Year 1 — Foundation of Analysis

Based on lectures by Kevin Buzzard

Notes taken by Chester Wong

First Term 2018

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

M1F

Propositions, Sets and Numbers

This chapter tells the basic mathematical logic and set theory. The proof examples are also very important.

Real Numbers

This chapter talks about the inequality of real numbers. It shows how the use of assumption in mathematics. The applying of assumption is the most important part in this chapter.

Complex Numbers

Similar to the real numbers chapter, but more assumptions.

Induction

This chapter is talking about different mathematical inductions, and how they actually works.

Picking and Choosing

A basic statistic chapter.

Completeness of Real numbers

It is really ann introduction of analysis course. It tells the concept of upper bound, epsilon delta proves, and the rigorous of maths.

Number theory

Very basic number theory. The most important part of solving the number theory questions are to find the divisors of both sides. And mostly, the number theory is considering the divisors. The Euclids algorithm to find λ and μ are also worths to revise. And the Fermat's Last Theorem are also very important.

Equivalence Relation

Introducing the binary relation, equivalence relation, and the equivalence relation's relationship with set theory.

Functions and Countability

Introduce the injection, surjection and bijection. And the bijection between countably infinite sets are also very important. And the uncountable set of $\mathbb{R}$ is because of the uncountable infinite subset of $\mathbb{Z}_{\geq 1}$

Contents

1 Propositions, Sets and Numbers

The propositions are like easy logic, and then a few sets and number concept will be discussed.

1.1 Propositions

Definition (Proposition)**.** A *proposition* is a **True** or **False** statement.

Example.

- $2 + 2 = 4$
- $2 + 2 = 100000000$
- Fermat's Last Theorem
- Riemann Hypothesis

There are some propositions that we don't know they are true or false, like Riemann hypothesis. However, in *classical mathematics*, mathematics of M1F, **every** proposition is either true or not. We are just not sure about some of them.

There are also some examples of things which are **not** propositions:

Example.

- $2 + 2$
- $2 = 2 = 4$

The first example is a number, but not proposition. It is not 'true' or 'false', it is 4. The second example doesn't even make sense. It is not a mathematical object.

1.2 Notation of proposition

There are few connectives between propositions, they are **and**, **or**, **not**, **implies**, **if and only if**

Definition (And)**.** If P and Q are propositions, "P *and* Q" is a proposition and can be written as $P \wedge Q$. $P \wedge Q$ are true when *both* P and Q are true.

We can see the relation of $P \wedge Q$, P, and Q by the truth table.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Example. $(2 + 2 = 4) \wedge (2 + 2 = 5)$ is false, since $2 + 2 = 5$ is false.

Definition (Or)**.** If P and Q are propositions, "P *or* Q" is a proposition and can be written as $P \vee Q$. $P \vee Q$ are true when *either* P, Q or *both* are true.

We can see the relation of $P \vee Q$, P, and Q by the truth table.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Example. $(2 + 2 = 4) \vee (2 + 2 = 5)$ is false, since $2 + 2 = 4$ is true.

Definition (Not)**.** If P is proposition, "not P" is a proposition and can be written as $\neg P$. $\neg P$ is the proposition which is "the opposite of P". If P is true then $\neg P$ is false, and if P is false then $\neg P$ is true.

We can see the relation of $\neg P$ and P by the truth table.

P	$\neg P$
T	F
F	T

Example. Let P be the Riemann hypothesis, then $P \vee \neg P$ is true, because in classical mathematics, the Riemann hypothesis is either true or false.

Definition (Implies)**.** If P and Q are propositions, "P *implies* Q" is a proposition and can be written as $P \implies Q$. $P \implies Q$ means if P is true, then Q is true as well.

We can see the relation of $P \implies Q$, P, and Q by the truth table.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

The only time that $P \implies Q$ is false is when P is true and Q is false.

Example. $(2+2 = 4) \implies (2+2 = 5)$ is false, but $(2+2 = 5) \implies (2+2 = 4)$ is true.

Notation. $Q \impliedby P$ is defined to be $P \implies Q$.

Definition (if and only if)**.** If P and Q are propositions, "P *if and only if* Q" is a proposition and can be written as $P \iff Q$. $P \iff Q$ is true when P and Q have the *same* truth value.

We can see the relation of $P \implies Q$, P, and Q by the truth table.

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

$\iff$ is the proposition version of $=$ for numbers. If x and y are equal numbers, we write $x = y$, but if P and Q are propositions with the same truth value, we write $P \iff Q$.

Example.

- $(P \implies Q) \iff (Q \impliedby P)$ is always true.
- $P \iff (\neg P)$ is always false.

1.3 Theorem of propositions

Theorem (Relation of *not, in* and *or*)**.** Let P and Q be propositions,

$$(\neg P) \vee (\neg Q) \iff \neg(P \wedge Q)$$

Proof. Consider the truth table,

P	Q	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q)$
T	T	$F \vee F \iff F$	$\neg(T) \iff F$
T	F	$F \vee T \iff T$	$\neg(F) \iff T$
F	T	$T \vee F \iff T$	$\neg(F) \iff T$
F	F	$T \vee T \iff T$	$\neg(F) \iff T$

We can see that the truth values of proposition $(\neg P) \vee (\neg Q)$ and $\neg(P \wedge Q)$ are always the same.

$$\therefore (\neg P) \vee (\neg Q) \iff \neg(P \wedge Q)$$

□

1.4 Sets

Definition (Set)**.** A *set* is a collection of stuff. The things in a set X are called the *elements* of X.

Note that there is a more rigorous definition of a set. The more rigorous one depends on which axiomatic foundation using for mathematics. If set theory is the foundation, the definition of a set will be "**Everything is a set.**".

1.5 Basic notation for sets.

Notation. We use { and } to denote sets.

Example.

- $\{1, 2, 3\}$ is a set.
- { me, you, the desk in my office } is a set.
- {} is a set. It exists, but it has no elements.
- $\{1, 2, 3, 2\}$ is a set.
- $\{1, 2, 3, 4, 5, ...\}$ is a set, and it is an infinite set.

We use the symbol $\in$ to denote set membership. If a is a thing (e.g. a number) and X is a set, then $a \in X$ is a proposition. The proposition $a \in X$ is true exactly when a is in set X.

Example.

- $2 \in \{1, 2, 3\}$. This means 2 is an element of set $\{1, 2, 3\}$.
- $x \in \{\}$ makes mathematical sense, but it is a false statement.

Notation. $\{\}$ has no elements, which is called the *empty set*. We use $\varnothing$ to notate an empty set.

1.6 Fundamental fact about equality of sets

Definition (Equality of sets)**.**

$$X = Y \iff (\forall a \in \Omega, a \in X \iff a \in Y)$$

It means two sets are equal if and only if they have the same elements.

Example. $\{1, 2, 3\}$ and $\{1, 2, 3, 2\}$ are equal.

Fundamental fact above is the rule for sets. If we need to count things, we can use other things, like multisets, lists, or sequences, instead of sets.

1.7 Notation of sets

1.7.1 Subsets

Notation. We use $\subseteq$ to denote subsets. $X \subseteq Y$ is a proposition saying that X is a subset of Y.

