Trusses: between braces and rings

Tomasz Brzeziński

Abstract An algebraic structure is a collection of sets with operations. Typical and most widespread across mathematics are systems such as a semigroup, monoid, group, ring, field, associative algebra, vector space or module. In this course we will study some simple algebraic systems which have recently gained prominent position in algebra and topology such as braces, racks or quandles (sets with two operations interacting with each other in prescribed ways). In particular we will explore a little known fact (first described nearly 100 years ago by Pruefer and Baer) that one can give a definition of a group without requesting existence of the neutral element and inverses by using a ternary rather than a binary operation (i.e. an operation with three rather than the usual two inputs). A set with such a suitable ternary operation is known as a heap. By picking an element in a heap, the ternary operation is reduced to the binary group operation, for which the chosen element is the neutral element (the resulting group is known as a retract). We will study properties and examples of heaps and relate them to the properties of corresponding groups (retracts). Next we will look at heaps with an additional binary operation that distributes over the ternary heap operation, known as trusses, relate them to both rings and braces, and study their properties and applications.

1

1.1 Introduction

The notes correspond to a 8-hours mini-course taught by Prof. Tomasz Brzeziński at the Department of Mathematics at ULB, Brussels, in May 2022. The course is

Tomasz Brzeziński
Swansea University (UK) and University of Bialystok (Poland), e-mail: t.brzezinski@swansea.ac.uk

addressed to Master and PhD students, researchers and any one else with an interest in (new) algebraic structures. The course is based on [2, 4, 5].

Notes by Leandro Vendramin. This version was compiled on Wednesday 18th May, 2022 at 11:49.

1.2 Algebraic structures

We start with some basic definitions from universal algebra. We refer to [6] for more details.

Definition 1.1. *An **algebraic structure** is a set A with a collection of maps (called operations) $\alpha_i\colon A^{|\alpha_i|} \to A$ for $i \in I$. By convention, $A^0 = \{*\}$. This algebraic structure on A will be denoted by $(A, (\alpha_i)_{i\in I})$. The number $|\alpha_i| \in \mathbb{Z}_{\geq 0}$ is the **arity** of the operation α_i.*

For example, let A be a set and $\alpha\colon A^{|\alpha|} \to A$ be a map. If $|\alpha| = 0$, then α is a nullary operation. If $|\alpha| = 1$, then α is a unary operation. If $|\alpha| = 2$, then α is a binary operation.

Example 1.2. A semigroup is a set A with an operation $A \times A \to A$, $(a, b) \mapsto ab$. Thus a semigroup is an algebraic structure.

Other examples of algebraic structures are monoids, groups, vector spaces.

Definition 1.3. *We say that the algebraic structures $(A, (\alpha_i)_{i\in I})$ and $(B, (\beta_i)_{i\in I})$ have the **same type** if $|\alpha_i| = |\beta_i|$ for all $i \in I$.*

Definition 1.4. *Let $(A, (\alpha_i)_{i\in I})$ and $(B, (\beta_i)_{i\in I})$ be algebraic structures of the same type. A map $f\colon A \to B$ is a **homomorphism** of algebraic structures if for every $i \in I$ the diagram*

$$\begin{array}{ccc} A^{|\alpha_i|} & \xrightarrow{\alpha_i} & A \\ {\scriptstyle f^{|\alpha_i|}}\downarrow & & \downarrow{\scriptstyle f} \\ B^{|\beta_i|} & \xrightarrow[\beta_i]{} & B \end{array}$$

is commutative.

If $f\colon A \to B$ is a map and $X \subseteq A$ is a subset, we write $f|_X$ to denote the restriction of f on X, that is the map $f\colon X \to B$, $x \mapsto f(x)$.

Exercise 1.5. If $f\colon (A, (\alpha_i)_{i\in I}) \to (B, (\beta_i)_{i\in I})$ is a homomorphism, then the **image** $\big(\mathrm{img}(f), (\beta_i|_{\mathrm{img}(f)})_{i\in I}\big)$ of f is an algebraic structure of the same type.

Definition 1.6. *A **congruence** on $(A, (\alpha_i)_{i\in I})$ is an equivalence relation R on A such that for every $i \in I$ one has*

$$a_k R b_k \quad \forall k \in \{1, \dots, |\alpha_i|\} \implies \alpha_i(a_1, \dots, a_{|\alpha_i|}) R \alpha_i(b_1, \dots, b_{|\alpha_i|}).$$

Exercise 1.7. Prove the following statements:

1) If R is a congruence on $(A, (\alpha_i)_{i\in I})$, then $(A/R, (\overline{\alpha_i})_{i\in I})$, where

$$\overline{\alpha_i}(\overline{a_1}, \dots, \overline{a_{|\alpha_i|}}) = \overline{\alpha_i(a_1, \dots, a_{|\alpha_i|})},$$

is an algebraic structure of the same type.
2) If $f\colon (A, (\alpha_i)_{i\in I}) \to (B, (\beta_i)_{i\in I})$ is a homomorphism, then

$$a(\ker f)b \iff f(a) = f(b)$$

is a congruence. This is known as the **kernel relation** $\ker f$.
3) Every congruence is a kernel relation.

1.3 Heaps

Definition 1.8. *A **heap** is a set H with a ternary operation $H \times H \times H \to H$, $(x, y, z) \mapsto [x, y, z]$, such that for all $a, b, c, d, e \in H$,*

$$[[a, b, c], d, e] = [a, b, [c, d, e]], \tag{1}$$
$$[a, a, b] = [b, a, a] = b. \tag{2}$$

Equality (2) is known as Malcev's identity.

Definition 1.9. *A heap H is **abelian** if $[a, b, c] = [c, b, a]$ for all $a, b, c \in H$.*

Homomorphism of heaps are defined in the usual way. Heaps and heap homomorphism for a category. It will be denoted by **Hp**.

1.4 Examples

The empty set $\emptyset$ is a heap. However, we will only work with non-empty heaps.

