Number Systems

Labix

May 24, 2025

Abstract

These notes will act as a development for the number systems from the natural numbers to the complex numbers.

Contents

1 The Set of Integers

1.1 Integers as an Equivalence Relation

Recall that using axioms in ZFC, we constructed the set of natural numbers

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

together with addition and multiplication.

Definition 1.1.1 (Relation on $\mathbb{N}^2$) Define a relation $\sim$ on $\mathbb{N}^2$ as follows. We say that $(r, s) \in \mathbb{N}^2$ is related to $(p, q) \in \mathbb{N}^2$ if $r + q = s + p$. We write the relation as $(r, s) \sim (p, q)$.

Lemma 1.1.2 The above relation on $\mathbb{N}^2$ is an equivalence relation.

Proof Let $(r, s) \in \mathbb{N}^2$. Since addition in $\mathbb{N}$ is commutative, we have $r + s = s + r$ so that $(r, s) \sim (s, r)$. Thus $\sim$ is reflexive.

Suppose that $(r, s) \sim (p, q)$. Then $r + q = s + p$. Rewriting the expression as $p + s = q + r$ by commutativity of addition, we conclude that $(p, q) \sim (r, s)$. The same argument shows that $(p, q) \sim (r, s)$ implies $(r, s) \sim (p, q)$. Thus $\sim$ is symmetric.

Suppose that $(r, s) \sim (p, q)$ and $(p, q) \sim (v, w)$. Then we have that $r + q = s + p$ and $p + w = q + v$. We can deduce that

$$\begin{aligned} r + q &= s + p \\ r + q + v &= s + p + v \\ r + p + w &= s + p + v \\ r + w &= s + v \end{aligned}$$

Hence $(r, s) \sim (v, w)$ and $\sim$ is transitive. We conclude that $\sim$ is an equivalence relation. ■

Definition 1.1.3 (Integers)
Define the set of integers to be the set of equivalence classes

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\sim}$$

We write $-n$ for the equivalence class $[(0, n)]$.

1.2 Divisibility

Definition 1.2.1 (Divisibility) Let $a, b \in \mathbb{Z}$. We define the relation

$$a | b$$

if and only if there exists some $k \in \mathbb{Z}$ such that $b = ak$. We say that a divides b in this case.

Proposition 1.2.2 Let $d, m, n \in \mathbb{Z}$. The relation $|$ has the following properties and thus is a partial order in $\mathbb{N}$.

- Reflexive: $n|n$
- Anti-symmetric: $m|n$ and $n|m \implies m = n$
- Transitive: $d|n$ and $n|m \implies d|m$
- Linear: $d|n$ and $d|m \implies d|(an + bm)$ for any $a, b \in \mathbb{Z}$
- $1|n$
- $n|0$

Proof We prove antisymmetry and transitivity and leave the others for the reader. Let $m, n, d \in \mathbb{Z}$.

- (Antisymmetry) If $m|n$ and $n|m$ then there exists some $k_1, k_2 \in \mathbb{N}$ such that $n = k_1 m$ and $m = k_2 n$ thus $n = k_1 k_2 n$. Then $k_1 k_2 = 1 \implies k_1 = k_2 = 1$ and $m = n$
- (Linearity) If $d|n$ and $n|m$ then there exists $k_1 k_2 \in \mathbb{N}$ such that $n = k_1 d$ and $m = k_2 n$. Then $m = k_2 k_1 d$ thus $d|m$

■

These properties will come up again and again and will be the foundation of number theory. It is safe to say that number theory is built upon the notion of divisibility.

1.3 The Division Algorithm

This section is dedicated to develop the Euclidean algorithm, a means to find the greatest common divisor. The gcd is a central notion in number theory as well.

Definition 1.3.1 (Greatest Common Divisor) Suppose that $m, n \in \mathbb{Z}$. A number $d \in \mathbb{N}$ such that

- $d \geq 0$
- $d|m$ and $d|n$
- $e|a$ and $e|b \implies e|d$

is called the greatest common divisor of m and n, denoted $\gcd(m, n)$.

