7.1: Introduction to Rings

Alex L.

November 4, 2024

1 Motivation

Introduce the concept of rings and fields, and provide definitions for terminology.

2 Content

Definition: (Rings) A **ring** R is a set with two binary operations, which we call: $+$ and $\times$ (additon and multiplication). The identity of $+$ will be 0, and the additive inverse of a will be $-a$. It also satisfies the following axioms:

1. Addition is commutative.

2. Multiplication is associative: $(a \times b) \times c = a \times (b \times c)$.

3. Forward and backward distribution holds: $a \times (b + c) = (a \times b) + (a \times c)$, and $(b + c) \times a = (b \times a) + (c \times a)$

Note that there doesn't need to be a multiplicative identity or multiplicative inverses for R to be a ring.

Proposition: If multiplication distributes over addition, then addition must be abelian.

Proof: Let's do a proof by contradiction, assume that addition isn't commutative when the distributive laws hold: Suppose we have the product

$$(1 + 1)(a + b)$$

where a and b are in R. We can distribute the right term into the left to get

$$1(a + b) + 1(a + b)$$

and this evaluates to

$$a + b + a + b$$

Now, lets evaluate again, this time distributing the left term into the right, to get

$$(1 + 1)a + (1 + 1)b$$

which turns into

$$a + a + b + b$$

By the distribution laws, these results must be equal, so we have

$$a + b + a + b = a + a + b + b$$

Then, by adding $-a$ to the left and $-b$ to the right, we get that $-a + a + b + a + b + -b = -a + a + a + b + b + -b$ which simplifies to

$$a + b = b + a$$

This is clearly a contradiction, so therefore, addition is commutative when the distributive laws hold.

Definition: (Special Types of Rings)

A ring is said to be **commutative** if multiplication is commutative.

A ring R is said to have an **identity** if there is a multiplicative identity, called 1, in R.

Definition: (Division Rings) If a ring R has a (multiplicative) identity 1, which is not equal to its additive identity 0, and each element a has a multiplicative inverse a^{-1}, then it is called a **division ring** or a **skew field**. If a division ring is also (multiplicatively) commutative, then it is called a **field**.

Example:

1. The simplest rings are trivial rings. Take $(R, +)$, the ring under only addition, to be any abelian group, and then define a multiplication operation such that $a \times b = 0$ for any a, b in R. In particular, if the abelian group we choose is the trivial group, then the ring is called a zero ring.

2. The integers $\mathbb{Z}$ under normal addition and multiplication is a ring, as the integers are a group under addition, and normal multiplication is associative and distributive. It is also (multiplicatively) commutative and has a (multiplicative) identity, 1.

3. The rational numbers, real numbers, and complex numbers under normal addition and multiplication are all rings. They are also commutative, have identities, and multiplicative inverses, so they are all fields as well.

4. The quotient group $\mathbb{Z}/n\mathbb{Z}$ under modular addition and multiplication is a ring with additive identity $\bar{0}$ (the equivalence class of 0), and multiplicative identity $\bar{1}$.

Theorem: Let $\mathbb{H}$, the Hamilton Quaternions, be the collection of all elements of the form $a + bi + cj + dk$, where a, b, c, d are real numbers. Define addition on $\mathbb{H}$ as: $(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$. Define multiplication on $\mathbb{H}$ using the distributive property, and simplify using the relations: $i^2 = j^2 = k^2 = -1$, and $ij = -ji = k$ and $jk = -kj = i$, and $ki = -ik = j$. Prove that $\mathbb{H}$ under the addition and multiplication defined above is a non-commutative ring with an identity. Prove that if we let the coefficients of the quaternions be real or rational, then $\mathbb{H}$ becomes a division ring.

Proof: Suppose that h_1, h_2, h_3 are in $\mathbb{H}$. In order to show that $\mathbb{H}$ is a ring, we need to show that $(\mathbb{H}, +)$ is an abelian group, and that our definition of multiplication on $\mathbb{H}$ is associative and distributes over addition.

Firstly, lets show that $(\mathbb{H}, +)$ is an abelian group. It is closed because

$$h_1 + h_2 = (a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

It has an identity, $0 = 0 + 0i + 0j + 0k$, and

$$0 + h_1 = (0 + a_1) + (0 + b_1)i + (0 + c_1)j + (0 + d_1)k = a_1 + b_1 i + c_1 j + d_1 k = (a_1 + 0) + (b_1 + 0)i + (c_1 + 0)j + (d_1 + 0)k = h_1 + 0 = h_1$$

It has inverses, $-h_1 = -a_1 + (-b_1)i + (-c_1)j + (-d_1)k$, as

$$h_1 + -h_1 = (a_1 - a_1) + (b_1 - b_1)i + (c_1 - c_1)j + (d_1 - d_1)k = 0 + 0i + 0j + 0k = 0$$

It is commutative, since

$$h_1 + h_2 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k = (a_2 + a_1) + (b_2 + b_1)i + (c_2 + c_1)j + (d_2 + d_1)k = h_2 + h_1$$

Therefore, $(\mathbb{H}, +)$ is an abelian group.