Example 1.10. If G is a group, then the operation

$$[a, b, c] = ab^{-1}c$$

turns G into a heap $H(G)$. Note that the heap G is abelian if and only if $H(G)$ is abelian. Moreover, if $f\colon G \to G_1$ is a homomorphism of groups, then $H(f)\colon H(G) \to H(G_1), x \mapsto f(x)$, is a homomorphism of heaps.

Example 1.11. Let G be a group and H be a subgroup of G. For every $a \in G$, the coset $aH = \{ah : h \in H\}$ is a heap with $[ax, ay, az] = axy^{-1}z$.

Recall that a **groupoid** is a small category $\mathcal{C}$ in which every morphism is an isomorphism. We write $\mathrm{Obj}(\mathcal{C})$ to denote the set of objects of $\mathcal{C}$. If $A, B \in \mathrm{Obj}(\mathcal{C})$, then $\mathcal{C}(A, B)$ will be the set of morphisms $A \to B$.

Example 1.12. Let $\mathcal{C}$ be a groupoid and $A, B \in \mathrm{Obj}(\mathcal{C})$. Then $\mathcal{C}(A, B)$ is a heap with $[f, g, h] = f \circ g^{-1} \circ h$. Note that this is well-defined, as

$$A \xrightarrow{\ h\ } B \underset{g}{\overset{g^{-1}}{\rightleftarrows}} A \xrightarrow{\ f\ } B$$

An **affine space** (over a field F) is a set A with a free and transitive action of an F-vector space $\overrightarrow{A}$. This means that there is a map $A \times \overrightarrow{A} \to A$, $(a, v) \mapsto a + v$, such that the following condition hold:

1) $a + (v + w) = (a + v) + w$ for all $a \in A$ and $v, w \in \overrightarrow{A}$.
2) $a + 0 = a$ for all $a \in A$.
3) For every $a, b \in A$ there exists a unique $\overrightarrow{ab} \in \overrightarrow{A}$ such that $b = a + \overrightarrow{ab}$.

Example 1.13. Let A be an affine space. Then A is an abelian heap with the operation $[a, b, c] = a + \overrightarrow{bc}$.

We first prove Malcev's identities: Clearly, $[a, a, b] = a + \overrightarrow{ab} = b$, as $\overrightarrow{ab}$ is the unique vector that sends a to b. Similarly, $[b, a, a] = b$, as $\overrightarrow{aa} = 0$.

We claim that $\overrightarrow{a(b+v)} = \overrightarrow{ab} + v$ for all $a, b \in A$ and $v \in \overrightarrow{A}$. In fact, using Malcev's identities,

$$a + \overrightarrow{a(b+v)} = b + v = \left(a + \overrightarrow{ab}\right) + v = a + \left(\overrightarrow{ab} + v\right).$$

Now we compute

$$\begin{aligned}[a, b, [c, x, y]] = \left[a, b, c + \overrightarrow{xy}\right] &= a + \overrightarrow{b\left(x + \overrightarrow{xy}\right)} \\ &= a + \left(\overrightarrow{bc} + \overrightarrow{xy}\right) = \left(a + \overrightarrow{bc}\right) + \overrightarrow{xy} = [[a, b, c], x, y].\end{aligned}$$

To prove that the heap is abelian we first note that since

$$a + \left(\overrightarrow{ab} + \overrightarrow{ba}\right) = b + \overrightarrow{ba} = a,$$

it follows that $\overrightarrow{ab} + \overrightarrow{ba} = 0$. Since

$$c = b + \overrightarrow{bc} = \left(a + \overrightarrow{ab}\right) + \overrightarrow{bc},$$

it follows that

$$[c, b, a] = c + \overrightarrow{ba} = a + \overrightarrow{ab} + \overrightarrow{bc} + \overrightarrow{ba} = a + \overrightarrow{bc} = [a, b, c].$$

1.5 Heaps vs. groups

We now summarize the relationship between groups and heaps. Let **Grp** denote the category of groups and group homomorphisms.

Theorem 1.14.

1) The assignment $G \to H(G)$ and $f \mapsto H(f)$ is a functor from **Grp** *to* **Hp**.
2) For any heap H and any $e \in H$, the operation $ab = [a, e, b]$ turns H into a group. This group is known as the ***retract*** *$G(H, e)$ of H at e.*
3) If $f\colon H \to H'$ is a heap homomorphism, then for all $e \in H$ and $e' \in H'$ the maps

$$f_e^{e'}\colon G(H,e) \to G(H',e'), \qquad a \mapsto [f(a), f(e), e'],$$
$$f_{e'}^{e}\colon G(H,e) \to G(H',e'), \qquad a \mapsto [e', f(e), f(a)],$$

are group homomorphisms.
4) If H is a heap and $e \in H$, then $H(G(H, e)) = H$.
5) If G is a group and $x \in G$, then $G(H(G), x) \simeq G$.

Sketch of the proof. Routine calculations prove 1), see Exercise 1.10.

Let us prove 2). By using (2) we obtain that e is the identity of $G(H, e)$. For example, $ae = [a, e, e] = a$. If $a \in H$, then $a^{-1} = [e, a, e]$. In fact,

$$aa^{-1} = [a, e, a^{-1}] = [a, e, [e, a, e]] = [[a, e, e], a, e] = [a, a, e] = e.$$

The associativity is left as an exercise.

3) Let us prove that $f_e^{e_1}$ is a group homomorphism. Let $a, b \in H(G)$. On the one hand,

$$\begin{aligned} f_e^{e_1}(ab) &= f_e^{e_1}([a, e, b]) \\ &= [f([a, e, b]), f(e), e_1] \\ &= [[f(a), f(e), f(b)], f(e), e_1] \\ &= [f(a), f(e), [f(b), f(e), e_1]]. \end{aligned}$$

On the other hand,

$$\begin{aligned} f_e^{e_1}(a) f_e^{e_1}(b) &= [f(a), f(e), e_1][f(b), f(e), e_1] \\ &= [[f(a), f(e), e_1], e_1, [f(b), f(e), e_1]] \\ &= [f(a), f(e), [e_1, e_1, [f(b), f(e), e_1]] \\ &= [f(a), f(e), [f(b), f(e), e_1]]. \end{aligned}$$

The other equality is similar.