Definition (Subset)**.**

$$X \subseteq Y \iff (\forall a \in \Omega, a \in X \implies a \in Y)$$

It means X is a subset of Y when every elements of X is also an element of Y.

Example.

- $\{1, 2\} \subseteq \{1, 2, 3\}$, since elements of set $\{1, 2\}$, 1 and 2 are both inthe set $\{1, 2, 3\}$.
- If a is my left shoe, b is my right hand, and c is my mother, then $\{a, b\} \subseteq \{a, b, c\}$

Notation. $X \supseteq Y$ means $X \subseteq Y$.

Theorem (Equality and subsets)**.** If X and Y are sets, then

$$X = Y \iff (X \subseteq Y \wedge Y \subseteq X)$$

Proof. From $X \subseteq Y$, we can deduce

$$a \in X \implies a \in Y \tag{1}$$

And from $Y \subseteq X$, we can deduce

$$a \in Y \implies a \in X \tag{2}$$

From (1) and (2), we can deduce that

$$a \in Y \iff a \in X$$

which is definition of $X = Y$

$$\therefore (X \subseteq Y \wedge Y \subseteq X) \implies X = Y \tag{a}$$

Similarly, From $X = Y$, we can deduce

$$a \in Y \iff a \in X$$

And it is equivalent to

$$\begin{gathered} a \in Y \implies a \in X \\ a \in X \implies a \in Y \end{gathered}$$

which are definition of $Y \subseteq X$ and $X \subseteq Y$.

$$\therefore X = Y \implies (X \subseteq Y \wedge Y \subseteq X) \tag{b}$$

With (a) and (b), we can conclude that,

$$X = Y \iff (X \subseteq Y \wedge Y \subseteq X)$$

□

1.8 Important sets

Example.

- $\mathbb{Z}$ Integers
- $\mathbb{Q}$ Rational numbers
- $\mathbb{R}$ Real numbers
- $\mathbb{C}$ Complex numbers

Definition (Integers $\mathbb{Z}$)**.**

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

There is a problem of unconsistent of natural numbers $\mathbb{N}$. Someone defined it as

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

Someone defined it as

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

In M1F, we will not use $\mathbb{N}$. Instead, we will use the following notations.

Notation.

$$\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, ...\}$$

$$\mathbb{Z}_{\geq 1} = \{1, 2, 3, ...\}$$

For set $\mathbb{R}$, there are some special notations.

Notation. Let a and b be real numbers,

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \wedge x \leq b\}$$

$$(a, b) = \{x \in \mathbb{R} \mid a < x \wedge x < b\}$$

$$[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$$

1.8.1 Universes

Notation. We use *universe* Ω to denote the set consisting of all the stuff we are interested in.

Universe means the set we are considering. For example, Ω could be a set of real numbers, or complex numbers. It depends on what we are considering.

1.8.2 For all

Notation. We use $\forall$ to say for all in mathematics.

Example. $\forall a \in \mathbb{Z}, 2a$ is even.
This means "For all integers a, $2a$ is an even number".

1.8.3 There exists

Notation. We use $\exists$ to say there exists inn mathematics.

Example. $\exists a \in \mathbb{Z}, a$ is even.
This means "There exists an integer a, which is an even number".

1.8.4 Union

Definition (Unions)**.**

$$\forall a \in \Omega, a \in X \cup Y \iff a \in X \vee a \in Y$$

It means the *union* of X and Y, $X \cup Y$ is all the stuff in either X, *or* Y, *or both.*

Example. Let $X = \{1, 2, 3\}$ and $Y = \{3, 4, 5\}$,
then $X \cup Y = \{1, 2, 3, 4, 5\}$.

We have some notations for intersection of large numbers of sets.
Let us define $I = \mathbb{Z}_{\geq 1} = \{1, 2, 3, ...\}$. For every $i \in I$, we have a set of real numbers $X_i \subseteq \mathbb{R}$.

Notation.

$$\bigcup_{i=1}^{\infty} X_i = \{a \in \Omega \mid \exists i \in \mathbb{Z}_{\geq 1}, a \in X_i\}$$

$$\bigcup_{i \in I} X_i = \{a \in \Omega \mid \exists i \in I, a \in X_i\}$$

Example. Let $I = \mathbb{R}$. If $i \in I$, and let $X_i = \{i\}$. What is $\bigcup_{i\in I} X_i$?

$$\bigcup_{i\in I} X_i = \{a \in \mathbb{R} \mid \exists i \in I, a \in X_i\}$$

$$\therefore \bigcup_{i\in I} X_i \subseteq \mathbb{R} \tag{1}$$

Let $a \in \mathbb{R}$,

$$a \in X_a = \{a\} \qquad \text{(by definition)}$$

$\therefore \exists i \in I = \mathbb{R}$ such that $a \in X_i = \{i\}$ when $i = a$.

$$\therefore \mathbb{R} \subseteq \bigcup_{i\in I} X_i \tag{2}$$

$$\bigcup_{i\in I} X_i = \mathbb{R}$$

1.8.5 Intersection

Definition (Intersection)**.**

$$\forall a \in \Omega, a \in X \cap Y \iff a \in X \land a \in Y$$

It means the *intersection* of X and Y, $X \cap Y$ is all the stuff in *both* X, *and* Y.

Example. Let $X = \{1, 2, 3\}$ and $Y = \{3, 4, 5\}$,
then $X \cap Y = \{3\}$.

We have some notations for intersection of large numbers of sets.
Let us define $I = \mathbb{Z}_{\geq 1} = \{1, 2, 3, ...\}$. For every $i \in I$, we have a set of real numbers $X_i \subseteq \mathbb{R}$.

Notation.

$$\bigcap_{i=1}^{\infty} X_i = \{a \in \Omega \mid \forall i \in \mathbb{Z}_{\geq 1}, a \in X_i\}$$

$$\bigcap_{i\in I} X_i = \{a \in \Omega \mid \forall i \in I, a \in X_i\}$$

Example. What is $\bigcap_{i=1}^{\infty} X_i$, where $X_i = [-i, i]$?
$\because X_1 \subseteq X_2 \subseteq X_3 \subseteq ...$, real numbers in all the X_i are the real numbers in X_1.
$\therefore \bigcap_{i=1}^{\infty} X_i = X_1$

1.8.6 Complements

Definition (Complements)**.**

$$\forall a \in \Omega, a \in X^c \iff \neg(a \in X)$$

It means if X is a subset of Ω, then its *complement* X^c is the set whose elements are all the things in Ω which are not in X.

Example. If our universe Ω is $\mathbb{Z}$, the integers, and if X is the set of even integers, then its *complement* X^c is the set of odd numbers.

Notation. $a \notin X$ is defined to be $\neg(a \in X)$, since a is not an element of X is also a proposition.

1.9 Notation of sets with certain property

Let X be the set of *integers*, and we want to consider the subset of X consisting of positive integers. We can write the subset as:

$$\{a \in X \mid a > 0\}$$

The line in the middle is pronounced “’such that”. So the full statement can be read as “the elements a of X such that $a > 0$”.