In contrast to the greatest common divisor, we also have the lowest common multiple. Although they work as a pair, we often see the notion of gcd come up more than lcm.

Definition 1.3.2 (Lowest Common Multiple) Suppose that $m, n \in \mathbb{Z}$. A number $l \in \mathbb{N}$ such that

- $l \geq 0$
- $m|l$ and $n|l$
- $m|e$ and $n|e \implies l|e$

is called the lowest common multiple of m and n, denoted $\operatorname{lcm}(m, n)$.

Beware that both of these definitions does not imply the uniqueness of such a number. However, with a little work, we will see that both of them are indeed unique. Readers should think about whether the existence of these numbers is guaranteed as well.

Proposition 1.3.3 Let $m, n \in \mathbb{Z}$. Then the numbers $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ are unique.

Proof By the third property of both numbers, we must have if c, d are $\gcd(m, n)/\operatorname{lcm}(m, n)$, then $c|d$ and $d|c$ thus $c = d$ and $\gcd(m, n)/\operatorname{lcm}(m, n)$ is unique. ■

We will see more on gcd and lcm when we deal with factorization. For now, we turn our heads to the division algorithm. This algorithm proves to us that upon dividing two integers, as long as they are not divisible by one or the other, you can always guarantee a remainder smaller than the divident.

Theorem 1.3.4 (The Division Algorithm) Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $b \neq 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$.

Proof We prove existence first by considering three cases.
Cases 1: b is divisible by a. If b is divisible by a then there exists $k \in \mathbb{Z}$ such that $b = ka$ thus $k = q$ and $r = 0$.

Case 2: b is positive and a does not divide b. Let

$$S = \{b - ka \in \mathbb{N} | k \in \mathbb{N}\}$$

Then $S \subseteq \mathbb{N}$ thus we can apply the well-ordering principle to S. Let r be the least natural number in S. Then $r \in S$ implies $r = b - ka$ for some $k \in \mathbb{N}$. Thus $b = ka + r$ for some k and r. We show that $r < a$. Suppose for a contradiction that $r \geq a$. Then $u = r - a \in \mathbb{N}$ and

$$b = ka + r \implies b = ka + (u - a) \implies b = (k-1)a + u$$

thus $u \in S$ and $u < r$, contradicting the fact that r is the least element in S. Thus $r \leq a$. If $r = a$, then

$$b = ka + a \implies b = (k+1)a$$

which means that $a|b$ which is false in our case. Thus we must have $r < a$.
Case 3: b is negative and a does not divide b. Then apply the exact same argument to the number $-b$ to get $(-b) = ka + r$ and $b = -ka - r$. Let $k' = -k - 1$ and $r' = -r + a$. Then

$$b = -ka - r = k'a + a + r' - a = k'a + r'$$

Since we have $0 \leq r < a$, we have $-a < -r \leq 0$ and $0 < r' \leq a$. Again $r' \neq a$ or else $a|b$ which contradicts our assumption.
We now prove uniqueness. Suppose that $b = aq_1 + r_1$ and $b = aq_2 + r_2$. Then $r_1 - r_2 = a(q_2 - q_1)$. We know that $-a < r_1 - r_2 < a$ thus $-a < a(q_2 - q_1) < a$ and $-1 < q_2 - q_1 < 1$ which is impossible for integers q_1, q_2 unless $q_1 = q_2$. If $q_1 = q_2$ then $r_1 = r_2$ and we are done. ■

The division algorithm does not require b to be larger than a. In fact, if a is larger than b, then the division algorithm simply gives a itself as the remainder. Before we reach our conclusion, we need one more proposition.

