HOW CAN IT BE THAT MATHEMATICS, BEING AFTER ALL A PRODUCT OF HUMAN THOUGHT WHICH IS INDEPENDENT OF EXPERIENCE, IS SO ADMIRABLY APPROPRIATE TO THE OBJECTS OF REALITY?

ALBERT EINSTEIN

"AND WHAT IS THE USE OF A BOOK," THOUGHT ALICE, "WITHOUT PICTURES OR CONVERSATIONS?"

LEWIS CARROLL (*ALICE IN WONDERLAND*)

. . . THE DESIGNER OF A NEW SYSTEM MUST NOT ONLY BE THE IMPLEMENTOR AND THE FIRST LARGE-SCALE USER; THE DESIGNER SHOULD ALSO WRITE THE FIRST USER MANUAL. . . IF I HAD NOT PARTICIPATED FULLY IN ALL THESE ACTIVITIES, LITERALLY HUNDREDS OF IMPROVEMENTS WOULD NEVER HAVE BEEN MADE, BECAUSE I WOULD NEVER HAVE THOUGHT OF THEM OR PERCEIVED WHY THEY WERE IMPORTANT.

DONALD E. KNUTH

QUANTUM COMMUNICATION

Contents

Building the Mathematical Foundation

Contents

The overall goal of this chapter is to build our way up to vector spaces. Vector spaces are the mathematical structure that underpins quantum mechanics and, by extension, quantum communication. After the development of vector spaces, we briefly discuss some additional mathematical topics that are useful in quantum communication.

Group Theory

To begin our adventure towards vector spaces, we start with, what I consider, the most fundamental mathematical structure: groups. Groups are *sets*[1] equipped with an *operation* that satisfies four axioms. Groups are ubiquitous in mathematics and physics, and they have

[1] Briefly, a **set** is a collection of well-defined, distinct objects.

applications in many fields, including cryptography, coding theory, and particle physics.

Operations

On any nonempty set A, an operation is a mapping from two elements in A onto some other, not necessarily unique, element in A. More formally,

Definition 1 (Operation)**.** A **binary operation** on a nonempty set A (simply, an **operation** on a set A), is a function $f : A \times A \to A$.

By this definition, A is closed under the operation defined by f.

We can familiarize ourselves with Defn. 1 by considering standard multiplication, denoted here by $(\cdot)$. Limiting ourself to the integers, $\mathbb{Z}$, we define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as $f(a, b) = a \cdot b$. One may repeat this process with integer addition $(+)$, defining $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as $f(a, b) = a + b$. As a last example, suppose $\vec{\mathbf{a}}$ and $\vec{\mathbf{b}}$ are vectors in $\mathbb{R}^3$. One way to define multiplication is the *vector product*, denoted $(\times)$, the mapping from two vectors to another vector, *i.e.*, $f : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f\left(\vec{\mathbf{a}}, \vec{\mathbf{b}}\right) = \vec{\mathbf{a}} \times \vec{\mathbf{b}}$.

Later in the text we will drop the mapping label of f and simply use, *e.g.*, $(a, b) = \square$, where $\square$ is to be filled.

Question 2. *Given Defn. 1, why would we not consider the scalar product of vectors to be a binary operation?*

Groups

Consider the set of integers equipped with addition, often denoted $(\mathbb{Z}, +)$. From our past experience, we can list a couple of facts about this set:

1. the sum of two integers is still an integer, and
2. the order in which we add integers does not affect the outcome.

In symbols, the first fact is written as $\forall\ a, b \in \mathbb{Z}, a + b \in \mathbb{Z}$. This is known as as the *closure* property. Similarly, the second fact is written as $\forall\ a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$. This is known as *associativity*.

These two facts are things we have taken for granted since elementary school. If we now consider the integer 0, we can add two more facts to our list:

3. the sum of any integer and 0 is simply that integer, *i.e.*, $\forall\ a \in \mathbb{Z}$, $a + 0 = a = 0 + a$, and
4. there exists a *negative* for each integer such that the sum of an integer and its negative is 0, *i.e.*, $\forall\ a \in \mathbb{Z}$, $a + (-a) = 0 = (-a) + a$.

Mathematicians refer to any element for which property 3 holds as the *additive identity* (or the *identity element* in general) and $-a$ is known as the *additive inverse* of a.

Stripping the addition operator from the set and replacing it with the multiplication operator, we now have $(\mathbb{Z}, \cdot)$. We have enough experience to know that the first two facts still hold, *i.e.*, the product of two integers is still an integer and multiplication of integers is associative. However, the identity element in this case would be the integer 1 since, $\forall\, a \in \mathbb{Z}$, $a \cdot 1 = a = 1 \cdot a$. We encounter an issue when trying to satisfy criterion 4 from above. $\forall a \in \mathbb{Z}$, we seek an integer a^{-1} s.t. $a \cdot a^{-1} = 1 = a^{-1}a$. In the special case of $a = 1$, we simply choose $a^{-1} = 1$ and we satisfy the criterion. However, for $a = 2$, we would need to choose $a^{-1} = \frac{1}{2}$, not an integer! Thus, we cannot satisfy criterion 4 for all integers in $\mathbb{Z}$.

The fact that the *set* $(\mathbb{Z}, +)$ carries this additional property makes it *special*. When abstracting the four properties discussed above, we arrive at the following definition for the first mathematical structure we will study:

Definition 3 (Group)**.** A **group** is a nonempty set G equipped with a binary operation $(*)$ that satisfies the following axioms: $\forall\, a, b, c \in G$,

1. $a * b \in G$ (Closure)
2. $a * (b * c) = (a * b) * c$, (Associativity)
3. $\exists\, e \in G$ s.t. $a * e = a = e * a$, (Identity)
4. $\forall\, a \in G$, $\exists\, a^{-1} \in G$ s.t. $a * a^{-1} = e = a^{-1} * a$. (Inverse)

By this definition, the integers equipped with addition form a group. Note that in the previous definition we explicitly stated the closure property as an axiom even though this is already part of the definition of an operation.

Unlike the integers, the set of rational numbers excluding zero, denoted $\mathbb{Q} \setminus \{0\}$, do form a group when equipped with multiplication. To see this, consider generic $a, b, c, d \in \mathbb{Z}$ with $b \neq 0$ and $d \neq 0$. Then the values $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ (we assume the fractions here are in simplest form but this need not be true for what follows). Clearly, the product of these two values is still rational: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$.[2] Associative multiplication in $\mathbb{Q}$ follows from the fact that multiplication of integers is associative. The identity element is the rational number 1 since $\frac{a}{b} \cdot 1 = \frac{a}{b} = 1 \cdot \frac{a}{b}$. Finally, every rational number except zero has a multiplicative inverse, namely its *reciprocal*, *e.g.* $\frac{b}{a}$, s.t. $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$. Thus, by Defn. 3, $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group. It can also be shown that $\mathbb{R} \setminus \{0\}$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ are all groups under multiplication.

[2] The set of rational numbers requires that the denominator be nonzero. From previous experience, we know that the product of two nonzero integers is also nonzero. This property is consequential of the set of integers, $\mathbb{Z}$, being an integral domain. This is a topic we cover in the following section.

We take a slight detour in our development of vector spaces to introduce an interesting application of groups in geometry. We start with the following definition:

Definition 4 (Symmetry group)**.** The **symmetry group** G of a mathematical object O is the set of all transformations that preserve the object's structure.

