Tomáš Nagy

Self-distributive quasigroups

Content

Section 1

Introduction and motivation

(Self)-distributivity

- Let A be a set with binary operations $*$ and $+$.

(Self)-distributivity

- Let A be a set with binary operations $*$ and $+$.
- Why should the identity $(a * b) * c = a * (b * c)$ hold?

(Self)-distributivity

- Let A be a set with binary operations $*$ and $+$.
- Why should the identity $(a * b) * c = a * (b * c)$ hold?
- Can we find another nice property instead of associativity?

(Self)-distributivity

- The operation $*$ can be distributive with respect to $+$:
  - $a * (b + c) = (a * b) + (a * c)$.
- Can we use it even when we have no $+$?

(Self)-distributivity

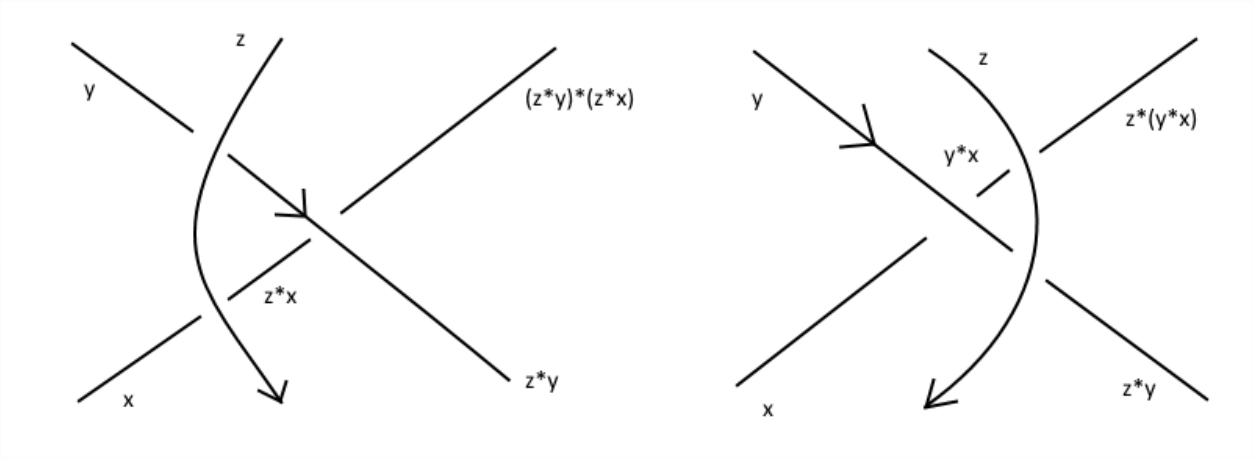
- The operation $*$ can be distributive with respect to $+$:
  - $a * (b + c) = (a * b) + (a * c)$.
- Can we use it even when we have no $+$?
- What about the identity $a * (b * c) = (a * b) * (a * c)$ (left self-distributivity)?

Self-distributive structures

- Where does self-distributivity appear in mathematics?
  - theory of symmetric spaces
  - set theory
  - low-dimensional topology: knots and tangles

Tangles

- Given strings with orientation.
- We want to label them by labels from set A s. t. for each crossing with upper string a, ”right”string b and ”left”string c it holds that $c = a * b$.
- The labeling should be invariant with respect to Reidemeister moves, i.e. ”basic manipulations with strings”:



Quasigroups

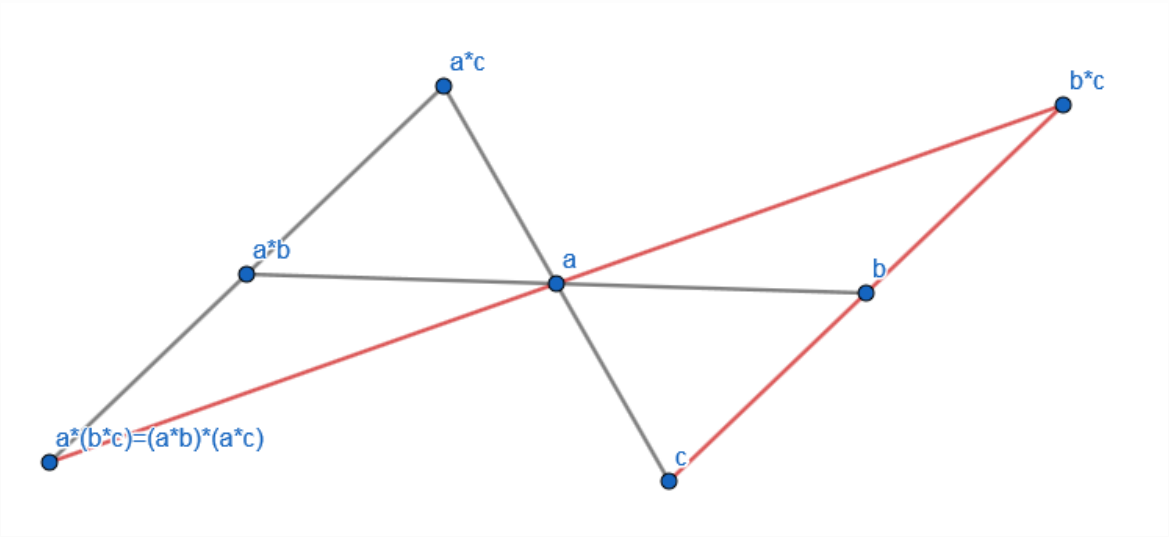
- How can non-associative ”group”look like?
- We have a structure $(A, *)$.
- We want to have something like a^{-1} but we don't have associativity.
  - We want to have a unique solutions to the equations $a * x = b$ and $y * a = b$.
  - Let us denote $x = a \backslash b$ (left division) and $y = b / a$ (right division).
  - A *quasigroup* is a set where those equations have unique solutions.
  - I.e. the multiplication table of $*$ is a latin square.

Section 2

Basic examples and properties

- Group conjugation:
  - Let $(G, \cdot, ^{-1})$ be a group and let us define an operation $a * b = aba^{-1}$.
  - This operation is left self-distributive: $a * (b * c) = abcb^{-1}a^{-1} = aba^{-1}aca^{-1}ab^{-1}a^{-1} = (a * b) * (b * c)$.
  - $(G, *)$ is rarely a quasigroup (but the equation $a * x = b$ has a unique solution).
  - Moreover, $*$ is idempotent, i.e. $a * a = a$.
  - Idempotent, left self-distributive structure with unique left division is called a *quandle*.

- Reflection in euclidean geometry:
  - Let a, b be two points and let us define $a * b$ to be the reflection of b over a.
  - This gives us also a quandle (but not necessarily a quasigroup, e.g. for reflection on a sphere).



- Convex combination:
  - Given a, b (elements of real vector space) we can define $a *_s b = sa + (1-s)b$ for $s \in [0, 1)$.
  - This operation is left self-distributive:
    $a *_s (b *_s c) = sa + (1-s)(sb + (1-s)c) =$
    $s^2 a + s(1-s)b + (1-s)sa + (1-s)^2 c = (a *_s b) *_s (a *_s c)$.
  - This gives us a quandle once more, and for $s \neq 0$ it is also a quasigroup. Quandle that is at the same time a quasigroup is also called a *latin quandle*.

How hard is it to study basic properties?

- Given a distributive quasigroup (e.g. self-distributive from both sides).
  - Does the identity $(a * b) * (c * d) = (a * c) * (b * d)$ (mediality) always hold?
  - No, the least counterexample has 81 elements.
- How many (non-isomorphic) self-distributive quasigroups of a given size exist? (enumeration)
- How many such quasigroups satisfying some other properties (e.g. non-medial) exist?
- We want to find a correspondence between self-distributive quasigroups and some other algebraical structures that are easier to describe.

