SYDE 113 Lecture Notes

Prof. Chrystopher L. Nehaniv
University of Waterloo

with assistance and transcription by Seyedeh Maryam Hosseini

1 Lecture 1. (September 8, 2020)

1.1 Number Systems

Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Note. Zero is an even number since it is multiple of two.

Integer numbers: $\mathbb{Z} = \{0, -1, 1, -2, 2, \dots\}$

Rational numbers: $\mathbb{Q} = \{\frac{p}{q} : \quad p, q \in \mathbb{Z}, \quad q \neq 0\}$.

Note some numbers have multiple representations, e.g. $\frac{2}{6} = \frac{1}{3}$.

Real numbers $\mathbb{R}$. These numbers can be given by decimal expansions. This includes numbers that have a non-terminating and non-repeating decimal expansion, such as $\sqrt{2}, \pi$, irrational real numbers. $\pi \approx 3.14159265358979\dots$. These are not in $\mathbb{Q}$. A real number is rational (in $\mathbb{Q}$) if and only if it has a terminating or repeating decimal expansion.

Note. $\frac{1}{3} = 0.333\dots$, then $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 0.999\dots$, which means $1 = 0.999\dots$. Therefore, we have more than one representation for the same number. These two representations each encode a different 'recipe' or 'history' or 'trajectory' for getting to the number: For example, $0.999\dots$ starts at 0, adds 9 tenths, then adds 9 one-hundredths, then 9 one-thousandths, etc., getting us closer and closer to 1, traveling $\frac{9}{10}$ of the remaining way with each new digit 9. In contrast, the decimal expansion $1.000\dots$ says to start at 1 and stay there, adding 0 tenths, hundredths, etc. These are two different trajectories for getting to 1. This means the decimal expansion encodes more information than just the numbr: includes a way to get to the number.

This relates to the notion of *limits* that you will see in your calculus class. These different representations are *not* the numbers themselves, but representations that lead us to them.

Complex numbers $\mathbb{C}$ extend the reals by introducing a new number i where $i^2 = -1$

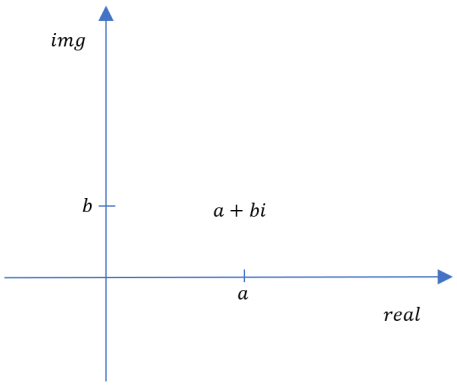

Figure 1: Complex Numbers. A two-dimensional plane with real and imaginary axes. The real line is the horizontal axis, with the orthogonal "imaginary" axis in a new dimension where a new number i with $i^2 = -1$ is one unit from the origin

Note. Real numbers are one-dimensional while complex numbers are 2D.

1.2 Coordinate Systems

n-dimensional space

In 1D, a line, you can coordinatize by choosing the origin, a positive direction and a unit length.

The following are coordinate systems on n-dimensional spaces. They assign to each point an n-tuple of real numbers:

$$\mathbb{R}^1 = \{x_1 : x_1 \in \mathbb{R}\}$$

$$\mathbb{R}^2 = \{(x_1, x_2) : x_i \in \mathbb{R}, \quad 1 \leq i \leq 2\}$$

$$\mathbb{R}^n = \{(x_1, \ldots x_n) : \quad x_i \in \mathbb{R} \quad 1 \leq i \leq n\}$$

The way of writing real numbers using decimal expansions and the n-tuples in $\mathbb{R}^n$ for points in n-dimensional space that we saw above are both examples of *coordinate systems* that allow us to exactly locate particular points in a set.*

Cartesian coordinatization: In these "Cartesian" coordinate systems on n-dimensional space using the n-tuples of $\mathbb{R}^n$, you need to choose origin and orthogonal directions, (and unit length).

For a two-dimensional plane, this comprises choosing the origin and two axes through it:

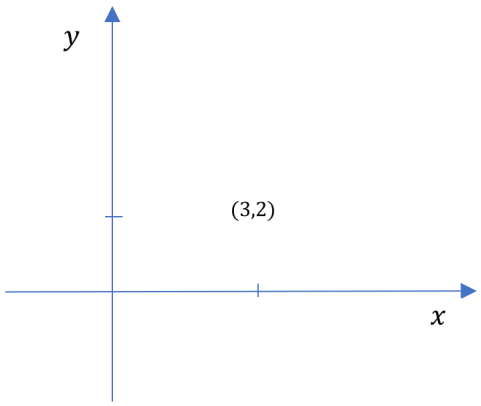

Figure 2: Cartesian coordinate system

Polar coordinatization: In this coordinate system, you need to choose an origin and direction heading out from it.

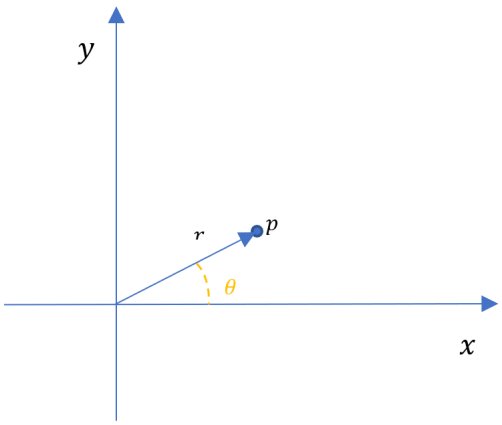

Figure 3: Polar coordinate system

*The decimal expansion tells us how to get to the number by successively adding different numbers of units, tenths, hundredths, and so on, with how many of each encoded by the digits. The n-tuple $(x_1, \ldots, x_n) \in \mathbb{R}^n$ tells how many units to go from the origin in each of n orthogonal directions along the axes to find a point in the n-dimensional space.

Here p is a point with polar coordinates (r, θ), where r is the distance from the origin and θ is the angle measured in the counter-clockwise direction from the direction we chose, so that $r \geq 0, \quad 0 \leq \theta < 2\pi$. Then θ gives an angle between $0°$ and $360°$. Alternatively, we often take $-\pi < \theta \leq \pi$ (i.e., with angle between $-180°$ and $180°$). Notice that the origin has multiple representations in polar coordinates.

Note. The polar coordinates can be transformed to Cartesian coordinates, and vice versa, using the formulae below:

Polar coordinates (r, θ)	Cartesian coordinates (x, y)
$r = \sqrt{x^2 + y^2}$	$x = r\cos(\theta)$
$\theta = \arctan(\frac{y}{x})$	$y = r\sin(\theta)$

The formula for θ comes from the fact that $\frac{y}{x} = \frac{r\cos\theta}{r\sin\theta} = \frac{\cos\theta}{\sin\theta} = \tan\theta$, and arctan is the inverse of tan.

Caveat. Since arctan is a periodic function, you need to be careful about the sign of the x and y to find the quadrant that θ belongs to.

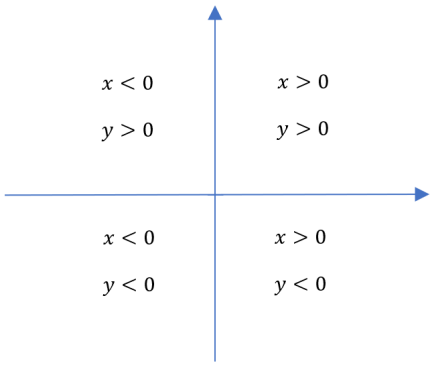

Figure 4: Quadrants and their corresponding x and y signs.

You may need to adjust θ by $+\pi$ or $-\pi$ ($180°$) since for example points $(2, 2)$ and $(-2, -2)$ have the same y/x but are in opposite quadrants. Also, for $x = 0$ we can't divide by zero, but have $\theta = \pi/2$ or $\theta = -\pi/2$ depending on the sign of y.

1.3 Metric Spaces

For the real line, we have one notion of distance between points is given by absolute value:

- for x, y in $\mathbb{R}^1$
  $d(x, y) = |x - y|$

In higher dimensions, there are several different useful distance metrics:

- The usual *Euclidean distance* (also called L_2 distance):
  For two points (x_1, y_1) and (x_2, y_2) in $\mathbb{R}^2$

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

- L_1 distance (*Manhattan* or taxicab distance)

$$L_1((x_1, y_1), (x_2, y_2)) = |x_1 - x_2| + |y_1 - y_2|$$

- L_∞ distance (*max distance* or Chebyshev distance)

$$L_\infty = \max\{|x_1 - x_2|, |y_1 - y_2|\}$$

Similarly, L_1, L_2, and L_∞ are defined in the analogous way on n-dimensional space $\mathbb{R}^n$. On $\mathbb{R}^1$ all three metrics agree. But they differ for $n > 1$.

Axioms. For X a metric space (set) with distance measure d, it is required that : $d : X \times X \to \mathbb{R}^+$, i.e., d is a function from ordered pairs of locations in X to non-negative real numbers.

To be a metric space, the following axioms hold $\forall x, y, z \in X$ ("for all locations x, y, z in X"),

1. $d(x, y) = d(y, x) \quad \forall x, y \in X$ (symmetry)
2. $d(x, y) = 0$ if and only $x = y$ (definiteness)
3. $d(x, y) + d(y, z) \geq d(x, z)$ (triangle inequality)

Other examples of metric spaces include distance travelling along the surface of a sphere (the earth). These are not the straight-line distance (since to get from Waterloo, Ontario to Sydney, Australia, we travel on the surface and don't go in a straight line through the earth!). Another metric space is a torus (donut) on whose surface a spider crawls to get to a fly.

There may be many different shortest paths to get from one point to another in these spaces. That same is true with the *max* and *Manhattan* distance, as we saw in examples in class.

But all satisfy the triangle inequality: if we travel from Waterloo to London, England and from there to Australia, the total distance is at least as much as when we travel directly from Waterloo to Australia!

Different metrics on spaces give different notions of geometry...

