21-127 Concepts of Mathematics

Based on Lectures by Professor Clive Newstead

Fall 2022

at Carnegie Mellon University

Notes by Lómenoirë Mortecc.

Contents

1 Logic

1.1 Proposition and Proof

- A **proposition** is a statement to which it makes sense to assign a truth value (either 'true' or 'false')
- A **proof** is an argument that demonstrates its truth (they have audiences!)

1.1.1 Examples of propositions

- true proposition:
  - π is irrational
  - Clive has 2 eyes
- false proposition:
  - It is currently raining
  - Clive has 3 eyes
  - $2 + 2 = 3$
- unknown/unproven proposition:
  - Every even number > 2 can be expressed as the sum of two prime numbers (aka Goldbach conjecture)
  - There is alien in space

1.2 Proof Terminology

1.2.1 Definitions

- **assumptions** are things we know or assume to be true
- **gaol** is what we are trying to show.

1.2.2 Some Acronyms

(Some are from other units)

- WTS = want to show
- AFSOC = as for sake of contradiction
- WLOG = with out loss of generality
- IS = induction step
- BC = base case
- IH = induction hypothesis
- s.t. = such that

1.3 Logical Structure

- **logical structure -** the skeleton of the proposition
- **symbolic logic -** the formal system we use to examine the structure of a proposition
- **propositional formula -** a symbolic expression that represents a proposition using:
  - **propositional variables** (usually p, q, r) for simpler propositions inside the big one
  - **logical operators -** symbols that combine things like 'and', 'not', 'or', 'if… then'…

1.3.1 Logical Operators

- **Conjunction** $\wedge$ approximately as "and"

- **Disjunction** $\vee$ approximately as "or" ([[The "or" ambiguity|inclusive]])
- **Implication** $\Rightarrow$ if something is true then something else is true
- **Bidirectional** $\Leftrightarrow$ if and only if (shortened as "iff") viz. $(p \Rightarrow q) \wedge (q \Rightarrow p)$
- **negation** $\neg$ approximately as "not"

1.3.2 Quantifiers

- **Universal Quantifier** $\forall$ - reads "for all"
  - $\forall x \in X, p(x)$ reads "all elements x in X satisfies $p(x)$"
- **Existential Quantifier** $\exists$ - reads "there exists"
  - $\exists x \in X, p(x)$ reads "there exists an x in X satisfies $p(x)$"

1.3.3 Logical Formulae

- A **logical formula** is an expression built using:
  - predicates i.e. statements e.g. $x > y$, $p(x)$, etc.
  - logical operators
  - quantifier

Every theorem we want to prove in [[21-127 Concepts of Mathematics]] can be expressed as a logical formula!!!

1.3.4 Logical Equivalency

Given logical formulae φ and ψ, they are **logically equivalent** if $\varphi \Leftrightarrow \psi$. We then write $\varphi \equiv \psi$.

1.3.5 Truth Table

Truth table is a good way to determine if logical formulae are logically equivalent.

A **truth table** of propositional formula φ is a tabular representation of the truth value of φ and its sub formulae depending on all possible combination of truth value of its propositional variables.

Truth table of some logical formulae

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Notice F $\Rightarrow$ T and F $\Rightarrow$ F. This is called "vacuous truth".

Theorem: Given logical formulae φ and ψ, then $\varphi \equiv \psi$ iff columns in their truth tables are the same.

Some useful logical equivalence:
- $(p \Rightarrow q) \equiv (\neg p \vee q)$
- $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ aka contrapositive

1.3.6 Maximal Negation

A logical formula is **maximally negated** if no $\neg$ sign is outside of other operators or quantifiers.

Informally, **deMorgan's laws** talk about duality viz. there's a way to go between $\wedge$ and $\vee$ and a way to go between $\forall$ and $\exists$.

Ways to "push" negation inward (provable, but omitted):

- Law of double negation
  - $\neg(\neg p) \equiv p$
- DeMorgan's law for logical operators
  - $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$
  - $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$
- DeMorgan's law for quantifiers. Let X be a set:
  - $\neg(\forall x \in X, p(x)) \equiv \exists x \in X, (\neg p(x))$
  - $\neg(\exists x \in X, p(x)) \equiv \forall x \in X, (\neg p(x))$
- Equivalency for implications
  - $\neg(p \Rightarrow q) \equiv p \wedge (\neg q)$
  - $\neg(p \Leftrightarrow q) \equiv (p \wedge (\neg q)) \vee ((\neg p) \wedge q)$

1.3.7 Proof Strategies using logical structure

- **Direct proof -** assume what's known, derive the conclusion
- **Proof by contradiction -** assume the opposite of the conclusion, derive a contradiction
- **Proving universally quantified statements -** prove the statement true for any arbitrary element
  - e.g. "every integer is rational". Proof: let $x \in \mathbb{Z}$, then $x = \frac{x}{1}$. $1 \in \mathbb{Z} => x$ rational.
- **Proving existential statements -** find one that satisfies the desired property!
  - e.g. "there exists a rational integer". Proof: $2 \in \mathbb{Z}$ and $2 \in \mathbb{Q}$ as required.