Section 3

Loops and representation theorems

Quasigroups and quandles

- A quasigroup is said to be *left self-distributive* if the identity $a * (b * c) = (a * b) * (a * c)$ holds.
- It is said to be *distributive* if it is both right and left self-distributive.
- It is said to be *medial* if the identity $(a * b) * (c * d) = (a * c) * (b * d)$ holds.
- It is said to be *(left)-involutory* if the identity $a * (a * b) = b$ holds.
- It is said to be *idempotent* if the identity $a * a = a$ holds.
- A structure $(Q, *)$ is said to be a quandle if it is left-selfdistributive, idempotent and the equation $a * x = b$ has a unique solution for all $a, b \in Q$.
- We say that a quandle is latin if it is also a quasigroup.
- For a quandle $(Q, *)$ we define $LMlt(Q) = \langle L_a | a \in Q \rangle$, where $L_a(b) = a * b$.
  - (All identities are universally quantified.)

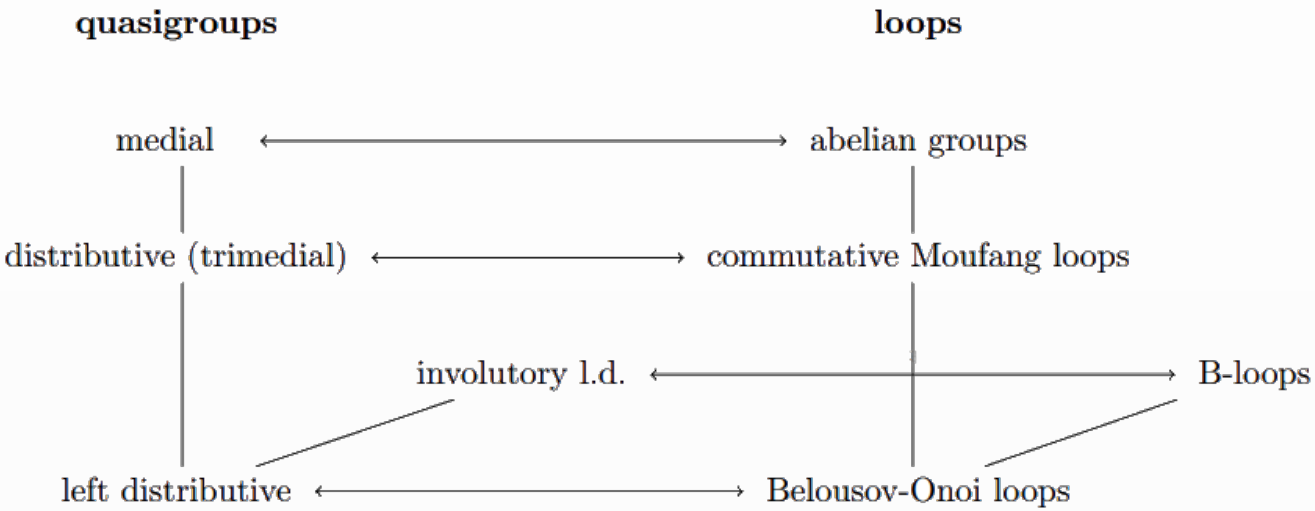
- Those statements follow easily from the definitions:
  - Left self-distributive quasigroup is a quandle.
  - Idempotent medial quasigroups are self-distributive.

Definition.

A loop is a quasigroup $(A, \cdot)$ that has a unit element 1 such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in A$.

- A loop is said to be *(left) Bol* if the identity $(x \cdot yx)z = x(y \cdot xz)$ holds.
- It is said to be *Moufang* if the identity $(xy \cdot x)z = x(y \cdot xz)$ holds.
- It is said to be *uniquely 2-divisible* if the mapping $x \mapsto x^2$ is a bijection.
- It is said to have *automorphic inverse property* if the identity $(xy)^{-1} = x^{-1}y^{-1}$ holds.
- It is said to be a *left Bruck loop* if it is a Bol loop with automorphic inverse property.
- Let $(Q_1, \cdot)$ and $(Q_2, *)$ be two loops. An *isotopy* between them is a triple of bijective mappings α, β, γ such that $\alpha(a) \cdot \beta(b) = \gamma(a * b)$.
  - (All identities are universally quantified.)

