Undergraduate Analysis Tools

October 19, 2012  File:unalan.tex
# Contents

## Part I Numbers

1. **Natural, integer, and rational Numbers**
   - 1.1 Limits in $\mathbb{Q}$
   - 1.2 The Problem with $\mathbb{Q}$
   - 1.3 Peano's arithmetic (Highly Optional)

2. **Fields**
   - 2.1 Basic Properties of Fields
   - 2.2 Ordered Fields

3. **Real Numbers**
   - 3.1 Extended real numbers
   - 3.2 Limsups and Liminfs
   - 3.3 Partitioning the Real Numbers
   - 3.4 The Decimal Representation of a Real Number
   - 3.5 Summary of Key Facts about Real Numbers
   - 3.6 (Optional) Proofs of Theorem 3.6 and Theorem 3.3

4. **Algebraic Properties of Complex Numbers**
   - 4.1 A Matrix Perspective (Optional)

5. **Limits, Continuity, and Compactness in $\mathbb{C}$**
   - 5.1 Closed and open subsets
   - 5.2 Compactness
   - 5.3 Uniform Convergence

6. **Set Operations and Countability**
   - 6.1 Exercises
Part II Appendices

A Appendix: Notation and Logic ............................................................................................................. 43

B Appendix: More Set Theoretic Properties (highly optional) ................................................................. 45
  B.1 Appendix: Zorn’s Lemma and the Hausdorff Maximal Principle (optional) ........................................ 45
  B.2 Cardinality ....................................................................................................................................... 47
  B.3 Formalities of Counting .................................................................................................................. 47

References .................................................................................................................................................. 51
Natural, integer, and rational Numbers

Notation 1.1 Let $\mathbb{N} = \{1, 2, \ldots \}$ denote the natural numbers, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$, 
\[ \mathbb{Z} := \{0, \pm 1, \pm 2, \ldots \} = \{\pm n : n \in \mathbb{N}_0\} \]
be the integers, and 
\[ \mathbb{Q} := \left\{ \frac{m}{n} : m \in \mathbb{Z} \text{ and } n \in \mathbb{N} \right\} \]
be the rationale numbers.

I am going to assume that the reader is familiar with all the standard arithmetic operations (addition, multiplication, inverses, etc.) on $\mathbb{N}_0$, $\mathbb{Z}$, and $\mathbb{Q}$. However let us review the important induction axiom of the natural numbers.

**Induction Axiom** If $S \subseteq \mathbb{N}$ is a subset such that $1 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

This axiom leads takes on two other useful forms which we describe in the next Propositions.

**Proposition 1.2 (Strong form of Induction).** Suppose $S \subseteq \mathbb{N}$ is a subset such that $1 \in S$ and $n + 1 \in S$ whenever $\{1, 2, \ldots, n\} \subset S$, then $S = \mathbb{N}$.

**Proof.** Let $T := \{n \in \mathbb{N} : \{1, 2, \ldots, n\} \subset S\}$. Then $1 \in T$ and if $n \in T$ then $n + 1 \in T$ by assumption. Therefore by the induction axiom, $T = \mathbb{N}$ so that $\{1, 2, \ldots, n\} \subset S$ in for all $n \in \mathbb{N}$. This suffices to show $S = \mathbb{N}$. ■

**Proposition 1.3 (Well ordering principle).** Suppose $S \subseteq \mathbb{N}$ is a non-empty subset, then there exists a smallest element $m$ of $S$.

**Proof.** Let $S$ be a subset of $\mathbb{N}$ for which there is no smallest element, $m \in S$. Let 
\[ T = \{n \in \mathbb{N} : n < s \text{ for all } s \in S\}. \]
If $1 \notin T$, then $1 \in S$ and $1$ would be a smallest element of $S$. Hence we must have $1 \in T$. Now suppose that $n \in T$ so that $n < s$ for all $s \in S$. If $n + 1 \notin T$ then there exists $s \in S$ such that $n < s \leq n + 1$ which would force $s = n + 1 \in S$. But we would then have $n + 1$ is the minimal element of $S$ which is assumed not to exist. So we have shown if $n \in T$ then $n + 1 \in T$. So by the induction axiom of $\mathbb{N}$ it follows that $T = \mathbb{N}$ and therefore $n \notin S$ for all $n \notin \mathbb{N}$, i.e. $S = \emptyset$. ■

Remark 1.4. Let us further observe that the well ordering principle implies the induction axiom. Indeed, suppose that $S \subseteq \mathbb{N}$ is a subset such that $1 \in S$ and $n + 1 \in S$ whenever $n \in S$. For sake of contradiction suppose that $S \neq \mathbb{N}$ so that $T := \mathbb{N} \setminus S$ is not empty. By the well ordering principle there $T$ has a unique minimal element $m$ and in particular $T \subset \{m, m + 1, \ldots \}$. This implies that $\{1, 2, \ldots, m - 1\} \subset S$ and then by assumption that $\{1, 2, \ldots, m\} \subset S$. But this then implies $T \subset \{m + 1, \ldots \}$ and therefore $m \notin T$ which violates $m$ being the minimal element of $T$. We have arrived at the desired contradiction and therefore conclude that $S = \mathbb{N}$.

Remark 1.5. Recall that, for $q \in \mathbb{Q}$, we define \[^1\]
\[ |q| = \begin{cases} q & \text{if } q \geq 0, \\ -q & \text{if } q < 0. \end{cases} \]
Recall that, for all $a, b \in \mathbb{Q}$,
\[ |a + b| \leq |a| + |b|, \quad |ab| = |a| |b|, \quad \text{and} \quad \left| \frac{1}{a} \right| = \frac{1}{|a|} \text{ when } a \neq 0. \]

It is also often useful to keep in mind that the following statements are equivalent for $a, b \in \mathbb{Q}$ with $b \geq 0$;
1. $|a| \leq b$,
2. $-b \leq a \leq b$, and
3. $\pm a \leq b$, i.e. $a \leq b$ and $-a \leq b$.

**Lemma 1.6.** If $a, b \in \mathbb{Q}$, then 
\[ ||b| - |a|| \leq |b - a| \quad (1.1) \]

**Proof.** Since both sides of Eq. (1.1) are symmetric in $a$ and $b$, we may assume that $|b| \geq |a|$ so that $||b| - |a|| = |b| - |a|$. Since 
\[ |b| = |b - a + a| \leq |b - a| + |a|, \]
it follows that 
\[^1\] Absolute values will be discussed in more generality in Section 2.2 below.
The proof of the previous lemma illustrates one of the key techniques of adding 0 to an expression. In this case we added 0 in the form of \(-a + a\) to \(b\). The next remark records a couple of other very important “tricks” in this subject. Taking to heart the following remarks will greatly aid the student in real analysis.

**Remark 1.7 (Some basic philosophies of real analysis).** Let \(a, b, \varepsilon\) be numbers (i.e. in \(\mathbb{Q}\) or later real numbers). We will often prove;

1. \(a \leq b\) by showing that \(a \leq b + \varepsilon\) for all \(\varepsilon > 0\). (See the next theorem.)
2. \(a = b\) by proving \(a \leq b\) and \(b \leq a\) or
3. \(a = b\) by showing \(|b - a| \leq \varepsilon\) for all \(\varepsilon > 0\).

**Theorem 1.8.** The rational \(\mathbb{Q}\) numbers have the following properties;

1. For any \(p \in \mathbb{Q}\) there exists \(N \in \mathbb{N}\) such that \(p < N\).
2. For any \(\varepsilon \in \mathbb{Q}\) with \(\varepsilon > 0\) there exists an \(N \in \mathbb{N}\) such that \(0 < \frac{1}{N} < \varepsilon\).
3. If \(a, b \in \mathbb{Q}\) and \(a \leq b + \varepsilon\) for all \(\varepsilon > 0\), then \(a \leq b\).

**Proof.**
1. If \(p \leq 0\) we may take \(N = 1\). So suppose that \(p = \frac{m}{n}\) with \(m, n \in \mathbb{N}\). In this case let \(N = m\).
2. Write \(\varepsilon = \frac{m}{n}\) with \(m, n \in \mathbb{N}\) and then take \(N = 2n\).
3. If \(a \leq b\) is false happens iff \(a > b\) which is equivalent to \(a - b > 0\). If we now let \(\varepsilon := \frac{a - b}{2} > 0\), then
   
   \[a = b + (b - a) > b + \varepsilon\]

which would violate the assumption that \(a \leq b + \varepsilon\) for all \(\varepsilon > 0\). \(\square\)

### 1.1 Limits in \(\mathbb{Q}\)

In this course we will often use the abbreviations, **i.o.** and **a.a.** which stand for **infinitely often** and **almost always** respectively. For example \(a_n \leq b_n\) a.a. \(n\) means there exists an \(N \in \mathbb{N}\) such that \(a_n \leq b_n\) for all \(n \geq N\) while \(a_n \leq b_n\) i.o. \(n\) means for all \(N \in \mathbb{N}\) there exists a \(n \geq N\) such that \(a_n \leq b_n\). So for example, \(1/n \leq 1/100\) for a.a. \(n\) while and \((-1)^n \geq 0\) i.o. By the way, it should be clear that if something happens for a.a. \(n\) then it also happens i.o. \(n\).

\(^2\) We will see that the real numbers have these same properties as well.

**Definition 1.9.** A sequence \(\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}\) **converges to** 0 \(\in \mathbb{Q}\) if for all \(\varepsilon > 0\) in \(\mathbb{Q}\) there exists \(N \in \mathbb{N}\) such that \(|a_n| \leq \varepsilon\) for all \(n \geq N\). Alternatively, put, for all \(\varepsilon > 0\) we have \(|a_n| \leq \varepsilon\) for a.a. \(n\). This may also be stated as for all \(M \in \mathbb{N}\), \(|a_n| \leq \frac{1}{M}\) for a.a. \(n\).

**Definition 1.10.** A sequence \(\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}\) converges to \(a \in \mathbb{Q}\) if \(|a - a_n| \to 0\) as \(n \to \infty\), i.e. if for all \(N \in \mathbb{N}\), \(|a - a_n| \leq \frac{1}{N}\) for a.a. \(n\). As usual if \(\{a_n\}_{n=1}^{\infty}\) converges to \(a\) we will write \(a_n \to a\) as \(n \to \infty\) or \(a = \lim_{n \to \infty} a_n\).

**Proposition 1.11.** If \(\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}\) converges to \(a \in \mathbb{Q}\), then \(\lim_{n \to \infty} |a_n| = |a|\).

**Proof.** From **Lemma 1.6** we have,

\[||a| - |a_n|| \leq |a - a_n|\]

Thus if \(\varepsilon > 0\) is given, by definition of \(a_n \to a\) there exists \(N \in \mathbb{N}\) such that \(|a - a_n| < \varepsilon\) for all \(n \geq N\). From the previously displayed equation, it follows that \(|a - |a_n|| < \varepsilon\) for all \(n \geq N\) and hence we may conclude that \(\lim_{n \to \infty} |a_n|\) exists and is equal to \(|a|\). \(\square\)

**Lemma 1.12 (Convergent sequences are bounded).** If \(\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}\) converges to \(a \in \mathbb{Q}\), then there exists \(M \in \mathbb{Q}\) such that \(|a_n| \leq M\) for all \(n \in \mathbb{N}\).

**Proof.** Taking \(\varepsilon = 1\) in the definition of \(a = \lim_{n \to \infty} a_n\) implies there exists \(N \in \mathbb{N}\) such that \(|a_n - a| \leq 1\) for all \(n \geq N\). Therefore,

\[|a_n| = |a_n - a + a| \leq |a_n - a| + |a| \leq 1 + |a|\]

for \(n \geq N\).

We may now take \(M := \max\left(\left\{|a_n|_{n=1}^{N}\right\} \cup \{1 + |a|\}\right)\).

**Theorem 1.13.** If \(\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}\) converges to \(a \in \mathbb{Q} \setminus \{0\}\), then

\[\lim_{n \to \infty} \frac{1}{a_n} = \frac{1}{a}\] \hspace{1cm} (1.2)

It is possible that \(a_n = 0\) for small \(n\) so that \(\frac{1}{a_n}\) is not defined but for large \(n\) this cannot happen and therefore it makes sense to talk about the limit which only depends on the tail of the sequences.

**Proof.** Since \(a \neq 0\) we know that \(|a| > 0\). Hence, there exists \(M := M|a| \in \mathbb{N}\) such that \(|a_n - a| < \frac{|a|}{2}\) for all \(n \geq M\). Therefore for \(n \geq M\)

\[|a| = |a - a_n + a_n| \leq |a - a_n| + |a_n| < \frac{|a|}{2} + |a_n|\]
from which it follows that $|a_n| > \frac{|a|}{2}$ for all $n \geq M$. If $\varepsilon > 0$ is given arbitrarily, we may choose $N \geq M$ such that $|a - a_n| < \varepsilon$ for all $n \geq M$. Then for $n \geq N$ we have,

$$\frac{1}{a_n} - \frac{1}{a} = \frac{1}{a + \delta_n} \frac{1}{a} = \frac{|a - a_n|}{|a|} < \frac{\varepsilon}{2|a|}. \quad (1.2)$$

As $\varepsilon > 0$ is arbitrary it follows that $\frac{2\varepsilon}{|a|} > 0$ is arbitrarily small as well (replace $\varepsilon$ by $\varepsilon |a|^2 / 2$ if you feel it is necessary), and hence we may conclude that Eq. (1.2) holds.

**Variation on the method.** In order to make these arguments more routine, it is often a good idea to write $a_n = a + \delta_n$ where $\delta_n := a_n - a$ is the error between $a_n$ and $a$. By assumption, $\lim_{n \to \infty} \delta_n = 0$ and so for any $\delta > 0$ given there exists $N(\delta) \in \mathbb{N}$ such that $|\delta_n| \leq \delta$. With this notation we have,

$$\frac{1}{a_n} - \frac{1}{a} = \frac{1}{a + \delta_n} - \frac{1}{a} = \frac{\delta_n}{a + \delta_n} \frac{1}{a} \leq \frac{\delta}{|a|(|a| - \delta)}. \quad (1.3)$$

So if we assume that $\delta \leq |a| / 2$ we find that

$$\frac{1}{a_n} - \frac{1}{a} \leq \frac{2\delta}{|a|^2} \text{ for all } n \geq N(\delta). \quad (1.3)$$

Taking $\delta = \delta(\varepsilon) = \min\{|a| / 2, |a|^2 \varepsilon / 2\}$ in Eq. (1.3) shows for $n \geq N(\delta(\varepsilon))$ that $\frac{1}{a_n} - \frac{1}{a} \leq \varepsilon$. Since $\varepsilon > 0$ is arbitrary we may conclude that $\lim_{n \to \infty} \frac{1}{a_n} = \frac{1}{a}$. \hfill \blacksquare

• End of Lecture 1, 9/28/2012

**Definition 1.14.** A sequence $\{a_n\}_{n=1}^\infty \subset \mathbb{Q}$ is **Cauchy** if $|a_n - a_m| \to 0$ as $m,n \to \infty$. More precisely we require for each $\varepsilon > 0$ in $\mathbb{Q}$ that $|a_m - a_n| \leq \varepsilon$ for a.a. pairs $(m,n)$, i.e. there should exists $N \in \mathbb{N}$ such that $|a_m - a_n| \leq \varepsilon$ for all $m,n \geq N$.

