Chapter Zero

The Language of Mathematics:

Sets, Axioms, Theorems & Proofs

Mathematics is a language, and Logic is its grammar.

You are taking a course in Linear Algebra because the major that you have chosen will make use of its techniques, both computational and theoretical, at some points in your career. Whether it is in engineering, computer science, chemistry, physics, economics, or of course, mathematics, you will encounter matrices, vector spaces and linear transformations. For most of you, this will be your first experience in an abstract course that emphasizes theory on an almost equal footing with computation.

The purpose of this introductory Chapter is to familiarize you with the basic components of the mathematical language, in particular, the study of sets (especially sets of numbers), subsets, operations on sets, logic, Axioms, Theorems, and basic guidelines on how to write a coherent and logically correct Proof for a Theorem.

Part I: Set Theory and Basic Logic

The ***set*** is the most basic object that we work with in mathematics:

> ***Definition:*** A ***set*** is an unordered collection of objects, called the ***elements*** of the set. A set can be described using the ***set-builder notation:***
>
> $$X = \{x \,|\, x \text{ possesses certain determinable qualities}\},$$
>
> or the ***roster method:***
>
> $$X = \{a, b, \ldots\},$$
>
> where we explicitly ***list*** the elements of X. The bar symbol "|" in set-builder notation represents the phrase "such that."

We will agree that such "objects" are already known to exist. They could consist of people, letters of the alphabet, real numbers, or functions. There is also a special set, called the ***empty set*** or the ***null-set***, that does not contain any elements. We represent the empty set symbolically as:

$$\emptyset \quad \text{or} \quad \{\ \ \}.$$

Early in life, we learn how to count using the set of ***natural numbers:***

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

We learn how to add, subtract, multiply and divide these numbers. Eventually, we learn about ***negative integers***, thus completing the set of all ***integers:***

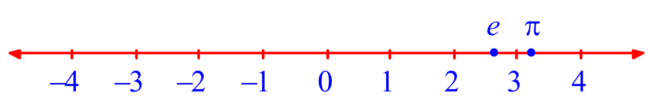
$$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We use the letter $\mathbb{Z}$ from ***Zahlen***, the German word for "number." Later on, we learn that some integers cannot be exactly divided by others, thus producing the concept of a ***fraction*** and the set of ***rational numbers:***

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \text{ and } b \text{ are integers, with } b \neq 0 \right\}.$$

Notice that we defined $\mathbb{Q}$ using set-builder notation. Still later on, we learn of the number π when we study the circumference and area of a circle. The number π is an ***irrational*** number, although it can be approximated by a fraction like 22/7 or as a decimal like 3.1416. When we learn to take square roots and cube roots, we encounter other examples of irrational numbers, such as $\sqrt{2}$ and $\sqrt[3]{5}$.

By combining the sets of rational and irrational numbers, we get the set of all ***real numbers*** $\mathbb{R}$. We visualize them as corresponding to points on a number line. A point is chosen to be "0," and another point to its right is chosen to be "1." The distance between these two points is the ***unit***, and subsequent integers are marked off using this unit. Real numbers are classified into positive numbers, negative numbers, and zero (which is neither positive nor negative). They are also ordered from left to right by our number line. We show the real number line below along with a couple of famous numbers:



The Real Number Line $\mathbb{R}$

Logical Statements and Axioms

An intelligent development of Set Theory requires us to develop in parallel a ***logical system***. The basic component of such a system is this:

Definition: A ***logical statement*** is a complete sentence that is either ***true*** or ***false***.

Examples: The statement:

The number 2 is an integer.

is a ***true*** logical statement. However:

The number 3/4 is an integer.

is a ***false*** logical statement. The statement:

Gustav Mahler is the greatest composer of all time.

is a sentence but it is ***not*** a logical statement, because the word "greatest" cannot be qualified. Thus, we cannot logically determine if this statement is true or false.□

In everyday life, especially in politics, one person can judge a statement to be true while someone else might decide that it is false. Such judgments depend on one's personal biases, how credible they deem the person who is making the argument, and how they appraise the facts that are carefully chosen (or omitted) to support the case. In mathematics, though, we have a logical system by which to determine the truth or falsehood of a logical statement, so that any two persons using this system will reach the ***same conclusion***. For the sake of sanity, we will need some starting points for our logical process:

> ***Definition:*** An ***Axiom*** is a logical statement that we will ***accept*** as true, that is, as reasonable human beings, we can ***mutually agree*** that such Axioms are true.

You can think of Axioms as analogous to the ***core beliefs*** of a philosophy or religion.

Examples: One of the most important Axioms of mathematics is this:

> The empty set $\emptyset$ exists.

In geometry, we accept as Axioms that ***points*** exist. We symbolize a point with a dot, although it is ***not literally*** a dot. We accept that through two distinct points there must exist a unique ***line***. We accept that any three non-collinear points (that is, three points through which no single line passes) determine a unique ***triangle***. We ***believe*** in the existence of these objects ***axiomatically***. We note, though, that these are Axioms in what we call ***Euclidean Geometry***, but there are other geometric systems that have very different Axioms for points, lines and triangles. □

Quantifiers

Most, if not all of the logical statements that we will encounter in Linear Algebra refer not just to numbers, but also to other objects that we will be constructing, such as vectors and matrices.

We will use what are called ***quantifiers*** in order to specify precisely what kind of object we are referring to:

> ***Definitions — Quantifiers:***
>
> There are two kinds of quantifiers: ***universal*** quantifiers and ***existential*** quantifiers.
>
> Examples of universal quantifiers are the words ***for any, for all*** and ***for every***, symbolized by $\forall$. They are often used in a logical statement to describe ***all*** members of a certain set.
>
> Examples of existential quantifiers are the phrases ***there is*** and ***there exists***, or their plural forms, ***there are*** and ***there exist***, symbolized by $\exists$. Existential quantifiers are often used to claim the existence (or non-existence) of a ***special*** element or elements of a certain set.

Example: In everyday life, we can make the following statement:

Everyone has a mother.

This is certainly a true logical statement. Let us express this statement more precisely using quantifiers:

> ***For every*** human being x, ***there exists*** another human being y who is the mother of x. □

Some of the best examples of logical statements involving quantifiers are found in the Axioms that define the Real Number system. Linear Algebra in a sense is a ***generalization*** of the real numbers, so it is worthwhile to formally study what most of us take for granted.

The Axioms for the Real Numbers

We will assume that the set of real numbers has been ***constructed*** for us, and that this set enjoys certain properties. Furthermore, we will mainly be interested in what are called the Field Axioms:

Axioms — The Field Axioms for the Set of Real Numbers:

There exists a set of Real Numbers, denoted $\mathbb{R}$, together with two binary operations:

$$+ \ \text{(addition)} \quad \text{and} \quad \bullet \ \text{(multiplication)}.$$

Furthermore, the members of $\mathbb{R}$ enjoy the following properties:

1. ***The Closure Property of Addition:***

   For all $x, y \in \mathbb{R}: x + y \in \mathbb{R}$ as well.

2. ***The Closure Property of Multiplication:***

   For all $x, y \in \mathbb{R}: x \bullet y \in \mathbb{R}$ as well.

3. ***The Commutative Property of Addition:***

   For all $x, y \in \mathbb{R}: x + y = y + x.$

4. ***The Commutative Property of Multiplication:***

   For all $x, y \in \mathbb{R}: x \bullet y = y \bullet x.$

5. ***The Associative Property of Addition:***

   For all $x, y, z \in \mathbb{R}: x + (y + z) = (x + y) + z.$

6. ***The Associative Property of Multiplication:***

   For all $x, y, z \in \mathbb{R}: x \bullet (y \bullet z) = (x \bullet y) \bullet z.$

7. ***The Distributive Property of Multiplication over Addition:***

   For all $x, y, z \in \mathbb{R}: x \bullet (y + z) = (x \bullet y) + (x \bullet z).$

8. ***The Existence of the Additive Identity:***

   There exists $0 \in \mathbb{R}$ such that ***for all*** $x \in \mathbb{R}: x + 0 = x = 0 + x.$

9. ***The Existence of the Multiplicative Identity:***

   There exists $1 \in \mathbb{R},\ 1 \neq 0,$ such that ***for all*** $x \in \mathbb{R}: x \bullet 1 = x = 1 \bullet x.$

10. ***The Existence of Additive Inverses:***

    For all $x \in \mathbb{R}$, ***there exists*** $-x \in \mathbb{R},$ such that: $x + (-x) = 0 = (-x) + x.$

11. ***The Existence of Multiplicative Inverses:***

    For all $x \in \mathbb{R},$ where $x \neq 0$, ***there exists*** $1/x \in \mathbb{R},$ such that:

    $$x \bullet (1/x) = 1 = (1/x) \bullet x.$$

Notice that each of the first seven Axioms begin with the quantifier ***For all***. These Axioms tell us that these properties are valid no matter which two or three real numbers we substitute into the expressions found in that Axiom. On the other hand, Axioms 8 and 9 begin with the quantifier ***There exists***, but in the second phrase, we see the quantifier ***for all***. Axioms 8 and 9 tell us that there are two ***special***, distinct real numbers, 0 and 1, for which two sets of equations are valid ***for all*** real numbers x:

$$x + 0 = x = 0 + x \quad \text{and} \quad x \cdot 1 = x = 1 \cdot x.$$

The numbers 0 and 1 are called ***identities*** because ***every*** $x \in \mathbb{R}$ preserves its identity under the corresponding operation. On the other hand, Axioms 10 and 11 begin with the quantifier ***For all***, but in the second phrase, we see the quantifier ***there exists*** — this is the ***opposite order*** of that found in Axioms 8 and 9. This means that once we ***choose*** x, we can find its additive inverse $-x$, such that:

$$x + (-x) = 0 = (-x) + x.$$

The additive inverse $-x$ ***depends*** on x. Similarly, the reciprocal $1/x$ depends on x, where $x \neq 0$.

We mentioned earlier that we develop our number system by starting with the natural numbers, then constructing negative integers and fractions. After this, though, it is surprisingly difficult to create the full set of real numbers. See Appendix A for a more thorough discussion of how to create numbers, and the complete set of Axioms that the set of real numbers satisfies. These include the ***Order Axioms***, which give us the rules for ***inequalities***, and the ***Completeness Axiom***, which distinguishes the real numbers from the rational numbers. Furthermore, although the 11 Axioms speak only about addition and multiplication, Axioms 10 and 11 allow us to define the related operations of ***subtraction*** and ***division***, and as usual, we will use the notation that is familiar to us:

> ***Definitions — Axioms for Subtraction and Division:***
> For all $x,\ y \in \mathbb{R}$, define the operation of ***subtraction*** by: $x - y = x + (-y)$.
> Similarly, if $y \neq 0$, define the operation of ***division*** by: $x/y = x \cdot (1/y)$.