Correspondence between quasigroups and loops



Quasigroups affine over a loop

- Let $(Q, \cdot)$ be a loop.
- A permutation φ of Q is called *affine* over $(Q, \cdot)$ if there exist an automorphism $\tilde{\varphi}$ and $q \in Q$ such that $\varphi(a) = q \cdot \tilde{\varphi}(a)$ or $\varphi(a) = \tilde{\varphi}(a) \cdot q$ for all $a \in Q$.
- A quasigroup $(Q, *)$ is called *affine* over loop $(Q, \cdot)$ if for every $a, b \in Q$ it holds that $a * b = \varphi(a) \cdot \psi(b)$, where φ, ψ are affine mappings over $(Q, \cdot)$ such that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$.

Theorem.

Let $(Q, *)$ be a quasigroup. Then, the following are equivalent:

1. $(Q, *)$ is medial,
2. $(Q, *)$ is affine over an abelian group.

Latin quandles affine over a group

Theorem.

Let $(Q, *)$ be a quasigroup. Then, the following are equivalent:

1. $(Q, *)$ is medial,
2. $(Q, *)$ is affine over an abelian group.

- If we know this theorem, what does it mean for a latin quandle (idempotent quasigroup) that it is affine over an abelian group?

Latin quandles affine over a group

Theorem.

Let $(Q, *)$ be a quasigroup. Then, the following are equivalent:

1. $(Q, *)$ is medial,
2. $(Q, *)$ is affine over an abelian group.

- If we know this theorem, what does it mean for a latin quandle (idempotent quasigroup) that it is affine over an abelian group?
- We call such a quandle an *affine quandle* and we denote it by $Aff(G, f)$ (for abelian group G).

Polynomial equivalence of structures

- Given an algebraical structure $(A, f_1, f_2, \cdots)$.
- *Term operation* is any operation that can be obtained by composition of basic operations $f_1, \cdots$.
- *Polynomial operation* is obtained from term operation by substituting constants for some variables.
- Two structures are called *polynomially (term) equivalent* if they have the same polynomial (term) operations.
- Term equivalent $\Rightarrow$ polynomially equivalent.

Affine quandles

- A structure is called *affine* if it is polynomially equivalent to some module.
- Medial idempotent quasigroup $Aff(Q, \varphi) = (Q, *, /, \backslash)$ is polynomially equivalent to $(Q, +, -, 0, \varphi, \varphi^{-1}, (1-\varphi), (1-\varphi)^{-1})$.
  - Why?
- $(Q, +, -, 0, \varphi, \varphi^{-1}, (1-\varphi), (1-\varphi)^{-1})$ is term equivalent to the module over the ring of Laurent polynomials $\mathbb{Z}[t, t^{-1}, s, s^{-1}]$ with underlying structure $(Q, +)$.
  - $t \cdot u$ is defined by $\varphi(u)$,
  - $s \cdot u$ is defined by $(1-\varphi)(u)$
  - $\cdots$.

Belousov-Onoi loops

- Let $(Q, \cdot)$ be a loop and $\psi \in Aut(Q)$. We will call $(Q, \cdot, \psi)$ a *Belousov-Onoi (BO) module* if the identity $\varphi(ab) \cdot \psi(ac) = a \cdot \varphi(b)\psi(c)$ holds (φ is defined by $\varphi(a) = a/\psi(a)$).
- Every group with its automorphism ψ is a BO-module, every Bruck loop with $\psi(x) = x^{-1}$ is a BO-module.

Theorem.

Let $(Q, \cdot, \psi)$ be a BO-module and let us define an operation $*$ on Q by $a * b = \varphi(a)\psi(b)$. Then, $(Q, *)$ is a quandle. It is a quasigroup if and only if φ is a permutation.

Belousov-Onoi loops

- If $(Q, \cdot, \psi)$ is a BO-module and φ (defined as above) is a permutation, then $(Q, \cdot)$ is called a *Belousov-Onoi loop* with respect to ψ. If φ is an automorphism, the representation of $(Q, *)$ over $(Q, \cdot)$ is called *right linear*.

Theorem.

The following are equivalent for a quasigroup $(Q, *)$:

1. it is left self-distributive,
2. it is right linear over a BO-loop.