**Exercise 1.1.** Show that all convergent sequences $\{a_n\}_{n=1}^\infty \subset \mathbb{Q}$ are Cauchy.

**Exercise 1.2.** Show all Cauchy sequences $\{a_n\}_{n=1}^\infty \subset \mathbb{Q}$ are Cauchy. Then $\lim_{n \to \infty} x_n = a$ implies $x_n = a_n$ for all $n \geq N$.

**Exercise 1.3.** Suppose $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are Cauchy sequences in $\mathbb{Q}$. Show $\{a_n + b_n\}_{n=1}^\infty$ and $\{a_n \cdot b_n\}_{n=1}^\infty$ are Cauchy.

**Exercise 1.4.** Assume that $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are convergent sequences in $\mathbb{Q}$. Show $\{a_n + b_n\}_{n=1}^\infty$ and $\{a_n \cdot b_n\}_{n=1}^\infty$ are convergent in $\mathbb{Q}$ and

$$\lim_{n \to \infty} (a_n + b_n) = \lim_{n \to \infty} a_n + \lim_{n \to \infty} b_n$$

and

$$\lim_{n \to \infty} (a_n b_n) = \lim_{n \to \infty} a_n \cdot \lim_{n \to \infty} b_n.$$

**Exercise 1.5.** Assume that $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are convergent sequences in $\mathbb{Q}$ such that $a_n \leq b_n$ for all $n$. Show $A := \lim_{n \to \infty} a_n \leq \lim_{n \to \infty} b_n =: B$.

**Exercise 1.6 (Sandwich Theorem).** Assume that $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are convergent sequences in $\mathbb{Q}$ such that $\lim_{n \to \infty} a_n = \lim_{n \to \infty} b_n$. If $\{x_n\}_{n=1}^\infty$ is another sequence in $\mathbb{Q}$ which satisfies $a_n \leq x_n \leq b_n$ for all $n$, then

$$\lim_{n \to \infty} x_n = a := \lim_{n \to \infty} a_n = \lim_{n \to \infty} b_n.$$  

Please note that that main part of the problem is to show that $\lim_{n \to \infty} x_n$ exists in $\mathbb{Q}$. **Hint:** start by showing: if $a \leq x \leq b$ then $|x| \leq \max\{|a|, |b|\}$.

**Definition 1.15 (Subsequence).** We say a sequence, $\{y_k\}_{k=1}^\infty$, is a **subsequence** of another sequence, $\{x_n\}_{n=1}^\infty$, provided there exists a strictly increasing function, $N \ni k \to n_k \in \mathbb{N}$ such that $y_k = x_{n_k}$ for all $k \in \mathbb{N}$. Example, $n_k = k^2 + 3$, and $\{y_k := x_{k^2 + 3}\}_{k=1}^\infty$ would be a subsequence of $\{x_n\}_{n=1}^\infty$.

**Exercise 1.7.** Suppose that $\{x_n\}_{n=1}^\infty$ is a Cauchy sequence in $\mathbb{Q}$ (or $\mathbb{R}$) which has a convergent subsequence, $\{y_k = x_{n_k}\}_{k=1}^\infty$ in $\mathbb{Q}$ (or $\mathbb{R}$). Show that $\lim_{n \to \infty} x_n$ exists and is equal to $\lim_{k \to \infty} y_k$.

### 1.2 The Problem with $\mathbb{Q}$

The problem with $\mathbb{Q}$ is that it is full of “holes.” To be more precise, $\mathbb{Q}$ is not “complete,” i.e. not all Cauchy sequences are convergent. In fact, according to Corollary ?? below, “most” Cauchy sequences of rational numbers do not converge to a rational number. Let us demonstrate some examples pointing out this flaw. We first pause to recall how to sum geometric series.

**Lemma 1.16 (Geometric Series).** Let $\alpha \in \mathbb{Q}$, $m,n \in \mathbb{Z}$ with $n \leq m$, and $S := \sum_{k=n}^m \alpha^k$. Then

$$S = \begin{cases} m - n + 1 & \text{if } \alpha = 1 \\ \frac{a^{m+1} - a^n}{\alpha - 1} & \text{if } \alpha \neq 1. \end{cases}$$
Moreover if \( 0 \leq \alpha < 1 \), then
\[
\sum_{k=n}^{m} \alpha^k = \alpha^n \frac{1 - \alpha^{m-n+1}}{1 - \alpha} \leq \frac{\alpha^n}{1 - \alpha}. \tag{1.4}
\]

**Proof.** When \( \alpha = 1 \),
\[
S = \sum_{k=n}^{m} 1^k = m - n + 1.
\]
If \( \alpha \neq 1 \), then
\[
\alpha S - S = \alpha^{m+1} - \alpha^n.
\]
Solving for \( S \) gives
\[
S = \sum_{k=n}^{m} \alpha^k = \frac{\alpha^{m+1} - \alpha^n}{\alpha - 1} \quad \text{if} \quad \alpha \neq 1. \tag{1.5}
\]

**Example 1.17.** Let \( S_n := \sum_{k=0}^{n} \frac{1}{k!} \in \mathbb{Q} \) for all \( n \in \mathbb{N} \). For \( n > m \) in \( \mathbb{N} \) we have,
\[
0 \leq S_n - S_m = \sum_{k=m+1}^{n} \frac{1}{k!} = \sum_{j=1}^{n-m} \frac{1}{(m+j)!}
= \frac{1}{(m+1)!} + \cdots + \frac{1}{m!}
\leq \frac{1}{m!} \left[ \frac{1}{m+1} + \left( \frac{1}{m+1} \right)^2 + \cdots + \left( \frac{1}{m+1} \right)^{n-m} \right]
\leq \frac{1}{m! m + 1} \cdot \frac{1}{\frac{1}{m+1}} = \frac{1}{m \cdot m!}. \tag{1.6}
\]

wherein we have used Eq. (1.4) for the last inequality. From this inequality it follows that \( \{S_n\}_{n=0}^{\infty} \) is a Cauchy sequence and we also have,
\[
\frac{1}{(m+1)!} \leq S_n - S_m \leq \frac{1}{m \cdot m!} \quad \text{for all} \quad n > m. \tag{1.7}
\]

Suppose that \( e := \lim_{n \to \infty} S_n \) were to exist in \( \mathbb{Q} \). Then letting \( n \to \infty \) in Eq. (1.7) would show,
\[
0 < \frac{1}{(m+1)!} \leq e - S_m \leq \frac{1}{m \cdot m!}.
\]
Multiplying this inequality by \( m! \) then implies,
\[
0 < m! e - m! S_m \leq \frac{1}{m}.
\]

However for \( m \) sufficiently large \( m! e \in \mathbb{N} \) (as \( e \) is assumed to be rational) and \( m! S_m \) is always in \( \mathbb{N} \) and therefore \( k := m! e - m! S_m \in \mathbb{N} \). But there is no element \( k \in \mathbb{N} \) such that \( 0 < k < \frac{1}{m} \) and hence we must conclude \( \lim_{n \to \infty} S_n \) can not exist in \( \mathbb{Q} \). **Moral:** the number \( e = \sum_{n=0}^{\infty} \frac{1}{m!} = \lim_{n \to \infty} (1 + \frac{1}{m})^n \) that you learned about in calculus is not in \( \mathbb{Q} \).

![Graph of partial sums](image)

**Example 1.18 (Square roots need not exist).** The square root, \( \sqrt{2} \), of 2 does not exist in \( \mathbb{Q} \). Indeed, if \( \sqrt{2} = \frac{m}{n} \) where \( m \) and \( n \) have no common factors (in particular no common factors of 2) so that either \( m \) or \( n \) is odd), then
\[
\frac{m^2}{n^2} = 2 \implies m^2 = 2n^2.
\]
This shows that \( m^2 \) is even which would then imply that \( m = 2k \) is even (since odd-odd=odd). However this implies \( 4k^2 = 2n^2 \) from which it follows that \( n^2 = 2k^2 \) is even and hence \( n \) is even. But this contradicts the assumption that \( m \) and \( n \) had no common factors (of 2).

**Exercise 1.8.** Use the following outline to construct another Cauchy sequence \( \{q_n\}_{n=1}^{\infty} \subset \mathbb{Q} \) which is not convergent in \( \mathbb{Q} \).

1. Recall that there is no element \( q \in \mathbb{Q} \) such that \( q^2 = 2 \). To each \( n \in \mathbb{N} \) let \( m_n \in \mathbb{N} \) be chosen so that...
and let \( q_n := \frac{m_n}{n^2} \).

2. Verify that \( q_n^2 \to 2 \) as \( n \to \infty \) and that \( \{q_n\}^\infty_{n=1} \) is a Cauchy sequence in \( \mathbb{Q} \).

3. Show \( \{q_n\}^\infty_{n=1} \) does not have a limit in \( \mathbb{Q} \).

\[ \frac{m_n^2}{n^2} < 2 < \left(\frac{m_n + 1}{n}\right)^2 \quad (1.8) \]

Example 1.19. It is also a fact that \( \pi \notin \mathbb{Q} \) where

\[
\pi = 2 \int_0^\infty \frac{1}{1 + x^2} \, dx = 2 \lim_{N \to \infty} \int_0^N \frac{1}{1 + x^2} \, dx
= 2 \lim_{N \to \infty} \sum_{k=1}^{N^2} \frac{1}{1 + \left(\frac{k}{N}\right)^2} \cdot \frac{1}{N}
= \lim_{N \to \infty} \sum_{k=1}^{N^2} \frac{2N}{N^2 + k^2}.
\]

The point is that the basic operations from calculus tend to produce “real numbers” which are not rational even though we start with only rational numbers.

- End of Lecture 2, 10/1/2012

1.3 Peano’s arithmetic (Highly Optional)

This section is for those who want to understand \( \mathbb{N} \) at a more fundamental level. Here we start with Peano’s rather minimalist axioms for \( \mathbb{N} \) and show how they lead to all the standard properties you are used to using for \( \mathbb{N} \). Here are the axioms:

non-empty \( \mathbb{N}_0 \) is a non-empty set which contains a distinguished element, 0.

We let \( \mathbb{N} := \mathbb{N}_0 \setminus \{0\} \) and call these the natural numbers.

Successor Function There is an injective\(^4\) function, \( s : \mathbb{N}_0 \to \mathbb{N} \) and we let

\( 1 := s(0) \in \mathbb{N} \).

Induction hypothesis If \( S \subset \mathbb{N}_0 \) is a set such that \( 0 \in S \) and \( s(n) \in S \) whenever \( n \in S \), then \( S = \mathbb{N}_0 \).

Assuming these axioms one may develop all of the properties or \( \mathbb{N}_0 \) that you are accustomed to seeing. I will develop the basic properties of addition, multiplication, and the ordering on \( \mathbb{N}_0 \) in this section. For more on this point

and then the further construction of \( \mathbb{Z} \) and \( \mathbb{Q} \) from \( \mathbb{N}_0 \), the reader is referred to the notes; \[ “Numbers” by M. Taylor \] You may also consult E. Landau’s book \[ ] for a very detailed (but perhaps too long winded) exposition of these topics.

Lemma 1.20. The map \( s : \mathbb{N}_0 \to \mathbb{N} \) is a bijection.

**Proof.** Let \( S := s(\mathbb{N}_0) \cup \{0\} \subset \mathbb{N}_0 \). Then \( 0 \in S \) and \( s(0) \in s(\mathbb{N}_0) \subset S \). Moreover if \( n \in \mathbb{N} \cap \mathbb{N} \) then \( s(n) \in s(\mathbb{N}_0) \subset S \) so that \( x \in S \implies s(x) \in S \) and hence \( S = \mathbb{N}_0 \) and therefore \( s(\mathbb{N}_0) = \mathbb{N} \).

Theorem 1.21 (Addition). There exists a function \( p : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \) such that \( p(x,0) = x \) for all \( x \in \mathbb{N}_0 \) and \( p(x,s(y)) = s(p(x,y)) \) for all \( x,y \in \mathbb{N}_0 \). Moreover, we may construct \( p \) so that \( p(s(x),y) = p(x,s(y)) \) for all \( x,y \in \mathbb{N}_0 \).

This function \( p \) satisfies the following properties;

1. \( p(x,0) = x = p(0,x) \) for all \( x \in \mathbb{N}_0 \),
2. \( p(x,1) = p(1,x) = s(x) \) for all \( x \in \mathbb{N}_0 \),
3. \( p(x,y) = p(y,x) \) for all \( x,y \in \mathbb{N}_0 \),
4. \( p(x,p(y,z)) = p(p(x,y),z) \) for all \( x,y,z \in \mathbb{N}_0 \).

**Proof.** We will construct \( p \) inductively. Let

\( S := \{x \in \mathbb{N} : \exists p_x : \mathbb{N}_0 \to \mathbb{N}_0 \ni p_x(0) = x \text{ and } p_x(s(y)) = s(p_x(y)) \forall y \in \mathbb{N}_0\} \).

Taking \( p_0(y) = y \) shows \( 0 \in S \). Moreover if \( x \in S \) we define

\( p_{s(x)}(y) := s(p_x(y)) \) for all \( y \in \mathbb{N}_0 \).

We then have \( p_{s(x)}(0) = s(p_x(0)) = s(x) \) and

\( p_{s(x)}(s(y)) := s(p_x(s(y))) = s \circ s(p_x(y)) = s(p_{s(x)}(y)) \)

which shows \( s(x) \in S \). Thus we may conclude \( S = \mathbb{N}_0 \) and we may now define \( p(x,y) := p_x(y) \) for all \( x,y \in \mathbb{N}_0 \). By construction this function satisfies,

\( p(s(x),y) = s(p(x,y)) = p(x,s(y)) \).

We now verify the properties in items 1. – 4.