Note. The XOR and AND binary operations are

XOR	0	1
0	0	1
1	1	0

AND	0	1
0	0	0
1	0	1

The XOR operation results in 1, if exactly one the inputs is 1. The AND function results in 1, if both inputs are 1.

[Discussed in only BME 1A group.]

2 Lecture 2. (September 10, 2020)

2.1 Set-Theoretic Operations

Definition. A *set* is a collection of things and is determined by its members.
These are two examples of sets:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

$$A = \{a, b, c\}$$

The notation $\in$ is used to express that an element is a member of a set; and $\notin$ is used to indicate that an element is not a member of a set. For example:

$$a \in A \quad \text{(read this as "}a \text{ is an element of } A\text{)}$$

$$d \notin A \quad \text{(read this as "}d \text{ is not an element of } A\text{"}$$

Definition. Suppose A and B are two sets. If $x \in A$ implies that $x \in B$, then A is a *subset* of B. That is,

$$A \subseteq B$$

means that same thing as

$$\forall x \, (x \in A \Rightarrow x \in B)$$

Here the symbol $\forall$ means "for all".
We sometimes read $A \subseteq B$ as "A is contained in B". This actually means that all the members of A are also members of B, as we just saw.

Sets A and B are equal if and only if they have the same members; or equivalently, they are contained in each other:

$$A = B \quad \Longleftrightarrow \quad A \subseteq B \quad \text{and} \quad B \subseteq A$$

Note. The order and repetition of elements in a set do not matter at all. For example, both these sets below are equal:

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

Definition. The *union* of two sets A and B is a collection of elements that are either in A or B:

$$A \cup B = \{x : \quad x \in A \quad \text{or} \quad x \in B\}$$

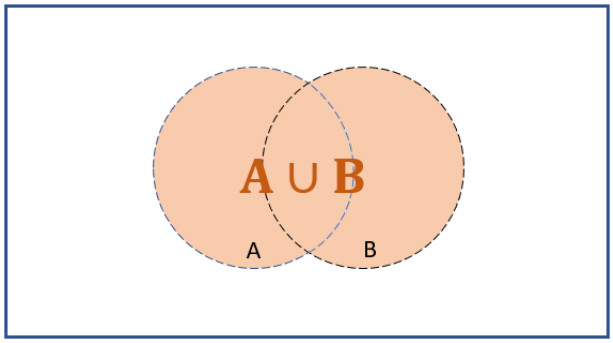

Figure 5: Venn diagram for the union of two sets.

Definition. The *intersection* of two sets A and B is a collection of elements that are in both A and B:

$$A \cap B = \{x : \quad x \in A \quad \text{and} \quad x \in B\}$$

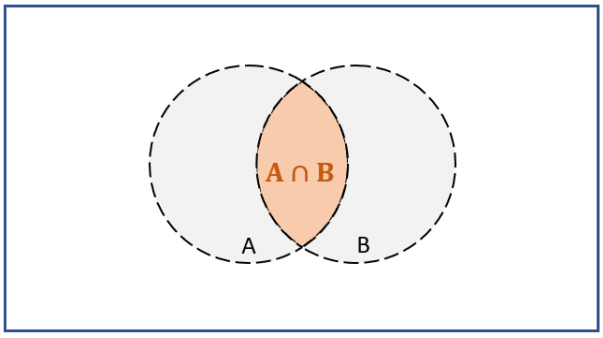

Figure 6: Venn diagram for the intersection of two sets.

For example, the intersection and union of $2\mathbb{N}$ (the even numbers) and $3\mathbb{N}$ (the multiples of 3) are:

$$\begin{aligned} 2\mathbb{N} &= \{0, 2, 4, 6, \dots\} \\ 3\mathbb{N} &= \{0, 3, 6, 9, \dots\} \\ 3\mathbb{N} \cap 2\mathbb{N} &= \{0, 6, 12, 18, \dots\} = 6\mathbb{N} \\ 3\mathbb{N} \cup 2\mathbb{N} &= \{0, 2, 3, 4, 6, 8, 9, \dots\} \end{aligned}$$

Definition. We write $A \setminus B$ for the set $\{a \in A : b \notin B\}$. The backslash $\setminus$ is read "*set minus*" (or "without"). The set $A \setminus B$ is the set obtained by removing any elements of B from A.

2.2 De Morgan's Laws

Definition. We often have a set X in mind as a *universe of discourse* containing everything that we are talking about in some particular context. For a subset A of this universal set X, the *complement* of A is all the elements of X which are not in A. It is denoted by $\overline{A}$ (and called the complement of A in X) or by $X \setminus A$ ("X without A") for a given universe set X.

$$\overline{A} = X \setminus A = \{x \in X : x \notin A\}$$

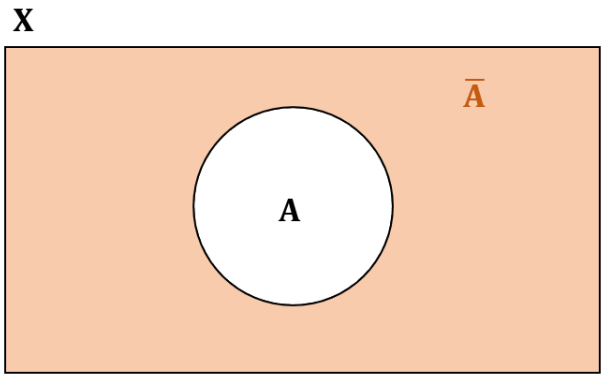

Figure 7: Complement of set A given the universe set X

De Morgan's law relates complement, intersection, and union. Actually there are two De Morgan's laws:

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$

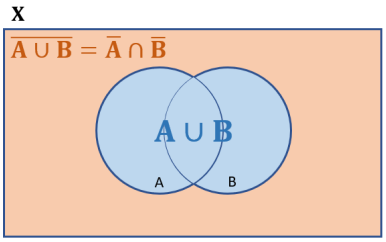

Figure 8: De Morgan's Law I. Complement of a Union is the Intersection of the Complements

Proof.

$$\begin{aligned} & x \in \overline{A \cup B} \\ \Leftrightarrow\ & x \notin A \cup B \\ \Leftrightarrow\ & x \notin A \quad \text{and} \quad x \notin B \\ \Leftrightarrow\ & x \in \overline{A} \quad \text{and} \quad x \in \overline{B} \\ \Leftrightarrow\ & x \in \overline{A} \cap \overline{B} \end{aligned}$$

This shows $\overline{A \cup B}$ and $\overline{A} \cap \overline{B}$ have exactly the same members. So these two sets are equal.

- $\overline{A \cap B} = \overline{A} \cup \overline{B}$

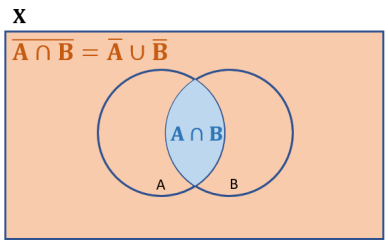

Figure 9: De Morgan's Law II. Complement of an Intersection is the Union of the Complements

Proof. For any arbitrary element x in the universal set X,

$$\begin{aligned} & x \in \overline{A \cap B} \\ \Leftrightarrow\ & x \notin A \cap B \\ \Leftrightarrow\ & x \notin A \quad \text{or} \quad x \notin B \\ \Leftrightarrow\ & x \in \overline{A} \quad \text{or} \quad x \notin \overline{B} \\ \Leftrightarrow\ & x \in \overline{A} \cup \overline{B} \end{aligned}$$

This shows the sets $\overline{A \cap B}$ and $\overline{A} \cup \overline{B}$ have the same members, so they are the same set.

2.3 Cartesian Product of Sets: Ordered Pairs and Tuples

Definition. Let A and B be two sets. The *direct product* of A and B is the set of all ordered pairs where the first one is a member of A and the second one is a member of B:

$$A \times B = \{(a, b) : \quad a \in A, \quad b \in B\}$$

This is also called the *Cartesian product* of sets A and B, simply the *product* of A and B. This is a way of "multiplying" sets.

For example, if $A = \{a_1, a_2\}$ and $B = 1, 2, 3$, then

$$A \times B = \{(a_1, 1), (a_1, 2), (a_1, 3), (a_2, 1), (a_2, 2), (a_2, 3)\}$$

Also, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$.

Additionally, the idea of direct product of sets can be generalized to more than two sets:

$$A \times B \times C = \{(x, y, z) : x \in A, y \in B, z \in C\}$$

The members of the set $A \times B \times C$ are ordered 3-tuples.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_k \in A_k, \quad 1 \leq k \leq n\}$$

Here the product is comprised on n-tuples with a member of A_k in position k.

We have already seen Cartesian products and n-tuples when we coordinatized n-dimensional space.

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \ldots \mathbb{R}}_{\text{n copies}}$$

2.4 Functions

Definition. A *function* $f : X \to Y$ is a 'machine' or rule that assigns for each input x an unique $y \in Y$. For a given input $x \in X$ it gives one and only one output value $f(x)$ in Y. If we give it the same input x later, it will still give $f(x)$ later.

The mapping below is an example of a function, where

$$f(1) = a, \quad f(2) = a, \quad f(3) = b$$

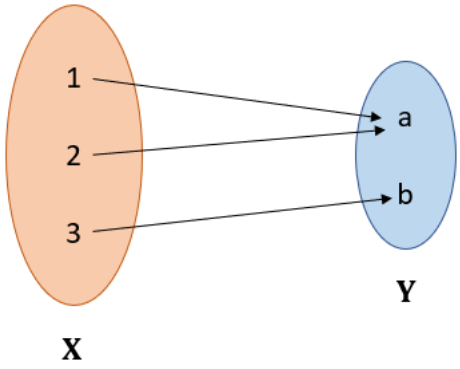

Figure 10: An example of a function.

Definition. The *graph* of function $f : X \to Y$ is the set of ordered pairs as follows:

$$\#f = \{(x, f(x)) \quad : \quad x \in X\}$$

Notice that the graph of f is a subset of $X \times Y$ since $f(x) \in Y$. That is, $\#f \subseteq X \times Y$.

