Math 273 Definitions and Theorems

Elijah Thompson

December 11, 2020

Contents

1 Integers and Division

1.1 Definitions

Definition 1.1 (Parity)**.** An integer $n \in \mathbb{Z}$ is even if and only if there exists $l \in \mathbb{Z}$ so that $n = 2l$. An integer $n \in \mathbb{Z}$ is odd if and only if there exists $l \in \mathbb{Z}$ so that $n = 2l + 1$

Definition 1.2 (Divisibility)**.** Let $a, b \in \mathbb{Z}$. a divides b, $a \mid b$, $\iff$ there exists $k \in \mathbb{Z}$ so that $b = ak$

Definition 1.3 (GCD)**.** Let $a, b \in \mathbb{Z}$, not both zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the unique integer d with the following properties:

1. $d \mid a$ and $d \mid b$
2. For all $c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \leq d$.

Definition 1.4 (Relatively Prime)**.** Let $a, b \in \mathbb{Z}$. Then a and b are relatively prime $\iff$ $\gcd(a, b) = 1$.

Definition 1.5 (Prime)**.** An integer n is prime $\iff$ $n > 1$ and for all $r, s \in \mathbb{N}$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$. On the other hand, n is composite $\iff$ $n > 1$ and there exist $r, s \in \mathbb{N}$ so that $n = rs$ and $1 < r, s < n$.

1.2 Theorems

Theorem (1). *For all integers a and b, if a and b are positive and a divides b, then a is less than b or a is equal to b.*

Proof. Suppose $a, b \in \mathbb{Z}$. Further suppose $a, b > 0$ and $a \mid b$. Then there exists $k \in \mathbb{Z}$ so that $ak = b$. Then since $a > 0$ and $ak = b > 0$, it follows that $k > 0$. Moreover, since $k \in \mathbb{Z}$ and $k > 0$, it follows that

$$1 \leq k$$

Thus, by multiplying both sides by a we find that $a \leq ak = b$, as claimed. ■

Theorem (2). *For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Axiom 1.6 (Well-Ordering Principle). *For any non-empty subset S of $\mathbb{N}$, there exists a least element $s \in S$ such that for all $x \in S$, $s \leq x$.*

Theorem (Quotient-Remainder). *For all $n \in \mathbb{Z}$ and $d \in \mathbb{N}$ there exists unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.*

Lemma 1.7 (Squares). *For all $n \in \mathbb{Z}$, if 2 divides n^2 then 2 divides n.*

Lemma 1.8 (gcd-lemma). *Let $a, b \in \mathbb{Z}$ not both zero. For any $q, r \in \mathbb{Z}$, if $a = qb + r$ then* $\gcd(a, b) = \gcd(b, r)$.

Theorem (Baezue's Identity). *For any $a, b \in \mathbb{Z}$ not both zero, there exists $x, y \in \mathbb{Z}$ so that* $\gcd(a, b) = ax + by$, *and* $\gcd(a, b)$ *is the smallest positive integer that can be written in the form $ax + by$, $x, y \in \mathbb{Z}$.*

Corollary 1.9. *For all $a, b \in \mathbb{Z}$, a and b are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ so that $xa + yb = 1$.*

Lemma 1.10 (4). *Let $p \in \mathbb{Z}$ be a prime. For any $a \in \mathbb{Z}$, if $p \mid a$, then $p \nmid (a + 1)$.*

Lemma 1.11 (5). *For all $n \in \mathbb{N}$, $n > 1$, there exists a prime p such that $p \mid n$.*

Theorem (6). *There are infinitely many prime numbers.*

Theorem (Fundamental Theorem of Arithmetic). *Given any integer n, $n > 1$, there exists a positive integer k, distinct primes $p_1, p_2, ..., p_k$, and positive integers $e_1, e_2, ..., e_k$ such that*

$$n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k},$$

and any other expansion for n as a product of prime numbers is identical to this one, except for possible reordering the prime factors.

Theorem (Prime or Composite). *For any natural number n, if $n > 1$ then n is either prime or composite.*

Theorem (Integral Combinations). *All integral combinations of natural numbers a and b are multiples of* $\gcd(a, b)$.

2 Modolar Arithmetic

2.1 Definitions

Definition 2.1 (Congruence modulo d)**.** Let $d \in \mathbb{N}$, $d > 1$. For any $a, b \in \mathbb{Z}$, if $d \mid a - b$, then we say that "a is congruent to b modulo d" and we write $a \equiv b \mod d$

Note. If $d \nmid a - b$, then we write $a \not\equiv b \mod d$.

