Loops with commuting inner mappings and of nilpotency class three

Aleš Drápal and Petr Vojtěchovský

Department of Algebra
Charles University in Prague
and
Department of Mathematics
University of Denver

Aug 23, 2007 / Loops '07, Prague

Notation

Q	loop
$M(Q) = \langle L_x,\ R_x;\ x \in Q \rangle$	multiplication group
$I(Q) = \{\varphi \in M(Q);\ \varphi(1) = 1\}$	inner mapping group
$Z_1(Q) = Z(Q)$ $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$	iterated centra
$\mathrm{cl}(Q) = \min\{m;\ Z_m(Q) = 1\}$	nilpotency class
$N(Q)$, $N_\rho(Q)$, $A(Q)$, T_x, $L(x,y)$	as usual

Questions

Main problem

Is Q nilpotent when $I(Q)$ is?

Restricted problem

Is Q nilpotent when $I(Q)$ is abelian?

Remark

$Q/Z(Q) \cong I(Q)$ when Q is a group.

Questions

Main problem

Is Q nilpotent when $I(Q)$ is?

Restricted problem

Is Q nilpotent when $I(Q)$ is abelian?

Remark

$Q/Z(Q) \cong I(Q)$ when Q is a group.

Questions

Main problem

Is Q nilpotent when $I(Q)$ is?

Restricted problem

Is Q nilpotent when $I(Q)$ is abelian?

Remark

$Q/Z(Q) \cong I(Q)$ when Q is a group.

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\ Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\ Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\ Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \le 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \le 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \le 2$ (G. Nagy, V.)
- $\exists\ Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\ Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\ Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

Partial answers

Below, Q is finite and $I(Q)$ is abelian.

- Q nilpotent (Kepka, Niemenmaa)
- Q CML $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Bruck)
- Q LCC $\Rightarrow \mathrm{cl}(Q) \leq 2$ (Csörgő, Drápal)
- Q Moufang p-loop, $p > 3 \Rightarrow \mathrm{cl}(Q) \leq 2$ (G. Nagy, V.)
- $\exists\, Q$, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő)
- $\exists\, Q$ Buchsteiner, $\mathrm{cl}(Q) = 3$, $|Q| = 2^7$ (Csörgő, Drápal, Kinyon)
- there are many loops Q with $\mathrm{cl}(Q) = 3$ (Drápal, V.)
- $\exists\, Q$ Moufang, $\mathrm{cl}(Q) = 3$, $|Q| = 2^{14}$ (G. Nagy, V.)

The first example

Example

Loop C constructed by Csörgő using loop folder (G, H, T), $|G| = 2^{13}$, $|H| = 2^6$, $|T| = 2^7$,

$N(C) = N_\rho(C)$ elementary abelian group of order 16, $|N_\lambda(C)| = |N_\mu(C)| = 32$,

$Z(C) = A(C)$ cyclic group of order 2,
$C/Z(C)$ a group (not abelian, of course),
$C/N(C)$ is an elementary abelian group

Central extensions

Definition

Q is an *extension* of K by F if $K \trianglelefteq Q$ and $Q/K \cong F$. The extension is *central* if $K \leq Z(Q)$.

Theorem (Central extensions)

Let Q be a loop and K an abelian group. Then Q is a central extension of K by $F = Q/K$ iff there exists a cocycle $\theta : F \times F \to K$ such that $(K \times F, *)$ given by

$$(a, x) * (b, y) = (a + b + \theta(x, y), xy)$$

is isomorphic to Q.

The above theorem is of no use when $\mathrm{cl}(Q) \geq 3$.

Central extensions

Definition

Q is an *extension* of K by F if $K \trianglelefteq Q$ and $Q/K \cong F$. The extension is *central* if $K \leq Z(Q)$.

Theorem (Central extensions)

Let Q be a loop and K an abelian group. Then Q is a central extension of K by $F = Q/K$ iff there exists a cocycle $\theta : F \times F \to K$ such that $(K \times F, *)$ given by

$$(a,x) * (b,y) = (a + b + \theta(x,y), xy)$$

is isomorphic to Q.

The above theorem is of no use when $\mathrm{cl}(Q) \geq 3$.

