Introducing trusses

Tomasz Brzeziński

Swansea University & University of Białystok

Keele, June 2019

References:

- TB, *Trusses: between braces and rings*, TAMS (2019)
- TB, *Towards semi-trusses*, Rev. Roumaine Math. Pures Appl. (2018)
- TB, *Trusses: Paragons, ideals and modules*, submitted (2019)
- TB & B Rybołowicz *On the category of modules over trusses*, in preparation.

Aim and philosophy:

Aim: To present an algebraic framework for studying braces and rings on equal footing.

Philosophy:

‘Identity-free’ framework

Specify identities

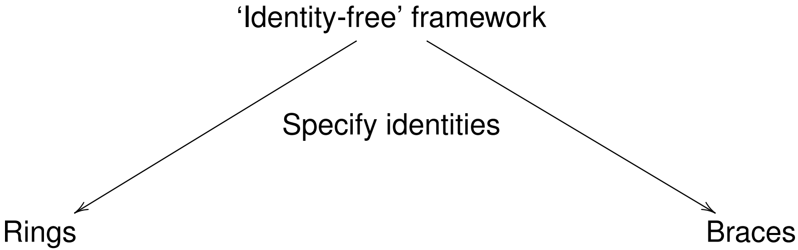
Rings

Braces

Aim and philosophy:

Aim: To present an algebraic framework for studying braces and rings on equal footing.

Philosophy:



Herds (or heaps or torsors)

H. Prüfer (1924), R. Baer (1929)

Definition

A *herd* (or *heap* or *torsor*) is a nonempty set A together with a ternary operation

$$[-,-,-] : A \times A \times A \to A,$$

such that for all $a_i \in A$, $i = 1, \ldots, 5$,

- $$[[a_1, a_2, a_3], a_4, a_5] = [a_1, a_2, [a_3, a_4, a_5]],$$
- $$[a_1, a_2, a_2] = a_1 = [a_2, a_2, a_1].$$

A herd $(A, [-,-,-])$ is said to be *abelian* if

$$[a, b, c] = [c, b, a], \quad \text{for all } a, b, c \in A.$$

Herds (or heaps or torsors)

H. Prüfer (1924), R. Baer (1929)

Definition

A *herd* (or *heap* or *torsor*) is a nonempty set A together with a ternary operation

$$[-,-,-] : A \times A \times A \to A,$$

such that for all $a_i \in A$, $i = 1, \ldots, 5$,

- $$[[a_1, a_2, a_3], a_4, a_5] = [a_1, a_2, [a_3, a_4, a_5]],$$
- $$[a_1, a_2, a_2] = a_1 = [a_2, a_2, a_1].$$

A herd $(A, [-,-,-])$ is said to be *abelian* if

$$[a, b, c] = [c, b, a], \quad \text{for all } a, b, c \in A.$$

Herds are in '1-1' correspondence with groups

- If $(A, \diamond)$ is a (abelian) group, then A is a (abelian) herd with operation
$$[a, b, c]_\diamond = a \diamond b^\diamond \diamond c.$$
Notation: $\mathcal{H}(A, \diamond)$.
- Let $(A, [-, -, -])$ be a (abelian) herd. For all $e \in A$,
$$a \diamond_e b := [a, e, b],$$
makes A into (abelian) group (with identity e and the inverse mapping $a \mapsto [e, a, e]$). Notation: $\mathcal{G}(A, e)$.
- Note:
  - $\mathcal{G}(A, e) \cong \mathcal{G}(A, f)$;
  - $\mathcal{H} \circ \mathcal{G} = \mathrm{id}$, i.e., irrespective of e: $[a, b, c]_{\diamond_e} = [a, b, c]$.

Herds are in '1-1' correspondence with groups

- If $(A, \diamond)$ is a (abelian) group, then A is a (abelian) herd with operation
$$[a, b, c]_\diamond = a \diamond b^\diamond \diamond c.$$
Notation: $\mathcal{H}(A, \diamond)$.
- Let $(A, [-, -, -])$ be a (abelian) herd. For all $e \in A$,
$$a \diamond_e b := [a, e, b],$$
makes A into (abelian) group (with identity e and the inverse mapping $a \mapsto [e, a, e]$). Notation: $\mathcal{G}(A, e)$.
- Note:
  - $\mathcal{G}(A, e) \cong \mathcal{G}(A, f)$;
  - $\mathcal{H} \circ \mathcal{G} = \mathrm{id}$, i.e., irrespective of e: $[a, b, c]_{\diamond_e} = [a, b, c]$.