Note. A function that maps X to Y can be expressed by either of the following notations:

$$f : X \to Y$$

$$X \xrightarrow{f} Y$$

Given function $f : X \to Y$, the set X is called the *domain* (or source) of f, and Y is called the *codomain* (or target) of f.

Note. The function might not hit every element of Y. For example, the function g below does not hit every element in its target $\mathbb{N}$:

$$\mathbb{N} \xrightarrow{g} \mathbb{N}$$

$$g(n) = 2n$$

Definition. The *image* of the function g is the set of elements in the target, which are hit by some elements in its domain. More specifically, the image of $f : X \to Y$ is

$$\text{Image of } f = f(X) = \{y \in Y : \exists\, x \in X \quad \text{with } f(x) = y\}$$

.

The symbol $\exists$ is read as "there exists".

For example, if $g : \mathbb{N} \to \mathbb{N}$ and $g(n) = 2n$, then the image of g is $g(\mathbb{N}) = 2\mathbb{N}$, the even numbers $\{0, 2, 4, \dots\} \subset \mathbb{N}$. (This is a *proper subset* of $\mathbb{N}$). Therefore, the function g does not hit all the elements in $\mathbb{N}$.

2.5 Three Kinds of Functions

- **Surjective (or onto).**

  Function f is *surjective* if Image of $f = Y$. We say f maps *onto* Y.

  For example, the function $h : \mathbb{R} \to \mathbb{R}, \quad h(r) = \frac{r}{2}$ hits every real number, meaning that the Image of $f = h(\mathbb{R}) = \mathbb{R}$. Therefore, the function h is an onto function.

- **Injective (or one-to-one).**

  A function is *injective* if it does not send any two points into the same place. We then also say f is *one-to-one*. Mathematically, the function f is injective if for all x and x' in X the following holds:

  $$\text{if } x \neq x' \text{ then } f(x) \neq f(x')$$

  which means that different points in the domain have to go to different places. We can also use the equivalent contrapositive formulation of this implication; the function f is injective if for all $x, x' \in X$:

  $$\text{if } f(x) = f(x'), \text{ then } x = x',$$

  which means that if two points go to the same place, they are the same.

- **Bijective (or one-to-one correspondence).**

  A function is bijective, if it is both injective and surjective. A bijective function is a one-to-one correspondence, which means that for every member of the domain, there is a unique there is a unique member in codomain, and for every member of the codomain there is a unique element of the domain. For example, function $h : \mathbb{R} \to \mathbb{R}, \quad h(r) = \frac{r}{2}$ is bijective.

  In the case of a bijective function, the function has an *inverse* given by sending each member of the target to the unique member of the source that maps to it.

Remark: We avoid the ambiguous term "range'. some people mean the codomain of a function when the talk about range, while others mean the image of the function. So you will need to check which they mean.

Whether or not a function is surjective depends on its target. You can always make a function surjective if you replace its target by its image.

Whether or not a function is injective only depends on whether it maps two points to the same place.

So, if you have an injective function $f : X \to Y$ you can make it into a bijection by restricting its codomain. $f : X \to Image(f)$.

2.6 Notations

2.6.1 Summation Notation.

We use $\sum$ which is the capital Greek letter sigma to denote summation. It is useful when you want to add up a lot of elements. For example:

$$\sum_{k=0}^{n} f(x_k) = f(x_0) + f(x_1) + \cdots + f(x_n)$$

This says to add up the values of f at the points x_k as the index k goes from 0 to k.
(Note: This is similar to a loop in programming.)

Here is how to write summation of the first n positive natural numbers:

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + n$$

The L_1 distance between two points $p = (x_1, x_2, x_3, x_4)$ and $q = (y_1, y_2, y_3, y_4)$ in $\mathbb{R}^4$ can be written in this way:

$$L_1(p, q) = \sum_{k=1}^{4} |x_k - y_k| = |x_1 - y_1| + |x_2 - y_2| + |x_3 - y_3| + |x_4 - y_4|$$

The next example shows adding up the first 100 positive even numbers, and factoring out their common factor 2:

$$\sum_{k=1}^{100} 2k = 2(\sum_{k=1}^{100} k)$$

2.6.2 Product Notation.

For this we use the capital Greek letter π to denote a product. It is useful when you want to multiply a lot of elements. For example:

$$\prod_{k=1}^{10} f(x_k) = f(x_1) \times f(x_2) \times \dots f(x_{10})$$

Factorial: product of positive natural numbers up to n
$6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1$

We can write this using the product notation:

$$n! = \prod_{k=1}^{n} k = n \times (n-1) \times \cdots \times 1$$

Note. The factorial function also has a *recursive* definition:

$$(n+1)! = (n+1) \times n!$$

This gives the value of the function in terms of previously defined values. We can apply the recursive definition til we get down to $n = 0$. There it is defined that $0! = 1$.

2.7 Empty Set.

The set without any members is called the *empty set* and is denoted by $\{\}$ or $\emptyset$. Also, the empty set is the subset of all set. Why? All its elements are in any set.

If you sum over an empty set of indices, the result is zero. If take a product over an empty of indices, the result is 1.

3 Lecture 3. (September 14, 2020)

3.1 Trigonometry

Trigonometry studies the relationship between angles and side lengths in a triangle.

3.1.1 How to think of cosine and sine

Let θ be any angle. Consider the unit circle (radius 1) with point (x, y) on the circle at angle θ, as measured counterclockwise from the positive horizontal axis. Since this is a unit circle, $x^2+y^2 = 1$.

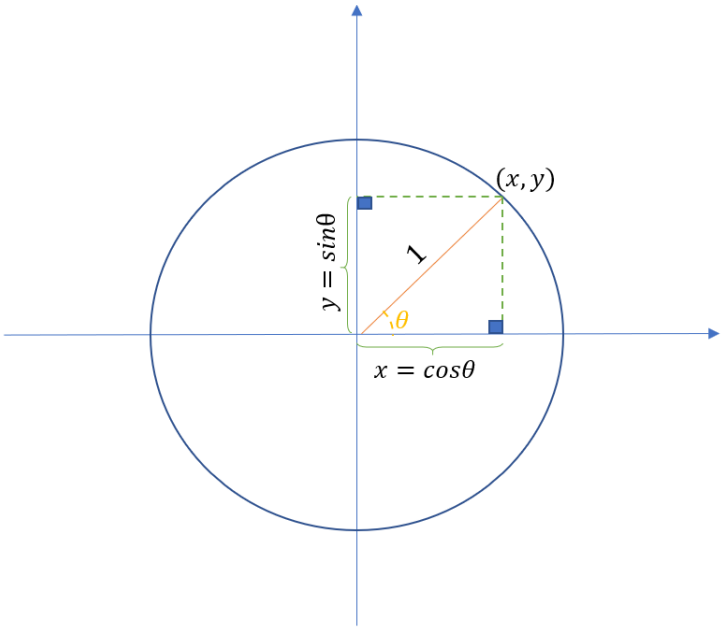

Figure 11: Unit circle with point (x, y) on the circle.

Then $\sin\theta$ and $\cos\theta$ are as follows:

$$\cos\theta = \frac{\text{adjacent}}{\text{hypotenuse}} = \frac{x}{1}$$

$$\sin\theta = \frac{\text{opposite}}{\text{hypotenuse}} = \frac{y}{1}$$

Therefore,

$$x = \cos\theta \quad y = \sin\theta.$$

So you can think of $\cos\theta$ and $\sin\theta$ as the x- and $y-$coordinates on the unit circle for the angle θ.

Since we have a right triangle, by the Pythagorean Theorem, we get the identity

$$\sin^2\theta + \cos^2\theta = 1.$$

You can scale this picture up or down (to a circle of radius r) as needed. Then, $\cos\theta = x/r$ and $\sin\theta = y/r$.

3.2 Properties of Functions

$$f : X \to Y$$

Recall. The graph of the function f is $\#f = \{\ (x, f(x))\ :\ x \in X\}$ and also

$$\#f \subseteq X \times Y$$

where $X \times Y$ is the ordered pairs such that the first member comes from X and the second member comes from Y.

Note. Since f is a function, there is only one $f(x)$ for each x.
The function $\sin\theta$ is shown below.

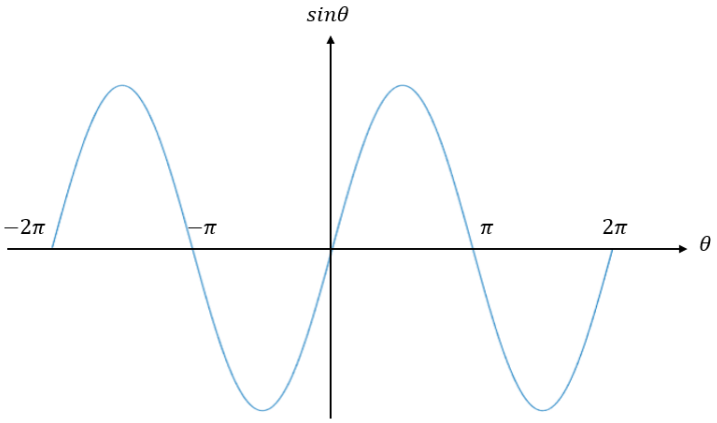

Figure 12: Sine function.

As can be seen, this function is not injective since it maps all $x = \{\ldots, -2\pi, -\pi, 0, \pi, 2\pi, \ldots\}$ to one point, zero.

$$\sin 2\pi = \sin \pi = \sin(-\pi) = \sin(0) = \sin(-2\pi) = 0$$

3.2.1 Horizontal Line Test for Injectivity

To check injectivity, if you can draw a horizontal line that hits the function more than once, the function is not injective.

For example, consider the absolute value function depicted below. As shown, this function is not injective since the horizontal line of $y = 2$ hits the function more than once. This means the function takes the value y more than once.