2 Sets

2.1 Defining Sets

- Informal: a **set** is a collection of objects called elements
- More formal: a **set** is a collections of objects from the **universe of discourse** called $\mathscr{U}$, which is supposedly the set of all mathematical objects but not itself.
  - Note quantifiers in [[Pure Math - Logic]] refers to $\mathscr{U}$ by default. So for example $\exists x, p(x) \equiv \exists x \in \mathscr{U}, p(x)$.
- Ways to specify a set
  - **Implied set** - list some elements, hopefully readers learn the pattern. eg.
    - $B = \{2, 3, 5, 7, 11, 13, ...\}$
  - **Set builder notation** - specify set using property. ex.
    - $C = \{x | x > 2\}$
    - $D = \{x | n \text{ is a prime number}\}$

2.1.1 Some Number Sets

- $\mathbb{N}$ = set of natural numbers (includes 0)
- $\mathbb{Z}$ = set of integers (from german word)
- $\mathbb{Q}$ = set of rational numbers (from italian word) = $\{x | x = \frac{a}{b} \text{ for some } a, b \in \mathbb{Z} \text{ with } b \neq 0\}$
- $\mathbb{R}$ = set of real numbers
- $\mathbb{C}$ = set of complex numbers

Fun fact: the truth value of $\pi^\pi \in \mathbb{R}$ is unknown yet.

2.1.2 Intervals

Let $a, b \in \mathbb{R}$ with $a < b$, then:

- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ - open interval
- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ closed interval

Variants on notation

- mixing { and (works.
- using infinity works
- but don't do $[-\infty, \infty]$

2.2 Set and its members

2.2.1 Membership of a set

- $x \in A$ indicates x is an element of the set A
- $x \notin A$ indicates x is not an element of the set A

2.2.2 Set being empty or non-empty

- A set X is **non-empty** or **inhabited** iff $\exists x, x \in X$. Otherwise, a set is **empty** and we write $X = \varnothing$.
- There exists a unique empty set.

2.3 Subsets

Given sets A and B, A is a **subset** of B if $\forall a \in A, a \in B$. We write $A \subseteq B$.

It follows that $\varnothing$ is a subset of all sets because every element of the empty set is vacuously in another other set.

2.3.1 Power Set

The **power set** of set X denoted by $\mathscr{P}(X)$ is the set of all subsets of X. That is, $\forall U, (U \in \mathscr{P}(X) \Leftrightarrow U \subseteq X)$.

2.3.2 Proof by Double Containment

Axiom: sets A and B are equal iff they are subset of each other viz. $(A = B) \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.

2.4 Set Operations

2.4.1 Basic Operations

Let's say we have sets X and Y.

- The **intersection** $X \cap Y = \{a \mid a \in X \wedge a \in Y\}$.
- The **union** $X \cup Y = \{a \mid a \in X \vee a \in Y\}$.
- The **relative complement** of X in Y is $X \setminus Y = \{a \mid a \in X \wedge a \notin Y\}$.

2.4.2 Indexed Operations

Let I be a set. Let X_i be a set for all $i \in I$.

- $\bigcap\limits_{i \in I} X_i = \{a \mid \forall i \in I, a \in X_i\}$. Essentially it's the set of things all sets have in common.
- $\bigcup\limits_{i \in I} X_i = \{a \mid \exists i \in I, a \in X_i\}$. Essentially it's the set of things that are in at least one of the sets.

Other notations:

- $\bigcap\limits_{i=1}^{\infty} X_i$
- $\bigcup\limits_{i=1}^{\infty} X_i$

2.4.3 Cartesian Product

Let's say we have sets X and Y.

The **cartesian product** $X \times Y = \{p \mid p = (x, y) \text{ for some } X \in X \text{ and } y \in Y\}$ viz. the set of all ordered pairs of x and y with $x \in X$ and $y \in Y$.

The k-fold cartesian product $X^k = \{t \mid t = (x_1, x_2, \ldots, x_k) \text{ for some elements } x_1, x_2, \ldots, x_k \in X\}$.

2.5 Partitions

A set can be divided into disjoint chunks. One definition of partition says that given set X and $\mathscr{S} \subseteq \mathscr{P}(X)$, we consider $\mathscr{S}$ to be a **partition** of X if:
- Every set in $\mathscr{S}$ is non-empty i.e. $\forall U \in \mathscr{S}, U \neq \varnothing$.
- Every element is in one and only one chunk. i.e. $\forall x \in X, (\exists! U \in \mathscr{S}, x \in U)$.

The consequences is that the intersection of any two chunks is empty, and that all the chunks in $\mathscr{S}$ union to our big set X.

Note that in [[Pure Math - Counting]], we use **finite partition**, in which we are allowed to have empty partitions.

3 Functions

3.1 Defining Function

3.1.1 What is a function

Given sets X and Y, a **function** f from X to Y, or $f : X \to Y$, is a mapping of each element $x \in X$ to a unique element $f(x) \in Y$. In symbolic expression:

$$\forall x \in X, \exists! y \in Y, y = f(x)$$

Some terminology:
- Let $x \in X$, then $f(x) \in Y$ is the **value** of f at x.
- X is called the **domain** aka **source** of f, and Y is called the **co-domain** aka **target** aka **range** of f.

