Book of Mathematical Problems

In Number Theory and Geometry

Jason Soegondo

Contents

Chapter 1

Preface

The best way to learn math is to do math. There is a large gap between knowing a concept and understanding it. For example, when reading a theorem and its given proof, the proof may be difficult to comprehend. But, it is a much more difficult task to have to create your own proof of the theorem, but the ingenuity required to do so is quite important. The hope is that the process of working through these problems and after much struggle finding a solution is incentive enough to continue working through the problems in the book. If you find a proof too difficult to solve, try to reason why you think a given theorem is true or false.

Chapter 2

Prerequisites

2.1 Logic

A **proposition** is a statement that is either true or false. For example, "$x > 0$" is either true or false. On the other hand, "How is the weather today" is not a proposition because it cannot be categorized as either true or false. An **argument** is made up of a **premise** and a **conclusion**. A premise is a set of propositions that support the conclusion while the conclusion is a proposition whose truthfullness follows from the premise.

As a logical consequence, if the premise is true, then the conclusion must be true. For example, consider the argument:

(1) I will draw either a circle or square

(2) I drew a circle

$\therefore$ I did not draw a square

Notice that if the premise is true, then it must be the case that the conclusion is also true. These types of arguments are **truth-perserving**

(1) A pair is a fruit

(2) An apple is a fruit

$\therefore$ A pair is an apple

Here, we can obviously see a situation where the premise is true, yet the conclusion is false. Arguments where the conclusion does not follow from the premise; arguments where the premise does not entail the conclusion are not truth-perserving.

This law of logic is called **Modus Ponens** and is very important in mathematics. Many theorems are written with an if A then B structure. This law lets us say that B follows from A, if A is true. Symbolically, we would write it as $((A \longrightarrow B) \land A) \vdash B$.

Modus Tollens follows from modus ponens by stating that if A implies B, then not A entails not B. Symbolically, $((A \longrightarrow B) \land \neg A) \vdash \neg B$.

A **Hypothetical Syllogism** states that if A implies B, and B implies C, then A implies C. Symbolically, $(A \longrightarrow B) \land (B \longrightarrow C) \vdash (A \longrightarrow C)$.

A **Disjunctive Syllogism** states that if either A or B is true, then A being true entails that B is not true and vice-versa. Symbolically, $((A \lor B) \land \neg B) \vdash A$. An exhaustive list of logic laws is given in the Index.

A **logical connective** in propositional logic expresses a binary relation between two propositions. The main connectives are the following:

Definition 2.1.1

- Conjunction $\land$

  In english, *and* can denote a conjunction.

- Disjunction $\lor$

  In english, *or* can denote a disjunction.

- Exclusive Disjunction $\veebar$

  In english, "either. . . or" statements can denote that two propositions that are connected by a disjunction are mutually exclusive.

- Negation $\neg$

  In english, *not* denotes a negation.

- Conditional $\longrightarrow$

  In english "if. . . then" statements denote a conditional. A implies B, and other structures can also be used to denote conditionals.

- Biconditional $\leftrightarrow$

  In english "if and only if" (*iff*) statements denote a biconditional.

Note:-

Consider the proposition $A \longrightarrow B$. Note that if A, then B. But notice that the following is also valid: $\neg A$, B. Logically, this is valid because B does not imply A. If the proposition was $A \leftrightarrow B$, then the pair $\neg A$, B would be invalid.

Note:-

To know whether the usage of a *disjunction* is exclusive $\veebar$ or inclusive $\vee$, decide whether the two propositions are mutually exclusive. For example $A \vee \neg A$ is a valid proposition and an exclusive disjunction. We can omit the use of $\veebar$ here because the exclusivity of the disjunction follows from the definition of negation. Another method to determining exclusivity is the language that may denote exclusivity such as the word *either*.

2.1.1 Validity

2.2 Notation

Definition 2.2.1

- $\forall$: symbolic for “for all“
- $\exists$: symbolic for “there exists“
- $\in$: symbolic for “in“
- $\ni$: symbolic for “such that“

2.3 Sets

This section will not cover sets in depth, but will cover set notation that will be used throughout this book. The purpose of this book is not to go in depth into set theory, but set theory is important to the axiomization of math. Therefore, it is useful to know a little bit about sets.

2.3.1 Common Sets

Definition 2.3.1

- $\mathbb{N}$ is the set of natural numbers $(1, 2, 3 \ldots)$
- $\mathbb{Z}$ is the set of integers $(\cdots - 2, -1, 0, 1, 2 \ldots)$
- $\mathbb{Q}$ is the set of rational numbers which is defined as any number that can be expressed with a fraction, ie: $\frac{1}{1}, \frac{13}{17}, \frac{199}{3} \ldots$
- $\mathbb{R}$ is the set of real numbers which encompasses the set of rational numbers and the set of irrational numbers.
- $\mathbb{C}$ is the set of complex numbers. Remember that complex numbers are numbers made up of a real part and an imaginary part $C + Xi$ where C is a real number and X is the coefficient of the imaginary part.

The empty set, $\{\}$ denoted with $\emptyset$, is a special set because it has no element and is subset to all non-empty sets. **Set-builder notation** is used to describe sets that are too big to list in braces: $E = 2n : n \in A$. In general: $X = \{A(x) : P\}$ in words, "for all A(x) such that P is true." Here are some intervals described with set notation.

- Closed interval: $(a, b) = \{x = \mathbb{R} : a < x < b\}$
- Open interval: $[a, b] = \{x = \mathbb{R} : a \leqslant x \leqslant b\}$
- Infinite interval: $(-\infty, b] = \{x = \mathbb{R} : x \leqslant b\}$

Cartesian Product

An ordered pair is a list (x, y) of two elements. The **Cartesian product** of two sets A and B is another set denoted as $A \times B$ which is defined as $A \times B = \{(a, b) : a \in A, b \in B\}$.
Given $A = \{k, l, m\}$ and $B = \{q, r\}$, $A \times B = (k, q), (k, r), (l, q), (l, r), (m, q), (m, r)$

The set $\mathbb{R} \times \mathbb{R}$, commonly denoted $\mathbb{R}^2$, is the set of points of the Cartesian plane. The set $\mathbb{R} \times \mathbb{N}$ would be a bunch of horizontal lines starting from $y = 1$ and the set $\mathbb{N} \times \mathbb{N}$ would just be a bunch of points located in the first quadrant of a cartesian plane.

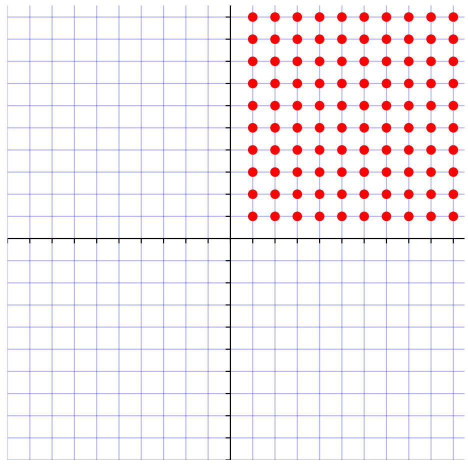


Figure 2.1: $\mathbb{N}^2$ in the cartesian plane.

Cartesian products can be done with more than two sets. The dimensionality of the ordered pairs within the product is equal to the amount of factors in the product.

Subsets

$\subseteq$ is symbolic for "subset of". We say that a set, A is a subset of another set, B if B contains all of the elements in A ($\forall a \in A, a \in B$). For example, $\mathbb{N} \subseteq \mathbb{Z}$ Likewise, $\mathbb{Z} \subseteq Q$ and $\mathbb{R} \subseteq \mathbb{C}$. See that $\mathbb{R} \subseteq \mathbb{C}$ because we can represent any real number with a complex number by letting the coefficient of the imaginary part equal 0. Given two sets, A and B, consider when $A \subseteq B$ and $B \subseteq A$. It follows that $A = B$. This fact is key in proving equality between two seemingly different sets.