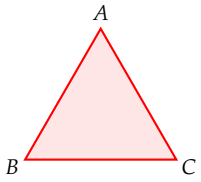

Figure 1: An equilateral triangle $\triangle ABC$. Note that the labels on the triangle's vertices are simply for us to visualize how the triangle is transformed. The labels do not imply that the triangle is oriented in any particular way.

For example, the symmetry group of an equilateral triangle $\triangle ABC$ (see Fig. 1) is the set of all transformations that preserve the triangle's shape, size, and *general* orientation. To build this group, we consider the following transformations:

1. Rotations: The triangle can be rotated (counterclockwise around its center) by 0°, 120°, or 240°. Assigning names to each of these transformations, we define $\{e, r, r^2\}$, where e is the identity transformation (no rotation), r is the 120° rotation, and r^2 is the 240° rotation. We see each of these transformations in action below:

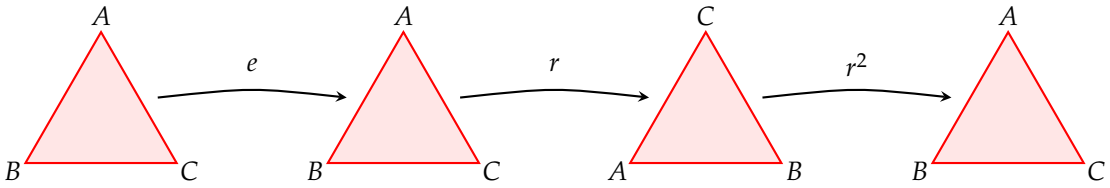

Figure 2: We see that the identity transformation e leaves the triangle unchanged, while the transformations r and r^2 rotate the triangle by 120° and 240° respectively. As one would expect, applying the r and r^2 rotations consecutively to the original triangle yields the original triangle again.

2. Reflections: Other than rotations around the centroid, we can also reflect the triangle about its axes of symmetry. We note that the equilateral triangle has three axes of symmetry, each passing through one vertex and the midpoint of the opposite side. We can label these reflections as x, h, and v (see Fig. 4). We thus expand our set of transformations to $\{e, r, r^2, x, h, v\}$.

   Applying these new transformations to the original triangle in Fig. 1, we arrive at the results seen in the following figure:

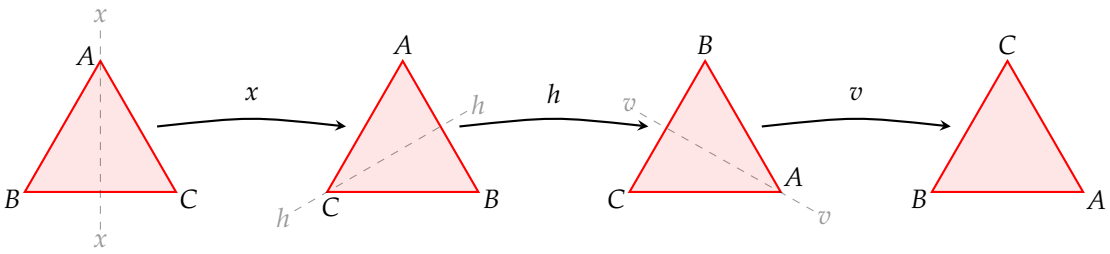

Figure 3: The axis of symmetry is shown (faintly) prior to reflection. Note that the final triangle here is not one that can be achieved via rotations alone. That is, applying x, h, and v consecutively is equivalent to simply applying the h transformation to the original triangle.

As seen in the previous figures, the transformations $\{e, r, r^2, x, h, v\}$ can be combined (*i.e.*, applied one after the other) to produce other, single transformations.

Now, if we think of a transformation as a function from the triangle onto itself, then the idea of combining transformations is equivalent to the composition of functions. In Fig. 3 (x followed by h and then followed by v), we can write $v \circ h \circ x$ (*i.e.*, first apply the x transformation, then the h, and finally the v) $= h$. In Fig. 2, we also saw that $r^2 \circ r = e$. Naming the set of transformations $D_3 \equiv \{e, r, r^2, x, h, v\}$[3] and equipping it with the composition operation, one can verify the Cayley table in Tab. 1.

Tab. 1 tells us that D_3 is closed under the composition operation, $(\circ)$, and composition of functions is known to be associative. Additionally, we've defined e as the identity element in this set and every element in D_3 has an inverse. For example, the inverse of r is r^2 since $r \circ r^2 = e = r^2 \circ r$. Similarly, the inverse of x is itself, *i.e.*, $x \circ x = e = x \circ x$. The same holds for h and v. Thus, we have shown that the set of transformations D_3 satisfies all four axioms in Defn. 3 and is therefore a group. In particular, it known as the **dihedral group** D_3, with the subscript of 3 indicating that our shape has 3 sides.

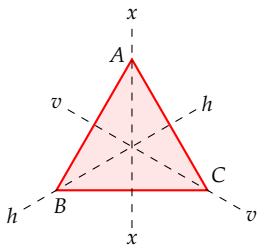

Figure 4: Showing all of the axes of rotation on the equilateral triangle $\triangle ABC$.

[3] We reserve the symbol $\equiv$ to denote a definition. This is different from the symbol $\square \equiv \square \pmod{\square}$ used to denote congruence, which we will see in the next section.

$\circ$	e	r	r^2	x	h	v
e	e	r	r^2	x	h	v
r	r	r^2	e	v	x	h
r^2	r^2	e	r	h	v	x
x	x	h	v	e	r	r^2
h	h	v	x	r^2	e	r
v	v	x	h	r	r^2	e

Table 1: The composition table for the symmetry group D_3 of the equilateral triangle. The way to read this table is as follows: the element in column i and row j is the result of applying the transformation i first and then the transformation j, *i.e.*, $j \circ i$. For example, the element in column r and row h is v, meaning that $h \circ r = v$.

In going through the above example, one may have noticed something rather peculiar about Tab. 1. Particularly, the fact the 3×3 block in the upper left corner is symmetric about the main diagonal, but no other 3×3 block in the table is symmetric. This symmetry tells us that, when applying rotations, the order in which we apply them does not matter. In other words, $r \circ r^2 = r^2 \circ r$, etc. This is not true for the reflections, however. For instance, $x \circ h \neq h \circ x$.

Groups that satisfy this additional property, the property of *commutativity*: $a * b = b * a$ for all $a, b \in G$, are called *abelian* groups. The name is derived from the mathematician Niels Henrik Abel, who made significant contributions to mathematics in the 19th century.

Definition 5 (Abelian group). A group is **abelian** if, $\forall\ a, b \in G$, it also satisfies the axiom

5. $a * b = b * a$. (Commutativity)

From what we mentioned in the previous paragraph, we see that the symmetry group D_3 is not abelian. However, the (proper) subgroup[4] of rotations, $\{e, r, r^2\}$, is abelian.

We can now return to the list at the start of this subsection and

[4] A nonempty subset H of a group G is a **subgroup** provided that it is closed and their exists an inverse for every element in the subgroup. This is true of the subset $\{e, r, r^2\}$ of D_3. We use the word 'proper' to say that the subgroup is not equal to the whole group D_3.

append this additional property:

5. the addition of integers is independent of the order of the integers (*i.e.*, it is *commutative*: $\forall\ a, b \in \mathbb{Z},\ a + b = b + a$),

stating that $(\mathbb{Z}, +)$ is an abelian group. By extension of the properties of $\mathbb{Z}$, $(\mathbb{Q}, +)$ is also an abelian group. Thus, it then follows that $(\mathbb{Z}, +)$ is a proper subgroup of $(\mathbb{Q}, +)$.