Section 4

Enumeration

Coset quandles

- Let G be a group and let $f \in Aut(G)$.
- Let $H \leq Fix(f) = \{g \in G | f(g) = g\}$.
- Let us define an operation $*$ on G/H by $aH * bH = af(a^{-1}b)H$.
- Then, $(G/H, *)$ is a quandle, called the *coset quandle*. And is denoted by $\mathbf{Q}_{Hom}(G, H, f)$.
- For an abelian group G, $Aff(G, f) = \mathbf{Q}_{Hom}(G, 1, f)$

Connected quandles

- A quandle $(Q, *)$ is called connected if $LMlt(Q)$ acts transitively on Q.
- Latin quandles are connected, $\mathbf{Q}_{Hom}(G, H, f)$ is connected.
- A *quandle envelope* is a pair (G, ζ) where G is a transitive group and $\zeta \in Z(G_e)$ such that $\langle g\zeta g^{-1} | g \in G \rangle = G$.
- We have the following correspondence between connected quandles and quandle envelopes:
  - Fix set Q and $e \in Q$.
  - Let $(Q, *)$ be a connected quandle. Then, $(LMlt(Q), L_e)$ is a quandle envelope.
  - Let (G, ζ) be a quandle envelope. Then, $\mathbf{Q}_{Hom}(G, G_e, f_\zeta)$ (with $f_\zeta(a) = \zeta a \zeta^{-1}$) is a connected quandle.
  - Moreover, those mappings are mutually inverse.

Enumeration of distributive quasigroups

Theorem.

Let $(Q, *)$ be a finite distributive quasigroup of order $p_1^{k_1}, \cdots, p_n^{k_n}$, where $p_1, \cdots, p_n$ are pairwise different primes. Then, $Q \simeq Q_1 \times \cdots \times Q_n$, where $|Q_i| = p_i^{k_i}$ and if Q_i is not medial, then $p_i = 3$ and $n_i \geq 4$.

- The smallest non-medial distributive quasigroup is of size 81.

Enumeration

- The correspondence between transitive groups and connected quandles allows us to enumerate all left self-distributive quasigroups of size ≤ 47.
- Let us denote by $LD(n)$ the number of non-medial left self-distributive quasigroups up to isomorphism.
- $ILD(n)$ denotes the number of non-medial involutory left self-distributive ones.
- $MI(n)$ denotes the number of medial idempotent quasigroups.
- The previous theorem gives us that $MI(k \cdot l) = MI(k) \cdot MI(l)$ for k, l coprime.

Enumeration

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**	16
$LD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	0
$ILD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0
$MI(n)$	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3	9

n	17	18	19	20	**21**	22	23	24	25	26	**27**	**28**	29	30	31	32
$LD(n)$	0	0	0	0	**2**	0	0	0	0	0	**32**	**2**	0	0	0	0
$ILD(n)$	0	0	0	0	**1**	0	0	0	0	0	**4**	**0**	0	0	0	0
$MI(n)$	15	0	17	3	5	0	21	2	34	0	30	5	27	0	29	8

	33	34	35	**36**	37	38	**39**	40	41	42	43	44	**45**	46	47	
$LD(n)$	**2**	0	0	**1**	0	0	**2**	0	0	0	0	0	**12**	0	0	
$ILD(n)$	**1**	0	0	**0**	0	0	**1**	0	0	0	0	0	**3**	0	0	
$MI(n)$	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45	

(Non-medial) latin quasigroups

- There is no left self-distributive quasigroup of order $4k + 2$, $k \geq 0$.
- Every connected quandle with p or p^2 elements, p prime, is medial.
- First example of non-medial left self-distributive quasigroup of order is due to Onoi in 1970, $k = 16$. This was also the first example of a distributive quasigroup that is not istopoic to any Bol loop (the smallest quasigroup with this property is of size 15).
- We can ask ourselves what is the least k for that there exists non-medial left self-distributive quasigroup of size 2^k.
- There is no such quasigroup for $k \leq 5$.
- We were able to find such quasigroup of size 2^k for all $k \geq 6$, $k \neq 7$.

Open problems

- There are still many open problems in this field:
  - Enumeration of certain classes of self-distributive quasigroups (e.g. of order pq, p, q primes).
  - Non-idempotent generalization of left self-distributive quasigroups: describe quasigroups that are right affine over BO-loops.
  - ”Non-associative modules”: affine representation over some generalization of modules.
  - ...

Thank you for your attention!