1. By construction \( p(x,0) = x \) for all \( x \in \mathbb{N}_0 \). Let \( S := \{x \in \mathbb{N} : p(0,x) = x\} \), then \( 0 \in S \) and if \( x \in S \) we have \( p(0,s(x)) = s(p(0,x)) = s(x) \) so that \( s(x) \in S \). Therefore \( S = \mathbb{N}_0 \) and the first item holds.
2. \( p(x,1) = p(x,s(0)) = s(p(x,0)) = s(x) \) and \( p(1,x) = p(s(0),x) = s(p(0,x)) = s(x) \) so that item 2. is proved.
3. Let $S = \{ x \in \mathbb{N}_0 : p(x, \cdot) = p(\cdot, x) \}$. Then by items 1 and 2, it follows that $0, 1 \in S$. Moreover if $x \in S$, then for all $y \in \mathbb{N}_0$ we find,

$$p(s(x), y) = s(p(x, y)) = s(p(y, x)) = p(y, s(x))$$

which shows $s(x) \in S$. Therefore $S = \mathbb{N}_0$ and item 3 is proved.

4. Let $S := \{ x \in \mathbb{N}_0 : p(x, p(y, z)) = p(p(x, y), z) \ \forall y, z \in \mathbb{N}_0 \}$. Then $0 \in S$ and if $x \in S$ we find,

$$p(s(x), p(y, z)) = s(p(x, p(y, z))) = s(p(p(x, y), z)) = p(s(p(x, y), z), z) = p(s(x), y, z)$$

which shows that $s(x) \in S$ and therefore $S = \mathbb{N}_0$ and item 4 is proved.

**Notation 1.22** We now write $x + y$ for $p(x, y)$ and refer to the symmetric binary operator, $+$, as addition.

To summarize we have now shown addition satisfies for all $x, y, z \in \mathbb{N}_0$:

1. $x + 0 = x + x = x$,
2. $s(x) = x + 1 = 1 + x$,
3. $x + y = y + x$,
4. $(x + y) + z = x + (y + z)$,
5. The induction hypothesis may now be written as; if $S \subseteq \mathbb{N}_0$ is a subset such that $0 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $S = \mathbb{N}_0$.

**Proposition 1.23 (Additive Cancellation).** If $x, y, z \in \mathbb{N}_0$ and $x + z = y + z$, then $x = y$.

**Proof.** Let $S$ be those $z \in \mathbb{N}_0$ for which the statement $x + z = y + z$ implies $x = y$ holds. It is clear that $0 \in S$. Moreover if $z \in S$ and $x + (z + 1) = y + (z + 1)$ then $(x + 1) + z = (y + 1) + z$ and so by the inductive hypothesis $s(x) = x + 1 = y + 1 = s(y)$. Recall that $s$ is one to one by assumption and therefore we may conclude $x = y$ and we have shown $s(z) \in S$. Therefore $S = \mathbb{N}_0$ and the proposition is proved.

**Definition 1.24.** Given $x, y \in \mathbb{N}_0$, we say $x < y$ iff $y = x + n$ for some $n \in \mathbb{N}$ and $x \leq y$ iff $y = x + n$ for some $n \in \mathbb{N}_0$. We further let

$$R_x := \{ x + n : n \in \mathbb{N}_0 \}$$

so that $y \geq x$ iff $y \in R_x$.

**Proposition 1.25.** If $x, y \in \mathbb{N}_0$ and $x \leq y$ and $y \leq x$ then $x = y$. Moreover if $x \leq y$ then either $x < y$ or $x = y$.

**Proof.** By assumption there exists $m, n \in \mathbb{N}_0$ such that $y = x + m$ and $x = y + n$ and therefore $y = y + (m + n)$. Hence by cancellation it follows that $m + n = 0$. If $n \neq 0$ then $n = s(x)$ for some $x \in \mathbb{N}_0$ and we have $m + n = m + s(x) = x + 1 \in \mathbb{N}$ which would imply $m + n \neq 0$. Thus we conclude that $m = 0 = n$ and therefore $x = y$.

If $x < y$ and $y \neq x$ then $y = x + n$ for some $n \in \mathbb{N}_0$ with $n \neq 0$, i.e. $x < y$.

**Proposition 1.26.** If $x, y \in \mathbb{N}_0$ then precisely one of the following three choices must hold, 1) $x < y$, 2) $x = y$, 3) $y < x$.

**Proof.** Suppose that $x \leq y$ does not hold, i.e. $y \notin R_x$. We wish to show that $y < x$, i.e. that $x = y + n$ for some $n \in \mathbb{N}$. We do this by induction on $y$. That is let $S$ be the the set of $y \in \mathbb{N}_0$ such that the statement $y \notin R_x$ implies $y < x$ holds. If $y = 0 \notin R_x$ implies $n := x \neq 0$ so that $x = y + n$, i.e. $y < x$. This shows $0 \in S$. Now suppose that $y \in S$ and that $y + 1 \notin R_x = \{ x + m : m \in \mathbb{N}_0 \}$. It follows that $y + 1 \neq x + m + 1$ for all $m \in \mathbb{N}_0$ and hence that $y \neq x + m$ for all $m \in \mathbb{N}_0$, i.e. $y \notin R_x$. So by induction $y < x$ and therefore $x = y + k$ for some $k \in \mathbb{N}$. Since $k \in \mathbb{N}$ we know there exists $k' \in \mathbb{N}_0$ such that $k = k'$ and it follows that $x = y + 1 + k'$, i.e. $y + 1 \leq x$. Since $y + 1 \notin R_x$ we may conclude that in fact $y + 1 < x$ and therefore $y + 1 \in S$. So by induction $S = \mathbb{N}_0$ and we have shown if $x < y$ does not hold iff $y \leq x$. Combining this statement with the Proposition 1.25 completes the proof.

We have now set up a satisfactory addition operations and ordering on $\mathbb{N}_0$. Our next goal is to define multiplication on $\mathbb{N}_0$.

**Theorem 1.27.** There exists a function $M : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ such that $M(x, 0) = 0$ for all $x \in \mathbb{N}_0$ and $M(x, y + 1) = M(x, y) + x$ for all $x, y \in \mathbb{N}_0$. This function $M$ satisfies the following properties:

1. $M(x, 0) = 0 = M(0, x)$ for all $x \in \mathbb{N}_0$,
2. $M(x, 1) = M(1, x) = x$ for all $x \in \mathbb{N}_0$,
3. $M(x, y) = M(x, y)$ for all $x, y \in \mathbb{N}_0$,
4. $M(x, y + z) = M(x, y) + M(x, z)$ for all $x, y, z \in \mathbb{N}_0$,
5. $M(x, M(y, z)) = M(M(x, y), z)$ for all $x, y, z \in \mathbb{N}_0$.

**Proof.** Let $S$ denote those $x \in \mathbb{N}_0$ such that there exists a function $M_x : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying $M_x(0) = 0$ and $M_x(y + 1) = M_x(y) + x$ for all $y \in \mathbb{N}_0$. Taking $M_0(y) := 0$ shows $0 \in S$. Moreover if $x \in S$ we define $M_{x + 1}(y) := M_x(y) + y$. Then $M_{x + 1}(0) = 0$ and

$$M_{x + 1}(y + 1) = M_x(y + 1) + y + 1 = M_x(y) + x + y + 1$$
while

\[ M_{x+1}(y) + (x + 1) = M_x(y) + y + x + 1 = M_{x+1}(y + 1). \]

This shows that \( x + 1 \in S \) and so by induction \( S = \mathbb{N}_0 \) and we may now define

\[ M(x, y) := M_x(y) \]

for all \( x, y \in \mathbb{N}_0 \). We now prove the properties of \( M \) stated above.

1. By construction \( M(x, 0) = 0 \) for all \( x \). Let \( S := \{ x \in \mathbb{N}_0 : M(0, x) = 0 \} \).
   Then \( 0 \in S \) and if \( x \in S \) we have
   \[ M(0, x + 1) = M(0, x) + 0 = 0 + 0 = 0 \]
   which shows \( x + 1 \in S \). Therefore by induction \( S = \mathbb{N}_0 \) and \( M(0, x) = 0 \)
   for all \( x \in \mathbb{N}_0 \).

2. \( M(x, 1) = M(x, 0 + 1) = M(x, 0) + x = 0 + x = x \) for all \( x \in \mathbb{N}_0 \). Let
   \( S := \{ x \in \mathbb{N}_0 : M(1, x) = x \} \). Then \( 0 \in S \) and if \( x \in S \) we have
   \[ M(1, x + 1) = M(1, x) + 1 = x + 1 \]
   which shows \( x + 1 \in S \). Therefore \( S = \mathbb{N}_0 \) and \( M(1, x) = x \) for all \( x \in \mathbb{N}_0 \).

3. Let \( S := \{ x \in \mathbb{N}_0 : M(x, \cdot) = M(\cdot, x) \} \). Then by items 1. and 2. we know that \( 0, 1 \in S \). Now suppose that \( x \in S \), then by construction,
   \[ M(x + 1, y) = M_{x+1}(y) = M(x, y) + y \]
   while
   \[ M(y, x + 1) = M(y, x) + y. \]
   The last two displayed equations along with the induction hypothesis shows \( x + 1 \in S \) and therefore \( S = \mathbb{N}_0 \) and item 3. is proved.

4. Let \( S \) denotes those \( x \in S \) such that \( M(x, y + z) = M(x, y) + M(x, z) \) for all \( y, z \in \mathbb{N}_0 \). Then \( 0, 1 \in S \) and if \( x \in S \) we have
   \[ M(x + 1, y + z) = M(x, y + z) + y + z \]
   \[ = M(x, y) + M(x, z) + y + z \]
   \[ = M(x, y) + y + M(x, z) + z \]
   \[ = M(x + 1, y) + M(x, z) \]
   which shows \( x + 1 \in S \). Therefore \( S = \mathbb{N}_0 \) and we have proved item 4.

5. Let
   \[ S := \{ x \in \mathbb{N}_0 : M(x, M(y, z)) = M(M(x, y), z) \ \forall y, z \in \mathbb{N}_0 \}. \]
   Then \( 0 \in S \) and if \( x \in S \) we find,
   \[ M(x + 1, M(y, z)) = M(x, M(y, z)) + M(y, z) \]
   while
   \[ M(M(x + 1, y), z) = M(M(x, y) + y, z) = M(M(x, y), z) + M(y, z). \]
   The last two equations along with the induction hypothesis shows \( x + 1 \in S \) and therefore \( S = \mathbb{N}_0 \) and item 5. is proved.

\[ \square \]

**Notation 1.28** We now write \( x \cdot y \) for \( M(x, y) \) and refer to the symmetric binary operator, \( \cdot \), as multiplication.

To summarize Theorem 1.27 we have shown multiplication satisfies for all \( x, y, z \in \mathbb{N}_0 \);
1. \( x \cdot 0 = 0 = 0 \cdot x \),
2. \( x \cdot 1 = x = 1 \cdot x \),
3. \( x \cdot y = y \cdot x \),
4. \( x \cdot (y + z) = x \cdot y + x \cdot z \),
5. \( (x \cdot y) \cdot z = x \cdot (y \cdot z) \).

**Proposition 1.29** (Multiplicative Cancellation). If \( x, y \in \mathbb{N}_0 \) and \( z \in \mathbb{N} \) such that \( x \cdot z = y \cdot z \), then \( x = y \).

**Proof.** If \( x \neq y \), say \( x < y \), then \( y = x + n \) for some \( n \in \mathbb{N} \) and therefore \( y \cdot z = (x + n) \cdot z = x \cdot z + n \cdot z \).

Hence if \( x \cdot z = y \cdot z \), then by additive cancellation we must have \( n \cdot z = 0 \). As \( n, x \in \mathbb{N} \) we may write \( n = n' + 1 \) and \( z = z' + 1 \) with \( n', z' \in \mathbb{N}_0 \) and therefore,
\[ 0 = n \cdot z = (n' + 1) \cdot (z' + 1) = n' \cdot z' + n' + z' + 1 \neq 0 \]
which is a contradiction.

\[ \square \]

**Remark 1.30** (Base 10 counting). The typical method of counting is to use base 10 enumeration of \( \mathbb{N}_0 \). The rules are;
\[ 0 = 0, \ 1 = 1, \ 2 := 1 + 1, \ 3 := 2 + 1, \ 4 := 3 + 1, \ 5 := 4 + 1 \]
\[ 6 := 5 + 1, \ 7 := 6 + 1, \ 8 := 7 + 1, \ 9 := 8 + 1, \ \text{and} \ 10 := 9 + 1. \]

Once these element of \( \mathbb{N}_0 \) have been defined, then given \( a_0, \ldots, a_n \in \{0, 1, \ldots, 9\} \) with \( a_n \neq 0 \), we let
\[ a_n a_{n-1} \ldots a_0 := \sum_{k=0}^{n} a_k 10^k. \]

For example, \( 35 = 3 \cdot 10 + 5 = 34 + 1 \), etc.

As mentioned above one can formalize \( \mathbb{Z} \) and \( \mathbb{Q} \) using \( \mathbb{N}_0 \) constructed above. I will omit the details here and refer the reader to the references already mentioned.
Fields

The basic question we want to eventually address is: What are the real numbers? Our answer is going to be: the real numbers is the essentially unique complete ordered field, see Theorem 3.3 below. In order to make sense of this answer we need to explain the terms, “complete,” “ordered,” and “field.” We will start with the notion of a field which loosely stated means something that can reasonably be interpreted a “numbers.”

Definition 2.1 (Fields, i.e.” numbers”). A field is a non-empty set \( F \) equipped with two operations called addition and multiplication, and denoted by \(+\) and \(\cdot\), respectively, such that the following axioms hold; (subtraction and division are defined implicitly in terms of the inverse operations of addition and multiplication):

1. **Closure of \( F \) under addition and multiplication.** For all \( a, b \in F \), both \( a + b \) and \( a \cdot b \) are in \( F \) (or more formally, \(+\) and \(\cdot\) are binary operations on \( F \)).

2. **Associativity of addition and multiplication.** For all \( a, b, \) and \( c \) in \( F \), the following equalities hold: \( a + (b + c) = (a + b) + c \) and \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \).

3. **Commutativity of addition and multiplication.** For all \( a \) and \( b \) in \( F \), the following equalities hold: \( a + b = b + a \) and \( a \cdot b = b \cdot a \).

4. **Additive and multiplicative identity.** There exists an element of \( F \), called the additive identity element and denoted by \( 0 = 0_F \), such that for all \( a \in F \), \( a + 0 = a \). Likewise, there is an element, called the multiplicative identity element and denoted by \( 1 = 1_F \), such that for all \( a \in F \), \( a \cdot 1 = a \). It is assumed that \( 0_F \neq 1_F \).

5. **Additive and multiplicative inverses.** For every \( a \) in \( F \), there exists an element \( -a \) in \( F \), such that \( a + (-a) = 0 \). Similarly, for any \( a \in F \) other than \( 0 \), there exists an element \( a^{-1} \) in \( F \), such that \( a \cdot a^{-1} = 1 \). (The elements \( a + (-b) \) and \( a \cdot b^{-1} \) are also denoted \( -b \) and \( a/b \), respectively.) In other words, subtraction and division operations exist.