3.1.2 How to define a function

1. List the values
   - e.g. $f : \{1, 2, 3\} \to \mathbb{R} \backslash \mathbb{Q}$ by defining $f(1) = \sqrt{2}, f(2) = \pi, f(3) = \sqrt{7}$.
2. Give a formula
   - e.g. $f : \mathbb{R} \to \mathbb{R}$ via $f(x) = e^{e^x}$ for all $x \in \mathbb{R}$.
3. An algorithm (must be deterministic)
   - e.g. take the input, add 3 to it, return 1 if it's prime and 0 otherwise.

3.1.3 Well-defineness of a function

Let there be sets X and Y and a function $f : X \to Y$.

A well-defined function must satisfy the following

- **Totality** - $f(x)$ is defined for all $x \in X$ (corresponds to $\forall x \in X$)
- **Existence** - $f(x)$ exists and $f(x) \in Y$ (corresponds to $\exists y \in Y, y = f(x)$)
- **Uniqueness** - $f(x)$ refers to only one y (corresponds to $\exists!$)

3.1.4 Graph of a function

Essentially another way to do the same thing of assigning unique output to every input.

Let there be a function $f : X \to Y$. Then the **graph** of f, written $Gr(f)$, is a subset of $X \times Y$ defined as the following:

$$Gr(f) \subseteq X \times Y \text{ and } Gr(f) = \{(x, y) \in X \times Y \mid y = f(x)\}$$

This can be understood as all (input, output) pairs of the function. It follows that:

$$(x, y) \in Gr(f) \Leftrightarrow f(x) = y$$

3.2 Function equality

3.2.1 Function extensionality axiom

via **Function extensionality axiom**, which basically treats two functions as black box and see if they do the same thing.

Take functions $f : X \to Y$ and $g : A \to B$. We say $f = g$ iff:

1. $X = A$ and $Y = B$, and
2. $\forall x \in X, f(x) = g(x)$ i.e. same output for all inputs.

Note that two functions with same domain and outputs but different co-domain are considered different.

3.2.2 Functions having same graph

It follows that if f and g have the same domain and co-domain, $f = g \Leftrightarrow Gr(f) = Gr(g)$.

3.3 Identity Function

The **identity function** on set X is $\text{id}_X : X \to X$ via $\text{id}_X(x) = x$ for all $x \in X$.

Useful: identity functions are bijections (well obviously)

3.4 Composite Function

Let $f : X \to Y$ and $g : Y \to Z$. The **composite** of f and g denoted by $g \circ f$, is a function $X \to Z$ via $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

Also let $h : Z \to U$. It follows that:
- $f \circ \text{id}_X = f = \text{id}_Y \circ f$ — compositing with identity function does nothing.
- $h \circ (g \circ f) = (h \circ g) \circ f$ — the order of brackets in a composition does nothing.

3.5 Images and Preimages

Given function $f : X \to Y$ and $U \subseteq X$ and $V \subseteq Y$, then:

- The **image** of U under f is $f[U] \subseteq Y$ given by $f[U] = \{y \in Y \mid \exists x \in U, y = f(x)\}$. Think of this as the set of all possible outputs given a set of inputs.
- The **image of** U is just $f[U]$.
- The **preimage** of V under f is the $f^{-1}[V] \subseteq X$ given by $f^{-1}[V] = \{x \in X \mid f(x) \in V\}$. Think of this as the set of inputs that, upon going through the function, lands in V.

3.6 Jections

Given function $f : X \to Y$:

- f is **injective** if $\forall a, b \in X, (f(a) = f(b) \Rightarrow a = b)$. Think of this as inputs map to unique outputs.
- f is **surjective** if $\forall y \in Y, \exists x \in X, y = f(x)$. Think of this as all outputs are mapped to from some element.
- f is **bijective** if it is both injective and surjective.
- f is **nonjective** (this is a joke) if it is neither bijective nor surjective

3.7 Inverses

Given function $f : X \to Y$:

- A **left inverse** of f is $g : Y \to X$ s.t. $g \circ f = \text{id}_X$
- A **left inverse** of f is $g : Y \to X$ s.t. $f \circ g = \text{id}_Y$

- The **inverse** of f is $f^{-1} : Y \to X$ s.t. $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$

Theorem: if f has a right inverse g_1 and right inverse g_2, then $g_1 = g_2$. *Proof* $g_1 = g_1 \circ \mathrm{id}_X = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2$.
It then follows that if a function has an inverse f^{-1}, it's both the left inverse and the right inverse, so f^{-1} is unique (which is why we wrote "the inverse").

Theorem: inverse and jections:
- If f has left inverse, then f injective. (The converse is true if X inhabited. Mostly because if $X = \varnothing$, there will be nothing to map to from Y, so the left inverse is not well defined)
- If f has right inverse, then f surjective.
- f has inverse iff f bijective.

4 Induction

4.1 Peano's Axioms

Let's forget everything we know about $\mathbb{N}$. We can define it again using Peano's axioms. It turns out that everything about $\mathbb{N}$ can be derived from Peano's axioms.

