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

A DESIGNER KNOWS THAT HE HAS ACHIEVED PERFECTION NOT WHEN THERE IS NOTHING LEFT TO ADD, BUT WHEN THERE IS NOTHING LEFT TO TAKE AWAY.
ANTOINE DE SAINT-EXUPÉRY

. . . 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

List of Figures

List of Tables

Insert cool dedication here.

Introduction

This serves as a gentle introduction to the vast topic of quantum communication. The mathematical foundation is built, not assumed.

Building the Mathematical Foundation

Contents

The topic of quantum communication, like most, requires a strong mathematician to build upon it. This chapter serves to build the mathematical foundation required to understand the majority of the text.[1] The topics covered here are not exhaustive, but they do provide a good starting point for the reader.

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.

[1] Very little of the foundation is built as we require it and not in this chapter; *e.g.*, Fourier analysis is covered later in the text when we run into quantum algorithms.

Group Theory

To begin our adventure towards vector spaces, we start with, what I consider, the most fundamental mathematical structure: groups. Groups are *sets*[2] equipped with an *operation* that satisfies four axioms. Groups are ubiquitous in mathematics and physics, and they have 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 $\mathbf{a}$ and $\mathbf{b}$ 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 $f(\mathbf{a},\mathbf{b}) = \mathbf{a} \times \mathbf{b}$.

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:

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

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.

Unlike the integers, the set of rational numbers, $\mathbb{Q}$, 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: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$.[3] Associative multiplication in $\mathbb{Q}$ follows from the fact that multiplication of integers is associative. The identity element is the rational number 1 since $\frac{a}{b} \cdot 1 = \frac{a}{b} = 1 \cdot \frac{a}{b}$.

[3] 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.

Finally, every rational number 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, $(\mathbb{Q}, \cdot)$ is a group.

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.

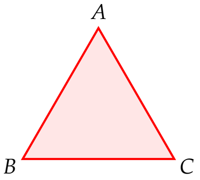

Figure 1: An equilateral triangle $\triangle ABC$. Note that the labels on the triangle's vertices are simply for us to visualize how the triangle is transformed. The labels do not imply that the triangle is oriented in any particular way.

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:

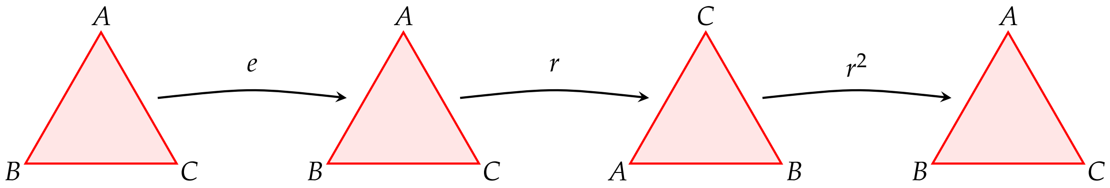

Figure 2: We see that the identity transformation e leaves the triangle unchanged, while the transformations r and r^2 rotate the triangle by 120° and 240° respectively. As one would expect, applying the r and r^2 rotations consecutively to the original triangle yields the original triangle again.

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 in Fig. 2.

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. 3). 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 Fig. 4.

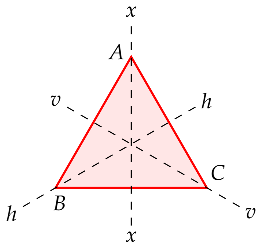

Figure 3: Showing all of the axes of rotation on the equilateral triangle $\triangle ABC$.

As seen in Figs. 2 and 4, the transformations $\{e, r, r^2, x, h, v\}$ can be combined (*i.e.*, applied one after the other) to produce other, single transformations.