Definition 2.2. For all $d \in \mathbb{N}$, $d > 1$, and for all $a, b \in \mathbb{Z}$, define

$$\begin{gathered} [a]_d + [b]_d = [a+b]_d \\ [a]_d[b]_d = [ab]_d \end{gathered} \tag{2.1}$$

2.2 Theorems

Lemma 2.3 (7)**.** *For all $d \in \mathbb{N}$, $d > 1$, and for all $n \in \mathbb{Z}$, n is congruent to one of $0, 1, ..., d-1$ modulo d.*

Lemma 2.4 (8)**.** *For all $d \in \mathbb{N}$, $d > 1$, and for all $a, b, r, s \in \mathbb{Z}$, if $a \equiv b \mod d$ and $r \equiv s \mod d$, then $a + r \equiv b + s \mod d$ and $ar \equiv bs \mod d$.*

Note. $\mathbb{Z}/d\mathbb{Z} = \{[a]_d : a \in \mathbb{Z}\}$, where $[a]_d = \{b \in \mathbb{Z} : b \equiv a \mod d\}$.

Corollary 2.5. *For all $d \in \mathbb{N}$, $d > 1$, and for all $a \in \mathbb{Z}$, if $\gcd(a, d) = 1$, then there exists an integer s so that $as \equiv 1 \mod d$. In this case, $[s]_d = [a]_d^{-1}$ is the multiplicative inverse of a modulo d.*

Theorem (Euclid's Lemma)**.** *For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$*

Corollary 2.6 (10)**.** *For all $a, b, c, d \in \mathbb{Z}$, where $d > 1$, if $\gcd(c, d) = 1$ and $ac \equiv bc \mod d$ then $a \equiv b \mod d$.*

Theorem (Fermat's Little Theorem)**.** *If p is prime, then for any $a \in \mathbb{Z}$ such that $p \nmid a$ and*

$$a^{p-1} \equiv 1 \mod p$$

Theorem (Chinese Remainder Theorem)**.** *Suppose that $n_1, n_2, ..., n_k \in \mathbb{N}$ are pairwise relatively prime (i.e. $\gcd(n_i, n_j) = 1$ for all $1 \leq i \neq j \leq k$) For all $a_1, a_2, ..., a_k \in \mathbb{Z}$, the system of congruences*

$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \vdots \\ x \equiv a_k \mod n_k \end{cases} \tag{2.2}$$

has a unique solution modulo $N = n_1 n_2 ... n_k$.

3 Sets

3.1 Definitions

Definition 3.1 (Set). 1. A set is a well-defined collection of objects

2. The objects that make up the set are called elements

Definition 3.2 (Subset). A is a subset of B, written $A \subset B \iff$ for all $x \in A$, $x \in B$.

Definition 3.3 (Proper Subset). A is a proper subset of B, written $A \subsetneq B \iff A \subset B$ and there exists $x \in B$ such that $x \notin A$.

Definition 3.4 (Equality). Let A and B be sets. Then $A = B \iff A \subset B$ and $B \subset A$.

Definition 3.5 (Cartesian Product). The **Cartesian Product** of sets A and B, denoted $A \times B$ is the set $\{(a, b) : a \in A \text{ and } b \in B\}$ of ordered pairs of elements in A and B.

3.2 Theorems

Lemma 3.6 (12). *For every set X, the empty set $\emptyset$ is a subset of X.*

Theorem (13). *Let A, B, and C be sets.*

1. $A \cap B \subset A$ *and* $A \cap B \subset B$
2. $A \subset A \cup B$ *and* $B \subset A \cup B$
3. *If* $A \subset B$ *and* $B \subset C$, *then* $A \subset C$

Lemma 3.7 (14). *For any sets A and B, if $A \subset B$, then $A \cap B = A$ and $A \cup B = B$.*

Lemma 3.8 (15). *There is only one set with no elements.*

Proposition 3.9 (16). *For all sets A, B, and C, if $A \subset B$ and $B \subset C^c$, then $A \cap B = \emptyset$.*

4 Functions

4.1 Definitions

Definition 4.1 (Function). A function from a set A to a set B is a subset f of $A \times B$ so that for all $x \in A$ there exists a unique $y \in B$ so that $(x, y) \in f$.

1. A is the **domain** of f
2. B is the **codomain** of f
3. If $(x, y) \in f$ we say that y is the image of x under f, and we write $f(x) = y$

Definition 4.2 (Composition). Let $f : A \to B$ and $g : B \to C$ be functions. The composition of g and f, or the composite of g and f, is the function $g \circ f : A \to C$ given by $(g \circ f)(x) = g(f(x))$ for all $x \in A$

Definition 4.3 (Bijectivity). Let $f : A \to B$ be a function.

1. f is injective $\iff$ for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$
2. f is surjective $\iff$ for all $b \in B$ there exists $a \in A$ so that $f(a) = b$
3. f is bijective $\iff$ it is both injective and surjective

Definition 4.4 (Identity). The identity function (on X) is the function $I_X : X \to X$ given by $I_X(x) = x$ for all $x \in X$

Note. The identity function is a bijection.