Theorems and Implications

Now that we agree that Axioms will be accepted as true, we will be concerned with logical statements which can be ***deduced*** from these Axioms:

> ***Definitions:*** A true logical statement which is not just an Axiom is called a ***Theorem***. Many of the Theorems that we will encounter in Linear Algebra are called ***implications***, and they are of the form: ***if*** p ***then*** q, where p and q are logical statements.
> This implication can also be written symbolically as: $p \Rightarrow q$ (pronounced as: p ***implies*** q).

An implication $p \Rightarrow q$ is true if the statement q is true whenever we know that the statement p is also true. The statements p and q are called ***conditions***. The condition p is called the ***hypothesis*** (or ***antecedent*** or the ***given conditions***), and q is called the ***conclusion*** or the ***consequent***. If such an implication is true, we say that condition p is ***sufficient*** for condition q, and condition q is ***necessary*** for condition p.

Example: In Calculus, we are familiar with the implication:

> ***Theorem:*** ***If*** $f(x)$ is ***differentiable*** at $x = a$, ***then*** $f(x)$ is also ***continuous*** at $x = a$.

Let us use this Theorem to further understand the meaning of the words "necessary" and "sufficient." This Theorem can be interpreted as saying that if we ***want*** $f(x)$ to be continuous at $x = a$, then it is ***sufficient*** that $f(x)$ be differentiable at $x = a$, that is, we have sufficiently paid for the condition of continuity if we have already paid for the ***stricter*** condition of differentiability.

Similarly, if we ***knew*** that $f(x)$ is differentiable at $x = a$, then it is ***necessary*** that $f(x)$ is also continuous at $x = a$: it cannot be discontinuous according to this Theorem.□

Although we will primarily be proving Theorems, it is also important to know when a logical statement is false. An implication $p \Rightarrow q$ can be demonstrated to be false by giving a ***counterexample***, which is a situation where the given condition p is ***true***, but the conclusion q is ***false***.

Example: Let us consider the statement:

If p is a prime number, then $2^p - 1$ is also a prime number.

Recall that an integer $p > 1$ is ***prime*** if the only integers that exactly divide p are 1 and p itself. If we look at the first few prime numbers $p = 2,\ 3,\ 5,\ 7$, we get:

$$\begin{array}{ll} 2^2 - 1 = 4 - 1 = 3 & \text{is prime,} \\ 2^3 - 1 = 8 - 1 = 7 & \text{is prime,} \\ 2^5 - 1 = 32 - 1 = 31 & \text{is prime, and} \\ 2^7 - 1 = 128 - 1 = 127 & \text{is also prime.} \end{array}$$

This might fool you to believe that the statement is true. However, for $p = 11$, we get:

$$2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89.$$

Thus, we found a ***counterexample*** to the statement above, and so this statement is ***false***.□

In fact, it turns out that the integers of the form $2^p - 1$ where p is a prime number are ***rarely*** prime, and we call such prime numbers ***Mersenne Primes***. As of May 2016, there are only 49 known Mersenne Primes, and the largest of these is $2^{74,207,281} - 1$. This is also the largest known prime number. If this number were expressed in the usual decimal form, it will be 22,338,618 ***digits*** long. Large prime numbers have important applications in ***cryptography***, a field of mathematics which allows us to safely provide personal information such as credit card numbers on the internet.

Negations

> ***Definition:*** The ***negation*** of the logical statement p is written symbolically as: ***not*** p.

The statement ***not*** p is true precisely when p is false, and vice versa. When a negated logical statement is written in plain English, we put the word "not" in a more natural or appropriate place. We can also use related words such as "never" to indicate a negation.

Examples: The statement:

"An integer is ***not*** a rational number."

is a ***false*** logical statement. On the other hand, the statement:

"The function $g(x) = 1/x$ is ***not*** continuous at $x = 0$."

is a ***true*** logical statement.□

Converse, Inverse, Contrapositive and Equivalence

By using negations or reversing the roles of the hypothesis and conclusion, we can construct three implications associated to an implication $p \Rightarrow q$:

> ***Definition:*** For the implication $p \Rightarrow q$, we call:
>
> $q \Rightarrow p$ the ***converse*** of $p \Rightarrow q$,
>
> ***not*** $p \Rightarrow$ ***not*** q the ***inverse*** of $p \Rightarrow q$, and
>
> ***not*** $q \Rightarrow$ ***not*** p the ***contrapositive*** of $p \Rightarrow q$.

Unfortunately, even if we knew that an implication is true, its converse or inverse are not always true.

Example: We saw earlier that the following statement is true:

"***If*** $f(x)$ is ***differentiable*** at $x = a$, ***then*** $f(x)$ is also ***continuous*** at $x = a$."

The ***converse*** of this statement is:

"***If*** $f(x)$ is ***continuous*** at $x = a$, ***then*** $f(x)$ is also ***differentiable*** at $x = a$."

This statement is ***false***, as shown by the counterexample $f(x) = |x|$, which is well known to be continuous at $x = 0$, but is ***not differentiable*** at $x = 0$. Similarly, the ***inverse*** of this Theorem is:

"***If*** $f(x)$ is ***not differentiable*** at $x = a$, ***then*** $f(x)$ is also ***not continuous*** at $x = a$."

The inverse is also ***false***: the same function $f(x) = |x|$ is ***not differentiable*** at $x = 0$, but it ***is*** continuous there. Finally, the ***contrapositive*** of our Theorem is:

"***If*** $f(x)$ is ***not continuous*** at $x = a$, ***then*** $f(x)$ is also ***not differentiable*** at $x = a$."

The contrapositive is a ***true*** statement: a function which is not continuous cannot be differentiable, because otherwise, it ***has to be*** continuous.□

If we know that $p \Rightarrow q$ and $q \Rightarrow p$ are ***both*** true, then we say that the conditions p and q are ***logically equivalent*** to each other, and we write the ***equivalence*** or ***double-implication:***

$$p \iff q \quad \text{(pronounced as: } p \textbf{\textit{ if and only if }} q\text{)}.$$

We saw above that the contrapositive of our Theorem is also true, and in fact, this is no accident. An implication is always logically equivalent to its contrapositive (as proven in Appendix B):

$$(p \Rightarrow q) \iff (\textbf{\textit{not}}\, q \Rightarrow \textbf{\textit{not}}\, p).$$

Later, if we want to prove that the statement $p \Rightarrow q$ is true, we can do so by proving its contrapositive. Similarly, the converse and the inverse of an implication are logically equivalent, and thus they are either both true or both false. We saw this demonstrated above with regards to differentiability versus continuity.

The contrapositive of an equivalence $p \iff q$ is also an equivalence, so we do not have to bother with changing the position of p and q. An equivalence is again equivalent to its contrapositive:

$$(p \iff q) \iff (\textbf{\textit{not}}\, p \iff \textbf{\textit{not}}\, q).$$

Logical Operations

We can combine two logical statements using the common words ***and*** and ***or***:

Definition: If p and q are logical statements, we can form their ***conjunction:***

$$p \textbf{\textit{ and }} q,$$

and their ***disjunction:***

$$p \textbf{\textit{ or }} q.$$

The conjunction p ***and*** q is true precisely if ***both*** conditions p and q are true. Similarly, the disjunction p ***or*** q is true precisely if ***either*** condition p or q is true (or possibly both are true).

Example: The statement:

$$\sqrt{2} \text{ is irrational } \textbf{\textit{and}} \text{ bigger than } 1.$$

is a ***true*** statement. However, the statement:

Every real number is either positive ***or*** negative.

is ***false*** because the real number 0 is neither positive nor negative.□

The negation of a conjunction or a disjunction is sometimes needed in order to understand a Theorem, or more importantly, to prove it. Fortunately, the following Theorem allows us to simplify these compound negations:

Theorem — De Morgan's Laws: For all logical statements p and q:

$$\textbf{\textit{not}}\,(p\ \textbf{\textit{and}}\ q) \Leftrightarrow (\textbf{\textit{not}}\,p)\ \textbf{\textit{or}}\ (\textbf{\textit{not}}\,q), \quad \text{and}$$

$$\textbf{\textit{not}}\,(p\ \textbf{\textit{or}}\ q) \Leftrightarrow (\textbf{\textit{not}}\,p)\ \textbf{\textit{and}}\ (\textbf{\textit{not}}\,q).$$

Note that De Morgan's Laws look very similar to the Distributive Property (with a slight twist), and in fact they are precisely that in the study of ***Boolean Algebras***.

De Morgan's Laws are proven in Appendix B.

Subsets and Set Operations

We can compare two sets and perform operations on two sets to create new sets.

Definitions: We say that a set X is a ***subset*** of another set Y if every member of X is also a member of Y. We write this symbolically as:

$$X \subseteq Y \Leftrightarrow (x \in X \Rightarrow x \in Y).$$

If X is a subset of Y, we can also say that X is ***contained*** in Y, or Y ***contains*** X. We can visualize sets and subsets using ***Venn Diagrams*** as follows:

We say X ***equals*** Y if X is a subset of Y and Y is a subset of X:

$$(X = Y) \Leftrightarrow \left(X \subseteq Y\ \textbf{and}\ Y \subseteq X\right).$$

Equivalently, every member of X is also a member of Y, and every member of Y is also a member of X:

$$(X = Y) \Leftrightarrow \left(x \in X \Rightarrow x \in Y\ \textbf{and}\ y \in Y \Rightarrow y \in X\right).$$

We combine two sets into a single set that contains precisely all the members of the two sets using the ***union*** operation:

$$X \cup Y = \left\{z \middle| z \in X\ \textbf{\textit{or}}\ z \in Y\right\}.$$

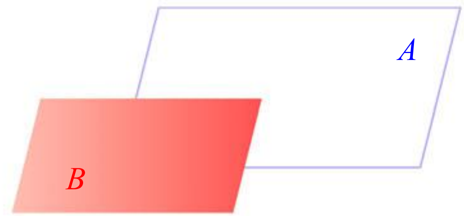
We determine all members common to both sets using the ***intersection*** operation:

$$X \cap Y = \left\{z \middle| z \in X\ \textbf{\textit{and}}\ z \in Y\right\}.$$

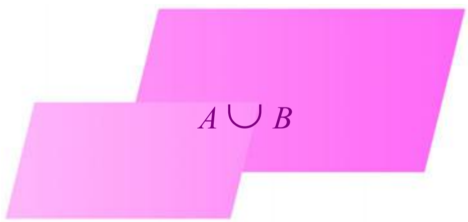
We can also take the ***difference*** or ***complement*** of two sets:

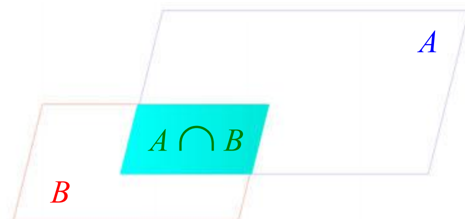
$$X - Y = \left\{z \middle| z \in X\ \textbf{\textit{and}}\ z \notin Y\right\}.$$

Notice the use of ***or*** and ***and*** in the definitions. We can also visualize these set operations using Venn diagrams. We first show two sets A and B below, highlighted separately for clarity:



Next, we show their union $A \cup B$, and their intersection $A \cap B$:





Finally, we show the two complements, $A - B$ and $B - A$:

Example: Suppose we have the sets (expressed in roster notation):

$$\begin{aligned} A &= \{b, d, e\}, \\ B &= \{a, b, c, d, e, f\}, \\ C &= \{c, e, h, k\}, \quad \text{and} \\ D &= \{d, e, g, k\}. \end{aligned}$$

Then $A \subseteq B$ because every member of A is also a member of B, and there are no other subset relationships among the four sets. Now, let us compute the following set operations:

$$\begin{aligned} C \cup D &= \{c, e, h, k\} \cup \{d, e, g, k\} = \{c, d, e, g, h, k\}, \\ C \cap D &= \{c, e, h, k\} \cap \{d, e, g, k\} = \{e, k\}, \\ C - D &= \{c, e, h, k\} - \{d, e, g, k\} = \{c, h\}, \quad \text{and} \\ D - C &= \{d, e, g, k\} - \{c, e, h, k\} = \{d, g\}. \end{aligned}$$

As a special bonus, notice that:

$$C \cup D = \{c, d, e, g, h, k\} = \{e, k\} \cup \{c, h\} \cup \{d, g\} = (C \cap D) \cup (C - D) \cup (D - C). \square$$

In the course of developing Linear Algebra, we will not just consider sets of real numbers, but also sets of ***vectors***, notably the Euclidean Spaces from Chapter 1, sets of ***polynomials***, and more generally, sets of ***functions*** (such as continuous functions and differentiable functions), and sets of ***matrices***. We will be gradually constructing these objects over time.

Part II: Proofs

Perhaps the most challenging task that you will be asked to do in Linear Algebra is to prove a Theorem. To accomplish this, you need to know what is expected of you:

> ***Definition:*** A ***proof*** for a Theorem is a sequence of true logical statements which ***convincingly*** and ***completely explains*** why a Theorem is true.

In many ways, a proof is very similar to an ***essay*** that you write for a course in Literature or History. It is also similar to a ***laboratory report***, say in Physics or Chemistry, where you have to logically analyze your data and defend your conclusions.

The main difference, though, is that every logical statement in a proof should be true, and must follow as a conclusion from a previously established true statement.

The method of reasoning that we will use is a method of deductive reasoning which is formally called ***modus ponens***. It basically works like this:

> Suppose you already know that an implication $p \Rightarrow q$ is true.
>
> Suppose you also established that condition p is satisfied.
>
> Therefore, it is logical to conclude that condition q is also satisfied.

Example: Let us demonstrate modus ponens on the following logical argument:

> In Calculus, we proved that:
> ***if*** $f(x)$ is a continuous odd function on $[-a, a]$, ***then*** $\int_{-a}^{a} f(x)\,dx = 0$.
>
> The function $f(x) = \sin^5(x)$ is continuous on $\mathbb{R}$, because it is the composition of two continuous functions. It is an odd function on $[-\pi/4, \pi/4]$, since:
>
> $$\sin^5(-x) = (-\sin(x))^5 = -\sin^5(x),$$
>
> where we used the odd property of both the sine function and the fifth power function.
>
> Therefore, $\int_{-\pi/4}^{\pi/4} \sin^5(x)\,dx = 0$. □

Notice that this reasoning allows us to compute this definite integral without the inconvenience of finding an antiderivative and applying the Fundamental Theorem of Calculus!

A proof often begins by understanding the ***meaning*** of the given conditions and the conclusion that you are supposed to reach. It is therefore important that you can recall and state the ***definitions*** of a variety of ***words*** and ***phrases*** that you will encounter in your study of Linear Algebra. After all, it would be impossible for you to explain how you obtained your conclusion if you do not even know what the conclusion is supposed to mean. We also use special ***symbols*** and ***notation***, so you must be familiar with them. Often, a previously proven Theorem can also be helpful to prove another Theorem. Start by ***identifying*** what is ***given*** (the hypotheses), and what it is that we want to ***show*** (the conclusion).

Rest assured, you will be shown examples which demonstrate proper techniques and reasoning, which you are encouraged to emulate as you learn and develop your own style. In the meantime, we present below some examples of general ***strategies*** and ***techniques*** which will be useful in the coming Chapters. These strategies are certainly not exhaustive: we sometimes combine several strategies to prove a Theorem, and the more difficult Theorems require a ***creative spark***. For our first example, though, let us see how to prove a Theorem using only the Axioms of the Real Number System:

Example: Let us prove the following:

> ***Theorem — The Multiplicative Property of Zero:*** For all $a \in \mathbb{R}$:
>
> $$0 \cdot a = 0 = a \cdot 0.$$

Proof: Suppose that a is any real number. We want to show that $0 \cdot a = 0$. If we can do this, then we can also conclude by the commutative property of multiplication that $a \cdot 0 = 0$ as well.

We will use a clever idea. We know the ***Identity Property*** of 0, that is, for all $x \in \mathbb{R}$:

$$0 + x = x = x + 0.$$

Since this is true for all real x, it is true in particular for $x = 0$, so we get:

$$0 + 0 = 0.$$

Now, if we multiply both sides of this equation by a, we get the equation:

$$(0 + 0) \cdot a = 0 \cdot a.$$

This equation is again a true equation because of the following Axiom:

> ***Axiom — The Substitution Principle:***
> If $x, y \in \mathbb{R}$ and $F(x)$ is an arithmetic expression involving x, and $x = y$, then $F(x) = F(y)$.

Simply put, if two quantities are the same, and we do the same arithmetic operations to both quantities, then the resulting quantities are still the same. Continuing now, by the ***Distributive Property***, we get:

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

Remember that we want to know exactly what $0 \cdot a$ is. All we know is that $0 \cdot a$ is ***some*** real number, by the ***Closure Property of Multiplication***. Thus it possesses an additive inverse, $-(0 \cdot a)$, by the ***Existence of Additive Inverses***. Let us add this to both sides of the equation:

$$-(0 \cdot a) + (0 \cdot a + 0 \cdot a) = -(0 \cdot a) + 0 \cdot a.$$

By the defining property of the additive inverse, $-(0 \cdot a) + 0 \cdot a = 0$, so we get:

$$-(0 \cdot a) + (0 \cdot a + 0 \cdot a) = 0.$$

But now, by the ***Associative Property of Addition***, the left side is:

$$(-(0 \cdot a) + 0 \cdot a) + 0 \cdot a = 0.$$

Thus, by the additive inverse property, as above, we get:

$$0 + (0 \cdot a) = 0.$$

(we enclosed $0 \cdot a$ in parentheses to emphasize that it is the quantity we are trying to study in our equation). Finally, by the additive property of 0 again, the left side reduces to $0 \cdot a$, so we get:

$$0 \cdot a = 0. \blacksquare$$

Case-by-Case Analysis

We can prove the implication $p \Rightarrow q$ if we can break down p into two or more cases, and every possibility for p is covered by at least one of the cases. If we can prove that q is true in ***each case***, the implication is true. This is also sometimes called ***Proof by Exhaustion***.

Example: Let us prove the following:

> ***Theorem — The Zero-Factors Theorem:*** For all $a, b \in \mathbb{R}$:
>
> $a \cdot b = 0$ ***if and only if*** either $a = 0$ ***or*** $b = 0$.

Proof: Since this is an ***if and only if*** Theorem, we must prove two implications. Let us begin with the converse, which is easier:

($\Leftarrow$) Suppose we are given that either $a = 0$ ***or*** $b = 0$. We must show that $a \cdot b = 0$. Since there are two possibilities for the given conditions, we have the following cases:

Case 1. If $a = 0$, then $a \cdot b = 0 \cdot b = 0$ by our previous Theorem.

Case 2. If $b = 0$, then $a \cdot b = a \cdot 0 = 0$, which is the exact same reasoning as Case 1.

Thus, if either $a = 0$ ***or*** $b = 0$, then $a \cdot b = 0$.

($\Rightarrow$) Suppose we are given that $a \cdot b = 0$. We must show that either $a = 0$ ***or*** $b = 0$.

Case 1. Suppose that $a = 0$. Then we are done, since the conclusion "$a = 0$ ***or*** $b = 0$" is satisfied.

Case 2. Suppose that $a \neq 0$. Notice that since this is the exact opposite of Case 1, we have covered ***all*** the possibilities. Now, since a is non-zero, by Axiom 11, it has a ***Multiplicative Inverse*** $1/a$. We are given that:

$$a \cdot b = 0.$$

By ***The Substitution Principle***, we can multiply both sides of the equation by $1/a$ and obtain:

$$(1/a) \cdot (a \cdot b) = (1/a) \cdot 0.$$

Since $1/a$ is again another real number, the right side of this equation is 0, as we already saw above. Now, the left side can be regrouped using Axiom 6, the ***Associative Property of Multiplication***. Thus, we get:

$$(1/a \cdot a) \cdot b = 0.$$

By the ***Multiplicative Inverse Property***, the product of a non-zero number and its reciprocal is 1, so we obtain: $1 \cdot b = 0$.

Finally, by Axiom 9, $1 \cdot b = b$, and thus we get: $b = 1 \cdot b = 0$.

Thus, if $a \neq 0$, then $b = 0$, completing the proof that either $a = 0$ ***or*** $b = 0$.

Notice that the two Cases for the forward implication are different from the two Cases for the converse. This frequently happens. $\blacksquare$

Proof by Contrapositive

We mentioned earlier that an implication $p \Rightarrow q$ is logically equivalent to its contrapositive, which is ***not*** $q \Rightarrow$ ***not*** p. Thus it may be worthwhile to write down the contrapositive of the Theorem we want to prove, and see if we get any ideas on how to prove it. This is the basic idea behind the technique called ***Proof by Contrapositive***, which is also known in Latin as ***modus tollens***.

The example we will discuss below deals with the set of integers, $\mathbb{Z}$. In order to fully appreciate this example, we need to introduce the following Axioms for $\mathbb{Z}$:

> ***Axioms — Closure Axioms for the Set of Integers:***
> If $a,\ b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$, $a-b \in \mathbb{Z}$, and $a \cdot b \in \mathbb{Z}$ as well.

> ***Definitions — Even and Odd Integers:***
> An integer $a \in \mathbb{Z}$ is ***even*** if there exists $c \in \mathbb{Z}$ such that $a = 2c$.
> An integer $b \in \mathbb{Z}$ is ***odd*** if there exists $d \in \mathbb{Z}$ such that $a = 2d+1$.