We prove 4). We start with a heap H. Fix $e \in H$ and construct the group $G(H, e)$ with multiplication $(x, y) \mapsto xy = [x, e, y]$. Now we construct the heap $H(G(H, e))$ with operation $(a, b, c) \mapsto ab^{-1}c$. Recall that $b^{-1} = [e, b, e]$. Thus

$$\begin{aligned} ab^{-1}c &= [ab^{-1}, e, c] = [[a, e, b^{-1}], e, c] \\ &= [[a, e, [e, b, e]], e, c] = [[[a, e, e], b, e], e, c] \\ &= [[a, b, e], e, c] = [a, b, [e, e, c]] = [a, b, c]. \end{aligned}$$

To prove 5) recall that G has multiplication $(a, b) \mapsto ab$. Then $H(G)$ is a heap with $[a, b, c] = ab^{-1}c$ and for $x \in G$, $G(H(G), x)$ is a group with multiplication $(a, b) \mapsto a \cdot b = [a, x, b] = ax^{-1}b$. The map $f\colon G \to G(H(G), x)$, $a \mapsto ax$ is a group homomorphism, as

$$f(ab) = (ab)x = (ax)x^{-1}(bx) = f(a)x^{-1}f(b) = f(a) \cdot f(b).$$

Moreover, f is bijective with inverse $G(H(G), x) \to G$, $a \mapsto ax^{-1}$. □

As an application of Theorem 1.14 we can quickly prove the several properties of heaps.

1.6 Properties of heaps

We now prove several properties of heaps. Instead of using Theorem 1.14 we rather provide heap-theoretic proofs.

Theorem 1.15. *Let H be a heap and $a, b, c, d, e \in H$. Then the following statements hold:*

1) If $[a, b, c] = d$, then $a = [d, c, b]$.
2) $[a, b, [c, d, e]] = [a, [d, c, b], e]$.
3) In $[a, b, c] = d$, any three elements determine the fourth one.
4) $a = b$ if and only if $[a, b, c] = c$ for all $c \in H$.

Proof. Let us start with 1). Using (1) and (2),

$$a = [a, b, b] = [a, b, [c, c, b]] = [[a, b, c], c, b] = [d, c, b].$$

We now prove 2). Let $a, b, c, d, e \in H$. Then (1) and (2) imply that

$$a = [[a, b, c], c, b] = [[[a, b, c], d, d], c, b] = [[a, b, c], d, [d, c, b]] .$$

Using 1) and Malcev's identities we obtain that

$$[a, b, c] = [a, [d, c, b], d] = [a, [d, c, b], [e, e, d]] = [[a, [d, c, b], e], e, d] .$$

Again by using 1) we conclude that

$$[a, [d, c, b], e] = [[a, b, c], d, e] .$$

Let us prove 3). Let $a, b, c \in H$ and $d = [a, b, c]$. In 1) we obtained that $a = [d, c, b]$. Similarly,

$$c = [b, b, c] = [[b, a, a], b, c] = [b, a, [a, b, c]] = [b, a, d].$$

Now using 2) we obtain

$$b = [b, a, a] = [c, c, [b, a, a]] = [c, [a, b, c], a] = [c, d, a].$$

To prove 4) note that, if $a = b$, then $[a, b, c] = [a, a, c] = c$ for all $c \in H$ by Malcev's identity. Conversely, if $[a, b, c] = c$ for all $c \in H$, then, in particular, $a = [a, b, b] = b$ by Malcev's identity. □

Exercise 1.16. Let H be a heap and $a, b \in H$. Prove that $a = b$ if and only if there exists $c \in H$ such that $[a, b, c] = c$.

For $n \in \mathbb{Z}_{\geq 2}$ let Sym_n be the symmetric group in n letters.

Exercise 1.17. In an abelian heap,

$$[x_1, y_1, x_2, y_2, \ldots, x_n, y_n, x_{n+1}] = [x_{\sigma(1)}, y_{\tau(1)}, \ldots, x_{\sigma(n)}, y_{\tau(n)}, x_{\sigma(n+1)}]$$

for all $\sigma \in \mathrm{Sym}_{n+1}$ and $\tau \in \mathrm{Sym}_n$.

The previous exercise and Malcev's identity (2) give a useful trick that avoids painful calculations in the context of abelian heaps. Let us do a concrete example:

$$[a, b, c, d, b] = [a, b, [c, d, b]] = [a, b, [b, d, c]] = [[a, b, b], d, c] = [a, d, c].$$

1.7 sub-heaps and the sub-heap relation

Definition 1.18. *Let H be a heap. A non-empty subset S of H is a **sub-heap** if $[s, s_1, s_2] \in S$ for all $s, s_1, s_2 \in S$.*

Exercise 1.19. Let H be a heap, $e \in H$ and S be a non-empty subset of H. Prove that S is a sub-heap if and only if S is a subgroup of $G(H, e)$.

If H is a heap and S is a sub-heap of H, we define a **sub-heap relation** as follows:

$$a \sim_S b \iff [a, b, s] \in S \text{ for some } s \in S.$$

Note that $a \sim_S b$ if and only if $[a, b, s] \in S$ for all $s \in S$.

Proposition 1.20. *Let H be a heap and S be a sub-heap. Then $\sim_S$ is an equivalence relation.*

Proof. Let $a, b, c \in S$. Then $a \sim_S a$, as $[a, a, a] = a$ by Malcev's identity. If $a \sim_S b$, then $[a, b, s] \in S$ for some $s \in S$. Thus, since

$$[b, a, [a, b, s]] = [[b, a, a], b, s] = [b, b, s] = s \in S,$$

we obtain that $b \sim_S a$. Finally, assume that $a \sim_S b$ and $b \sim_S c$. We know that $c \sim_S a$, so $[c, a, s] \in S$ for some $s \in S$. Thus

$$[a, c, [c, a, s]] = [[a, c, c], a, s] = [a, a, s] = s \in S$$

and hence $a \sim_S c$. □

2

Let H be a heap and $S \subseteq H$ be a sub-heap. For $a \in H$ the orbit of a is the set

$$\overline{a} = \{c \in H : c \sim_S a\}$$

We write H/S to denote the set of equivalence classes.