Definition 4.5. A function $g : B \to A$ is an inverse of $f : A \to B \iff g \circ f = I_A$ and $f \circ g = I_B$.

Definition 4.6 (Cardinality). Let A and B be two sets. A and B have the same **cardinality**, written $|A| = |B|$, $\iff$ there exists a bijection $f : A \to B$. A is said to be finite $\iff$ there exists $n \in \mathbb{N}$ so that $|A| = |\{1, ..., n\}|$

Definition 4.7 (Countable). Let A be an infinite set. A is countable $\iff$ $|A| = |\mathbb{N}|$. A is uncountable $\iff$ A is not countable.

Definition 4.8 (Image). Let $f : A \to B$ be a function, the image of f is the set

$$\mathrm{Im}(f) := \{b \in B : \exists a \in A, f(a) = b\}$$

Definition 4.9 (Boundedness). Let $S \subset \mathbb{R}$. We say that S is bounded if and only if there exists $M \in \mathbb{R}$ so that for all $x \in S$, $|x| < M$. Otherwise, S is unbounded

Definition 4.10. Let $f : \mathbb{R} \to \mathbb{R}$ be a function. Let $A \subset \mathbb{R}$.

1. f is strictly increasing on A $\iff$ for all $a, b \in A$ if $a < b$ then $f(a) < f(b)$
2. f is strictly decreasing on A $\iff$ for all $a, b \in A$ if $a < b$ then $f(a) > f(b)$

3. f is non-decreasing on A $\iff$ for all $a, b \in A$ if $a < b$ then $f(a) \leq f(b)$
4. f is non-increasing on A $\iff$ for all $a, b \in A$ if $a < b$ then $f(a) \geq f(b)$
5. f is monotone on A $\iff$ f is non-decreasing on A or f is non-increasing on A
6. f is strictly monotone on A $\iff$ f is increasing on A or f is decreasing on A
7. f is bounded on A $\iff$ $\mathrm{Im}(f)$ is a bounded subset of $\mathbb{R}$
8. f is unbounded on A $\iff$ $\mathrm{Im}(f)$ is not bounded on A.

4.2 Theorems

Lemma 4.11 (17). *A function $f : A \to B$ is a bijection $\iff$ f has a two-sided inverse.*

Lemma 4.12 (18). *If $f : A \to B$ is a bijection, then the inverse function is unique and we denote it by $f^{-1} : B \to A$.*

Corollary 4.13 (19). *If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection with inverse f.*

Proposition 4.14 (20). *$\mathbb{Z}$ is countable.*

Theorem (Composition). *The composition of two surjections is a surjection and the composition of two injections is an injection.*

Theorem (Unions of Countable Sets). *For any $n \in \mathbb{N}$, if $\mathcal{A} = \{A_1, ..., A_n\}$ is a collection of countable sets, then*

$$\bigcup_{A_i \in \mathcal{A}} A_i \tag{4.1}$$

is also countable.

Theorem (Inverses). *Let $f : A \to B$ be a function. If f has a left-sided inverse then f is injective, and if f has a right-sided inverse then f is surjective.*

Theorem (Equivalent Definitions of Countable). *Let A be an infinite set. Then A is countable if and only if*

1. *there exists an injection $f : A \to \mathbb{N}$*
2. *there exists a surjection $g : \mathbb{N} \to A$*

5 Relations

5.1 Definitions

Definition 5.1 (Relation)**.** Let A be a set. A (binary) relation on a set A is a subset of $A \times A$.

Definition 5.2 (Properties)**.** Let R be a relation on A.

1. R is **reflexive** $\iff$ for all $x \in A$, $x \ R \ x$
2. R is **symmetric** $\iff$ for all $x, y \in A$, if $x \ R \ y$ then $y \ R \ x$
3. R is **transitive** $\iff$ for all $x, y, z \in A$, if $x \ R \ y$ and $y \ R \ z$ then $x \ R \ z$

Definition 5.3 (Equivalence Relation)**.** Let R be a relation on a set A. Then R is an equivalence relation $\iff$ R is reflexive, symmetric, and transitive.

5.2 Theorems

Lemma 5.4 (21)**.** *Let A be a set. Let R be an equivalence relation on A. Define* $[a] = \{b \in A : a \ R \ b\}$ *to be the equivalence class of* $a \in A$*. The set A is the disjoint union of distinct equivalence classes.*

Theorem (21)**.** *Let* $n \in \mathbb{Z}$*,* $n > 1$*. The relation congruence modulo n is an equivalence relation on* $\mathbb{Z}$ *with distinct equivalence classes* $[0], [1], ..., [n-1]$.