It is easy to see from these two definitions that every integer is either even or odd, but not both. Now we are ready:

Example: Let us prove the following using the technique of Proof by Contrapositive:

> ***Theorem:*** For all $a,\ b \in \mathbb{Z}$:
> If the product $a \cdot b$ is ***odd***, then ***both*** a and b are ***odd***.

Proof: Our first step is to write the contrapositive. The conclusion is "both a and b are odd." Since the word ***and*** is in this phrase, we can use De Morgan's Laws to simplify its negation:

not (both a ***and*** b are odd) $\Leftrightarrow$
(a is ***not*** odd) ***or*** (b is ***not*** odd) $\Leftrightarrow$
a is even ***or*** b is even.

Thus, the contrapositive of the Theorem we want to prove is:

> ***Theorem:*** For all $a,\ b \in \mathbb{Z}$:
> If a is even ***or*** b is even, then $a \cdot b$ is even.

This statement is easier to prove, and all we need is a Case-by-Case analysis:

Case 1. Suppose that a is even. Then a has the form $a = 2 \cdot c$ for some integer c. Thus:

$$a \cdot b = (2 \cdot c) \cdot b = 2 \cdot (c \cdot b),$$

by the Associative Property of Multiplication. Since $c \cdot b \in \mathbb{Z}$ by Closure, $2 \cdot (c \cdot b)$ is even. Thus, $a \cdot b$ is even. A similar argument works for ***Case 2***, where we assume that b is even.■

Proof by Contradiction

The method of ***Proof by Contradiction*** (or ***reductio ad absurdum***) is often used in order to show that an object does not exist, or in situations when it is difficult to show that an implication is true directly. The idea is to assume that the mythical object does exist, or more generally, the opposite of the conclusion is true. In the course of our reasoning, we should arrive at a condition which ***contradicts*** one of the given conditions, or a condition which has already been concluded to be true (thus producing an ***absurdity*** or contradiction). The only problem with attempting a proof by contradiction is that it is ***not guaranteed*** that you will eventually encounter a contradiction. As in all techniques, give it a ***try***.

Example: One of the best applications of Proof by Contradiction is the classic proof of the following:

> ***Theorem:*** The real number $\sqrt{2}$ is ***irrational***.

Proof: Let us assume the ***opposite*** of the conclusion, that is, $\sqrt{2}$ is ***rational***. Thus, we can write:

$$\sqrt{2} = \frac{a}{b}, \text{ where } a \text{ and } b \text{ are positive } \textbf{\textit{integers}}.$$

We must make one important requirement to make the proof work: recall from basic Arithmetic that every fraction can be reduced to ***lowest form***, so we will require that a and b have ***no common factor*** except of course for 1. Now, squaring both sides of this equation, we get: $2 = a^2/b^2$, or $a^2 = 2b^2$.

This last equation tells us that a^2 must be an ***even*** number. But if a^2 is even, then a itself has to be even. To see this convincingly, we can also use Proof by Contradiction: if a^2 were even but a were odd, then $a = 2d + 1$ for some integer d, and we get:

$$a^2 = (2d+1)^2 = 4d^2 + 4d + 1 = 2(2d^2 + 2d) + 1.$$

Since $2d^2 + 2d$ is an integer, a^2 is ***odd***. Thus, we get a contradiction, and so a must be even. Now, we can write $a = 2m$, where m is an integer, and substituting this in the equation $a^2 = 2b^2$, we get:

$$(2m)^2 = 2b^2 \quad \text{or} \quad 4m^2 = 2b^2 \quad \text{or} \quad b^2 = 2m^2.$$

Thus b^2 is also even, and by the same reasoning above, b itself must be even. Therefore, the equation $\sqrt{2} = a/b$ led us to the conclusion that ***both*** a and b are even. This violates the requirement that a and b have no common factor aside from 1. We have reached a contradiction, and so our assumption that $\sqrt{2}$ is rational had to be ***false***, and so its opposite is ***true***: $\sqrt{2}$ must be ***irrational***.■

Proof by Induction

Another technique which is useful in Linear Algebra is the ***Principle of Mathematical Induction***. The Theorems that "induction" (as it is more briefly called) applies to are often about natural numbers or positive integers. Since this statement refers to an integer n, we often write the statement as $\boldsymbol{p(n)}$. As this is seen in Precalculus, let us use an example to review how this technique works.

Example: Use the Principle of Mathematical Induction to prove the following formula:

> ***Theorem:*** For all positive integers n: $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Proof: Induction is accomplished in three major steps:

1. The Basis Step. We will first prove that the statement is true when $n = 1$, that is, $p(1)$ is true. The left side of the equation thus stops at 1^2. The right side is:

$$\frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1,$$

so $p(1)$ is indeed true.

2. The Inductive Hypothesis. In this step, we will simply ***assume*** that the statement is true when n is some positive integer k. In other words, we assume that $p(k)$ is true.

Thus, we rewrite the equation in the statement by replacing n with k:

The Inductive Hypothesis: Assume:

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Notice that since we have already done Step 1, we have the right to make this assumption, because we have proven it to be true for at least one instance: $k = 1$.

3. The Inductive Step. This is of course where most of the hard work comes in. We must now show that the statement is still true when $n = k+1$, or in other words, that $p(k+1)$ is true.

We begin this step by stating $p(k+1)$, so that we explicitly see what it is we need to prove. Thus, we replace n with $k+1$ (in this case, ***four*** times):

The Inductive Step: Prove:

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+1+1)(2[k+1]+1)}{6}.$$

Notice that the left side of the equation now has ***one more term*** at the end. Now, we can proceed to prove that this equation is true. The Inductive Hypothesis tells us that the first k terms on the left side of this equation can be replaced, as follows:

$$\begin{aligned}
&1^2 + 2^2 + \cdots + k^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{(by the Inductive Hypothesis)} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} && \text{(combining fractions)} \\
&= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} && \text{(factoring out } k+1\text{)} \\
&= \frac{(k+1)[2k^2 + k + 6k + 6]}{6} && \text{(distributing the parentheses)} \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6}.
\end{aligned}$$

However, the right side of our equation in the Inductive Step is:

$$\begin{aligned} & \frac{(k+1)(k+1+1)(2[k+1]+1)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} && \text{(simplifying)} \\ &= \frac{(k+1)(2k^2+4k+3k+6)}{6} && \text{(distributing two factors)} \\ &= \frac{(k+1)(2k^2+7k+6)}{6}, \end{aligned}$$

thus proving that both sides of $p(k+1)$ are the same. This completes our Proof by Induction.■

Why does this reasoning make sense? We were able to show that the Theorem is true if $n = 1$. If we put Steps 2 and 3 together, then we know that if the statement is true when $n = k$, then it is also true when $n = k+1$. Since we knew that the statement was true when $n = 1$, by modus ponens, it is also true when $n = 2$. But now that we know it is also true when $n = 2$, again, by modus ponens, it is also true when $n = 3$. And so on!

Conjectures and Demonstrations

It might shock you to know that there are ***many*** statements in mathematics which have not been determined to be true or false. They are called ***conjectures***. However, we can try to ***demonstrate*** that it is ***plausible*** for the conjecture to be true by giving examples where the conjecture is satisfied. These demonstrations are ***not*** replacements for a complete proof.

Example: Perhaps the most famous, and certainly one of the oldest and most easily stated conjectures of mathematics is called ***Goldbach's Conjecture***. It was stated in 1742 by the Prussian mathematician Christian Goldbach, in a letter to the great Leonhard Euler. The modern statement is as follows:

> ***Goldbach's Conjecture:*** Every ***even integer*** bigger than 2 can be expressed as the sum of ***two prime numbers***.

We can demonstrate that this conjecture is plausible with the examples:

$$18 = 13 + 5 \quad \text{and} \quad 50 = 3 + 47.$$

Goldbach's Conjecture has been verified for a large range of positive even numbers, but experts feel that we are still a long way from proving it in general.□

Unfortunately, most modern conjectures cannot be understood unless one has spent years studying the background material of their associated fields. Their pursuit falls within the realm of ***mathematical research***. As you learn to understand and prove basic Theorems in Linear Algebra, your skills in learning to read Theorems and prove Theorems on your own will improve over time. It is possible that someday, you will prove a deep and complicated Theorem that nobody has ever proven before.

Chapter Zero Summary:

A ***set*** is an unordered collection of objects called ***elements***. Important sets include the empty set ϕ, the sets of natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, and real numbers $\mathbb{R}$.

A ***logical statement*** is a sentence which can be determined to be either ***true*** or ***false***. An ***Axiom*** is a logical statement that we will ***accept*** as true. The ***negation*** of the logical statement p, written as ***not*** p, is true exactly when p is false.

Universal quantifiers are the words ***for any, for all*** and ***for every***. ***Existential quantifiers*** are the phrases ***there is*** and ***there exists*** or their plural forms ***there are*** and ***there exist***.

The ***Field Axioms*** for the set of Real Numbers describe eleven important properties that we agree the set of real numbers possesses.

A true logical statement which is not just an Axiom is called a ***Theorem***. An ***implication*** has the form: ***if*** p ***then*** q, written symbolically as $p \Rightarrow q$. An implication can be demonstrated to be ***false*** by giving a ***counterexample***, a situation where p is true, but q is false.

The ***negation*** of the logical statement p, written as ***not*** p, is true exactly when p is false.

For an implication $p \Rightarrow q$, we call $q \Rightarrow p$ the ***converse*** of $p \Rightarrow q$, ***not*** $p \Rightarrow$ ***not*** q the ***inverse*** of $p \Rightarrow q$, and ***not*** $q \Rightarrow$ ***not*** p the ***contrapositive*** of $p \Rightarrow q$.

If $p \Rightarrow q$ and $q \Rightarrow p$ are ***both*** true, then we say that p and q are ***equivalent*** to each other. We write the ***equivalence*** or ***double-implication*** $p \Leftrightarrow q$, pronounced as p ***if and only if*** q.

The implication $p \Rightarrow q$ is equivalent to its contrapositive ***not*** $q \Rightarrow$ ***not*** p.

The ***conjunction*** p ***and*** q is true precisely if ***both*** conditions p and q are true.

The ***disjunction*** p ***or*** q is true precisely if ***either*** condition p or q is true.

De Morgan's Laws: For all logical statements p and q: ***not*** $(p \textbf{ and } q)$ is logically equivalent to $(\textbf{not } p)$ ***or*** $(\textbf{not } q)$, and similarly, ***not*** $(p \textbf{ or } q)$ is logically equivalent to $(\textbf{not } p)$ ***and*** $(\textbf{not } q)$.