Further Resources

1. *Abstract Algebra: An Introduction* (3rd ed.) by Thomas W. Hungerford.

   This an excellent text that covers the basics of abstract algebra, including groups, rings, and fields. It is well-structured and provides a solid foundation for further study of algebra. I generally recommend the entire text but the chapter relevant to this section is chapter 7. Do note that Hungerford's development starts with rings and then moves on to groups, which is the opposite of how we are developing the material here.

2. *Abstract Algebra and Concrete* (ed. 2.6) by Frederick M. Goodman.

   This is, in my opinion, one of the best introductory texts on abstract algebra. It's also *free*.[5] The content that has the most relevance to this section is in chapter 1. In particular, sections 1.1-1.4, which generously covers symmetries, and section 1.10, which starts going over groups. Note that Goodman relies on congruence classes by section 1.10, so I would recommend holding off on this section until we cover congruence classes in the next section.

   [5] See page ix of the text for its cost.

3. *A Crash Course on Group Theory* by Peter J. Cameron.

   This is one of Cameron's several (*free*) texts on group theory and abstract algebra. All of chapter 1 is relevant to this section, but I would recommend at least reading sections 1.1 and 1.2.

4. *Elements of Abstract and Linear Algebra* by Edwin H. Connell.

   Like we do in this text, Connell starts with groups and then moves on to rings and linear algebra. Chapter 2 in Connell's text is dedicated to groups and, though it looks a bit intimidating at first, it is actually quite approachable. Pages 21-25 cover material similar to what we've shown here. Connell's text is also *free*.

Ring Theory

Rings are a natural extension of groups. Rings are sets equipped with two binary operations that generalize the arithmetic operations of addition and multiplication. Before we define rings formally, we first intrpoduce the concepts of *congruence* and *modular arithmetic*. These will not only be useful in our development of ring theory, but also in understanding the structure of rings themselves.

Congruence and Modular Arithmetic

Consider $a, b, c \in \mathbb{Z}$ with $c > 0$. We say ***a* is congruent to *b* modulo *c*** if c divides the difference of a and b. In symbols, $a \equiv b (\mathrm{mod}\, n)$ if $c|(a-b)$.[6] For example, $15 \equiv 6 (\mathrm{mod}\, 3)$ since 3 divides $15 - 6 = 9$. Additionally, $23 \equiv -1 (\mathrm{mod}\, 6)$ since 6 divides $23 - (-1) = 24$.

Now, let $a, c \in \mathbb{Z}$ with $c > 0$. The **congruence class of *a* modulo *c***, denoted $[a]$, is the set of all integers congruent to a modulo c, *i.e.*,

$$[a] = \{n : n \in Z \text{ and } n \equiv a (\mathrm{mod}\, c)\}. \tag{1}$$

For example, in congruence modulo 7, $[5] = \{\ldots, -9, -2, 5, 12, 19, \ldots\}$.[7] Restructuring this, equivalently $[5] = \{5, 5 \pm 7, 5 \pm 14, \ldots\}$. Thus, Eqn. (1) can be expressed instead as follows

$$[a] = \{a + kc : k \in Z\}, \tag{2}$$

a more digestible version.

Compactly, the set of all congruence classes modulo n is denoted $\mathbb{Z}_n$, read "$\mathbb{Z}$ mod n."[8] One may anticipate an issue in terms of representatives of these classes. For example, since $4 \equiv 7 (\mathrm{mod}\, 3)$, $4 \equiv 16 (\mathrm{mod}\, 3)$, and $4 \equiv -2 (\mathrm{mod}\, 3)$, it can be argued that $[4] = [7] = [16] = [-2]$ should all be in $\mathbb{Z}_3$. However, since they are all equivalent by Eqn. (2), actually **none** of them will be in $\mathbb{Z}_3$. We avoid this redundancy by only including classes where the representative is less than the value of n. For example, $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Every integer (class) can then be mapped onto (to) a class within $\mathbb{Z}_3$.

Finally, addition and multiplication in $\mathbb{Z}_n$ are defined by $[a] \oplus [b] = [a + b]$ and $[a] \odot [b] = [ab]$, respectively. Tables 2 and 3 show the addition and multiplication Cayley tables for all elements of $\mathbb{Z}_3$. Note that, *e.g.*, in Table 2 $[2] \oplus [2] = [1]$, replacing $[4]$.

A further study can be done at this point and it is strongly encouraged that the reader explore congruence and modular arithmetic more deeply. However, for our purposes, this introduction suffices.

[6] When expressing congruence, the symbol '$\equiv$' must accompanied by '$(\mathrm{mod}\, n)$' in order for it to actually *mean* anything. Without this, the same symbol of '$\equiv$' is used for definitions.

[7] We must emphasize what the congruence class is with respect to since, notice, [5] by itself is insufficient information.
One may also arrive at Eqn. (2) by the definition of congruence in the previous paragraph. We know that $n \equiv a (\mathrm{mod}\, c) \implies c|(n-a)$, which means $\exists\, k \in Z$ s.t. $n - a = kc$, hence $n = a + kc$.

[8] It is important to emphasize that this is a set of congruence classes, not integers. Each class itself is a set of integers, as seen in the previous paragraph.

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Table 2: Addition table for elements of $\mathbb{Z}_3$.

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Table 3: Multiplication table for elements of $\mathbb{Z}_3$.

Question 6. *Make the Cayley tables for addition and multiplication in $\mathbb{Z}_4$. What do you notice about the column/row of* [2] *under addition?*

Rings

Like groups, rings are best motivated by the generalization of properties of arithmetic in $\mathbb{Z}$ and $\mathbb{Z}_n$. Recall that in the Groups subsection we found that $(\mathbb{Z}, +)$ is an abelian group. Adding on to the 5 properties of abelian groups, we can list the following properties of the integers equipped with multiplication:

6. multiplication is closed, *i.e.*, the product of integers remains an integer;
7. multiplication is associative, *i.e.*, the *order in which we multiply* does not change the outcome;
8. the distributive properties hold;
9. multiplication is commutative, *i.e.*, the *order of the integers* being multiplied does not change the outcome;
10. a multiplicative identity exists, namely the integer 1, which can be multiplied to every integer without altering their value; and lastly
11. if the product of two integers is zero, then at least one of the original integers was itself zero.

Question 7. *Using Tables 2 and 3, verify that all of these properties hold for $\mathbb{Z}_3$.*

Question 8. *Do properties 6-11 hold for $\mathbb{Z}_n$, for any value of n? In particular, does property 11 hold for $\mathbb{Z}_4$? What about, $\mathbb{Z}_5$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$? If you start to think the trend is parity-dependent, consider $\mathbb{Z}_2$. What must be true of n for properties 6-11 to hold for $\mathbb{Z}_n$?*

The last property in the list above is not something we often explore in elementary mathematics, maybe because it's trivial in the integers. This triviality will vanish as we move to more abstract settings. We begin the abstraction of these common properties with the following definition:

Definition 9 (Ring)**.** A **ring** is an additive abelian group R equipped with multiplication, $(\cdot)$, s.t. $\forall\, a, b, c \in R$

6. $a \cdot b \in R$, (Closure under multiplication)
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, (Associative multiplication)
8. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. (Distributive properties)

Because a ring is equipped with both addition and multiplication, we introduce the *distributive properties* to relate the two operations. These properties are axioms that must be satisfied in order for a set with two binary operations to be considered a ring.