6 Construction of $\mathbb{Z}$ and $\mathbb{Q}$

6.1 Definitions

Definition 6.1 (Relation on $\mathbb{N} \times \mathbb{N}$)**.** Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ as follows:

$$\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N}, (a, b) \sim (c, d) \iff a + d = c + b$$

Definition 6.2 (Integers)**.** $\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim = \{[(a, b)] : a, b \in \mathbb{N}\}$ to be the set of equivalence classes of $\sim$ on $\mathbb{N} \times \mathbb{N}$.

Definition 6.3 (Integer Operations)**.** For all $[(a, b)], [(c, d)] \in \mathbb{Z}$, we define operations $+$ and $\times$ by:

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

and

$$[(a, b)] \times [(c, d)] = [(ac + bd, ad + bc)]$$

Definition 6.4 (Relations on $\mathbb{Z} \times \mathbb{Z}^*$)**.** We define the relation $\approx$ on $\mathbb{Z} \times \mathbb{Z}^*$ by for all $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, $(a, b) \approx (c, d) \iff ad = bc$.

Definition 6.5 ($\mathbb{Q}$)**.** The rational numbers $\mathbb{Q}$ are defined to be the equivalence classes for the relation $\approx$

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \approx = \{[(a,b)] : (a,b) \in \mathbb{Z} \times \mathbb{Z}^*\}$$

We identify (a,b) with $\frac{a}{b}$

Definition 6.6 (Rational Operations)**.** For all $[(a,b)], [(c,d)] \in \mathbb{Q}$ we define operations $+$ and $\times$ by:

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

and

$$[(a,b)] \times [(c,d)] = [(ac, bd)]$$

Definition 6.7 (Lowest Terms)**.** A rational number $\frac{a}{b} \in \mathbb{Q}$ is in lowest terms $\iff$ $b > 0$ and $\gcd(a,b) = 1$.

Definition 6.8 (Irrational)**.** Let $x \in \mathbb{R}$ be a real number, then x is irrational $\iff$ $x \notin \mathbb{Q}$.

6.2 Theorems

Proposition 6.9 (22)**.** *The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is an equivalence relation.*

Theorem (23)**.** *The operations defined on $\mathbb{Z}$ form a commutative ring with identity (in particular $\mathbb{Z}$ is an integral domain).*

Lemma 6.10 (24)**.** *For any $n \in \mathbb{Z}$, $0n = 0$.*

Lemma 6.11 (25)**.** *For any $a \in \mathbb{Z}$, the additive inverse $-a$ is unique and $-a = (-1)a$.*

Proposition 6.12 (26)**.** *The relation $\approx$ $\mathbb{Z} \times \mathbb{Z}^*$ is an equivalence relation.*

Theorem (27)**.** *The operations on $\mathbb{Q}$ define a field.*

Lemma 6.13 (28)**.** *For all $q \in \mathbb{Q}$, $q = \frac{a}{b}$ is in lowest terms if and only if b is the smallest positive integer such that $q = \frac{a}{b}$*

Lemma 6.14 (29)**.** *The real numbers are the disjoint union of the rational numbers and the irrational numbers.*

Theorem (Irrationality of $\sqrt{2}$)**.** *The square root of 2 is irrational.*

Corollary 6.15 (Irrational Prime Roots)**.** *For all $p \in \mathbb{N}$, if p is a prime then $\sqrt{p} \notin \mathbb{Q}$.*

7 Sequences in $\mathbb{Q}$

7.1 Definitions

Definition 7.1 (Sequence)**.** A sequence in a set A is a function $a : \mathbb{N} \to A$. By convention we write $a_n = a(n)$ for all $n \in \mathbb{N}$, and we write $a : \mathbb{N} \to A$ as $\{a_n\} = \{a_n\}_{n=1}^{\infty}$.

Remark 7.2 (Order on $\mathbb{Q}$). On $\mathbb{N}$ we have a notion of $<$ that we can transport to $\mathbb{Q}$ to get an ordering on $\mathbb{Q}$ and

$$\mathbb{Q}^+ := \{q \in \mathbb{Q} : q > 0\}$$

Definition 7.3 (Convergence)**.** Let $\{a_n\}$ be a sequence of rational numbers. The sequence $\{a_n\}$ converges to a limit $L \in \mathbb{Q} \iff$ for all $\frac{1}{M} \in \mathbb{Q}$, $\frac{1}{M} > 0$, there exists $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, if $n \geq N$ then $|a_n - L| < \frac{1}{M}$. If $\{a_n\}$ converges and has limit L, we write $a_n \to L$. If $\{a_n\}$ does not converge we say it diverges.

Definition 7.4 (Cauchy Sequences in $\mathbb{Q}$)**.** Let $\{a_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{Q}$. $\{a_n\}_{n=1}^{\infty}$ is Cauchy $\iff$ for all $\frac{1}{M} \in \mathbb{Q}$, $\frac{1}{M} > 0$, there exists $N \in \mathbb{N}$ so that for all $m, n \in \mathbb{N}$, if $m, n \geq N$ then $|a_n - a_m| < \frac{1}{M}$.