Central extensions

Definition

Q is an *extension* of K by F if $K \trianglelefteq Q$ and $Q/K \cong F$. The extension is *central* if $K \le Z(Q)$.

Theorem (Central extensions)

Let Q be a loop and K an abelian group. Then Q is a central extension of K by $F = Q/K$ iff there exists a cocycle $\theta : F \times F \to K$ such that $(K \times F, *)$ given by

$$(a, x) * (b, y) = (a + b + \theta(x, y), xy)$$

is isomorphic to Q.

The above theorem is of no use when $\mathrm{cl}(Q) \ge 3$.

Nuclear extensions

Definition

Extension Q of K by F is *nuclear* if $K \leq N(Q)$.

Lemma (Leong)

Let Q be a loop with a normal subloop $K \leq N(Q)$. For each $x \in Q$, define $\varphi_x = T_x|_K$. Then $\varphi_x \in \mathrm{Aut}(K)$, and the mapping $\varphi : Q \to \mathrm{Aut}(K)$, $x \mapsto \varphi_x$ is a homomorphism.

Theorem (Nuclear extensions of loops)

Let K be an abelian group and Q, F loops. Then Q is a nuclear extension of K by F iff there exists $\theta : F \times F \to K$ and a homomorphism $\varphi : F \to \mathrm{Aut}(K)$ such that $(K \times F, *)$ given by

$$(a, x) * (b, y) = (a + \varphi_x(b) + \theta(x, y), xy)$$

is isomorphic to Q.

Nuclear extensions

Definition

Extension Q of K by F is *nuclear* if $K \leq N(Q)$.

Lemma (Leong)

Let Q be a loop with a normal subloop $K \leq N(Q)$. For each $x \in Q$, define $\varphi_x = T_x|_K$. Then $\varphi_x \in \mathrm{Aut}(K)$, and the mapping $\varphi : Q \to \mathrm{Aut}(K)$, $x \mapsto \varphi_x$ is a homomorphism.

Theorem (Nuclear extensions of loops)

Let K be an abelian group and Q, F loops. Then Q is a nuclear extension of K by F iff there exists $\theta : F \times F \to K$ and a homomorphism $\varphi : F \to \mathrm{Aut}(K)$ such that $(K \times F, *)$ given by

$$(a, x) * (b, y) = (a + \varphi_x(b) + \theta(x, y), xy)$$

is isomorphic to Q.

Nuclear extensions

Definition

Extension Q of K by F is *nuclear* if $K \leq N(Q)$.

Lemma (Leong)

Let Q be a loop with a normal subloop $K \leq N(Q)$. For each $x \in Q$, define $\varphi_x = T_x|_K$. Then $\varphi_x \in \mathrm{Aut}(K)$, and the mapping $\varphi : Q \to \mathrm{Aut}(K)$, $x \mapsto \varphi_x$ is a homomorphism.

Theorem (Nuclear extensions of loops)

Let K be an abelian group and Q, F loops. Then Q is a nuclear extension of K by F iff there exists $\theta : F \times F \to K$ and a homomorphism $\varphi : F \to \mathrm{Aut}(K)$ such that $(K \times F, *)$ given by

$$(a, x) * (b, y) = (a + \varphi_x(b) + \theta(x, y), xy)$$

is isomorphic to Q.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Greedy algorithm

Let's go back to the loop C:

- $A(C) = Z(C) = \{1, h\}$
- split Cayley table of C into blocks according to $N(C)$
- try to replace xy with xyh in two diagonally opposite blocks
- keep the change that minimizes the number of nonassociating triples
- repeat

The algorithm results in a loop $\overline{C}$ that is more symmetric than C.