6. **Distributivity of multiplication over addition.** For all \( a, b \) and \( c \) in \( F \), the following equality holds: \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \).

(Nota that all but the last axiom are exactly the axioms for a commutative group, while the last axiom is a compatibility condition between the two operations.)

### 2.1 Basic Properties of Fields

Here are some sample properties about fields. For more information about Fields see 5-8 of Rudin.

**Lemma 2.2.** Let \( F \) be a field, then;

1. There is only one additive and multiplicative inverses.
2. If \( x, y, z \in F \) with \( x \neq 0 \) and \( xy = xz \) then \( y = z \).
3. \( 0 \cdot x = 0 \) for all \( x \in F \).
4. If \( x, y \in F \) such that \( xy = 0 \) then \( x = 0 \) or \( y = 0 \).
5. \( (-x) y = - (xy) \).
6. \( -(-x) = x \) for all \( x \in F \).
7. \( (-x) (-y) = xy \) or all \( x, y \in F \).

**Proof.** We take each item in turn.

1. Suppose that \( x + y = 0 = x + y' \), then adding \(-x\) to both sides of this equation shows \( y = y' \). Taking \( y = -x \) then shows \( y = -x = y' \), i.e. additive inverses are unique. Similarly if \( x \neq 0 \) and \( xy = 1 \) then multiplying this equation by \( x^{-1} \) shows \( y = x^{-1} \) and so there is only one multiplicative inverse.

2. If \( xy = xz \) then multiplying this equation by \( x^{-1} \) shows \( y = z \).

3. \( 0 \cdot x + z = 0 \cdot x + 1 \cdot x = (0 + 1) \cdot x = 1 \cdot x = x \).

Adding \(-x\) to both side of this equation using associativity and commutativity of addition then implies \( 0 \cdot x = 0 \).

4. If \( x \in F \setminus \{0\} \) and \( y \in F \) such that \( xy = 0 \), then \( 0 = x^{-1} \cdot 0 = x^{-1} (xy) = (x^{-1}x) y = 1y = y \).

5. \( (-x) y + xy = (-x + x) \cdot y = 0 \cdot y = 0 \implies (-x) y = -(xy) \).

6. Since \( (-x) + x = 0 \) we have \( -(-x) = x \).

7. \( (-x)(-y) = -(x \cdot (-y)) = -(-xy) = xy \) by 6.

**Example 2.3.** Here are a few examples of Fields;
1. $\mathbb{F}_2 = \{0, 1\}$ with $0 + 0 = 0 = 1 + 1$, and $0 + 1 = 1 + 0 = 0$ and $0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0$ and $1 \cdot 1 = 1$. In this case $-1 = 1$, $1^{-1} = 1$ and $-0 = 0$.

2. $\mathbb{Q}$ - the rational numbers with the usual addition and multiplication of fractions. ($\dfrac{m}{n}$)$^{-1} = \dfrac{n}{m}$ if $m \neq 0$ and $-\dfrac{m}{n} = \dfrac{-m}{n}$.

3. $\mathbb{Q} = \mathbb{Q}(t)$ where

$$Q(t) = \left\{ \frac{p(t)}{q(t)} : p(t) \text{ and } q(t) \text{ are polynomials over } \mathbb{Q} \ni q(t) \neq 0 \right\}.$$ 

Again the multiplication and addition are as usual.

**Example 2.4.** $\mathbb{Z}$ is not a field. For example, 2 has no multiplicative inverse in $\mathbb{Z}$. The inverse to 2, $2^{-1}$, should be $\frac{1}{2}$ but this is not in $\mathbb{Z}$.

**Definition 2.5.** We say a map $\varphi : \mathbb{Z} \rightarrow \mathbb{F}$ is a (ring) homomorphism iff $\varphi(1) = 1_{\mathbb{F}}, \varphi(0) = 0_{\mathbb{F}}$, and for all $x, y \in \mathbb{Z}$,

$$\varphi(x + y) = \varphi(x) + \varphi(y) \text{ and } \varphi(xy) = \varphi(x) \varphi(y).$$

[The assumption that $\varphi(0) = 0_{\mathbb{F}}$ is redundant since $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ and therefore $\varphi(0) = 0_{\mathbb{F}}$.]

**Lemma 2.6.** For every field $\mathbb{F}$ there a unique (ring) homomorphism, $\varphi : \mathbb{Z} \rightarrow \mathbb{F}$. In fact, $\varphi(n) = n1_{\mathbb{F}}$ for all $n \in \mathbb{Z}$ where $01_{\mathbb{F}} = 0_{\mathbb{F}}$,

$$n1_{\mathbb{F}} := \underbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}} \text{ if } n \in \mathbb{N} \text{ and } \quad (-n)1_{\mathbb{F}} := -(n1_{\mathbb{F}}) \quad \text{ if } n \in \mathbb{N}.$$ 

[The map $\varphi$ need not be injective as is seen by taking $\mathbb{F} = \mathbb{F}_2$.]

**Proof.** Let us first work on $\mathbb{N}_0 \subseteq \mathbb{Z}$. We must define $\varphi(0) = 0$ and $\varphi(1) = 1$ and then $\varphi$ inductively by $\varphi(n + 1) = \varphi(n) + \varphi(1) = \varphi(n) + 1_{\mathbb{F}}$ so that

$$\varphi(n) = \underbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}} \text{ } \text{ } \text{n times}$$

We now write $n1_{\mathbb{F}}$ for $\varphi(n)$ with the convention that $01_{\mathbb{F}} = 0_{\mathbb{F}}$. For $n \in \mathbb{N}$ we must set $\varphi(-n) = -\varphi(n) = -(n1_{\mathbb{F}})$. Thus we have $\varphi(n) = n1_{\mathbb{F}}$ for all $n \in \mathbb{Z}$.

We now must show $\varphi$ is a homomorphism.

**Additive homomorphism:** First suppose that $m, n \in \mathbb{N}_0$ and let

$S := \{m \in \mathbb{N}_0 : \varphi(mn) = \varphi(m) \varphi(n) \text{ for all } n \in \mathbb{N}_0\}.$

It is easily seen that 0, 1 $\in S$. Moreover if $m \in S$ and $n \in \mathbb{N}_0$, then

$$\varphi((m + 1)n) = \varphi((mn + n) = \varphi(mn) + \varphi(n)$$

$$= \varphi(m) \varphi(n) + \varphi(n) = (\varphi(m) + 1_{\mathbb{F}}) \varphi(n)$$

$$= \varphi(m + 1) \varphi(n),$$

which shows $m + 1 \in S$. Therefore by induction, $S = \mathbb{N}_0$ and $\varphi(mn) = \varphi(m) \varphi(n)$ for all $m, n \in \mathbb{N}_0$.

If $m, n \in \mathbb{N}_0$, then

$$\varphi((-m)n) = \varphi(-mn) = -\varphi(mn) = -[\varphi(m) \varphi(n)] = [-\varphi(m)] \varphi(n) = \varphi(-m) \varphi(n)$$

and

$$\varphi((-m)(-n)) = \varphi(mn) = \varphi(mn) = (-\varphi(m))(-\varphi(n)) = -\varphi(m) \varphi(-n)$$

which completes the verification that $\varphi$ is a multiplicative homomorphism. 

$\varphi((m + 1) + n) = \varphi(m + n + 1) = \varphi(m) + \varphi(n + 1)$$

$$= \varphi(m) + \varphi(n) + 1_{\mathbb{F}}$$

$$= \varphi(m) + 1_{\mathbb{F}} + \varphi(n) = \varphi(m + 1) + \varphi(n)$$

which shows $m + 1 \in S$. Therefore by induction, $S = \mathbb{N}_0$ and $\varphi(m + n) = \varphi(m) + \varphi(n)$ for all $m, n \in \mathbb{N}_0$.

If $m \in \mathbb{N}_0$ we have $\varphi(-m) = -\varphi(m)$ by construction. If $n > m \in \mathbb{N}_0$, then

$$\varphi(n + (-m)) + \varphi(m) = \varphi(n - m) + \varphi(m) = \varphi(n)$$

so that

$$\varphi(n + (-m)) = \varphi(n) + (-\varphi(m)) = \varphi(n) + \varphi(-m).$$

If $n < m \in \mathbb{N}_0$, then

$$\varphi(n + (-m)) = -\varphi(m - n) = -[[\varphi(m) - \varphi(n)] = \varphi(n) + \varphi(-m)$$

and if $m, n \in \mathbb{N}_0$, then

$$\varphi(-n + (-m)) = \varphi(-(n + m)) = -\varphi(n + m)$$

$$= -[\varphi(n) + \varphi(m)] = -\varphi(n) - \varphi(m)$$

$$= \varphi(-n) + \varphi(-m).$$

Putting all of this together shows $\varphi$ is an additive homomorphism.

**Multiplicative homomorphism:** First suppose that $m, n \in \mathbb{N}_0$ and let

$$S := \{m \in \mathbb{N}_0 : \varphi(mn) = \varphi(m) \varphi(n) \text{ for all } n \in \mathbb{N}_0\}.$$

One easily sees that 0 $\in S$ and that 1 $\in S$ by construction. Moreover if $m \in S$, then
2.2 Ordered Fields

Definition 2.7 (Ordered Field). We say $\mathbb{F}$ is an **ordered field** if there exists, $P \subset \mathbb{F}$, called the positive elements, such that

Ord 1. $\mathbb{F}$ is the disjoint union of $P$, $\{0\}$, and $-P$, i.e. if $x \in \mathbb{F}$ then precisely one of following happens; $x \in P$, $x = 0$, or $-x \in P$.

Ord 2. $P + P \subset P$ and $P \cdot P \subset P$.

Lemma 2.8. Let $(\mathbb{F}, P)$ be an ordered field, then:

1. For all $x \in \mathbb{F} \setminus \{0\}$, $x^2 \in P$. In particular $1 = 1^2 \in P$.
2. If $x \in P$ and $y \in -P$ then $xy \in -P$.
3. If $x \in P$ then $x^{-1} \in P$.

**Proof.** If $x \in P$ then $x^2 \in P \cdot P \subset P$ while if $x \in -P$ then $-x \in P$ and $x^2 = (-x)^2 \in P$. For item 3. we have $x \cdot x^{-1} = 1$.

Example 2.9. The field $\mathbb{F} = \{0, 1\}$ is not ordered. The only possible choice for $P$ is $P = \{1\}$ which does not work since $1 + 1 = 0 \not\in P$.

Example 2.10. Take $\mathbb{F} = \mathbb{Q}$ and $P = \left\{ \frac{m}{n} : m, n > 0 \right\}$. This is in fact the unique choice we can make for $P$ in this case. Indeed suppose that $P$ is any order on $\mathbb{Q}$. By Lemma 2.8 we know $1 \in P$ and then by induction it follows that $\mathbb{N} \subset P$. Then again by Lemma 2.8 we must have $m \cdot n^{-1} \in P$ for all $m, n \in \mathbb{Q}$.

Example 2.11. Take $\mathbb{F} = \mathbb{Q}(t)$ and

$$P = \left\{ \frac{p(t)}{q(t)} \in \mathbb{F} : \frac{p(t)}{q(t)} > 0 \text{ for } t > 0 \text{ large} \right\},$$

i.e. $\frac{p(t)}{q(t)} \in P$ iff the highest order coefficients of $p(t)$ and $q(t)$ have the same sign. For example $\frac{t^2 - 25t + 7}{t^4 + 10t^3} \in P$ while $\frac{t^2 + 25t + 7}{t^4 + 10t^3} \not\in P$.

Notice that $t > n$ for all $n \in \mathbb{N}$ and $\frac{t}{n} < \frac{t}{2}$ for all $n \in \mathbb{N}$. This is kind of strange and explains why you have to prove the “obvious” in this course!!!

**Moral:** obvious statements are often false.

**Notation 2.12 (Max and Min)** We will often use the following notation in the sequel. If $a, b$ are elements of an ordered field, let

$$a \wedge b := \min(a, b) = \begin{cases} a & \text{if } a \leq b \\ b & \text{if } b \leq a \end{cases}$$

and

$$a \vee b := \max(a, b) = \begin{cases} b & \text{if } a \leq b \\ a & \text{if } b \leq a \end{cases}.$$

More generally if $\{a_i\}_{i=1}^n \subset \mathbb{F}$ we let

$$a_1 \wedge \cdots \wedge a_n := \min(a_1, \ldots, a_n) \quad \text{and} \quad a_1 \vee \cdots \vee a_n := \max(a_1, \ldots, a_n)$$

be the smallest and largest element in the finite list $(a_1, \ldots, a_n)$.

**Definition 2.13.** Suppose that $\mathbb{F}$ and $\mathbb{G}$ are fields. A map, $\varphi : \mathbb{F} \rightarrow \mathbb{G}$ is a (field) homomorphism iff $\varphi(1_\mathbb{F}) = 1_\mathbb{G}$, $\varphi(0_\mathbb{F}) = 0_\mathbb{G}$, and for all $x, y \in \mathbb{F}$:

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{and} \quad \varphi(xy) = \varphi(x) \varphi(y).$$

Lemma 2.14 ($\mathbb{Q}$ embeds into an ordered field). For every ordered field $(\mathbb{F}, P)$, there is a unique field homomorphism, $\varphi : \mathbb{Q} \rightarrow \mathbb{F}$. In fact,

$$\varphi \left( \frac{m}{n} \right) = \frac{m}{n} \cdot 1_\mathbb{F} := m1_\mathbb{F} \cdot (n1_\mathbb{F})^{-1}$$

$n$ times

where $n1_\mathbb{F} := 1_\mathbb{F} + \cdots + 1_\mathbb{F}$ and $(-n)1_\mathbb{F} := -(n1_\mathbb{F})$ for $n \in \mathbb{N}$ and $0 \cdot 1_\mathbb{F} = 0_\mathbb{F}$.

Moreover;

1. $\varphi(x) \in P$ whenever $x > 0$,
2. and $\varphi$ is injective. Thus we may identify $\mathbb{Q}$ with $\varphi(\mathbb{Q})$ and consider $\mathbb{Q}$ as a sub-field of $\mathbb{F}$.

[In particular, ordered fields must be fields with an infinite number of elements in it.]