We use the symbol 0_R to denote the additive identity in a ring R. As of now, rings lack a multiplicative identity, denoted 1_R, and the existence of inverses for multiplication for them to form a group under multiplication as well. However, notice that rings introduce the distributive properties, which are not present in groups.

Rings which carry additional properties to the eight in Defn. 9 are given a different name. For example, a ring whose elements

commute under multiplication is given a different name, though not as special as a commutative group:

Definition 10 (Commutative ring)**.** A ring R is a **commutative ring** if it satisfies the following axiom: $\forall\ a, b \in R$,

9. $ab = ba$. (Commutative multiplication)

If a ring forms both an additive abelian group and a multiplicative abelian group, we call it the following:

Definition 11 (Ring with identity)**.** A ring R which contains an element, say 1_R, satisfying the following axiom: $\forall\ a \in R$,

10. $a1_R = a = 1_R a$, (Multiplicative identity)

is a **ring with identity**.

Example 12. The set of integers $\mathbb{Z}$ equipped with the usual addition and multiplication operations, $(\mathbb{Z}, +, \cdot)$, is a commutative ring with identity. It satisfies all 10 properties listed in Defns. 9 through 11.

Example 13. Let E be the set of even integers. We claim that $(E, +, \cdot)$ is a commutative ring, but not a ring with identity. To see this, we verify that it satisfies properties 1-9 in Defns. 9 and 10.

1. If $a \in E$ and $b \in E$, then $a + b \in E$ since the sum of two even integers is even. That is, $a + b = 2m + 2n = 2(m + n)$ for some $m, n \in \mathbb{Z}$.
2. By the associativity of addition in $\mathbb{Z}$, $a + (b + c) = (a + b) + c$.
3. The additive identity in E is 0 since $\forall\ a \in E$, $a + 0 = a$. 0 is even since $0 = 2 \cdot 0$.
4. For any $a \in E$, the additive inverse is $-a$ since $a + (-a) = 0$. Note that $-a$ is even since $a = 2k$ for some $k \in \mathbb{Z} \implies -a = -2k = 2(-k)$.
5. By the commutativity of addition in $\mathbb{Z}$, $a + b = b + a$.

6. If $a \in E$ and $b \in E$, then $ab \in E$ since the product of two even integers is even. That is, $ab = (2m)(2n) = 2(2mn)$ for some $m, n \in \mathbb{Z}$.
7. By the associativity of multiplication in $\mathbb{Z}$, $a(bc) = (ab)c$.
8. By the distributive properties in $\mathbb{Z}$, $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.
9. By the commutativity of multiplication in $\mathbb{Z}$, $ab = ba$.

There is no multiplicative identity in E since $1 \notin E$. Thus, $(E, +, \cdot)$ is not a ring with identity.

Question 14. *Verify that the set of odd integers with the usual addition and multiplication is not a ring.*

Example 15. Consider the set of congruence class modulo n in $\mathbb{Z}$, $\mathbb{Z}_n$. We seek to show that $(\mathbb{Z}_n, \oplus, \odot)$ is a commutative ring with identity. To do so, we must verify that it satisfies all 10 properties listed in Defns. 9 through 11.

1. If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \oplus [b] = [a+b] \in \mathbb{Z}_n$ by definition of addition in $\mathbb{Z}_n$.
2. By the definition of addition in $\mathbb{Z}_n$, $[a] \oplus ([b] \oplus [c]) = [a] \oplus [b+c] = [a + (b+c)] = [(a+b) + c] = [a+b] \oplus [c] = ([a] \oplus [b]) \oplus [c]$.
3. The additive identity in $\mathbb{Z}_n$ is $[0]$ since $\forall\ [a] \in \mathbb{Z}_n$, $[a] \oplus [0] = [a+0] = [a]$.
4. For any $[a] \in \mathbb{Z}_n$, the additive inverse is $[-a]$ since $[a] \oplus [-a] = [a + (-a)] = [a - a] = [0]$.
5. By definition of addition in $\mathbb{Z}_n$, $[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$.
6. If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \odot [b] = [ab] \in \mathbb{Z}_n$ by definition of multiplication in $\mathbb{Z}_n$.
7. By the definition of multiplication in $\mathbb{Z}_n$, $[a] \odot ([b] \odot [c]) = [a] \odot [bc] = [a(bc)] = [(ab)c] = [ab] \odot [c] = ([a] \odot [b]) \odot [c]$.
8. By the definition of addition and multiplication in $\mathbb{Z}_n$, $[a] \odot ([b] \oplus [c]) = [a] \odot [b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] = ([a] \odot [b]) \oplus ([a] \odot [c])$. Similarly, $([a] \oplus [b]) \odot [c] = [ac] \oplus [bc]$.
9. By the definition of multiplication in $\mathbb{Z}_n$, $[a] \odot [b] = [ab] = [ba] = [b] \odot [a]$.

10. The multiplicative identity in $\mathbb{Z}_n$ is $[1]$ since $\forall\ [a] \in \mathbb{Z}_n$, $[a] \odot [1] = [a \cdot 1] = [a]$.

As an interesting note, suppose n is not prime. Then, there exists $a, b \in \mathbb{Z}$ s.t. $1 < a < n$, $1 < b < n$, and $ab = n$. Thus, in $\mathbb{Z}_n$, $[a] \odot [b] = [ab] = [n] = [0]$, even though neither $[a]$ nor $[b]$ is equal to $[0]$. Therefore, when n is not prime, $\mathbb{Z}_n$ contains what we call **zero divisors**, elements x and y such that $x \neq 0_R$, $y \neq 0_R$, but $xy = 0_R$. This property will be important later on when we study fields.

The study of rings often involves studying polynomials with coefficients in a given ring. For example, one may study polynomials with integer coefficients. However, this is not something useful for our current development. As an alternative, we instead consider matrices.

Matrices

For the time being, we will not formally define matrices. Instead, we will provide an informal, very boring definition of what a matrix is, followed by some examples of matrix operations. A more formal definition will be provided later in the text when we study vector spaces.

Definition 16 (Matrix)**.** Let m and n be positive integers. An m-by-n **matrix A** is a rectagular array of elements arranged in m rows and n columns, denoted

$$\mathbf{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

The notation a_{ij} denotes the element in the i-th row and the j-th column of $\mathbf{A}$. In other words, the first index refers to the row and the second index refers to the column.

Notice that the definition says nothing about what the elements a_{ij} are. In theory, they can be elements from any set, it simply depends on what you want to achieve with the matrices. For our purposes, we will consider matrices with real number entries, denoted $\mathbf{M}(\mathbb{R})$.