Power Sets

If A is a set, the **power set** is another set denoted as $\mathscr{P}(A)$ and is the set of all subsets of A: $\mathscr{P}(A) = \{X : X \subseteq A\}$. If A is a finite set then $|\mathscr{P}(A)| = 2^{|A|}$ Where $|\ |$ denotes cardinality. For example, $\mathscr{P}(\mathbb{R}^2)$ contains every coordinate pair that is in the 2D plane.

Set Operations

Definition 2.3.2

The **union** of two sets A and B is: $A \cup B = \{x : (x \in A) \vee (x \in B)\}$

The **intersection** of two sets A and B is: $A \cap B = \{x : (x \in A) \wedge (x \in B)\}$

The **difference** of two sets A and B is: $A - B = \{x : (x \in A) \wedge (x \notin B)\}$

In other words, $A \cup B$ is the set of all elements in A, in B, or both. $A \cap B$ is the set of all elements in both A and B. $A - B$ is the set of all elements in A but not in B

Notice that when $A = \{(x, x^2) : x \in \mathbb{R}\}$ and $B = \{(x, x + 2) : x \in \mathbb{R}\}$; in other words, when A and B are a set of function input and output pairs, $A \cap B$ is a set containing the point(s) of intersection between the two functions. Two sets, A and B are said to be disjoint sets if they share no elements in common.

Complement

A *universal set*, denoted by U, is a set where for all sets A, it is the case that $A \in U$ and $\forall x \in A : x \in U$. By this definition, $U \in U$. But this is disallowed in most systems of set theory. For example, in *Zermelo-Fraenkel* set theory the *axiom of foundation* says that for all sets $A \neq \emptyset$, there exists a set B in A that does not intsersect with A. Now, consider the set $\{A\}$. By the axiom of foundation, there exist a set in $\{A\}$ that is disjoint from it, therefore $A \cap \{A\} = \emptyset$. Which is to say that $A \notin A$. So, sets cannot be self-referential. Consider a universal set that is not self-referential. Suppose that there is a set U where $A \subseteq U$ then $U - A$ is the **complement** of A denoted by $\bar{A}$. Here, U is a larger set than A that happens to contain A and all other sets that are under consideration for the specific scenario. For example if $A = \{x \in \mathbb{Z} : x = 2n + 1, n \in \mathbb{Z}\}$ we could say that $U = \mathbb{Z}$. or $U = \mathbb{Q}$ or $U = \mathbb{R}$ and so on.

2.3.2 Ordering

The ordering of a set is how the elements in the set are arranged. Order is denoted with the symbol $<$. Naturally we would order a set of numbers from least to greatest. For example, the set $\{1, 11, 18, 19\}$ in its *standard* ordering ($\leqslant$) is as we see it on the page. The natural numbers in its standard ordering is equivalent to counting from 1 upwards, $\{1, 2, 3 \ldots\}$. But, there are other ways that a set can be ordered in. For example, we can order the natural numbers such that the odd numbers come before the even numbers like so $\{1, 3, 5 \ldots 2, 4, 6 \ldots\}$

Well-ordering

A set is considered well-ordered if every subset of that set has a least element. If a set is bounded from below, Consider the set $X = \{x \in \mathbb{Z} : x \geqslant n\}$. It has a least element n. Likewise, if a set is bounded from above, $Y = \{y \in \mathbb{Z} : y \leqslant n\}$, then it has a greatest element n. The set X is well ordered because in its standard ordering, $(n, x_1, x_2 \ldots)$ has a least element. On the other hand, Y in its standard ordering $(\ldots y_2, y_1, n)$ is not well-ordered. But there are orderings of Y that are well ordered. An obvious well-order on y is $(n, y_1, y_2 \ldots)$. In fact, the **well-ordering theorem** states that every set has a well-ordering that satisfies the *trichonomy* and *transitive* laws which will be discussed in the real numbers section.

Notice that the natural numbers in its standard ordering is well-ordered. It isn't difficult to verify this since the standard ordering of natural numbers $(1, 2, 3 \ldots)$ is obviously well-ordered with 1 being the least element of the set. This property of the natural numbers is often called the **well-ordering principle**. In general, it is pretty obvious to see that
$X \subseteq \{n, (n+1), (n+2), (n+3) \ldots\}$, $n \in \mathbb{Z}$ is well ordered. On the other hand, the standard order on real numbers is not well-ordered. To see this, take the inverval $\{(0, 1)\} \subseteq \mathbb{R}$. There is no least element in the subset because there are infinitely many elements between 0 and 1; that is, for $\frac{1}{n} \in [0, 1]$ there will always be $\frac{1}{n+1} \in [0, 1]$ smaller than it.

Note:-

Whether the natural numbers include 0 or not is a matter of debate. But for the book, the natural numbers exclude 0. We will refer to the set of natural numbers including 0 as *non-negative integers*.

Chapter 3

Numbers

3.1 Powers

Powers represent repeated multiplication.

$a^3 = a * a * a$

$a^n = a * a * a \dots$

and so on. The following properties are rather useful to memorize, they follow rather intuitvively from the definition of a power and the associative property.

Proposition 3.1.1

- $a^n * a^m = a^{n+m}$
- $(a^n)^m = a^{n*m}$
- $(ab)^m = a^m b^m$
- $\forall n, m \in \mathbb{Z}$

Intuitively, we know that positive exponents are defined as repeated multiplication, the inverse of multiplication as we know is division. So perhpas we can treat negative powers as repeated division which is just repeated multiplication of the multiplicative inverse. We use this fact to find the value of x^0. Which is just $x^0 = x^{-1}x^1$. That is, $x^{-1}x^1 = \frac{x}{x} = 1$.

But we can also find the value of x^0 for any number x using only the properties from **3.1.1**.

Since 0^m will always equal 0 we can assume that $x \neq 0$.

Let $b = x^0$

$x = x^1 = x^{1+0} = x^1 x^0$

$x = xb$

Multiply both sides by x^{-1}

by the first property $x^1 x^{-1} = x^0$

$x^0 = x^0 b$

$b = 1$

From 3.1.1 and $x^0 = 1$, it follows that a negative power of x^{-m} must satisfy the following equation $x^m x^{-m} = 1$. Then, we can certainly say that the negative power represent the multiplicative inverse of a positive power. That is, $x^{-1} = \frac{1}{x}$

Proposition 3.1.2

- $a^{-4} = \frac{1}{a} * \frac{1}{a} * \frac{1}{a} * \frac{1}{a}$
- $\frac{a^n}{a^m} = a^{n-m}$
- $a^{-n} = (a^n)^{-1} = (a^{-1})^n = \frac{1}{a^n}$

These properties of negative powers can be derived with the previous properties along with the definition of negative powers as multiplicative inverses.

3.2 Roots

A square root of a number x is represented with the symbol $\sqrt{x}$. A root of a number x is a number y that when squared results in x. A square has exactly two roots, one negative and another positive. In other words, x^2 has one positive and one negative root. To see this, consider when $x = y^2$. Rearrange the equation to $x^2 - y^2 = 0$, then factor the term into a product $(x - y)(x + y) = 0$. The two roots can be found by eliminating terms and solving for x. The roots for this particular equation are y and $-y$.

The square root of a number x, by convention is the **positive** value of its roots. For example, let $x = 4$, then the square root of x is the following: $x^2 - 4 = 0$. The roots come out to be ± 2. We agree to say that $\sqrt{4} = 2$ and not $\sqrt{4} = \pm 2$ or $\sqrt{4} = -2$.

By convention the square root is always the positive number. But algebraically, the second root needs to be accounted for. Given $x^2 = 16$, $x = \pm 4$.

Definition 3.2.1

In general, given a square, $x^2 = y, \quad x = \pm\sqrt{y}$

Roots are defined as fractional powers $r = a^{\frac{1}{n}}$ where $n \in \mathbb{Z}$. Using power rules, we can rearrange the equation by raising both sides to the n-th power so that the root r is defined as $r^n = a$ We say that r is the n-th root of a and that $r = {}^{n}\sqrt{a}$. The same power rules that apply to integer powers apply to fractional powers as well.