**Proof.** From Lemma 2.6 we know there is a unique ring homomorphism, $\varphi : \mathbb{Z} \rightarrow \mathbb{F}$, given by $\varphi(m) = m \cdot 1_\mathbb{F}$. So for $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ we must have

$$\varphi \left( \frac{m}{n} \right) \cdot n1_\mathbb{F} = \varphi \left( \frac{m}{n} \right) \cdot \varphi(n) = \varphi \left( \frac{m}{n} \cdot n \right) = \varphi(m) = m1_\mathbb{F}$$

which forces us to define $\varphi$ as in Eq. (2.1). Notice that is easy to verify by induction that $n1_\mathbb{F} = \varphi(n) \in P$ for all $n \in \mathbb{N}$ and in particular $n1_\mathbb{F} \not= 0$ for $n \in \mathbb{N}$. In particular if $x = m/n > 0$ then $\varphi \left( \frac{m}{n} \right) = m1_\mathbb{F} \cdot (n1_\mathbb{F})^{-1} \in P$ by Lemma 2.8. We must still check that $\varphi$ is well defined homomorphism.

**Well defined.** Suppose that $k \in \mathbb{N}$, we must show

$$(km)1_\mathbb{F} \cdot ((kn)1_\mathbb{F})^{-1} = m1_\mathbb{F} \cdot (n1_\mathbb{F})^{-1}.$$

By cross multiplying, this will happen iff

$$(km)1_\mathbb{F} \cdot (n1_\mathbb{F}) = ((kn)1_\mathbb{F}) \cdot m1_\mathbb{F}$$

which is the case as \( \varphi : \mathbb{Z} \to F \) is a ring homomorphism.

**Homomorphism property.** We have
\[
\varphi \left( \frac{m}{n} + \frac{p}{q} \right) = \varphi \left( \frac{m+p}{n} \right) = \varphi (m+p) \cdot \varphi (n)^{-1} \\
= [\varphi (m) + \varphi (p)] \cdot \varphi (n)^{-1} \\
= \varphi (m) \cdot \varphi (n)^{-1} + \varphi (p) \cdot \varphi (n)^{-1} \\
= \varphi \left( \frac{m}{n} \right) + \varphi \left( \frac{p}{q} \right)
\]
and
\[
\varphi \left( \frac{m}{n} \right) \varphi \left( \frac{q}{p} \right) = \varphi (m) \varphi (n)^{-1} \varphi (q) \varphi (p)^{-1} \\
= \varphi (m) \frac{q}{p} [\varphi (n) \varphi (p)]^{-1} \\
= \varphi (mq) [\varphi (np)]^{-1} = \varphi \left( \frac{mq}{np} \right).
\]

**Injectivity.** If \( 0 = \varphi \left( \frac{m}{n} \right) \) then
\[
0 = \varphi (m) \cdot \varphi (n)^{-1}
\]
which implies \( \varphi (m) = 0 \) which happens iff \( m = 0 \), i.e. \( m/n = 0 \).

\[\square\]

End of Lecture 3, 10/3/2012

**Notation 2.15** If \((F, P)\) is an ordered field we write \( x > y \) iff \( x - y \in P \). We also write \( x \geq y \) iff \( x > y \) or \( x = y \).

Notice that if \( x, y \in F \) then either \( x - y = 0 \) (i.e. \( x = y \)), or \( x - y \in P \) (i.e. \( x > y \)), or \( x - y \in -P \) (i.e. \( y - x \in P \) and \( y > x \)). Also in this notation we have
\[
P = \{x \in F : x > 0\}, \\
-P = \{x \in F : x < 0 \text{ i.e. } 0 > x\}.
\]

**Lemma 2.16.** Suppose that \( x < y \) and \( y < z \) and \( a > 0 \). Then \( x < z \) and \( ax < ay \).

**Proof.** By assumption \( y - x \in P \) and \( z - y \in P \), therefore \( z - x = (y - x) + (z - y) \in P \), i.e. \( z > x \). Moreover, \( a \in P \) and \( (y - x) \in P \) implies
\[
P \ni a(y - x) = ay - ax.
\]
That is \( ay > ax \).

\[\square\]

**Exercise 2.1.** Let \((F, P)\) be an ordered field and \( x, y \in F \) with \( y > x \). Show:
1. \( y + a > x + a \) for all \( a \in F \),
2. \(-x > -y \),
3. if we further suppose \( x > 0 \), show \( \frac{1}{x} > \frac{1}{y} \).

**Definition 2.17.** Given \( x \in F \), we say that \( y \in F \) is a square root of \( x \) if \( y^2 = x \).

[From Lemma 2.8 it follows that if \( x \in F \) has a square root then \( x \geq 0 \).]

**Lemma 2.18.** Suppose \( x, y \in F \) with \( x^2 = y^2 \), then either \( x = y \) or \( x = -y \). In particular, there are at most 2 square roots of any number \( x \geq 0 \) in \( F \).

**Proof.** Observe that
\[
(x-y)(x+y) = (x-y)x + (x-y)y \\
= x^2 - xy + xy - y^2 = x^2 - y^2 = 0.
\]
Thus it follows that either \( x - y = 0 \) or \( x + y = 0 \), i.e. \( x = y \) or \( x = -y \). \[\square\]

**Definition 2.19.** If \( x > 0 \) admits a square root we let \( \sqrt{x} \) be the unique positive root. We also define \( \sqrt{0} = 0 \).

**Lemma 2.20.** Suppose that \( 0 < x < y \), i.e. \( x, y - x \in P \), then \( x^2 < y^2 \).

**Proof.** By Lemma 2.16 we know \( x \cdot x < x \cdot y \) and \( x \cdot y < y \cdot y \) and therefore \( x^2 < y^2 \).

\[\square\]

**Corollary 2.21.** If \( 0 \leq x < y \) and \( \sqrt{x} \) and \( \sqrt{y} \) exists, then \( 0 \leq \sqrt{x} < \sqrt{y} \).

**Proof.** If \( \sqrt{x} = \sqrt{y} \) then \( x = (\sqrt{x})^2 = (\sqrt{y})^2 = y \) which is impossible. Similarly if \( \sqrt{x} > \sqrt{y} \) then
\[
x = (\sqrt{x})^2 > (\sqrt{y})^2 = y
\]
which is again false.

**Alternatively:** starting with \( y^2 - x^2 = (y-x)(y+x) \) and then replacing \( y \) and \( x \) by \( \sqrt{y} \) and \( \sqrt{x} \) respectively (assuming they exist) shows,
\[
y - x = (\sqrt{y} - \sqrt{x})(\sqrt{y} + \sqrt{x}) \implies \sqrt{y} - \sqrt{x} = (y-x)(\sqrt{y} + \sqrt{x})^{-1}
\]
from which it follows that \( \sqrt{y} - \sqrt{x} \in P \) if \((y-x) \in P \). More importantly this shows \( \sqrt{y} \) depends “continuously” in on \( y \).

\[\square\]

**Definition 2.22.** The absolute value, \(|x|\), of \( x \) in ordered field \( F \) is defined by
\[
|x| = \begin{cases} 
  x & \text{if } x \geq 0 \\
  -x & \text{if } x < 0
\end{cases}
\]
Alternatively we may define
\[
|x| = \sqrt{x^2}.
\]
Proposition 2.23. For all \( x, y \in \mathbb{F} \), then
1. \( |x| \geq 0 \)
2. \( |xy| = |x| |y| \)
3. \( |x + y| \leq |x| + |y| \).

Proof. 1 holds by definition since \(-x > 0\) if \( x < 0 \).
2. As \( |x| |y| \geq 0 \) and \((|x| |y|)^2 = |x|^2 |y|^2 = x^2 y^2 = (xy)^2\), we have
\[
|x| |y| = \sqrt{(xy)^2} = |xy|.
\]
3. It suffices to show \( |x + y| \leq (|x| + |y|)^2 \). However,
\[
|x + y|^2 = (x + y)^2 = x^2 + y^2 + 2xy
\]
\[
\leq x^2 + y^2 + 2|x|y \quad (xy \leq |xy|)
\]
\[
= |x|^2 + |y|^2 + 2|x| |y|
\]
\[
= (|x| + |y|)^2.
\]

Definition 2.24. Let \((\mathbb{F}, P)\) be an ordered field and \( S \) be a subset of \( \mathbb{F} \).

1. We say that \( S \subset \mathbb{F} \) is bounded from above (below) if there exists \( x \in \mathbb{F} \) such that \( x \geq s \) (\( x \leq s \)) for all \( s \in S \). Any such \( x \) is called an upper (lower) bound of \( S \).
2. If \( S \) is bounded from above (below), we say that \( y \in \mathbb{F} \) is a least upper bound (greatest lower bound) for \( S \) if \( y \) is an upper (lower) bound for \( S \) and \( y \leq x \) (\( y \geq x \)) for any other upper (lower) bound, \( x \), of \( S \).

Notice that least upper bounds and greatest lower bounds are unique if they exist. We will write and
\[
y = \text{l.u.b.} (S) = \sup (S)
\]
if \( y \) is the least upper bound for \( S \) and
\[
y = \text{g.l.b.} (S) = \inf (S)
\]
if \( y \) is the greatest lower bound for \( S \).

Example 2.25. Let \( \mathbb{F} = \mathbb{Q} \), then;
1. \( \text{max} (a, b) \) and \( \text{min} (a, b) \) are least upper respectively greatest lower bounds respectively for \( S = \{ a, b \} \). More generally, if \( S = \{ a_1, \ldots, a_n \} \), then
\[
\sup (S) = a_1 \vee \cdots \vee a_n := \text{max} (a_1, \ldots, a_n) \quad \text{and} \quad \inf (S) = a_1 \wedge \cdots \wedge a_n := \text{min} (a_1, \ldots, a_n).
\]
2. \( S = \mathbb{N} \) is not bounded from above while \( \inf (S) = 1 \).
3. \( S = \{ 1 - \frac{1}{n} : n \in \mathbb{N} \} \) is bounded from above and \( 1 = \sup (S) \) while \( \inf (S) = \frac{1}{2} \).
4. Let
\[
S = \{ 1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, \ldots \}
\]
where I am getting these digits from the decimal expansion of \( \sqrt{2} \);
\[
\sqrt{2} \approx 1.41421356237309504880168872420969807856967187537694807317667973799.
\]
In this case \( S \) is bounded above by 2, or 1.42, or 1.415, etc. Nevertheless \( \sqrt{2} = \sup (S) \) does not exists in \( \mathbb{Q} \).

Example 2.26. Now let \( \mathbb{F} = \mathbb{Q} (t) \) be the field of rational functions described in Example 2.11 then; \( S = \mathbb{N} \) is bounded from above. For example \( t \) is an upper bound but there is not least upper bound. For example \( \frac{1}{m} t \) is also an upper bound for \( S \).

End of Lecture 4, 10/5/2012

Definition 2.27 (Dedekind Cuts). A subset \( \alpha \subset \mathbb{Q} \) is called a cut (see [2, p. 17]) if;
1. \( \alpha \) is a proper subset of \( \mathbb{Q} \), i.e. \( \alpha \neq \emptyset \) and \( \alpha \neq \mathbb{Q} \),
2. if \( p \in \alpha \) and \( q \in \mathbb{Q} \) and \( q < p \), then \( q \in \alpha \),
3. if \( p \in \alpha \), then there exists \( r \in \alpha \) with \( r > p \).

Example 2.28. To each \( a \in \mathbb{Q} \), let \( \alpha_a := \{ q \in \mathbb{Q} : q < a \} \). Then \( \alpha_a \) is a cut and \( a \) is the least upper bound of \( \alpha_a \) in \( \mathbb{Q} \).

Example 2.29. Let \( \{ S_n \}_{n=0}^{\infty} \subset \mathbb{Q} \) be any bounded sequence such that \( S_n \leq S_{n+1} \) for all \( n \). Then
\[
\alpha := \bigcup_{n=0}^{\infty} \alpha_{S_n} = \{ q \in \mathbb{Q} : q < S_n \ \text{a.a.} \ n \}
\]
is a cut as the reader should verify. Let us further suppose that \( \lim_{n \to \infty} S_n \) does not exist in \( \mathbb{Q} \). [For example from Example 1.17 we may take \( S_n := \sum_{k=0}^{n} \frac{1}{k} \in \mathbb{Q} \).] If \( m \in \mathbb{Q} \) is an upper bound for \( \alpha \), then \( m \geq S_n \) for all \( n \) since if \( m < S_n \) for some \( n \) then \( q := \frac{1}{2} (m + S_n) \in \alpha \) with \( q > m \). Since \( \lim_{n \to \infty} S_n \neq m \) as \( m \in \mathbb{Q} \) there must exists \( \varepsilon > 0 \) such that
\[
m - S_n = |m - S_n| \geq \varepsilon \quad \text{i.o.} \ n.
\]
As \( m - S_n \) is decreasing we may conclude that \( m - S_n \geq \varepsilon \) for all \( n \), i.e. \( S_n \leq m - \varepsilon \) for all \( n \). From this it now follows that \( m - \varepsilon \) is an upper bound for \( \alpha \) which is strictly smaller that \( m \). So there can be no least upper bound.
Real Numbers

As we saw in Section 1.2, \( \mathbb{Q} \) is full of holes and calculus tends to produce answers which live in these holes. So it is imperative that we fill the holes. Doing so will lead to the real numbers provided we fill in the holes without adding too much extra filler along the way. One good answer to the question, What are the real numbers?, is contained in the statement of Theorem 3.3.

**Definition 3.1.** An order preserving field isomorphism between two ordered fields, \( (\mathbb{F}, P) \) and \( (\mathbb{F}_2, P_2) \), is a bijection, \( f : \mathbb{F} \to \mathbb{F}_2 \) such that \( f(0) = 0, f(1) = 1, f(P_i) = P_2 \), and

\[
f(x + y) = f(x) + f(y) \quad \text{and} \quad f(xy) = f(x)f(y)
\]
for all \( x, y \in \mathbb{F}_1 \).

**Definition 3.2.** An ordered field \( (\mathbb{F}, P) \) has the least upper bound property (or is complete) if every non-empty subset, \( S \subset \mathbb{F} \), which is bounded from above possesses a least upper bound in \( \mathbb{F} \). [As we have seen in examples above, \( \mathbb{Q} \) does not have the least upper bound property.]

**Theorem 3.3 (The real numbers).** Up to order preserving field isomorphism (see Definition 3.7), there is exactly one complete ordered field. It is this field that we refer to as the real numbers and denote by \( \mathbb{R} \).

**Definition 3.4.** We say two Cauchy sequences \( \{a_n\}_{n=1}^{\infty} \) and \( \{b_n\}_{n=1}^{\infty} \) of rational numbers are equivalent and write \( \{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty} \) iff

\[
\lim_{n \to \infty} |a_n - b_n| = 0.
\]

We then define \( \alpha := \left\{\{a_n\}_{n=1}^{\infty} \right\} \) to be the equivalence class of the Cauchy sequence \( \{a_n\}_{n=1}^{\infty} \) and refer to the collection of these equivalence classes as the real numbers. The set of real numbers will be denoted by \( \mathbb{R} \).