Herds are in '1-1' correspondence with groups

- If $(A, \diamond)$ is a (abelian) group, then A is a (abelian) herd with operation
$$[a, b, c]_\diamond = a \diamond b^\diamond \diamond c.$$
Notation: $\mathcal{H}(A, \diamond)$.
- Let $(A, [-, -, -])$ be a (abelian) herd. For all $e \in A$,
$$a \diamond_e b := [a, e, b],$$
makes A into (abelian) group (with identity e and the inverse mapping $a \mapsto [e, a, e]$). Notation: $\mathcal{G}(A, e)$.
- Note:
  - $\mathcal{G}(A, e) \cong \mathcal{G}(A, f)$;
  - $\mathcal{H} \circ \mathcal{G} = \mathrm{id}$, i.e., irrespective of e: $[a, b, c]_{\diamond_e} = [a, b, c]$.

Herds are 'groups without specified identity'

- There if a forgetful functor

$$\mathbf{Grp} \longrightarrow \mathbf{Set}_*.$$

- Morphisms from $(A, [-,-,-])$ to $(B, [-,-,-])$ are functions $f : A \to B$ respecting ternary operations:

$$f([a,b,c]) = [f(a), f(b), f(c)].$$

- There is a forgetful functor

$$\mathbf{Hrd} \longrightarrow \mathbf{Set},$$

but not to the category of based sets.
- Worth noting:

$$\mathrm{Aut}(A, [-,-,-]_\diamond) = \mathrm{Hol}(A, \diamond).$$

Herds are ‘groups without specified identity’

- There if a forgetful functor

$$\mathbf{Grp} \longrightarrow \mathbf{Set}_*.$$

- Morphisms from $(A, [-,-,-])$ to $(B, [-,-,-])$ are functions $f : A \to B$ respecting ternary operations:

$$f([a,b,c]) = [f(a), f(b), f(c)].$$

- There is a forgetful functor

$$\mathbf{Hrd} \longrightarrow \mathbf{Set},$$

but not to the category of based sets.

- Worth noting:

$$\mathrm{Aut}(A, [-,-,-]_\diamond) = \mathrm{Hol}(A, \diamond).$$

Herds are ‘groups without specified identity’

- There if a forgetful functor

$$\mathbf{Grp} \longrightarrow \mathbf{Set}_*.$$

- Morphisms from $(A, [-,-,-])$ to $(B, [-,-,-])$ are functions $f : A \to B$ respecting ternary operations:

$$f([a,b,c]) = [f(a), f(b), f(c)].$$

- There is a forgetful functor

$$\mathbf{Hrd} \longrightarrow \mathbf{Set},$$

but not to the category of based sets.

- Worth noting:

$$\mathrm{Aut}(A, [-,-,-]_\diamond) = \mathrm{Hol}(A, \diamond).$$

Constructions on herds

- Quotient herds: A subherd S of A (i.e., $[s, s', s''] \in S$, for all $s, s', s'' \in S$) defines an equivalence relation $\sim_S$ on A:

$$a \sim_S b \quad \equiv \quad \exists s \in S, [a, b, s] \in S$$
$$\equiv \quad \forall s \in S, [a, b, s] \in S.$$

  If A is abelian (or S is normal), $A/S := A/\sim_S$ is a herd.
- Free herds: X - a set.
  - $W(X)$ reduced (no consecutive identical letters) words in X of odd length.
  - Operation: $[w_1, w_2, w_3] = w_1 w_2^t w_3$ followed by pruning.

  Altogether: a free herd on X. Can be abelianised to give $\mathcal{A}(X)$.

