $g(x,y,z) = g(z,y,x)$ for every $x,y,z \in V$. Define $\theta : V^2 \to Z$ by $\theta(x,y) = g(x,x+y,y)$. Then $Q = V \ltimes_\theta Z$ is a commutative A-loop of exponent 2.

Moreover, $(y,b) \in N_\mu(Q)$ if and only if the induced bilinear form $g(y,-,-) : V^2 \to \mathbb{F}_2$ is symmetric.

Example

Let $\{e_1, e_2, \dots, e_n\}$ be a basis of V, with $n \geq 3$. For all i, set $g(e_i, e_i, e_{i+1}) = 1$, where $n+1$ is identified with 1, and $g(e_i, e_j, e_k) = 0$ otherwise.

For $x = \sum \alpha_j e_j$ we have $g(x, e_i, e_{i+1}) = \alpha_i$ and $g(x, e_{i+1}, e_i) = 0$ and therefore $g(x, -, -)$ is symmetric if and only if $x = 0$.

Cocycles from Trilinear Forms

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

Let $Z = \mathbb{F}_2$ and let V be a vector space over $\mathbb{F}_2$. Let $g : V^3 \to \mathbb{F}_2$ be a trilinear form such that $g(x, y, z) = g(z, y, x)$ for every $x, y, z \in V$. Define $\theta : V^2 \to Z$ by $\theta(x, y) = g(x, x + y, y)$. Then $Q = V \ltimes_\theta Z$ is a commutative A-loop of exponent 2.

Moreover, $(y, b) \in N_\mu(Q)$ if and only if the induced bilinear form $g(y, -, -) : V^2 \to \mathbb{F}_2$ is symmetric.

Example

Let $\{e_1, e_2, \ldots, e_n\}$ be a basis of V, with $n \geq 3$. For all i, set $g(e_i, e_i, e_{i+1}) = 1$, where $n + 1$ is identified with 1, and $g(e_i, e_j, e_k) = 0$ otherwise.

For $x = \sum \alpha_j e_j$ we have $g(x, e_i, e_{i+1}) = \alpha_i$ and $g(x, e_{i+1}, e_i) = 0$ and therefore $g(x, -, -)$ is symmetric if and only if $x = 0$.

Cocycles from Trilinear Forms

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

Let $Z = \mathbb{F}_2$ and let V be a vector space over $\mathbb{F}_2$. Let $g : V^3 \to \mathbb{F}_2$ be a trilinear form such that $g(x, y, z) = g(z, y, x)$ for every $x, y, z \in V$. Define $\theta : V^2 \to Z$ by $\theta(x, y) = g(x, x + y, y)$. Then $Q = V \ltimes_\theta Z$ is a commutative A-loop of exponent 2.

Moreover, $(y, b) \in N_\mu(Q)$ if and only if the induced bilinear form $g(y, -, -) : V^2 \to \mathbb{F}_2$ is symmetric.

Example

Let $\{e_1, e_2, \dots, e_n\}$ be a basis of V, with $n \geq 3$. For all i, set $g(e_i, e_i, e_{i+1}) = 1$, where $n + 1$ is identified with 1, and $g(e_i, e_j, e_k) = 0$ otherwise.

For $x = \sum \alpha_j e_j$ we have $g(x, e_i, e_{i+1}) = \alpha_i$ and $g(x, e_{i+1}, e_i) = 0$ and therefore $g(x, -, -)$ is symmetric if and only if $x = 0$.

Drápal's Construction of Commutative A-loops

Theorem (A. Drápal; P.J. & D. Simon)

Let K be the q-element finite field, $\mathrm{char}(K) \neq 2$. Let k be an odd divisor either of $q-1$ or of $q+1$. Take ξ, 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 A-loop, $Z(Q) = 1$ and $N_\mu(Q) = K$.

Conjecture

If k and q are primes then the construction gives the only (up to isomorphism) non-associative commutative A-loop of order kq.