1.10 Theorem of sets

Theorem (A theorem of complement)**.** Let X and Y be sets.
If $X, Y \subseteq \Omega$,

$$(X \cup Y = \Omega) \wedge (X \cap Y = \varnothing) \implies X = Y^c$$

Proof. Let $a \in \Omega$, P be proposition $a \in X$, Q be proposition $a \in Y$,

$$
\begin{array}{llll}
 & a \in X \cup Y & \iff (a \in X) \vee (a \in Y) & \text{(Union definition)} \\
\therefore & a \in X \cup Y & \iff P \vee Q & \\
\because & X \cup Y = \Omega & & \\
\therefore & a \in X \cup Y & \iff \top & \\
 & P \vee Q & \iff \top & \\
 & a \in X \cap Y & \iff (a \in X) \wedge (a \in Y) & \text{(Intersection definition)} \\
\therefore & a \in X \cup Y & \iff P \wedge Q & \\
\because & X \cup Y = \varnothing & & \\
\therefore & a \in X \cup Y & \iff \bot & \\
 & P \wedge Q & \iff \bot & \\
 & \neg(P \wedge Q) & \iff \top & \\
\therefore & P \vee Q & \iff \neg(P \wedge Q) & \\
\therefore & P & \iff \neg Q & \\
 & a \in X & \iff \neg(a \in Y) & \\
 & a \in X & \iff a \in Y^c & \text{(Complement definition)} \\
\therefore & X = Y^c & &
\end{array}
$$

$$(X \cup Y = \Omega) \wedge (X \cap Y = \varnothing) \implies X = Y^c$$

□

Let $S = \{a \in \mathbb{R} \mid a > 0\}$

Proposition (S has a smallest element)**.**

$$P := \exists s \in S, \forall t \in S, s \leq t$$

Proof. Consider $\neg P$,

$$\neg P = \forall s \in S, \exists t \in S, s > t$$

Let $s \in S$,
$\frac{s}{2}$ will also be a real number, and it is smaller than s.
$\therefore \neg P$ is true, and so P is a false proposition.
Hence, S does not have a smallest statement. □

1.11 Some Proof Examples

Lemma 1.1. If x is an integer, and x^2 is even, then x is even.

Proof. Assume x is an integer and x^2 is even.
Assume for contradiction that x is odd.
Then, $x = 2t + 1$, so $x^2 = 4t^2 + 4t + 1$.
$x^2 = 2(2t^2 + 2t) + 1$, which is an odd number.
However, we assumed that x^2 is even at the beginning, so contradiction occurs. $(\Rightarrow\!\Leftarrow)$
Hence, the assumption that x is odd must be wrong, so x should be even. □

Lemma 1.2. $\sqrt{2}$ is irrational.

Proof. Assume for a conntradiction that $\sqrt{2}$ is rational.
Write $\sqrt{2} = \frac{a}{b}$, with $a, b \in \mathbb{Z}_{\geq 1}$, and at least one of them is odd.
By squaring both sides, we can deduce

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

$$2b^2 = a^2$$

It shows that a^2 is an even number. By Lemma 1.1, a will be even.
Write $a = 2c$, with $c \in \mathbb{Z}_{\geq 1}$, we can deduce

$$2b^2 = (2c)^2$$

$$2b^2 = 4c^2$$

$$b^2 = 2c^2$$

Similarly, by Lemma 1.1, b will be even.
However, we assumed that one of a, b is odd, so contradiction occurs.$(\Rightarrow\!\Leftarrow)$
Hence, the assumption that $\sqrt{2}$ is rational is wrong, so $\sqrt{2}$ is irrational. □

Lemma 1.3.

$$a, b \in \mathbb{Q} \implies a + b, a - b, ab \in \mathbb{Q}$$

Proof. Write $a = \frac{m}{n}$, $b = \frac{r}{s}$, with $m, n, r, s \in \mathbb{Z}$ annd $n, s \neq 0$
We can deduce,

$$a \pm b = \frac{ms \pm rn}{ns}$$

Since $ms \pm rn \in \mathbb{Z}$ and $ns \neq 0$, therefore $a \pm b \in \mathbb{Q}$
We cann also deduce,

$$ab = \frac{mr}{ns}$$

Since $mr \in \mathbb{Z}$ and $ns \neq 0$, therefore $ab \in \mathbb{Q}$

□

Corollary 1.4.

$$a \in \mathbb{Q}, b \notin \mathbb{Q} \implies a + b \notin \mathbb{Q}$$

Proof. Assume $a \in \mathbb{Q}, b \notin \mathbb{Q}$. And we also assume, $a + b \in \mathbb{Q}$ for contradiction.
We know $b = (a + b) - a$, and $a + b, a \in \mathbb{Q}$ by assumption.
By Lemma 1.3, $b \in \mathbb{Q}$.
However, we assumed $b \in \mathbb{Q}$ at the beginning. ($\Rightarrow\Leftarrow$)
Hence, assumption $a + b \in \mathbb{Q}$ is false, so Corollary 1.4 is proved. □

Corollary 1.5. There are infinitely many irrational numbers.

Proof. There are infinitely many integers. Consider $n \in \mathbb{Z}$,

$$a = n + \sqrt{2}$$

$\sqrt{2}$ is irrational by Lemma 1.2, and $a \notin \mathbb{Q}$ by Corollary 1.4.
Thus there are infinitely many a.
Therefore, there are infinitely many irrational numbers. □

2 Real Numbers

2.1 Introduction

Assume we have constructed the real numbers complete with $+, -, \times, \div$.
We have also proved the facts that if $a, b, c \in \mathbb{R}$, then

- $a + b = b + a$
- $a(b + c) = ab + ac$
- $1 \times a = a$
- $0 \neq 1$
- so on

Assume we have defined $<$ on the $\mathbb{R}$. It means if $a, b \in \mathbb{R}$, we have proposition $a < b$. Lets define four axioms.

Axiom (A1)**.** $\forall a, b, t \in \mathbb{R}, a < b \implies a + t < b + t$

Axiom (A2)**.** $\forall a, b, c \in \mathbb{R}, a < b \land b < c \implies a < c$

Axiom (A3)**.** $\forall a \in \mathbb{R}$, exactly one of $a < 0, a = 0, 0 < a$ is true.

Axiom (A4)**.** $\forall a, b \in \mathbb{R}, 0 < a \land 0 < b \implies 0 < ab$

Notation. Note that $a > b$ is defined to be $b < a$.

2.2 Some proves of Real Numbers

Lemma 2.1. $\forall a, b \in \mathbb{R}, a < b \implies -b < -a$

Proof. Assume we have $a < b$,
Let $t = -a - b$,

$$a < b \implies a + t < b + t \tag{A1}$$
$$a - a - b < b - a - b$$
$$\therefore -b < -a$$

□

Lemma 2.2. $x < 0 \implies -x > 0$

Proof. Assume we have $x < 0$
Let $a = x, b = 0$

$$a < b \implies -b < -a \tag{Lemma 2.1}$$
$$\therefore 0 < -x$$

□

Lemma 2.3. $a \neq 0 \implies a^2 > 0$

Proof. Assume we have $a \neq 0$
By A3, one of $a < 0$, $a > 0$ will be true.
For $a < 0$,

$$0 < -a \qquad \text{(Lemma 2.2)}$$

$$0 < (-a) \times (-a) \qquad \text{(A4)}$$

$$0 < a^2$$

For $0 < a$,

$$0 < a \times a \qquad \text{(A4)}$$

$$0 < a^2$$

Hence, $a^2 > 0$ □

Definition ($\leq$)**.** If $a, b \in \mathbb{R}$, $a \leq b$ mean either $a < b$ or $a = b$.
We also define $a \geq b$ means $b \leq a$.