Theorem 2.1. *Let H be a heap and S be a sub-heap of H. The following statements hold:*

1) For every $s \in S$, $\overline{s} = S$.
2) For every $a \in H$, $\overline{a}$ is a sub-heap of H.
3) For every $a, b \in H$, the map

$$\tau_b^a : H \to H, \quad c \mapsto [c, b, a],$$

is an automorphism of heaps.
4) For every $a, b \in H$, $\overline{a} \simeq \overline{b}$ as heaps.
5) For every $a \in H$, $\sim_S = \sim_{\overline{a}}$.

Proof. Let us first prove 1). Let $s \in S$. To prove that $\overline{s} \subseteq S$ let $a \in H$ be such that $a \sim_S s$. Then $[a, s, t] = u \in S$ for some $t \in S$. By Theorem 1.15, $a = [u, t, s] \in S$, as S is a sub-heap. Conversely,

if $a \in S$, then, in particular, $[a, s, s] \in S$. Thus $a \sim_S s$.

We now prove 2). Let $x, y, z \in S$ be such that $x, y, z \in \overline{a}$. Since $x \sim_S a$ and $y \sim_S a$, it follows that $x \sim_S y$, so there exists $s \in S$ such that $[x, y, s] \in S$. Since

$$[[x, y, z], z, s] = [x, y, [z, z, s]] = [x, y, s] \in S,$$

one has $[x, y, z] \sim_S z$. Now the claim follows since $z \sim_S a$.

Let us prove 3). On the one hand,

$$\tau_b^a([x, y, z]) = [[x, y, z], b, a]] = [x, y, [z, b, a]].$$

On the other hand, using Theorem 1.14 and Malcev's identities:

$$\begin{aligned}[\tau_b^a(x), \tau_b^a(y), \tau_b^a(z)] &= [[x,b,a],[y,b,a],[z,b,a]] \\ &= [x,b,[a,[y,b,a],[z,b,a]] \\ &= [x,b,[a,[a,b,y],[z,b,a]] \\ &= [x,b,[[a,a,b],[y,[z,b,a]] \\ &= [[x,b,b],[y,[z,b,a]] \\ &= [x,y,[z,b,a]].\end{aligned}$$

The map τ_b^a is bijective with inverse τ_a^b, as, for example,

$$\tau_b^a\tau_a^b(c) = \tau_b^a([c,a,b]) = [[c,a,b],b,a] = [c,a,[b,b,a]] = [c,a,a] = c.$$

4) Let $a, b \in H$. The map τ_a^b is an automorphism of heaps such that $\tau_a^b(a) = b$. We claim that $\tau_a^b(\overline{a}) = \overline{b}$. Let $x \in H$ be such that $x \sim_S a$. In particular, $a \sim_S x$, so $[a,x,s] \in S$ for some $s \in S$. Now $\tau_a^b(x) \sim_S b$, as

$$\begin{aligned}\left[\tau_a^b(x), b, [a,x,s]\right] &= [[x,a,b],b,[a,x,s]] \\ &= [x,a,[b,b,[a,x,s]] = [x,a,[a,x,s]] = s \in S.\end{aligned}$$

5) Assume first that $x \sim_{\overline{a}} y$. Then there exists $b \in \overline{a}$ such that $[x,y,b] \sim_S a$. Since $[x,y,b] \sim_S a$ and $b \sim_S a$, it follows that $[x,y,b] \sim_S b$. Thus there exists $s \in S$ such that

$$[x,y,s] = [x,y,[b,b,s]] = [[x,y,b],b,s] \in S.$$

That is $x \sim_S y$. Conversely, assume now that $x \sim_S y$. Then there exists $s \in S$ such that

$$[[x,y,b],b,s] = [x,y,[b,b,s]] = [x,y,s] \in S.$$

Let $b \in \overline{a}$. Since $[x,y,b] \sim_S b$, it follows that $[x,y,b] \sim_S a$ and hence $x \sim_{\overline{a}} y$. □

Definition 2.2. *A sub-heap S of H is **normal** if for every $a \in H$ and $s, e \in H$ one has $[[a,e,s],a,e] \in S$.*

Note a sub-heap S of H is normal if and only if for every $a \in H$ and $s, e \in S$ there exists $t \in S$ such that $[a,e,s] = [t,e,a]$.

Exercise 2.3. Prove that a sub-heap S of H is normal if and only if S is a normal subgroup of $G(H,e)$ for every $e \in S$.

Theorem 2.4. *Let $f : H \to K$ be a homomorphism of heaps. For $c \in H$ let*

$$\overline{c} = \{b \in H : f(b) = f(c)\}$$

be the equivalence class of c with respect to $\ker(f)$. *Then $\overline{c}$ is a sub-heap of H.*

Proof. To prove that $\overline{c}$ is a sub-heap first note that $c \in \overline{c}$, so $\overline{c}$ is non-empty. Now let $x, y, z \in \overline{c}$. Then $f(x) = f(y) = f(z) = [x,y,z] \in \overline{c}$, as

$$f([x,y,z]) = [f(x),f(y),f(z)] = [f(c),f(c),f(c)] = f(c).$$

To prove that $\overline{c}$ is normal let $x, y \in \overline{c}$ and $a \in H$. Since $f(x) = f(y) = f(c)$,

$$\begin{aligned} f([[x,y,s],x,y]]) &= [[f(a),f(x),f(y)],f(a),f(x)] \\ &= [[f(a),f(c),f(c)],f(a),f(c)] \\ &= [f(a),f(a),f(c)] = f(c). \end{aligned}$$ □

Definition 2.5. *Let $f\colon H \to K$ be a homomorphism of heaps and $e \in f(H)$. An e-kernel of f is defined as the set*

$$\ker_e f = \{a \in H : f(a) = e\}.$$

Theorem 2.6. *Let $f\colon H \to K$ be a homomorphism of heaps and $e \in f(H)$.*

1) $\ker_e f$ *is a normal sub-heap of H.*
2) $a \sim_{\ker_e f} b$ if and only if $f(a) = f(b)$.
3) For every $e, e_1 \in f(H)$, $\ker_e f \simeq \ker_{e_1} f$.