Peano's axioms basically says that:
- $\mathbb{N}$ is a set,
- Zero is in this set i.e. $0 \in \mathbb{N}$,
- There is some successor function $s : \mathbb{N} \to \mathbb{N}$ that satisfies:
- $0 \notin s[\mathbb{N}]$ i.e. 0 is never an output of s,
- s is injective
- For all sets X, if ($0 \in X$ and for all $n \in \mathbb{N}$, $n \in X$ implies $s(n) \in X$), then $\mathbb{N} \in X$. (viz. if X contains 0 and all the natural numbers in X "ensures" that the next natural number is in X, then X contains $\mathbb{N}$).

(The successor function s is essentially a function that adds one.)

We can then define the natural numbers we know by:
- $1 = s(0)$
- $2 = s(1)$
- $3 = s(2)$
- $\ldots$

And we can prove things using the property of s. For example, $1 \neq 2$. *Proof* AFSOC assume $1 = 2$. Then $s(0) = s(1)$, so $0 = 1$ since s injective. Then $0 = s(0)$. But 0 is not in the image of s. Contradiction $\square$.

4.2 Recursion theorem

(this is an informal statement) Any function $f : \mathbb{N} \to X$ can be completely defined by:
- Stating the value of $f(0) \in X$
- Specify the value of $f(s(n))$ in terms of n and $f(n)$.
Essentially, say what the function does to the first element, and say what the function does next to the next element based on what it did for the current element.

For example, we can define factorial, viz. $f : \mathbb{N} \to \mathbb{N}$ via $f(n) = n!$,by:
- $f(0) = 1$ viz. $0! = 1$
- $f(n+1) = (n+1)f(n)$ viz. $(n+1)! = n!(n+1)$

This can also be used to define indexed sum and product recursively.

- Sum:
  - $\displaystyle\sum_{k=1}^{0} a_k = 0$
  - $\displaystyle\sum_{k=1}^{n+1} a_k = \left(\sum_{k=1}^{n} a_k\right) + a_{n+1}$
- Product:
  - $\displaystyle\prod_{k=1}^{0} a_k = 0$

- $\prod_{k=1}^{n+1} a_k = \left(\prod_{k=1}^{n} a_k\right) \cdot a_{n+1}$

4.3 Weak Induction

4.3.1 Weak induction principle

Say we have a logical formula $p(n)$ with $n \in \mathbb{N}$.

Theorem: if $p(0)$ true and $\forall n \in \mathbb{N}, (p(n) \Rightarrow p(n+1))$, then $\forall n \in \mathbb{N}, p(n)$ is true. (Proof is somewhere)

4.3.2 Proof by weak induction

This is a proof strategy using the weak induction principle.

To prove $p(n)$ true for all $n \in \mathbb{N}$, we can:
- show $p(0)$ is true. This is called the **base case**.
- show $\forall n \in \mathbb{N}$ (our **induction variable**), $p(n)$ (**induction hypothesis**) implies $p(n+1)$ (**induction goal**). This whole whole thing is the **induction step**.

Or, if we have a base case that is not zero, say n_0, we can prove $\forall n \geq n_0, p(n)$ using a similar strategy:
- show $p(n_0)$ is true
- let $n \geq n_0$, show $p(n)$ implies $p(n+1)$.

4.4 Strong Induction

4.4.1 Strong induction principle

Say we have a logical formula $p(n)$ with $n \in \mathbb{N}$.

Theorem:

$$[p(n_0) \wedge \forall n \geq n_0, ((\forall k \in [n_0, n], p(k)) \Rightarrow p(n+1))] \Rightarrow [\forall n \geq n_0, p(n)]$$

This can be proven by weak induction!

4.4.2 Proof by strong induction

To prove $\forall n \geq n_0, p(n)$ we can do:
- show $p(n_0)$ is true (**base case**)
- let $n \geq n_0$, assume $p(k)$ for all $n_0 \leq k \leq n$, derive $p(n+1)$ (**induction step**)

4.4.3 Strong induction with multiple base cases

To prove $\forall n \geq n_{-r}, p(n)$ with some $r \in \mathbb{N}$ we can do:
- prove $p(n_{-r}) \wedge p(n_{-r+1}) \wedge \cdots \wedge p(n_{-1}) \wedge p(n_0)$
- let $n \geq n_0$, assume $p(k)$ for all $n_{-r} \leq k \leq n$, derive $p(n+1)$

4.5 Well-Ordering Principle

Theorem: every non-empty subset of $\mathbb{N}$ has a least element.

Sketch of the proof by induction
- (BC) Let $X \subseteq \mathbb{N}$. Assume $0 \in X$ then 0 is the least element
- (IS) Let $n \geq 0$. Assume for all $0 \leq k \leq n$, every subset of $\mathbb{N}$ with k as an element has a least element.
- Let $X \subseteq \mathbb{N}$. Assume $n + 1 \in X$. Case on $n + 1$ being least or not least. Case 1 is trivial, case 2 means some element k is less than $n + 1$ X therefore has least element by IH.

5 Number Theory

5.1 Division Theorem

The division theorem states that for integers $a, b \in \mathbb{Z}$ with $b \neq 0$, there exists unique pair $(q, r) \in \mathbb{Z}^2$ s.t.

$$(a = qb + r) \wedge (0 \leq r < |b|)$$

We often understand q as the quotient and r as the remainder when a is divided by b.