3.3 Absolute Values

Absolute values are denoted with the symbol $||$, so the absolute value of x is $|x|$. Terms within the absolute value are always positive. For example, $|a| = a|$ and $|-a| = a$. The absolute value of any number a is $\sqrt{a^2}$.

When solving for unknowns within absolute values, it may be more intuitive to know the process of removing an absolute value out of an equation. Suppose $|2x + 12| = 11$. Knowing the properties of an absolute value, we can rewrite this equation as $2x + 12 = \pm 11$ which are two different equations. Solving both equations, we get $x = -\frac{23}{2}$ and $x = -\frac{1}{2}$

3.4 Factorials

Factorials can be thought of the non-negative integers, $(0, 1, 2...)$. Given $n!$ where ! is used to denote the n-th factorial, $n!$ is the product of the natural numbers $(1, 2, 3...)$ preceeding n and n itself. For example $4! = 1 * 2 * 3 * 4$. Notice that factorials act on whole numbers. So by the definition given above, $0! = 0$. But as some of you may already know, $0!$ is in fact equal to 1. Factorials are defined as

Definition 3.4.1

$n! = n\ (n-1)! \quad \text{for } n \geqslant 1$

If $0! = 0$, then $1! = 0$ by this definition. So, it must be the case that $0! = 1$.

Another way to think of factorials is as the amount of permutations of a set containing n elements.

For example, $3! = 6$. A set with 3 elements, $\{a, b, c\}$ has the following permutations: $\{a, b, c\}$, $\{a, c, b\}$, $\{b, a, c\}$, $\{b, c, a\}$, $\{c, b, a\}$, $\{c, a, b\}$. For 0!, it represents the amount of permutations of the empty set $\{\}$, commonly denoted $\emptyset$. The only permutation of the empty set is obviously the empty set itself; therefore, $0! = 1$.

3.5 Rational Numbers

Rational numbers are numbers that can be expressed as a fraction between integers. They can be expressed with decimals as well,

$\frac{2}{10} = 0.2, \quad \frac{2}{100} = 0.02$

Multiplication of fractions

$\frac{\alpha}{\beta} * \frac{\gamma}{\phi} = \frac{\alpha\gamma}{\beta\phi} \qquad \frac{\alpha}{\beta} * \frac{\beta}{\gamma} = \frac{\alpha}{\gamma}$

Remember that products can be broken up into their factors

$\frac{\alpha}{\beta} * \frac{\beta}{\gamma} = \alpha * \frac{1}{\beta} * \beta * \frac{1}{\gamma}$

Addition of fractions

$\frac{\alpha}{\gamma} + \frac{\beta}{\gamma} = \frac{\alpha+\beta}{\gamma} = \frac{1}{\gamma}(\alpha + \beta)$

In practice, when you want to add fractions together, you want a **common denominator** so that you can use the distributive property.

$\frac{a}{m} + \frac{b}{n}$

$\frac{n}{n}(\frac{a}{m}) + \frac{m}{m}(\frac{b}{n}) = \frac{an}{mn} + \frac{bm}{mn}$

$\frac{1}{mn}(an + bm) = \frac{an+bm}{mn}$

When you have an expression equating two fractions together

$\frac{a}{b} = \frac{c}{d}$

you can use **cross multiplication** to turn the fractions into integers (note that integers are a subset of rational numbers because $\forall a \in \mathbb{Z}, a = \frac{a}{1}$).

$\frac{a}{b} \times \frac{c}{d}, \qquad \frac{a}{b} = \frac{c}{d}$ is equivalent to $ad = cb$

Cross multiplication makes sense because because an expression of equality must retain equality. That is to say, everytime one side of an equality is changed, the other side must be changed in the same way.

$\frac{a}{b} = \frac{c}{d}$

$b * \frac{a}{b} = b * \frac{c}{d} \;\longrightarrow\; a = \frac{cb}{d}$

$d * a = d * \frac{cb}{d} \;\longrightarrow\; ad = cb$

Definition 3.5.1

- A number d divides q if $q = ds$ for some integer s. We write it as $d \mid q$
- A **reducible fraction** is a fraction whose numerator and denominator share a common divisor, that is $\frac{da}{db}$ where d is the common divisor.
- An **irreducible fraction**, or a fraction in lowest form is a fraction whose numerator and denominator are **coprime** with one another. Which is to say that their greatest common divisor is 1.

Theorem 3.5.1

All positive rational numbers can be expressed as an irreducible fraction.

Proof: A rational number can be expressed as $\frac{a}{b}$. Assume that a and b are reducible. Then, they share a greatest common divisors $d > 1$. That is, $a = dn$ and $b = dm$ for some numbers n and m.

Suppose that n and m are not coprime, then they share a common divisor $p > 1$ such that $n = ps$ and $m = pt$

$\frac{a}{b} = \frac{dps}{dpt}$

Then, $dp > d$ and dp is the greatest common divisor of a and b which is a contradiction because d is the greatest common divisor. So, n and m *must* be coprime. 😄

This theorem is important in solving problems that involve rational numbers. Keep this theorem in mind for the problem set.

Claim 3.5.1

$\frac{a}{0}$ is undefined for all integers a

Remember that division is defined as $\frac{a}{b} = q$ for some unique q. That is, $a = qb$. But if $b = 0$ then $a = 0q$. Suppose $a \neq 0$, then there is no q that can satisfy this equation. Suppose $a = 0$, then q is not unique. Thus, $\frac{a}{0}$ is undefined. You will be asked to prove the uniqueness of q in the problem set.

3.5.1 Radical Denominators

When a denominator of some term contains a radical, you can turn the radical into a rational number. This is called rationalizing the denominator. Consider the equation $\frac{1}{\sqrt{2}}$. To get rid of the radical simply multiply the numerator and denominator by $\sqrt{2}$.

$(\frac{1}{\sqrt{2}})(\frac{\sqrt{2}}{\sqrt{2}}) = \frac{\sqrt{2}}{2}$

Recall the property $a^2 - b^2 = (a+b)(a-b)$. If we were given $\frac{1}{12-\sqrt{6}}$ the property can be used to rationalize the denominator $(\frac{1}{12-\sqrt{6}})(\frac{12+\sqrt{6}}{12+\sqrt{6}}) = \frac{12+\sqrt{6}}{138}$.

Example Rationalize the denominator of the given fraction $\frac{c}{\sqrt{11}-4}$.

$\frac{c}{-(4-\sqrt{11})}$

$(\frac{c}{-(4-\sqrt{11})})(\frac{4+\sqrt{11}}{4+\sqrt{11}})$

$\frac{4c+c\sqrt{11}}{-5}$

In general given an equation in the form $\frac{c}{a+\sqrt{b}}$, you can rationalize the denominator by multiplying the numerator and denominator by $a - \sqrt{b}$. If the denominator is in the form $a + \sqrt{b}$ then multiply by $a - \sqrt{b}$.

3.6 Systems

A **Linear equation** is an equation with unknown variables. $x - y = 3$ is a simple linear equation. You can rearrange it so that y becomes a function of x. So, $y = x + 3$ is the just same equation in what is known as *y-intercept* form. It is referred to as such because the constant in front of the x is the value of the function y when $x = 0$. The *y-intercept* form is also rather convenient because it clearly shows y as a function of x. Remember that variables are distinct from one another, so you can choose to rearrange the equation however you like. By isolate x, we get $x = y - 3$ which represents x as a function of y.

This section will focus on linear equations with two unknowns. The benefit to working with equations that only have two unknowns is that graphing utilities like *desmos* are widely available to help visualize them.

A **system of equations** is a set of equations that share common variables. Systems are represented like so:

$ax + by = c$

$dx + ny = t$

$mx + sy = k$

$\vdots$

Finding a solution to a system of equations means to find a set of unknowns that satisfy all equations in the system. There are some systems that have more than one solution like the system

$x^2 + y = 0$

$x^4 + y = 0$

Since 2 and 4 are different powers, it is obvious that the two equations only intersect when $x = \pm 1$ and $x = 0$. $(1, 1), (-1, 1), (0, 0)$ are the three solutions to the system.