Proof. Let us prove 1). By definition, $\ker_e f$ is non-empty. If $x, y, z \in \ker_e f$, then $f(x) = f(y) = f(z) = e$. Since f is a heap homomorphism,

$$f([x,y,z]) = [f(x),f(y),f(z)] = [e,e,e] = e$$

and hence $[x,y,z] \in \ker_e f$. To prove that $\ker_e f$ is normal note that

$$f([[a,x,y],a,x]) = [[f(a),f(x),f(y)],f(a),f(x)] = [[f(a),e,e],f(a),e] = e.$$

Now we prove 2). Let $S = \ker_e f$. Then

$$\begin{aligned} a \sim_S b &\iff [a,b,s] \in S \text{ for some } s \in S \\ &\iff f([a,b,s]) = e \text{ for some } s \in H \text{ such that } f(s) = e \\ &\iff [f(a),f(b),e] = e \\ &\iff f(a) = f(b), \end{aligned}$$

by Exercise 1.16.

Finally we prove 3). Let $x, y \in H$ be such that $f(x) = e$ and $f(y) = e_1$. Note that

$$\ker_e f = \{a \in H : f(a) = e\} = \{a \in H : f(a) = f(x)\} = \overline{x}$$

Similarly, $\ker_{e_1} f = \overline{y}$. We know that both $\overline{x}$ and $\overline{y}$ are sub-heaps of H. They are isomorphic, as $\tau_x^y(\overline{x}) = \overline{y}$. In fact, if $z \in \overline{x}$, then $\tau_x^y(z) \in \overline{y}$, as

$$f(\tau_x^y(z)) = f([z,x,y]) = [f(z),f(x),f(y)] = [f(x),f(x),f(y)] = f(y).$$ □

We leave the proof of the following result as an exercise.

Corollary 2.7. *Every congruence of heaps is a sub-heap relation with respect to a normal sub-heap.*

2.1 Universal differences between heaps and groups

Let X be a non-empty set. The set $W(X)$ of reduced words on X is defined as the set of words $x_1 \cdots x_{2n+1}$ in elements of X of odd length such that no consecutive letters are the same, i.e.

$$W(X) = \{x_1 \cdots x_{2n+1} : n \geq 1,\ x_1, \ldots, x_{2n+1} \in X,\ x_i \neq x_{i+1} \text{ for all } i\}$$

For a word $x_1 \cdots x_{2n+1}$ the opposite word is

$$(x_1 \cdots x_{2n+1})^{\mathrm{t}} = x_{2n+1} \cdots x_2 x_1.$$

On $W(X)$ we define a ternary operation $[-,-,-]$ by *grafting and pruning*. What does it mean? If $u, v, w \in W(X)$, then $[u, v, w]$ is obtained by removing (or pruning) all pairs of consecutive equal letters from $uv^{\mathrm{t}}w$ (obtained by concatenation of u, v^{t} and w). One proves that $(W(X), [-,-,-])$ is a heap. It is the **free heap** on X and it will be denoted by $\mathcal{H}(X)$.

Definition 2.8. *Let X be a set. A **free heap** on $\mathcal{H}(X)$ is a heap with with the following property: for any heap H and any map $f\colon X \to H$ there exists a unique heap homomorphism $\varphi\colon \mathcal{H}(X) \to H$ such that*

$$\begin{array}{ccc} X & \xrightarrow{\ \iota\ } & \mathcal{H}(X) \\ {\scriptstyle f}\big\downarrow & \swarrow_{\varphi} & \\ H & & \end{array}$$

commutes, where $\iota\colon X \to W(X)$ denotes the inclusion.

Example 2.9. $\mathcal{H}(\{x\}) = \{x\}$.

Example 2.10. $\mathcal{H}(\{x, y\}) \simeq \mathcal{H}(\mathbb{Z})$ via $x \mapsto 0$ and

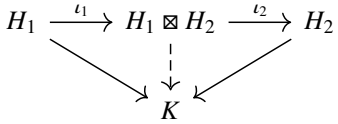
$$\underbrace{xyx \cdots yx}_{n\text{-times } y} \mapsto -n, \quad \underbrace{yx \cdots yx}_{n\text{-times } y} \mapsto n.$$

Example 2.11. Let X be a set. The **free abelian heap** $\mathcal{A}(X)$ is defined as the free heap $\mathcal{H}(X)$ on X modulo the action of $\bigcup_n \left(\mathrm{Sym}_{n+1} \times \mathrm{Sym}_n\right)$ given by

$$(\sigma, \tau) \cdot x_1 y_1 x_2 y_2 \cdots x_n y_n x_{n+1} = x_{\sigma(1)} y_{\tau(1)} x_{\sigma(2)} y_{\tau(2)} \cdots x_{\sigma(n)} y_{\sigma(n)} x_{\sigma(n+1)}$$

for $\sigma \in \mathrm{Sym}_{n+1}$ and $\tau \in \mathrm{Sym}_n$.

We now describe the **direct sum** (or coproduct) $H_1 \boxtimes H_2$ of the abelian heaps H_1 and H_2. It is precisely the coproduct of H_1 and H_2 in the category of abelian heaps:



where $\iota_1 : H_1 \to H_1 \boxtimes H_2$ and $\iota_2 : H_2 \to H_1 \boxtimes H_2$ are the inclusions.

