Distributive Quasigroups of Size 243

Přemysl Jedlička
with David Stanovský and Petr Vojtěchovský

Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture) in Prague

6th February 2016
Brno

Faculty of Engineering

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Medial Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *medial* if it satisfies

$$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u).$$

Theorem (K. Toyoda; R. Bruck)

A groupoid $(Q, \cdot)$ is a medial quasigroup if and only if there exist

- *an abelian group $(Q, +, 0)$,*
- *two commuting automorphisms $\varphi, \psi \in \mathrm{Aut}(Q, +)$,*
- *a constant $c \in Q$,*

such that, for each $x, y \in Q$,

$$x \cdot y = \varphi(x) + \psi(y) + c.$$

Medial Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *medial* if it satisfies

$$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u).$$

Theorem (K. Toyoda; R. Bruck)

A groupoid $(Q, \cdot)$ is a medial quasigroup if and only if there exist

- *an abelian group $(Q, +, 0)$,*
- *two commuting automorphisms $\varphi, \psi \in \mathrm{Aut}(Q, +)$,*
- *a constant $c \in Q$,*

such that, for each $x, y \in Q$,

$$x \cdot y = \varphi(x) + \psi(y) + c.$$

Trimedial Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *trimedial* if every 3-generated sub-groupoid is medial

Theorem (T. Kepka)

A groupoid $(Q, \cdot)$ is a tri-medial quasigroup if and only if there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *two commuting 1-central automorphisms $\varphi, \psi \in \mathrm{Aut}(Q, +)$,*
- *a constant $c \in Z(Q)$,*

such that, for each $x, y \in Q$,

$$x \cdot y = \varphi(x) + \psi(y) + c.$$

Trimedial Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *trimedial* if every 3-generated sub-groupoid is medial

Theorem (T. Kepka)

A groupoid $(Q, \cdot)$ is a tri-medial quasigroup if and only if there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *two commuting 1-central automorphisms $\varphi, \psi \in \mathrm{Aut}(Q, +)$,*
- *a constant $c \in Z(Q)$,*

such that, for each $x, y \in Q$,

$$x \cdot y = \varphi(x) + \psi(y) + c.$$

Moufang Loops

Definition

Let $(Q, +)$ be a quasigroup. Then Q is a *loop* if there exists a neutral element 0 in Q.

Definition

A loop $(Q, +, 0)$ is called a *Moufang loop* if it satisfies

$$x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z.$$

Definition

The center of a loop Q is the set

$$Z(Q) = \{a \in Q;\ ax = xa,\ a \cdot xy = ax \cdot y,\ x \cdot ay = xa \cdot y,\ xy \cdot a = x \cdot ya;\ \forall x, y \in Q\}$$

Moufang Loops

Definition

Let $(Q, +)$ be a quasigroup. Then Q is a *loop* if there exists a neutral element 0 in Q.

Definition

A loop $(Q, +, 0)$ is called a *Moufang loop* if it satisfies

$$x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z.$$

Definition

The center of a loop Q is the set

$$Z(Q) = \{a \in Q;\ ax = xa,\ a \cdot xy = ax \cdot y,\ x \cdot ay = xa \cdot y,\ xy \cdot a = x \cdot ya;\ \forall x, y \in Q\}$$

Commutative Moufang Loops

Definition

Let Q be a loop and let $\alpha : Q \to Q$. We denote by $\hat{\alpha}$ the mapping $x \mapsto x + \alpha(x)$.
We say that α is 1-central, if $\hat{\alpha}(x) \in Z(Q)$, for all $x \in Q$.

Proposition (R. Bruck)

Let $(Q, +, 0)$ be a commutative Moufang loop. Then $3Q \subseteq Z(Q)$.

Corollary

Let Q be a finite commutative Moufang loop. If $|Q|$ is coprime to 3 then Q is an abelian group.

Example

The mapping $x \mapsto 2x$ is a 1-central automorphism of a commutative Moufang loop.