Corollary 2.4. If $x \in \mathbb{R}$, then $x^2 \geq 0$ with equality if and only if $x = 0$

Proof. If $x = 0$, $x^2 = 0$, $\therefore x^2 \geq 0$
If $x \neq 0$, $x^2 > 0$ by Lemma 2.3. Hence, $x^2 \geq 0$ is not true when $x \neq 0$
$\therefore x^2 \geq 0$ with equality $\iff x = 0$ □

Lemma 2.5. If $x < y$ and $c > 0$, then $cx < cy$.

Proof. Assume we have $x < y$.
Applying A1 with $t = -x$, $x - x < y - x$, we have

$$0 < y - x$$

Applying A4 with $a = y - x$ and $b = c$, we have

$$0 < c(y - x)$$

$$0 < cy - cx$$

Applying A1 again, with $t = cx$,

$$0 + cx < (cy - cx) + cx$$

we have

$$cx < cy$$

□

Lemma 2.6. If $0 < a < b$ and $0 < c < d$ then $ac < bd$.

Proof. Assume we have $0 < a < b$, it means $0 < a$ and $a < b$.
By A2, we will have $0 < b$.
Similarly, $0 < c < d$ means $0 < c$, $c < d$ and $0 < d$.
By Lemma 2.5, $a < b$ and $c > 0$, we can deduce

$$ac < bc$$

By Lemma 2.5, $c < d$ and $b > 0$, we can deduce

$$bc < bd$$

By A2, $ac < bc$ and $bc < bd$, we can conclude

$$ac < bd$$

□

Corollary 2.7. If $x > y > 0$ then $x^2 > y^2$

Proof. Assume we have $0 < y < x$.
By applying Lemma 2.6 to $0 < y < x$ twice, we can conclude

$$y \times y < x \times x$$

$$y^2 < x^2$$

□

Corollary 2.8. $1 > 0$

Proof. We know that $1 \neq 0$. By applying Lemma 2.7, we can deduce

$$1^2 > 0$$

$$1 > 0$$

□

Lemma 2.9. If $x > 0$ then $\frac{1}{x} > 0$.

Proof. Assume we have $x > 0$, and $\frac{1}{x} \neq 0$. By Lemma 2.7, we can deduce

$$\frac{1}{x^2} > 0$$

By Lemma 2.5, $0 < x$ and $0 < \frac{1}{x^2}$, we can deduce

$$0 < x \times \frac{1}{x^2}$$

$$\frac{1}{x} > 0$$

□

Lemma 2.10. If $x > 0$ and $y < 0$, then $xy < 0$

Proof. Assume we have $x > 0$, $y < 0$.
By Lemma 2.2, $-y > 0$.
By A4, $x > 0$ and $-y > 0$, we will have

$$0 < -xy$$

By A1, let $t = xy$, we will have

$$0 + xy < -xy + xy$$

$$xy < 0$$

□

Lemma 2.11. If $x < 0$, $y < 0$, then $xy > 0$

Proof. Assume we have $x < 0$ and $y < 0$,
By Lemma 2.2, we will have $-x > 0$ and $-y > 0$
By A4, $0 < -x$ and $0 < -y$, we will have

$$0 < (-x)(-y)$$

$$xy > 0$$

□

3 Complex Number

3.1 Introduction

In this chapter, it will record the definition of the complex numbers. The construct of complex numbers will not be recorded. And we will assume the facts of real numbers.

3.2 Definition

Definition 3.1 (Complex number)**.** A complex number is an ordered pair (x, y) of real numbers.

Ordered pair means "$(a, b) \neq (b, a)$".

Definition 3.2 (Map from $\mathbb{R}$ to $\mathbb{C}$)**.** We identify the real number r with the complex number $(r, 0)$.

Definition 3.3 (i)**.** We define the complex number i to be $(0, 1)$.

Definition 3.4 (Addition of $\mathbb{C}$)**.** If $z = (u, v)$ and $w = (x, y) \in \mathbb{C}$,

$$z + w = ((u + x), (v + y))$$

Definition 3.5 (Multiplication of $\mathbb{C}$)**.** If $z = (u, v)$ and $w = (x, y) \in \mathbb{C}$,

$$z \times w = zw = ((xu - yv), (xv + yu))$$

Definition 3.6 (Conjugate)**.** The complex conjugate of a complex number (x, y) is the complex number $(x, -y)$.

Definition 3.7 (Modulus)**.** The modulus of a complex number (x, y) is the real number $\sqrt{x^2 + y^2}$

Notation. The modulus of a complex number z is defined to be $|z|$

Definition 3.8 (Argument)**.** The argument of a complex number $z = (x, y)$ is the unique angle θ, such that $\sin\theta = \frac{y}{|z|}$ and $\cos\theta = \frac{x}{|z|}$

Definition 3.9 (cis)**.** If $\theta \in \mathbb{R}$, then $cis(\theta) := \cos\theta + i\sin\theta$.

3.3 Theorem of Complex Numbers

Theorem 3.10 ($|z| \in \mathbb{R}^+$)**.** If z is a non-zero complex number, then $|z| \in \mathbb{R}^+$.

Theorem 3.11 (Multiplication of conjugate)**.** If $z \in \mathbb{C}$, then $z\overline{z} = |z|^2$.

Theorem 3.12 (Inverse)**.** If $z \in \mathbb{C}$ is non-zero, then there exists $w \in \mathbb{C}$ such that $zw = 1$.

Theorem 3.13 (De Moivres theorem)**.** If $\theta, \phi \in \mathbb{R}$, then $cis(\theta+\phi) = cis(\theta)cis(\phi)$.

Theorem 3.14 (Power of $\mathbb{C}$)**.** If $n \in \mathbb{Z}_{\geq 1}$, then $cis(n\theta) = (cis(\theta))^n$

4 Induction

4.1 Introduction

The *principle of mathematical induction* is a technique for proving *infinitely* many propositions at once.

Assume that we know two things,

- $P(1)$ is true.
- For every positive integer d, we can deduce $P(d+1)$ from $P(d)$.

4.2 Proof

Assuming we have the two things above.
Is it really that it can prove $P(n), \forall n \in \mathbb{Z}_{\geq 1}$?
Here is a proof.