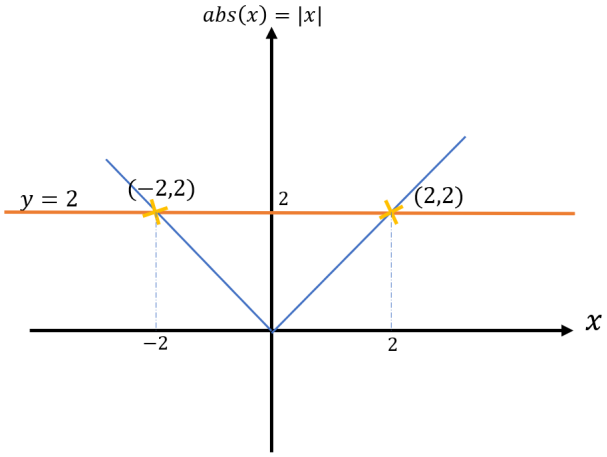

Figure 13: Absolute value function.

As another example, the horizontal line below hits the $\sin\theta$ function multiple times, therefore $sin\theta$ is not injective.

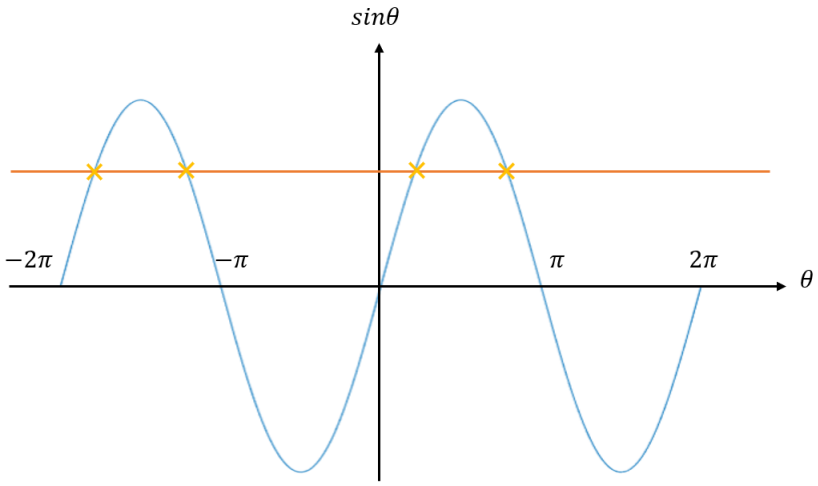

Figure 14: Caption

In other words, the $\sin\theta$ is a periodic function, so it will take one value several times.

Note. Depending on the codomain or target of $\sin\theta$, this function might be surjective or not. For exmaple, if

$$\sin: \quad \mathbb{R} \to [-1, 1]$$

then the function is surjective. However, if we change the codomain, the function might not become surjective.

Because the function value is always between -1 and 1; and for example $\sqrt{2} \notin$ Image(sin)

3.2.2 Vertical Line Test

To check that a graph is a function, vertical line test is applied; if this vertical line hits the graph more than once, the graph is not a function. It takes more than one value for a given x value.

Consider the pairs of points below

$$\{(x, y): \quad (x-c)^2 + y^2 = r^2\} \subseteq \mathbb{R} \times \mathbb{R}$$

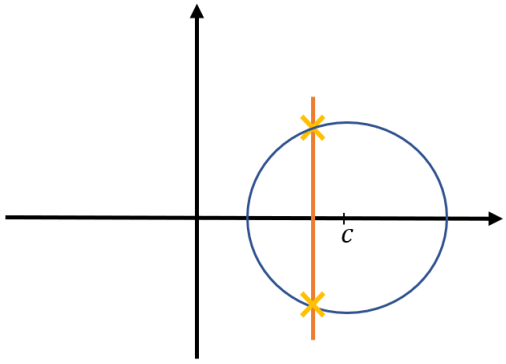

Figure 15: Circle at point $(c, 0)$

By drawing vertical line, we find that there exist some x mapped to different y, therefore this is not a function, but a relation.

Also if any vertical line misses the graph, it's not the graph of a function, since it's not defined at that x-value.

Definition. Let A and B be two sets, then $R \subseteq A \times B$ is called a *relation* from A to B.

A relation $R \subseteq A \times B$ is the graph of a function if both conditions below are satisfied:

- 1. Vertical line test: if $\quad (a, b) \in R, \quad (a, b') \in R \quad$ then $\quad b = b'$

- 2. Defined everywhere in domain: for all $a \in A$ $\exists$ a $b \in B$ s.t. $(a, b) \in R$

Example. Is the graph in blue the graph of a function?

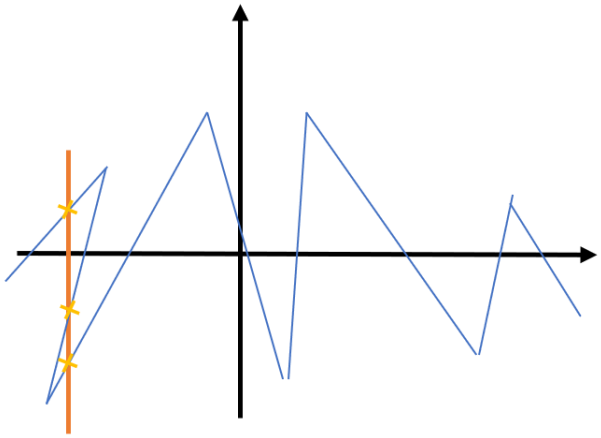

Figure 16: Relation example

Answer. No, it is not. Although this graph is defined everywhere and passed the first condition, it fails the vertical line test since this line hits the graph more than once. Therefore, it is not a function.

Example. Is $\sqrt{x}$ a function?

Answer. It depends how we define the domain and codomain. If both domain and codomain are non-negative numbers ($\mathbb{R}^+$), then it is a function. Otherwise, it is not.

Example. Is $g(y) = \frac{1}{x}$ a function?

Answer. It depends on how we define its domain and codomain. If we define function g as

$$g: \quad \mathbb{R}\backslash\{0\} \to \mathbb{R}$$

it is a function. However, if we define it as

$$g: \quad \mathbb{R} \to \mathbb{R}$$

It is not a function since it is not defined at zero, so it does not pass the second condition.

Note. The function $g(y) = \frac{1}{x}$ is not surjective since there is no correspondence to $y = 0$.

3.3 Composition of Functions

Consider three sets X, Y, Z and two functions $g : X \to Y$ and $f : Y \to Z$, if $x \in X$, then the composition of g and f is

$$f \circ g : X \to Z$$
$$\underbrace{(f \circ g)}_{\text{composite function}} \quad (x) = f(g(x))$$

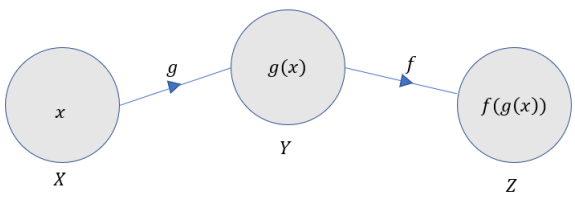

Figure 17: Composite function.

which means "f following g", or "first g then f".

Example. Lets $g(x) = \frac{1}{x}$ and $f(x) = x + 1$. Find $f \circ g$ and $g \circ f$.
Answer.

$$\big(f \circ g\big)(x) = f(g(x)) = f(1/x) = \frac{1}{x} + 1$$

$$\big(g \circ f\big)(x) = g(f(x)) = g(x+1) = \frac{1}{x+1}$$

These two are different functions with different domains of definition. The first is undefined at 0, the second is undefined at -1, but defined elsewhere. So, in the composition of functions, the order matters.

3.4 Function Operations

- Add

$$\big(f + g\big)(x) = f(x) + g(x)$$

- Subtraction

$$\big(f - g\big)(x) = f(x) - g(x)$$

- Multiply

$$\big(fg\big)(x) = f(x)g(x)$$

- Division

$$\big(\frac{f}{g}\big)(x) = \frac{f(x)}{g(x)} \quad \text{for } g(x) \neq 0$$

Example. Lets $f(x) = x^2$ and $g(x) = x^3$, find $\big($ f-g$\big)(7)$ and $\big(fg\big)(7)$.
Answer.

$$\big(f - g\big)(7) = f(7) - g(7) = 7^2 - 7^3$$

$$\big(fg\big)(x) = f(x) \times g(x) = x^2 \times x^3 = x^5, \quad \text{then} \quad \big(fg\big)(7) = 7^5$$

Note. In adding and multiplying, order does not matter. But it does for subtracting and dividng functions.

3.5 Domain and Codomain Sets

Consider a set X, we denote the number of elements in set X as

$$\#\text{number of elements in } X = |X|$$

That is, is also called *cardinality* of the set $|X|$.
For example,

$$|\{a, b, c\}| = 3$$

$$|\emptyset| = 0$$

$$|\{a, a\}| = 1 \text{ (only count unique elements)}$$

Definition. A set is a *finite* set if the number of elements in that set is finite. In particular, there are three facts relating the sizes of the domain and codomain:

- if X and Z are finite sets and $g : X \to Z$ is injective, then set Z has at least as many points as X does, $|Z| \geq |X|$.
- if X and Z are finite sets and $g : X \to Z$ is surjective, then $|X| \geq |Z|$.
- if X and Z are finite sets such that $|X| = |Z|$, and $g : X \to Z$ is injective, then g takes every value in Z; therefore, g is surjective.

3.6 The Finite World

In the finite world, this leads an two important result:

- if X and Z are finite sets and $g : X \to Z$ is surjective and $|X| = |Z|$, then g is injective.
- if X and Z are finite sets and $g : X \to Z$ is injective and $|X| = |Z|$, then g is surjective

from the previous two items, in the finite world where X and Z are finite and $g : X \to Z$:

$$\text{if } |X| = |Z|, \text{ then } g \text{ is injective if and only if } g \text{ is surjective.}$$

3.6.1 Finite vs. Infinite

The above assertions are not necessarily true in infinite world! For example, the function $h : \mathbb{N} \to \mathbb{N}$, $h(n) = n + 1$ is not surjective since $0 \notin Image(h)$, but it is injective. Another example, $g : \mathbb{Z} \to \mathbb{N}$, $g(z) = |z|$ is not injective since $g(-1) = g(1) = 1$, but surjective since every element in $\mathbb{N}$ is hit. Therefore, infinite world and finite world are completely different in this regard.