A set X is a ***subset*** of another set Y if every member of X is also a member of Y. We write this symbolically as $X \subseteq Y$. Two sets X and Y are ***equal*** if X is a subset of Y and Y is a subset of X, or equivalently, every member of X is also a member of Y, and vice versa:

$$(X = Y) \Leftrightarrow (X \subseteq Y \textbf{ and } Y \subseteq X) \Leftrightarrow (x \in X \Rightarrow x \in Y \textbf{ and } y \in Y \Rightarrow y \in X).$$

Given two sets X and Y, we can find:

- their ***union:*** $X \cup Y = \{z \mid z \in X \textbf{ or } z \in Y\}$;
- their ***intersection:*** $X \cap Y = \{z \mid z \in X \textbf{ and } z \in Y\}$; and
- their ***difference*** or ***complement:*** $X - Y = \{z \mid z \in X \textbf{ and } z \notin Y\}$.

A ***proof*** for a Theorem is a sequence of true logical statements which ***convincingly*** and ***completely explains*** why a Theorem is true.

A good way to begin a proof is by identifying the given conditions and the conclusion that we want to show. It is also a good idea to write down definitions for terms that are found in the Theorem. The main logical technique in writing proofs is ***modus ponens***. We also use techniques such as:

- Case-by-Case Analysis
- Proof by Contrapositive
- Proof by Contradiction
- Proof by Mathematical Induction.

Chapter Zero Exercises

For Exercises (1) to (6): Decide if the following statements are logical statements or not, and if a statement is logical, classify it as True or False.

1. If x is a real number and $|x| < 3$, then $-3 < x < 3$.
2. If x and y are real numbers and $x < y$, then $x^2 < y^2$.
3. If x and y are real numbers and $0 < x < y$, then $1/y < 1/x$.
4. Every real number has a square root which is also a real number.
5. As of March 2016, Roger Federer holds the record for the most number of consecutive weeks as the world's number 1 tennis player.
6. The Golden State Warriors are the best team in the NBA. Why is this different from Exercise 5?

For Exercises (7) to (10): Write the converse, inverse and contrapositive of the following:

7. If you do your homework before dinner, you can watch TV tonight.
8. If it rains tomorrow, we will not go to the beach.
9. If $0 \leq x \leq \pi/2$, then $\cos(x) \geq 0$. (challenge: write the inverse and contrapositive without using the word "not")
10. If $f(x)$ is continuous on the closed interval $[a,b]$ then $f(x)$ possesses both a maximum and a minimum on $[a,b]$.

For Exercises (11) and (12): For the sets A and B, find $A \cup B$, $A \cap B$, $A - B$ and $B - A$:

11. $A = \{a,c,f,h,i,j,m\}$, $B = \{b,c,g,h,j,p,q\}$.
12. $A = \{a,d,g,h,j,p,r,t\}$, $B = \{b,d,g,h,k,p,q,s,t,v\}$.

For Exercises (13) to (22): Prove the following Theorems concerning Real Numbers using only the 11 Field Axioms (and possibly Theorems that were proven in Chapter Zero). Specify in your proof which Axiom or Theorem you are using at ***each*** step.

13. Prove ***The Cancellation Law for Addition:*** For all $x, y, c \in \mathbb{R}$:

$$\text{If } x + c = y + c, \text{ then } x = y.$$

14. Prove ***The Cancellation Law for Multiplication:*** For all $x, y, k \in \mathbb{R}$, $k \neq 0$:

$$\text{If } k \cdot x = k \cdot y, \text{ then } x = y.$$

15. Use The Multiplicative Property of Zero to prove that 0 ***cannot*** have a multiplicative inverse. Hint: Use Proof by Contradiction: Suppose 0 ***has*** a multiplicative inverse x. . .
16. Prove ***The Uniqueness of Additive Inverses:*** Suppose $x \in \mathbb{R}$. If $w \in \mathbb{R}$ is any real number with the property that $x + w = 0 = w + x$, then $w = -x$. In other words, $-x$ is the only real number that satisfies the above equations.
17. Use the previous Exercise to show that $-0 = 0$. Hint: which Field Axiom tells us what $0 + 0$ is?
18. Use the Uniqueness of Additive Inverses to prove that for all $x \in \mathbb{R}$: $-x = (-1) \cdot x$. Hint: simplify $x + (-1) \cdot x$.
19. ***The Double Negation Property:*** Use some of the previous Exercises to show that: For all $x \in \mathbb{R}$: $-(-x) = x$.
20. Prove ***The Uniqueness of Multiplicative Inverses:*** Suppose $x \in \mathbb{R}$ and $x \neq 0$. If $y \in \mathbb{R}$ is any real number with the property that $x \cdot y = 1 = y \cdot x$, then $y = 1/x$. In other $1/x$ is the only real number that satisfies the above equations.

21. Prove ***The Double Reciprocal Property:*** For all $x \in \mathbb{R}$, $x \neq 0$: $1/(1/x) = x$.

22. ***Solving Algebraic Equations:*** Prove that for all $x, a, b \in \mathbb{R}$:

    a. if $x + a = b$, then $x = b - a$.

    b. if $a \neq 0$ and $ax = b$, then $x = b/a$.

23. Prove by Contradiction that there is no ***largest*** positive real number.

24. Prove by Contradiction that there is no ***smallest*** positive real number.

25. Suppose that $n \in \mathbb{Z}$ and n factors as $n = a \cdot b$, where $a, b \in \mathbb{Z}$ and both are positive. Use Proof by Contradiction to show that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

26. Use the previous Exercise to prove: If n is ***not*** a prime number (that is, n is ***composite***), then n has a prime factor which is at most $\sqrt{n}$.

27. Write the contrapositive of the statement in the previous Exercise. Use this to decide if 11303 is prime or composite.

    For Exercises (28) to (31): Use the technique of Proof by Contrapositive to prove the following statements. You may use De Morgan's Law to simplify the contrapositive, when applicable:

28. For all $a, b \in \mathbb{Z}$: if $a \cdot b$ is even, then either a is even ***or*** b is even.

29. For all $a, b \in \mathbb{Z}$: if $a + b$ is even, then either a and b are both odd ***or*** both even.

30. For all $a \in \mathbb{Z}$: a^2 is even ***if and only if*** a is even.

31. For all $x, y \in \mathbb{R}$: if $x \cdot y$ is irrational, then either a is irrational ***or*** b is irrational.

    Negating Statements with Quantifiers: A logical statement that begins with a quantifier is negated as follows: ***not*** $(\forall x : p)$ is equivalent to: $\exists x$: ***not*** (p). This should make sense: if it is ***not true*** that ***all*** x possess property p, then ***at least one*** x does ***not*** possess property p.

    Similarly: ***not*** $(\exists x : p)$ is equivalent to: $\forall x$: ***not*** (p).

    Thus, the negation of "All of my friends are Democrats" is "One of my friends is not a Democrat." Notice that "None of my friends are Democrats" is wrong.

    Similarly, the negation of "One of my brothers is left-handed" is "All of my brothers are right-handed." It is not "One of my brothers is right-handed."

    For Exercises (32) to (35): Write the negation of the following statements, and determine whether the original statement or its negation is true:

32. Every real number x has a multiplicative inverse $1/x$.

33. There exists a real number x such that $x^2 < 0$.

34. There exists a negative number x such that $x^2 = 4$.

35. All prime numbers are odd.

36. Demonstrate Goldbach's Conjecture using: $130 = ? + ?$

37. Rewrite Goldbach's Conjecture using the quantifiers "for every" and "there exist."

38. ***The Twin Prime Conjecture:*** Twin primes are pairs of prime numbers that differ only by 2. For example, $(11, 13)$ are twin primes, as are $(41, 43)$. The Twin Prime Conjecture states that there are an ***infinite*** number of twin primes. What are the next years after 2016 that are twin primes?

39. ***The Fibonacci Prime Conjecture:*** The ***Fibonacci Numbers*** are those in the infinite sequence:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ \ldots$$

    where the next number (starting with the third) is the sum of the previous two numbers. Notice that 2, 3, 5, 13 and 89 are primes that appear in this sequence, so they are called ***Fibonacci Primes***. The Fibonacci Prime Conjecture states that there are an infinite number of Fibonacci primes. Find the next Fibonacci prime after 89.

For Exercises (40) to (49): Prove the following by Mathematical Induction:
For all positive integers n:

40. $1^2 + 3^2 + \cdots + (2n-1)^2 = \dfrac{n(2n+1)(2n-1)}{3}$
41. $1^3 + 2^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$
42. $1^3 + 3^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$
43. $1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3}$
44. $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$
45. $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n \cdot (n+1)} = \dfrac{n}{n+1}$
46. $\dfrac{1}{1 \cdot 3} + \dfrac{1}{3 \cdot 5} + \cdots + \dfrac{1}{(2n-1) \cdot (2n+1)} = \dfrac{n}{2n+1}$
47. $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = 2[(n-1)2^n + 1]$
48. $1 \cdot 3 + 2 \cdot 3^2 + 3 \cdot 3^3 + \cdots + n \cdot 3^n = \frac{3}{4}[(2n-1)3^n + 1]$
49. $n < 2^n$ (this might require a little bit of creativity in Step 3).
50. An ***n-gon*** is a polygon with n vertices (thus a triangle is a 3-*gon* and a quadrilateral is a 4-*gon*). We know from basic geometry that the sum of the angles of any triangle is 180^0. Use Induction to prove that the sum of the interior angles of a convex *n-gon* is $(n-2) \cdot 180^0$ (a polygon is ***convex*** if any line segment connecting two points inside the polygon is entirely within the polygon). Hint: in the inductive step, cut out a triangle using three consecutive vertices. Draw some pictures.
51. Suppose that A and B are subsets of X. Prove that $A \cap B$ is the ***largest*** subset of X which is ***contained*** in both A and B. In other words, prove that if $C \subset A$ and $C \subset B$, then $C \subset A \cap B$.
52. Suppose that A and B are any two subsets of a set X. Prove that $A \cup B$ is the ***smallest*** subset of X which ***contains*** both A and B. In other words, prove that if $A \subset D$ and $B \subset D$, then $A \cup B \subset D$.
53. Suppose that A and B are any two sets. Prove that (a) $(A - B) \cap B = \emptyset$, and (b) $A \cup B = (A \cap B) \cup (B - A) \cup (A - B)$, and each of the three sets in this union have no element in common with the other two. Hint: draw a diagram.
54. ***Properties of Set Union and Intersection:***
    a. If X and Y are two sets, write down the definition of $X \cup Y$.
    b. Similarly, write down the definition of $X \cap Y$.
    c. If A and B are two sets, write down what it means for A to be a subset of B, that is $A \subseteq B$.
    d. Similarly, what does it mean for $A = B$?
    e. Now, use the previous parts to prove that $X \subseteq X \cup Y$ ***and*** $Y \subseteq X \cup Y$
    f. State and prove a similar statement regarding X, Y and $X \cap Y$.
    g. Prove that $X \subseteq Y$ ***if and only if*** $Y = X \cup Y$.
    h. Similarly, prove that $X \subseteq Y$ ***if and only if*** $X = X \cap Y$. Notice that it is now X on the left side of the equation.