Proof. Let S be a set that $S = \{n \in \mathbb{Z}_{\geq 1} \mid \neg P(n)\}$.
Assuming S is non-empty.
Let e be the smallest element of S.
We know that $e \neq 1$, since $P(1)$ is true.
Let $e = d + 1$, and $d \in \mathbb{Z}_{\geq 1} \because e \neq 1$
Since e is the smallest element of S, thereofore $P(d)$ is true.
$\because P(d) \implies P(d+1)$, $\therefore P(d+1)$is true.
Hence, $P(e)$ is true. However, e should be in S, so $P(e)$ should be false.
Hence, contradiction occurs. ($\Rightarrow\!\Leftarrow$)
Therefore, the assumption of S is non-empty will be false. There does not exist a $n \in \mathbb{Z}_{\geq 1}$ such that $P(n)$ is false.
We can then conclude that $P(n), \forall n \in \mathbb{Z}_{\geq 1}$. □

4.3 Other induction

Theorem (Induction of different base)**.** If $k \in \mathbb{Z}$ is a fixed base, and $Q(m)$ are propositions for $m = k, k+1, k+2, ...$ and:

- $Q(k)$ is true
- $Q(e) \implies Q(e+1)$, $\forall e \geq k$

then $Q(m)$ is true $\forall m \geq k$.

Theorem (Strong Induction)**.** If $Q(m)$ are propositions for $m \in \mathbb{Z}_{\geq 1}$, and we know that:

- $Q(1)$ is true.
- $\forall d \in \mathbb{Z}_{\geq 1}$, $\bigwedge_{i=1}^{d} Q(i) \implies Q(d+1)$.

then $Q(n)$ is true for all $n \geq 1$.

Proof. Let $P(n)$ be the proposition that $\bigwedge_{i=1}^{n} Q(i)$.
For $n = 1$,
$P(1) = Q(1)$ which is true.
$\therefore P(1)$ is true.
Assume $P(k)$ is true, for $k \in \mathbb{Z}_{\geq 1}$, which means:
$\bigwedge_{i=1}^{k} Q(i)$ is true For $n = k + 1$,
$\because \bigwedge_{i=1}^{k} Q(i) \implies Q(k + 1)$
$\therefore (\bigwedge_{i=1}^{k} Q(i)) \wedge Q(k + 1)$ is true.
$\therefore \bigwedge_{i=1}^{k+1} Q(i) = P(k + 1)$ is true.
By the principle of mathematical induction, $P(n)$ is true, $\forall n \in \mathbb{Z}_{\geq 1}$
Since $P(n) \implies Q(n)$,
Hence, we can conclude that $Q(m)$ is true, $\forall m \geq k$. □

5 Picking and Choosing

5.1 Introduction

There are ways to do counting. And here, some theorems of counting are recorded. However, proof is not provided.

5.2 Theorem

Theorem 5.1 (Multiplication Principle)**.** Let P be process with n steps, and suppose that for $1 \leq r \leq n$, the number of choices for the rth step is a_r, independent of which choices are made in the first $r-1$ steps.
Then the process can be done in $a_1 a_2 a_3 ... a_n$

Theorem 5.2 (Size n set ordering)**.** There are $n!$ ways of linearly ordering a set of size n.

Definition 5.3 (Binomial Coefficient)**.** If $r, n \in \mathbb{Z}_{\geq 0}$ with $0 \leq r \leq n$, define the binomial coefficient $\binom{n}{r}$ to be the number of r-element subsets of a set of size n.

Theorem 5.4 ($\binom{n}{r}$)**.**

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Theorem 5.5 (Binomial Theorem)**.**

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

Definition 5.6 (Multinomial Coefficient)**.** Say $n, d \in \mathbb{Z}_{\geq 0}$ and we have d non-negative integers $r_1, r_2, r_3, ..., r_d$ with $r_1 + r_2 + \ + r_d = n$. The multinomial coefficient $\binom{n}{r_1, r_2, ..., r_d}$ is defined to be the number of ways we can partition a set S of size n up into d disjoint subsets X_1 of size r_1, X_2 of size r_2, ..., X_d of size r_d.

Theorem 5.7 ($\binom{n}{r_1, r_2, ..., r_d}$)**.** Say $n, d \in \mathbb{Z}_{\geq 0}$ and $r_1, r_2, ..., r_d \mathbb{Z}_{\geq 0}$ satisfy $\sum_{i=1}^{d} r_i = n$.

$$\binom{n}{r_1, r_2, ..., r_d} = \frac{n!}{r_1! r_2! ... r_d!}$$

Theorem 5.8 (Multinomial Theorem)**.**

$$(a_1 + a_2 + a_3 + ... + a_d)^n = \sum \left(\binom{n}{r_1, r_2, ..., r_d} \prod_{i=1}^{d} a_i^{r_i} \right)$$

6 Completeness of Real numbers

6.1 Introduction

There is an axiom for the real numbers.

Completeness axiom for the real numbers:
"Any non-empty set of real numbers which is bounded above, has a least upper bound".

This chapter will discuss the meaning of these words.

6.2 Definition

Definition. Let $S \subseteq \mathbb{R}$,

- We say a real number $b \in \mathbb{R}$ is an upper bound for S if $\forall s \in S, s \leq b$.
- We say S is bounded above if there exists a real number $b \in \mathbb{R}$ which is an upper bound for S.

Definition. Let $S \subseteq \mathbb{R}$ be a set of real numbers. We say that $l \in \mathbb{R}$ is a least upper bound for S if it satisfies both of the following two properties:

- l is an upper bound for S.
- If $b \in \mathbb{R}$ is any upper bound for S then $l \leq b$.

Example. Find the least upper bound for $S = (0, 1)$.
We can spot that $l = 1$ is an upper bound for S.
Since $s \in S \implies s < 1 \implies s \leq 1$
Let $b \in \mathbb{R}$ be any upper boundfor S, i.e $\forall s \in S, s \leq b$.
Assume $b < l = 1$,
Since $\frac{1}{2} \in S$, so $\frac{1}{2} \leq b$.
Let a be the average of b and 1, so $a = \frac{b+1}{2}$. Then,

$$0 < \frac{1}{2} \leq b < \frac{b+1}{2} = a < 1$$

Obviously, $a \in S$, since $0 < a < 1$.
If b is an upper bound of S, then $b \geq a$, but now $b < a$.
Hence, contradiction occurs. ($\Rightarrow\!\Leftarrow$)
There does not exist an upper bound $b < l$.
Hence, $l = 1$ is the least upper bound of S.

6.3 Theorem

Theorem 6.1. Say $S \subseteq \mathbb{R}$, and l_1, l_2 are both least upper bounds for S.
Then $l_1 = l_2$.

Proof. By definition, l_1, l_2 are both upper bounds.
By definition again, since l_1 is a least upper bound and l_2 is an upper bound, so it implies $l_1 \leq l_2$.
Similarly, since l_2 is also least upper bound, so $l_2 \leq l_1$.
With $l_1 \leq l_2$ and $l_2 \leq l_1$, $l_1 = l_2$ □

Example. Show that $\mathbb{R}$ is not bounded above.
Assume there exists l is an upper bound of $\mathbb{R}$.
By definition, $\forall r \in \mathbb{R}, r \leq l$ and $l \in \mathbb{R}$.
Since $l + 1 \in \mathbb{R}$ as l and 1 are also real numbers.
Therefore, $l + 1 \leq l$.
Obviously, $l + 1 > l$. But now it shows that $l + 1 \leq l$. Thus, contradiction occurs. $(\Rightarrow\Leftarrow)$
Hence, there does not exist upper bound for $\mathbb{R}$. Thus, $\mathbb{R}$ is not bounded above.