Proposition 1.3.5 Suppose that $m \geq n > 0$ are natural numbers with $m = qn + r$ for some $q, r \in \mathbb{N}$. Then

$$\gcd(m, n) = \gcd(n, r)$$

Proof Suppose that $d = \gcd(m, n)$. Then we know that $d < n$ from definition. We want to show that d satisfies the three results of a gcd but in terms of n and r. Since $d|n$ and $d|m$, by linearity we must have $d|r$.
Now suppose for a contradiction that there exists e such that e is a common divisor of n and r and $e > d$. Then $e|n$ and $e|r$ by definition thus $e|m$ by linearity. $e|m$ and $e|n$ implies that e is a larger common divisor of m and n than d. However this is not possible since d is assumed to be the largest among the common divisors. This is a contradiction thus $d = \gcd(n, r)$ and we are done. ■

Theorem 1.3.6 (Euclid's Algorithm) Suppose that $m \geq n > 0$ are natural numbers. We have the following inequalities.

$$m = nq_1 + r_1 \text{ with } 0 < r_1 < n$$

$$n = r_1 q_2 + r_2 \text{ with } 0 < r_2 < n$$

$$r_1 = r_2 q_3 + r_3 \text{ with } 0 < r_3 < n$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$r_{k-2} = r_{k-1} q_k + r_k \text{ with } 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k q_{k-1}$$

From this, we have $r_k | r_{k-1}$, $r_k | r_{k-2} \dots r_k | n$ and $r_k | m$.

Proof The first part of the results is due to the repeated use of the division algorithm. For the second part, we have

$$\gcd(m,n) = \gcd(n,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{k-1},r_k) = r_k$$

and we are done. ■

Lemma 1.3.7 (Bezout's Lemma) Let $a, b \in \mathbb{Z}$ such that they are not both 0. Then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a,b)$$

Proof Reconstruct x and y using the Euclidean Algorithm. This is possible since $\gcd(m,n) = r_k$ and every $r_1, \dots, r_{k-1}$ has a factor of r_k in it. ■

Lemma 1.3.8 Let $a, b \in \mathbb{Z}$ such that they are not both 0. Then the equation

$$ax + by = \gcd(a,b)$$

has an infinite number of integer solutions.

Proof Using Bezout's Lemma, we conclude that (x_0, y_0) is a solution to the equation. But then

$$(x_0 - bt, y + at)$$

are also solutions for $t \in \mathbb{Z}$ since

$$a(x_0 - bt) + b(y + at) = ax + by = \gcd(a,b)$$

■

Corollary 1.3.9 Let $a, b \in \mathbb{Z}$ such that they are not both 0 and $d \in \mathbb{Z}$. Then d divides a and b if and only if $d| \gcd(a,b)$.

1.4 Unique Factorization

Definition 1.4.1 (Prime Numbers) We say that $n \in \mathbb{N}$ is a prime number if and only if it has exactly two factors, which is 1 and n. Else n is composite.

Lemma 1.4.2 Every integer is divisible by a prime.

Lemma 1.4.3 Every integer $n > 1$ can be written as a product of primes.

Theorem 1.4.4 There is an infinite number of primes.

Proposition 1.4.5 (Euclid's Lemma) Suppose that $p, m, n \in \mathbb{N}$, with p prime and $m, n > 1$. Suppose that $p|mn$. Then p divides at least one of m or n.

Proposition 1.4.6 Suppose that p is a prime such that $p|a_1a_2\cdots a_k$. Then $p|a_i$ for some $i \in \{1, 2, \dots, k\}$

Theorem 1.4.7 (Fundamental Theorem of Arithmetic) Suppose that $n \neq 0$ is a natural number. Then there exists exactly one prime factorization for every n, meaning that the decomposition

$$n = \prod_{k=1}^{n} p_k^{s_k}$$

where p_k is prime exists and is unique.

Theorem 1.4.8 Suppose that $m, n \in \mathbb{N}$. Suppose that

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_q^{\beta_q}$$

with $p_1 = 2$, $p_2 = 3$, $p_3 = 5 \dots$. Without loss of generality $r \leq q$. Then

$$\gcd(m,n) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_q^{\min(\alpha_q,\beta_q)}$$

$$\operatorname{lcm}(m,n) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_q^{\max(\alpha_q,\beta_q)}$$

Proposition 1.4.9 Suppose that m and n are natural numbers. Then

$$\gcd(m,n) \times \operatorname{lcm}(m,n) = m \times n$$

Proof Since $\min\{a,b\} \cdot \max\{a,b\} = ab$, from the above theorem, we have that $\gcd(m,n) \times \operatorname{lcm}(m,n) = m \times n$ and we are done. ■

2 Rational Numbers

2.1 Introduction to Rationals

Definition 2.1.1 Define a relation $\sim$ on $\mathbb{Z}^2$ as follows. We say that $(a, b) \in \mathbb{Z}^2$ is related to $(c, d) \in \mathbb{Z}^2$ if $ad = bc$. We write the relation as $(a, b) \sim (c, d)$.