55. ***The Method of Descent:*** The Principle of Mathematical Induction goes ***forward***, that is, we start with proving the case when $n = 1$, then we assume that the case when $n = k$ is true, and finally we prove that the case when $n = k + 1$, that is, the next ***bigger*** case, is also true. However, sometimes it is useful to go ***backwards*** instead of forward. This is possible because 1 is the ***smallest*** positive integer, and thus if we start with a positive integer n and go lower and lower, we will eventually hit 1 and then we cannot go any lower. We will illustrate this idea, formally called The Method of Infinite Descent or more simply as The Method of Descent, to prove:

Every integer N which is bigger than 1 is either ***prime***

or has a prime factor q which is ***less than*** N.

Recall that an integer p is prime if $p > 1$ and the ***only way*** we can factor p into two positive integers as $p = a \cdot b$ is if ***either*** $a = 1$ and $b = p$ ***or*** $a = p$ and $b = 1$. For example, $7 = 1 \cdot 7 = 7 \cdot 1$, and there are no other ways to factor 7 into two positive integers. It is important to remember that 1 is ***not*** a prime number.

a. Warm-up: List down the first ten prime numbers.

b. Now, suppose N is an integer bigger than 1 and N is not prime. Use the definition above to show that we can factor N as $N = N_1 \cdot N$, where $1 < N_1 < N$ ***and*** $1 < N_2 < N$.

c. Explain why the proof is finished if ***either*** N_1 is prime or N_2 is prime.

d. Suppose now that ***neither*** N_1 nor N_2 is prime. We will ignore N_2 and focus our attention on N_1. Repeat the arguments above and factor N_1 as $N_1 = N_3 \cdot N_4$. What can we now say about N_3 and N_4?

e. We now come to the Method of Descent. Explain why we can keep performing this argument until we produce a list of positive integers: $N > N_1 > N_3 > \ldots$ and explain why this list must ***end*** with some prime number $N_k = q$ which divides N.

f. Explain why we ignored N_2 in part (d). Could we have ignored N_1 instead? How will this affect the list in (e)?

56. Use the previous Exercise to show that every positive integer N can be completely factored into primes: $N = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, for some finite set of primes $\{p_1, p_2, \ldots, p_k\}$.

Note that we take this property for granted when we are first learning Algebra. More precisely, every positive integer N can be factored ***uniquely*** into a product of primes, that is, any two factorizations into primes must have exactly the same primes appearing with the same frequency but possibly in a different order. This is known as the ***Fundamental Theorem of Arithmetic***, and could also be proven by the Method of Descent, but the proof is much more complicated.

57. ***The Infinitude of Primes:*** Our goal in this Exercise is to show that the set of prime numbers is ***infinite***. Thus, if the set of primes is $P = \{2, 3, 5, 7, 11, \ldots\}$, then this list will never terminate.

a. Warm-up: prove that if the integers a and b are both divisible by the integer c, then $a - b$ and $a + b$ are also divisible by c. (We say that an integer x is ***divisible*** by a non-zero integer y if x/y is also an integer).

Now, we will use Proof by Contradiction to prove our main goal. Suppose that P above is a ***finite set***, so the complete set of primes becomes $P = \{2, 3, 5, 7, 11, \ldots, p_L\}$ where p_L is the largest prime number. Let us construct the number $N = (2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_L) + 1$. We will proceed with a Case-by-Case Analysis:

b. Suppose that N is prime. Show that we have a contradiction and thus our proof is finished.

c. Now, suppose that N is not prime (thus we have considered both possibilities about N). The Exercise from The Method of Descent says that N must be divisible by a prime q which is smaller than N. Show that q is ***missing*** from the set P above, and explain why this is a contradiction and our proof is also finished. Hint: (a) could be useful.

58. ***Powersets:*** If $X = \{x_1, x_2, \ldots, x_n\}$ is a finite set, we define $\wp(X)$, the ***powerset*** of X, to be the set of all subsets of X. For example, if $X = \{a, b\}$, then $\wp(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, and thus $\wp(X)$ has 4 elements.

a. If $X = \{a, b, c\}$, list all the members of $\wp(X)$. How many subsets does X have?

b. Separate the list that you got in part (a) into two columns. Place on the left column those subsets that contain c and place on the right column those that do not contain c.

c. Now, ***cross out*** c from each subset on the left column. What do you notice?

d. Prove by induction that if $X = \{x_1, x_2, \ldots, x_n\}$, then $\wp(X)$ has 2^n elements. Hint: in the induction step, we want to show that the number of subsets of $\{x_1, x_2, \ldots, x_{k+1}\}$ is ***double*** the number of subsets of $\{x_1, x_2, \ldots, x_k\}$. Think of how to generalize parts (b) and (c).

e. Show that the set of subsets of a finite set X has strictly more members than X itself. Hint: Use one of the Exercises above on Induction.

59. The purpose of this Exercise is to prove that for any real number a:

$$\sqrt{a^2} = |a|.$$

Recall that the ***absolute value*** of any real number a is defined by:

$$|a| = \begin{cases} a & \text{if } a \geq 0, \text{ and} \\ -a & \text{if } a < 0. \end{cases}$$

We also know that the function $f(x) = x^2$ is not one-to-one on $(-\infty, \infty)$, but it is one-to-one if the domain is restricted to $[0, \infty)$. In this case, the range of $f(x)$ is also $[0, \infty)$, and so we will define the ***square root*** of a non-negative real number, $b \in [0, \infty)$, as:

$$\sqrt{b} = c, \text{ where } c \in [0, \infty), \text{ and } b = c^2.$$

a. Warm-up: use the definition above to explain why for any real number a: $|a| \geq 0$.

b. Again, using the definition, show that $|a|^2 = a^2$.

c. Our next goal is to show that $\sqrt{b}$ is ***unique***. In other words, prove that if c and d are two real numbers such that $c \geq 0$, and $d \geq 0$, and $b = c^2 = d^2$, then $c = d$. Hint: rewrite this equation into: $c^2 - d^2 = 0$ and use the Zero Factors Theorem.

d. Rewrite the definition for $\sqrt{b}$ to define $\sqrt{a^2}$.

e. Put together all the steps above to write a complete proof that $\sqrt{a^2} = |a|$.

Positive Numbers and the Order Axioms: In some of the Exercises above, we assumed that the reader was familiar with the basic properties of positive numbers and inequalities. We can formalize these properties with these additional ***Axioms for Positive Numbers:***

There exists a non-empty subset $\mathbb{R}^+ \subset \mathbb{R}$, consisting of the ***positive real numbers***, such that the following properties are accepted to be true:

a. ***Closure*** under Addition and Multiplication: If $x, y \in \mathbb{R}^+$, then $x + y \in \mathbb{R}^+$, and $x \cdot y \in \mathbb{R}^+$.

b. Zero is ***not*** positive: $0 \notin \mathbb{R}^+$.

c. ***The Dichotomy Property:*** If $x \neq 0$, then either $x \in \mathbb{R}^+$, or $-x \in \mathbb{R}^+$, but ***not*** both.

Using only these three Axioms, prove the following statements (as usual, an earlier Exercise can be used to prove a later Exercise, if applicable).

60. Prove that $1 \in \mathbb{R}^+$. Hint: Use Proof by Contradiction. Suppose instead $-1 \in \mathbb{R}^+$. What do the Closure properties and the Dichotomy Property tell us?
61. Use the previous Exercise to show that the set of positive integers $\{1, 2, 3, \ldots, n, n+1, \ldots\}$ is a subset of $\mathbb{R}^+$. Hint: use the Closure property, and Induction.
62. Prove the ***Reciprocal Property*** for $\mathbb{R}^+$: For all $x \in \mathbb{R}$, $x \neq 0$: $x \in \mathbb{R}^+$ ***if and only if*** $1/x \in \mathbb{R}^+$. See the hints in the two previous Exercises.

The Dichotomy Property creates another set, $\mathbb{R}^-$, consisting of the ***negative real numbers:***

$$\mathbb{R}^- = \{x \in \mathbb{R} \mid -x \in \mathbb{R}^+\}.$$

63. Notice that in the definition for $\mathbb{R}^-$, there is no mention of x being non-zero (unlike in The Dichotomy Property). Use Proof by Contradiction to prove that zero is ***not*** negative either.

This last Exercise tells us that we have three ***disjoint*** and exhaustive subsets of $\mathbb{R}$:

$$\mathbb{R} = \mathbb{R}^- \cup \{0\} \cup \mathbb{R}^+.$$

In other words, every real number is either negative, zero, or positive, and these three sets have no number in common.

64. Prove that $\mathbb{R}^-$ is Closed under Addition.
65. Prove that if $x, y \in \mathbb{R}^-$, then $x \cdot y \in \mathbb{R}^+$. Thus, $\mathbb{R}^-$ is ***not*** closed under Multiplication.
66. Prove that if $x \in \mathbb{R}^-$ and $y \in \mathbb{R}^+$, then $x \cdot y \in \mathbb{R}^-$.
67. Combine the Exercises above to prove: For all $x, y \in \mathbb{R}$:

$$x \cdot y \in \mathbb{R}^+ \ \textbf{\textit{if and only if}} \ x \text{ and } y \in \mathbb{R}^+ \ \textbf{\textit{or}} \ x \text{ and } y \in \mathbb{R}^-.$$

68. Prove the ***Reciprocal Property*** for $\mathbb{R}^-$: For all $x \in \mathbb{R}$, $x \neq 0$: $x \in \mathbb{R}^-$ ***if and only if*** $1/x \in \mathbb{R}^-$.