Sketch of proof: existence part by constructing the set $X = \{n \in \mathbb{N} \mid \exists q \in \mathbb{Z}, a = qb + n\}$ and using WOP to show it has a least element and show that it is less than $|b|$. Uniqueness part by assuming two pairs fit the definition and showing they are equal.

5.2 Divisibility

We write $b \mid a$ to say $a \in \mathbb{Z}$ is divisible $b \in \mathbb{Z}$.

When $b \neq 0$, $b \mid a$ iff the remainder when a divided by b is equal to 0.

5.3 Common Divisor

Take $a, b \in \mathbb{Z}$.

A **common divisor** of a and b is $c \in \mathbb{Z}, (c \mid a \wedge c \mid b)$. Viz. an integer that divides both a and b.

A **greatest common divisor** of a and b is $d \in \mathbb{Z}$ s.t.
- d is a common divisor of a and b viz. $d \mid a \wedge d \mid b$
- d can be divided by all other common divisors $\forall c \in \mathbb{Z}, ((c \mid a \wedge c \mid b) \Rightarrow c \mid d)$.

5.3.1 Almost uniqueness of GCDs

Take $a, b \in \mathbb{Z}$. If d_1 is a GCD, then $-d_1$ is a GCD. In other words, if d_1 and d_2 are GCDs, then $d_1 = d_2 \vee d_1 = -d_2$.

(Proof should be straightforward)

But then it means that (a, b) has a unique non-negative GCD. We write $\gcd(a, b)$ to refer to the non-negative GCD.

5.3.2 Strats for proving things about GCDs

1. Show that an expression satisfies the definition of a GCD

5.3.3 GCD techniques

Theorem: given $a, b, q, r \in \mathbb{Z}$, $a = qb + r \Rightarrow \gcd(a, b) = \gcd(b, r)$. Note that q and r do not have to be the quotient and remainder. This theorem allows us to "reduce" a gcd expression (and give rise to the Euclidean algorithm).

Euclidean algorithm can be used to find gcd! It's given as follows

```
int Euclidean(int a, int b) {
    // clean up
    if (a < 0) a = -a;
    if (b < 0) b = -b;
    if (a < b) {
        int temp = a; a = b; b = temp; // swap the vars
    }

    // do stuff
    if (b == 0) return a;
    int r = a % b;
    Euclidean(b, r);
}
```

5.4 Coprima

Let $a, b \in \mathbb{Z}$. We say they are coprime (write $a \perp b$) if $\gcd(a, b) = 1$.

Lemma: $n \perp n + 1$ for all $n \in \mathbb{Z}$. *Proof* we can instead show $nx + (n + 1)y = 1$ has integer solution. Well, $n(-1) + (n + 1)(1) = 1$ works $\square$.

Useful:
$a \perp b \Leftrightarrow$
- $\gcd(a, b) = 1$
- a and b have no common prime divisor
- a has multiplicative inverse mod b
- b has multiplicative inverse mod a

5.5 Linear Diophantine Equations

Equations that take the form of $ax + by = c$ where $a, x, b, y, c \in \mathbb{Z}$.

5.5.1 Bézout's lemma

Let $a, b, c \in \mathbb{Z}$. The diophantine equation $ax + by = c$ has integer solution(s) iff $\gcd(a, b) \mid c$.

5.5.2 Extended Euclidean algorithm

This helps us to find a solution for $ax + by = c$ with $a, b, c \in \mathbb{Z}$.

The algorithm:
1. Do the Euclidean algorithm but keep track of remainders.
2. If $\gcd(a, b) \mid c$, continue. Else, break since no solution.
3. Isolate remainders and substitute back repeatedly.
4. Scale equation to get c on one side.

5.6 Primes

5.6.1 Definitions of primes

Let $p \in \mathbb{Z}$

p is **ring theoretically prime** if $|p| > 0$ and $\forall a, b \in \mathbb{Z}, p \mid ab \Rightarrow (a \mid a \vee p \mid b)$.

p is **irreducible prime** if $|p| > 0$ and $\forall a, b \in \mathbb{Z}, p = ab \Rightarrow (a = \text{ś}1 \vee b = \text{ś}1)$. Alternatively, $\forall a \in \mathbb{Z}, a \mid p \Rightarrow (a = \text{ś}1 \vee a = \text{ś}p)$.

Useful: it follows that a positive prime $p > 0$ is irreducible iff its only positive divisors are 1 and p.

5.6.2 Fundamental theorem of arithmetic

Informally, it says that every non-zero integer have a unique prime factorisation.

Formally, let $n \in \mathbb{Z}$ with $n \neq 0$.

Then $n = up_1p_2 \dots p_r$ s.t.
- $r \in \mathbb{Z}$
- $u \in \{-1, 1\}$
- p_i is for all $1 \leq i \leq r$
- $0 \leq p_1 \leq p_2 \leq \dots \leq p_r$

The expansion $up_1p_2 \dots p_r$ is the prime factor expansion of n. And $(u, p_1, p_2, \dots, p_r) \in \mathbb{Z}^{r+1}$ is unique.