Commutative Moufang Loops

Definition

Let Q be a loop and let $\alpha : Q \to Q$. We denote by $\hat{\alpha}$ the mapping $x \mapsto x + \alpha(x)$.
We say that α is 1-central, if $\hat{\alpha}(x) \in Z(Q)$, for all $x \in Q$.

Proposition (R. Bruck)

Let $(Q, +, 0)$ be a commutative Moufang loop. Then $3Q \subseteq Z(Q)$.

Corollary

Let Q be a finite commutative Moufang loop. If $|Q|$ is coprime to 3 then Q is an abelian group.

Example

The mapping $x \mapsto 2x$ is a 1-central automorphism of a commutative Moufang loop.

Commutative Moufang Loops

Definition

Let Q be a loop and let $\alpha : Q \to Q$. We denote by $\hat{\alpha}$ the mapping $x \mapsto x + \alpha(x)$.
We say that α is 1-central, if $\hat{\alpha}(x) \in Z(Q)$, for all $x \in Q$.

Proposition (R. Bruck)

Let $(Q, +, 0)$ be a commutative Moufang loop. Then $3Q \subseteq Z(Q)$.

Corollary

Let Q be a finite commutative Moufang loop. If $|Q|$ is coprime to 3 then Q is an abelian group.

Example

The mapping $x \mapsto 2x$ is a 1-central automorphism of a commutative Moufang loop.

Commutative Moufang Loops

Definition

Let Q be a loop and let $\alpha : Q \to Q$. We denote by $\hat{\alpha}$ the mapping $x \mapsto x + \alpha(x)$.
We say that α is 1-central, if $\hat{\alpha}(x) \in Z(Q)$, for all $x \in Q$.

Proposition (R. Bruck)

Let $(Q, +, 0)$ be a commutative Moufang loop. Then $3Q \subseteq Z(Q)$.

Corollary

Let Q be a finite commutative Moufang loop. If $|Q|$ is coprime to 3 then Q is an abelian group.

Example

The mapping $x \mapsto 2x$ is a 1-central automorphism of a commutative Moufang loop.

Distributive Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *distributive* if it satisfies

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$$
$$(x \cdot y) \cdot z = (x \cdot z) \cdot (y \cdot z).$$

Theorem (V. D. Belousov)

A quasigroup is distributive if and only if it is idempotent and trimedial.

Corollary (V. D. Belousov; J.-P. Soublin)

A groupoid $(Q, \cdot)$ is a distributive quasigroup iff there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *a 1-central automorphism ψ with $id - \psi \in \mathrm{Aut}(Q, +)$,*

such that $x \cdot y = (x - \psi(x)) + \psi(y)$.

Distributive Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *distributive* if it satisfies

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$$
$$(x \cdot y) \cdot z = (x \cdot z) \cdot (y \cdot z).$$

Theorem (V. D. Belousov)

A quasigroup is distributive if and only if it is idempotent and trimedial.

Corollary (V. D. Belousov; J.-P. Soublin)

A groupoid $(Q, \cdot)$ is a distributive quasigroup iff there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *a 1-central automorphism ψ with $id - \psi \in \mathrm{Aut}(Q, +)$,*

such that $x \cdot y = (x - \psi(x)) + \psi(y)$.

Distributive Quasigroups

Definition

A groupoid $(Q, \cdot)$ is called *distributive* if it satisfies

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$$
$$(x \cdot y) \cdot z = (x \cdot z) \cdot (y \cdot z).$$

Theorem (V. D. Belousov)

A quasigroup is distributive if and only if it is idempotent and trimedial.

Corollary (V. D. Belousov; J.-P. Soublin)

A groupoid $(Q, \cdot)$ is a distributive quasigroup iff there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *a 1-central automorphism ψ with $id - \psi \in \mathrm{Aut}(Q, +)$,*

such that $x \cdot y = (x - \psi(x)) + \psi(y)$.