Constructions on herds

- Quotient herds: A subherd S of A (i.e., $[s, s', s''] \in S$, for all $s, s', s'' \in S$) defines an equivalence relation $\sim_S$ on A:

$$\begin{aligned} a \sim_S b &\equiv \exists s \in S, [a, b, s] \in S \\ &\equiv \forall s \in S, [a, b, s] \in S. \end{aligned}$$

  If A is abelian (or S is normal), $A/S := A/\sim_S$ is a herd.
- Free herds: X - a set.
  - $W(X)$ reduced (no consecutive identical letters) words in X of odd length.
  - Operation: $[w_1, w_2, w_3] = w_1 w_2^t w_3$ followed by pruning.

  Altogether: a free herd on X. Can be abelianised to give $\mathcal{A}(X)$.

Constructions on herds (cd)

- Coproduct:
  - A, B – abelian herds.
  - $A \sqcup B$ is a free abelian herd $\mathcal{A}(A \sqcup B)$ modulo relations determined by $[- - -]_A$ and $[- - -]_B$.
  - $$A \sqcup B = \mathcal{H}\left(\mathcal{G}(A, e_A) \oplus \mathcal{G}(B, e_B) \oplus \mathbb{Z}\right).$$
- Kernels: A *kernel* of a herd morphism $f : A \to B$ is defined as

$$\ker_e f = f^{-1}(e) = \{a \in A \mid f(a) = e\}, \qquad e \in \mathrm{Im}(f) \subseteq B.$$

  - $\ker_e f$ is a (normal) sub-herd of A.
  - Different choices of e lead to isomorphic sub-herds.
  - $\sim_{\ker_e f}$ is the same as the kernel relation,

$$a \sim_{\ker_e f} b \qquad \text{iff} \qquad f(a) = f(b).$$

Constructions on herds (cd)

- Coproduct:
  - A, B – abelian herds.
  - $A \sqcup B$ is a free abelian herd $\mathcal{A}(A \sqcup B)$ modulo relations determined by $[- - -]_A$ and $[- - -]_B$.
  - $$A \sqcup B = \mathcal{H}\left(\mathcal{G}(A, e_A) \oplus \mathcal{G}(B, e_B) \oplus \mathbb{Z}\right).$$
- Kernels: A *kernel* of a herd morphism $f : A \to B$ is defined as

$$\ker_e f = f^{-1}(e) = \{a \in A \mid f(a) = e\}, \qquad e \in \mathrm{Im}(f) \subseteq B.$$

  - $\ker_e f$ is a (normal) sub-herd of A.
  - Different choices of e lead to isomorphic sub-herds.
  - $\sim_{\ker_e f}$ is the same as the kernel relation,

$$a \sim_{\ker_e f} b \qquad \text{iff} \qquad f(a) = f(b).$$

Trusses

- A *left skew truss* is a herd $(A, [-,-,-])$ together with an associative operation $\cdot$ that left distributes over $[-,-,-]$, i.e.,
$$a \cdot [b, c, d] = [a \cdot b, a \cdot c, a \cdot d].$$
- If $(A, [-,-,-])$ is abelian, then we have a *left truss*.
- Right (skew) trusses are defined similarly.
- A *truss* is a triple $(A, [-,-,-], \cdot)$ that is both left and right truss.
- A morphism of (left/right skew) trusses is a function preserving both the ternary and binary operations.

Trusses: between braces and (near-)rings

Let $(A, [-,-,-], \cdot)$ be a left skew truss.

- Assume that $(A, \cdot)$ is a group with a neutral element e. Then $(A, \diamond_e, \cdot)$ is a left skew brace, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e a^{\diamond_e} \diamond_e (a \cdot c).$$

- Assume that $e \in A$ is such that

$$a \cdot e = e, \qquad \text{for all } a \in A.$$

Then $(A, \diamond_e, \cdot)$ is a left near-ring, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e (a \cdot c).$$

Trusses: between braces and (near-)rings

Let $(A, [-,-,-], \cdot)$ be a left skew truss.

- Assume that $(A, \cdot)$ is a group with a neutral element e. Then $(A, \diamond_e, \cdot)$ is a left skew brace, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e a^{\diamond_e} \diamond_e (a \cdot c).$$

- Assume that $e \in A$ is such that

$$a \cdot e = e, \qquad \text{for all } a \in A.$$

Then $(A, \diamond_e, \cdot)$ is a left near-ring, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e (a \cdot c).$$

Trusses: between braces and (near-)rings

Let $(A, [-,-,-], \cdot)$ be a left skew truss.