Example 17. Let $\mathbf{M}(\mathbb{R})$ be the set of all 2×2 matrices with real number entries. That is, $\mathbf{M}(\mathbb{R})$ contains all arrays of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where a, b, c, and d are real numbers. Two matrices are equal if and only if their corresponding entries are equal, *i.e.*,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \iff a = e,\ b = f,\ c = g,\ d = h.$$

For example,

$$\begin{pmatrix} 4 & 9 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1+3 & 4+5 \\ 7-7 & 8-6 \end{pmatrix}, \quad \text{but} \quad \begin{pmatrix} 4 & 9 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 4 & 9 \\ 2 & 0 \end{pmatrix}.$$

Addition of matrices is done entry-wise:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

For example,

$$\begin{pmatrix} 1 & -2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1+5 & -2+6 \\ 3+7 & 4+8 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 10 & 12 \end{pmatrix}.$$

Multiplication of matrices is a bit more involved. The product of two 2×2 matrices is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

For example,

$$\begin{pmatrix} 7 & 2 \\ 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 6 \\ 8 & 4 \end{pmatrix} = \begin{pmatrix} 7\cdot 1+2\cdot 8 & 7\cdot 6+2\cdot 4 \\ 0\cdot 1+5\cdot 8 & 0\cdot 6+5\cdot 4 \end{pmatrix} = \begin{pmatrix} 23 & 50 \\ 40 & 20 \end{pmatrix}.$$

Reversing the order of the factors in matrix multiplication *may* produce a different result, as is the case in our previous example:

$$\begin{pmatrix} 1 & 6 \\ 8 & 4 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1\cdot 7+6\cdot 0 & 1\cdot 2+6\cdot 5 \\ 8\cdot 7+4\cdot 0 & 8\cdot 2+4\cdot 5 \end{pmatrix} = \begin{pmatrix} 7 & 32 \\ 56 & 48 \end{pmatrix}.$$

Multiplication is therefore not commutative in general for matrices. One can verify that $(\mathbf{M}(\mathbb{R}), +, \cdot)$ satisfies all the properties of a ring as given in Defn. 9 and is thus a ring. The zero element of said ring is the zero matrix

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

and the matrix $\mathbf{X} = \left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ is a solution of

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \mathbf{X} = \mathbf{0},$$

thus $\mathbf{X}$ is the additive inverse of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The multiplicative identity element is the identity matrix

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

satisfying

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \mathbf{I} = \mathbf{I} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Interestingly, two nonzero matrices can multiply to give the zero matrix. For example,

$$\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} -3 & -9 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 4 \cdot (-3) + 6 \cdot 2 & 4 \cdot (-9) + 6 \cdot 6 \\ 2 \cdot (-3) + 3 \cdot 2 & 2 \cdot (-9) + 3 \cdot 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Using the same definitions of matrix addition and multiplication as above, we can construct other rings using matrices. Consider the following question:

Question 18. *Let* $\mathbf{K}(\mathbb{R})$ *be the set of all* 2×2 *matrices of the form*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

where $a, b \in \mathbb{R}$. *Show that* $(\mathbf{K}(\mathbb{R}), +, \cdot)$ *is a commutative ring with identity.*

In the examples we've done so far, we've seen a couple of rings that have the property of two nonzero elements multiplying to give zero. In the following subsection, we explore rings that do not have this property. We also explore rings which have an additional, new property. Rings with these additional properties are given special names and are of incredible importance in the study of algebra.

Integral Domains and Fields

Definition 19 (Integral domain)**.** An **integral domain** is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the following axiom: $\forall a, b \in R$,

11. if $ab = 0$, then $a = 0$ or $b = 0$.

The condition $1_R \neq 0_R$ is included here to avoid trivial cases where the ring contains only one element; namely, the ring $\{0_R\}$. Elements of a ring that are themselves nonzero but multiply to give zero are called **zero divisors**:

Definition 20 (Zero divisor)**.** An element a in a ring R is a **zero divisor** provided that $a \neq 0_R$ and $\exists\, b \in R$, with $b \neq 0_R$, s.t. $ab = 0_R$.

Looking back at Example 17, we see that $\mathbf{M}(\mathbb{R})$ is not an integral domain since it contains zero divisors; namely, the two nonzero matrices that we multiplied to get the zero matrix, $\left(\begin{smallmatrix} 4 & 6 \\ 2 & 3 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -3 & -9 \\ 2 & 6 \end{smallmatrix}\right)$.

Recall our short dicussion in the section on groups, where we mentioned that $(\mathbb{Z}, \cdot)$ is not a group because not every integer has a multiplicative inverse. However, we pointed out that $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group because every nonzero rational number has a multiplicative inverse. Thus far in our development, we have not studied rings where every nonzero element has a multiplicative inverse. We do so now with the following definition:

Definition 21 (Field)**.** A **field** is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the following axiom: $\forall\, a \in R$, with $a \neq 0_R$,

12. $\exists\, a^{-1} \in R$ s.t. $aa^{-1} = 1$.

Note axiom 11 is not mentioned explicitly in the definition of a field. However, it can be shown that every field is an integral domain.[9]

[9] The inverse of this is not true, however, as it is not generally true that an integral domain is a field. Take, for example, $\mathbb{Z}$. It is an integral domain but not a field. Interestingly, it is true that a *finite* integral domain is a field.

Example 22. The set of rational numbers $\mathbb{Q}$ equipped with the usual addition and multiplication operations, $(\mathbb{Q}, +, \cdot)$, is a field. It satisfies all 12 properties listed in Defns. 9 through 21. The set of real numbers $\mathbb{R}$ is also a field under the usual addition and multiplication.

Resources

1. *Abstract Algebra: An Introduction* (3rd ed.) by Thomas W. Hungerford.

Complex Numbers

Introduction

Definition 23 (Complex numbers)**.** The set of **complex numbers**, denoted $\mathbb{C}$, is defined as pairs of real numbers,

$$\mathbb{C} \equiv \{(x, y) : x, y \in \mathbb{R}\},$$

equipped with addition

$$(x_1, y_1) + (x_2, y_2) \equiv (x_1 + x_2, y_1 + y_2),$$

and multiplication

$$(x_1, y_1) \cdot (x_2, y_2) \equiv (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2).$$

By the definition above complex numbers of the form $(x, 0)$ behave like real numbers under addition and multiplication:

$$(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0), \quad \text{and} \quad (x_1, 0) \cdot (x_2, 0) = (x_1 x_2, 0).$$

Furthermore, the complex numbers $(0, 0)$ and $(1, 0)$ serve as the additive and multiplicative identities, respectively. With all of this, we now show that $(\mathbb{C}, +, \cdot)$ is a field:

Proposition 24. *The set of complex numbers $\mathbb{C}$ equipped with the addition and multiplication operations defined above, $(\mathbb{C}, +, \cdot)$, is a field.*

Proof. We must verify that $(\mathbb{C}, +, \cdot)$ satisfies all 11 properties listed in Defns. 9 through 21. $\forall\ (x_1, y_1)$, (x_2, y_2), $(x_3, y_3) \in \mathbb{C}$,

1. $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \in \mathbb{C}$ by closure of addition in $\mathbb{R}$,
2. $(x_1, y_1) + [(x_2, y_2) + (x_3, y_3)] = (x_1, y_1) + (x_2 + x_3, y_2 + y_3) = (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) = (x_1 + x_2, y_1 + y_2) + (x_3, y_3) = [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3)$ by associativity of addition in $\mathbb{R}$,
3. $\exists 0_F \in \mathbb{C}$, namely $(0, 0)$, s.t. $(x_1, y_1) + (0, 0) = (x_1 + 0, y_1 + 0) = (x_1, y_1) = (0 + x_1, 0 + y_1) = (0, 0) + (x_1, y_1)$ by the additive identity property in $\mathbb{R}$,