3.7 Directed Graphs

Definition. Let V be a set of vertices and $R \subseteq V \times V$ be a relation on V. The *directed graph* is the visualization of the relation R.

As an example, suppose that $V = \{a, b\}$ is the set of vertices and $\{(a, b), (b, a), (a, a)\} \subseteq R$, then the directed graph of R is:

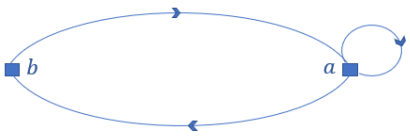

Figure 18: Directed graph example

A directed graph is also called a “digraph”.

4 Lecture 4. (September 17, 2020) : Relations and Inverses

Recall. A relation $R \subseteq X \times Y$ is a subset of a direct product, which is made of ordered pairs.

$$R \subseteq \underbrace{X \times Y}_{\text{Cartesian product}} = \{(x, y) : x \in X, y \in Y\}$$

Recall. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$

Definition. The *inverse relation* is

$$R^{-1} = \{(y, x) : (x, y) \in R\} \subseteq Y \times X$$

This is just swapping the first and second coordinates.

If you graph the relation it corresponds to flipping (reflecting) across the diagonal. [Figure not typeset yet]

Note. The inverse of an inverse relation is the original relation:

$$(R^{-1})^{-1} = R$$

Example. Consider function $f : B \to A$ as follow

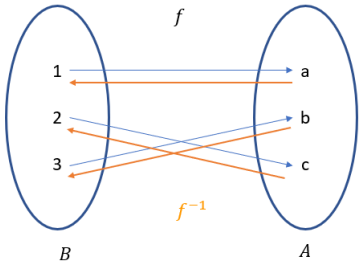

Figure 19: Sample function

This function is injective, surjective and bijective.

The graph of this function is:

$$\#f \subseteq B \times A$$

$$\#f = \{(1, a), (2, c), (3, b)\}$$

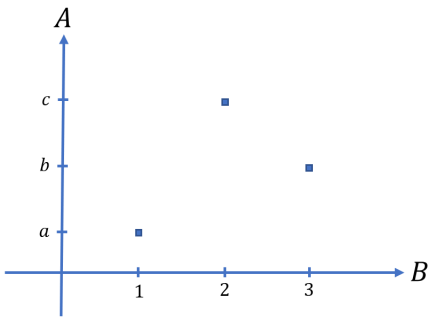

Figure 20: The graph of the function f

Also, the inverse relation for the graph of the function f is

$$\#(f^{-1}) = (\#f)^{-1} = \{(a, 1), (c, 2), (b, 3)\}$$

$$(\#f)^{-1} \subseteq A \times B$$

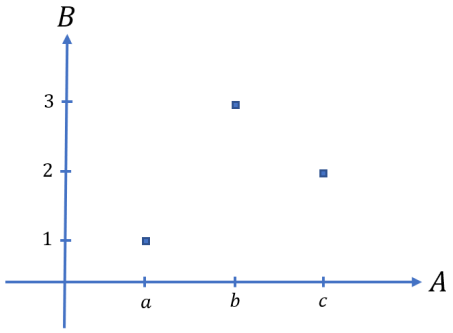

Figure 21: The inverse relation of the graph of f

Also, since the function is one-to-one correspondence, the inverse function of f is $f^{-1} : A \to B$ which is shown in red in Fig.19.

Additionally, we can write the composition of f and its inverse as

$$f \circ f^{-1} : A \to A \text{ (the identity map on set } A)$$
$$f^{-1} \circ f : B \to B \text{ (the identity map on set } B)$$

4.1 Exponential Functions

The exponential function is defined as

$$\exp(x) : x \to e^x$$
$$\exp : \mathbb{R} \to \mathbb{R}^+ \backslash \{0\}$$

The exponential function is bijection; therefore, it has an inverse, the log function:

$$\log : \mathbb{R}^+ \backslash \{0\} \to \mathbb{R}$$

Note. The exponential and log function are inverse of each other:

$$\exp(\log(y)) = y$$
$$\log(\exp(x)) = x$$

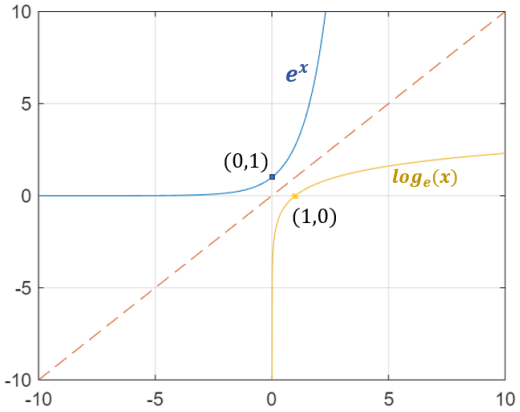

Figure 22: Exponential function and its inverse function, log(x).

Note. The graph of the exponential function is

$$\# \exp = \{(r, \exp(r)) : r \in \mathbb{R}\}$$

Note. One important property of the exponential function is

- $\exp(x+y) = \exp(x)\exp(y)$
- $\log(xy) = \log x + \log y$
- Homomorphism property $\underbrace{\mathbb{R}}_{under+} \overset{\exp}{\underset{\log}{\rightleftarrows}} \underbrace{\mathbb{R}^+\backslash\{0\}}_{under\times}$

Under these bijections, addition in $\mathbb{R}$ is transformed to multiplication in the positive reals by exp, and, in the other direction, multiplication of positive real numbers is transformed to addition. We say the mappings "respect" the operations on these sets.

5 Lecture 5. (September 21, 2020): Logarithms in Base b & Modulo n Arithmetic

5.1 Logarithms to different bases

Recall. The exponential and logarithm are inverse operations of each other; and both of these functions are bijective (one-to-one correspondences).

Exponential	Logarithm
$2^x : \mathbb{R} \to \mathbb{R}^+ \backslash \{0\}$	$\log_2 : \mathbb{R}^+ \backslash \{0\} \to \mathbb{R}$
$2^x \times 2^y = 2^{x+y}$	$\log_2(xy) = \log_2 x + \log_2 y$

Table 1: Exponential and logarithm relationship in base 2.

The above table represents the relationship between exponential and logarithm operation in base 2; however, the analogous relations also holds for any other bases, for example:

Exponential	Logarithm
3^x	$\log_3$
4^x	$\log_4$
10^x	$\log_{10}$
e^x	$\log_e$

Table 2: Exponential and logarithm relationship in some bases.

In the table above, $e = 2.7182818\cdots \in \mathbb{R}\backslash\mathbb{Q}$ is called Euler's number which is a very special irrational number.

The following relationship always holds, and defines logarithm base a :

$$x = a^y \iff \log_a x = y$$

In this course, we take $a > 1$.

Note. In computer science, the base 2 is most common:

$$x = 2^y \iff \log_2 x = y$$

Note. The log base e is also common and is called *natural log* and denoted by $\ln = \log_e$:

$$x = e^y \iff \ln x = \log_e x = y$$

Some properties of log function are as follows:

- Convert from base a to base b:

$$\log_b x = \frac{\log_a x}{\log_a b}$$

Proof. Let's define $y = \log_b x$:

$$\begin{aligned} & y = \log_b x \\ \Rightarrow\ & x = b^y \\ \Rightarrow\ & \log_a x = \log_a(b^y) = y \log_a b \\ \Rightarrow\ & \tfrac{\log_a x}{\log_a b} = y = \log_b x \quad \text{dividing by } \log_a b \neq 0, \text{ since } b \neq 1 \end{aligned}$$

Notice that this shows the logarithm in one base is a constant multiple of the logarithm in any other base.

- Homomorphism property of log

  Using logarithms, we can convert multiplication, an expensive operation, to addition, which is much cheaper computationally.

$$\log : \mathbb{R}^+\backslash\{0\} \to \mathbb{R} \quad \text{natural log (ln)}$$
$$\log(x \cdot y) = \log x + \log y$$
$$(\mathbb{R}^+\backslash\{0\}, \cdot) \longrightarrow (\mathbb{R}, +)$$

- Homomorphism property of exp

  We can invert the process with exp, which takes sums to products

$$\exp : \mathbb{R} \to \mathbb{R}^+\backslash\{0\}$$
$$\exp(x + y) = (\exp x) \times (\exp y) \text{ or equivalently } (e^{x+y} = e^x.e^y)$$
$$(\mathbb{R}, +) \longrightarrow (\mathbb{R}^+\backslash\{0\}, \cdot)$$

  Note. The homomorphism property is also called *structure-preserving mapping*, and works for any base b.

5.2 Modulo n arithmetic (mod n)

Modulo n arithmetic, also called *mod n* and also *modular arithmetic*, is concerned with remainders when we divide by n. Some examples of modular arithmetic are the 60 minute-, 60 second- and 12- and 24- hour cycles in clock time.

Another example is $\mathbb{Z}_5$ that means you need to count to 5 and if you reach 5, repeat from the beginning.

Definition. Formally, for integers a and b, equivalence modulo 5 is defined by

$$a \equiv b \mod 5 \quad \Leftrightarrow \quad a - b = 5k \quad \text{for some integer } k$$

That is, a and b differ by a multiple of 5.

We also write this as $[a]_5 = [b]_5$, or if it's clear we're working modulo 5, we just write $[a] = [b]$. For different values of b, the set $[b]$ of integers equivalent to b modulo 5 is:

- $b = 0$

  $[0] = \{\dots, -5, 0, 5, 10, \dots\}$

- $b = 1$

  $[1] = \{\dots, -4, 1, 6, 11, \dots\}$

- $b = 2$

  $[2] = \{\dots, -3, 2, 7, 12, \dots\}$

- $b = 3$

  $[3] = \{\dots, -2, 3, 8, 13, \dots\}$

- $b = 4$

  $[4] = \{\dots, -1, 4, 9, 14, \dots\}$

It is evident that the integer numbers on the number line are wrapped around in a circle consisting of these classes. This partitions $\mathbb{Z}$ into 5 classes. These classes each have infinitely many numbers and are **disjoint**. The set $\mathbb{Z}$ is the union of these classes:

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$$

The (finite) set of these 5 classes is called is $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

Note. The modulo 5 class is determined by the remainder when we divide by 5.
We write for example, $[6] = [1]$, or $1 \equiv 6 \pmod 5$ (read "1 is congruent to 6 modulo 5")

Note that for negative numbers, the remainders are negative so we need to add 5 to find the canonical representative of the class, e.g. $-11 = -2 \times 5 + (-1)$, so $[-11] = [-1] = [-1 + 5] = [4]$.