For example, $-12 = (-1) \cdot 2 \cdot 2 \cdot 3$.

5.6.3 There exists infinitely many primes!

Proof: Let X be set of $r \in \mathbb{N}$ primes. So $X = \{p_1, \dots, p_r\}$. It's sufficient to find another prime p that is not in X. Well, let n be the product of all primes in X. Then $n + 1 \perp n$ so $n + 1$ have no common prime factor with n. But $n + 1 \geq 2$ and so by FTA $n + 1$ has some prime factor that is not in X. So we found a new prime.

5.7 Modular Arithmetics

(For programmers, forget about the `%` operation for now)

5.7.1 Congruence and Modulus

Let $a, b, n \in \mathbb{Z}$, we say that a is **congruent** to b **modulo** n if either (note these imply each other):
- $n \mid a - b$
- $n \mid b - a$
- $a = kn + b$ for some $k \in \mathbb{Z}$

We denote this by writing $a \equiv b \bmod n$ or $a \equiv_n b$. We call the number n the **modulus** of the congruence.

Fun fact $\equiv_n$ is an equivalence relation. See [[Pure Math - Relations]].

5.7.2 Modular arithmetic

Unlike normal arithmetic with $=$, there are certain things cannot do with $\equiv_n$. Let $x, y, a, b \in \mathbb{Z}$ with $x \equiv_n y$ and $a \equiv_n b$, here are three allowed operations:

1. **addition:** $x + a \equiv_n y + b$
2. **multiplication:** $xa \equiv_n yb$
3. **subtraction:** $x - a \equiv_n y - b$ (basically adding the after multiplying $-1 \equiv_n -1$)

Warning: division and square root don't always work.

5.7.3 Multiplicative inverse

Let $a, n \in \mathbb{Z}$, the **multiplicative inverse** of a mod n is $u \in \mathbb{Z}$ such that $au \equiv_n 1$. Think of this as the number that "cancels" the a in a congruence expression (e.g. $ax \equiv_n b \Leftrightarrow x \equiv_n ub$ for some $b \in \mathbb{Z}$).

Theorem: such multiplicative inverse exists only iff $a \perp n$. (There is a short proof using Bézout)

6 Relations

6.1 Defining Relation

A relation applies to a set and talks about how elements in that set are related.

Formally, let there be set X and a relation R on the set X. Then R is a declaration for each pair $(a, b) \in X^2$ as to whether they are related or not. If a is related to b, we write $a\ R\ b$, otherwise we write $a \not R\ b$.

6.1.1 Relation extensionality axiom

This is similar to the [[Pure Math - Functions#Function extensionality axiom]]. Basically, we consider relations to be equal iff they relate the same pairs of elements (duh). Symbolically, R and S on X are equal iff $\forall a, b \in X, (a\ R\ b \Leftrightarrow a\ S\ b)$.

6.1.2 Graph of relation

Let there be set X and a relation R on the set X. The **graph** of R is the set of pairs $(a, b) \in X^2$ such that $a\ R\ b$. That is,

$$\mathrm{Gr}(R) = \{(a, b) \in X^2 \mid a\ R\ b\} \subseteq X^2$$

Relations are always well defined :)

Another way to define relation equality, therefore, is to say that they have the same graph:

$$R = S \Leftrightarrow \mathrm{Gr}(R) = \mathrm{Gr}(S)$$

where R and S are relations on X.

6.1.3 Empty relation

We can have relation E with $\mathrm{Gr}(E) = \varnothing$. This is the same thing as saying nothing is related.

6.2 Properties of relations

Let R be a relation on X. R can have these properties

Reflexivity: R is reflexive if $\forall x \in X, x\ R\ x$. That is, every element is related to itself

Symmetry: R is symmetric if $\forall a, b \in X, (a\ R\ b) \Leftrightarrow (b\ R\ a)$. That is, relation always go in two directions.

Antisymmetry: R is antisymmetric if $\forall a, b \in X, (a\ R\ b \wedge b\ R\ a) \Rightarrow (a = b)$. That is, things related in both direction are equal.

Transitivity: R is transitive if $\forall a, b, c \in X, (a\ R\ b \wedge b\ R\ c) \Rightarrow (a\ R\ c)$. Think of it as we can somehow chain relations.

6.2.1 Proving properties of relations

The usual strategy is just to show the relation satisfy a property.

6.3 Equivalence Relation

An **equivalence relation** is a relation that is reflexive, symmetric, and transitive. (Note it could be antisymmetry too)

6.3.1 Equivalence class

Given equivalence relation $\sim$ on X and element $x \in X$, we can create a set of all elements that x is related to by $\sim$. We call this a **equivalence class**. This set $[a]_\sim$ is defined by $\{a \in X \mid a \sim x\}$.

Notice that this means the same equivalence class could be represented using different element of X, which we call representatives. Take the set $\{0, 1, 2, 3\}$ and the relation $\equiv_2$, then $[0]_{\equiv_2} = [2]_{\equiv_2} = \{0, 2\}$ and $[1]_{\equiv_2} = [3]_{\equiv_2} = \{1, 3\}$.