Second example

$$\mathbb{F}_2 = \{0, 1\}$$
$$K = (\mathbb{F}_2)^3$$
$$D_8 = \langle \sigma, \rho; \sigma^2 = \rho^4 = (\sigma\rho)^2 = 1 \rangle$$
$$F = \mathbb{F}_2 \times D_8$$

$$\varphi : F \to \mathrm{Aut}(K)$$
$$\varphi_{(\ell,\, \rho^{2i}\sigma^j(\sigma\rho)^k)}(a, b, c) = (a + kb + jc,\, b,\, c)$$

$$\theta : F \times F \to K$$
$$\theta((\ell,\, \rho^{2i}\sigma^j(\sigma\rho)^k),\, (\ell',\, \rho^{2i'}\sigma^{j'}(\sigma\rho)^{k'})) = (\ell' i,\, \ell' j,\, \ell' k)$$

$$\overline{C} = (K \times F, *)$$
$$(a, x) * (b, y) = (a + \varphi_x(b) + \theta(x, y),\, xy)$$

Group modifications

- G a group
- $K \trianglelefteq G$
- $\mu : G/K \times G/K \to G$ with $\mu(K, xK) = \mu(xK, K) = 1$

$$x * y = xy\mu(xK, yK)$$

Group modifications

- G a group
- $K \trianglelefteq G$
- $\mu : G/K \times G/K \to G$ with $\mu(K, xK) = \mu(xK, K) = 1$

$$x * y = xy\mu(xK, yK)$$

Group modifications

- G a group
- $K \trianglelefteq G$
- $\mu : G/K \times G/K \to G$ with $\mu(K, xK) = \mu(xK, K) = 1$

$$x * y = xy\mu(xK, yK)$$

Group modifications

- G a group
- $K \trianglelefteq G$
- $\mu : G/K \times G/K \to G$ with $\mu(K, xK) = \mu(xK, K) = 1$

$$x * y = xy\mu(xK, yK)$$

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x, y), R(x, y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \le K \le N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \le Z(G)$, $K \trianglelefteq G$, and $N/K \le Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \le Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G\rangle$ is abelian.*

The setup

- $Z \leq K \leq N \trianglelefteq G$ (think: N is nucleus, Z is center)
- N is abelian, G/N is abelian
- $Z \leq Z(G)$, $K \trianglelefteq G$, and $N/K \leq Z(G/K)$
- $\mu : G/K \times G/K \to Z$
- $Q = (G, *)$.

Theorem

We have:

- *Q is a loop,*
- *$Z \leq Z(G) \cap Z(Q)$ and $G/Z \cong Q/Z$ is a group,*
- *the subgroup $\langle L(x,y), R(x,y);\ x, y \in G \rangle$ is abelian.*

To make $I(Q)$ commutative

Consider

$$\mu(xy,z) = \mu(x,z)\mu(y,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{1}$$
$$\mu(x,yz) = \mu(x,y)\mu(x,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{2}$$
$$z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y), \tag{3}$$

where $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$.

Theorem

- *If (1), (2) hold then $N \leq N(Q)$ and T_x commute with $L(u,v)$, $R(u,v)$.*
- *If (1), (2) hold then $I(Q)$ is commutative iff (3) holds.*

To make $I(Q)$ commutative

Consider

$$\mu(xy,z) = \mu(x,z)\mu(y,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{1}$$
$$\mu(x,yz) = \mu(x,y)\mu(x,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{2}$$
$$z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y), \tag{3}$$

where $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$.

Theorem

- *If* (1), (2) *hold then* $N \leq N(Q)$ *and* T_x *commute with* $L(u,v)$, $R(u,v)$.
- *If* (1), (2) *hold then* $I(Q)$ *is commutative iff* (3) *holds.*

To make $I(Q)$ commutative

Consider

$$\mu(xy,z) = \mu(x,z)\mu(y,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{1}$$
$$\mu(x,yz) = \mu(x,y)\mu(x,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{2}$$
$$z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y), \tag{3}$$

where $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$.

Theorem

- *If* (1), (2) *hold then* $N \leq N(Q)$ *and* T_x *commute with* $L(u,v)$, $R(u,v)$.
- *If* (1), (2) *hold then* $I(Q)$ *is commutative iff* (3) *holds.*

To make $I(Q)$ commutative

Consider

$$\mu(xy,z) = \mu(x,z)\mu(y,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{1}$$
$$\mu(x,yz) = \mu(x,y)\mu(x,z) \text{ if } \{x,y,z\} \cap N \neq \emptyset, \tag{2}$$
$$z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y), \tag{3}$$

where $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$.