Let U be the disjoiunt union of H_1 and H_2 and $\mathcal{A}(U)$ be the free abelian heap on U...

$$H_1 \boxtimes H_2 = \mathcal{H}\left(G(H_1, e_1) \oplus G(H_2, e_2) \oplus \mathbb{Z}\right)$$

2.2 Trusses

Definition 2.12. *A left (resp. right)* ***skew truss*** *is a heap $(T, [-,-,-])$ with an associative binary operation $(x, y) \mapsto xy$ such that*

$$a[b,c,d] = [ab, ac, ad] \qquad \textit{(resp. } [a,b,c]d = [ad, bd, cd]\textit{).}$$

If T is an abelian heap, then we drop skew from the terminology. A ***truss*** *is a left and right truss.*

Example 2.13. The set $2\mathbb{Z} + 1 = \{2m + 1 : m \in \mathbb{Z}\}$ is a truss with the usual multiplication and $[x, y, z] = x - y + z$.

Example 2.14. The set

$$\frac{2\mathbb{Z}+1}{2\mathbb{Z}+1} = \left\{\frac{a}{b} : a, b \text{ odd integers}\right\}$$

is a truss with the usual multiplication and $[x, y, z] = x - y + z$. Note that both operations are well-defined.

Example 2.15. Let H be an abelian heap. The set $\mathrm{End}(H)$ of heap endomorphisms of H is an abelian heap with

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

We prove that the operation is well-defined. Since H is abelian, we can use Exercise 1.17 to obtain that

$$\begin{aligned}
[f, g, h]\left([a, b, c]\right) &= [f([a, b, c]), g([a, b, c]), h([a, b, c])] \\
&= [[f(a), f(b), f(c)], [g(a), g(b), g(c)], [h(a), h(b), h(c)]] \\
&= [[f(a), g(a), h(a)], [f(b), g(b), h(b)], [f(c), g(c), h(c)]] \\
&= [[f, g, h](a), [f, g, h](b), [f, g, h](c)] \,.
\end{aligned}$$

Moreover, $\mathrm{End}(H)$ is a truss with the usual composition:

$$([f,g,h]\circ k)\,(a) = [f(k(a)), g(k(a), h(k(a))]$$

and

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

Let F be a field. An associative F-algebra is an F-vector space A with a bilinear associative multiplication. In particular, A is a ring. What if A is replaced by an affine space?

Example 2.16. Let F be a field. Then F acts on A by $(\lambda, a, b)\mapsto a+\lambda\overrightarrow{ab}$. An affine transformation is a pair $\left(f, \overrightarrow{f}\right)$, where $f\colon A\to B$ is a map and $\overrightarrow{f}\colon \overrightarrow{A}\to\overrightarrow{B}$ is a linear transformation such that

$$\overrightarrow{f}\left(\overrightarrow{ab}\right) = \overrightarrow{f(a)f(b)}$$

for all $a, b\in A$. In particular, this implies that

$$\begin{aligned}[f(a), f(b), f(c)] = f(a) + \overrightarrow{f(b)f(c)} &= f(a) + \overrightarrow{f}\left(\overrightarrow{bc}\right)\\ &= f(a) + \overrightarrow{f(a)f\left(a+\overrightarrow{bc}\right)} = f\left(a+\overrightarrow{bc}\right) = f\left([a,b,c]\right)\end{aligned}$$

for all $a, b, c\in A$.

Let $m\colon A\times A\to A$, $(x,y)\mapsto xy$, be the multiplication map. If m is bi-affine, then, in particular,

$$[a,b,c]d = m([a,b,c],d) = [m(a,d), m(b,d), m(c,d)] = [ad, bd, cd].$$

Thus an affine space with an F-affine multiplication is a truss.

A (left) **skew ring** is a triple $(A,+,\cdot)$, where $(A,+)$ is a group, $(A,\cdot)$ is a semigroup and $a(b+c) = ab - a + ac$ for all $a, b, c\in A$.

Example 2.17. A (left) skew ring is a (left) truss with

$$a[b,c,d] = a(b-c+d) = ab - ac + ad = [ab, ac, ad].$$

A **skew left brace** is a triple $(A,+,\cdot)$, where $(A,+)$ and $(A,\cdot)$ are groups and $a(b+c) = ab - a + ac$ holds for all $a, b, c\in A$. It follows that $1_A = 0_A$.

Proposition 2.18.

1) Let B be a skew left brace. Then $(H(B),\cdot)$ is a skew left truss.
2) Let T be a skew left truss such that $(T,\cdot)$ is a group. If 1_T denotes the neutral element of $(T,\cdot)$, then $x+y = [x, 1_T, y]$ turns $G(T, 1_T)$ into a skew left brace.

Sketch of the proof. We first prove 1). Note that $x\cdot(-y) = x - x\cdot y + x$ for all $x, y \in B$. Now

$$\begin{aligned} a[b,c,d] &= a(b-c+d) \\ &= ab - a + a(-c) - a + ad \\ &= ab - ac + ad \\ &= [ab, ac, ad]. \end{aligned}$$

We now prove 2). Let $a, b, c \in T$. Then

$$x(y+z) = x[y, 1_T, z] = [xy, x, xz] = xy - x + xz.$$

From this the claim follows. □

2.3 Trusses on $\mathbb{Z}$

The additive group $\mathbb{Z}$ is a heap with the operation $[a,b,c] = a - b + c$. Following [3] we now describe the truss structures over $(\mathbb{Z}, [-,-,-])$.

Let

$$\begin{aligned} I_2(\mathbb{Z}) &= \left\{ q \in M_2(\mathbb{Z}) : q^2 = q,\ \mathrm{trace}(q) = 1 \right\} \\ &= \left\{ \begin{pmatrix} b & a \\ -c & 1-b \end{pmatrix} : a, b \in \mathbb{Z},\ ac = b(b-1) \right\}. \end{aligned}$$

The trusses on $\mathbb{Z}$ are:

1) $m \cdot n = m$.
2) $m \cdot n = n$.
3) $m \cdot n = amn + b(m+n) + c$. This truss will be denoted by $\mathbb{Z}(a,b,c)$.