Some systems have infinitely many solutions

$x - y = 3$

$2x - 2y = 6$

Because $x - y = 3$ and $2x - 2y = 6$ are actually the same equation, this system actually has infinitely many solutions.

Some systems have no solution like the following

$x + y = 8$

$x + y = 4$

Which very obviously has no pair that can satisfy the equation.

Finally, there are cases where there is only one solution

$2x - 2y = 0$

$10x - 5y = 0$

Where $(x = 0, y = 0)$ is the only solution that exists.

Often times when solving for points of intersection between two or more equations, the given equations are already in y-intercept form. If that it the case, then solving the system becomes trivial. Because y is a function of x , that is $f : X \rightarrow Y$, for all equations in y-intercept form, if you let the equations equal each other you can then solve for the independent variable rather easily and the value for the dependent variable follows.

Tips for Solving Systems

1. **Elimination**, the process of isolating a variable in one equation so that the same variable can be substituted into another equation.

2. **Addition**, the process of adding two equations together such that it eliminates a variable.

3.6.1 Quadratics

A polynomial is an equation with unknowns where the only operations that it can include are multiplication, addition and subtraction. A quadratic is a second degree polynomial, meaning that the unknowns are raised to the second power. One application is to solve for the roots of a quadratic equation. When we solve for the roots of a quadratic, we are interested in seeing what values of x result in $y = 0$. For example, $y = x^2 + 5x + 6$ is a quadratic equation. isolating the two variables, we get the general form of a quadratic equation, $y = ax^2 + bx + c$. for some constants a, b, c. Notice that for the previous equation, there exists a pair of numbers that when added together results in b and when multiplied together results in c. In this case, it is the 2 and 3. We can then rewrite it as $y = (x+3)(x+2)$. Solving for $y = 0$, we find that $x = -3$ and $x = -2$ are solutions to this particular quadratic.

Claim 3.6.1

In general, for any quadratic equation $y = ax^2 + bx + c$, if there exists n, m such that $b = n + m$ and $c = nm$, then the quadratic equation can be separated into two linear equations.

The above method is the easiest method in the process of solving a quadratic. But, many quadratics do not come in that form, therefore we find other methods to solve quadratic equations. Consider $y = 3x^2 + 10x + 8$. We can solve this quadratic by splitting the bx term so that the quadratic can be rewritten as a product of linear equations. In this example, we want to find two numbers whose sum is 10 and whose product is $3(8) = 24$. We find that 6 and 4 make satisfy our proposition. Then we can rewrite it as $y = 3x^2 + 6x + 4x + 8$ which can be written as $y = 3x(x+2) + 4(x+2)$, or $y = (x+2)(3x+4)$. The reasoning for this method is that we want to find one number that is a multiple of a and another number that is a multiple of c. If we can split b into those two numbers, then we can factor the quadratic into two separate linear equations. That is to say, we want to find two numbers whose product is ac and whose sum is b.

Claim 3.6.2

If there exists n, m such that $y = ax^2 + nx + mx + c$ where the sum of n, m is b and the product is ac, then the quadratic can be written as a product of two linear equations.

Given the quadratic equation $y = 7x^2 + 11x + 3$, it becomes obvious to us that the previous two methods do not work. When this is the case, we introduce the method known as completing the square. The reasoning behind completing the square is to add a number to the equation that allows us to rewrite it as a perfect square $(x+q)^2 = d$. First we would want to divide the equation by the leading coefficient, $x^2 + \frac{11}{7}x = -\frac{3}{7}$. We then add onto the equation then number needed to complete the square, $(\frac{b}{2})^2$. In this case, we will add $\frac{121}{196}$ to the equation which will be $x^2 + \frac{11}{7}x + \frac{121}{196} = \frac{37}{196}$. Completing the square, we get $(x + \frac{11}{7})^2 = \frac{37}{196}$. Now solving for x is rather routine, $x = -\frac{11}{7} \pm \sqrt{(\frac{37}{196})}$.

Theorem 3.6.1

For any quadratic equation in the form $y = ax^2 + bx + c$. The roots of the quadratic is given by the formula $x = \frac{b \pm \sqrt{b^2 - 4ac}}{2a}$. As long as $b^2 - 4ac \geqslant 0$. Otherwise, the roots are not in the real numbers.

Proof: A quadratic is written in the form $y = ax^2 + bx + c$. Solving for the roots, we let $y = 0$. To complete the square we first divide by a.

$\frac{x^2+bx}{a} = -\frac{c}{a}$. We then want to add $(\frac{b}{2a})^2$ to both sides.

$\frac{x^2+bx}{a} + (\frac{b}{2a})^2 = (\frac{b}{2a})^2 - \frac{c}{a}$

$\frac{4a^2x^2+4abx+b^2}{4a^2} = \frac{b^2-4ac}{4a^2}$

$4a^2x^2 + 4abx + b^2 = b^2 - 4ac$

$(2ax + b)^2 = b^2 - 4ac$

$2ax + b = \pm\sqrt{b^2 - 4ac}$

$x = \frac{b \pm \sqrt{b^2-4ac}}{2a}$ 😄

3.7 Inequalities

When we refer to a number greater than 6, we write $x > 6$. If the number is less than 6, then we write $x < 6$. If the number is greater than or equal to 6 then we write $x \geqslant 6$. If the number is less than or equal to 6 we write $x \leqslant 6$. Consider the inequality $x > 6$.

Inequalities are relations on a set. Our intuitive understanding is that relations like less than ($<$) and greater than ($>$) hold for some pair of elements in a set, but not for others. For example $2 > 7$ is true, but $9 > 7$ is false because we define the relationship in that way. More specifically, we define inequalities such that

Definition 3.7.1

- $x > y$ holds when $x - y$ is positive.
- $x < y$ holds when $y - x$ is positive.
- $x \geqslant y$ holds when either $x > y$ or $x = y$.
- $x \leqslant y$ holds when either $x < y$ or $x = y$.

Note:-

You can add different values to sides of an inequality as long as said values retain the relation. For example, if the inequality was $x > y$, you can add values such that $x + 5 > y + 3$ and the inequality will still be true.

3.8 Definitions

Definition 3.8.1

- An even number x is defined as $x = 2n\ \forall n \in \mathbb{Z}$
- An odd number x is defined as $x = 2n + 1\ \forall n \in \mathbb{Z}$
- If a number d divdes a number c, $d|c$ and $\exists q \in \mathbb{Z} \ni c = dq$

All rational numbers can be represented in reduced form which is when both the numerator and denominator share no common factor. Consider the special case $\frac{a}{b}$. Where both a and b are even, they share common factors, making them reducible.

Definition 3.8.2

- A number p is irrational if $p \neq \frac{n}{m}\ \ \forall n, m \in \mathbb{Z}$
- A set of size n has $n!$ possible non-repeating permutations

In choosing elements for a permutation of a set with a cardinality of n, the first element of the permutation has n possible elements to choose from. The next element has $n - 1$ elements to choose from, the next has $n - 2$ and so on until the last element of the permutation which would only have a single element to choose from. By the multiplication principle we denote the total number of possible permutations with $n!$.

Proposition 3.8.1

$A = \frac{n!}{(n-k)!}$ is the amount of permutations with k elements of a set with n elements

The first element of the permutation has n possible elements, the next choice has $n-1$ possible choices and so on until the last element of the permutation which will have $n-k+1$ choice of possible elements. If $n = 5$, then $n! = (1)(2)(3)(4)(5)$. If $k = 3$, then $(n-k)! = (1)(2)$. If the latter were to divide the former, the result is $(3)(4)(5)$ which is the same pattern as $(n), (n-1)\ldots(n-k+1)$.

Definition 3.8.3

$T = \frac{n!}{k!(n-k)!}$ if $0 \leqslant k \leqslant n$

$T = \binom{n}{k}$ is called n choose k, or the *binomial coefficient.*

T is the amount of unique subsets of n of size k. Each k-subset of the set of size n has $k!$ possible permutations. Therefore, multiplying the amount of subsets by $k!$ actually results in the amount of k-sized permutations of the set which we know is $\frac{n!}{(n-k)!}$. It follows that dividing $\frac{n!}{(n-k)!}$ by $k!$ would then result in the amount of unique subsets.