**Notation 3.5** Let \( i : \mathbb{Q} \to \mathbb{R} \) be defined by \( i(a) := \left\{[a, a, a, \ldots] \right\} \), i.e. \( i(a) \) is the equivalence class of the constant sequence \( a \).

Notice that if \( i(a) = i(b) \) iff \( a = \lim_{n \to \infty} a = \lim_{n \to \infty} b = b \). Thus the map, \( i : \mathbb{Q} \to \mathbb{R} \) is injective and we will often simply identify \( a \) with \( i(a) \) and in this way consider \( \mathbb{Q} \) as a subset of \( \mathbb{R} \).

**Theorem 3.6.** Let \( \mathbb{R} \) be as in Definition 3.4. For \( \alpha := \left\{\{a_n\}_{n=1}^{\infty} \right\} \) and \( \beta := \left\{\{b_n\}_{n=1}^{\infty} \right\} \) in \( \mathbb{R} \) we define

\[
\alpha + \beta = \left\{\{a_n + b_n\}_{n=1}^{\infty} \right\} \quad \text{and} \quad \alpha \cdot \beta = \left\{\{a_n \cdot b_n\}_{n=1}^{\infty} \right\}.
\]

1. With these definitions, \( \mathbb{R} \), satisfies the axioms of a field.
2. Moreover, we can make this into an ordered field by setting \( P := \{a \in \mathbb{R} : \alpha > 0 \} \) where we say \( \alpha > 0 \) iff there exists an \( N \in \mathbb{N} \) such that \( \alpha > \frac{1}{N} \) for a.a. \( n \).
3. The ordered field \( (\mathbb{R}, P) \) is complete, i.e. has the least upper bound property.

The proof of Theorem 3.6 and Theorem 3.3 will be relegated to Section 3.6 at the end of this chapter. For an alternative existence proof of \( \mathbb{R} \) using Dedekind cuts as the elements of \( \mathbb{R} \) is covered in Rudin [2] pages 17-21. One may also construct the Real numbers using decimal expansions, see T. Gower’s notes on real numbers as decimals. We will prove the uniqueness assertion of Theorem 3.3 in Section 3.7 at the end of this section. From now on we are going to take Theorem 3.3 for granted and derive from this the “familiar” properties of the real numbers.

Observe that \( \mathbb{Q}, \mathbb{Q}(t), \mathbb{R}(t) \) are not complete and hence are not the real numbers, \( \mathbb{R} \). For example \( \mathbb{N} \subset \mathbb{Q}(t) \) (or \( \mathbb{N} \subset \mathbb{R}(t) \)) is bounded by \( t \) say but has no least upper bound. However, we do know that \( \mathbb{Q} \subset \mathbb{R} \) by Lemma 2.14. We will soon see that \( \mathbb{Q} \) is “dense” in \( \mathbb{R} \). We now pause to discuss some of the basic properties of \( \mathbb{R} \).

**Theorem 3.7.** Suppose that \( \mathbb{R} \) is a complete ordered field which we assume we have already embedded \( \mathbb{Q} \) into \( \mathbb{R} \) as in Lemma 2.14. Then;

1. For all \( x \geq 0 \) there exists \( n \in \mathbb{N} \) such that \( n \geq x \).
2. For all \( \varepsilon > 0 \) in \( \mathbb{R} \) there exists \( n \in \mathbb{N} \) such that \( 0 < \frac{1}{n} \leq \varepsilon \).
3. If \( \varepsilon \geq 0 \) satisfies \( \varepsilon 
 \begin{align*}
\text{Proof.} & \quad \text{We take each item in turn.} \\
& \quad 1. \text{If } n < x \text{ for all } n \in \mathbb{N}, \text{then } \mathbb{N} \text{ is bounded from above and so } a := \sup(\mathbb{N}) \text{ exists in } \mathbb{R} \text{ by the completeness axiom. As } a \text{ is the least upper bound for } N \text{ there must be an } n \in \mathbb{N} \text{ such that } n > a - 1. \text{ However this implies } n+1 > a \text{ which violates } a \text{ be an upper bound for } N. \\
& \quad \text{Roughly speaking here, you should think of } a = \lim_{n \to \infty} a_n \text{ and so } a > 0 \text{ should happen iff } a > \frac{1}{N} \text{ for some } N \in \mathbb{N} \text{ which then implies } a_n \geq \frac{1}{N} \text{ for a.a. } n.
\end{align*}
Proposition 3.8. If \( \mathbb{R} \) is a complete ordered field, then every subset \( S \subset \mathbb{R} \) which is bounded from below has a greatest lower bound, \( \text{glb}(S) = \inf(S) \). In fact,
\[
\inf(S) = -\sup(-S).
\]

**Proof.** We let \( m := -\sup(-S) \). Then we have \( -s \leq m \) for all \( s \in S \), hence \( m \) is a lower bound for \( S \). Moreover if \( \varepsilon > 0 \) is given there exists \( s_\varepsilon \in S \) such that \( -s_\varepsilon \geq -m - \varepsilon \), i.e. \( s_\varepsilon \leq m + \varepsilon \). This shows that any lower bound, \( k \) of \( S \) must satisfy, \( k \leq m + \varepsilon \) for all \( \varepsilon > 0 \), i.e. \( k \leq m \). This shows that \( m \) is the greatest lower bound for \( S \).

Let me sketch one way to construct \( \mathbb{R} \) based on Cauchy sequences of rational numbers.

**Definition 3.9.** A sequence \( \{q_n\}_{n=1}^\infty \subset \mathbb{R} \) converges to \( 0 \in \mathbb{R} \) if for all \( \varepsilon > 0 \) in \( \mathbb{R} \) there exists \( N \in \mathbb{N} \) such that \( |q_n| \leq \varepsilon \) for all \( n \geq N \). Alternatively put, for all \( M \in \mathbb{N} \) we have \( |q_n| \leq \frac{1}{M} \) for a.a. \( n \).

**Definition 3.10.** A sequence \( \{q_n\}_{n=1}^\infty \subset \mathbb{R} \) converges to \( q \in \mathbb{R} \) if \( |q - q_n| \to 0 \) as \( n \to \infty \), i.e. if for all \( N \in \mathbb{N} \), \( |q - q_n| \leq \frac{1}{M} \) for a.a. \( n \). As usual if \( \{q_n\}_{n=1}^\infty \) converges to \( q \) we will write \( q_n \to q \) as \( n \to \infty \) or \( q = \lim_{n \to \infty} q_n \).

**Definition 3.11.** A sequence \( \{q_n\}_{n=1}^\infty \subset \mathbb{R} \) is **Cauchy** if \( |q_n - q_m| \to 0 \) as \( m, n \to \infty \). More precisely we require for each \( \varepsilon > 0 \) in \( \mathbb{R} \) that \( |q_m - q_n| \leq \varepsilon \) for a.a. pairs \( (m, n) \), i.e. there should exists \( N \in \mathbb{N} \) such that \( |q_m - q_n| \leq \varepsilon \) for all \( m, n \geq N \).

The next few results are analogous to what you have already shown in the case \( \mathbb{R} \) is replaced by \( \mathbb{Q} \). As the proofs are essentially identical to those of Theorem 1.13 and Exercise 1.6.

**Proposition 3.12.** If \( \{a_n\}_{n=1}^\infty \subset \mathbb{R} \) is a convergent sequence then it is Cauchy.

If \( \{a_n\}_{n=1}^\infty \) is Cauchy sequence then it is bounded.

We are going to show shortly that the converse is true as well!
1. **Proof 1.** Let $\alpha_m := \{y \in \mathbb{Q} : y < m\}$ and $M := \sup \alpha_m \in \mathbb{R}$. Then $M \leq m$. If $M \neq m$ then $M < m$. To see this last case is not possible let $\varepsilon := m - M > 0$ and choose $n \in \mathbb{N}$ such that $0 < \frac{1}{n} \leq \varepsilon$. Then choose $y \in \mathbb{Q}$ such that

$$M - \frac{1}{2n} < y < M.$$ 

From this it follows that

$$M < y + \frac{1}{2n} < M + \frac{1}{2n} < m$$

which shows $y + \frac{1}{2n} \in \alpha_m$ is greater than $M$ violating the assumption that $M$ is an upper bound for $\alpha_m$.

**Proof 2.** [Here is a slight rewriting of the above argument.] Choose $y_n \in \alpha_m$ such that $y_n \uparrow M$ as $m \to \infty$. Choose $n \in \mathbb{N}$ so that $m - M > \frac{1}{n}$. Then $y_m + \frac{1}{n} \uparrow M + \frac{1}{n} < m$ as $m \to \infty$. So for large $m$, $y_m + \frac{1}{n} < m$ while $y_m - \frac{1}{n} > M$, i.e. $y_m + \frac{1}{n} \in \alpha_m$ yet $y_m + \frac{1}{n} > M$. This violates the assumption that $M$ is an upper bound for $\alpha_m$.

2. By item 1, and Theorem 3.14 we can choose $q \in \alpha_b$ to be as close to $b$ as we choose and in particular $q$ can be chosen to be in $\alpha_b$ with $q > a$.

3. You are asked to prove this in Exercise 3.1 below.

**Exercise 3.1.** Suppose that $\alpha \subset \mathbb{Q}$ is a cut as in Definition 2.27. Show $\alpha$ is bounded from above. Then let $m := \sup \alpha$ and show that $\alpha = \alpha_m$, where $\alpha_m$

$$\alpha_m := \{y \in \mathbb{Q} : y < m\}.$$

Also verify that $\alpha_m$ is a cut for all $m \in \mathbb{R}$. [In this way we see that we may identify $\mathbb{R}$ with the cuts of $\mathbb{Q}$. This should motivate Dedekind’s construction of the real numbers as described in Rudin.]

**Proposition 3.17 (Rationals are dense in the reals).** For all $b \in \mathbb{R}$, there exists $q_n \in \mathbb{Q}$ such that $q_n \uparrow b$. Similarly there exists $p_n \in \mathbb{Q}$ such that $p_n \downarrow b$.

**Proof.** Given $b \in \mathbb{Q}$ we know that $b = \sup \alpha_b$ by Theorem 3.16. Then by Theorem 3.14 there exists $q_n \in \alpha_b$ such that $q_n \uparrow b$ as $n \to \infty$. The second assertion can be proved in much the same way as the first. Alternatively, let $q_n \in \mathbb{Q}$ such that $q_n \uparrow -b$ and set $p_n := -q_n \in \mathbb{Q}$. Then $p_n \downarrow b$.

**Definition 3.18.** The real numbers which are not rational are called **irrational**\(^3\) so the irrational numbers are $\mathbb{R} \setminus \mathbb{Q}$.

---

**3.1 Extended real numbers**

**Notation 3.21** The extended real numbers is the set $\mathbb{R} := \mathbb{R} \cup \{\pm \infty\}$, i.e. it is $\mathbb{R}$ with two new points called $\infty$ and $-\infty$. We use the following conventions,

\(^3\) For what it is worth, as dictionary definition of irrational is “not consistent with or using reason”. Let’s try to use irrational numbers in a rational way!

$\begin{align*}
\text{Example 3.19 (Euler’s number).} & \quad \text{Let } S_n := \sum_{k=0}^{n} \frac{1}{m} \text{ for all } n \in \mathbb{N}_0. \text{ We define Euler’s number to be,} \\
& \quad e := \lim_{n \to \infty} S_n = \sup \{S_n : n \in \mathbb{N}_0\} \in \mathbb{R}. \\
\text{From Example 1.17 we have seen that } e \in \mathbb{R} \setminus \mathbb{Q}. \\
\text{Theorem 3.20 (n}^{th}\text{ - roots).} & \quad \text{Let } n \in \mathbb{N} \text{ and } x > 0 \in \mathbb{R}, \text{ then there exists a unique } y \in \mathbb{R}_+ \text{ such that } y^n = x. \text{ We of course denote } y \text{ by } x^{1/n} \text{ for } \sqrt[n]{x}. \text{ The function } x \to x^{1/n} \text{ is increasing. [See Rudin for more properties of } x^{1/n} \text{ and } x^{m/n} \text{ where } m \in \mathbb{Z} \text{ and } n \in \mathbb{N}.] \\
\text{Proof. Uniqueness.} & \quad \text{First of } t > s \geq 0 \text{ then } t^n > s^n \geq 0 \text{ as can be proved by induction.} \text{ Thus if } x, y \geq 0 \text{ and } x^n = y^n \text{ then } x = y \text{ for otherwise } x > y \text{ or } y > x \text{ in which case } x^n > y^n \text{ or } y^n > x^n \text{ respectively. This shows that there is at most one } n^{th} - \text{root if it exists. I also claim that } x^{1/n} < y^{1/n} \text{ if } x < y. \text{ If not then } x^{1/n} \geq y^{1/n} \text{ and this would then imply } x = (x^{1/n})^n \geq (y^{1/n})^n = y \text{ which contradicts } x < y. \\
\text{Existence.} & \quad \text{Let } A := \{t \in \mathbb{R}_+ : t^n \leq x\}. \text{ If } t = \frac{x^{1/n}}{k} \in (0, 1), \text{ then } t^n \leq t \leq x \text{ so that } t \in A \text{ and } A \neq \emptyset. \text{ If } t = 1 + x, \text{ then } t^n = (1 + x)^n \geq 1 + nx > x \text{ and therefore } A \text{ is bounded from above. Hence we may define } y := \sup A. \text{ We will now show that } y^n = x. \\
\text{By Theorem 3.14 there exists } t_k \in A \text{ such that } t_k \uparrow y \text{ as } k \to \infty. \text{ By definition of } A, t_k^n \leq x \text{ for all } k. \text{ Passing to the limit as } k \to \infty \text{ in this inequality implies } y^n = \lim_{k \to \infty} t_k^n \leq x. \\
\text{If } y^n < x \text{ then (using the Binomial theorem) and properties of limits,} \\
\left( y + \frac{1}{m} \right)^n = y^n + \sum_{k=1}^{n} \binom{n}{k} y^{n-k} \left( \frac{1}{m} \right)^k \to y^n < x \text{ as } m \to \infty.
\end{align*}$
\[ \pm \infty \cdot a = \pm \infty \text{ if } a \in \mathbb{R} \text{ with } a > 0, \pm \infty \cdot a = \mp \infty \text{ if } a \in \mathbb{R} \text{ with } a < 0, \pm \infty + a = \pm \infty \text{ for any } a \in \mathbb{R}, \infty + \infty = \infty \text{ and } -\infty - \infty = -\infty \text{ while the following expressions are not defined; } \]

\[ \infty - \infty, -\infty + \infty, \infty/\infty, 0 \cdot \infty, \text{ and } \infty \cdot 0. \]

A sequence \( a_n \in \mathbb{R} \) is said to converge to \( \infty \) (\( -\infty \)) if for all \( M \in \mathbb{R} \) there exists \( m \in \mathbb{N} \) such that \( a_n \geq M \) \((a_n \leq M)\) for all \( n \geq m \). In these cases we write \( \lim_{n \to \infty} a_n = \pm \infty \) or \( a_n \to \pm \infty \) as \( n \to \infty \).