One proves that $\mathbb{Z}(a,b,c) \simeq \mathbb{Z}(\alpha,\beta,\gamma)$ if and only if

$$\begin{pmatrix} \beta & \alpha \\ -\gamma & 1-\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ k & \pm 1 \end{pmatrix} \begin{pmatrix} b & a \\ -c & 1-b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \mp k & \pm 1 \end{pmatrix}$$

for some $k \in \mathbb{Z}$.

Note that

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

is the infinite-dihedral group. So isomorphism classes of commutative truss structures on $(\mathbb{Z}, [-,-,-])$ are in bijective correspondence with orbits of the conjugation action of D_∞ on $I_2(\mathbb{Z})$.

3

3.1 A binary perspective

Let T be a truss and $e \in T$. Let $\sigma_L \colon T \to T$, $\sigma_L(a) = ae$, and $\sigma_R \colon T \to T$, $\sigma_R(a) = ea$. Note that $\sigma_L(e) = \sigma_R(e)$. Construct $(T, [-,-,-])$ to the retract $G(T, e)$. Then

$$a(b + c) = a[b, e, c] = ab - ae + ac = ab - \sigma_L(a) + ac$$

and similarly $(a + b)c = ab - \sigma_R(c) + bc$. So one can think of trusses as tuples $(T, +, \cdot, \sigma_L, \sigma_R)$ with $\sigma_L(a) = a0$ and $\sigma_R(a) = 0a$. This is a different algebraic structure, though!

1) If $\sigma_L(a) = \sigma_R(a) = 0$ for all a, then we obtain a ring.
2) If $\sigma_L(a) = \sigma_R(a) = a$ for all a, then we obtain a skew left brace such that $(a + b)c = ac - c + ab$ for all a, b, c.

3.2 Trusses and rings

Example 3.1. Let R be a ring. Then $H(R, +)$ is a heap with $[a, b, c] = a - b + c$. Thus $(H(R, +), \cdot)$ is a truss. It will be denoted by $T(R)$.

Theorem 3.2. *Let T be a truss. For every $e \in T$, $G(T, e)$ is an associative ring with operations $a \cdot b = [ab, ae, e^2, eb, e]$ and $a + b = [a, e, b]$. This ring will be denoted by $R(T, e)$. The map $\tau_e^f : T \to T$, $a \mapsto [a, e, f]$, is an isomorphism of rings $R(T, e) \to R(T, f)$.*

Sketch of the proof. Note that T is an abelian heap. Let us prove the distributivity. On the one hand,

$$\begin{aligned} a \cdot (b + c) &= a \cdot [b, e, c] \\ &= [a[b, e, c], ae, e^2, e[b, e, c], e] \\ &= [ab, ae, ac, ae, e^2, eb, e^2, ec, e]. \end{aligned}$$

On the other hand,

$$\begin{aligned} a \cdot b + a \cdot c &= [a \cdot b, e, a \cdot c] \\ &= [ab, ae, e^2, eb, e, e, ac, ae, e^2, ec, e] \\ &= [ab, ae, e^2, eb, ac, ae, e^2, ec, e]. \end{aligned}$$

So the distributivity follows from Exercise 1.17.

The other axioms defining a ring are checked in a similar way.

To prove that $\tau_e^f : R(T,e) \to R(T,f)$ is a bijective ring homomorphism, we first note that $\tau_e^f(\tau_f^e(a)) = a$ and $\tau_f^e(\tau_e^f(a)) = a$ for all $a \in T$. Then we use Exercise 1.17 to compute

$$\tau_e^f(a \cdot b) = [a \cdot b, e, f] = [[ab, ae, e^2, eb, e], e, f] = [ab, ae, e^2, eb, f]$$

and

$$\begin{aligned}\tau_e^f(a) \cdot \tau_e^f(b) &= [[a,e,f][b,e,f], [a,e,f]f, f^2, f[b,e,f], f] \\ &= [ab, ae, af, eb, e^2, ef, fb, fe, f^2, af, ef, f^2, f^2, fb, fe, f^2, f] \\ &= [ab, ae, e^2, eb, f].\end{aligned}$$

□

Exercise 3.3. Describe the trusses structures on $H(\mathbb{Z})$.

3.3 Trusses in ideal extension of rings

Definition 3.4. *An exact sequence of non-unitary rings and homomorphisms*

$$0 \longrightarrow R \xrightarrow{\Psi_R} S \xrightarrow{\Psi_{\mathbb{Z}}} \mathbb{Z} \longrightarrow 0$$

is called an ***ideal extension*** *of R to S by $\mathbb{Z}$.*

A **sub-truss** of T is a non-empty subset of T closed under both operations.

Proposition 3.5. *If $q \in \Psi_{\mathbb{Z}}^{-1}(1)$, then $q + \Psi_R(R)$ is a sub-truss of $T(S)$.*

Proof. Let $a = q + \Psi_R(x)$, $b = q + \Psi_R(y)$ and $c = q + \Psi_R(z)$. On the one hand,

$$[a,b,c] = a - b + c = q + \Psi_R([x,y,z]) \in q + \Psi_R(R).$$

On the other hand,

$$ab = (q + \Psi_R(x))(q + \Psi_R(y)) = q^2 + q\Psi_R(y) + \Psi_R(x)q + \Psi_R(x)\Psi_R(y).$$

Note that $q\Psi_R(y) + \Psi_R(x)q + \Psi_R(x)\Psi_R(y) \in \Psi_R(R)$. Moreover,

$$q^2 = q + (q^2 - q) \in q + \Psi_R(R),$$

as $q^2 - q \in \ker \Psi_{\mathbb{Z}} = \Psi_R(R)$, since

$$\Psi_{\mathbb{Z}}(q^2 - q) = \Psi_{\mathbb{Z}}(q)^2 - \Psi_{\mathbb{Z}}(q) = 1^2 - 1 = 0.$$

□

3.4 Ideal extensions and double homothetism

We first start with some definitions that independently go back to Mac Lane, Hoschild and Petrich.

