Towards the Classification of Finite Left Distributive Quasigroups

Jan Vlachy

Universiteit Utrecht

Loops '11

Outline

Outline

Left Distributive Quasigroups

Definition

For $(Q, \cdot)$:

- left translation $\lambda_a : x \mapsto ax$
- right translation $\rho_a : x \mapsto xa$
- $(Q, \cdot)$ is a quasigroup $\equiv$ the translations are bijections of Q
- $\mathrm{LMlt}(Q) \equiv \{$group generated by left translations$\}$

Definition

A quasigroup is left distributive (LD) if

- the left translations are automorphisms
- or equivalently: $x(yz) = (xy)(xz)$

- left distributive $\Rightarrow$ idempotent (that is: $xx = x, \ x \in Q$)

All quasigroups in this talk are finite.

Why should we care?

Medial Property

$(xy)(uv) = (xu)(yv)$

Eighth Belousov's problem

Is there a LD quasigroup not isotopic to a Bol loop?

Definition

quandle $\equiv$ left distributive idempotent left quasigroup

Why should we care?

Medial Property

$(xy)(uv) = (xu)(yv)$

Eighth Belousov's problem

Is there a LD quasigroup not isotopic to a Bol loop?

Definition

quandle $\equiv$ left distributive idempotent left quasigroup

Why should we care?

Medial Property

$(xy)(uv) = (xu)(yv)$

Eighth Belousov's problem

Is there a LD quasigroup not isotopic to a Bol loop?

Definition

quandle $\equiv$ left distributive idempotent left quasigroup

Examples

Examples

- $\mathbb{F}$ a finite field, given nonzero $\mu, \nu \in \mathbb{F}$ with $\mu + \nu = 1$. Take
$$x \circ y := \mu x + \nu y$$
- G, a group with a fixed point free automorphism ϕ. Take
$$x \circ y := x\phi(x^{-1}y)$$
- Take $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$ with generators a, b. Take
$$a^i b^j \circ a^{i'} b^{j'} = \begin{cases} a^i b^{2j+4j'} & \text{if } (i - i') \equiv_3 0 \\ a^{i+1} b^2 b^{4(j+j')} & \text{if } (i - i') \equiv_3 -1 \\ a^{i-1} b^{4(j+j')} & \text{if } (i - i') \equiv_3 1 \end{cases}$$

Outline

Galkin's representation 1/2

Construction

Consider

- G, a finite group
- ϕ, an automorphism of G
- $T \leq G$, the subgroup of fixed points of ϕ.

Consider $(G/T, \circ)$, where

$$xT \circ yT := x\phi(x^{-1}y)T$$

- Result: a quandle.
- Suitable choice of ϕ : $(G/T, \circ)$ is already a LD quasigroup.

For $(Q, \cdot)$ LD quasigroup, take:

- $e \in Q$ arbitrary
- $G = \mathrm{LMlt}(Q)$, the left multiplication group
- $\phi =$ the conjugation by λ_e
- then $T = \mathrm{LMlt}(Q)_e$

Theorem (Existence of Galkin's representation)

$$(Q, \cdot) \simeq (G/T, \circ)$$
$$q \mapsto \lambda_{q/e} \mathrm{LMlt}(Q)_e$$

- Typically: more groups G with $(Q, \cdot) \simeq (G/T, \circ)$
- The smallest such G is the commutator subgroup of $\mathrm{LMlt}(Q)$.

Galkin's representation 2/2

For $(Q, \cdot)$ LD quasigroup, take:

- $e \in Q$ arbitrary
- $G = \mathrm{LMlt}(Q)$, the left multiplication group
- $\phi =$ the conjugation by λ_e
- then $T = \mathrm{LMlt}(Q)_e$

Theorem (Existence of Galkin's representation)

$$(Q, \cdot) \simeq (G/T, \circ)$$
$$q \mapsto \lambda_{q/e}\,\mathrm{LMlt}(Q)_e$$

- Typically: more groups G with $(Q, \cdot) \simeq (G/T, \circ)$
- The smallest such G is the commutator subgroup of $\mathrm{LMlt}(Q)$.

A brief note on “cohomological methods”

Let X a LDQ, Y its factorquasigroup; we can write

$$X \simeq Y \times_\beta S,$$

where S is a set, β is a “cocycle”.

Outline

Classical results

Theorem (Medial QG; Toyoda)

Let $(Q, \circ)$ be a MIQ. There exists:

- $(Q, +)$*, an abelian group*
- β*, an automorphism of* $(Q, +)$

with:

$$x \circ y = (id_Q - \beta)(x) + \beta(y), \quad \text{for all } x, y \in Q$$

Theorem (Distributive QG; Galkin)

Let Q be a distributive quasigroup. Then

$$Q \simeq Q_A \times Q_3$$

- Q_A *is a medial quasigroup of order not divided by 3.*
- Q_3 *is a distributive quasigroup of order* 3^k*.*

Recent theoretical results

Theorem (Simple LDQ; Vlachy; Ježek and Kepka)

Every simple LDQ is medial.

Theorem (LDQ of order p^2; Graña)

Every LDQ of order p^2 is medial.

Recent computational results

Two different approaches:

Using model builders (Stanovsky)

- Enumeration feasible up to order cca 30.
- Further classification up to isomorphism is computationally demanding.

Using classification of transitive groups (Vendramin)

- For an indecomposable quandle of order n, LMlt is a transitive group of degree n.
- Transitive groups of degree up to 35 are known.
- Enumeration of LDQ (up to isomorphism) up to order 35 follows.

Summary

To Remember

- Questions about LDQ reduces to questions about LMlt.
- Particular classes of LDQ are easy to classify, in the general case only partial results are known.

End

Thanks

- David Stanovsky
- Gabor Nagy
- Edwin Clark

Any questions?

Definitions

Definition (Isotopy)

(α, β, γ) triple of bijections of Q and P is an *isotopy* of $(Q, \star)$ and $(P, \circ)$, iff

$$\gamma(x \star y) = \alpha(x) \circ \beta(y), \qquad \text{for all } x, y \in Q$$

Definition (Indecomposable quandle)

A quandle Q is indecomposable $\equiv$ LMlt(Q) is transitive.

- Let $(Y, \circ)$ a quandle, S a set.
- Let $\alpha_{i,j}(s,t) : Y \times Y \to \mathrm{Fun}(S \times S, S)$.

Define $(Y \times_\alpha S, \star)$ by

$$(i,s) \star (j,t) := (i \circ j, \alpha_{ij}(s,t)).$$

It is a quandle iff

Dynamical cocycle

for α it holds:

1. $\alpha_{ij}(s, \cdot)$ is a bijection
2. $\alpha_{i,j\circ k}(s,\cdot)\alpha_{j,k}(t,\cdot) = \alpha_{i\circ j, i\circ k}(\alpha_{ij}(s,t),\cdot)\alpha_{i,k}(s,\cdot)$
3. $\alpha_{i,i}(s,s) = s$

Condition on the automorphism in the Galkin's construction

- As mentioned: Galkin's representation always yields a quandle.
- Yields a LDQ if and only if

$$x\phi(x^{-1}) \in sTs^{-1} \Rightarrow x \in T,$$

for any $x, s \in G$.

"List" of medial simple quasigroups

Theorem (Ježek and Kepka)

Simple medial idempotent quasigroups are exactly those of the form $(\mathbb{F}, \circ_{\mu,\nu})$, where $\mathbb{F}$ is a finite field, μ and ν are generators of $\mathbb{F}$, $\mu + \nu = 1$ and

$$x \circ_{\mu,\nu} y := \mu x + \nu y.$$