4. $\forall\ (x_1, y_1) \in \mathbb{C}$, $\exists$ an additive inverse, namely $(-x_1, -y_1)$, s.t. $(x_1, y_1) + (-x_1, -y_1) = (x_1 - x_1, y_1 - y_1) = (0, 0) = (-x_1 + x_1, -y_1 + y_1) = (-x_1, -y_1) + (x_1, y_1)$ by the additive inverse property in $\mathbb{R}$,
5. $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1)$ by commutativity of addition in $\mathbb{R}$,
6. $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \in \mathbb{C}$ by closure of multiplication (and addition) in $\mathbb{R}$,
7. $(x_1, y_1) \cdot [(x_2, y_2) \cdot (x_3, y_3)] = (x_1, y_1) \cdot (x_2x_3 - y_2y_3, x_2y_3 + y_2x_3) = (x_1(x_2x_3 - y_2y_3) - y_1(x_2y_3 + y_2x_3), x_1(x_2y_3 + y_2x_3) + y_1(x_2x_3 - y_2y_3)) = (x_1x_2x_3 - x_1y_2y_3 - y_1x_2y_3 - y_1y_2x_3, x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 - y_1y_2y_3) = (x_1x_2x_3 - y_1y_2x_3 - x_1y_2y_3 - y_1x_2y_3, x_1y_2x_3 + y_1x_2x_3 + x_1x_2y_3 - y_1y_2y_3) = ((x_1x_2 - y_1y_2)x_3 - (x_1y_2 + y_1x_2)y_3, (x_1y_2 + y_1x_2)x_3 + (x_1x_2 - y_1y_2)y_3) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \cdot (x_3, y_3) = [(x_1, y_1) \cdot (x_2, y_2)] \cdot (x_3, y_3)$ by associativity of multiplication and addition in $\mathbb{R}$,
8. $(x_1, y_1) \cdot [(x_2, y_2) + (x_3, y_3)] = (x_1, y_1) \cdot (x_2 + x_3, y_2 + y_3) = (x_1(x_2 + x_3) - y_1(y_2 + y_3), x_1(y_2 + y_3) + y_1(x_2 + x_3)) = (x_1x_2 + x_1x_3 - y_1y_2 - y_1y_3, x_1y_2 + x_1y_3 + y_1x_2 + y_1x_3) = ((x_1x_2 - y_1y_2) + (x_1x_3 - y_1y_3), (x_1y_2 + y_1x_2) + (x_1y_3 + y_1x_3)) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) + (x_1x_3 - y_1y_3, x_1y_3 + y_1x_3) = (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)$. Similarly, $[(x_1, y_1) + (x_2, y_2)] \cdot (x_3, y_3) = (x_1, y_1) \cdot (x_3, y_3) + (x_2, y_2) \cdot (x_3, y_3)$ by associativity of multiplication and addition in $\mathbb{R}$,
9. $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) = (x_2x_1 - y_2y_1, x_2y_1 + y_2x_1) = (x_2, y_2) \cdot (x_1, y_1)$ by commutativity of multiplication and addition in $\mathbb{R}$,
10. $\exists 1_F \in \mathbb{C}$, namely $(1, 0)$, s.t. $(x_1, y_1) \cdot (1, 0) = (x_1 \cdot 1 - y_1 \cdot 0, x_1 \cdot 0 + y_1 \cdot 1) = (x_1, y_1) = (1 \cdot x_1 - 0 \cdot y_1, 1 \cdot y_1 + 0 \cdot x_1) = (1, 0) \cdot (x_1, y_1)$ by the multiplicative identity property in $\mathbb{R}$,
11. $\forall\ (x_1, y_1) \in \mathbb{C}$, with $(x_1, y_1) \neq (0, 0)$, $\exists$ a multiplicative inverse, namely $\left(\frac{x_1}{x_1^2+y_1^2}, \frac{-y_1}{x_1^2+y_1^2}\right)$, s.t.

$$(x_1, y_1) \cdot \left(\frac{x_1}{x_1^2 + y_1^2}, \frac{-y_1}{x_1^2 + y_1^2}\right) = \left(\frac{x_1^2 + y_1^2}{x_1^2 + y_1^2}, \frac{0}{x_1^2 + y_1^2}\right) = (1, 0) = \left(\frac{x_1}{x_1^2 + y_1^2}, \frac{-y_1}{x_1^2 + y_1^2}\right) \cdot (x_1, y_1).$$

□

The multiplicative inverse used in the proof of property 11 above is derived from the fact that if we want

$$(x_1, y_1) \cdot (a, b) = (1, 0),$$

then we must have

$$(x_1a - y_1b, x_1b + y_1a) = (1, 0),$$

which gives us the system of equations

$$\begin{aligned} x_1a - y_1b &= 1, \\ x_1b + y_1a &= 0. \end{aligned}$$

Solving this system for a and b,

$$x_1b + y_1a = 0 \quad \Longrightarrow \quad b = \frac{-y_1a}{x_1} \quad \text{(assuming } x_1 \neq 0\text{)},$$

$$\therefore, x_1a - y_1\left(\frac{-y_1a}{x_1}\right) = 1 \quad \Longrightarrow \quad x_1a + \frac{y_1^2a}{x_1} = 1 \quad \Longrightarrow \quad \boxed{a = \frac{x_1}{x_1^2 + y_1^2}} \quad \text{and} \quad b = \frac{-y_1a}{x_1} = \boxed{\frac{-y_1}{x_1^2 + y_1^2}}.$$

The definition of multiplication in $\mathbb{C}$ may seem innocent at first glance, but it has deep implications. In particular, notice that

$$(0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0). \tag{3}$$

This identity, together with the fact that

$$(a,0)\cdot(x,y) = (ax,ay),$$

allows for an alternative notation for complex numbers. Specifically, we can write

$$(x,y) = (x,0)+(0,y) = (x,0)\cdot(1,0)+(y,0)\cdot(0,1),$$

where since $(x,0)$ and $(y,0)$ behave like real numbers, we can denote them simply as x and y, respectively. That is, we can write

$$(x,y) = x\cdot(1,0)+y\cdot(0,1).$$

This means that we can write any complex number (x,y) as a linear combination $(1,0)$ and $(0,1)$ with coefficients x and y. $(1,0)$, in turn, behaves like the real number 1, while $(0,1)$ behaves like a new number, call it i. Then the complex number that we used to call (x,y) can now be written as

$$(x,y) = x\cdot 1 + y\cdot i = x+yi.$$

Eqn. (3) then tells us that $i^2 = -1$.[10]

Definition 25. The number x is called the **real part** and y the **imaginary part** of the complex number $x+yi$, often denoted $\mathrm{Re}\,(x+yi) = x$ and $\mathrm{Im}\,(x+yi) = y$, respectively.

[10] $i^2 = -1$ reveals that i is the square root of -1. This not only says that an equation such as $x^2+1 = 0$ has a solution (or that the polynomial x^2+1 is *reducible*), but every nonconstant polynomial has roots in $\mathbb{C}$. This is the content of the Fundamental Theorem of Algebra, a deep and important result in mathematics that we will, unfortunately, ignore here.

Geometric Representation

Complex numbers are usually denoted by a single letter, such as z. Thus, we often write $z = x+yi$, where $x,y\in\mathbb{R}$. Because the product is commutative, there is no difference between writing $x+yi$ and $x+iy$. Visually, complex numbers can be represented as points in the Euclidean plane $\mathbb{R}^2$ having Cartesian coordinates (x,y). In this context we refer to $\mathbb{R}^2$ as the **complex plane** (alternatively, the **Argand plane** or the **Gaussian plane**).[11] We use the horizontal axis (the x-axis) to represent the real part of a complex number and the vertical axis (the y-axis) to represent the imaginary part.