Theorem

- *If* (1), (2) *hold then* $N \leq N(Q)$ *and* T_x *commute with* $L(u,v)$, $R(u,v)$.
- *If* (1), (2) *hold then* $I(Q)$ *is commutative iff* (3) *holds.*

Structure of δ

Lemma

If (3) holds then both G and Q are of nilpotency class ≤ 3.

Lemma

Assume that (1)–(3) hold. Then Q is of nilpotency class three and G is of nilpotency class two if and only if $\delta([x,y],z) = \delta([x,z],y)$ for every x, y, $z \in G$, and $\delta([x,y],z) \neq 1$ for some x, y, $z \in G$.

Theorem

Assume that (1)–(3) hold, G is of nilpotency class two and Q is of nilpotency class three. Then there exists a subgroup $A \le Z$ of exponent two and a nontrivial symmetric triadditive mapping $f : (G/N)^3 \to A$ such that $\delta([x,y],z) = f(xN, yN, zN)$ for all x, y, $z \in G$.

Structure of δ

Lemma

If (3) holds then both G and Q are of nilpotency class ≤ 3.

Lemma

Assume that (1)–(3) hold. Then Q is of nilpotency class three and G is of nilpotency class two if and only if $\delta([x,y],z) = \delta([x,z],y)$ for every x, y, $z \in G$, and $\delta([x,y],z) \neq 1$ for some x, y, $z \in G$.

Theorem

Assume that (1)–(3) hold, G is of nilpotency class two and Q is of nilpotency class three. Then there exists a subgroup $A \leq Z$ of exponent two and a nontrivial symmetric triadditive mapping $f : (G/N)^3 \to A$ such that $\delta([x,y],z) = f(xN,yN,zN)$ for all x, y, $z \in G$.

Structure of δ

Lemma

If (3) *holds then both* G *and* Q *are of nilpotency class* ≤ 3.

Lemma

Assume that (1)–(3) *hold. Then* Q *is of nilpotency class three and* G *is of nilpotency class two if and only if* $\delta([x,y],z) = \delta([x,z],y)$ *for every* x, y, $z \in G$, *and* $\delta([x,y],z) \neq 1$ *for some* x, y, $z \in G$.

Theorem

Assume that (1)–(3) *hold,* G *is of nilpotency class two and* Q *is of nilpotency class three. Then there exists a subgroup* $A \leq Z$ *of exponent two and a nontrivial symmetric triadditive mapping* $f : (G/N)^3 \to A$ *such that* $\delta([x,y],z) = f(xN, yN, zN)$ *for all* x, y, $z \in G$.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x, y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x, y) = \mu(x, y)\mu(y, x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x, y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x, y) = \mu(x, y)\mu(y, x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x,y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x,y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x, y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x, y) = \mu(x, y)\mu(y, x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x, y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x, y) = \mu(x, y)\mu(y, x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Constructing many examples

- H a group satisfying $H' = Z(H)$ boolean, H/H' boolean
- H/H' has basis $\{e_i H';\ 1 \le i \le n\}$
- H' has basis $\{[e_i, e_j];\ 1 \le i < j \le n\}$
- $f : (H/H')^3 \to \mathbb{F}_2$ symmetric trilinear alternating form
- construct $\delta : H \times H \to A$ so that $f(xH', yH', zH') = \delta([x, y], z)$
- construct $\mu : H \times H \to A$ so that $\delta(x, y) = \mu(x, y)\mu(y, x)^{-1}$ and (1)–(3) hold
- let $G = \mathbb{F}_2 \times H = \mathcal{C}(H, \mu)$, say.

Minimal situation

- to have nontrivial f, need $\dim(H/H') = 3$
- then $\dim(H') = 3$

There are 10 such groups H, and 2^{28} ways to obtain μ for each of them.

Example

Let $f : (\mathbb{F}_2^3)^3 \to \mathbb{F}_2$ be the determinant, H the first loop in the GAP libraries with the above properties (of order 64), all parameters for δ and μ trivial. Then $\mathcal{C}(H,\mu) \cong C$.