Decomposition of Finite Distributive Quasigroups

Theorem (B. Fisher, J. D. H. Smith)

Let Q be a finite distributive quasigroup. Then

$$Q \cong Q_1 \times \cdots \times Q_k$$

where $|Q_i| = p_i^{n_i}$, for some prime p_i.
Moreover, if, for some $i \leqslant k$, Q_i is not medial then $p_i = 3$.

Theorem (T. Kepka, P. Němec)

There are 6 non-medial distributive quasigroups of size 81, up to isomorphism.

Decomposition of Finite Distributive Quasigroups

Theorem (B. Fisher, J. D. H. Smith)

Let Q be a finite distributive quasigroup. Then

$$Q \cong Q_1 \times \cdots \times Q_k$$

where $|Q_i| = p_i^{n_i}$, for some prime p_i.
Moreover, if, for some $i \leqslant k$, Q_i is not medial then $p_i = 3$.

Theorem (T. Kepka, P. Němec)

There are 6 non-medial distributive quasigroups of size 81, up to isomorphism.

1-central Automorphisms

Lemma (P.J., D.S., P.V.)

Let Q be a commutative Moufang loop. A mapping $\alpha : Q \to Q$ is a 1-central automorphism if and only if $\hat{\alpha}$ is a fix-point-free endomorphism $Q \to Z(Q)$.
Moreover, the endomorphism $id - \alpha$ is a bijection if and only if $\hat{\alpha}(x) = 2x$ implies $x = 0$.

Corollary

A groupoid $(Q, \cdot)$ is a distributive quasigroup iff there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *an endomorphism $\hat{\psi} : Q \to Z(Q)$ satisfying $\hat{\psi}(x) \notin \{x, 2x\}$, for each $x \neq 0$,*

such that, for all $x, y \in Q$,

$$x \cdot y = 2x - y + \hat{\psi}(y - x).$$

1-central Automorphisms

Lemma (P.J., D.S., P.V.)

Let Q be a commutative Moufang loop. A mapping $\alpha : Q \to Q$ is a 1-central automorphism if and only if $\hat{\alpha}$ is a fix-point-free endomorphism $Q \to Z(Q)$.
Moreover, the endomorphism $id - \alpha$ is a bijection if and only if $\hat{\alpha}(x) = 2x$ implies $x = 0$.

Corollary

A groupoid $(Q, \cdot)$ is a distributive quasigroup iff there exist

- *a commutative Moufang loop $(Q, +, 0)$,*
- *an endomorphism $\hat{\psi} : Q \to Z(Q)$ satisfying $\hat{\psi}(x) \notin \{x, 2x\}$, for each $x \neq 0$,*

such that, for all $x, y \in Q$,

$$x \cdot y = 2x - y + \hat{\psi}(y - x).$$

Isomorphism of Distributive Quasigroups

Proposition

Let Q_1 and Q_2 be commutative Moufang loops and let $\hat{\psi}_i : Q_i \to Z(Q_i)$ be endomorphism, for $i \in \{1,2\}$. The associated distributive quasigroups are isomorphic if and only if there exists an isomorphism $f : Q_1 \to Q_2$ such that

$$\hat{\psi}_1 = f^{-1} \circ \hat{\psi}_2 \circ f.$$

Enumeration of Distributive Quasigroups of Size 243

Theorem (T. Kepka, P. Němec)

There exist 6 non-associative commutative Moufang loops of order 243.

Theorem (P.J., D.S., P.V.)

There exist 92 non-medial distributive quasigroups of order 243.

Enumeration of Distributive Quasigroups of Size 243

Theorem (T. Kepka, P. Němec)

There exist 6 non-associative commutative Moufang loops of order 243.

Theorem (P.J., D.S., P.V.)

There exist 92 non-medial distributive quasigroups of order 243.