3.8.1 Exercises

Question 1

(a). Prove that if x is even, then x^2 is even

(b). Prove that the converse is also true. If x^2 is even, then x is even.

Question 2

(a). Prove that if x is odd, then x^3 is odd

(b). Prove that the converse is also true.

Question 3

(a) Prove that the sum of two even numbers is even

(b). Prove that the sum of two odd numbers is also even

Question 4

x and y are positive real numbers. If $x < y$ then show that $x^2 < y^2$

Question 5

Given $a, b, c \in \mathbb{Z}$, if $a^2|b$ and $b^3|c$ show that $a^6|c$

Question 6

Given $a, b, c \in \mathbb{Z}$, if $b|a^2$ and $c|b^3$ show that $c|a^6$

Question 7

Show that $\binom{2n}{n}$ is even for all whole numbers n

Question 8

Show that $\sqrt{2}$ is irrational

Question 9

Prove that $n!$ is always even if $n > 1$

3.9 Geometry

Geometry is much more intuitive than analysis. Throughout the book, there may be problems where a geometric interpretation is easier than an analytical one. For the problem set, do not be overly concerned with solving the problem through analysis. A geometric argument is also valid.

Proposition 3.9.1

- For any two points P and Q, the segments $(P, Q) = (Q, P)$. In other words, the distance between P and Q is always the length of the segment.

- The distance between P and $Q = 0$ *iff* (if and only if) $P = Q$. Otherwise, the distance between P and $Q \geqslant 0$.

- With points P, Q, M, The distance $(P, M) \leqslant (P, Q) + (M, Q)$.

See how the third proposition is true for any combination of three points. Moreover, $(P, M) = (P, Q) + (Q, M)$ *iff* P, Q, M lie on the same line. Which is to say that there is a point Q on the line $\overline{PQ}$ such that the distance between P and Q is s and $0 \leqslant s \leqslant d$

Definition 3.9.1

- The length that lies between two points P, Q is called the **segment** formed by P and Q denoted by $\overline{PQ}$.

- A **ray** is a line that passes through a point.

- The **angle** between two rays sharing a point of intersection, A and B is denoted with $\angle AB$. In this notation, the angle starts from A and ends at B. On the other hand, $\angle BA$ would start at B and end at A. The order in which the rays are placed matters for the notation.

If the rays A and B were to lie on each other, then either $\angle AB = 0$ or $\angle BA = 0$. This angle is called the **zero angle**. The opposite angle is called the **full angle**. Notice that one full rotation through the plane forms a circle. Indeed, the full angle is defined as the length of the circumference of a **unit circle** (a circle with a radius of 1). Which makes the full angle 2π.

Proposition 3.9.2

- π is the ratio between the circumference of a circle and its diameter, $\frac{circumference}{diameter}$ where $\pi \approx 3.14\ldots$.

- It follows that the circumference in terms of pi is $2r * \pi$ or more commonly written as $2\pi r$.

- The area of a circle is given by the formula $A = 2\pi r^2$.

Definition 3.9.2

- A triangle is a **right triangle** *iff* the **legs** of the triangle make a right angle. A right angle is 90° or $\frac{\pi}{2}$ radians. The legs are two segments $\overline{PQ}$ and $\overline{PM}$ that make up the right angle. Furthermore, $\overline{PQ}$ and $\overline{PM}$ are **perpendicular** with each other. The third side of a right triangle, $\overline{QM}$, is called the **hypotenuse**.

- A line is perpendicular with another line if their intersection forms a right angle.

- Lines are **parallel** with each other if they never intersect.

Intuitively, we can suppose that two segments of two parallel lines are parallel with each other as well.

Proposition 3.9.3

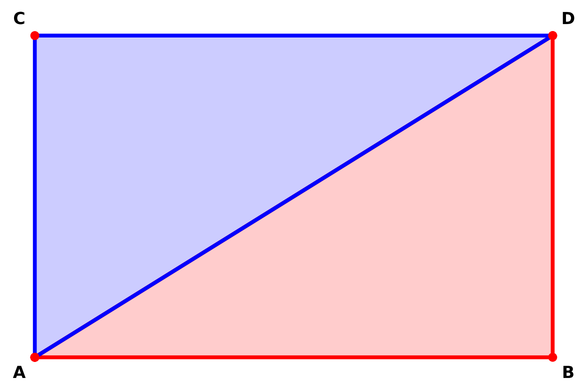
- Two right triangles $\triangle ABC$ and $\triangle DEF$ with legs $\overline{PQ}, \overline{PM}$ and $\overline{P'Q'}, \overline{P'M'}$ respectively are **congruent** *iff* Their legs are equal to each other. That is, $\overline{PQ} = \overline{P'Q'}$ and $\overline{PM} = \overline{P'M'}$.

The length of the legs is all that is necessary in order to show congruence. If the lengths of the legs are equal, it follows that the third side is equal for both triangles as we will show with the Pythagorean theorem later. Furthermore, the area of both triangles is equal and the angles of both triangles is also equal.

Proposition 3.9.4

The sum of the angles of a right triangle other than the right triangle sum up to 90° or $\frac{\pi}{2}$.

Consider a rectangle formed by points A, B, C, D.



Notice that parallel segments $\overline{AC}$ and $\overline{BD}$ are equal in length. Likewise, $\overline{AB}$ and $\overline{CD}$ are also equal in length. $\overline{AD}$ divides the rectangle into two right triangles. By **3.9.3** we know that the two right triangles that make up the rectangle are congruent by our assertion that parallel segments of a rectangle are equal in length.

Theorem 3.9.1

The area of a right triangle is given by $\frac{ab}{2}$ where a and b are the legs of the right triangle.

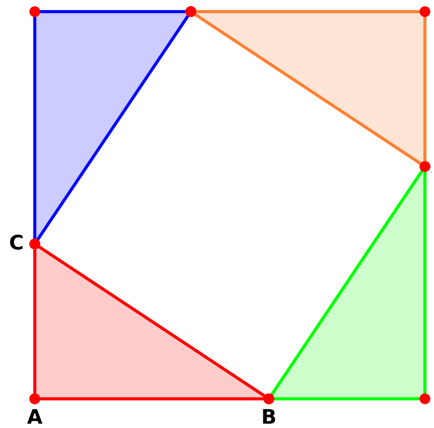
Assuming that area of the rectangle is given by $A = ab$ where a is the length of the segment $\overline{AB}$ and b is the length of $\overline{AC}$ we can say that the two triangles are congruent. Furthermore, the area of one triangle is half the area of the rectangle.

Theorem 3.9.2 Pythagorean Theorem

Suppose that a and b are the lengths of the legs of a triangle and c is the length of the hypotenuse. Then $a^2 + b^2 = c^2$.

We arrange 4 congruent triangles such that a square is formed whose sides are the hypotenuse of the 4 triangles. Arranging it in that way will form a larger outer square.

Proof: Let $a = \overline{AB}$, $b = \overline{AC}$, and $c = \overline{CB}$. Notice that the length of each side of the square is $a + b$. Therefore, the area of the square is $(a + b)^2$. We can write the area of the square as an equality, $(a + b)^2 = c^2 + 4(\frac{ab}{2})$.



$a^2 + 2ab + b^2 = c^2 + 2ab$

$a^2 + b^2 = c^2$ 😄

3.9.1 Exercises

Definition 3.9.3

- A **perpendicular bisector** is a line perpendicular to a segment and whose endpoint lie on the middle of the segment.
- An **angle bisector** is a line that bisects the angle.
- An **altitude** of a triangle is a line perpendicular to an edge and whose endpoint lie on a vertex.

Question 10

Given two points P, Q and an arbitrary point R, Show that the line segments $\overline{PR}$ and $\overline{QR}$ are equal *iff* R lies in the perpendicular bisector of $\overline{PQ}$.