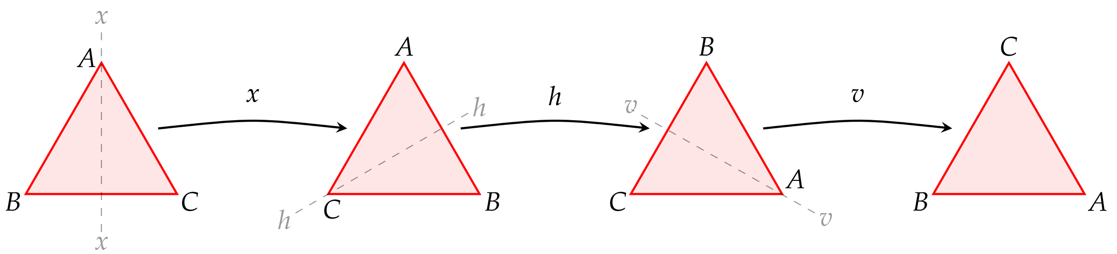

Figure 4: The axis of symmetry is shown (faintly) prior to reflection. Note that the final triangle here is not one that can be achieved via rotations alone. That is, applying x, h, and v consecutively is equivalent to simply applying the h transformation to the original triangle.

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. 4 (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 $D_3 \equiv \{e, r, r^2, x, h, v\}$[4] 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.

$\circ$	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 the 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

[4] 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.

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[5] of rotations, $\{e, r, r^2\}$, is abelian.

We can now return to the list at the start of this subsection and 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 in the elegant field 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, of the best introductory texts on abstract algebra. It's also *free*.[6] 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.

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

[5] 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 for the subgroup $\{e, r, r^2\}$ of D_3. We use the word 'proper' to say that the subgroup is not equal to the whole group D_3.

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

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

A natural extension of groups are **rings**, which 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 concept of *congruence* and *modular arithmetic*, which 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, $a \equiv b (\operatorname{mod} n)$ if $c | (a - b)$.[7] For example, $15 \equiv 6 (\operatorname{mod} 3)$ since 3 divides $15 - 6 = 9$. Additionally, $23 \equiv -1 (\operatorname{mod} 6)$ 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.*,

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

For example, in congruence modulo 7, $[5] = \{\ldots, -9, -2, 5, 12, 19, \ldots\}$.[8] 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."[9] One may anticipate an issue in terms of representatives of these classes. For example, since $4 \equiv 7 (\operatorname{mod} 3)$, $4 \equiv 16 (\operatorname{mod} 3)$, and $4 \equiv -2 (\operatorname{mod} 3)$, 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 can then be mapped onto 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

$\oplus$	[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 $\mathbb{Z}_3$.

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

[8] 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 $n \equiv a (\operatorname{mod} c) \implies c | (n - a)$, which means $\exists k \in Z$ s.t. $n - a = kc$, hence $n = a + kc$.

[9] Note that this is a set of congruence classes, not integers. Each class itself is a set of integers, as seen in the previous paragraph.

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.

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:

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.

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)

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**.

Integral Domains and Fields

Definition 12 (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 $b = 0$.

Definition 13 (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 $a \neq 0$,

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

Resources

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

Vector Spaces

Definition 14 (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

$$w = a_1v_1 + a_2v_2 + \cdots + a_nv_n \tag{3}$$

for $a_i \in F$.

Definition 15 (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 16 (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 17 (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 18 (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 19. *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. 16. 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

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

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 20. *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.

Probability Theory

Notationally, if A is some event of interest, then $P(A)$ is the probability that A occurs.

Definition 21. Let A and B both be subsets of a sample space Ω. We say that A and B are **independent** if and only if

$$P(A \cap B) = P(A)P(B).$$

In other words, if the probability of the intersection of two events is equal to the product of their individual probabilities, then the two events are independent. If this condition does not hold, then the two events are **dependent**.

Definition 22 (Expectation Value)**.** The **expectation value** (or **expected value**) of a random quantity X, denoted $\langle X \rangle$ (or $\mathbb{E}[X]$), is defined as

$$\langle X \rangle = \sum_{x \in X(\Omega)} x P(X = x).$$

where the sum is over all possible values x that X can take on.

Bibliography