Axiom (Completeness axiom)**.** If $S \subseteq \mathbb{R}$ is non-empty and bounded above, then S has a supremum.

Theorem 6.2. If $x \in \mathbb{R}$, then there is an integer n with $n > x$.

Proof. Assume for some $x \in \mathbb{R}$, there does not exist integer $n > x$.
Then, $\forall n \in \mathbb{Z}, n \leq x$.
Therefore x would be an upper bound of $\mathbb{Z}$.
Since $\mathbb{Z}$ is non-empty and bounded above, so there exists $\sup(\mathbb{Z})$.
Let $l = \sup(\mathbb{Z})$.
We know that $l - 1 < l$, so $l - 1$ will not be an upper bound of $\mathbb{Z}$.
If $l - 1$ is not an upper bound of $\mathbb{Z}$, then there exists $n \in \mathbb{Z}, n > l - 1$.
Therefore, $n + 1 > l$. However, $n + 1 \in \mathbb{Z}$ and l is an upper bound. Thus, $n + 1 > l$ does not exist.
Hence, contradiction occurs. $(\Rightarrow\Leftarrow)$
Thus, if $x \in \mathbb{R}$, then there is an integer n with $n > x$. □

Theorem 6.3 (Floor function)**.** If $x \in \mathbb{R}$, there is a unique integer n with $n \leq x < n + 1$.

Proof. Assume we have $x \in \mathbb{R}$,
By Theorem 6.2, there exist integer B that satisfy $B > x$, and there also exists integer A that satisfy $A > -x$. Thus, $-A < x < B$.
Consider the set of integers i, with $-A \leq i$ and $i \leq x$. (Let it be I)
This set will be finite, since we know that $-A$ is in the set, but B is not.
Therefore, there must be a largest integer n in the set I, and $n + 1$ is not.
Hence, there exists integer n that satisfy $n \leq x < n + 1$.

Assume the integer n is not unique. There also exists m that satisy $m \leq x < m+1$ and $n \neq m$.
If $n \neq m$, then $n < m$ or $m < n$.
If $n < m$, then $n + 1 \leq m$. Thus,

$$x < n + 1 \leq m \leq x$$

Hence, contradiction occurs. $(\Rightarrow\Leftarrow)$
Thus, $n < m$ is false. And similarly, $m < n$ is also false.
Hence, the integer n is unique. □

Theorem 6.4. If $x < y$ are real numbers, then there is a rational number q with $x < q < y$.

Proof. If $x < y$, then $(y - x) > 0 \implies \frac{2}{y-x} > 0$.
By Theorem 6.2, there exist integer D such that $D > \frac{2}{y-x}$ and so, $(y - x) > \frac{2}{D}$.

Set $N = \lfloor Dy \rfloor - 1 < Dy$, so $\frac{N}{D} < y$.
And $N + 2 = \lfloor Dy \rfloor + 1 > Dy \implies N > Dy - 2$.

$$x = y - (y - x) < y - \frac{2}{D} = \frac{Dy - 2}{D} < \frac{N}{D} < y$$

Therefore, $\frac{N}{D}$ is a rational number that satisfy $x < q < y$. □

Example. There is a positive real number whose square is 2.

Proof.

Lemma 6.5. Say $l \in \mathbb{R}_{\geq 1}$ and $l^2 > 2$.
Then there exists $\epsilon > 0$ such that $l - \epsilon > 0$ and $(l - \epsilon)^2 > 2$.

Proof. Set $\delta = \frac{l^2-2}{2}$, so $l^2 > l^2 - \delta = \frac{l^2+2}{2} > 2$.
Set $\epsilon = \min\left\{\frac{\delta}{2l}, \frac{l}{2}\right\}$. Thus, $\epsilon \leq \frac{l}{2} < l$, so $l - \epsilon > 0$.

$$\begin{aligned}(l - \epsilon)^2 &= l^2 - 2l\epsilon + \epsilon^2 \\ &\geq l^2 - 2l\epsilon \\ &\geq l^2 - \delta > 2\end{aligned}$$

□

Lemma 6.6. Say $l \in \mathbb{R}_{\geq 1}$ and $l^2 < 2$.
Then there exists $\epsilon > 0$ such that $l + \epsilon > 0$ and $(l + \epsilon)^2 < 2$.

Proof. Set $\delta = \frac{2-l^2}{2}$, so $l^2 < l^2 + \delta = \frac{l^2+2}{2} < 2$.
Set $\epsilon = \min\left\{\frac{\delta}{2}, \frac{\delta}{4l}, 1\right\}$.

$$\begin{aligned}0 < \epsilon \leq 1 &\implies \epsilon^2 < \epsilon \leq \frac{\delta}{2} \\ \epsilon \leq \frac{\delta}{4l} &\implies 2l\epsilon \leq \frac{\delta}{2}\end{aligned}$$

$$\begin{aligned}(l + \epsilon)^2 &= l^2 + 2l\epsilon + \epsilon^2 \\ &\leq l^2 + \frac{\delta}{2} + \frac{\delta}{2} \\ &= l^2 + \delta < 2\end{aligned}$$

□

Consider set $S = \{x \in \mathbb{R} | x^2 < 2\}$.
Obviously, S is non-empty, as $1 \in S$, since $1^2 = 1 < 2$.
S is also bounded above, as $10 \notin S$, since $10^2 = 100 > 2 > x^2$.
Thus, $\forall s \in S, 10 \geq s$ is true, and so S is bounded above.
By the completness of $\mathbb{R}$, S will have a least upper bound, say l.
By the rule of inequlaity, one of $l^2 = 2$, $l^2 < 2$ and $l^2 > 2$ will be true.
Assume $l^2 < 2$, by Lemma 6.6, there exist $x, \epsilon \in \mathbb{R}, x = l + \epsilon$ with $x^2 < 2$, so $x \in S$, l will not be upper bound of S as $x = l + \epsilon > l$. Thus, $l^2 < 2$ is false.
Assume $l^2 > 2$, by Lemma 6.5, there exist $x, \epsilon \in \mathbb{R}, x = l - \epsilon$ with $x^2 > 2$, so x will be an upper bound. Thus, l will not be the least upper bound, as $x = l - \epsilon < l$. Thus, $l^2 > 2$ is false.
Hence, $l^2 = 2$ will be true, since l does exist. □

7 Number theory

7.1 Introduction

In this chapter, some basic number theory will be discussed.

7.2 Theorems and Definitions

Lemma. Say $a \in Z$ and $b \in \mathbb{Z}_{\geq 1}$ are integers. Then,

- We can write $a = qb + r$ with q (quotient) an integer, and r (remainder) an integer satisfying $0 \leq r < b$.
- If $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$,then $q = q'$ and $r = r'$.

Proof. We have $b \geq 1$, so $b \neq 0$.
Set $x = \frac{a}{b}$ and $q = \lfloor x \rfloor$.
Thus, $q \leq x < q + 1$, and so $qb \leq bx < b(q + 1)$.

$$qb \leq a < qb + b$$

Hence, there must exist r such that $a = qb + r$ and $0 \leq r < b$.