Secondly, we want to show that $h_1 \times (h_2 \times h_3) = (h_1 \times h_2) \times h_3$ to prove multiplicative associativity. Calculating the left hand side, we get

$$h_1 \times (h_2 \times h_3) = (a_1 + b_1 i + c_1 j + d_1 k) \times ((a_2 + b_2 i + c_2 j + d_2 k) \times (a_3 + b_3 i + c_3 j + d_3 k))$$

Expanding, we get $(a_1 + b_1 i + c_1 j + d_1 k) \times (a_2 a_3 + a_2 b_3 i + a_2 c_3 j + a_2 d_3 k + a_3 b_2 i - b_2 b_3 + b_2 c_3 k - b_2 d_3 j + a_3 c_2 j - c_2 b_3 k - c_2 c_3 + c_2 d_3 i + a_3 d_2 k + b_3 d_2 j - c_3 d_2 i - d_2 d_3)$, and expanding further, we get $a_1 a_2 a_3 - a_1 b_2 b_3 - a_1 c_2 c_3 - a_1 d_2 d_3 + a_1 a_2 b_3 i + a_1 a_3 b_2 i + a_1 c_2 d_3 i - a_1 c_3 d_2 i + a_1 a_2 c_3 j + a_1 a_3 c_2 j + a_1 b_3 d_2 j - a_1 b_2 d_3 j + a_1 a_2 d_3 k + a_1 b_2 c_3 k - a_1 c_3 d_2 i - a_1 c_2 b_3 k + b_1 a_2 a_3 i - b_1 b_2 b_3 i - b_1 c_2 c_3 i - b_1 d_2 d_3 i - b_1 a_2 b_3 - b_1 a_3 b_2 - b_1 c_2 d_3 + b_1 c_3 d_2 + b_1 a_2 c_3 k + b_1 a_3 c_2 k + b_1 b_3 d_2 k - b_2 d_3 b_1 k - b_1 a_2 d_3 j - b_2 c_3 b_1 j - $$

$b_1a_3d_2j + b_1c_2b_3j + c_1a_2a_3j - c_1b_2b_3j - c_1c_2c_3j - c_1d_2d_3j - c_1a_2b_3k - c_1a_3b_2k - c_1c_2d_3k + c_1c_3d_2k - c_1a_2c_3 - c_1a_3c_2 - c_1b_3d_3 + c_1b_2d_3 + c_1a_2d_3i + c_1b_2c_3i + c_1a_3d_2i - c_1c_2b_3i + d_1a_2a_3k - d_1b_2b_3k - d_1c_2c_3k - d_1d_2d_3k - d_1a_2b_3i + d_1a_3b_2j + d_1c_2d_3j - d_1c_3d_2j - d_1a_2c_3i - d_1a_3c_2i - d_1b_3d_2i + d_1b_2d_3i - d_1a_2d_30d_1b_2c_3 - d_1a_3d_2 + d_1c_2b_3$

For the right hand side, we have:

$$(h_1 \times h_2) \times h_3 = ((a_1 + b_1i + c_1j + d_1k) \times (a_2 + b_2i + c_2j + d_2k)) \times (a_3 + b_3i + c_3j + d_3k)$$