Lemma 2.1.2 The above relation $\sim$ on $\mathbb{Z}^2$ is an equivalence relation.

Definition 2.1.3 (Rational Numbers) Define the set of rational numbers $\mathbb{Q}$ to be the set of equivalence classes of $\mathbb{Z} \times \mathbb{Z}$ under R. Each equivalence class $E_{(a,b)}$ is denoted by $\frac{a}{b}$.

Definition 2.1.4 (Reduced Form) Suppose that $a \in \mathbb{Q}$. $a = \frac{r}{s}$ is a reduced form if

- $s > 0$
- $\gcd(r, s) = 1$

Theorem 2.1.5 For every $x \in \mathbb{Q}$, x has exactly one reduced form.

3 Real Numbers

3.1 Real Numbers as Dedekind Cuts

Definition 3.1.1 (Dedekind Cuts) A dedekind cut A is a subset of $\mathbb{Q}$ such that the following are true.

- A is non-empty
- $A \neq \mathbb{Q}$
- For all $x, y \in \mathbb{Q}$ such that $x < y$ and $y \in A$, we have that $x \in A$
- For all $x \in A$, there exists $y \in A$ such that $x < y$

Definition 3.1.2 (Real Numbers) We define the set of real numbers $\mathbb{R}$ as the set of all dedekind cuts of $\mathbb{Q}$.

Proposition 3.1.3 Define addition, subtraction, multiplication, division as follows. Then the resulting set is also a dedekind cut.

- $A + B = \{a + b : a \in A \text{ and } b \in B\}$
- $A - B = \{a - b : a \in A \text{ and } b \in \mathbb{Q} \setminus B\}$
- $A \times B = \{a \times b : a \in A \text{ and } b \in B\}$ if $A, B \geq 0$ or $A, B \leq 0$. If at one of $A, B < 0$ then use the identity $-(-A \times B)$ or $-(A \times -B)$ depending on whether $A < 0$ or $B < 0$ respectively.
- $A/B = \{a/b : a \in A \text{ and } b \in \mathbb{Q} \setminus B\}$ if $A, B \geq 0$ or $A, B \leq 0$. Use the similar approach as multiplication when one of $A, B < 0$.

Proposition 3.1.4 The following are true regarding addition of real numbers.

- Associative: For all $x, y, z \in \mathbb{R}$, $(x + y) + z = x + (y + z)$
- Additive Identity: $0 \in \mathbb{R}$ is a real number that satisfies $x + 0 = x = 0 + x$ for all $x \in \mathbb{R}$.
- Additive Inverse: For all $x \in \mathbb{R}$, $-x \in \mathbb{R}$ is a real number that satisfies $x + (-x) = 0 = (-x) + x$
- Commutative: For all $x, y \in \mathbb{R}$, $x + y = y + x$

Proposition 3.1.5 The following are true regarding multiplication of real numbers.

- Associative: For all $x, y, z \in \mathbb{R}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Multiplicative Identity: $1 \in \mathbb{R}$ is a real number that satisfies $x \cdot 1 = x = 1 \cdot x$ for all $x \in \mathbb{R} \setminus \{0\}$.
- Multiplicative Inverse: For all $x \in \mathbb{R} \setminus \{0\}$, x^{-1} is a real number that satisfies $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.
- Commutative: For all $x, y \in \mathbb{R}$, $xy = yx$.

3.2 Irrational Numbers

Proposition 3.2.1 The function $\iota : \mathbb{Q} \to \mathbb{R}$ given by

$$\iota(p) = \{p \in \mathbb{Q} \mid x < q\}$$

defines a bijection from $\mathbb{Q}$ to $\iota(\mathbb{Q})$.