7.2 Theorems

Lemma 7.5 (32 Triangle Inequality)**.** *For all $a, b \in \mathbb{Q}$, $|a + b| \leq |a| + |b|$.*

Lemma 7.6 (33)**.** *If $\{a_n\} \subset \mathbb{Q}$ converges to $L \in \mathbb{Q}$, then $\{a_n\}$ is Cauchy.*

Theorem (Countability)**.** *The rational numbers are countable.*

8 Constructing $\mathbb{R}$

8.1 Definitions

Definition 8.1 (Binary Operations)**.** Let S be a set. A binary operation on S is a function $*: S \times S \to S$. For all $x, y \in S$, we usually denote $*((x, y))$ by $x * y$

1. The binary operation $*$ on S is commutative $\iff$ for all $x, y \in S$ $x * y = y * x$
2. The binary operation $*$ on S is associative $\iff$ for all $x, y, z \in S$, $(x*y)*z = x*(y*z)$
3. An element $e \in S$ is an identity element for $*$ $\iff$ for all $x \in S$ $x * e = e * x = x$.

Definition 8.2 (Field)**.** A field is a triple $(F, +, *)$ consisting of a set F and two binary operations which form abelian groups over F and for all $a, b, c \in F$,

$$a(b + c) = ab + ac$$

Definition 8.3 (Order Axioms)**.** A positive set in a field F is a subset $P \subset F$ such that

1. $\forall x, y \in P, x + y \in P$
2. $\forall x, y \in P, xy \in P$
3. $\forall x \in F$, exactly one of: $x = 0$, $x \in P$ or $-x \in P$ is true (Trichotomy Property).

Define $\forall x, y \in F, x < y \iff y - x \in P$

Definition 8.4 (Relation on $\mathcal{S}$)**.** For all $\{a_n\}, \{b_n\} \in \mathcal{S}$, $\{a_n\} \sim \{b_n\} \iff \{a_n\} - \{b_n\}$ converges to 0.

Definition 8.5 (Real Numbers)**.** The real numbers $\mathbb{R}$ are defined to be the set

$$\mathbb{R} := \mathcal{S}/\sim = \{[\{a_n\}] : \{a_n\} \in \mathcal{S}\}$$

of equivalence classes on $\mathcal{S}$ under the equivalence relation $\sim$

Definition 8.6 (Positive Reals)**.** The real number $\alpha \in \mathbb{R}$ is positive $\iff$ for all $\{a_n\} \in \alpha$, there exist $k, N \in \mathbb{N}$ so that if $n \geq N$, then $a_n > \frac{1}{k}$. The real number $\alpha \in \mathbb{R}$ is positive $\iff$ $-\alpha = [\{-a_n\} : \{a_n\} \in \alpha]$ is positive.

Definition 8.7 (Operations on $\mathbb{R}$)**.** Let $\alpha, \beta \in \mathbb{R}$. Choose representatives $\{a_n\} \in \alpha$, $\{b_n\} \in \beta$. Then $\alpha + \beta = [\{a_n + b_n\}]$ and $\alpha\beta = [\{a_n b_n\}]$

8.2 Theorems

Lemma 8.8 (35)**.** *Let $\mathcal{S}$ be the set of Cauchy sequences of rational numbers. For all $\{a_n\}, \{b_n\} \in \mathcal{S}$ and $c \in \mathbb{Q}$.*

1. $\{a_n\} + \{b_n\} = \{a_n + b_n\} \in \mathcal{S}$
2. $\{a_n\}\{b_n\} = \{a_n b_n\} \in \mathcal{S}$
3. $c\{a_n\} = \{ca_n\} \in \mathcal{S}$

Proposition 8.9 (36)**.** *The relation $\sim$ on $\mathcal{S}$ is an equivalence relation.*

Proposition 8.10 (37)**.** *Addition and multiplication on $\mathbb{R}$ is well-defined.*

Lemma 8.11 (38)**.** *If a Cauchy sequence $\{a_n\} \in \mathcal{S}$ has a convergent subsequence $\{a_{n_j}\}_{j=1}^{\infty}$, $n_j \in \mathbb{N}$, then $\{a_n\}$ converges to the same limit.*

Lemma 8.12 (39)**.** *For all Cauchy sequences $\{a_n\}, \{b_n\} \in \mathcal{S}$*

1. *If $a_n \to 0$ and $b_n \to 0$, then $\{a_n + b_n\}$ converges to 0.*
2. *If $a_n \to 0$, then $\{a_n b_n\}$ converges to 0.*

9 Properties on $\mathbb{R}$

9.1 Definitions

Definition 9.1 (Completeness)**.** An ordered field F is complete $\iff$ for all sequences $\{a_n\} \subset F$, if $\{a_n\}$ is cauchy then $\{a_n\}$ converges.