In Fig. 5, we plot the complex numbers $z = 2+i$ and $w = -1+2i$ in the complex plane. Notice that the sum of these two complex

[11] Notice that the plane is defined as $\mathbb{R}^2$, not $\mathbb{C}^2$. The complex plane is a way of visualizing complex numbers, which are elements of $\mathbb{C}$, using points in $\mathbb{R}^2$.

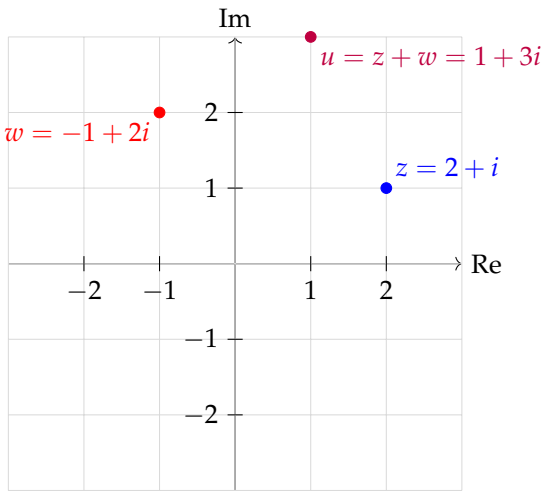

Figure 5: The complex plane. The horizontal axis represents the real part of a complex number, and the vertical axis represents the imaginary part. Here, we plot the complex numbers $z = 2 + i$, $w = -1 + 2i$, and their sum $u = z + w = 1 + 3i$. Notice that the sum of complex numbers is simply the sum of their corresponding coordinates in the plane.

numbers, $u = z + w = 1 + 3i$, is represented by the point obtained by adding their corresponding coordinates in the plane. Going back to our original definition of complex numbers as pairs of real numbers, we see that this is precisely how addition is defined in $\mathbb{C}$:

$$(2,1) + (-1,2) = (2 + (-1), 1 + 2) = (1,3).$$

One may prefer our original notation of complex numbers as pairs of real numbers when performing addition. Doing so is particularly useful when considering complex numbers as straight arrows starting from the origin $(0,0)$ and ending at the point (x,y) in the complex plane. Fig. 5 is the as in Fig. 6.

These arrows are more formally known as **vectors**. A vector in $\mathbb{R}^2$ is an ordered pair of real numbers that can be represented as an arrow in the plane. Vectors have both a magnitude (or length) and a direction. We define these notions for complex numbers as follows:

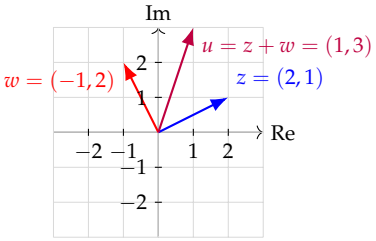

Figure 6: The complex plane with vectors representing complex numbers. Here, the complex numbers $z = (2,1)$, $w = (-1,2)$, and their sum $u = z + w = (1,3)$ are represented as arrows starting from the origin. The sum of complex numbers corresponds to the vector addition of their respective arrows.

Definition 26. The **modulus** (or **magnitude**) of a complex number $z = x + yi$ is

$$r = |z| \equiv \sqrt{x^2 + y^2},$$

and an **argument** (or **angle**) of z is any real number ϕ s.t.

$$x = r\cos(\phi) \quad \text{and} \quad y = r\sin(\phi).$$

By the above definition we can represent any complex number $z = x + yi$ in terms of its modulus r and an argument ϕ as

$$z = r\cos(\phi) + ir\sin(\phi).$$

The periodic nature of the trigonometric functions implies that if ϕ is an argument of z, then so is $\phi + 2\pi k$ for any integer k. Thus, every nonzero complex number has infinitely many arguments differing by integer multiples of 2π. The number $0 = 0 + 0i$ has modulus 0 and every real number ϕ is an argument.

Example 27. The modulus of the complex number $z = 1 + i\sqrt{3}$ is given by

$$r = |z| = \sqrt{1^2 + \left(\sqrt{3}\right)^2} = \sqrt{4} = 2.$$

To find an argument ϕ of z, we solve the system of equations

$$\begin{aligned} 1 &= 2\cos(\phi), \\ \sqrt{3} &= 2\sin(\phi). \end{aligned}$$

Solving the first equation for $\cos(\phi)$ tells us that $\phi = \frac{\pi}{3}, \frac{5\pi}{3}$. Similarly, solving the second equation for $\sin(\phi)$ tells us that $\phi = \frac{\pi}{3}, \frac{2\pi}{3}$. The only value of ϕ that satisfies both equations is $\phi = \frac{\pi}{3}$. Thus, one argument of z is $\frac{\pi}{3}$, and all other arguments are given by

$$\phi = \frac{\pi}{3} + 2\pi k, \quad k \in \mathbb{Z}.$$

Example 28. Given the modulus $r = 3$ and an argument $\phi = \frac{\pi}{4}$, we can find the corresponding complex number z as follows:

$$\begin{aligned} z &= r\cos(\phi) + ir\sin(\phi) \\ &= 3\cos\left(\frac{\pi}{4}\right) + 3i\sin\left(\frac{\pi}{4}\right) \\ &= \frac{3\sqrt{2}}{2} + \frac{3\sqrt{2}}{2}i. \end{aligned}$$

Prior to proceeding, recall the following trigonometric identities:

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta), \tag{4}$$

$$\sin(\alpha + \beta) = \cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta). \tag{5}$$

Now, consider two complex numbers $z_1 = r_1\cos(\phi_1) + ir_1\sin(\phi_1)$ and $z_2 = r_2\cos(\phi_2) + ir_2\sin(\phi_2)$. Their product is given by

$$
\begin{aligned}
z_1 z_2 &= (r_1\cos(\phi_1) + i r_1 \sin(\phi_1)) \cdot (r_2\cos(\phi_2) + i r_2 \sin(\phi_2)) \\
&= r_1 r_2 \Big[\cos(\phi_1)\cos(\phi_2) + i\cos(\phi_1)\sin(\phi_2) + i\sin(\phi_1)\cos(\phi_2) + i^2 \sin(\phi_1)\sin(\phi_2)\Big] \\
&= r_1 r_2 [\cos(\phi_1)\cos(\phi_2) - \sin(\phi_1)\sin(\phi_2) + i\cos(\phi_1)\sin(\phi_2) + i\sin(\phi_1)\cos(\phi_2)] \\
&= r_1 r_2 [\cos(\phi_1)\cos(\phi_2) - \sin(\phi_1)\sin(\phi_2) + i(\cos(\phi_1)\sin(\phi_2) + \sin(\phi_1)\cos(\phi_2))] \\
&= r_1 r_2 [\cos(\phi_1 + \phi_2) + i\sin(\phi_1 + \phi_2)], \quad \text{by Eqns. (4), (5).}
\end{aligned} \tag{6}
$$

Thus, the modulus of the product $z_1 z_2$ is the product of the moduli of z_1 and z_2, and an argument of $z_1 z_2$ is the sum of an argument of z_1 and an argument of z_2. In view of the above calculation, we will deal

