Algebraic Wheel Theory in Lean 4

Yan Yablonovskiy

October 7, 2025

Chapter 1

Algebraic Wheels

1.1 Definition of a Wheel

Algebraic wheels are structures generalising a commutative semiring, attempting to make sense of 'division' by zero.

Loosely speaking, given a semiring R and it's associated monoids, one may extend the semiring in a variety of well-known ways. Considering an additive inverse extends a commutative semiring, to a structure with a given name: a commutative ring, and attempting the same succesfully for the multiplicative monoid yields a field.

Working backwards, given a set M with two monoids – one in additive notation and one in multiplicative. The path to obtain a semiring is clear, a wheel however generalises the semiring by removing the usual distributivity and defines a new unary map $wDiv$.

Definition 1 (Wheel). A Wheel W is an algebraic structure which has two binary operations $(+, *)$, like a ring. Similarly to a commutative ring, a Wheel is a commutative monoid in both operations. Additionally, there is a multiplicative unary map $wDiv$ which is an involution, as well as a few idiosyncratic properties in the interactions of the $+$,$*$ and $wDiv$.

1. Involution: $\forall w \in W, wDiv(wDiv(w)) = w$
2. Multiplicative automophism: $\forall w, v \in W, wDiv(wv) = wDiv(w)wDiv(v)$
3. Right distributivity rule 1: $\forall w, v, u \in W, (w + v)u + 0u = wu + vu$
4. Right distributivity rule 2: $\forall w, v, u \in W, (w + 0v)u + 0u = wu + 0v$
5. Right wDiv distributivity: $\forall w, v, u \in W, (w + uv)wDiv(u) = wDiv(u) + v + 0u$
6. Division by 0: $\forall w \in W, 0Div(0) + w = 0Div(0)$
7. Zero squared: $0 * 0 = 0$
8. Division rule: $\forall w, v \in W, wDiv(w + 0v) = wDiv(w) + 0v$

Whenever not specified, the notation for the monoids is assumed to be $(+, *)$ with neutral elements 0 and 1 respectively.

1.1.1 Basic results

Here we collate some very simple propositions that are straightforward given the Wheel definition. These are designed to be auxillary and thus somewhat assorted and perhaps trivial, however mechanisation demands specification of what is typically deemed trivial.

Define the notation $\backslash_a := wDiv$ for brevity.

Proposition 2 (**Unit preserving**). *Given a Wheel W , then $\backslash_a 1 = 1$ where 1 is the neutral element of the multiplicative commutative monoid.*

Proposition 3.
Given a Wheel W and any two elements $a, b \in W$, then:

$$0a + 0b = 0ab$$

Proposition 4. *Given a Wheel W and any element $a \in W$, then:*

$$(0\backslash_a 0)a = 0\backslash_a 0$$

Proposition 5 (**Dividing by self**). *Given a Wheel W and any element $a \in W$, then:*

$$a\backslash_a a = 1 + 0(a\backslash_a a)$$

Proposition 6 (**Right cancellation**). *Given a Wheel W and any elements $a, b, c \in W$ such that $ac = bc$, then:*

$$a + 0c\backslash_a c = b + 0c\backslash_a c$$

Proposition 7 (**Monoid Automorphism**). *Given a Wheel W , $wDiv$ is a monoid automorphism for $(1, *)$.*

1.1.2 Unital interactions

This section examines how a Wheel W behaves when an element $x \in W$ happens to be a unit in the multiplicative monoid.

Proposition 8. *Given a Wheel W, and $x \in W$ a unit in the multiplicative monoid of W, then the unit and self Wheel division are related by:*

$$x^{-1} + 0\backslash_a x = \backslash_a x + 0x^{-1} \tag{1.1}$$

where $x^{-1} \in W$ is the associated two-sided multiplicative inverse of the unit x.

Proposition 9. *Given a Wheel W, and $x \in W$ a unit in the multiplicative monoid of W, then zero enjoys the following identity:*

$$0\backslash_a x + 0\backslash_a x^{-1} = 0 \tag{1.2}$$

where $x^{-1} \in W$ is the associated two-sided multiplicative inverse of the unit x.