Definition 9.2 (Upper Bound)**.** If $S \subset F$ is a subset, then $\beta \in F$ is an upper bound for S if for all $x \in S$ $x \leq \beta$. An upper bound β for S is a least upper bound of S $\iff$ for all upper bounds β' of S, $\beta \leq \beta'$

Definition 9.3 (Archimedean Property)**.** For all $x, y \in \mathbb{R}$, if $x > 0$ then there exists $n \in \mathbb{N}$ so that $nx > y$

Definition 9.4 (Infimums and Supremums)**.** Suppose that $S \subset \mathbb{R}$ that is bounded. Then the greatest lower bound of S is called the infimum of S, and denoted $\inf(S)$. Equivalently, the least upper bound of S is called the supremum of S, and denoted $\sup(S)$.

9.2 Theorems

Lemma 9.5 (Lemma X)**.** *An ordered field F is complete and has the Archimedean property $\iff$ for every nonempty subset $U \subset F$, if U has an upper bound in F, then U has a least upper bound on F.*

Theorem ($\mathbb{R}$ has the Least Upper Bound Property)**.** *For every nonempty subset U of $\mathbb{R}$, if U has an upper bound then U has a least upper bound.*

Corollary 9.6 (41 Existence of Root 2)**.** *The square root of 2 is a real number.*

Theorem (42 Archimedean Property of $\mathbb{R}$)**.** *For all $x, y \in \mathbb{R}$, if $x > 0$, then there exists $n \in \mathbb{N}$ so that $nx > y$.*

Corollary 9.7 (43)**.** *The Archimedean property of $\mathbb{R}$ is equivalent to the following statement:*

$$\forall \varepsilon \in \mathbb{R}, \varepsilon > 0, \exists n \in \mathbb{N} : 0 < \frac{1}{n} < \varepsilon$$

Theorem (Sup and Inf)**.** *The Greatest Lower Bound property is equivalent to the Least Upper Bound property.*

10 Sequences in $\mathbb{R}$

10.1 Definitions

Definition 10.1 (Sequences)**.** Let $\{a_n\}$ be a sequence of real numbers.

1. $\{a_n\}$ converges to $L \in \mathbb{R} \iff$ for all $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exists $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, if $n \geq N$ then $|a_n - L| < \varepsilon$
2. $\{a_n\}$ is Cauchy $\iff$ for all $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exists $N \in \mathbb{N}$ so that for all $m, n \in \mathbb{N}$, if $m, n \geq N$ then $|a_n - a_m| < \varepsilon$
3. $\{a_n\}$ is bounded $\iff$ there exists $M \in \mathbb{R}$ so that for all $n \in \mathbb{N}$ $|a_n| < M$

10.2 Theorems

Lemma 10.2 (33$\mathbb{R}$)**.** *If $\{a_n\} \subset \mathbb{R}$ converges, then $\{a_n\}$ is cauchy.*

Lemma 10.3 (38$\mathbb{R}$)**.** *If a Cauchy sequence $\{a_n\} \subset \mathbb{R}$ has a convergent subsequence $\{a_{n_k}\}$, then $\{a_n\}$ also converges to the same limit.*

Lemma 10.4 (44)**.** *If $\{a_n\} \subset \mathbb{R}$ is a cauchy sequence, then $\{a_n\}$ is bounded.*

Theorem (Bolzano-Weierstrass)**.** *For any sequence $\{a_n\} \subset \mathbb{R}$, if $\{a_n\}$ is bounded, then $\{a_n\}$ has a convergent subsequence.*

Corollary 10.5 (45)**.** *For any sequence $\{a_n\} \subset \mathbb{R}$, $\{a_n\}$ converges $\iff$ $\{a_n\}$ is Cauchy.*

Proposition 10.6 (46 Limit Laws)**.** *Let $\{a_n\}, \{b_n\} \subset \mathbb{R}$ be convergent sequences that converge to $A, B \in \mathbb{R}$ respectively.*

1. $\lim\limits_{n\to\infty} (a_n + b_n) = A + B$
2. $\lim\limits_{n\to\infty} (a_n b_n) = AB$
3. *If $B \neq 0$, then* $\lim\limits_{n\to\infty} \frac{a_n}{b_n} = \frac{A}{B}$

11 Basic Topology

11.1 Definitions

Definition 11.1 (Open Ball)**.** Let $a \in \mathbb{R}$ and let $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$. We define

$$B_\varepsilon(a) := \{x \in \mathbb{R} : |x - a| < \varepsilon\} \tag{11.1}$$

to be the open ball of radius ε centred at a.

Definition 11.2 (Open)**.** A subset $S \subset \mathbb{R}$ is open $\iff$ for all $x \in S$ there exists $\varepsilon \in \mathbb{R}$ so that $\varepsilon > 0$ and $B_\varepsilon(x) \subset S$.