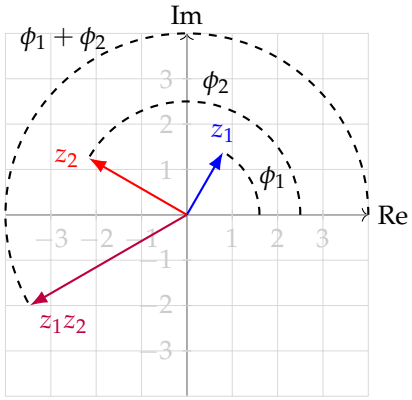

Figure 7: The complex plane with vectors representing complex numbers z_1, z_2, and their product $z_1 z_2$. The modulus of the product is the product of the moduli of z_1 and z_2, and an argument of the product is the sum of an argument of z_1 and an argument of z_2.

with complex numbers of the form $\cos(\phi) + i\sin(\phi)$, where ϕ is a real number. To simplify notation, we define

$$e^{i\phi} \equiv \cos(\phi) + i\sin(\phi). \tag{7}$$

At this point, this exponential notation is indeed purely a notation. However, later on we will see that this notation has deeper implications and connections to other areas of mathematics.

We demonstate the usefulness of this notation with the following proposition.

Proposition 29. *For any $\phi, \phi_1, \phi_2 \in \mathbb{R}$,*

1. $e^{i\phi_1} e^{i\phi_2} = e^{i(\phi_1+\phi_2)}$,
2. $e^{i0} = 1$,
3. $\frac{1}{e^{i\phi}} = e^{-i\phi}$,
4. $e^{i(\phi+2\pi)} = e^{i\phi}$,
5. $\left|e^{i\phi}\right| = 1$,
6. $\frac{d}{d\phi} e^{i\phi} = i e^{i\phi}$.

Proof. Going one by one:

1. Follows directly from Eqn. (6) with $r_1 = r_2 = 1$.
2. Follows directly from Eqn. (7) as

$$e^{i0} = \cos(0) + i\sin(0) = 1 + i \cdot 0 = 1.$$

3. To show that $\frac{1}{e^{i\phi}} = e^{-i\phi}$, we need to show that $e^{i\phi} \cdot e^{-i\phi} = 1$. This follows directly from property 1 and property 2 as
$$e^{i\phi} \cdot e^{-i\phi} = e^{i(\phi-\phi)} = e^{i0} = 1.$$
4. Follows directly from Eqn. (7) as
$$e^{i(\phi+2\pi)} = \cos(\phi + 2\pi) + i\sin(\phi + 2\pi) = \cos(\phi) + i\sin(\phi) = e^{i\phi},$$
by the periodicity of the trigonometric functions.
5. Follows directly from Eqn. (7) as
$$\left|e^{i\phi}\right| = \sqrt{\cos^2(\phi) + \sin^2(\phi)} = \sqrt{1} = 1,$$
by the definition of modulus in Defn. 26.
6. Follows directly from Eqn. (7) as
$$\frac{d}{d\phi} e^{i\phi} = \frac{d}{d\phi}[\cos(\phi) + i\sin(\phi)] = -\sin(\phi) + i\cos(\phi) = i[\cos(\phi) + i\sin(\phi)] = i\, e^{i\phi}.$$

□

With our new notation we can now express any complex number $z = x + yi$ in terms of its modulus r and an argument ϕ as
$$z = x + yi = r\, e^{i\phi}.$$

With this new representation we now have five different ways of representing a complex number z:

Formal (x, y)	Algebraic:	rectangular $x + iy$	exponential $re^{i\theta}$
	Geometric:	cartesian 	polar 

Table 4: Different representations of a complex number z.

Vector Spaces

Definition 30 (Vector space)**.** Let F be a field. A **vector space over F** is an additive abelian group (*i.e.*, an abelian group equipped with addition) V equipped with scalar multiplication s.t., $\forall\ a_1, a_2, a_3 \in F$ and $v_1, v_2, v_3 \in V$,

1. $a_1(v_1 + v_2) = a_1v_1 + a_1v_2$,

2. $(a_1 + a_2)v_1 = a_1v_1 + a_2v_1$,

3. $a_1(a_2v_1) = (a_1a_2)v_1$,

4. $1_Fv_1 = v_1$,

where 1_F is the multiplicative identity in F.

Suppose V is a vector space over a field F and that w and v_1, v_2, …, v_n are elements of V. We say that w is a **linear combination** of v_1, v_2, …, v_n if w can be written in the form

$$w = a_1v_1 + a_2v_2 + \cdots + a_nv_n \tag{8}$$

for $a_i \in F$.

Definition 31 (Span)**.** If every element of a vector space V over a field F is a linear combination of v_1, v_2, …, v_n, we say that the set $\{v_1, v_2, \ldots, v_n\}$ **spans** V over F.

Definition 32 (Linear independence)**.** A subset $\{v_1, v_2, \ldots, v_n\}$ of a vector space V over a field F is said to be **linearly independent** over F provided that whenever

$$f_1v_1 + f_2v_2 + \cdots + f_nv_n = 0_V,$$

with each $f_i \in F$, then, $\forall i$, $f_i = 0_F$. A set that is not linearly independent is said to be **linearly dependent**.

Definition 33 (Basis)**.** A subset $\{v_1, v_2, \ldots, v_n\}$ of a vector space V over a field F is said to be a **basis** of V if it spans V and is linearly independent over F.

Definition 34 (Dimensionality)**.** If a vector space V over a field F has a finite basis, then V is said to be **finite dimensional** over F. The **dimension of** V **over** F is the number of elements in *any* basis of V. If V does not have a finite basis, then V is said to be **infinite dimensional** over F.

Lemma 35. *Let V be a vector space over a field F. The subset $\{v_1, v_2, \ldots, v_n\}$ of V is linearly dependent over F iff some v_k is a linear combination of v_1, v_2, …, v_{k-1}.*

Proof. If some v_k is a linear combination of other elements in V, then the set is linearly dependent by Defn. 32. Conversely, suppose $\{v_1, v_2, \ldots, v_n\}$ is linearly dependent. Then $\exists\, f_1, \ldots, f_n \in F$, not all zero, s.t. $f_1v_1 + f_2v_2 + \cdots + f_nv_n = 0_V$. Let k be the largest index s.t. f_k is nonzero. Then $f_i = 0_F$ for $i > k$ and

$$\begin{aligned} f_1v_1 + f_2v_2 + \cdots + f_kv_k &= 0_V \\ f_kv_k &= -f_1v_1 - f_2v_2 - \cdots - f_{k-1}v_{k-1}. \end{aligned}$$

Since F is a field and $f_k \neq 0_F$, f_k^{-1} exists. Multiplying the preceding equation by f_k^{-1}, we have

$$v_k = -f_k^{-1}f_1v_1 - f_k^{-1}f_2v_2 - \cdots - f_k^{-1}f_{k-1}v_{k-1},$$

showing that v_k is a linear combination of the preceding v's. □

Lemma 36. *Let V be a vector space over a field F that is spanned by the set $\{v_1, v_2, \ldots, v_n\}$. If $\{u_1, u_2, \ldots, u_m\}$ is any linearly independent subset of V, then $m \leqslant n$.*

Resources

1. *Abstract Algebra: An Introduction* (3rd ed.) by Thomas W. Hungerford.

Bibliography