For any subset \( A \subseteq \mathbb{R} \), let \( \sup A \) and \( \inf A \) denote the least upper bound and greatest lower bound of \( A \) respectively. The convention being that \( \sup A = \infty \) if \( \infty \in \mathbb{R} \) or \( A \) is not bounded from above and \( \inf A = -\infty \) if \( -\infty \in \mathbb{R} \) or \( A \) is not bounded from below. We will also use the conventions that \( \sup \emptyset = -\infty \) and \( \inf \emptyset = +\infty \). The next theorem is a fairly simple but often useful result about computing least upper bounds.

**Theorem 3.22 (Sup Sup Theorem).** Suppose that \( A \) is a subset of \( \mathbb{R} \) such that \( A = \bigcup_{\alpha \in I} A_{\alpha} \) where \( A_{\alpha} \subset A \) and \( I \) is some index set. Then

\[ \sup A = \sup_{\alpha \in I} \sup A_{\alpha}. \]

The convention here is that the supremum of a set which is not bounded from above is \( \infty \) and the sup \( \emptyset = -\infty \). \( \square \)

**Proof.** Let \( M := \sup A \) and \( M_\alpha := \sup A_{\alpha} \) for all \( \alpha \in I \). As \( A_{\alpha} \subset A \) we have \( M_\alpha \leq M \) for all \( \alpha \in I \) and therefore \( \sup_{\alpha \in I} M_\alpha \leq M \). Conversely, if \( \lambda \in A \), then \( \lambda \in M_\alpha \) for some \( \alpha \in I \) and therefore \( \lambda \leq M_\alpha \). From this it follows that \( \lambda \leq \sup_{\alpha \in I} M_\alpha \) and as \( \lambda \in A \) is arbitrary we may conclude that \( M = \sup A \leq \sup_{\alpha \in I} M_\alpha \). \( \square \)

The next corollary records a typical way the Sup Sup theorem is used.

**Corollary 3.23.** Suppose that \( X \) and \( Y \) are sets and \( S : X \times Y \to \mathbb{R} \) is a function. Then

\[ \sup_{x \in X} \sup_{y \in Y} S(x, y) = \sup_{(x, y) \in X \times Y} S(x, y). \]

In particular, if \( S_{m, n} \in \mathbb{R} \) for all \( m, n \in \mathbb{N} \), then

\[ \sup_{m} \sup_{n} S_{m, n} = \sup_{(m, n)} S_{m, n} = \sup_{m} \sup_{n} S_{m, n}. \]

**Proof.** Let \( A := \{ S(x, y) : (x, y) \in X \times Y \} \), and for \( x \in X \) let \( A_x := \{ S(x, y) : y \in Y \} \). Then \( A = \bigcup_{x \in X} A_x \) and therefore,

\[ \sup_{(x, y) \in X \times Y} S(x, y) = \sup_{x \in X} \sup_{y \in Y} S(x, y) = \sup_{x \in X} \sup_{y \in Y} S(x, y). \]

The same reasoning also shows,

\[ \sup_{(x, y) \in X \times Y} S(x, y) = \sup_{x \in X} \sup_{y \in Y} S(x, y). \]

The next Lemma records some basic limit theorems involving the extended real numbers.

**Lemma 3.24.** Suppose \( \{a_n\}_{n=1}^{\infty} \) and \( \{b_n\}_{n=1}^{\infty} \) are convergent sequences in \( \overline{\mathbb{R}} \), then:

1. If \( a_n \leq b_n \) for a.a. \( n \) then \( \lim_{n \to \infty} a_n \leq \lim_{n \to \infty} b_n \).
2. If \( c \in \mathbb{R} \), \( \lim_{n \to \infty} (ca_n) = c \lim_{n \to \infty} a_n \).
3. If \( \{a_n + b_n\}_{n=1}^{\infty} \) is convergent and

\[ \lim_{n \to \infty} (a_n + b_n) = \lim_{n \to \infty} a_n + \lim_{n \to \infty} b_n \] (3.1)

provided the right hand side is not of the form \( \infty - \infty \).
4. \( \{a_nb_n\}_{n=1}^{\infty} \) is convergent and

\[ \lim_{n \to \infty} (a_nb_n) = \lim_{n \to \infty} a_n \cdot \lim_{n \to \infty} b_n \] (3.2)

provided the right hand side is not of the form \( \pm \infty \cdot 0 \) or \( 0 \cdot (\pm \infty) \).

Before going to the proof consider the simple example where \( a_n = n \) and \( b_n = -an + c \) with \( a > 0 \) and \( c \in \mathbb{R} \). Then\(^5\)

\[ \lim_{n \to \infty} (a_nb_n) = \begin{cases} 
\infty & \text{if } a < 1 \\
0 & \text{if } a = 1 \\
\infty & \text{if } a > 1
\end{cases} \]

while

\[ \lim_{n \to \infty} a_n + \lim_{n \to \infty} b_n = "\infty - \infty." \]

This shows that the requirement that the right side of Eq. (3.1) is not of form \( \infty - \infty \) is necessary in Lemma 3.24. Similarly by considering the examples \( a_n = n \) and \( b_n = n^{-\alpha} \) with \( \alpha > 0 \) shows the necessity for assuming right hand side of Eq. (3.2) is not of the form \( \infty \cdot 0 \).

**Proof.** The proofs of items 1. and 2. are left to the reader.\(^6\)

\(^5\) The only sequences that do not converge in \( \overline{\mathbb{R}} \) are those which oscillate too much.

\(^6\) This example shows that if you formally arrive at an expression like \( \infty - \infty \), then you should work harder to decide what it really means!
Proof of Eq. (3.1). Let $a := \lim_{n \to \infty} a_n$ and $b := \lim_{n \to \infty} b_n$.

Case 1. Suppose $b = \infty$ in which case we must assume $a > -\infty$. In this case, for every $M > 0$, there exists $N$ such that $b_n \geq M$ and $a_n \geq a - 1$ for all $n \geq N$ and this implies

$$a_n + b_n \geq M + a - 1 \text{ for all } n \geq N.$$ 

Since $M$ is arbitrary it follows that $a_n + b_n \to \infty$ as $n \to \infty$. The cases where $b = -\infty$ or $a = \pm \infty$ are handled similarly.

Case 2. If $a, b \in \mathbb{R}$, then for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that

$$|a - a_n| \leq \varepsilon \text{ and } |b - b_n| \leq \varepsilon \text{ for all } n \geq N.$$ 

Therefore,

$$|a + b - (a_n + b_n)| = |a - a_n + b - b_n| \leq |a - a_n| + |b - b_n| \leq 2\varepsilon$$

for all $n \geq N$. Since $n$ is arbitrary, it follows that $\lim_{n \to \infty} (a_n + b_n) = a + b$.

Proof of Eq. (3.2). It will be left to the reader to prove the case where $l_{a_n}$ and $l_{b_n}$ exist in $\mathbb{R}$. I will only consider the case where $a = \lim_{n \to \infty} a_n \neq 0$ and $\lim_{n \to \infty} b_n = \infty$ here. Let us also suppose that $a > 0$ (the case $a < 0$ is handled similarly) and let $\alpha := \min\left(\frac{a}{2}, 1\right)$. Given any $M < \infty$, there exists $N \in \mathbb{N}$ such that $a_n \geq \alpha$ and $b_n \geq M$ for all $n \geq N$ and for this choice of $N$, $a_n b_n \geq M \alpha$ for all $n \geq N$. Since $a > 0$ is fixed and $M$ is arbitrary it follows that $\lim_{n \to \infty} (a_n b_n) = \infty$ as desired. ■

Exercise 3.2. Show $\lim_{n \to \infty} a^n = \infty$ and $\lim_{n \to \infty} \frac{1}{a^n} = 0$ whenever $a > 1$.

Exercise 3.3. Suppose $a > 1$ and $k \in \mathbb{N}$, show there is a constant $c = c(a, k) > 0$ such that $a^n \geq cn^k$ for all $n \in \mathbb{N}$. [In words, $a^n$ grows in $n$ faster than any polynomial in $n$.]

Lemma 3.25. Suppose that $\{a_n\}_{n=1}^\infty \subset \mathbb{R}$ and $\lim_{n \to \infty} a_n = A \in \mathbb{R}$. Then every subsequence, $\{b_k := a_{n_k}\}_{k=1}^\infty$, also converges to $A$.

Exercise 3.4. Prove Lemma 3.25.

3.2 Limsups and Liminfs

Notation 3.26 Suppose that $\{x_n\}_{n=1}^\infty \subset \overline{\mathbb{R}}$ is a sequence of numbers. Then

$$\liminf_{n \to \infty} x_n = \lim_{n \to \infty} \inf\{x_k : k \geq n\} \quad (3.3)$$

$$\limsup_{n \to \infty} x_n = \lim_{n \to \infty} \sup\{x_k : k \geq n\}. \quad (3.4)$$

We will also write $\underline{\lim}$ for $\liminf$ and $\overline{\lim}$ for $\limsup$.

Remark 3.27. Notice that if $a_k := \inf\{x_k : k \geq n\}$ and $b_k := \sup\{x_k : k \geq n\}$, then $\{a_k\}$ is an increasing sequence while $\{b_k\}$ is a decreasing sequence. Therefore the limits in Eq. (3.3) and Eq. (3.4) always exist in $\mathbb{R}$ (see Theorem 3.15) and

$$\lim_{n \to \infty} \inf_{n \to \infty} x_n = \sup_{n \to \infty} \inf\{x_k : k \geq n\}$$

$$\lim_{n \to \infty} \sup_{n \to \infty} x_n = \inf_{n \to \infty} \sup\{x_k : k \geq n\}.$$ 

Owing to the following exercise, one may reduce properties of the lim inf to those of the lim sup.

Exercise 3.5. Show $\liminf_{n \to \infty}(-a_n) = -\limsup_{n \to \infty} a_n$.

Exercise 3.6. Let $\{a_n\}_{n=1}^\infty$ be the sequence given by,

$$(-1, 2, 3, -1, 2, 3, -1, 2, 3, \ldots).$$

Find $\limsup_{n \to \infty} a_n$ and $\liminf_{n \to \infty} a_n$.

Exercise 3.7. If $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are two sequences such that $a_n \leq b_n$ for a.a. $n$, then

$$\lim\sup_{n \to \infty} a_n \leq \lim\sup_{n \to \infty} b_n \text{ and } \lim\inf_{n \to \infty} a_n \leq \lim\inf_{n \to \infty} b_n. \quad (3.5)$$

The following proposition contains some basic properties of liminf and limsup.

Proposition 3.28. Let $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ be two sequences of real numbers. Then

1. $\liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n$.

2. $\lim_{n \to \infty} a_n$ exists in $\overline{\mathbb{R}}$ iff

$$\lim\inf_{n \to \infty} a_n = \lim\sup_{n \to \infty} a_n \in \overline{\mathbb{R}}.$$

3. $\limsup_{n \to \infty} (a_n + b_n) \leq \limsup_{n \to \infty} a_n + \limsup_{n \to \infty} b_n \quad (3.6)$

whenever the right side of this equation is not of the form $\infty - \infty$.

4. If $a_n \geq 0$ and $b_n \geq 0$ for all $n \in \mathbb{N}$, then

$$\lim\sup_{n \to \infty} (a_n b_n) \leq \lim\sup_{n \to \infty} a_n \cdot \lim\sup_{n \to \infty} b_n, \quad (3.7)$$

provided the right hand side of (3.7) is not of the form $0 \cdot \infty$ or $\infty \cdot 0$. 


The proof for the case $A$; i.e. that 

$\epsilon > 0$ for every $\epsilon > 0$ and therefore by the Sandwich theorem, $\liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n$.

2. ($\Rightarrow$) Let $A := \liminf_{n \to \infty} a_n = \limsup_{n \to \infty} a_n \in \mathbb{R}$. Since 

$$\inf_{k \geq n} a_k \leq a_n \leq \sup_{k \geq n} a_k,$$

if $A \in \mathbb{R}$ then it follows by the sandwich theorem that $\lim_{n \to \infty} a_n = A$. If $A = \infty$, then for all $M \in \mathbb{N}$ we have $M \leq \inf_{k \geq n} a_k$ for a.a. $n$. Therefore $a_k \geq M$ for a.a. $k$ and we have shown $\lim_{k \to \infty} a_k = \infty$. If $A = -\infty$ then for all $M \in \mathbb{N}$ we have $\sup_{k \geq n} a_k \leq -M$ for a.a. $n$. Therefore $a_k \leq -M$ for a.a. $k$ and we have shown $\lim_{k \to \infty} a_k = -\infty$.

($\Leftarrow$) Conversely, suppose that $\lim_{n \to \infty} a_n = A \in \mathbb{R}$ exists. If $A \in \mathbb{R}$, then for every $\epsilon > 0$ there exists $N(\epsilon) \in \mathbb{N}$ such that $|A - a_n| \leq \epsilon$ for all $n \geq N(\epsilon)$, i.e.

$$A - \epsilon \leq a_n \leq A + \epsilon$$

for all $n \geq N(\epsilon)$.

From this we learn that 

$$-\epsilon \leq a_n \leq A + \epsilon$$

and so passing to the limit as $n \to \infty$ implies 

$$A - \epsilon \leq \liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n \leq A + \epsilon.$$ 

Since $\epsilon > 0$ is arbitrary, it follows that 

$$A \leq \liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n \leq A,$$

i.e. that $A = \liminf_{n \to \infty} a_n = \limsup_{n \to \infty} a_n$.

If $A = \infty$, then for all $M > 0$ there exists $N = N(M)$ such that $a_n \geq M$ for all $n \geq N$. This show that $\liminf_{n \to \infty} a_n \geq M$ and since $M$ is arbitrary it follows that 

$$\infty \leq \liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n.$$ 

The proof for the case $A = -\infty$ is analogous to the $A = \infty$ case.

**Exercise 3.8.** Show that 

$$\limsup_{n \to \infty} (a_n + b_n) \leq \limsup_{n \to \infty} a_n + \limsup_{n \to \infty} b_n$$

provided that the right side of Eq. (3.5) is well defined, i.e. no $\infty - \infty$ or $-\infty + \infty$ type expressions. (It is OK to have $\infty + \infty = \infty$ or $-\infty - \infty = -\infty$, etc.)