Definition 11.3 (Closed)**.** A subset $S \subset \mathbb{R}$ is closed $\iff$ its complement, S^c, is open. (or if it contains all of its accumulation points)

11.2 Theorems

Theorem (Unions and Intersections)**.** *The arbitrary union of open sets is an open set, and the finite intersection of open sets is an open set. Arbitrary intersections of closed sets are closed and finite unions of closed sets are closed.*

12 Function Limits

12.1 Definitions

Definition 12.1 (Types of Boundedness)**.** A sequence $\{a_n\} \subset \mathbb{R}$ is

1. $\{a_n\}$ is bounded above $\iff$ there exists $U \in \mathbb{R}$ so that for all $n \in \mathbb{N}$ $a_n \leq U$
2. $\{a_n\}$ is bounded below $\iff$ there exists $L \in \mathbb{R}$ so that for all $n \in \mathbb{N}$ $a_n \geq L$

On the other hand $\{a_n\}$ is unbounded $\iff$ for all $M \in \mathbb{R}$ there exists $n \in \mathbb{N}$ so that $a_n > M$ or $a_n < -M$ ($|a_n| > M$)

Definition 12.2 (Diverging to Infinity)**.** Let $\{a_n\} \subset \mathbb{R}$ be a sequence.

1. $\{a_n\}$ diverges to ∞ $\iff$ for all $M \in \mathbb{N}$, there exists $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, if $n \geq N$ then $a_n > M$
2. $\{a_n\}$ diverges to $-\infty$ $\iff$ for all $M \in \mathbb{N}$, there exists $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n \geq N$, then $a_n < -M$

Definition 12.3 (Function Limits)**.** The limit of a function $f : \mathbb{R} \to \mathbb{R}$ as x approaches $a \in \mathbb{R}$ exists and is equal to the real number L $\iff$ for all $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exists $\delta \in \mathbb{R}$, $\delta > 0$ so that for all $x \in \mathbb{R}$, if $|x - a| < \delta$ then $|f(x) - L| < \varepsilon$.

Definition 12.4 (Continuity)**.** The function f is continuous at a $\iff$ for all $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exists $\delta \in \mathbb{R}$, $\delta > 0$ so that for all $x \in \mathbb{R}$, if $|x - a| < \delta$ then $|f(x) - f(a)| < \varepsilon$.

Definition 12.5 (Nested Interval Property)**.** Let $\{I_n\}$ be a sequence of closed intervals, with I_n of length $d_n \in \mathbb{R}$, such that $I_{n+1} \subset I_n$, for all $n \in \mathbb{N}$, and such that the sequence of lengths, $\{d_n\}$, converges to 0. The Nested Interval Property states that given such a sequence,

$$\bigcap_{n=1}^{\infty} I_n = \{x\} \tag{12.1}$$

for some $x \in \mathbb{R}$.

12.2 Theorems

Theorem (Sequence Continuity)**.** *If $f : \mathbb{R} \to \mathbb{R}$ is a function, then f is continuous at a point $a \in \mathbb{R}$ if and only if for all sequences $\{s_n\} \subset \mathbb{R}$, if $\{s_n\}$ converges to a, then $\{f(s_n)\}$ converges to $f(a)$.*

Theorem (Open Sets and Continuity)**.** *The function $f : \mathbb{R} \to \mathbb{R}$ is continuous everywhere $\iff$ for all open sets U of $\mathbb{R}$, the pre-image $f^{-1}(U)$ is open.*

Theorem (Nested Interval and LUB)**.** *The Least Upper Bound property and the Nested Interval property are equivalent.*

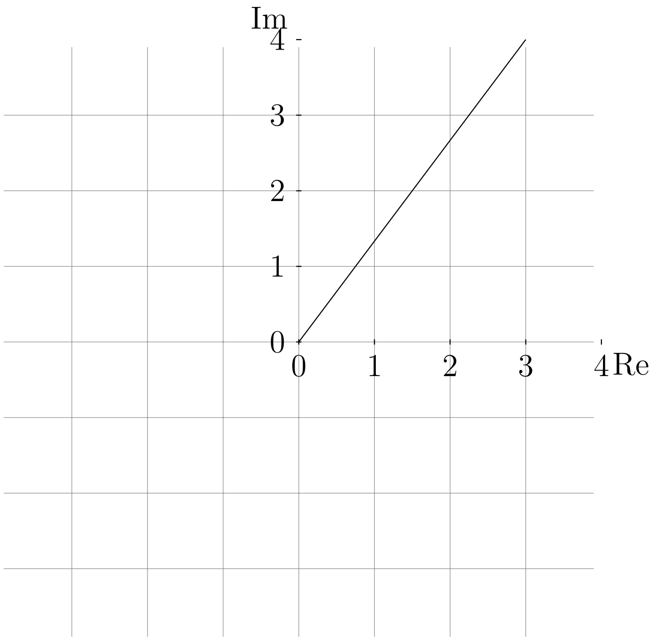
13 Complex Numbers

13.1 Definitions

Definition 13.1 (Complex Set)**.** The set of complex numbers z is defined as

$$\mathbb{C} := \{x + iy : x, y \in \mathbb{R}\}$$

where i is the imaginary unit, that is, $i^2 = -1$.