Next, the set $\mathbb{R}^+$ allow us to establish an ***ordering*** of the real numbers:

We will say that $x > y$ (in words: x is ***greater than*** y) if $x - y \in \mathbb{R}^+$. Similarly, $x < y$ (x is less than y) means $y > x$, $x \leq y$ means $x < y$ ***or*** $x = y$, and $x \geq y$ means $x > y$ ***or*** $x = y$. In the following statements, assume that $x, y, z \in \mathbb{R}$:

69. Prove that $x < y$ ***if and only if*** $x - y \in \mathbb{R}^-$.
70. Prove the ***Trichotomy Property: Exactly one*** of the following three possibilities is true: $x = y$, ***or*** $x < y$, ***or*** $y < x$.
71. Prove the ***Transitive Property:*** If $x > y$ and $y > z$, then $x > z$.
72. Prove that if $x < y$ and $z \in \mathbb{R}^+$, then $x \cdot z < y \cdot z$ and $x \cdot (-z) > y \cdot (-z)$.
73. Prove the ***Order Property for Reciprocals:*** For all $x, y \in \mathbb{R}$:

$$\text{If } x > 0 \ \textbf{\textit{and}} \ y > x, \text{ then } 1/x > 1/y.$$

$$\text{If } y < 0 \ \textbf{\textit{and}} \ y > x, \text{ then } 1/x > 1/y.$$

74. Prove the ***Squeeze Theorem for Inequalities:*** For all $x, y, z \in \mathbb{R}$:

$$\text{If } x \leq y \ \textbf{\textit{and}} \ y \leq x, \text{ then } x = y.$$

75. Let us define the imaginary unit i to be a number (or quantity) with the property that: $i^2 = i \cdot i = -1$. Prove that such a number ***cannot*** be a real number. Hint: if $i \in \mathbb{R}$, then either $i \in \mathbb{R}^+$ or $i \in \mathbb{R}^-$ or $i = 0$. Show that all these possibilities lead to a contradiction.

Chapter 1

The Canvas of Linear Algebra:

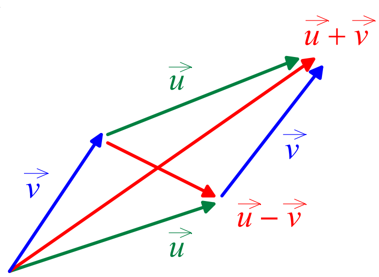
Euclidean Spaces and Subspaces

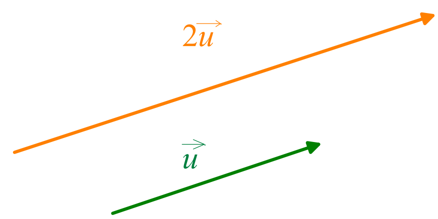
We study Calculus because we are interested in real numbers and functions that operate on them, such as polynomial, rational, radical, trigonometric, exponential and logarithmic functions. We want to study their graphs, derivatives, extreme values, concavity, antiderivatives, Taylor series, and so on..

In the same spirit, we define Linear Algebra as follows:

> ***Linear Algebra*** is the study of sets called ***vector spaces,*** which are generalizations of numbers, their ***structure***, and functions with special properties called ***linear transformations*** that map one vector space to another.

In this Chapter, we will look at the basic kind of vector space, called ***Euclidean n-space*** or $\mathbb{R}^n$. Vectors in $\mathbb{R}^2$ and $\mathbb{R}^3$ can be visualized as arrows, and the basic operations of ***vector addition, subtraction*** and ***scalar multiplication*** can be interpreted geometrically:





From these two basic operations, we will construct ***linear combinations*** of vectors, and form the ***Span*** of a set of vectors. We will see that these Spans are the fundamental examples of ***subspaces***, and that we can describe these subspaces as the Span of a finite set of vectors called a ***basis***, which have as few vectors as possible. A basis for a subspace enjoys a special property called ***linear independence***, that allows us to describe subspaces in the most efficient way.

The main computational tool of Linear Algebra is called the ***Gauss-Jordan Algorithm***. We will introduce it in this Chapter, and see that it is useful to solve a general system of linear equations. We will also see the concept of the ***dot product*** and the relationship of ***orthogonality***, and we will see that subspaces of Euclidean n-space come in pairs called ***orthogonal complements***.

1.1 The Main Subject: Euclidean Spaces

In ordinary algebra, we see ordered pairs of numbers such as $(3,-5)$. Our first step will be to generalize these objects:

Definition: An ***ordered n-tuple*** or ***vector*** $\vec{v}$ is an ordered list of n real numbers:

$$\vec{v} = \langle v_1, v_2, \ldots, v_n \rangle.$$

Example: $\langle 2,-1,4 \rangle$ is an ordered 3-tuple (more naturally called an ordered ***triple***), and $\langle 5,7,-3,0,6,2 \rangle$ is an ordered ***6-tuple***.□

Definition: The set of all possible n-tuples is called ***Euclidean n-space***, denoted by the symbol $\mathbb{R}^n$:

$$\mathbb{R}^n = \{ \vec{v} = \langle v_1, v_2, \ldots, v_n \rangle \mid v_1, v_2, \ldots, v_n \in \mathbb{R} \}.$$

Euclidean n-space is the main subject of linear algebra, and it is the fundamental example of a category of objects called ***vector spaces***. Almost all concepts that we will encounter are related to vector spaces. The number $\boldsymbol{n}$ is called the ***dimension*** of the space, and we will refer to $\mathbb{R}^2$ as 2-dimensional space, $\mathbb{R}^3$ as 3-dimensional space, and so on. Euclidean n-spaces are referred to collectively as ***Euclidean spaces***. A vector $\vec{v}$ from $\mathbb{R}^n$ is more specifically called an ***n-dimensional vector***, although we will simply say "vector" when we know which Euclidean space $\vec{v}$ comes from. We use an ***arrow*** on top of a letter to denote that the symbol is a vector. The entries within each vector are called the ***components*** of the vector, and they are numbered with a subscript from 1 to n. We will also agree that $\mathbb{R}^1 = \{ \vec{v} = \langle v_1 \rangle \mid v_1 \in \mathbb{R} \} = \mathbb{R}$, the set of real numbers.

Example: Let $\vec{v} = \langle 7,0,-5,1 \rangle \in \mathbb{R}^4$. We say that $v_1 = 7$, $v_2 = 0$, $v_3 = -5$ and $v_4 = 1$.□

To distinguish real numbers from vectors, we will also refer to real numbers as ***scalars***.

Definition: Two vectors $\vec{u} = \langle u_1, u_2, \ldots, u_n \rangle$ and $\vec{v} = \langle v_1, v_2, \ldots, v_n \rangle$ from $\mathbb{R}^n$ are ***equal*** if all of their components are ***pairwise equal***, that is, $u_i = v_i$ for $i = 1 \ldots n$. Two vectors from ***different*** Euclidean spaces are ***never*** equal.

Example: In $\mathbb{R}^3$, We can say that $\langle 2, 3^2, \cos(\pi) \rangle = \left\langle \sqrt{4}, 9, -1 \right\rangle$, but $\langle -2,5,7 \rangle \neq \langle 5,-2,7 \rangle$.□

Many of the Axioms for Real Numbers that we saw in Chapter Zero have analogs in Euclidean spaces. Let us start by generalizing the scalar zero and the additive inverse of a real number:

Definitions: Each $\mathbb{R}^n$ has a special element called the ***zero vector***, also called the ***additive identity***, all of whose components are zero: $\vec{\mathbf{0}}_n = \langle 0, 0, \ldots, 0 \rangle$.
Every vector $\vec{v} = \langle v_1, v_2, \ldots, v_n \rangle \in \mathbb{R}^n$ has its own ***additive inverse*** or ***negative:***

$$-\vec{v} = \langle -v_1, -v_2, \ldots, -v_n \rangle.$$

Example: In $\mathbb{R}^5$, the zero vector will be written as $\vec{0}_5 = \langle 0, 0, 0, 0, 0 \rangle$. Notice that we do ***not*** put a subscript on the zeroes. If $\vec{v} = \langle 4, -2, 0, 7, -6 \rangle$, then $-\vec{v} = \langle -4, 2, 0, -7, 6 \rangle$.

Vector Arithmetic

Vectors in $\mathbb{R}^n$ are manipulated in two basic ways:

> ***Definitions:*** If $\vec{u} = \langle u_1, u_2, \ldots, u_n \rangle$ and $\vec{v} = \langle v_1, v_2, \ldots, v_n \rangle$ are vectors in $\mathbb{R}^n$, we define the ***vector sum:***
>
> $$\vec{u} + \vec{v} = \langle u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n \rangle,$$
>
> and if $r \in \mathbb{R}$, we define the ***scalar product:***
>
> $$r \cdot \vec{v} = r\vec{v} = \langle rv_1, rv_2, \ldots, rv_n \rangle.$$
>
> We will call the operation of finding the vector sum as ***vector addition***, and the operation of finding a scalar product as ***scalar multiplication***. We can also define ***vector subtraction*** by:
>
> $$\vec{u} - \vec{v} = \vec{u} + (-\vec{v}) = \langle u_1 - v_1, u_2 - v_2, \ldots, u_n - v_n \rangle.$$

Example: Let $\vec{u} = \langle 3, -5, 6, 7 \rangle$ and $\vec{v} = \langle -4, 2, 3, -2 \rangle$. Then:

$$\begin{aligned}
\vec{u} + \vec{v} &= \langle 3 + (-4), -5 + 2, 6 + 3, 7 + (-2) \rangle \\
&= \langle -1, -3, 9, 5 \rangle, \\
-\vec{v} &= \langle 4, -2, -3, 2 \rangle, \\
5\vec{u} &= \langle 5 \cdot 3, 5(-5), 5 \cdot 6, 5 \cdot 7 \rangle \\
&= \langle 15, -25, 30, 35 \rangle, \text{ and} \\
\vec{u} - \vec{v} &= \langle 3 - (-4), -5 - 2, 6 - 3, 7 - (-2) \rangle \\
&= \langle 7, -7, 3, 9 \rangle. \square
\end{aligned}$$

Something funny happens when we multiply any vector by zero:

> ***Theorem: The Multiplicative Property of the Scalar Zero:***
> Let $\vec{v} = \langle v_1, v_2, \ldots, v_n \rangle \in \mathbb{R}^n$. Then:
>
> $$0 \cdot \vec{v} = \vec{\mathbf{0}}_n.$$

Proof: We apply the definition of scalar multiplication:

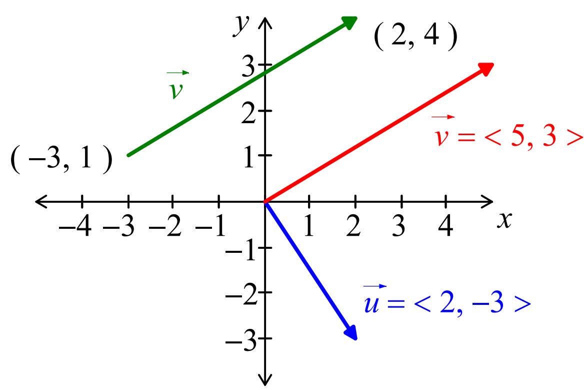
$$\begin{aligned}
0 \cdot \vec{v} &= \left\langle 0 \cdot v_1, 0 \cdot v_2, \ldots, 0 \cdot v_n \right\rangle \\
&= \langle 0, 0, \ldots, 0 \rangle = \vec{\mathbf{0}}_n,
\end{aligned}$$

where we used the Multiplicative Property of Zero in every component, that is, $0 \cdot v_i = 0$ for all $i = 1 \ldots n$. ■

Visualizing Vectors from $\mathbb{R}^2$

The Euclidean space $\mathbb{R}^2$ is easy to visualize. We will use the standard ***xy-plane***, also known as the ***Cartesian plane***. As usual, we will denote by (a, b) the ***point*** on the Cartesian plane with coordinates $x = a$ and $y = b$. A vector in $\mathbb{R}^2$ will be represented using ***arrows*** (also called ***directed line segments***). The arrow representing $\vec{u} = \langle u_1, u_2 \rangle$ is in ***standard position*** if the ***tail*** is at the ***origin*** $(0, 0)$ and the ***head*** is at the point (u_1, u_2). If the tail is not at the origin but at some other point P, we say that the vector has been ***translated to P***. The zero vector $\vec{\mathbf{0}}_2$ is represented by the ***origin*** $(0, 0)$, or any ***point*** on the Cartesian plane for that matter. Notice also that since $-\vec{u} = \langle -u_1, -u_2 \rangle$, we ***reverse*** the arrow for $\vec{u}$ in order to draw the arrow for $-\vec{u}$. A vector whose tail is at P and head is at Q is denoted $\overrightarrow{PQ}$. We also say that $\overrightarrow{PQ}$ is the vector ***from*** P ***to*** Q. We remark that the Cartesian plane is not $\mathbb{R}^2$ but is a framework where we draw the vectors of $\mathbb{R}^2$.