This shows that we can identify $\mathbb{Q}$ as a subset of $\mathbb{R}$.

Definition 3.2.2 (Irrational Numbers) Let $x \in \mathbb{R}$. We say that x is an irrational number if $x \notin \text{im}(\iota)$.

Theorem 3.2.3 There exists an irrational number.

Proof We want to show that there is an irrational number represented by a dedekind cut such that its square is 2. Consider the set $A = \{x \in \mathbb{Q} : x < 0 \text{ or } x^2 < 2\}$. A is non-empty since $0 \in A$. $A \neq \mathbb{Q}$ since $3 \notin A$. Suppose $p \in A$. We then need to show that $q \in A$ whenever $q < p$. When $0 \leq q < p$, we have $0 \leq q^2 < p^2$ from ordering of rationals. When $q < 0$, then $q \in A$ by definition of A. Thus this is true. Now we need to show that there is always a rational q larger than p which

is in A. Choose $q = \frac{2p+2}{p+2}$, then $p < q$ and $q^2 < 2$. Thus A is a dedekind cut.
Now consider $A \times A$. We have $A \times A \leq 2$ since for all $x, y \in A$, we have $x^2 < 2$ and $y^2 < 2$ and thus $xy < 2$ whenever $xy \geq 0$. Thus the set $A \times A = \{r \in \mathbb{Q} : r < 0 \text{ or } r = xy \text{ for some } x, y \in A \text{ and } x, y > 0\}$ is less than or equal to 2. We know that $A \times A$ is a dedekind cut. But we want to know if $A \times A$ represents the number 2. Suppose that $u \in A \times A$. Then we know that from A, there exists a number $v \in A$ such that $u < v^2 < 2$. And this applies for every u. Then we know that $A \times A = 2$ since $A \times A = \{x \in \mathbb{Q} : x < 2\}$, which is our definition of rational numbers with dedekind cut.
We have proved that there exists a dedekind cut such that its square is 2. But is that dedekind cut irrational? We now represent A with $\sqrt{2}$. Suppose that $\sqrt{2}$ is rational. Then we can write it is as $\frac{m}{n}$ in reduced form. Then we have $2n^2 = m^2$. Then $2|m^2$ thus $2|m$. Let $m = 2k$ for some $k \in \mathbb{N}$. Then $2k^2 = n^2$ which similarly implies that $2|n$. This contradicts the fact that $\frac{m}{n}$ is in reduced form, thus $\sqrt{2}$ is in fact not rational, and is an irrational number. ■

3.3 Ordering and Absolute Values

Definition 3.3.1 (Order) If A, B are dedekind cuts then we say that $A < B$ if and only if $A \subset B$.

Theorem 3.3.2 (Bernoulli's Inequality) For all $x \geq -1$ and $n \in \mathbb{N}$,

$$(1+x)^n \geq 1 + nx$$

Proof We prove the inequality by induction on n. In the case of $n = 1$, we have $1 + x \geq 1 + x$, which is true for all x. Now suppose that the inequality works for some $n \in \mathbb{N}$. We have

$$\begin{aligned} (1+x)^{n+1} &\geq (1+x)(1+nx) && \text{(Induction Hypothesis and } x \geq -1) \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x && (\text{since } x^2 \geq 0) \end{aligned}$$

Thus we have the Bernoulli's Inequality by the principle of mathematical induction. ■

The absolute value is an important function when it comes to defining useful concepts such as distances in the field of real.

Definition 3.3.3 (The Absolute Value) The absolute value of a real number x is defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0 \end{cases}$$

The absolute value has some properties that are extremely useful in certain circumstances, notably number 4 and 5.

Proposition 3.3.4 The absolute Value has the folowing properties

1. $|x| \geq 0$
2. $|xy| = |x||y|$
3. $|\frac{x}{y}| = \frac{|x|}{|y|}$
4. $|x + y| \leq |x| + |y|$
5. $||x| - |y|| \leq |x - y|$

Proof I left out the proofs of (2) and (3) since they are simplay obtained via case by case analysis.