Exercise: Check that $a \equiv b \mod 5$ is the case exactly when a and b have the same remainder when divided by 5, adjusting a negative remainder by adding 5.

5.3 Properties of Modular Arithmetic

5.3.1 Surjectivity

In above example, every integer is mapped to one of those five classes. Let call this function h:

$$\mathbb{Z} \xrightarrow{h} \mathbb{Z}_5$$

$$n \mapsto [n]$$

The function h maps n to n modulo 5.
The function h is surjective.

5.3.2 Homomorphism Properites.

Let $[n]$ and $[m]$ be two classes in the set $\mathbb{Z}_5$, then their sum like this:

$$[n] + [m] := [n + m]$$

Then $[n+m]$ is the class of $n+m \mod 5$. This addition modulo 5 is *well-defined*, which means that it does not matter which representatives you choose, you always get the same class. The examples below make this more clear:

$$[4] + [1] = [5] = [0]$$

$$[9] + [-4] = [5] = [0]$$

$$[14] + [6] = [20] = [0]$$

- **Addition is well-defined.**

  Let m and n be from two classes in modulo 5; q and r be any two elements belonging to the classes of n and m respectively:

  $$\begin{array}{l} q \in [n] \Rightarrow n - q = 5k, \text{ for some } k \in \mathbb{Z} \\ r \in [m] \Rightarrow m - r = 5j, \text{ for some } j \in \mathbb{Z} \end{array} \Longrightarrow [n + m] = [r + q]$$

  Proof.

  $q \in [n]$ implies that $n - q = 5k$, similarly $r \in [m]$ implies that $m - r = 5j$ for some $k, j \in \mathbb{Z}$. Then,

  $$\begin{aligned} n + m &= \underbrace{q + 5k}_{n} + \underbrace{r + 5j}_{m} \\ &= q + r + \underbrace{5(k + j)}_{\text{a multiple of 5}} \\ &\Longrightarrow [n + m] = [q + r] \Longrightarrow n + m \equiv q + r \pmod 5 \end{aligned}$$

  Note. The modulus 5 is not special. The arguments above hold true for all moduli $n \geq 2$, such as modulo 10, modulo 4, modulo 2, etc.

- **Negative is well-defined.**

  For a given class n:

  $$-[n] = [-n]$$

  For example, in modulo 5, $-[2] = [-2] = [3]$.

- **Multiplication.**

  Let $[n]$ and $[m]$ be two classes modulo 5, then define their product:

  $$[n] \times [m] := [nm]$$

  For example, in modulo 5:

  $$[1] \times [3] = [1 \times 3] = [3]$$
  $$[6] \times [3] = [6 \times 3] = [18] = [3]$$

  As usual we may write $[n][m]$ for the product $[n] \times [m]$.

  Multiplication is well-defined.

  Proof. We must show it does not matter what representative you choose. Let n', n, m', m be integer numbers such that $[n] = [n']$ and $[m] = [m']$, which means $n, n' \in [n]$ and $m, m' \in [m]$. This means that

  $$n' - n = 5k \text{ and } m' - m = 5j; \text{ for some } k, j \in \mathbb{Z}$$

  Then,

  $$\begin{aligned} n'm' &= (n + 5k)(m + 5j) \\ &= nm + 5nj + 5mk + 5^2kj \\ &= nm + 5(nj + mk + 5kj) \\ &\Rightarrow [n'm'] = [nm]. \end{aligned}$$

  That is, the result of multiplying $[n]$ and $[m]$ is the same, even if one chooses different representatives.

5.3.3 Summary

Integers modulo 5 can be represented as function h:

$$\mathbb{Z} \xrightarrow{h} \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$
$$h(n) = [n]$$

This function:

- preserves addition
  $$h(n + m) = h(n) + h(m)$$
  $$[n + m] = [n] + [m]$$
- preserves multiplication
  $$h(nm) = h(n) \times h(m)$$
  $$[nm] = [n][m]$$
- is homomorphism in two ways:
  $$(\mathbb{Z}, \times) \to (\mathbb{Z}_5, \times)$$
  $$(\mathbb{Z}, +) \to (\mathbb{Z}_5, +)$$

  Again, exactly the same reasoning works for any integer modulus $n \geq 2$.

6 Lecture 6. (September 24, 2020): Base n expansions & Geometry of Complex Numbers

For the given integer base expansion $n \in \mathbb{Z}$, $n \geq 2$ and also the digit set is $\{0, 1, \ldots, n-1\}$:
A number in integer base n expansion is denoted (or encoded) by:

$$d_k d_{k-1} \ldots d_1 d_0, \quad d_j \in \{0, 1, \ldots, n-1\}$$

and its value is

$$\sum_{j=0}^{k} (d_j \times n^j) = (d_k \times n^k) + (d_{k-1} \times n^{k-1}) + \ldots (d_1 \times n^1) + (d_0 \times n^0)$$

6.1 Three important bases

- Binary
  $n = 2$ and digits are $\{0, 1\}$.
  (A digit for base 2 is also called a "bit", which a word derived from "binary digit".)
- Decimal
  $n = 10$ and digits are $\{0, 1, \ldots, 9\}$
  For example, $203 = 2 \times 10^2 + 0 \times 10^1 + 3 \times 10^0$
- Hexadecimal
  $n = 16$ and digits are $\{0, 1, \ldots, 9, \underbrace{A}_{10}, B, C, D, E, \underbrace{F}_{15}\}$
  For example, let's convert FF from the base 16 to the base 10.

$$\begin{aligned}(FF)_{16} &= 15 \times 16^1 + 15 \times 16^0 \\ &= 240 + 15 \\ &= (255)_{10}\end{aligned}$$

This means that we have different representations of the same number.

Example. Converting from binary to decimal:

$$\begin{aligned}(11111111)_2 &= \sum_{j=0}^{7} 1 \times 2^j \\ &= 2^7 + 2^6 + \cdots + 2^2 + 2^2 + 2^0 \\ &= (255)_{10} \\ &= (FF)_{16} \\ &= (FF)_{hex}\end{aligned}$$

Note. Four bits encode a digit in $\{0, 1, \ldots, 9, A, \ldots, F\}$. Therefore, we can transform a binary number into a hexadecimal number by replacing the binary numbers in groups of four. For example, consider the binary number 10011111 which we divide it into groups of four as follow:

$$\underbrace{1001}_{\text{group 1}} \; \underbrace{1111}_{\text{group 2}}$$

$$\text{group 1: } 1001 = 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 8 + 1 = 9$$

$$\text{group 2: } 1111 = F$$

$$(10011111)_2 = (9F)_{hex}$$

This works since $16 = 2^4$. It's important to take the groups of four bits so the last group aligns with the units (2^0 digit) in binary.

Note. There is also a trick to convert a hexadecimal number into a binary number. To do that, you just need to replace each hexadecimal digit by a four binary digits. For example:

$$(FF)_{16} = (\underbrace{1111}_{F}\underbrace{1111}_{F})_2$$

Example. Converting a hexadecimal number to decimal:

$$\begin{aligned}(9F)_{hex} &= 9 \times 16^1 + 15 \times 16^0 \\ &= 144 + 15 \\ &= (169)_{10}\end{aligned}$$

Example. Converting a decimal number to hexadecimal:

$$\begin{aligned}(100)_{10} &= 6 \times 16^2 + 0 \times 16^1 + 0 \times 16^0 \\ &= (64)_{16}\end{aligned}$$

$$\begin{aligned}(257)_{10} &= 1 \times 16^2 + 0 \times 16^1 + 1 \times 16^0 \\ &= 256 + 0 + 1 \\ &= (101)_{16}\end{aligned}$$

6.2 Negatives

The negatives are denoted by prepending a minus sign. For example,

$$(-257)_{10} = (-101)_{16}$$

Note. The minus sign needs only one bit (or one binary digit) of information to store it.
Example.

$$\begin{aligned}(-FF)_{hex} &= (-255)_{10} \\ &= (-11111111)_2\end{aligned}$$

Also base 60 has been used for geometry, chronometry and astronomy since ancient times. There, base 60 used in breaking down angles in minutes (1/60 th of a degree) and seconds (1/60 th of minute).

