7.1: Introduction to Rings

Alex L.

December 14, 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, called "addition" and "multiplication", along with eight criteria:

1. $(R, +)$, the group formed by R under addition, is closed
2. $(R, +)$ has an identity called 0
3. $(R, +)$ is associative
4. All elements of $(R, +)$ have inverses
5. $(R, +)$ is commutative
6. $(R, \cdot)$, the ring under multiplication, is closed
7. $(R, \cdot)$ is associative
8. The distributive property holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

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. (criterion 8 implies criterion 5)

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 $\bar{1}$.
5. We can even have a ring of functions! Let X be a nonempty set and A be a ring, and let R be the set of all functions mapping X to A. Then, let f, g be members of R, and let x be a member of X. We can define addition of elements of R to be $(f+g)(x) = f(x)+g(x)$, and since $f(x)$ and $g(x)$ are members of A, they will commute under addition. Also, there will be an element x_I where $f(x_I) = 0_A$, the identity in A, by the definition of a mapping, there will be inverses, because there are additive inverses in A, and it is closed because $(A,+)$ is closed. If we also define multiplication by $(f \cdot g)(x) = f(x)g(x)$, then we also have multiplication which is associative and distributes over addition, as $f(x)$ and $g(x)$ are members of the ring A.
6. We can construct rings without multiplicative identities as well. Suppose we create a ring out of the even integers, $2\mathbb{Z}$, under addition and multiplication of integers. The identity for multiplication of integers, 1, is not in $2\mathbb{Z}$.

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: $(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k$. 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

$$h_1+h_2 = (a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k$$

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

$$0+h_1 = (0+a_1)+(0+b_1)i+(0+c_1)j+(0+d_1)k = a_1+b_1i+c_1j+d_1k = (a_1+0)+(b_1+0)i+(c_1+0)j+(d_1+0)k = h_1+0 = h_1$$

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 $a_1 a_2 a_3 - a_1 b_2 b_3 - a_1 c_2 c_3 - a_1 d_2 d_3 + a_1 a_2 b_3 i + a_1 a_3 b_2 i + a_1 c_2 d_3 i - a_1 c_3 d_2 i + a_1 a_2 c_3 j + a_1 a_3 c_2 j + a_1 b_3 d_2 j - a_1 b_2 d_3 j + a_1 a_2 d_3 k + a_1 b_2 c_3 k - a_1 c_3 d_2 i - a_1 c_2 b_3 k + b_1 a_2 a_3 i - b_1 b_2 b_3 i - b_1 c_2 c_3 i - b_1 d_2 d_3 i - b_1 a_2 b_3 - b_1 a_3 b_2 - b_1 c_2 d_3 + b_1 c_3 d_2 + b_1 a_2 c_3 k + b_1 a_3 c_2 k + b_1 b_3 d_2 k - b_2 d_3 b_1 k - b_1 a_2 d_3 j - b_2 c_3 b_1 j - b_1 a_3 d_2 j + b_1 c_2 b_3 j + c_1 a_2 a_3 j - c_1 b_2 b_3 j - c_1 c_2 c_3 j - c_1 d_2 d_3 j - c_1 a_2 b_3 k - c_1 a_3 b_2 k - c_1 c_2 d_3 k + c_1 c_3 d_2 k - c_1 a_2 c_3 - c_1 a_3 c_2 - c_1 b_3 d_3 + c_1 b_2 d_3 + c_1 a_2 d_3 i + c_1 b_2 c_3 i + c_1 a_3 d_2 i - c_1 c_2 b_3 i + d_1 a_2 a_3 k - d_1 b_2 b_3 k - d_1 c_2 c_3 k - d_1 d_2 d_3 k - d_1 a_2 b_3 i + d_1 a_3 b_2 j + d_1 c_2 d_3 j - d_1 c_3 d_2 j - d_1 a_2 c_3 i - d_1 a_3 c_2 i - d_1 b_3 d_2 i + d_1 b_2 d_3 i - d_1 a_2 d_3 0 d_1 b_2 c_3 - d_1 a_3 d_2 + d_1 c_2 b_3$

For the right hand side, we have:

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

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

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

Now, lets confirm the right hand side of the left distribution: $(h_1 \times h_2) + (h_1 \times h_3) = a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k + a_2 b_i - b_1 b_2 + b_1 c_2 k - b_1 d_2 + a_2 c_1 j - b_2 c_1 k - c_1 c_2 + c_1 d_2 i + a_2 d_1 k + b_2 d_1 j - c_2 d_1 i - d_1 d_2 + a_1 a_3 + a_1 b_3 i + a_1 c_3 j + a_1 d_3 k + a_3 b_1 i - b_1 b_3 + b_1 c_3 k - b_1 d_3 + a_3 c_1 j - b_3 c_1 k - c_1 c_3 + c_1 d_3 i + a_3 d_1 k + b_3 d_1 j - c_3 d_1 i - d_1 d_3$

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

Now, lets confirm the right distribution:

The left hand side becomes: $(h_1 + h_2) \times h_3 = a_1 a_3 + a_2 a_3 + a_3 b_1 i + a_3 b_2 i + a_3 c_1 j + a_3 c_2 j + a_3 d_1 k + a_3 d_2 k + a_3 b_1 i + a_3 b_2 i - b_1 b_3 - b_2 b_3 + b_1 c_3 k + b_2 c_3 k - b_1 d_3 j - b_2 d_3 j + a_3 c_1 j + a_3 c_2 j - b_3 c_1 k - b_3 c_2 k - c_1 c_3 - c_2 c_3 + c_1 d_3 i + c_2 d_3 i + a_3 d_1 k + a_3 d_2 k + b_3 d_1 j j + b_3 d_2 j - c_3 d_1 i - c_3 d_2 i - d_1 d_3 - d_2 d_3$