6.3.2 Quotient

The **quotient** is defined as $X/{\sim} = \{U \subseteq X \mid \exists a \in X, U = [a]_\sim\}$ viz. the set of all equivalence classes.

Lemma: equivalence in the set X $\Leftrightarrow$ equality of equivalence class in $X/{\sim}$. Symbolically, $\forall a, b \in X, (a \sim b) \Leftrightarrow ([a]_\sim = [b]_\sim)$. (The proof should be straightforward)

Theorem: each equivalence relation $\sim$ on X corresponds with a unique partition of X, namely $\mathscr{S} = X/{\sim}$. Proof omitted.

6.4 Partial Order Relation

An **equivalence relation** is a relation that is reflexive, not symmetric, antisymmetric, and transitive. (They behave like $\leq$ or $\subseteq$, and their symbol often look like $\leq$ or $\subseteq$).

6.4.1 Bounds and mums

Let $\preceq$ be a partial order relation on X and $A \subseteq X$.

An **upper bound** for A under $\preceq$ is an element in X that is "greater" than all elements in A. That is, $u \in X$ s.t. $\forall a \in A, a \preceq u$.

An **lower bound** for A under $\preceq$ is an element in X that is "lower" than all elements in A. That is, $l \in X$ s.t. $\forall a \in A, l \preceq a$.

The **supremum** for A under $\preceq$ is the "least" upper bound. That is, $\sup_\preceq(A) = s \in X$ such that $(\forall a \in A, a \preceq s) \wedge (\forall u \in X, (\forall a \in A, a \preceq u) \Rightarrow (s \preceq u))$ viz. it's an upper bound and it's "less" than all other possible upper bounds.

The **infimum** for A under $\preceq$ is the "greatest" lower bound. That is, $\inf_\preceq(A) = i \in X$ such that $(\forall a \in A, i \preceq a) \wedge (\forall l \in X, (\forall a \in A, l \preceq a) \Rightarrow (l \preceq i))$ viz. it's a lower bound and it's "greater" than all other possible lower bounds.

Useful: The supremum of $\{X, Y\}$ under $\subseteq$ where X, Y are sets is equal to $X \cup Y$. The infimum is $X \cap Y$.

6.4.2 Existence of bounds and mums

Completeness axiom: for all subset X of $\mathbb{R}$, X has an upper bound implies it has a supremum. Simile for infimum. Think about why.

Uniqueness theorem: if a infimum exists, it's unique; if a supremum exists it's unique. This comes straight out of definition of the mums and antisymmetry of the partial order relation.

7 Counting

We're talking about counting how many things are in a set. Not to be confused with counting with finders.

7.1 Finite and Infinite Sets

Note $[n]$ for some $n \in \mathbb{N}$ denotes $\{i \in \mathbb{Z}^+ \mid i \leq n\} = \{1, 2, 3, \ldots, n\}$. (Note $[0] = \varnothing$)

7.1.1 Finite sets and their sizes

A set X is **finite** if we can find a bijection between $[n]$ for some $n \in \mathbb{N}$ and X. Think of it as assigning a number to each element of X. This number assignment is known as an **enumeration** of X.

A consequence is that this number n is unique and is equal to the size of X. We can write $|X| = n$. $|X|$ is called the **size** or **cardinality** of X.

7.1.2 Comparing sizes of finite sets

Let $m, n \in \mathbb{N}$

- If an injective $f : [m] \to [n]$ exists, then $m \leq n$
- If a surjective $f : [m] \to [n]$ exists, then $m \geq n$
- A bijective $f : [m] \to [n]$ iff $m = n$

Since we can biject $[m]$ with set X with $|X| = m$ and $[n]$ with set Y with $|Y| = n$, we can tweak the previous statement to conclude:

- If Y finite and an injective $f : X \to N$ exists, then X finite and $|X| \leq |Y|$
- If X finite and a surjective $f : X \to N$ exists, then Y finite and $|X| \geq |Y|$
- Suppose X or Y finite, then a bijective $f : X \to N$ exists iff $|X| = |Y|$

7.1.3 Size of sets from manipulating finite sets

Let X, Y be finite sets. We have that:

- $X \cap Y$ finite and $|X \cap Y| \leq \min(|X|, |Y|)$
- $X \cup Y$ finite and $|X \cup Y| \geq \max(|X|, |Y|)$ and $|X \cup Y| = |X| + |Y| - |X \cap Y|$.
- $X \times Y$ finite and $|X \times Y| = |X| \cdot |Y|$

7.2 Addition Principle

7.2.1 Finite partition

A finite partition divides a finite set into subsets that are **pairwise disjoint** and **union to the larger set**.

- **pairwise disjoint** means the intersection between any two set in the partition is empty.
- **union to the larger set** just means all the element in the larger set can be found in one of sets in the partition.

7.2.2 Counting by adding

Take finite set X and suppose $\{A_1, A_2, \ldots, A_n\}$ is a finite partition of X, then $|X| = \sum_{i=1}^{n} |A_i|$.

7.3 Multiplication Principle

7.3.1 Multiplication principle

Omitted. . . .