Remark

We were not able to find two sets of parameters yielding isomorphic loops.

Minimal situation

- to have nontrivial f, need $\dim(H/H') = 3$
- then $\dim(H') = 3$

There are 10 such groups H, and 2^{28} ways to obtain μ for each of them.

Example

Let $f : (\mathbb{F}_2^3)^3 \to \mathbb{F}_2$ be the determinant, H the first loop in the GAP libraries with the above properties (of order 64), all parameters for δ and μ trivial. Then $\mathcal{C}(H, \mu) \cong C$.

Remark

We were not able to find two sets of parameters yielding isomorphic loops.

Minimal situation

- to have nontrivial f, need $\dim(H/H') = 3$
- then $\dim(H') = 3$

There are 10 such groups H, and 2^{28} ways to obtain μ for each of them.

Example

Let $f : (\mathbb{F}_2^3)^3 \to \mathbb{F}_2$ be the determinant, H the first loop in the GAP libraries with the above properties (of order 64), all parameters for δ and μ trivial. Then $\mathcal{C}(H, \mu) \cong C$.

Remark

We were not able to find two sets of parameters yielding isomorphic loops.

Minimal situation

- to have nontrivial f, need $\dim(H/H') = 3$
- then $\dim(H') = 3$

There are 10 such groups H, and 2^{28} ways to obtain μ for each of them.

Example

Let $f : (\mathbb{F}_2^3)^3 \to \mathbb{F}_2$ be the determinant, H the first loop in the GAP libraries with the above properties (of order 64), all parameters for δ and μ trivial. Then $\mathcal{C}(H, \mu) \cong C$.

Remark

We were not able to find two sets of parameters yielding isomorphic loops.

Minimal situation

- to have nontrivial f, need $\dim(H/H') = 3$
- then $\dim(H') = 3$

There are 10 such groups H, and 2^{28} ways to obtain μ for each of them.

Example

Let $f : (\mathbb{F}_2^3)^3 \to \mathbb{F}_2$ be the determinant, H the first loop in the GAP libraries with the above properties (of order 64), all parameters for δ and μ trivial. Then $\mathcal{C}(H, \mu) \cong C$.

Remark

We were not able to find two sets of parameters yielding isomorphic loops.

Lemma

$I(C(H,\mu))$ is an elementary abelian 2-group.

Observation

It appears that $|M(C(H,\mu))| \geq 2^{13}$ when $|H| = 64$.

Lemma

$I(C(H,\mu))$ is an elementary abelian 2-group.

Observation

It appears that $|M(C(H,\mu))| \geq 2^{13}$ when $|H| = 64$.

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a,b,c) * (a',b',c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a,b,c),(a',b',c'),(a'',b'',c'')] = (0,0,aa'a'')$
- $[[x,y],z] = 2[x,y,z]$
- $L(x,y)z = R(x,y)z = z + [x,y,z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_xT_y(z))(T_yT_x(z))^{-1} = -4[x,y,z]$.

Bruck's construction

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a, b, c) * (a', b', c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a, b, c), (a', b', c'), (a'', b'', c'')] = (0, 0, aa'a'')$
- $[[x, y], z] = 2[x, y, z]$
- $L(x, y)z = R(x, y)z = z + [x, y, z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_x T_y(z))(T_y T_x(z))^{-1} = -4[x, y, z]$.

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a, b, c) * (a', b', c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a, b, c), (a', b', c'), (a'', b'', c'')] = (0, 0, aa'a'')$
- $[[x, y], z] = 2[x, y, z]$
- $L(x, y)z = R(x, y)z = z + [x, y, z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_x T_y(z))(T_y T_x(z))^{-1} = -4[x, y, z]$.

Bruck's construction

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a, b, c) * (a', b', c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a, b, c), (a', b', c'), (a'', b'', c'')] = (0, 0, aa'a'')$
- $[[x, y], z] = 2[x, y, z]$
- $L(x, y)z = R(x, y)z = z + [x, y, z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_xT_y(z))(T_yT_x(z))^{-1} = -4[x, y, z].$

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a, b, c) * (a', b', c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a, b, c), (a', b', c'), (a'', b'', c'')] = (0, 0, aa'a'')$
- $[[x, y], z] = 2[x, y, z]$
- $L(x, y)z = R(x, y)z = z + [x, y, z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_x T_y(z))(T_y T_x(z))^{-1} = -4[x, y, z]$.