Example: In the picture below, $\vec{u} = \langle 2, -3 \rangle$ is in standard position, and we show $\vec{v} = \langle 5, 3 \rangle$ both in standard position and with its tail translated to $(-3, 1)$.



Plotting Vectors in $\mathbb{R}^2$

Notice that the ***head*** of the second $\vec{v}$ is not at $(5, 3)$, but rather is at $(-3 + 5, 1 + 3) = (2, 4)$. □

In general, the signs of u_1 and u_2 tell us the direction that $\vec{u} = \langle u_1, u_2 \rangle$ is pointing, so if both are positive, then $\vec{u}$ is pointing ***right*** and ***up***. Thus, we have the following:

Theorem: Let $\vec{u} = \langle u_1, u_2 \rangle \in \mathbb{R}^2$, and $P(a_1, b_1)$ a point on the Cartesian plane. If $\vec{u}$ is translated to P, then the head of $\vec{u}$ will be located at $Q(a_2, b_2)$, where:

$$a_2 = a_1 + u_1, \quad \text{and} \quad b_2 = b_1 + u_2.$$

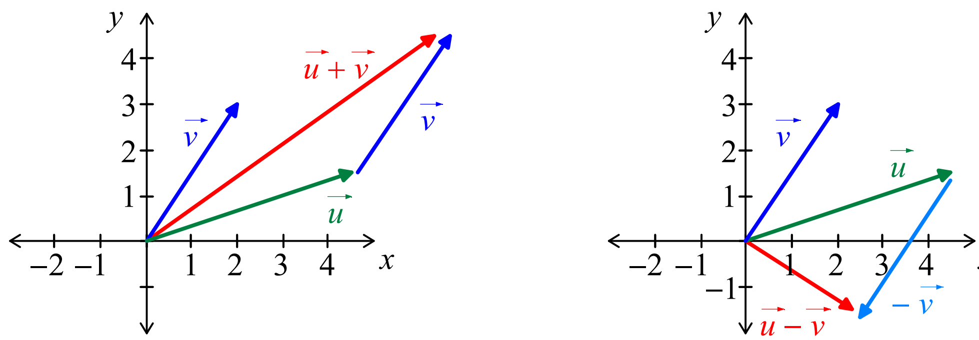
Conversely, if $P(a_1, b_1)$ and $Q(a_2, b_2)$ are two points on the Cartesian plane, then the vector $\vec{u} \in \mathbb{R}^2$ from P to Q is:

$$\vec{u} = \overrightarrow{PQ} = \langle a_2 - a_1, b_2 - b_1 \rangle.$$

We leave the proof as an Exercise.

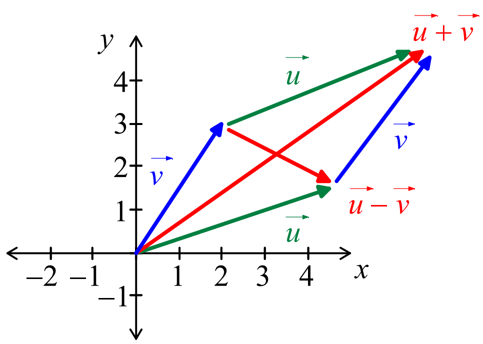
The Geometry of Vector Arithmetic in $\mathbb{R}^2$

Let us think of vector sums and differences from a geometric point of view. To get the vector sum $\vec{u}+\vec{v}$, we put $\vec{u}$ in standard position and translate $\vec{v}$ to the head of $\vec{u}$. We obtain $\vec{u}+\vec{v}$ as the arrow from the origin to the head of $\vec{v}$. Similarly, to get $\vec{u}-\vec{v}$ we put $\vec{u}$ in standard position, reverse $\vec{v}$ (thus getting $-\vec{v}$) and translate it to the head of $\vec{u}$. To obtain $\vec{u}-\vec{v}$, we draw the arrow from the origin to the head of $-\vec{v}$, as we did for $\vec{u}+\vec{v}$.

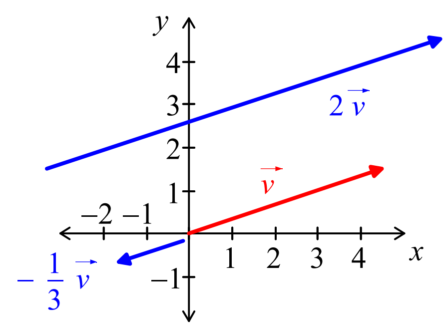


Vector Addition and Subtraction in $\mathbb{R}^2$

These two operations can be seen in a single vector diagram, called ***The Parallelogram Principle*** (where $\vec{u}-\vec{v}$ is translated to the head of $\vec{v}$).



The Parallelogram Principle:
Vector Addition and Subtraction



Scalar Multiplication

Similarly, scalar multiplication has the geometric effect of lengthening or shortening a vector, while preserving or reversing its direction (if the scalar is negative), as shown on the right above.

As we can see, the process of scalar multiplication results in vectors that are pointing in the ***same*** or ***opposite*** directions (we translated $2\vec{v}$ so that it will not overlap with $\vec{v}$). However, we saw that for any vector $\vec{v} \in \mathbb{R}^n$: $0 \cdot \vec{v} = \vec{\mathbf{0}}_n$. It is therefore reasonable to define the following concept:

Definition: Axiom for Parallel Vectors:

We say that two vectors $\vec{u}$, $\vec{v} \in \mathbb{R}^n$ are ***parallel to each other*** if there exists either $a \in \mathbb{R}$ ***or*** $b \in \mathbb{R}$ such that:

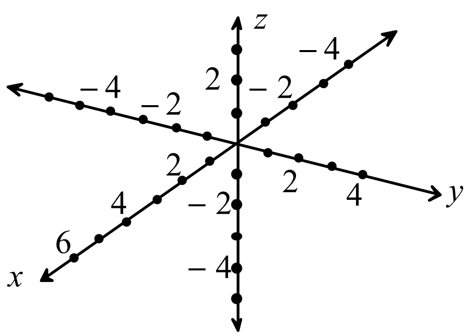
$$\vec{u} = a \cdot \vec{v} \quad \textbf{\textit{or}} \quad \vec{v} = b \cdot \vec{u}.$$

Consequently, this means that $\vec{\mathbf{0}}_n$ is parallel to ***all*** vectors $\vec{v} \in \mathbb{R}^n$, since $\vec{\mathbf{0}}_n = 0 \cdot \vec{v}$.

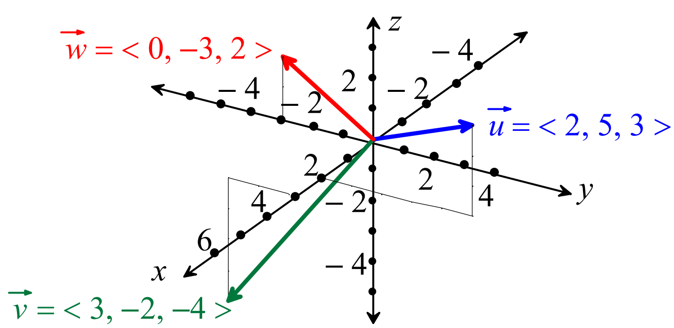
You will show in the Exercises that when $\vec{u}$ and $\vec{v}$ are ***non-zero*** parallel vectors, then a and b both exist and are non-zero scalars, and furthermore, $a = 1/b$.

Visualizing Vectors from $\mathbb{R}^3$

The picture for $\mathbb{R}^3$ requires some imagination. The best way to start is to stand in front of a corner of your room and look down at the corner joining the floor and two walls. The corner will be the origin. The edge on your left is the positive x-axis, the edge on your right is the positive y-axis, and the edge going up is the positive z-axis. To draw this on paper, start by drawing the z-axis as a vertical line. Next, draw the x and y axes as shown below on the left, where the y-axis is slightly rotated clockwise (around 20^0) from the horizontal direction, and the positive x-axis makes an angle of about 120^0 from the positive z-axis. As usual, we mark off a scale on each axis. These three axes determine our ***Cartesian space***. The "floor" determined by the x and y axes is called the xy-plane, the "left side wall" determined by the x and z axes is called the xz-plane, and the "back wall" determined by the y and z axes is called the yz-plane. These three coordinate planes divide Cartesian space into eight ***octants***. The only standard convention is naming the 1st octant as that where the x, y and z coordinates are all positive. As before, we remark that Cartesian space is ***not*** $\mathbb{R}^3$ but it is a framework where we can visualize the vectors of $\mathbb{R}^3$.



Cartesian Space



Plotting Vectors from $\mathbb{R}^3$ in Standard Position

Example: We have plotted in the diagram above on the right three vectors in standard position: $\vec{u} = \langle 2, 5, 3 \rangle$, $\vec{v} = \langle 3, -2, -4 \rangle$ and $\vec{w} = \langle 0, -3, 2 \rangle$.

To plot $\vec{u} = \langle 2, 5, 3 \rangle$, we start at the origin, go forward on the x-axis to 2, go right parallel to the y-axis by 5 units, then go up parallel to the z-axis by 3 units. To plot $\vec{v} = \langle 3, -2, -4 \rangle$, we go forward by 3 units on the x-axis, go left 2 units parallel to the y-axis, and go down 4 units parallel to the z-axis. To plot $\vec{w} = \langle 0, -3, 2 \rangle$, we directly go 3 units left on the y-axis, then go up 2 units up parallel to the z-axis. $\square$