1. When $x \geq 0$ we have $|x| = x \geq 0$. When $x < 0$ we have $|x| = -x > 0$

2. We start by squaring the left hand side of the inequality.

$$\begin{aligned}|x+y|^2 &= (x+y)^2\\ &= x^2+2xy+y^2\\ &\leq |x|^2+2|x||y|+|y|^2\\ &= (|x|+|y|)^2\end{aligned}$$

Since the both sides of the inequality is non-negative, we can take the square root on both sides, thus obtaining $|x+y| \leq |x|+|y|$.

3. Choose x to be $x-y$ in (4) and we obtain $|x|-|y| \leq |x-y|$. Similarly, choosing y to be $y-x$ in (4), we find that $|y|-|x| \leq |y-x| = |x-y|$. Thus we have $||x|-|y|| \leq |x-y|$.

■

3.4 The Binomial Theorem

Definition 3.4.1 (The Binomial Coefficient) Let $n, r \in \mathbb{N}$ with $n > 0$. We define the binomial coefficient $\binom{n}{r}$ to mean the number $\frac{n!}{r!(n-r)!}$ when $r \leq n$. When $r > m$ then $\binom{n}{r} = 0$.

Proposition 3.4.2 Let $n, r \in \mathbb{N}$ with $0 < r < n$, we have $\binom{n}{r} = \binom{n}{n-r}$.

Proposition 3.4.3 Let $n, r \in \mathbb{N}$ with $0 < r < n$, we have $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$.

Theorem 3.4.4 (The Binomial Theorem) Suppose $a, b \in \mathbb{R}$. Then

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

Theorem 3.4.5 [Vandermonde's Theorem] Suppose that $a, b, n \in \mathbb{N}$. Then

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}$$

4 Complex Numbers

4.1 Introduction to Complex Numbers

Definition 4.1.1 (Complex Numbers) Define the set of complex numbers $\mathbb{C}$ to be $\mathbb{R}^2$. For each pair of real numbers $(a, b) \in \mathbb{R}^2$.

For each pair of real numbers $(a, b) \in \mathbb{R}^2$, we write $a + b\sqrt{-1}$ to represent the pair (a, b) to indicate that we are working over the complex numbers.

Definition 4.1.2 (Complex Addition) Define complex addition to be the function $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ given by

$$(a, b) + (c, d) = (a + c, b + d)$$

Definition 4.1.3 (Complex Multiplication) Define complex multiplication to be the function $\cdot$: $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ given by

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Proposition 4.1.4 The following are true regarding addition of complex numbers.

- Associative: For all $x, y, z \in \mathbb{C}$, $(x + y) + z = x + (y + z)$
- Additive Identity: $0 = (0, 0) \in \mathbb{C}$ is a complex number that satisfies $x + 0 = x = 0 + x$ for all $x \in \mathbb{C}$.
- Additive Inverse: For all $x \in \mathbb{C}$, $-x \in \mathbb{C}$ is a complex number that satisfies $x + (-x) = 0 = (-x) + x$
- Commutative: For all $x, y \in \mathbb{C}$, $x + y = y + x$

Proposition 4.1.5 The following are true regarding multiplication of complex numbers.

- Associative: For all $x, y, z \in \mathbb{C}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Multiplicative Identity: $1 = (1, 0) \in \mathbb{C}$ is a complex number that satisfies $x \cdot 1 = x = 1 \cdot x$ for all $x \in \mathbb{C} \setminus \{0\}$.
- Multiplicative Inverse: For all $x \in \mathbb{C} \setminus \{0\}$, x^{-1} is a complex number that satisfies $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.
- Commutative: For all $x, y \in \mathbb{C}$, $xy = yx$.

Definition 4.1.6 (Conjugation) Define conjugation to be a function $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$ given by

$$\overline{(a, b)} = (a, -b)$$

We say that $(a, -b)$ is the conjugation of the complex number $(a, b) \in \mathbb{C}$.

Proposition 4.1.7 The following are true regarding conjugation.