Definition 13.2 (Modulus)**.** The modulus of $z = x + iy \in \mathbb{C}$ is denoted by $|Z|$ and is equal to $|z| = \sqrt{x^2 + y^2}$.

Definition 13.3 (Polar Form)**.** For all $z \in \mathbb{C}$, there exists $\arg(z) \in \mathbb{R}$ so that $0 \leq \arg(z) < 2\pi$ and

$$z = |z|(\cos(\arg(z)) + i \sin(\arg(z))) = |z|e^{i \arg(z)}$$

13.2 Theorems

Lemma 13.4 (47)**.** *$\mathbb{C}$ is a field under addition and multiplication.*

Lemma 13.5 (48)**.** *For all $z \in \mathbb{C}$, $z\overline{z} \in \mathbb{R}$, $z\overline{z} \geq 0$ an $|z| = \sqrt{z\overline{z}}$*

Lemma 13.6 (49)**.** *Let $z \in \mathbb{C}$*

1. *The additive inverse of z is $-z \in \mathbb{C}$*
2. *If $z \neq 0$, then the multiplicative inverse of z is $\frac{1}{z} = \frac{\overline{z}}{|z|^2} \in \mathbb{C}$*

Lemma 13.7 (50 Triangle Inequality)**.** *For all $z, w \in \mathbb{C}$, $|z + w| \leq |z| + |w|$. Moreover, $|z + w| = |z| + |w| \iff$ there exists $r \in \mathbb{R}$, $r \geq 0$, so that $w = rz$.*

Lemma 13.8 (51)**.** *If $z = r_1 e^{i\theta_1}$ and $w = r_2 e^{i\theta_2}$, then $zw = r_1 r_2 e^{i(\theta_1 + \theta_2)}$.*

14 Fundamental Theorem of Algebra

14.1 Definitions

Definition 14.1 (Polynomial Ring over a Field)**.** Let F be a field. The ring of polynomials with coefficients in F is the set

$$F[x] = \{a_0 + a_1 x + ... + a_n x^n : n \in \mathbb{N}, a_i \in F, \forall 0 \leq i \leq n\}$$

which is the set of polynomials with coefficients in F.

Definition 14.2 (Degree)**.** Let $f(x) \in F[x]$. The degree of f is the largest integer $n \in \mathbb{Z}$ so that $a_n \neq 0$ in the expansion of f:

$$deg(a_0 + a_1 x + ... + a_n x^n) = n$$

Definition 14.3 (Rational Functions)**.** The rational functions with coefficients in F are

$$F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F[x], q(x) \neq 0 \right\}$$

Definition 14.4 (Factors)**.** Let $p(x), q(x), m(x) \in F[x]$. If $p(x) = q(x)m(x)$, then $q(x)$ is a factor of $p(x)$ ($q(x) \neq 0$).

Definition 14.5 (Algebraically Closed)**.** A field F is algebraically closed $\iff$ for all $f \in F[x]$ if $\deg(f) \geq 1$, then f has a root in F.

Definition 14.6 (Gaussian Integers)**.** We define the Gaussian integers as the set

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$$

14.2 Theorems

Theorem (Quotient Remainder Theorem for F[x]**.** *] For any polynomials $p(x), q(x) \in F[x]$ if $\deg(q) \leq \deg(p)$ and $q(x) \neq 0$, then there exist $m(x), r(x) \in F[x]$ so that*

$$\frac{p(x)}{q(x)} = m(x) + \frac{r(x)}{q(x)}$$

and $0 \leq \deg(r) < \deg(p)$

Lemma 14.7 (52)**.** *Let $f(x) \in F[x]$. For all $\alpha \in F$, α is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$.*

Theorem (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is algebraically closed*

Corollary 14.8 (53)**.** *Every nonconstant polynomial $f(x) \in \mathbb{C}[x]$ can be factored completely into a product of linear terms. That is, for all $f(x) \in \mathbb{C}[x]$, if $\deg(f) = n \geq 1$, there exist $k, \alpha_1, ..., \alpha_n \in \mathbb{C}$ so that*

$$f(x) = k(x - \alpha_1)...(x - \alpha_n)$$

Lemma 14.9 (54)**.** *For any $z, w \in \mathbb{Z}[i]$, $-z, \overline{z}, z + w, zw \in \mathbb{Z}[i]$.*