6.3 Expansion Base n of Real Numbers

In previous section, we discussed the integer base n numbers; however, in this section we want to introduce real base n numbers. Generally, a **real number in base n expansion** is denoted by:

$$d_k d_{k-1} \dots d_1 d_0 . d_{-1} d_{-2} \dots d_{-m}, \quad d_j \in \{0, 1, \dots, n-1\}$$

and its value is

$$\sum_{j=-m}^{k} (d_j \times n^j).$$

Example in decimal:

$$\begin{aligned}\pi &= 3.14151926\dots \\ &= 3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + \dots\end{aligned}$$

Examples in binary:

$$\begin{aligned}(1.01)_2 &= 1 \times 2^0 + 0 \times 2^{-1} + 1 \times 2^{-2} \\ &= 1 + 0 \times \frac{1}{2} + 1 \times \frac{1}{4} \\ &= 1 + 0 + 0.25 \\ &= (1.25)_{10}\end{aligned}$$

$(-1.01)_2 = (-1.25)_{10}$

$$\begin{aligned}(101.01)_2 &= 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 + 0 \times 2^{-1} + 1 \times 2^{-2} \\ &= 4 + 1.25 \\ &= (5.25)_{10}\end{aligned}$$

Example in base 3:

$$\begin{aligned}(1.01)_3 &= 1 \times 3^0 + 0 \times 3^{-1} + 1 \times 3^{-2} \\ &= 1\frac{1}{9} \\ &= 1.111\ldots \\ &= (1.\bar{1})_{10}\end{aligned}$$

6.4 Complex Numbers & Trigonometry: The Geometry of Multiplication in $\mathbb{C}$

The geometry of complex numbers is shown in the figure below. The r and θ are defined as

$$\begin{aligned} r = |z| &= \sqrt{z\bar{z}} \\ &= \sqrt{(x+iy)(x-iy)} \\ &= \sqrt{x^2 + ixy - ixy - i^2y^2} \quad \text{and since } i^2 = -1 \\ &= \sqrt{x^2+y^2} \end{aligned}$$

$$\theta = \arctan\frac{y}{x}, \text{adjusted by } \pm\pi \text{ for possible quadrant correction}$$

$$\arg z = \theta$$

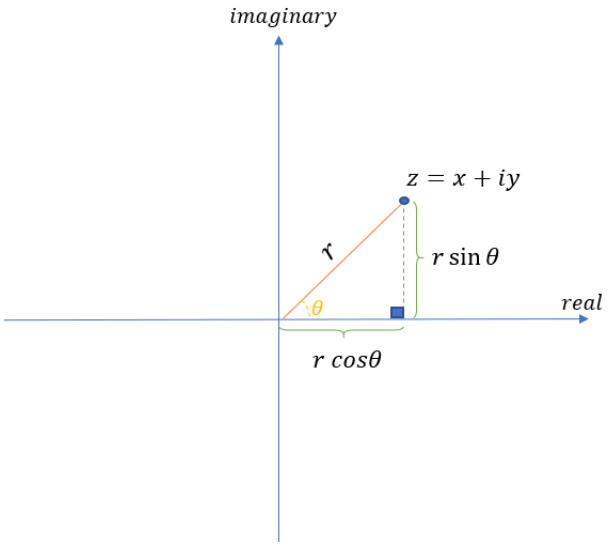

Figure 23: Geometry of complex numbers.

6.4.1 Multiplication of Complex Numbers

Let $z = x + iy$ and $z' = x' + iy'$ be two complex numbers. Then we can write them in this form:

$$z = x + iy = r\cos\theta + ir\sin\theta = r(\cos\theta + i\sin\theta)$$

$$z' = x' + iy' = r'\cos\theta' + ir'\sin\theta' = r'(\cos\theta' + i\sin\theta'),$$

where $r' = |z'|$ and $\theta' = \arg z'$.

The product of these two complex numbers is

$$\begin{aligned} zz' &= r(\cos\theta + i\sin\theta)\ r(\cos\theta' + i\sin\theta') \\ &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'\Big((\cos\theta\cos\theta' - \sin\theta\sin\theta') + i(\cos\theta\sin\theta' + \sin\theta\cos\theta')\Big) \\ &\quad \text{by the sum of angles formulas for cosine and sine:} \\ &= rr'\Big(\cos(\theta+\theta') + i\sin(\theta+\theta')\Big) \\ &= rr'\cos(\theta+\theta') + irr'\sin(\theta+\theta') \end{aligned}$$

Observe that this has real coordinate $rr'\cos(\theta+\theta')$ and imaginary coordinate $rr'\sin(\theta+\theta')$. Thus, the point zz' is distance $|z||z'|$ from the origin, at angle $\theta + \theta'$.

Therefore,

$$|zz'| = rr' = |z||z'|$$

$$\begin{aligned}\arg(zz') &= \theta + \theta' \\ &= \arg z + \arg z'\end{aligned}$$

We have just established the following properties of complex multiplication:

Theorem. The norm function, $f : \mathbb{C} \to \mathbb{R}^+$, $f(z) = |z|$, is homomorphism under multiplication.

$$\underbrace{|zz'|}_{\text{product in } \mathbb{C}} = \underbrace{|z||z'|}_{\text{product in } \mathbb{R}^+}$$

$$(\mathbb{C}, .) \to (\mathbb{R}^+, \times)$$

Theorem. The arg function is homomorphism taking multiplication to addition modulo 2π:

$$\arg : (\mathbb{C}, .) \to [0, 2\pi), \text{modulo } 2\pi$$

$$\arg(zz') = \underbrace{\arg z}_{\theta} + \underbrace{\arg z'}_{\theta'} = \underbrace{\theta + \theta'}_{\text{modulo } 2\pi}$$

Here in the target, two real numbers are the same modulo 2π if they differ by a multiple of 2π. (Notice this is very like modulo n for an integer $n > 1$.)

Geometric Interpretation. If you multiply two complex numbers, lengths multiply and angles add.

6.5 Mappings Preserving Structure

We've seen many examples of structure-preserving mappings. These are called *homomorphisms.*[†] Here is a general definition: Given a set S with operation $*$ and a set T with operation $\times$, a function $h : S \to T$ is a *homomorphism* from $(S, *)$ to $(T, +)$ if for all $s, s' \in S$, the following holds:

$$h(s * s') = h(s) \times h(s').$$

Here $*$ is some operation in S like multiplication or addition, that combines two members of the set S to get a result in S.[‡] Similarly, $\times$ is such an operation on T. The equation says: we can use the operation in S and then map by h, or, alternatively, before applying an operate we use h map to elements of T and then use its . In either case we get the same result.

One says h "transforms" the operation $*$ in the source S to the operation $\times$ in the target T. For example, log transforms a product in the positive reals to a sum in the reals $\log(x \times y) = \log x + \log y$.

[†]There is a brief introduction in Schaum's Linear Algebra Appendix B.2. The appendix refers to groups, but the notation of homomorphisms can be be made much more general. Later you will studying *linear mappings* which are another kind of homomorphism between vector spaces such as $\mathbb{R}^m$ and $\mathbb{R}^n$.

[‡]This is call a "binary operation on S", that is a function from $S \times S$ to S, e.g. $+$ is a binary operation on $\mathbb{R}$, but so is subtraction or multiplication.

7 Lecture 7. (September 28, 2020): Proofs & Logic

7.1 Propositional Logic -Digital Logic in Computers

Mathematical proposition (sentence) must be either true or false.

The symbol T is used for true and symbol F is used for false propositions.

Let p, q, and r be three propositions. The below is the list of some important propositional logic:

- Logical Negation

  The logical negation is a not function denoted by $\neg$.

  $$\neg : \{T, F\} \to \{T, F\}$$

  Given a proposition, not logical negation returns the opposite truth value. The below is the logical negation truth table.

p	$\neg p$
T	F
F	T

- AND

  The AND operation is a logical function denoted by $\wedge$:

  $$\wedge : \{T, F\} \times \{T, F\} \to \{T, F\}$$

  The below is the AND truth table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

  Note. The result of AND operation is true if and only if both p and q are true.

- OR

  The OR operation is a logical function denoted by $\vee$:

  $$\vee : \{T, F\} \times \{T, F\} \to \{T, F\}$$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

  Note. The result of the OR operation is true if and only if at least one of p and q is true.

- Implies

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

  Note. The order matters in implies operation, which means $p \to q$ is not the same as $q \to p$.

7.2 Predicate Logic

Consider the universe and sets A and B shown below. If x is a member of the universe, $x \in U$, $A(x)$ means that x is a member of A, $x \in A$.

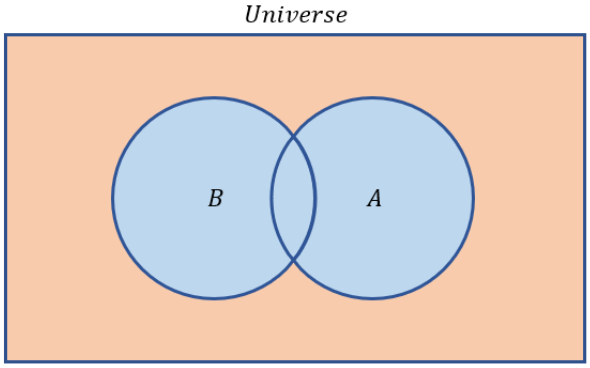

Figure 24: Universe and sets A and B

Also, if $x \notin A$, we can denote it with one of the statements below. These are the same.

$$\neg A(x)$$

$$x \notin A$$

$$x \in \bar{A}$$

Recall. The relation is defined as $R \subset U \times U$.

Consider two points $x, y \in U$. The statement x and y are related is true if and only they are the member of a relation R.

7.3 Mathematical Induction(recursion)

Basically, the concept of mathematical induction is like climbing a ladder.

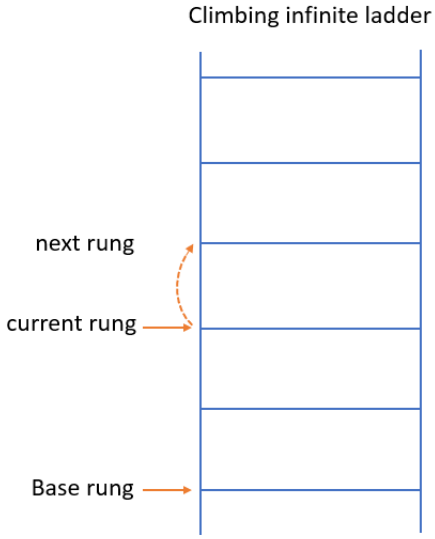

Figure 25: Induction illustration.

If we can get to the base rung, and we can show that we can get from the current rung to the next one, then we can climb the ladder to reach any run. This is how we can prove an assertion holds for each number in the infinite set $\mathbb{N}$. In mathematical induction, we start from the beginning

and show that it is true for all natural numbers. Think of the rungs of ladder as the all different natural numbers.

idea of induction:

Step 0: formulate a mathematical assertion $P(n)$ about n clearly

Step 1: prove and check a base case (e.g, $n = 0$, or $n = 2$, or $n = -3$)

$$P(0)$$

Step 2: assume true for n, and then show true for $n + 1$

$$P(k) \implies P(k + 1)$$

Example. Let $P(n)$ be the sum of the first n positive integers. Prove

$$P(n) : \sum_{j=1}^{n} j = \frac{n(n+1)}{2} \quad \forall n \geq 1$$

Base case: $n = 1$

the statement "the sum of first 1 positive number is $\frac{1(1+1)}{2}$" is true.