7.3.2 Counting by multiplying

The multiplication principle allows us to count the number of elements in a finite set X by specifying a procedure to specify elements in X uniquely. When done correctly, $|X|$ will equal the product of the number of choices at each step.

Example:

Let X be the set of all subsets of $[3] = \{1, 2, 3\}$. Then we can specify an element of X by the following procedure:
1. Decide if 1 is in the set — 2 choices
2. Decide if 2 is in the set — 2 choices
3. Decide if 3 is in the set — 2 choices
So $|X| = 2^3$.

7.4 Binomial Coefficient

The **bionomial coefficient** $\binom{n}{k}$ for any $n, k \in \mathbb{N}$ is defined by $\binom{n}{k} = |\{U \subseteq [n] \mid |U| = k\}|$. It can be understood as the number of subsets of a set of size n that have size k.

We can derive that (can be done by counting!):

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \begin{cases} \frac{n!}{k!(n-k)!} & \text{if } k \leqslant n \\ 0 & \text{if } k > n \end{cases}$$

7.5 Factorial

Instead of defining factorial recursively, we can define it by counting!

Let $n \in \mathbb{N}$, then $n!$ is defined as:
- The number of bijections $f : [n] \to [n]$
- The number of ways to list n things in an order so that each thing appear exactly once
- The number of ways to arrange n things in order
- . . .

This is kind of nice isn't it?

7.6 Proof by double counting

To prove two expressions are equal, we can define a set X in a way that we can count $|X|$ one way to get the RHS expression and another way to get the LHS expression.

7.7 Countability

7.7.1 Categories of countability

Other than a set being **finite** (which obviously makes it countable), we can have:

- A set A being **countably infinite** if we can find a bijection $f : \mathbb{N} \to A$
- A set B being **countable** if it's finite or countably infinite
- A set C being **uncountable** if it's not countable
- Known countable sets:
  - $\mathbb{N}$ (of course it bijects itself!)
  - $\mathbb{Z}$ (by doing some trick with number assignments, like $0, 1, -1, 2, -2, \ldots$)
  - $\mathbb{N}^2$ (we can list things diagonally)
  - $\mathbb{Q}$ (we can define surjection $f : \mathbb{Z} \times (\mathbb{Z} \setminus 0) \to \mathbb{Q}$ via $f(a, b) = \frac{a}{b}$)
- Known uncountable:
  - $\mathscr{P}(\mathbb{N})$
  - $\mathbb{R}$

7.7.2 Contability by jections

Given a set C which is countable:
- If an injective $f : X \to C$ exists, then X countable. Think of it as X being not bigger than a countable set.
- If an surjective $f : C \to X$ exists, then X countable. Think of it as a countable set being not smaller than X.

7.8 Operations on Countable Sets

We can prove that:

- Cartesian product of finitely many countable sets is countable (imagine going in diagonally in high dimensions where each axis is one component of the cartesian product)
- Union of countably many countable sets is countable. (imagine putting sets in grid and listing elements diagonally)

7.9 Cantor's Diagonal Argument

This is how we can prove a set is uncountable. To prove X uncountable, we do:

1. Let there be function $f : \mathbb{N} \to X$. WTS this function cannot be surjective (and thus not bijective)
2. Construct some bad element $b \in X$ in terms of f in a way that b and $f(n)$ disagrees on something for all $n \in \mathbb{N}$
3. Then show $b \neq f(n)$ for any $n \in \mathbb{N}$. This implies not all $b \in X$ can be mapped from $\mathbb{N}$, hence making f not surjective.

7.10 Cardinality

The **cardinality** of set X, denoted $|X|$, is a measure of the "size" of X in terms of how well X can inject or surject with other sets.

Let X, Y be sets.

- If there is bijection $f : X \to Y$, then $|X| = |Y|$
- If there is injection $f : X \to Y$, then $|X| \leq |Y|$
- If there is injection $f : X \to Y$ but no surjection $g : X \to Y$, then $|X| < |Y|$.

It can be easily proven that the cardinality $\leq$ relation is reflexive and transitive.

7.10.1 Cantor–Schröder–Bernstein theorem (let's call it CSB)

It says $\leq$ is antisymmetric on cardinalities. Therefor, for all sets X, Y, if there exists injection $f : X \to Y$ and injection $g : Y \to X$, we will have $|X| \leq |Y|$ and $|X| \geq |Y|$, which will imply $|X| = |Y|$.

7.10.2 Cantor's theorem

Says that the power set of all sets have strictly greater cardinality than the set itself viz. $\forall X \in \mathscr{U}, |X| < |\mathscr{P}(X)|$.

Proof: we want some injection $I : X \to \mathscr{P}(X)$ but no surjection $S : \mathscr{P}(X) \to X$.
Well, $I(x) = x$ for all $x \in X$ is surjective.
Suppose there is a surjection $S : \mathscr{P}(X) \to X$
Let $B = \{x \in X \mid x \notin S(x)\} \in \mathscr{P}(X)$.
So $B \neq F(x)$ for any $x \in X$. So S not surjective.

Fun fact—this statement is provably unprovable: "$\exists X \in \mathscr{U}, |\mathbb{N}| < |X| < |\mathbb{R}|$?"

Bish. Bash. Bosh. :)