Proposition 10. *Given a Wheel W, and $x \in W$ a unit in the multiplicative monoid of W, then:*

$$x^{-1} = \backslash_a x + 0x^{-1}\backslash_a x^{-1} \tag{1.3}$$

where $x^{-1} \in W$ is the associated two-sided multiplicative inverse of the unit x.

Proposition 11. *Given a Wheel W, and $x \in W$ a unit in the multiplicative monoid of W, then:*

$$\backslash_a x = x^{-1} + 0x\backslash_a x \tag{1.4}$$

where $x^{-1} \in W$ is the associated two-sided multiplicative inverse of the unit x.

1.1.3 The trivial wheel

Given some set β, if there exist two commutative monoids which can be defined on this set, assume one is taken with additive notation and the other with multiplicative. Then there exists a wheel for β : the trivial wheel containing the multiplicative unit.

Proposition 12. *Suppose there is a set β and there exist two commutative monoids which can be defined on this set, in additive and multiplicative notation. Then $\{1\}$ is a Wheel with wheel division being the identity map.*

If given a wheel W, one may ask if it is the trivial wheel. This may be answered by comparing any two values out of $0, 1, \backslash_a 0, 0\backslash_a 0$ as below:

Proposition 13. *If any two of the elements $0, 1, \backslash_a 0$ and $0\backslash_a 0$ are equal in a wheel W, then W is trivial.*

1.2 Algebraic structures

Given a wheel W, certain sub-sets form familiar structures.

1.2.1 Induced semiring

Consider the subset:

$$\mathcal{R}_W := \{w \in W | 0 * w = 0\}$$

then $\mathcal{R}$ turns out to be a commutative unital semiring.

Remark 1.2.1. *For the purposes of this document, we assume semirings to be unital and commutative by default.*

Firstly,

Definition 14 ($\mathcal{R}_W$ is a commutative magma in * and +). Given a wheel W, then $\mathcal{R}_W$ is a commutative magma in both the wheel operations.

This is primarily to address the 'closure' of the algebraic operations in the sub-set. To achieve a semi-ring, we further need two commutative monoids: one for each of the wheel operations. Having closure, what is left to prove is a neutral element and associativity.

Definition 15 ($\mathcal{R}_W$ is a commutative monoid in * and +). Given a wheel W, then $\mathcal{R}_W$ is a commutative monoid in both the wheel operations.

Finally, the interaction between the two monoids must be distributive, and the semiring has been defined:

Definition 16 ($\mathcal{R}_W$ is a semiring in * and +). Given a wheel W, then $\mathcal{R}_W$ is a semiring in * and +.

1.2.2 Induced commutative group

In this section, consider the subset of a wheel W:

$$\mathcal{S}_W := \{w \in W | 0 * w = 0 \wedge 0 * \backslash_a w = 0\},$$

note that $\mathcal{R}_W$ is a subset of this set. Once more, begining with the closure of the binary operation * inherited from the wheel:

Definition 17 (**$\mathcal{S}_W$ is a commutative magma in ***). Given a wheel W, then $\mathcal{S}_W$ is a commutative magma in the * wheel operation.

Followed by the commutative monoid:

Definition 18 (**$\mathcal{S}_W$ is a commutative monoid in ***). Given a wheel W, then $\mathcal{S}_W$ is a commutative monoid in the * wheel operation.

And finally, the induced commutative group,

Definition 19 (**$\mathcal{S}_W$ is a commutative group in ***). Given a wheel W, then $\mathcal{S}_W$ is a commutative group in *.

This shows that every element of $\mathcal{S}_W$ is $\backslash_a$-invertible. Furthermore, if an element of $\mathcal{R}_W$ is a $\backslash_a$-unit, then it is contained in $\mathcal{S}_W$:

Proposition 20. *For a wheel W, if $x \in \mathcal{R}_W$ is $\backslash_a$-invertible, then $x \in \mathcal{S}_W$.*

Proposition 21. *For a wheel W, if $x \in \mathcal{R}_W$ is a unit, then is is also a unit in the original wheel.*

1.2.3 Involution Monoid

An Involution is a monoid with a special involution operation , interacting in a particular way with the monoid operation.