Bruck's construction

Theorem (Bruck, G. Nagy, V.)

Let A be an associative algebra over any ring, B a subspace of A such that $xy = -yx$ for every $x, y \in B$. Let B_n be the subspace of A generated by products of at most n elements of B. Define multiplication on $Q = B \times B_2 \times B_3$ by

$$(a, b, c) * (a', b', c') = (a + a', b + b' + aa', c + c' + ba').$$

Then Q is a Moufang loop, and

- $[(a, b, c), (a', b', c'), (a'', b'', c'')] = (0, 0, aa'a'')$
- $[[x, y], z] = 2[x, y, z]$
- $L(x, y)z = R(x, y)z = z + [x, y, z]$
- *generators of $I(Q)$ commute, except possibly for two conjugations*
- $(T_x T_y(z))(T_y T_x(z))^{-1} = -4[x, y, z]$.

Exterior algebras

We need a suitable algebra A for Bruck's construction.

Definition (Exterior algebra)

Let R be a ring, $n > 0$. *Exterior algebra* $\mathcal{E}_n(R)$ on n-generators over R is a vector space over R with basis

$$\{a(S);\ S \subseteq \{1, \dots, n\}\}$$

with multiplication

$$a(S)a(T) = 0$$

if $S \cap T \neq \emptyset$, and

$$a(S)a(T) = \mathrm{sgn}(\pi)a(S \cup T)$$

otherwise, where π is a permutation that reorders S, T into $S \cup T$.

We need a suitable algebra A for Bruck's construction.

Definition (Exterior algebra)

Let R be a ring, $n > 0$. *Exterior algebra* $\mathcal{E}_n(R)$ on n-generators over R is a vector space over R with basis

$$\{a(S);\ S \subseteq \{1, \dots, n\}\}$$

with multiplication

$$a(S)a(T) = 0$$

if $S \cap T \neq \emptyset$, and

$$a(S)a(T) = \mathrm{sgn}(\pi)a(S \cup T)$$

otherwise, where π is a permutation that reorders S, T into $S \cup T$.

Moufang loop

Theorem

Let R be a ring satisfying $2R \neq 0$, $4R = 0$. Let $A = \mathcal{E}_n(R)$, where $n \geq 3$. Then Bruck's construction applied to A yields a Moufang loop Q with abelian $I(Q)$ and of nilpotency class 3.

Example (Smallest known Moufang example)

$R = \mathbb{Z}_4$, $n = 3$ yields Q of order $2^{14} = 4^7$.
Here is the multiplication table for nonidentity basis elements in $\mathcal{E}_3(R)$:

	a_1	a_2	a_3	a_{12}	a_{13}	a_{23}	a_{123}
a_1	0	a_{12}	a_{13}	0	0	a_{123}	0
a_2	$-a_{12}$	0	a_{23}	0	$-a_{123}$	0	0
a_3	$-a_{13}$	$-a_{23}$	0	a_{123}	0	0	0
a_{12}	0	0	a_{123}	0	0	0	0
a_{13}	0	$-a_{123}$	0	0	0	0	0
a_{23}	a_{123}	0	0	0	0	0	0
a_{123}	0	0	0	0	0	0	0

.

Thus $B = \langle a_1, a_2, a_3\rangle$, $B_2 = \langle a_{12}, a_{13}, a_{23}\rangle$, $B_3 = \langle a_{123}\rangle$.

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?

Open problems

Call a loop Q with $I(Q)$ abelian and of nilpotency class at least 3 a *loop of Csörgő type*.

- Is there a loop of Csörgő type with $\mathrm{cl}(Q) > 3$?
- Is the nilpotency class of a loop of Csörgő type bounded?
- Is there a loop of Csörgő type with $|Q| < 128$?
- Is there a p-loop of Csörgő for some $p > 2$?
- Is there a Moufang 3-loop of Csörgő type?