Say $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$.
We can deduce

$$b(q - q') = r' - r$$

Obviously, the left side will be a multiple of b and hence it is either 0 or has absolute value at least b.
The right size is the difference of two elements of $[0, b)$, and hence the difference is in $(-b, b)$. Thus, it has an absolute value less than b.
In order to make both sides equal, both sides must be zero.
Hence, $r' - r = 0 \implies r' = r$ and $b(q - q') \implies q' = q$ since $b \neq 0$. □

Definition. If $a, b \in \mathbb{Z}$ then we say a divides b if there exists some $k \in \mathbb{Z}$ such that $b = ka$.

Notation. We say a is a *divisor* of b.
We write $a \mid b$ for "a divides b".

Theorem. If $d, x, y \in \mathbb{Z}$ with $d \mid x$ and $d \mid y$, then $\forall \lambda, \mu \in \mathbb{Z}$ we also have $d \mid (\lambda x + \mu y)$.

Proof. By definition, we know that $d \mid x$ and $d \mid y$ can deduce there exists $k_1, k_2 \in \mathbb{Z}$ such that $x = k_1 d$ and $y = k_2 d$.

$$\begin{aligned}\lambda x + \mu y &= \lambda(k_1 d) + \mu(k_2 d)\\ &= d(\lambda k_1) + d(\mu k_2)\\ &= d(\lambda k_1 + \mu k_2)\end{aligned}$$

Since $\lambda k_1 + \mu k_2 \in \mathbb{Z}$, so $d \mid (\lambda x + \mu y)$. □

Definition. $d \in \mathbb{Z}_{\geq 1}$ is the greatest common divisor of a and b, if:

- $d \mid a$ and $d \mid b$
- If $e \in \mathbb{Z}_{\geq 1}$ satisfies $e \mid a$ and $e \mid b$, then $e \leq b$

7.3 Euclids algorithm

We can use Euclids algorithm to deduce the *g.c.d* (Greatest common divisor) of two positive integers a annd b.

Consider the sequences:

$$r_n = \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor .r_{n+1} + r_{n+2}$$

By substituting $r_1 = a$ and $r_2 = b$, and work out the sequence r until $r_{k+1} = 0$, then r_k will be the $g.c.d(a, b)$.

Example. Find the $g.c.d(54, 21)$.

$$r_{n+2} = r_n - \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor .r_{n+1}$$

$$\begin{aligned} r_1 &= 54 \\ r_2 &= 21 \\ r_3 &= 54 - 2 \times 21 = 12 \\ r_4 &= 21 - 1 \times 12 = 9 \\ r_5 &= 12 - 1 \times 9 = 3 \\ r_6 &= 9 - 3 \times 3 = 0 \end{aligned}$$

Hence, $g.c.d(54, 21) = r_5 = 3$

Lemma. If Euclids algorithm applied to a and b returns the positive integer d, then $d \mid a$ and $d \mid b$.

Proof. Let $d = r_n$.
We know that $r_1 = a > r_2 = b > r_3 > ... > r_n = d > r_{n+1} = 0$.
Let $P(j)$ be proposition that $\forall j < n, d \mid r_{n-j}$.
When $j = 0$, $r_{n-0} = r_n = d$. Hence, $d \mid r_n$.
$\therefore P(0)$ is true.
When $j = 1$, $r_{n-1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor r_n + r_{n+1}$.
Since $r_{n+1} = 0$ and $r_n = d$, so

$$r_{n-1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor d$$

Hence, $d \mid r_{n-1}$. $\therefore P(1)$ is true.
Assume $P(k), P(k + 1)$, i.e $d \mid r_{n-k}$ and $d \mid r_{n-(k+1)}$ are true.
When $j = k + 2$,

$$r_{n-(k+2)} = \left\lfloor \frac{r_{n-(k+2)}}{r_{n-(k+1)}} \right\rfloor r_{n-(k+1)} + r_{n-k}$$

Therefore,for some $\lambda, \mu \in \mathbb{Z}$

$$r_{n-(k+2)} = \left\lfloor \frac{r_{n-(k+2)}}{r_{n-(k+1)}} \right\rfloor (\lambda d) + \mu d$$

Hence, $d \mid r_{n-(k+2)}$. Thus, $P(k + 2)$ is true.
By the principle of mathematical induction, $P(j)$ is true $\forall j \in \mathbb{Z}_{\leq 0}$ and $j < n$
With $P(n - 2)$ and $P(n - 1)$, we can deduce that $d \mid r_2$ and $d \mid r_1$.
Hence, $d \mid b$ and $d \mid a$. □

Lemma. If Euclids algorithm applied to a and b returns the positive integer d, then for all divisors e of a and b, we have $e \mid d$.

Proof. Let $P(j)$ be proposition that $e \mid r_j$, $\forall j \in \mathbb{Z}_{>0}$ and $j \leq N$.
When $j = 1$, $r_1 = a$. We are given that $e \mid a$, so $P(1)$ is true.
When $j = 2$, $r_2 = b$. We are given that $e \mid b$, so $P(2)$ is true.
Assume $P(k), P(k+1)$ are true, i.e. $e \mid r_k$ and $e \mid r_{k+1}$ for some k. When $j = k+2$,

$$r_{k+2} = r_k - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor .r_{k+1}$$

Therefore,for some $\lambda, \mu \in \mathbb{Z}$

$$r_{k+2} = \lambda e - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor .\mu e$$

Hence, $e \mid r_{k+2}$. $P(k+2)$ is true.
By the principle of mathematical induction, $P(j)$ is true $\forall j \in \mathbb{Z}_{>0}$ and $j \leq N$
With $P(n)$, we can deduce that $e \mid (r_n = d)$. □

Theorem. Euclids algorithm, applied to two positive integers a and b, returns the $g.c.d(a, b)$.

Proof. Applying the previous two lemmas. □

Theorem. If a and b are positive integers, and if $d = g.c.d(a, b)$, then any common divisor e of a and b divides d.

Proof. Applying the previous lemma and theorem. □

Theorem. If a, b are positive integers, then there exists integers λ and μ such that $\lambda a + \mu b = g.c.d(a, b)$.

Proof. Let $P(j)$ be proposition that there exist $\lambda_j a + \mu_j b = r_j$ for positive integer j, and $j \leq n$.
When $j = 1$, $r_1 = a$, therefore $r_1 = 1 \times a + 0 \times b$.
$\therefore P(1)$ is true.
When $j = 2$, $r_2 = b$, therefore $r_2 = 0 \times a + 1 \times b$.
$\therefore P(1)$ is true.
Assume $P(k), P(k+1)$ are true, i.e there exists $\lambda_k, \lambda_{k+1}, \mu_k, \mu_{k+1}$ such that $\lambda_k a + \mu_k b = r_k$ and $\lambda_{k+1} a + \mu_{k+1} b = r_{k+1}$
When $j = k+2$,

$$r_{k+2} = r_k - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor .r_{k+1}$$

Therefore,

$$r_{k+2} = (\lambda_k a + \mu_k b) - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor .(\lambda_{k+1} a + \mu_{k+1} b = r_{k+1})$$

Hence,

$$r_{k+2} = (\lambda_k - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor \lambda_{k+1})a + (\mu_k - \left\lfloor \frac{r_k}{r_{k+1}} \right\rfloor \mu_{k+1})b$$

$\therefore P(k+2)$ is true.
By the principle of mathematical induction, $P(j)$ is true for positive integer j, and $j \leq n$.
With $P(n)$, there exist λ_n, μ_n such that $\lambda_n a + \mu_n b = r_n = d = g.c.d(a, b)$. □

7.4 Factorization into primes

Lemma. If p is prime and $a \in \mathbb{Z}_{\geq 1}$, and if $p \nmid a$, then $g.c.d(p, a) = 1$.