Definition 22 (**Involution Monoid**). Given a monoid $(M, *)$, M is called an involution monoid for an involutive function $\star : M \to M$ which skew-distributes over $*$. In other words, $(M, *)$ is a monoid, with an associated map $\star : M \to M$ such that:

1. $\forall x \in M,\ x \star \star = x$

2. $\forall x, y \in M, (x * y)\star = y \star * x\star$.

This is denoted as $(M, *, \star)$ or simply $(M, \star)$ if $*$ is inferrable from surrounding context.

Several structures can be made into an involution monoid:

Proposition 23. *Any abelian group is an involution monoid with $x\star = x^{-1}$.*

Proposition 24. *Any field with decideable equality is an involution monoid with $x\star = x^{-1}$ for x non-zero and 0 otherwise.*

Proposition 25. *The monoid of $n \times n$ R-valued matrices form an involution monoid with $x\star = x^T$ and R a commutative ring.*

Furthermore the notion of a $\star$-unit is defined on an involution monoid as a regular monoid unit, except that the two-sided inverse must equal to the $\star$ operation.

Definition 26 (**$\star$-unit**). An element of an involution monoid $x \in (M, \star)$ is a $\star$-unit if $x^{-1} = x\star$.

Definition 27 (**$\star$-invertible**). An involution monoid $(M, \star)$ is $\star$-invertible if every unit is a $\star$-unit.

The morphisms that respect such structures are similarly defined:

Definition 28 (**Involution Monoid Homomorphism**). If there are two involution monoids, $(M_1, \star_1)$ and $(M_2, \star_2)$, a monoid homomorphism $f : M_1 \to M_2$ is an involution monoid homomorphism if $\forall x \in M_1, f(x\star_1) = f(x)\star_2$.

1.2.4 Commutative monoid to Involution monoid

It is possible, given a commutative monoid M, to construct an involution monoid contained within M. To begin with , an Involution monoid may be defined on $M \times M$, with $(x_1, x_2)\star = (x_2, x_1)$.

Definition 29. Given a commutative monoid M, there is an involution monoid on $M \times M$ with $(x_1, x_2)\star = (x_2, x_1)$, and the usual pointwise monoid operation taken from M.

Define an equivalence relation on $M \times M$:

Definition 30. $(x, y) \equiv (x', y')$ iff $\exists s_1, s_2 \in M, (s_1, s_1)(x, y) = (s_2, s_2)(x', y')$

The equivalence relation gives rise to the corresponding quotient space:

Definition 31. Denote the quotient space $M_X^* := M \times M/\equiv$.

1.2.5 Wheel Module

Definition 32. Let W be a wheel. A W-module, or WheelModule, is a commutative monoid $(M, 0, +)$ with multiplication by W-elements defined (formally, a function $(H \times M) \to M$ written $(x, m) \to x \bullet m$) such that for any $x, x' \in W$, $m, m' \in M$ the following hold:

1. $(xx') \bullet m = x \bullet (x' \bullet m)$

2. $1 \bullet m = m$

3. $(x + x') \bullet m + 0 \bullet m = x \bullet m + x' \bullet m$

4. $x \bullet (m + m') + x \bullet 0 = x \bullet m + x \bullet m'$

5. $(\backslash_a x) \bullet m + m' + x \bullet 0 = \backslash_a x \bullet (m + x \bullet m')$

6. $(\backslash_a x) \bullet m + m' + x \bullet 0 = \backslash_a x \bullet (m + x \bullet m')$

7. $x \bullet (m + 0 \bullet m') = x \bullet m + 0 \bullet m'$

8. $m + (\backslash_a 0) \bullet 0 = (\backslash_a 0) \bullet 0$

Chapter 2

References

[1] JESPER CARLSTRÖM. “Wheels – on division by zero”. In: Mathematical Structures in Computer Science 14.1 (2004), pp. 143–184. doi: 10.1017/S0960129503004110.