- For all $z \in \mathbb{C}$, $\overline{\overline{z}} = z$
- For all $z, w \in \mathbb{C}$, $\overline{z + w} = \overline{z} + \overline{w}$
- For all $z, w \in \mathbb{C}$, $\overline{zw} = \overline{zw}$

4.2 Polar Representation of Complex Numbers

Definition 4.2.1 (Modulus) Define modulus to be the function $|\cdot| : \mathbb{C} \to \mathbb{R}$ given by

$$|(a, b)| = \sqrt{a^2 + b^2}$$

We say that $|(a, b)|$ is the modulus of the complex number $(a, b) \in \mathbb{C}$.

Proposition 4.2.2 Then the following are true regarding the modulus.

- $|z|^2 = |z||\bar{z}|$
- $|\bar{z}| = |z|$
- $|zw| = |z||w|$
- $z\bar{z} = |z|^2$
- $|z + w| \leq |z| + |w|$
- $|z - w| = ||z| - |w||$

Definition 4.2.3 (Argument) Define argument to be the function $\arg : \mathbb{C} \to \mathcal{P}(\mathbb{R})$ given by

$$\arg((a, b)) = \left\{ \theta \in \mathbb{R} \mid \cos(\theta) = \frac{a}{|(a, b|} \text{ and } \sin(\theta) = \frac{b}{|(a, b|} \right\}$$

Proposition 4.2.4 The following are true regarding the argument.

- $\arg(zw) = \arg(z) + \arg(w) = \{\theta + \phi \mid \theta \in \arg(z), \phi \in \arg(w)\}$
- $\arg(\bar{z}) = -\arg(z)$

Lemma 4.2.5 Let $z \in \mathbb{C}$ be a complex number. Then there exists a unique real number $\theta \in \mathbb{R}$ such that $\theta \in \arg(z)$ and $-\pi < \theta \leq \pi$.

Definition 4.2.6 (Principal Argument) Define the principal argument function $\text{Arg} : \mathbb{C} \to \mathbb{R}$ to be the function sending $z \in \mathbb{C}$ to the unique real number $\text{Arg}(z) \in \mathbb{R}$ such that $-\pi < \text{Arg}(z) \leq \pi$ and $\text{Arg}(z) \in \arg(z)$.

Lemma 4.2.7 Let $z \in \mathbb{C}$ be a complex number. Then

$$\arg(z) = \{\text{Arg}(z) + 2\pi k \mid k \in \mathbb{Z}\}$$

Definition 4.2.8 (Polar Form) Let $z \in \mathbb{C}$ be a complex number. Define the polar form of z to be the expression

$$z = |z| \left(\cos(\text{Arg}(z)) + \sqrt{-1}\sin(\text{Arg}(z))\right)$$

Proposition 4.2.9 Suppose that $z = r(\cos(\theta) + i\sin(\theta))$ and $w = s(\cos(\phi) + i\sin(\phi))$.

- $zw = rs(\cos(\theta + \phi) + i\sin(\theta + \phi))$
- $\frac{1}{z} = \frac{1}{r}(\cos(-\theta) + i\sin(-\theta))$
- $\frac{z}{w} = \frac{r}{s}(\cos(\theta - \phi) + i\sin(\theta - \phi))$
- $\bar{z} = r(\cos(-\theta) + i\sin(-\theta))$

4.3 Roots of Complex Numbers

Definition 4.3.1 (nth Roots) Let $w \neq 0$ be a complex number and n a positive integer. A number z is called the nth root of w if and only if $z^n = w$.

Theorem 4.3.2 (De Moivre's Theorem) Suppose that $r \in \mathbb{Q}$. Then $(\cos\theta + i\sin\theta)^r = \cos(r\theta) + i\sin(r\theta)$

Theorem 4.3.3 (Roots of Unity) Suppose that $z = re^{i\theta}$. Then the nth roots of z are

$$r^{\frac{1}{n}} \left[\cos\left(\frac{(\theta + 2\pi k)i}{n}\right) + i\sin\left(\frac{(\theta + 2\pi k)i}{n}\right)\right]$$

where $k = 0, 1, \dots, n - 1$.