Expanding, we get $(a_1a_2 + a_2b_2i + a_1c_2j + a_2d_2k + a_2b_1i - b_1b_2 + b_1c_2k - b_1d_2k + a_2c_1k - b_2c_1k - c_1c_2 + c_1d_2i + a_2d_1k + b_2d_1j - c_2d_1i - d_1d_2) \times (a_3 + b_3i + c_3j + d_3k)$, and expanding further, we get $a_1a_2a_3 + a_1a_3b_2i + a_1a_3c_2j + a_1a_3d_2k + a_2a_3b_1i - a_2b_1b_2 + a_3b_1c_2k - a_3b_1d_2j + a_2a_3c_1j - a_2b_2c_1k - a_3c_1c_2 + a_3c_1d_2i + a_2a_3d_1k + a_3b_2d_1k - a_3c_2d_1i - a_3d_1d_2 + a_1a_2b_3i - a_1b_2b_3 - a_1b_3c_2k + a_1b_3d_2j - a_2b_1b_3 - b_1b_2b_3i + b_1b_3c_3j + b_1b_3d_2k - a_2b_3c_1k - b_2b_3c_1j - -b_3c_1c_2i - b_3c_1d_2 + a_2b_3d_1j - b_2b_3d_1k + b_3c_3d_1 - b_3d_1d_2i + a_2a_2c_3j + a_1b_2c_3k - a_1c_2c_3 - a_1c_3d_2i + a_2b_1c_3k - b_1b_2c_3j - b_1c_2c_3i + b_1c_3d_2 - a_2c_1c_3 + b_2c_1c_3 - c_1c_2c_3j + c_1c_3d_2k - a_2c_3d_1i - b_2c_3d_1 - c_2c_3d_1k - c_3d_1d_2j + a_1a_2d_3k - a_1b_2d_3j + a_1c_2d_3i - a_2d_2d_3 - a_2b_1d_3j - b_1b_2d_3k - b_1c_2d_3 - b_1d_2d_3i + a_2c_1d_3i + b_2c_1d_3 - c_1c_2d_3k - c_1d_2d_3j - a_2d_1d_3 + b_2d_1d_3i + c_2d_1d_3j - d_1d_2d_3k.$

Matching terms, we get that both sides are equal, and so therefore, our definition of mutliplication of Hamilton quaternions is associative.

Lastly, we want to confirm that multiplication is distributive over addition. Lets first confirm the left side of the left distribution: $h_1 \times (h_2 + h_3) = a_1a_2 + a_1a_3 + a_1b_2i + a_1b_3i + a_1c_2j + a_1c_3j + a_1d_2k + a_1d_3k + a_2b_1i + a_3b_1i - b_1b_2 - b_1b_3 + b_1c_2k + b_1c_3k - b_1d_2j - b_1d_3j + a_2c_1j + a_3c_1j - b_2c_1k - b_3c_1k - c_1c_2 - c_1c_3 + c_1d_2i + c_1d_3i + a_2d_1k + a_3d_1k + b_2d_1j + b_3d_1j - c_2d_1i - c_3d_1i - d_1d_2 - d_1d_3$

Now, lets confirm the right hand side of the left distribution: $(h_1 \times h_2) + (h_1 \times h_3) = a_1a_2 + a_1b_2i + a_1c_2j + a_1d_2k + a_2b_i - b_1b_2 + b_1c_2k - b_1d_2 + a_2c_1j - b_2c_1k - c_1c_2 + c_1d_2i + a_2d_1k + b_2d_1j - c_2d_1i - d_1d_2 + a_1a_3 + a_1b_3i + a_1c_3j + a_1d_3k + a_3b_1i - b_1b_3 + b_1c_3k - b_1d_3 + a_3c_1j - b_3c_1k - c_1c_3 + c_1d_3i + a_3d_1k + b_3d_1j - c_3d_1i - d_1d_3$

As we can see, they contain the same terms, so the equality holds.

Now, lets confirm the right distribution:

The left hand side becomes: $(h_1 + h_2) \times h_3 = a_1a_3 + a_2a_3 + a_3b_1i + a_3b_2i + a_3c_1j + a_3c_2j + a_3d_1k + a_3d_2k + a_3b_1i + a_3b_2i - b_1b_3 - b_2b_3 + b_1c_3k + b_2c_3k - b_1d_3j - b_2d_3j + a_3c_1j + a_3c_2j - b_3c_1k - b_3c_2k - c_1c_3 - c_2c_3 + c_1d_3i + c_2d_3i + a_3d_1k + a_3d_2k + b_3d_1jj + b_3d_2j - c_3d_1i - c_3d_2i - d_1d_3 - d_2d_3$

And the right side becomes: $(h_1 \times h_3) + (h_2 \times h_3) = a_1a_3 + a_1b_3i + a_1c_3j + a_1d_3k + a_3b_1i - b_1b_3 + b_1c_3k - b_1d_3j + a_3c_1j - b_3c_1k - c_1c_3 + c_1d_3i + a_3d_1k + b_3d_1j - d_1c_3i - d_1d_3 + a_2a_3 + a_2b_3i + a_3c_3j + a_3d_3k + a_3b_2i - b_2b_3 + b_2c_3k - b_2d_3j + a_3c_2j - b_3c_2k - c_3c_3 + c_2d_3i + a_3d_2k + b_3d_2j - d_2c_3i - d_2d_3$

They also have the same terms, so the equality holds.

Since we proved that $(\mathbb{H}, +)$ is an abelian group, and that multiplication is associative and distributive, we show that $\mathbb{H}$ is a ring.''