Question 11

Prove that the sum of angles of a triangle equal $180°$.

Question 12

Prove that the area of a generic triangle is equal to half its base times height. $A = \frac{bh}{2}$.

Question 13

Show that the hypotenuse of a right triangle is greater than or equal to the length of either of its legs.

Question 14

(a.) Show that the hypotenuse of a right triangle is greater than or equal to the length of either of its legs.

(b.) Let P be a point and let L be a line. Show that the smallest distance between P and any point M on the line L is Q.

3.10 Congruence

A **mapping** of a set A onto itself is an association between a point P onto another point Q where P and Q are both in A . A mapping is represented with a special arrow $P \mapsto Q$. Here, Q is the value of the mapping at P, or Q corresponds to P under the mapping, or that P is mapped on Q.

A mapping is also known as a **function**, denoted as $F(P)$ where F is a symbol denoting the function and P is a value that is within the **domain** of the function; the domain being the set of all values where F is defined.

Definition 3.10.1

1. A mapping F corresponds to another mapping G if and only if $F(P) = G(P)$ for all values P.

2. If a mapping f maps every value in the set onto a constant C, then we say that F is a constant mapping.

3. The identity mapping of F, denoted with I is a mapping such that $I(F(P))$ for all values P.

4. The identity mapping of F, denoted with I is a mapping such that $I(F(P))$ for all values P.

Suppose that F is a mapping of a set A onto itself, we denote it as $F : A \longrightarrow A$. For now, suppose that the mapping is that of a plane onto itself; that is, $F : X^2 \longrightarrow X^2$. We say that F is *distance perserving* if and only if for every pair of points P and Q in X, the distance between P and Q is equal to the distance between $F(P)$ and $F(Q)$. Mappings that satisfy said biconditional are known as **isometries**.

Theorem 3.10.1

Assuming that F is an *isometry*, the line segment formed by points P and Q, $\overline{PQ}$, under the mapping F is the line segment formed by the mapping of $F(P)$ and $F(Q)$.

Proof: Let R be any point on the line $\overline{PQ}$. Since an isometry preserves distance, we know that the distance of the line formed by P and R and the line formed by $F(P)$ and $F(R)$ are equal. Likewise, the distance between the line formed by R and Q is equal to the line formed by $F(R)$ and $F(Q)$. Therefore, $(P, R) + (R, Q) = (F(P), F(R)) + (F(R), F(Q))$, or $(P, Q) = (F(P), F(Q)$. Since R lies on $\overline{PQ}$ and $F(R)$ lies on the line segment formed by $F(P)$ and $F(Q)$ then $F(P)$ and $F(Q)$ form a line segment $\overline{F(P)F(Q)}$.

To prove that every point on $\bar{(}F(P), F(Q))$ can be expressed as a mapping under F of $R \in \overline{PQ}$. Let $F(R)$ be a point on the segment that is d distance from $F(P)$ and let R be a point on $\overline{PQ}$ that is d distance from P. Since $F(P)$ is a mapping of P under F, it follows that $F(R)$ is a mapping of R under F. 😊

A **fixed point** is a point P such that $P = F(P)$.

Theorem 3.10.2

Assuming that F is an *isometry*, suppose that P and Q are distinct points that are fixed. Then every point on $\overline{PQ}$ is a fixed point of F.

Proof: First we note that if M lies on the segment (P, Q), then $(P, M) = (P, F(M))$ and $(M, Q) = (F(M), Q)$ since isometries preserve distance. Thus, $(P, F(M)) + (F(M), Q) = (P, Q)$ which means that $F(M)$ lies on (P, Q). It follows that $M = F(M)$.

Next consider the situation when M does not lie on the segment (P, Q), but instead lies on a ray passing through P and Q. Then $(P, M) = (P, F(M))$ and $(P, F(M)) = (P, Q) + (Q, F(M))$. It follows that P, Q, and $F(M)$ lie on the same line segment and that $M = F(M)$. If M lies on the ray from Q through P, the proof is similar, but with P and Q swapped. 😊

When we apply two isometries to a plane, we **compose** them. Symbolically, we can write it as $F(G(P))$ where F and G are isometries. We can represent the composite of F and G as a mapping of a point P on the plane.$P \mapsto F(G(P))$. This mapping is called the composite of G and F and is denoted as $F \circ G$.

Question 15

Let ℓ and $\jmath$ be parallel lines. Prove that $F(\ell)$ and $F(\jmath)$ are parallel if F is an isometry.

Chapter 4

Miscellaneous

4.1 Matrices and Linear Maps

Definition 4.1.1

Linear Maps are mappings that have the following properties:

1. Parallel lines stay parallel.
2. Even spacing is preserved ie: even if the spacing between two points change, the spacing between all points is changed consistently.
3. The origin is fixed in place.

Definition 4.1.2

A **vector space** is a set of vectors that satisfy the *field axioms*. There are 6 field axioms:

1. Associativity of addition and multiplication:

   $a + (b + c) = (a + b) + c \qquad a(bc) = (ab)c$

2. Commutativity of addition and multiplication:

   $a + b = b + a \qquad ab = ba$

3. Additive and Multiplicative Identity:

   $\exists 0 \in F \ni a + 0 = a \qquad \exists 1 \in F \ni a \cdot 1 = 1$

4. Additive Inverse:

   $\forall a \in F, \exists - a \ni a + (-a) = 0$ Where $-a$ is called the additive inverse.

5. Multiplicative Inverse:

   $\forall a \in F, \exists a^{-1} \ni a \cdot a^{-1} = 1$ Where a^{-1} is called the multiplicative inverse.

6. Distributivity of multiplication over addition $a \cdot (b + c) = ab + ac$

Given a set of elements G, A **linear combination** in a vector space F is is an element in F of the form $a_1 g_1 + a_2 g_2 \ldots a_i g_i$ Where a_i are scalars and $g_i \in G$. All vectors in a vector space F can be represented as a linear combination of the **basis vectors** of F.

The elements of a subset G of F are said to be **linearly independent** if they cannot be written as a linear combination of another element of G. Otherwise, they are **linearly dependent**.

A **linear subspace** or vector subspace, W of a vector space V is a non-empty subset of V that is *closed* under vector addition and scalar multiplication. This implies that every linear combination of elements of W belong to W.

A subset of a vector space is a **basis** if its elements are linearly independent and *span* the vector space. All **bases** of a vector space have the same cardinality which is called the **dimension** of the vector space.

Consider the basis vectors,

$$i = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \; j = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \; k = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The linear subspace formed by the three vectors is clearly $\mathbb{R}3$. Thus, we say that the **span** of the vector space with basis ijk is $\mathbb{R}^3$.

Given a subset G of a vector space V, the span of G is the smallest linear subspace of V that contains G. The span of G is also the set of all linear combinations of elements of G. If W is the span of G, then G *spans* or *generates* W and that G is a *spanning set* or generating set of W.

The standard bases vectors for a vector space are known as the ijk coordinates. But calling it ijk limits the coordinates to three dimensions. To generalize it, the standard bases vectors for any n dimensional vector space are the unit orthogonal vectors of that space. So in $\mathbb{R}^2$,

$$i = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } j = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

are the standard bases. A linear map from ijk coordinates to another coordinate system is usually represented with matrices; this operation is called a linear transformation or a change of bases. Generally, multiplying any vector in the ijk space by a transformation matrix gets us the output of the linear map. To see why this is true, we first note that every vector in the **span** of the vector space is a linear combination of the **bases** of the space. Therefore, we can write all vectors in terms of the bases vectors that we choose

$$\begin{bmatrix} x \\ y \end{bmatrix} = a_1 \begin{bmatrix} i_1 \\ i_2 \end{bmatrix} + a_2 \begin{bmatrix} j_1 \\ j_2 \end{bmatrix}$$

From this information, we can replace i and j in the equation with the new basis vectors and we can do this with a very nice mathematical construct known as a **matrix**

$$\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = x \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + y \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 x + b_1 y \\ a_2 x + b_2 y \end{bmatrix}$$

But note that this is only true if the bases for $\begin{bmatrix} x & y \end{bmatrix}$ are the unit vectors. See why this is true. If the bases for the vector happen to be another transformation of the standard angles, we will need to find the original scalars which can be found with a system of linear equations which will be discussed later.