Induction step: Assume $P(k)$. Show $P(k + 1)$ holds.

assuming that $P(k)$ is true $\implies P(k) : \sum_{j=1}^{k} j = \frac{k(k+1)}{2}$

then

$$\begin{aligned} P(k+1) &= \sum_{j=1}^{k+1} j \\ &= \underbrace{\Big(\sum_{j=1}^{k} j\Big)}_{P(k)} + k + 1 \\ &= \frac{(k+1)k}{2} + k + 1 \\ &= \frac{(k+1)k + 2k + 2}{2} \\ &= \frac{(k+2)(k+1)}{2} \end{aligned}$$

Therefore,

$$P(k) \implies P(k + 1)$$

Example. Prove that the sum of the first n odd integers is n^2.

We know that

$$\underbrace{1 + 3 + 5 + \cdots + (2n - 1)}_{\text{the first } n \text{ odd integers}} = \sum_{k=1}^{n} (2k + 1)$$

We want to prove by mathematical induction that

$$P(n) : \sum_{k=1}^{n} (2k - 1) = n^2 \quad \forall n \geq 1$$

Base case: $n = 1$

$$(2 \times 1 - 1) = 1^2 \implies P(1) \text{ is true}$$

Induction step:

Assume $P(n)$. Show $P(n + 1)$ holds.

This means that the induction hypothesis is $P(n) : \sum_{k=1}^{n} (2k - 1) = n^2$, and we need to prove

$$\sum_{k=1}^{n+1} (2k - 1) \stackrel{?}{=} (n + 1)^2$$

$$\sum_{k=1}^{n+1}(2k-1) = \underbrace{\Big(\sum_{k=1}^{n}(2k-1)\Big)}_{n^2} + 2(n+1) - 1$$
$$= n^2 + 2n + 1$$
$$= (n+1)^2$$

Therefore,

$$P(n) \implies P(n+1)$$

Finally, by induction

$$\sum_{j=1}^{n}(2k-1) = n^2 \quad \forall n \geq 1$$

7.3.1 Fundamental Theorem of Arithmetic

A natural number $p > 1$ is *prime* if its only divisors are 1 and p.

Fundamental Theorem of Arithmetic. Every positive integer, $n \geq 1$, is the product of primes in a unique way.

The proof of this theorem uses induction, but is a little complicated. Instead, we will now state and prove part of this theorem by mathematical induction.

Theorem. Every positive integer, $n \geq 1$, is the product of primes.

Proof by Mathematical Induction. We want to prove this theorem using induction.

$$P(n): \text{ all } k \text{ from 1 to } n \text{ are products of primes}$$

Base case: $n = 1$ or $n = 2$ We can use either $P(1)$ or $P(2)$ for the base case:

$$P(1) : 1 = \prod \quad \text{(empty product)}$$

$$P(2) : 2 = \prod_{i=1}^{1} 2$$

Induction step:
$P(n) \implies P(n+1)$: to show $n+1$ is a product of primes
The $n+1$ is either

- $n+1$ is prime, in which case $n+1$ is a product of 1 prime.
- $n+1$ is not a prime. Then $n+1 = a \times b \quad a, b > 1$ and $a, b \neq n+1$

Next, by induction hypothesis, $P(n)$, a is product of primes and b is a product of primes. Then, since $n+1 = a \times b$, we conclude $n+1$ is a product of primes too.

Therefore,

$$P(n) \implies P(n+1)$$

Finally, using induction, we proved that

$$\forall n \geq 1 \quad P(n): \text{ is a product of primes.}$$

7.4 Proof by Contradiction

A contradiction is any absurd or impossible statement For example $0 = 1$, or the assertion that both a proposition and its negation must hold.

In this method of proof, we assume the negation of what we want to prove. If this leads to a contradiction, then our assumption must have been incorrect. Therefore the assertion we wanted to prove holds. The following proof is attributed to the ancient Greek mathematician Euclid.

Theorem. There are infinitely many prime numbers.

Proof (by contradiction).
Suppose NOT, which means there are not infinitely many primes. Then

$$\text{Primes} = \{P_1, P_2, \ldots, P_N\}, \quad |Primes| = N, \quad (N \text{ is finite})$$

Consider $M = (P_1 \times P_2 \times \cdots \times P_N) + 1$. Obviously,

$$M > P_j, \quad \forall P_j \in \text{Primes}$$

and also

$$\begin{aligned} M &\equiv 1 \pmod{P_1} \\ M &\equiv 1 \pmod{P_2} \\ &\vdots \\ M &\equiv 1 \pmod{P_N} \end{aligned}$$

which means that M is not divisible by any prime!

Therefore, M is a prime. (since every $n \geq 1$ is a product primes.) This is a contraction, since M is larger than any number in (finite) set of primes; therefore, the assumption that prime numbers are finite is wrong. Therefore, |Primes| is infinite, which means there are infinitely many prime numbers.

8 Lecture 8. (October 1, 2020) [typesetting to be completed]

8.1 Complex Exponentiation

The complex exponential function is defined as

$$e^z : \mathbb{C} \to \mathbb{C}$$

If $z = x + iy$, then

$$e^{x+iy} = e^x\Big(\cos y + i \sin y\Big)$$

If $x = 0$, z is pure imaginary and

$$e^z = e^{iy} = \cos y + i \sin y \qquad (\text{since } e^0 = 1)$$

which is a point on a unit circle since $\cos^2 y + \sin^2 y = 1$

Note. For any $\theta \in \mathbb{R}$,

$$e^{i\theta} \in \underbrace{S^1 = \{z \in \mathbb{C} : |z| = 1\}}_{\text{unit circle}}$$

Euler's Formula. For any $\theta \in \mathbb{R}$, $e^{i\theta} = \cos\theta + i \sin\theta$.

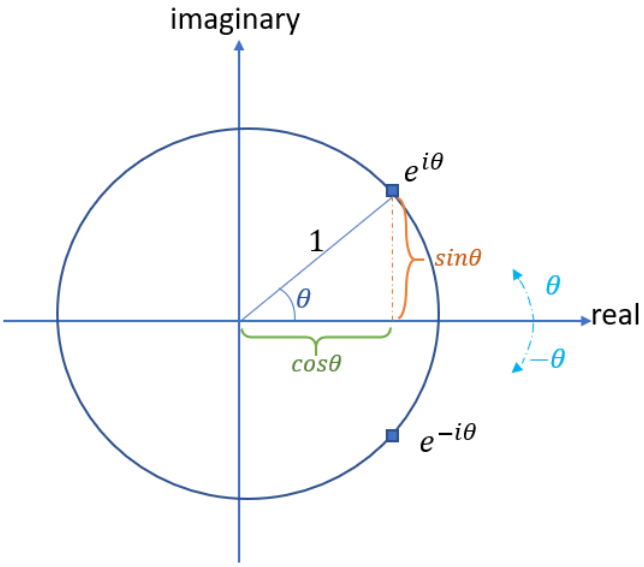

Figure 26: complex number on a unit circle.

Note. $e^{i\theta} \times e^{-i\theta} = 1e^{i(\theta-\theta)} = e^0 = 1$

Recall. $\forall z, z' \in \mathbb{C}, |z||z'| = |zz'|$.

If $zz' = 0$, then

$$\begin{aligned} zz' = 0 &\implies |zz'| = 0 \\ &\implies |z||z'| = 0 \\ &\implies |z| = 0 \text{ or } |z'| = 0 \\ &\implies z = 0 \text{ or } z' = 0 \end{aligned}$$

Therefore, $(\mathbb{C}, \times)$ has no "zero divisors". Just like in $\mathbb{R}$,

$$xy = 0 \iff x = 0 \text{ or } y = 0$$

holds for complex numbers.

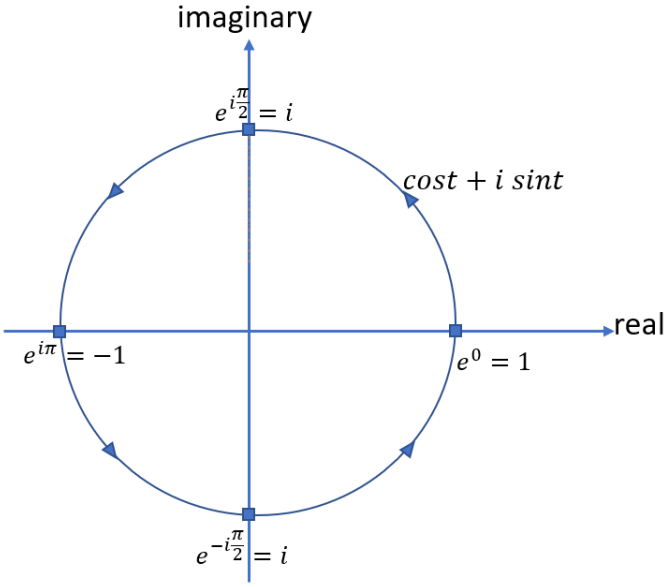

Figure 27: The function e^{it} on the unit circle.

Consider function $f(t) = e^{it}, \quad t \in \mathbb{R}$:

$$t = 0 \mapsto f(0) = e^{i0} = 1$$

$$t = \frac{\pi}{2} \mapsto f(\frac{\pi}{2}) = e^{i\frac{\pi}{2}} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = 0 + i = i$$

$$t = \pi \mapsto f(\pi) = e^{i\pi} = -1$$

$$t = \frac{\pi}{2} \mapsto f(\frac{\pi}{2}) = e^{-i\frac{\pi}{2}} = -i$$

This is the same as

$$t = \frac{3\pi}{2} \mapsto f(\frac{3\pi}{2}) = e^{-i\frac{\pi}{2}} = -i$$

Also, since cos and sin have period 2π, we have $e^{it} = \cos t + i\sin t = e^{i(t+2\pi)}$. Thus,

$$\forall t \in \mathbb{R}.\, f(t) = f(t + 2\pi).$$

The function $f(t) = e^{it}$ wraps $\mathbb{R}$ counterclockwise around the unit circle S^1:

$$f\Big([0, 2\pi)\Big) = \mathrm{S}^1$$