Example of a Distributive Quasigroup of Size 243

Fact (H. Zassenhaus)

The set $\mathbb{Z}_3^5$ *with the operation*

$$(a_1,b_1,c_1,d_1,e_1)+(a_2,b_2,c_2,d_2,e_2)=$$
$$(a_1+a_2+(e_1+e_2)\cdot(c_1d_2-d_1c_2), b_1+b_2, c_1+c_2, d_1+d_2, e_1+e_2)$$

is a non-associative CML of order 243 and exponent 3.

Proposition (P.J., D.S., P.V.)

Up to conjugacy, there are six endomorphisms $\hat{\psi}: Q \to Z(Q)$ *satisfying* $\hat{\psi}(x) \notin \{x, 2x\}$, *for all* $x \neq 0$:

$$(a,b,c,d,e) \mapsto (0,0,0,0,0) \qquad (a,b,c,d,e) \mapsto (b,0,0,0,0)$$
$$(a,b,c,d,e) \mapsto (c,0,0,0,0) \qquad (a,b,c,d,e) \mapsto (0,c,0,0,0)$$
$$(a,b,c,d,e) \mapsto (b,c,0,0,0) \qquad (a,b,c,d,e) \mapsto (c,d,0,0,0)$$

Example of a Distributive Quasigroup of Size 243

Fact (H. Zassenhaus)

The set $\mathbb{Z}_3^5$ with the operation

$$(a_1, b_1, c_1, d_1, e_1) + (a_2, b_2, c_2, d_2, e_2) =$$
$$(a_1 + a_2 + (e_1 + e_2) \cdot (c_1 d_2 - d_1 c_2), b_1 + b_2, c_1 + c_2, d_1 + d_2, e_1 + e_2)$$

is a non-associative CML of order 243 and exponent 3.

Proposition (P.J., D.S., P.V.)

Up to conjugacy, there are six endomorphisms $\hat{\psi} : Q \to Z(Q)$ satisfying $\hat{\psi}(x) \notin \{x, 2x\}$, for all $x \neq 0$:

$$(a,b,c,d,e) \mapsto (0,0,0,0,0) \qquad (a,b,c,d,e) \mapsto (b,0,0,0,0)$$
$$(a,b,c,d,e) \mapsto (c,0,0,0,0) \qquad (a,b,c,d,e) \mapsto (0,c,0,0,0)$$
$$(a,b,c,d,e) \mapsto (b,c,0,0,0) \qquad (a,b,c,d,e) \mapsto (c,d,0,0,0)$$

Steiner and Mendelsohn Distributive Quasigroups

Proposition (D. Donovan, T. Griggs, T. McCourt, J. Opršal, D. Stanovský)

A distributive quasigroup $(Q,\cdot)$ *satisfies*

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

if and only if $\hat{\psi}^2-3\hat{\psi}+3x=0$. *Such a quasigroup is called distributive Mendelsohn quasigroup.*
Moreover, Q is also commutative if and only if $(Q,+)$ *is of exponent 3 and* $\hat{\psi}=0$. *Such quasigroups are called distributive Steiner quasigroups.*

Proposition (P.J., D.S., P.V.)

There are 6 non-medial Mendelsohn quasigroups of order 243, one of them being Steiner.

Steiner and Mendelsohn Distributive Quasigroups

Proposition (D. Donovan, T. Griggs, T. McCourt, J. Opršal, D. Stanovský)

A distributive quasigroup $(Q, \cdot)$ *satisfies*

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

if and only if $\hat{\psi}^2 - 3\hat{\psi} + 3x = 0$. *Such a quasigroup is called distributive Mendelsohn quasigroup.*
Moreover, Q is also commutative if and only if $(Q, +)$ *is of exponent 3 and* $\hat{\psi} = 0$. *Such quasigroups are called distributive Steiner quasigroups.*

Proposition (P.J., D.S., P.V.)

There are 6 non-medial Mendelsohn quasigroups of order 243, one of them being Steiner.