4.1.1 Determinant

The determinant can be described as a scalar that describes the factor in which a space changes in a given transformation.

eg: $\begin{bmatrix} 3 & 2 \\ 0 & 2 \end{bmatrix}$ scales ij by a factor of 6. See why this is the case given the above definition.

Remember that in a linear transformation, gridlines remain parallel and evenly spaced (by the property that lines remain lines after a linear transformation) Therefore, the factor in which the bases are scaled after a change of base operation is the factor at which all other vectors will be scaled. This factor is known as the **determinant**.

Proposition 4.1.1

The determinant is 0 if it condenses all points in a n dimensional space into a $n - k$ dimensional space where $k \leqslant n$.

The determinant can also be a negative number. To explain, it is easier to start with the case where the vector space is $\mathbb{R}^2$. Notice that in the default orientation, the standard basis j is to the left hand of i. If a transformation results in j to the right hand of i, then we say that the transformation **inverses the orientation**. Whenever orientation is flipped, the determinant is negative. eg:

$$\begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$$

flips orientation because i corresponds to $\begin{bmatrix} 1 & 1 \end{bmatrix}$ and j corresponds to $\begin{bmatrix} 2 & -1 \end{bmatrix}$ in the transformation and $\begin{bmatrix} 2 & -1 \end{bmatrix}$ is obviously to the right hand of $\begin{bmatrix} 1 & 1 \end{bmatrix}$.

For $\mathbb{R}^3$, the right hand rule for determinants states that the determinant is positive if the basis form a right hand coordinate system ie: if letting the index finger point to i and the middle finger point to j, the thumb naturally points to k. We agree to say that in the default orientation ijk is *right handed*.

Therefore, if you need to use your left hand so that the thumb faces k, then the basis form a left hand coordinate system and the determinant is negative.

Chapter 5

Solutions

5.1 Numbers

Solution 1

(a.) Prove that if x is even, then x^2 is even

$x = 2n,\ n \in \mathbb{Z}$

$x^2 = 4n^2$

$x^2 = 2(2n^2)$

(b.) Prove that the converse it also true

Suppose x is not even, then x is odd. $x^2 = (2n+1)(2n+1)$ for $n \in \mathbb{Z}$

$x^2 = 4n^2 + 4n + 1$

$x^2 = 2(2n^2 + 2n) + 1$

which contradicts our assertion that x^2 is odd. Therefore x must be even.

Note that a direct way of proving (b.) would required proving that the square of an even number is even.

Solution 2

(a.) Prove that if x is odd, then x^3 is odd

$x = 2n+1,\ n \in \mathbb{Z}$

$x^3 = (2n+1)(2n+1)(2n+1)$

$x^3 = 8n^3 + 12n^2 + 6n + 1$

$x^3 = 2(4n^3 + 6n^2 + 3n) + 1$

(b.) Prove that the converse is also true

Suppose that x is even

$x^3 = (2n)(2n)(2n)$ for some $n \in \mathbb{Z}$

$x^3 = 8n^3 = 2(4n^3)$

But we asserted that x^3 is odd, therefore we were wrong to assume that x is even.

Solution 3

(a.) Prove that the sum of two even numbers is even

$2n + 2m = 2k,\ n, m, k \in \mathbb{Z}$

$2(n + m) = 2k$ let $n + m = k$

(b.) Prove that the sum of two odd numbers is also even

$(2n + 1) + (2m + 1) = 2k,\ n, m, k, \in \mathbb{Z}$

$2(n + \frac{1}{2}) + 2(m + \frac{1}{2}) = 2k$

$2(n + m + 1) = 2k$

Solution 4

x and y are positive real numbers. If $x < y$ then show that $x^2 < y^2$

Suppose that $x^2 \geqslant y^2$ then

$y^2 - x^2 \leqslant 0$

$(y + x)(y - x) \leqslant 0$ *Note:* $(y - x) \geqslant 0$ because $x < y$

We get that $y \leqslant x$ and $y \leqslant -x$ which is a contradiction because $y > x$ and y is positive

Solution 5

Given $a, b, c \in \mathbb{Z}$, if $a^2|b$ and $b^3|c$ show that $a^6|c$

$b = a^2 n$

$c = b^3 m$

$c = (a^2 n)^3 m$

$c = a^6 n^3 m$

Solution 6

Given $a, b, c \in \mathbb{Z}$, if $b|a^2$ and $c|b^3$ show that $c|a^6$

$a^2 = bn$

$b^3 = cm$

$b = \frac{a^2}{n}$

$\frac{a^6}{n^3} = cm$

$a^6 = cmn^3$

Solution 7

Show that $\binom{2n}{n}$ is even for all whole numbers n

$|M| = 2n$

$\forall X_i \subseteq M$ where $|X_i| = n$, $|M - X_i| = 2n - n = n$

For each X_i, there is a corresponding X_j where $X_i \cap X_j = \{\}$. Therefore, the amount of subsets of M must be even.

Solution 8

Show that $\sqrt{2}$ is irrational

Suppose that $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{a}{b}$ for some integers a and b.

Since all rational numbers have the property that a and b cannot share a common factor, we can assume that $\frac{a}{b}$ is reduced.

$\sqrt{2}b = a$

$2b^2 = a^2$ it was proven that a is even in an earlier *lemma*.

So, $a = 2n$ for some $n \in \mathbb{Z}$

$b^2 = 2n^2$.

Since a and b are both even, they share a common factor–which is a contradiction because all fractions can be represented in reduced form. So $\sqrt{2}$ must be irrational.

Solution 9

Prove that $n!$ is always even if $n > 1$

The product of two even numbers is even:

$(2n)(2k)$

$2(nk)$

The product of an even number and an odd number is even:

$(2n)(2k + 1)$

$4nk + 2n$

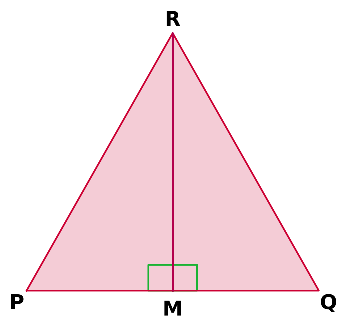
$2(2nk + n)$

Since the factors of $n!$ has at least one even number, $n!$ is even.

5.2 Geometry

Solution 10

Given two points P, Q and an arbitrary point R. The line segments $\overline{PR}$ and $\overline{QR}$ are equal *iff* R lies in the perpendicular bisector of $\overline{PQ}$.



Notice that if R lies on the perpendicular bisector of $\overline{PQ}$, then the perpendicular bisector $\overline{MR}$, where M is a point that divides QR, divides the triangle formed by $\overline{PR}$, $\overline{QR}$ and $\overline{PQ}$ into two right triangles by definition of a perpendicular bisector.

We can then use the pythagoren theorem to see that the $\overline{PM}^2 + \overline{MR}^2 = \overline{MQ}^2 + \overline{MR}^2 = \overline{PR}^2 = \overline{QR}^2$. Thus, $\overline{PR} = \overline{QR}$.

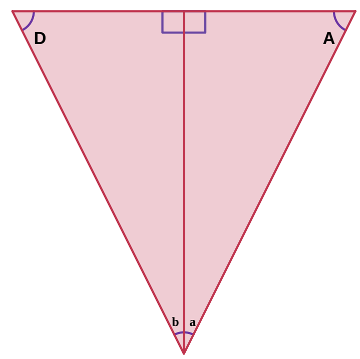
The converse follows from the pythagorean theorem.

$\overline{MR}^2 + b^2 = \overline{PR} = \overline{QR}$

Thus, $\overline{PM} = \overline{MQ}$. Which proves that M bisects $\overline{PQ}$.