- Assume that $(A, \cdot)$ is a group with a neutral element e. Then $(A, \diamond_e, \cdot)$ is a left skew brace, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e a^{\diamond_e} \diamond_e (a \cdot c).$$

- Assume that $e \in A$ is such that

$$a \cdot e = e, \qquad \text{for all } a \in A.$$

  Then $(A, \diamond_e, \cdot)$ is a left near-ring, i.e.

$$a \cdot (b \diamond_e c) = (a \cdot b) \diamond_e (a \cdot c).$$

Trusses: generalised distributivity

Let $(A, \diamond)$ be a group and $(A, \cdot)$ be a semigroup. TFAE:

- There exists $\sigma : A \to A$, such that
$$a \cdot (b \diamond c) = (a \cdot b) \diamond \sigma(a)^{\diamond} \diamond (a \cdot c).$$
- There exists $\lambda : A \times A \to A$, such that,
$$a \cdot (b \diamond c) = (a \cdot b) \diamond \lambda(a, c).$$
- There exists $\mu : A \times A \to A$, such that
$$a \cdot (b \diamond c) = \mu(a, b) \diamond (a \cdot c).$$
- There exist $\kappa, \hat{\kappa} : A \times A \to A$, such that
$$a \cdot (b \diamond c) = \kappa(a, b) \diamond \hat{\kappa}(a, c).$$
- $(A, [-, -, -]_{\diamond}, \cdot)$ is a left skew truss.

Trusses from split-exact sequences of groups

- Let $(A, \diamond)$ be a middle term of a split-exact sequence of groups

$$1 \longrightarrow G \longrightarrow A \underset{\beta}{\overset{\alpha}{\rightleftarrows}} H \longrightarrow 1$$

- Let $\cdot$ be an operation on A defined as

$$a \cdot b = a \diamond \beta(\alpha(b)) \quad \text{or} \quad a \cdot b = \beta(\alpha(a)) \diamond b.$$

- Then $(A, [-,-,-]_\diamond, \cdot)$ is a left skew truss.

The endomorphism truss

- Let $(A, [-,-,-])$ be an abelian herd.
- Set $\mathcal{E}(A) := \mathrm{End}(A, [-,-,-])$.
- $\mathcal{E}(A)$ is an abelian herd with inherited operation

$$[f, g, h](a) = [f(a), g(a), h(a)].$$

- $\mathcal{E}(A)$ together with $[-,-,-]$ and composition $\circ$ is a truss.

Notes on the endomorphism truss:

- Choosing the group structure $f \diamond_{\mathrm{id}} g$ on $\mathcal{E}(A)$, we obtain a two-sided brace-type distributive law between $\diamond_{\mathrm{id}}$ and $\circ$.
- Fix $e \in A$, and let $\varepsilon : A \to A$, be given by $\varepsilon : a \mapsto e$. Then $\varepsilon \in \mathcal{E}(A)$, and choosing the group structure $f \diamond_{\varepsilon} g$ on $\mathcal{E}(A)$ we get a ring $(\mathcal{E}(A), \diamond_{\varepsilon}, \circ)$.
- The left multiplication map

$$\ell : A \to \mathcal{E}(A), \qquad a \mapsto [b \mapsto a \cdot b],$$

is a morphism of trusses.

Truss structures on $(\mathbb{Z}, [- - -]_+)$:

Theorem

(1) Non-commutative truss structures, ,

$$m \cdot n = m \quad \text{or} \quad m \cdot n = n, \qquad \forall m, n \in \mathbb{Z}.$$

(2) Commutative truss structures are in 1-1 correspondence with elements of

$$\mathcal{I}_2(\mathbb{Z}) = \{e \in M_2(\mathbb{Z}) \mid e^2 = e,\ \mathrm{Tr}\, e = 1\}.$$

(3) Isomorphism classes of truss structures in (2) are in 1-1 correspondence with orbits of the action of

$$D_\infty = \left\{ \begin{pmatrix} 1 & 0 \\ k & \pm 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\}.$$