Drápal's Construction of Commutative A-loops

Theorem (A. Drápal; P.J. & D. Simon)

Let K be the q-element finite field, $\mathrm{char}(K) \neq 2$. Let k be an odd divisor either of $q-1$ or of $q+1$. Take ξ, 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 A-loop, $Z(Q) = 1$ and $N_\mu(Q) = K$.

Conjecture

If k and q are primes then the construction gives the only (up to isomorphism) non-associative commutative A-loop of order kq.

Commutative A-loops of order p^3

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

We define a loop $Q(\mathbb{Z}_n)$ as the set $\mathbb{Z}_n^3$ with an operation

$$(x_1, x_2, x_3) * (y_1, y_2, y_3) = (x_1 + y_1 + (x_2 + y_2)x_3y_3, \quad x_2 + y_2 \, , \, x_3 + y_3).$$

This loop is a commutative A-loop, its center is $\mathbb{Z}_n$ and its middle nucleus is $\mathbb{Z}_n^2$.

Commutative A-loops of order p^3

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

We define a loop $Q_{a,b}(\mathbb{Z}_n)$ as the set $\mathbb{Z}_n^3$ with an operation

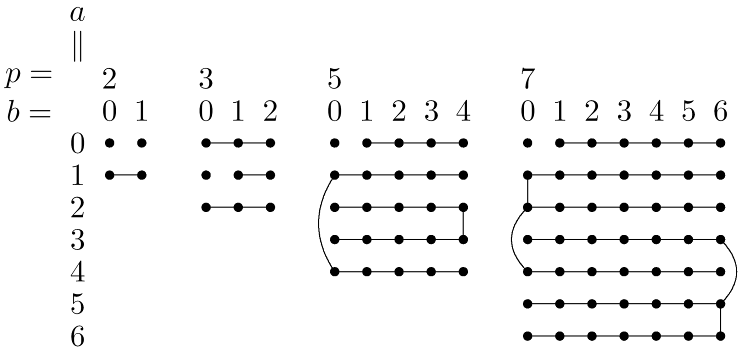
$$(x_1,x_2,x_3)*(y_1,y_2,y_3) = (x_1+y_1+(x_2+y_2)x_3y_3 \\ + a(x_2,y_2)_n + b(x_3,y_3)_n \ ,\ x_2+y_2 \ ,\ x_3+y_3),$$

where the overflow indicator $(x,y)_n$ is defined by

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

This loop is a commutative A-loop, its center is $\mathbb{Z}_n$ and its middle nucleus is $\mathbb{Z}_n^2$.

Isomorphisms of Loops of Order p^3



Conjecture

Up to isomorphism, there are exactly four non-associative commutative A-loops of order p^3.

Enumeration

loop order	all loops (non-associative)	exponent p + non-trivial center	trivial center
8	4	1	1
15	1	–	1
16	46	10	2
21	1	–	1
24	4	–	0
27	4	0	0
30	1	–	0
32	???	211	6 + ?
33	1	–	1
39	1	–	1
40	4	–	0
42	1	–	0
45	2 + ?	–	1 + ?

Questions

Question:

Does there exist any finite simple non-associative commutative A-loop? If does, it has to be a loop of exponent two.

Question:

Does there exist a (finite) commutative A-loop with trivial middle nucleus?

Question:

Find more examples of commutative A-loops.

Questions

Question:

Does there exist any finite simple non-associative commutative A-loop? If does, it has to be a loop of exponent two.

Question:

Does there exist a (finite) commutative A-loop with trivial middle nucleus?

Question:

Find more examples of commutative A-loops.

Questions

Question:

Does there exist any finite simple non-associative commutative A-loop? If does, it has to be a loop of exponent two.

Question:

Does there exist a (finite) commutative A-loop with trivial middle nucleus?

Question:

Find more examples of commutative A-loops.

Bibliography

- 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, 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
- M. K. Kinyon, K. Kunen, J. D. Phillips:
  Some notes on the structure of A-loops (preprint)