And the right side becomes: $(h_1 \times h_3) + (h_2 \times h_3) = a_1 a_3 + a_1 b_3 i + a_1 c_3 j + a_1 d_3 k + a_3 b_1 i - b_1 b_3 + b_1 c_3 k - b_1 d_3 j + a_3 c_1 j - b_3 c_1 k - c_1 c_3 + c_1 d_3 i + a_3 d_1 k + b_3 d_1 j - d_1 c_3 i - d_1 d_3 + a_2 a_3 + a_2 b_3 i + a_3 c_3 j + a_3 d_3 k + a_3 b_2 i - b_2 b_3 + b_2 c_3 k - b_2 d_3 j + a_3 c_2 j - b_3 c_2 k - c_3 c_3 + c_2 d_3 i + a_3 d_2 k + b_3 d_2 j - d_2 c_3 i - d_2 d_3$

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.

Proposition: Let R be a ring and let a and b be in R. Then:

1. $0a = a0 = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$
4. If R has a multiplicative identity 1, then it is unique and $-a = (-1)a$.

Proof:

1. If we expand zero to form $0a = (0 + 0)a$ and then distribute, we get $0a = 0a + 0a$. Then, if we subtract by $0a$ on both sides, we get that $0 = 0a$
2. If we have $(-a)b = -ab$, we can add ab on both sides to get $ab + (-a)b = 0$. Then, we can un-distribute to get $(a - a)b = 0$, so $0b = 0$, showing that the equality holds.
3. Likewise, if we have $(-a)(-b) = ab$, we can add $-ab$ to both sides to get $(-a)(-b) + (-ab) = 0$. Then, by un-distributing the b, we get that $(-a)(-b + b) = 0$, so $(-a)0 = 0$, so the equality holds.
4. Suppose R had two multiplicative identities, i and j. Then, $ia = a = ja$ so $ia - ja = 0$, so $(i - j)a = 0$, and this can only happen if $i - j = 0$, meaning $i = j$. For the second part, we have $-a = (-1)a$, and by adding a to both sides, we get $0 = (-1)a + a$. We know that $a = 1a$ by definition of multiplicative identity, so we substitute to get $0 = (-1)a + 1a$, then, by un-distributing, we get $0 = (-1 + 1)a$, so $0 = 0a$, which is a true statement, meaning our prior statement is true.

Definition: (Zero Divisors) Let R be a ring. If there exists a pair of nonzero elements a, b in R such that $ab = 0$, then a and b are **zero divisors**.

In particular, a is called a left zero divisor and b is called a right zero divisor.

Definition: (Units) Assume that R has an identity $1 \neq 0$. If there exists a pair of (not nessecarily unique) elements u and v in R such that $uv = vu = 1$, then these elements are called **units**. In other words, if an element has a multiplicative inverse, it is a unit.

The set of all units forms a group under multiplication, which we will call $R^\times$.

Theorem: A zero divisor can never be a unit and fields contain no zero divisors.

Proof: Suppose we have zero divisors $ab = 0$ and we say that a is actually also a unit to some element v such that $va = 1$. Then, $b = 1b = (va)b = v(ab) = v0 = 0$, but zero divisors must be nonzero elements, which gets us to a contradiction. Therefore, zero divisors can never be units.

Since every element in a field has a multiplicative inverse, that means that every element in a field is a unit, so fields can't have any zero divisors.

Definition: (Integral Domains) A commutative ring with $1 \neq 0$ is an integral domain if it has no zero divisors.

Proposition: If R is a ring and a, b, c are in R and a is not a zero divisors. Then, if $ab = ac$ then $a = 0$ or $b = c$.

Proof: Subtract ac from both sides to get $ab - ac = 0$. Then, un-distribute the a to get $a(b - c) = 0$. The only way this is true is if $a = 0$ or $b - c = 0$, and we can rearrange the latter to get $b = c$.

Corollary: Any finite integral domain is a field.

Proof: Suppose we have an integral domain R and a element a in R, and a map $x \to ax$. This mapping is injective because if two elements in the image, $ar_1 = ar_2$, then by the cancellation property, $r_1 = r_2$. It is also surjective since if you pick an element in the image, like ar_k, I can show you that the mapping takes r_k to ar_k. As such, this map is a bijection. Since the ring is closed, the image must be a copy of the original ring. As such, there will be a multiplicative identity 1 in the image, and therefore, $ab = 1$, so a is a unit. The catch is, a is arbitrary, so every element of R is a unit,

so R is a field.

Definition: (Subrings) A subring S of R is a ring that is a subset of the elements in R.

3 Exercises

1. Show that $(-1)^2 = 1$. **Proof:** $(-1)^2 = (-1)(-1) = (1)(1)$by the proposition that (-a)(-b) = ab = 1.
2. Prove that if u is a unit in R then so is $-u$. **Proof:** $ua = 1$ for some a in R. $(-u)(-a) = ua$ and $-a$ is in R because additive inverses are in R, so $(-u)(-a) = 1$ so $-u$ is a unit.
3. Let R be a ring with a (multiplicative) identity and let S be a subring of R containing the identity as well. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false. **Proof:** If u is a unit in S, then there is some element a such that $ua = 1$. Since S is a subring of R, then a is also in R, so $ua = 1$ in R as well. The opposite isn't nessecarily true because a might be in the ring but not in the subring.