# MA542 Lecture

Timothy Kohl

Boston University

January 24, 2025

# Other Ring Examples

We saw earlier the definition of the complex numbers:

$$\begin{aligned} \mathbb{C} &= \{a + b\ i \mid a, b \in \mathbb{R},\ i^2 = -1\} \\ (a+bi)+(c+di) &= (a+c)+(b+d)i \\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i \end{aligned}$$

and that $\mathbb{C}$ can also be viewed as a vector space in that every $z \in \mathbb{C}$ is of the form $z = a + bi = a \cdot 1 + b \cdot i$.

i.e. every element of $\mathbb{C}$ is a linear combination of $\{1, i\}$

This begs the question as to whether one could generalize this idea, and indeed there is, but there are some startling contrasts in comparison to $\mathbb{C}$.

The Quaternions (Hamiltonians) as a set is

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

namely linear combinations of $\{1, i, j, k\}$ (so that $\mathbb{H}$ is additively just like the vector space $\mathbb{R}^4$) but where the $i, j, k$ have the following properties:

$$\begin{aligned} &1 \cdot i = i,\ 1 \cdot j = j,\ 1 \cdot k = k \\ &i^2 = j^2 = k^2 = -1 \\ &ij = k,\ jk = i,\ ki = j \\ &ji = -k,\ kj = -i,\ ik = -j \end{aligned}$$

where a product $(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)$ is expanded out and simplified according to the rules governing 1, $i$, $j$, and $k$ as above.

One may (with some effort!) verify that $\mathbb{H}$ is a ring, with additive identity $0 + 0i + 0j + 0k$ and multiplicative identity $1 + 0i + 0j + 0k$.

The other properties (such as associativity) are messy to check, but do hold.

One of the principal observations is that $\mathbb{H}$ is a non-commutative ring, which stems of course from the rules governing how the 'basis' elements are multiplied.

The similarity to $\mathbb{C}$ is obvious in that $j$ and $k$ are two other 'square roots of $-1$' but what is also interesting is the following similarity with $\mathbb{C}$ which we'll discuss in more generality later.

If $z = a + bi \in \mathbb{C}$ where $(a, b) \neq (0, 0)$ (i.e. not the zero element of $\mathbb{C}$) then we have

$$\begin{aligned}\frac{1}{a+bi} &= \frac{1}{a+bi}\frac{a-bi}{a-bi}\\ &= \frac{a-bi}{a^2+b^2}\\ &= \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\end{aligned}$$

where (since $a, b \in \mathbb{R}$ are not both zero) we have that $a^2 + b^2 > 0$ and so

$$\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i \in \mathbb{C}$$

which means every non-zero element of $\mathbb{C}$ has a multiplicative inverse, which makes $\mathbb{C}$ into what we call a *field*.

In a similar way although requiring a bit more work :-),one may show that every non-zero $h = a + bi + cj + dk \in \mathbb{H}$ has a multiplicative inverse as well.

However, as $\mathbb{H}$ is non-commutative, we use the term division ring to characterize $\mathbb{H}$.

We'll talk more about fields later on.

## Definition

If $R_1, R_2 \ldots R_n$ are rings then we define the direct product

$$R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}$$

namely the set of $n$-tuples of elements with each component coming from the different rings, and where

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

and the operations in the $i$-th component are computed with respect to $(R_i, +_i, \cdot_i)$ (i.e. that ring's addition and multiplication)

Note, the zero element is $(0_1, 0_2, \ldots, 0_n)$ where $0_i$ is the zero element of $R_i$.

For small examples, we can list out the elements in the direct product, e.g.

Let $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$ then

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

where it's obviously the case that the $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_3| = 2 \cdot 3 = 6$.

Note: In some circumstances, such as when each ring is commutative we write

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

in place of $R_1 \times R_2 \times \cdots \times R_n$.

For now, don't worry about that distinction.

Just as one does when first encountering the axioms for a group, there are some fundamental properties of rings which can be derived solely from the axioms.

In particular, they don't depend on thinking of some particular example of a ring.

Recall for a group $(G, *)$ how one proves the uniqueness of the identity.

If there were *two* identity elements $e$ and $e'$ then $e * e' = e'$ because $e$ is an identity, but also $e * e' = e$ since $e'$ is an identity and so $e = e'$.

# Properties of Rings

Let $R$ be a ring, and let $a, b, c \in R$.

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = ab$
4. If we define $b - c$ to mean $b + (-c)$ then $a \cdot (b - c) = a \cdot b - a \cdot c$ and $(b - c) \cdot a = (b \cdot a - c \cdot a)$. If $R$ has unity 1 then
5. $(-1) \cdot a = -a$
6. $(-1) \cdot (-1) = 1$

Let's examine some of these.

FACT 1: $a \cdot 0 = 0$ and $0 \cdot a = 0$
PROOF: Consider $a \cdot (0+0) = a \cdot 0 + a \cdot 0$ by the distributive law, but since 0 is the additive identity, $0 + 0 = 0$ so we have

$$a \cdot 0 = a \cdot 0 + a \cdot 0$$

and if $-a \cdot 0$ is the additive inverse of $a \cdot 0$ (which exists) then

$$\begin{gathered} a \cdot 0 = a \cdot 0 + a \cdot 0 \\ \downarrow \\ a \cdot 0 + (-a \cdot 0) = a \cdot 0 + a \cdot 0 + (-a \cdot 0) \\ \downarrow \\ 0 = a \cdot 0 + 0 \\ \downarrow \\ 0 = a \cdot 0 \qquad \square \end{gathered}$$

FACT 3 $(-a) \cdot (-b) = ab$
Going forward, let's drop the '$\cdot$' for multiplication unless we need it!

PROOF: Consider $(-a + a)(-b)$ which equals $0(-b)$ which is 0 by FACT 1.
However it also equals $(-a)(-b) + a(-b)$ but by FACT 2, $a(-b) = -(ab)$ so we have

$$\begin{array}{c} (-a)(-b) + (-(ab)) = 0 \\ \downarrow \\ (-a)(-b) = ab \end{array}$$

The other facts are left for exercises.