Solution 11

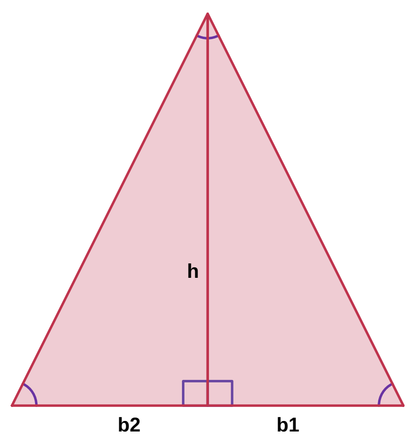
Prove that the sum of angles of a triangle equal 180°.



We begin by splitting the generic triangle into two right triangles by drawing an *altitude*. In deciding the altitude, we choose to draw the altitude that passes through the vertex with the largest angle. This gurantees that the altitude will always be inside the triangle. Notice that $D + b = 90°$ because the sum of angles other than the right angle is $90°$. Likewise, $A + a = 90°$. Therefore, $D + b + A + a = 180$.

Solution 12

Prove that the area of a generic triangle is equal to half its base times height. $A = \frac{bh}{2}$.



We draw an altitude across the triangle such that it is split into two right triangles. The area of the whole triangle is $\frac{b_1 h}{2} + \frac{b_2 h}{2}$, or $\frac{h(b_1+b_2)}{2} = \frac{bh}{2}$.

Solution 13

(a.) Show that the hypotenuse of a right triangle is greater than or equal to the length of either of its legs.

We prove this by contradiction. Suppose that the length of an arbitrary leg a is greater than the length of the hypotenuse c. Then $a > c$ and $a^2 > c^2$. Let b be the length of the other leg, then $a^2 + b^2 > c^2 + b^2$. This inequality implies that $a^2 + b^2 > c^2$ which contradicts the pythagoren theorem.

(b.) Let P be a point and let L be a line. Show that the smallest distance between P and any point M on the line L is Q.

The proof follows from **(a.)**

Solution 14

Let ℓ and $\mathscr{s}$ be parallel lines. Prove that $F(\ell)$ and $F(\mathscr{s})$ are parallel if F is an isometry.

Since the shortest distance between two points is a straight line and isometries are distance preserving, $F(\ell)$ and $F(\mathscr{s})$ must be parallel. If they were not parallel, then the distances between endpoints would be different which would contradict our assumption that F is an isomorphism.

Solution 15

Let ℓ and $\mathscr{s}$ be perpendicular lines. Prove that $F(\ell)$ and $F(\mathscr{s})$ are perpendicular if F is an isometry.

If we let the two lines intersect at an endpoint, We can model the distance between the distinct endpoints of the two lines as $\mathscr{c}$ in the equation $\ell^2 + \mathscr{s}^2 = \mathscr{c}^2$. Suppose that ℓ and $\mathscr{s}$ are not perpendicular. Then if the angle between the two is acute, the distance between the distinct endpoints can be modeled as c in the equation $\mathscr{a}^2 + \mathscr{b}^2 = \mathscr{c}^2$ where $\mathscr{a}$ is the altitude of the triangle formed by ℓ, $\mathscr{s}$ and $\mathscr{b}$ is the line from the distinct endpoints of ℓ and $\mathscr{s}$. On the otherhand, if the angle is obtuse, the distance between the two endpoints can be modeled as $\mathscr{c}$ in the equation $\mathscr{h}^2 + (\mathscr{w} + \mathscr{s})^2 = c^2$ where $\mathscr{h}$ and $\mathscr{w}$ is the height and width of the distinct endpoint of ℓ respectively. Therefore, we've shown that the distance between distinct endpoints differ when ℓ and $\jmath$ are not perpendicular.

Chapter 6

Index

6.1 Logic Laws

Law	Definition	Symbolic Representation
Modus Ponens	The consequence follows from the premise.	$((A \rightarrow B) \wedge A) \vdash B$
Modus Tollens	If the premise is false, then the conclusion is false.	$((A \rightarrow B) \wedge \neg A) \vdash \neg B$
Hypothetical Syllogism	If A implies B and B implies C, then A implies C.	$(A \rightarrow B) \wedge (B \rightarrow C) \vdash (A \rightarrow C)$
Disjunctive Syllogism	If A or B, then not B implies A and vice-versa.	$((A \vee B) \wedge \neg B) \vdash A$
Constructive Dilemma	If A implies B and C implies D, then A or C entails B or D.	$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee C) \vdash (B \vee D)$
Destructive Dilemma	If A implies B and C implies D, then not B or not D entails not A or not C.	$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (\neg B \vee \neg D) \vdash (\neg A \vee \neg C)$
Bidirectional Dilemma	If A implies B and C implies D, then A or not C entails B or not D.	$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee \neg C) \vdash (B \vee \neg D)$
Simplification	If A and B, then A holds.	$(A \wedge B) \vdash A$
Conjunction	If A, B is true respectively then A and B is true.	$A, B \vdash (A \wedge B)$
Addition	If A, then A or B holds.	$A, B \vdash (A \vee B)$
Composition	If A implies B and A implies C and A, then both B and C holds.	$(A \rightarrow B) \wedge (A \rightarrow C) \vdash (A \rightarrow (B \wedge C))$
De Morgan's Law(1)	The negation of the proposition A and B is the following: not A or not B.	$\neg(A \wedge B) \vdash (\neg A \vee \neg B)$

De Morgan's Law(2)	The negation of the proposition A or B is the following: not A and not B.	$\neg(A \vee B) \vdash (\neg A \wedge \neg B)$
Commutation(1)	The proposition A and B is equivalent to B and A.	$(A \wedge B) \vdash (B \wedge A)$
Commutation(2)	The proposition A or B is equivalent to B or A.	$(A \vee B) \vdash (B \vee A)$
Commutation(3)	The proposition "A is equivalent to B" is the same as "B is equivalent to A".	$(A \equiv B) \vdash (B \equiv A)$
Association(1)	The proposition (A and B) and C is the same as A and (B and C).	$(A \wedge B) \wedge C \vdash A(B \wedge C)$
Association(2)	The proposition (A or B) or C is the same as A or (B or C).	$(A \vee B) \vee C \vdash A(B \vee C)$
Distrbution(1)	The proposition A and (B or C) is the same as (A and B) or (A and C).	$A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$
Distrbution(2)	The proposition A or (B and C) is the same as (A or B) and (A or C).	$A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C)$
Double Negation	The negation of not A, is equivalent to A.	$A \vdash \neg\neg A$
Transposition	If A implies B, then not A implies not B	$(A \rightarrow B) \vdash (\neg A \rightarrow \neg B)$
Material Implication	If A implies B, then not A or B	$(A \rightarrow B) \vdash (\neg A \vee B)$
Material Equivalence(1)	If A implies B and vice-versa, then A implies B and B implies A both hold.	$(A \leftrightarrow B) \vdash (A \rightarrow B) \wedge (B \rightarrow A)$
Material Equivalence(2)	If A implies B and vice-versa, either A and B holds or not B and not A holds.	$(A \leftrightarrow B) \vdash (A \wedge B) \vee (\neg A \wedge \neg B)$

Material Equivalence(3)	If A implies B and vice-versa, then (A or not B) holds or (not A or B) holds.	$(A \leftrightarrow B) \vdash (A \lor \neg B) \land (\neg A \lor B)$
Exportation	If A and B implies C, then A implies that B implies C.	$(A \land B) \longrightarrow C \vdash A \longrightarrow (C \longrightarrow B)$
Tautology(1)	A and A is equivalent to A.	$(A \land A) \vdash A$
Tautology(2)	A or A is equivalent to A.	$(A \lor A) \vdash A$
Terium non datur	Given a proposition P, either P or not P.	$\vdash P \lor \neg P$
Law of Non-Contradiction	The proposition "it is not the case that P and not P" is true.	$\vdash \neg(P \land \neg P)$

Table 6.1: List of logic laws courtesy of Wikipedia.

Note:-

Some of the logic laws such as *Material Equivalence(2)* and *Terium non datur* are obviously exclusive which is why an exclusive-or $\veebar$ is ommited.