Truss structures on $(\mathbb{Z}, [- - -]_+)$:

Theorem

(1) Non-commutative truss structures, ,

$$m \cdot n = m \quad \text{or} \quad m \cdot n = n, \qquad \forall m, n \in \mathbb{Z}.$$

(2) Commutative truss structures are in 1-1 correspondence with elements of

$$\mathcal{I}_2(\mathbb{Z}) = \{e \in M_2(\mathbb{Z}) \mid e^2 = e, \ \mathrm{Tr}\, e = 1\}.$$

(3) Isomorphism classes of truss structures in (2) are in 1-1 correspondence with orbits of the action of

$$D_\infty = \left\{ \begin{pmatrix} 1 & 0 \\ k & \pm 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\}.$$

Truss structures on $(\mathbb{Z}, [- - -]_+)$:

Theorem

(1) Non-commutative truss structures, ,

$$m \cdot n = m \quad \text{or} \quad m \cdot n = n, \qquad \forall m, n \in \mathbb{Z}.$$

(2) Commutative truss structures are in 1-1 correspondence with elements of

$$\mathcal{I}_2(\mathbb{Z}) = \{e \in M_2(\mathbb{Z}) \mid e^2 = e, \ \mathrm{Tr}\, e = 1\}.$$

(3) Isomorphism classes of truss structures in (2) are in 1-1 correspondence with orbits of the action of

$$D_\infty = \left\{ \begin{pmatrix} 1 & 0 \\ k & \pm 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\}.$$

Trusses and ring theory: ideals, quotients, paragons

Many techniques and constructions familiar in ring theory can be applied to trusses **but not necessarily in a straightforward way.**

- An *ideal* of $(A, [-,-,-], \cdot)$ is a sub-herd X such that,

$$a \cdot x, \quad x \cdot a \in X, \qquad \text{for all } x \in X, a \in A.$$

- The quotient $A/X := A/\sim_X$ is a truss with operations

$$[\overline{a}, \overline{b}, \overline{c}] = \overline{[a, b, c]}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- However... a kernel of a truss homomorphism is not necessarily an ideal.

Trusses and ring theory: ideals, quotients, paragons

Many techniques and constructions familiar in ring theory can be applied to trusses **but not necessarily in a straightforward way.**

- An *ideal* of $(A, [-,-,-], \cdot)$ is a sub-herd X such that,

$$a \cdot x, \quad x \cdot a \in X, \qquad \text{for all } x \in X, a \in A.$$

- The quotient $A/X := A/\sim_X$ is a truss with operations

$$[\overline{a}, \overline{b}, \overline{c}] = \overline{[a, b, c]}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- However... a kernel of a truss homomorphism is not necessarily an ideal.

Trusses and ring theory: ideals, quotients, paragons

Many techniques and constructions familiar in ring theory can be applied to trusses **but not necessarily in a straightforward way.**

- An *ideal* of $(A, [-,-,-], \cdot)$ is a sub-herd X such that,

$$a \cdot x, \;\; x \cdot a \in X, \qquad \text{for all } x \in X, a \in A.$$

- The quotient $A/X := A/\sim_X$ is a truss with operations

$$[\overline{a}, \overline{b}, \overline{c}] = \overline{[a, b, c]}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- However... a kernel of a truss homomorphism is not necessarily an ideal.

Trusses and ring theory: ideals, quotients, paragons

Many techniques and constructions familiar in ring theory can be applied to trusses **but not necessarily in a straightforward way.**

- An *ideal* of $(A, [-,-,-], \cdot)$ is a sub-herd X such that,

$$a \cdot x, \quad x \cdot a \in X, \qquad \text{for all } x \in X, a \in A.$$

- The quotient $A/X := A/\sim_X$ is a truss with operations

$$[\overline{a}, \overline{b}, \overline{c}] = \overline{[a,b,c]}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- However... a kernel of a truss homomorphism is not necessarily an ideal.

Trusses and ring theory: ideals, quotients, paragons

A *(left, right) paragon* in A is a sub-herd P such that, for all $p, q \in P$ and $a \in A$,

$$[ap, aq, q], \quad [pa, qa, q] \in P.$$

- Kernel is a paragon.
- A/P is a truss.
- For example, the set of odd integers is a paragon in $\mathbb{Z}$.
- In case of braces: paragon is what is called an ideal.