Definition 3.6. *Let R be a ring. A **bimultiplication** (or multiplier) on R is a pair of additive endomorphisms $\sigma = (\sigma_L, \sigma_R)$, where $\sigma_L, \sigma_R \colon R \to R$ such that*

$$\sigma_R(ab) = \sigma_R(a)b, \quad \sigma_L(ab)a\sigma_L(b), \quad a\sigma_R(b) = \sigma_L(a)b$$

for all $a, b \in R$.

Definition 3.7. *A bimultiplication σ is a **double homothetism** (or self-permutable) if $\sigma_L \circ \sigma_R = \sigma_R \circ \sigma_L$.*

The following result appears in [1].

Theorem 3.8. *Let R be a ring, σ be a double homothetism and $s \in R$. Assume that $\sigma_L^2(a) = \sigma_L(a) + sa$ and $\sigma_R^2(a) = \sigma_R(a) + sa$ for all $a \in R$. Then the following statement hold:*

1) The abelian group $R \times \mathbb{Z}$ is a ring with

$$(a, k)(b, l) = (ab + l\sigma_L(a) + k\sigma_R(b) + kls, kl).$$

It will be denoted by $R(\sigma, s)$.
2) The sequence

$$0 \longrightarrow R \xrightarrow{\Psi_R} R(\sigma, s) \xrightarrow{\Psi_{\mathbb{Z}}} \mathbb{Z} \longrightarrow 0 \ ,$$

where $\psi_R(r) = (r, 0)$ and $\psi_{\mathbb{Z}}(r, k) = k$, is an ideal extension.
3) Any ideal ring extension of R by $\mathbb{Z}$ is of this kind.

Sketch of the proof. 1) and 2) follow by direct calculation.

To prove 3) first note that the sequence of abelian groups

$$0 \longrightarrow R \xrightarrow{\Psi_R} S \xrightarrow{\Psi_{\mathbb{Z}}} \mathbb{Z} \longrightarrow 0$$

splits. This means that there is a diagram

$$0 \longrightarrow R \underset{\zeta}{\overset{\Psi_R}{\rightleftarrows}} S \underset{\kappa}{\overset{\Psi_{\mathbb{Z}}}{\rightleftarrows}} \mathbb{Z} \longrightarrow 0$$

with exact rows. For $q \in \Psi_{\mathbb{Z}}^{-1}(1)$ let

$$\sigma_R(a) = \zeta(q\Psi_R(a)), \quad \sigma_L(a) = \zeta(\Psi_R(a)q), \quad s = \zeta(q^2 - q).$$

Then $\theta \colon R(\sigma, s) \to S$, $(a, \eta) \mapsto \Psi_R(a) + \eta q$, is a bijective homomorphism of rings. □

3.5 Ideal extension from trusses

Theorem 3.9.

Sketch of the proof. 1) and 2) follow by a direct calculation.
3) follows from Theorem 3.2.
4)... □

3.6 Some lessons

1) Up to isomorphism trusses determine and are determined by ideal ring extensions by integers.
2) Ideal ring extensions of R by $\mathbb{Z}$ correspond to homothetic data in R.
3) To classify trusses built on R is equivalent to classify homothetic data on R.

Example 3.10. Let A be an abelian group...

3.7 Congruences of trusses: paragons

Definition 3.11. *A **left (resp. right) paragon** in a truss T is a sub-heap P of T such that for all $p, q \in P$ and all $a \in T$ one has $[ap, aq, q] \in P$ (resp. $[pa, qa, q] \in P$). A **paragon** is a left paragon that is also a right paragon.*

Example 3.12. Let R be a ring and I be a left ideal of R. Then $a + I$ is a left paragon in $T(R)$ for every $a \in R$. In fact, every coset is a sub-heap and

$$\begin{aligned}[b(a+x), b(a+y), a+y] &= ba + bx - (ba + by) + a + y \\ &= a + b(x-y) + y \in a + I\end{aligned}$$

for all $x, y \in I$.

Let T and T' be (left) trusses. A map $f : T \to T'$ is a **homomorphism of (left) trusses** if f is a heap homomorphism, i.e. $f([a, b, c]) = [f(a), f(b), f(c)]$ for all $a, b, c \in A$, and $f(ab) = f(a)f(b)$ for all $a, b \in A$.

Proposition 3.13. *Let $f : T \to T'$ be a left trusses homomorphism. Then $P = f^{-1}(b)$ is a paragon in T for all $b \in T'$.*

Proof. Let $a \in T$ and $p, q \in f^{-1}(b)$. Then

$$\begin{aligned}f([ap, aq, q]) &= [f(ap), f(aq), f(q)] \\ &= [f(a)f(p), f(a)f(q), f(q)] = [f(a)b, f(a)b, b] = b.\end{aligned}$$

Similarly, $f([pa, qa, q]) = b$. □

References

1. R. R. Andruszkiewicz, T. Brzeziński, and B. Rybołowicz. Ideal ring extensions and trusses. *J. Algebra*, 600:237–278, 2022.
2. T. Brzeziński. Trusses: between braces and rings. *Trans. Amer. Math. Soc.*, 372(6):4149–4176, 2019.
3. T. Brzeziński. Trusses: paragons, ideals and modules. *J. Pure Appl. Algebra*, 224(6):106258, 39, 2020.
4. T. Brzeziński and B. Rybołowicz. Modules over trusses vs modules over rings: direct sums and free modules. *Algebr. Represent. Theory*, 25(1):1–23, 2022.
5. T. Brzeziński, B. Rybołowicz, and P. Saracco. On functors between categories of modules over trusses. *J. Pure Appl. Algebra*, 226(11):Paper No. 107091, 2022.
6. P. M. Cohn. *Universal algebra*, volume 6 of *Mathematics and its Applications*. D. Reidel Publishing Co., Dordrecht-Boston, Mass., second edition, 1981.