Lemma. If $a, b, c \in \mathbb{Z}_{\geq 1}$ with $a \mid bc$ and $g.c.d(a, b) = 1$, then $a \mid c$.

Theorem. If $p, b, c \in \mathbb{Z}_{\geq 1}$ with p prime, and if $p \mid bc$, then $p \mid b$ or $p \mid c$.

Theorem. If $n \geq 1$ and $a_1, a_2, ..., a_n$ are all positive integers, with $p \mid \prod_{i=1}^{n} a_i$, then $p \mid a_j$ for some j with $1 \leq j \leq n$.

Theorem. Every positive integer is uniquely a product of prime numbers.

Theorem. If $a, b, c, n \in \mathbb{Z}_{\geq 1}$ with $g.c.d(a, b) = 1$, and if $ab = c^n$, then both a and b are nth powers of positive integers.

Theorem. If $a, n \in \mathbb{Z}_{\geq 1}$ and if there exists $b \in \mathbb{Q}_{>0}$ with $b^n = a$,then $b \in Z$.

7.5 Congruence

Definition. $\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{Z}_{\geq 1}$,

$$a \equiv b \mod m \iff \exists\ k \in \mathbb{Z}, a - b = m \times k$$

Theorem. Say $m \in \mathbb{Z}_{\geq 1}$ and $a, b, c \in \mathbb{Z}$

- $a \equiv a \mod m$
- If $a \equiv b \mod m$, then $b \equiv a \mod m$
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$

Theorem. Say $m \in \mathbb{Z}_{\geq 1}$, $a, b, s, t \in \mathbb{Z}$, $a \equiv s \mod m$ and $b \equiv t \mod m$

- $a + b \equiv s + t \mod m$
- $a - b \equiv s - t \mod m$
- $ab \equiv st \mod m$

Theorem (Fermat's Little Theorem)**.** If $a \in \mathbb{Z}$ and $p \in \mathbb{Z}_{>1}$ is a prime number, then

- $a^p \equiv a \mod p$
- if $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$

8 Equivalence Relation

8.1 Binary Relation

Definition. A binary relation on S is a function, which takes as input an ordered pair of elements of S, and outputs either true or false.

We can think it as a function to see if the ordered pair is in the relation subset. Say $R \subseteq S \times S$. If the pair is in R, then it outputs true, otherwise it outputs false.

8.2 Equivalence Relation

Definition. Let S be a set and let $\sim$ be a binary relation on S.

- We say $\sim$ is reflexive if $\forall s \in S, s \sim s$.
- We say $\sim$ is symmetric if $\forall s, t \in S, s \sim t \implies t \sim s$.
- We say $\sim$ is transitive if $\forall s, t, u \in S, s \sim t \wedge t \sim u \implies s \sim u$.

Definition (Partition)**.** A partition of a set S is: an index set I, and non-empty subsets C_i of S for every $i \in I$, with the property that $i \neq j \implies C_i \cap C_j = \varnothing$, and $\bigcup_{i \in I} C_i = S$.

Definition (Equivalence Class)**.** Let S be a set and let $\sim$ be an equivalence relation on S. Let $a \in S$ be an element. The equivalence class $Cl(a)$ of a is the following subset of S:

$$Cl(a) := \{ \ b \in S \mid a \sim b \ \}$$

Notation. $[a]_\sim$ is another representation of $Cl(a)$.

Lemma. Say $\sim$ is an equivalence relation on S, and $a, b \in S$. If $a \sim b$ then $Cl(b) \subseteq Cl(a)$.

Corollary. Say $\sim$ is an equivalence relation on S, and $a, b \in S$. If $a \sim b$ then $Cl(b) = Cl(a)$.

Proposition. If $a, b \in S$ then either $Cl(a) = Cl(b)$, or $Cl(a) \cap Cl(b) = \varnothing$.

Theorem. Let S be a set.

- If $\sim$ is an equivalence relation on S, and P is the partition of S corresponding to equivalence classes for $\sim$, then the equivalence relation associated to P is the same as $\sim$.
- If P is a partition of S, and $\sim$ is the associated equivalence relation, then the equivalence classes for $\sim$ are equal to the parts of P.

9 Functions and Countability

Definition. Here are the definitions of injection, surjection and bijection.

- We say f is injective, or an injection, if $\forall a, b \in X, f(a) = f(b) \implies a = b$.
- We say f is surjective, or a surjection, if $f(X) = Y$, or equivalently if $\forall y \in Y, \exists\ x \in X, f(x) = y$.
- We say f is bijective, or a bijection, if it is both injective and surjective.

Definition. Say $f : X \to Y$ is a function. We say that a function $g : Y \to X$ is a two-sided inverse for f if the composite function $g \circ f : X \to X$ is the identity function, and also the composite function $f \circ g : Y \to Y$ is the identity function.

Theorem. Say X and Y are sets, and $f : X \to Y$ is a function. Then f is a bijection if and only if f has a two-sided inverse $g : Y \to X$.

Now say X and Y and Z are three sets, and $f : X \to Y$ and $g : Y \to Z$ are functions. Recall that in this situation we can define $h := g \circ f$, so $h : X \to Z$.

Theorem. Some properties of composite function.

- If f and g are both injections, then h is an injection.
- If f and g are both surjections, then h is a surjection.
- If f and g are both bijections, then h is a bijection.

Definition. $X \leftrightarrow Y$ means that there exists a bijection $f : X \to Y$.

Definition. If a set bijects with $\{1, 2, 3, ..., n\}$ we define its cardinality to be n.

Theorem. If X and Y are finite sets, then $X \leftrightarrow Y$ if and only if X and Y have the same cardinality.

Definition. Let X be a set. By an infinite sequence $x_1, x_2, ..., x_n, ...$ of elements of X, or more precisely an infinite sequence indexed by $\mathbb{Z}_{\geq 1}$, I just mean a map $\mathbb{Z}_{\geq 1} \to X$, where the notation we use for the map is $d \mapsto x_d$.

Definition. A set is *countably infinite* if it bijects with $\mathbb{Z}_{\geq 1}$.

Definition. If X and Y are sets, then the product $X \times Y$ of X and Y is defined to be the set of ordered pairs (x, y) with $x \in X$ and $y \in Y$.

Proposition. $\mathbb{Q}$ is countably infinite.

We can say $Z_{\geq 1} \leftrightarrow Z_{\geq 0} \leftrightarrow Z \leftrightarrow Q$.

Proposition. $\mathbb{R}$ is uncountably infinte.

This is because there is an injection from the set of subsets of $\mathbb{Z}_{\geq 1}$. However, the the set of all subsets of $\mathbb{Z}_{\geq 1}$ is not countably infinte.