Modules of trusses

- A *left module* over a truss $(A, [-,-,-], \cdot)$ is an abelian herd $(M, [-,-,-])$ together with a morphism of trusses

$$\pi_M : A \to \mathcal{E}(M).$$

- The *action* of A on M, $a \triangleright m := \pi_M(a)(m)$, satisfies:

  Distributive laws:

$$a \triangleright [m_1, m_2, m_3] = [a \triangleright m_1, a \triangleright m_2, a \triangleright m_3],$$

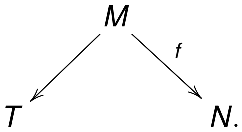
$$[a, b, c] \triangleright m = [a \triangleright m, b \triangleright m, c \triangleright m],$$

  Associative law:

$$a \triangleright (b \triangleright m) = (a \cdot b) \triangleright m.$$

Category of modules

- Morphisms of modules over trusses are defined as functions preserving the ternary operations and actions; category $A - \mathbf{Mod}$.
- Right modules, bimodules defined analogously.
- $A - \mathbf{Mod}$ has a terminal object $T = \{0\}$ but not an initial object.
- $A - \mathbf{Mod}$ has cokernels, i.e. pushouts of



Category of modules

- $A - \mathbf{Mod}$ has quotients:
  - Take a submodule N of M.
  - Define an equivalence relation, for $m_1, m_2 \in M$,

$$m_1 \sim_N m_2 \quad \text{iff} \quad \exists n \in N,\ [m_1, m_2, n] \in N.$$

  - $\overline{M} := M/N := M/\sim_N$,

$$[\overline{m_1}, \overline{m_2}, \overline{m_3}] = \overline{[m_1, m_2, m_3]}, \quad a \triangleright \overline{m} = \overline{a \triangleright m}.$$

- Given a morphism of A-modules $f : M \to N$,

$$\mathrm{coker}(f) = N/\mathrm{Im(f)}.$$

Induced submodules

Many constructions of modules over rings can be applied to trusses **but not necessarily in a straightforward way.**

- An A-module M an *induced* action: fix $e \in M$,

$$a \triangleright_e m = [a \triangleright m, a \triangleright e, e].$$

- The element e is an *absorber* for $\triangleright_e$, i.e.

$$\forall a \in A, \quad a \triangleright_e e = e,$$

  hence $\triangleright_e$ distributes over the binary operation $\diamond_e$ on M.
- Different choices of e yield isomorphic modules.
- The kernel of $f : M \to N$ is an induced submodule of M.
- If N is a sub-herd of M, then M/N has an A-module structure such that $M \to M/N$ is a module morphism if and only if N is an induced submodule of M.

Induced submodules

Many constructions of modules over rings can be applied to trusses **but not necessarily in a straightforward way.**

- An A-module M an *induced* action: fix $e \in M$,

$$a \triangleright_e m = [a \triangleright m, a \triangleright e, e].$$

- The element e is an *absorber* for $\triangleright_e$, i.e.

$$\forall a \in A, \quad a \triangleright_e e = e,$$

  hence $\triangleright_e$ distributes over the binary operation $\diamond_e$ on M.
- Different choices of e yield isomorphic modules.
- The kernel of $f : M \to N$ is an induced submodule of M.
- If N is a sub-herd of M, then M/N has an A-module structure such that $M \to M/N$ is a module morphism if and only if N is an induced submodule of M.

Endomorphism and matrix trusses

- For any A-module M,

$$\mathrm{End}_A(M)$$

  is a truss in the same way as endomorphisms of an abelian herd.
- A^n is an A-module: for all $a = (a_i), b = (b_i), c = (c_i) \in A^n$, $x \in A$,

$$[a, b, c]_i = [a_i, b_i, c_i], \qquad (x \triangleright a)_i = x \triangleright a_i.$$

- $M_n(A) := \mathrm{End}_A(A^n)$ is a (matrix) truss.
- $\mathrm{End}_A(A^n)$ satisfy a brace-type distributive law between $\diamond_{\mathrm{id}}$ and $\circ$.