**Exercise 3.9.** Suppose that $a_n \geq 0$ and $b_n \geq 0$ for all $n \in \mathbb{N}$. Show 

$$\limsup_{n \to \infty} (a_n b_n) \leq \limsup_{n \to \infty} a_n \cdot \limsup_{n \to \infty} b_n,$$

provided the right hand side of Eq. (3.9) is not of the form $0 \cdot \infty$ or $\infty \cdot 0$.

* End of Lecture 7, 10/12/2012.

**Exercise 3.10.** If $a_n \geq 0$, then $\lim_{n \to \infty} a_n = 0$ iff $\limsup_{n \to \infty} a_n = 0$.

**Proposition 3.29.** Suppose that $\{a_n\}_{n=1}^{\infty}$ is a sequence of real numbers and let 

$$B := \{y \in \mathbb{R} : a_n \geq y \text{ for i.o. } n\}.$$ 

Then $\sup B = \limsup_{n \to \infty} a_n$ with the convention that $\sup B = -\infty$ if $B = \emptyset$.

**Proof.** If $\{a_n\}_{n=1}^{\infty}$ is not bounded from above, then $B$ is not bounded from above and $\sup B = \infty = \limsup_{n \to \infty} a_n$. If $B = \emptyset$ so that $\sup B = -\infty$, then for all $y \in \mathbb{R}$ we must have $a_n < y$ for a.a. $n$. This then implies $\limsup_{n \to \infty} a_n \leq y$ for all $y \in \mathbb{R}$ from which we conclude that $\limsup_{n \to \infty} a_n = -\infty$. So let us now assume that $B \neq \emptyset$ and $\{a_n\}_{n=1}^{\infty}$ is bounded in which case $B$ is bounded from above. Let us set $\beta := \sup B \in \mathbb{R}$ and $a^* := \limsup_{n \to \infty} a_n$.

If $y > \beta$, then $a_n < y$ for a.a. $n$ from which it follows that $a^* := \limsup_{n \to \infty} a_n \leq y$. We may now let $y \downarrow \beta$ in order to see that $a^* \leq \beta$. Now suppose that $y < \beta$, then $a_n \geq y$ for a.a. $n$ and hence $a^* = \limsup_{n \to \infty} a_n \geq y$. Letting $y \uparrow \beta$ then shows $a^* \geq \beta$. Thus we have shown $a^* = \beta$.

**Theorem 3.30.** There is a subsequence $\{a_{n_k}\}_{k=1}^{\infty}$ of $\{a_n\}_{n=1}^{\infty}$ such that 

$$\lim_{k \to \infty} a_{n_k} = \limsup_{n \to \infty} a_n.$$ Similarly, there is a subsequence $\{a_{n_k}\}_{k=1}^{\infty}$ of $\{a_n\}_{n=1}^{\infty}$ such that 

$$\lim_{k \to \infty} a_{n_k} = \liminf_{n \to \infty} a_n.$$ Moreover, every convergent subsequence, $\{b_k := a_{n_k}\}_{k=1}^{\infty}$ of $\{a_n\}_{n=1}^{\infty}$ satisfies, 

$$\liminf_{n \to \infty} a_n \leq \limsup_{k \to \infty} b_k \leq \limsup_{n \to \infty} a_n.$$ 

**Proof.** Let me prove the last assertion first. Suppose that $b_k := a_{n_k}$ is some convergent subsequence of $\{a_n\}_{n=1}^{\infty}$. We then have, 

$$\inf_{n \geq n_k} a_n \leq b_k \leq \sup_{n \geq n_k} a_n \text{ for all } k \in \mathbb{N}.$$ 

Passing to the limit in this equation then implies, 

$$\liminf_{n \to \infty} a_n \leq \limsup_{k \to \infty} b_k \leq \limsup_{n \to \infty} a_n = \limsup_{n \to \infty} a_n.$$ 

This can be done more formally by choosing a sequence $\{y_k\}_{k=1}^{\infty}$ such that $y_k \downarrow \alpha$ so that $a^* := \limsup_{n \to \infty} y_k = \alpha$. 

---

We have used, \( \{\inf_{n \geq k} a_n\}_{k=1}^{\infty} \) and \( \{\sup_{n \geq k} a_n\}_{k=1}^{\infty} \) are subsequence of the convergent sequences of \( \{\inf_{n \geq k} a_n\}_{k=1}^{\infty} \) and \( \{\sup_{n \geq k} a_n\}_{k=1}^{\infty} \) respectively and therefore converge to the same limits respectively, see Lemma 3.25.

Now let us prove the first assertions. I will cover the \( \limsup \) case here as the \( \liminf \) case is similar or can be deduced from the \( \limsup \) case with the aid of Exercise 3.5. Let \( A := \limsup_{n \to \infty} a_n \). We will need to consider three case, \( A \in \mathbb{R} \), \( A = \infty \), and \( A = -\infty \).

i) \( A \in \mathbb{R} \), then by Proposition 3.29, for all \( k \in \mathbb{N} \) we have \( A - \frac{1}{k} \leq a_n \) for infinitely many \( n \). In particular we can choose \( n_1 < n_2 < n_3 < \ldots \) inductively so that \( A - \frac{1}{k} \leq a_{n_k} \) for all \( k \). Since

\[
A - \frac{1}{k} \leq a_{n_k} \leq \sup_{m \geq n_k} a_m
\]

and the limit as \( k \to \infty \) of both extremes of this inequality are \( A \), it follow from the sandwich inequality that \( \lim_{k \to \infty} a_{n_k} = A \).

ii) If \( A = \limsup_{n \to \infty} a_n = \infty \), then \( \sup_{k \geq n} a_k = \infty \) for all \( n \in \mathbb{N} \) which implies for all \( M < \infty \) that \( a_k \geq M \) i.o. \( k \). Working similarly to case i) we can choose \( n_1 < n_2 < n_3 < \ldots \) so that \( a_{n_k} \geq k \) for all \( k \) and therefore \( \lim_{k \to \infty} a_{n_k} = \infty \).

iii) Finally suppose that \( A = \limsup_{n \to \infty} a_n = -\infty \) so that for all \( M \in \mathbb{N} \) there exists \( N \in \mathbb{N} \) such that \( \sup_{k \geq n} a_k \leq -M \) for all \( n \geq N \), i.e. \( a_n \leq -M \) for all \( n \geq N \). In this case it follows that in fact \( \lim_{n \to \infty} a_n = -\infty \) and we do not have to even choose as subsequence.

\[ \blacksquare \]

Corollary 3.31 (Bolzano–Weierstrass Property / Compactness). Every bounded sequence of real numbers, \( \{a_n\}_{n=1}^{\infty} \), has a convergent in \( \mathbb{R} \) subsequence, \( \{a_{n_k}\}_{k=1}^{\infty} \). If we drop the bounded assumption then we may only assert that there is a subsequence which is convergent in \( \mathbb{R} \).

\[ \blacksquare \]

Proof. Let \( M < \infty \) such that \( |a_n| \leq M \) for all \( n \in \mathbb{N} \), i.e. \( -M \leq a_n \leq M \) for all \( n \). We may then conclude from Exercise 3.7 that,

\[
-M \leq \limsup_{n \to \infty} a_n \leq M.
\]

It now follows from Theorem 3.30 that there exists a subsequence, \( \{a_{n_k}\}_{k=1}^{\infty} \), of \( \{a_n\}_{n=1}^{\infty} \) such that

\[
\lim_{k \to \infty} a_{n_k} = \limsup_{n \to \infty} a_n \in [-M, M] \subset \mathbb{R}.
\]

\[ \blacksquare \]

Theorem 3.32 (\( \mathbb{R} \) is Cauchy complete). If \( \{a_n\}_{n=1}^{\infty} \subset \mathbb{R} \) is a Cauchy sequence, then \( \lim_{n \to \infty} a_n \) exists in \( \mathbb{R} \) and in fact,

\[
\lim_{n \to \infty} a_n = \limsup_{n \to \infty} a_n = \liminf_{n \to \infty} a_n.
\]

Proof. We will give two proofs of this important theorem. Each proof uses the fact that \( \{a_n\}_{n=1}^{\infty} \subset \mathbb{R} \) is Cauchy implies \( \{a_n\}_{n=1}^{\infty} \) is bounded. This is proved exactly in the same way as the solution to Exercise 1.2.

First proof. By Corollary 3.31 there is a subsequence, \( \{a_{n_k}\}_{k=1}^{\infty} \), such that \( \lim_{k \to \infty} a_{n_k} = L \in \mathbb{R} \). As in the proof of Exercise 1.7 it follows that \( \lim_{n \to \infty} a_n \) exists and is equal to \( L \).

Second proof. Let \( a := \liminf_{n \to \infty} a_n \) and \( b := \limsup_{n \to \infty} a_n \). It suffices to show \( a = b \). As we always know that \( a \leq b \) it will suffice to show \( b \leq a \). Given \( \varepsilon > 0 \), there exists \( N \in \mathbb{N} \) such that

\[
|a_n - a| < \varepsilon \text{ for all } n, n \geq N.
\]

In particular, for \( m, n \geq k \geq N \) we have \( a_m \leq a_n + \varepsilon \) and hence

\[
b \leq \sup_{m \geq k} a_m \leq a_n + \varepsilon \text{ for all } n \geq k.
\]

From this inequality we may further conclude,

\[
b \leq \inf_{n \geq k} a_n + \varepsilon \leq a + \varepsilon.
\]

As \( \varepsilon > 0 \) is arbitrary, we have indeed shown \( b \leq a \).

\[ \blacksquare \]

- End of Lecture 8, 10/15/2012.

Exercise 3.11. Suppose that \( \{a_n\}_{n=1}^{\infty} \) is a sequence of real numbers and let

\[
A := \{y \in \mathbb{R} : a_n \geq y \text{ for a.a. } n\}.
\]

Then \( \sup A = \liminf_{n \to \infty} a_n \) with the convention that \( \sup \emptyset = -\infty \) if \( A = \emptyset \).

Exercise 3.12. Suppose that \( \{a_n\}_{n=1}^{\infty} \) is a sequence of real numbers. Show \( \limsup_{n \to \infty} a_n = a^* \in \mathbb{R} \) iff for all \( \varepsilon > 0 \),

\[
a_n \leq a^* + \varepsilon \text{ for a.a. } n \text{ and } a^* - \varepsilon \leq a_n \text{ i.o. } n.
\]

Similarly, show \( \liminf_{n \to \infty} a_n = a_* \in \mathbb{R} \) iff for all \( \varepsilon > 0 \),

\[
a_n \geq a_* + \varepsilon \text{ i.o. } n \text{ and } a_* - \varepsilon \leq a_n \text{ for a.a. } n.
\]

Notice that this exercise gives another proof of item 2. of Proposition 3.28 in the case all limits are real valued.
Exercise 3.13 (Cauchy Complete \implies L.U.B. Property). Suppose that $\mathbb{R}$ denotes any ordered field which is Cauchy complete. Show $\mathbb{R}$ has the least upper bound property and therefore is the field of real numbers.

3.3 Partitioning the Real Numbers

Notation 3.33 (Intervals) For $a, b \in \mathbb{R}$ with $a < b$ we define,

$$
(a, b) := \{x \in \mathbb{R} : a < x < b\}, \quad [a, b) := \{x \in \mathbb{R} : a \leq x < b\}, \quad (a, b] := \{x \in \mathbb{R} : a < x \leq b\}, \quad \text{and} \quad [a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}.
$$

We also also $a = -\infty$ in the intervals, $(a, b)$ and $(a, b]$ and allows $b = +\infty$ in the intervals $(a, b)$ and $[a, b)$.

Notation 3.34 (Pairwise disjoint unions) If $X$ is a set and $A_\alpha \subset X$ for $\alpha \in I$, we write $X = \sum_{\alpha \in I} A_\alpha$ to mean $X = \cup_{\alpha \in I} A_\alpha$ and $A_\alpha \cap A_\beta$ for all $\alpha \neq \beta$.

Exercise 3.14. Suppose that $a, b, c, d \in \mathbb{R}$ such that $a < b \leq c < d$. Show $(a, b] \cap [c, d) = \emptyset$ and $[a, b) \cap [c, d] = \emptyset$.

Lemma 3.35 (Well Ordering II). Suppose that $S$ is a non-empty subset of $\mathbb{Z}$ which is bounded from below, then $\inf(S) \in S$, i.e. $S$ has a unique minimizer.

Proof. As $S$ is bounded from below, there exists $k \in \mathbb{Z}$ such that $k \leq s$ for all $s \in S$. Therefore $\tilde{S} := \{s - k + 1 : s \in S\} \subset \mathbb{N}$ and hence by the well ordering principle, $m := \min(\tilde{S})$ exists. That is $m \leq s - k + 1$ for all $s \in S$ and there exists $s_0 \in S$ such that $m = s_0 - k + 1$. These last statements are equivalent to saying,

$$s_0 = m + k - 1 \leq s$$

for all $s \in S$,

which is to say $s_0 = \min(S)$.

Proposition 3.36. Suppose that $\{S_n\}_{n=0}^\infty \subset \mathbb{R}$ such that $S_n < S_{n+1}$ for all $n \in \mathbb{Z}$, $\lim_{n \to \infty} S_n = \infty$ and $\lim_{n \to -\infty} S_n = -\infty$. Then

$$
\sum_{n \in \mathbb{Z}} (S_{n-1}, S_n) = \mathbb{R} = \sum_{n \in \mathbb{Z}} [S_n, S_{n+1}). \quad (3.10)
$$

Proof. The fact that $(S_n, S_{n+1}] \cap (S_m, S_{m+1}) = \emptyset$ follows from Exercise 3.14. For $x \in \mathbb{R}$, let

$$n_0 := \min \{\{n \in \mathbb{Z} : x \leq S_n\}\}$$

which exists since $\{n \in \mathbb{Z} : x \leq S_n\}$ is non-empty as $S_n \to \infty$ as $n \to \infty$ and is bounded from below since $S_n \to -\infty$ as $n \to -\infty$. It then follows that $x \leq S_{n_0}$ while $x \notin S_{n_0-1}$, i.e. $S_{n_0-1} < x \leq S_{n_0}$ and we have shown $x \in (S_{n_0-1}, S_{n_0}]$, which completes the proof of the first equality in Eq. (3.10). The proof of the second equality is similar and so will be omitted.

Proposition 3.37. Suppose that $-\infty < a < b < \infty$ and $\{S_n\}_{n=0}^N \subset [a, b]$ such that $a = S_0 < S_1 < \cdots < S_{N-1} < S_N = b$, then

$$[a, b) = \sum_{n=1}^N [S_{n-1}, S_n).$$

This result also holds if $N = \infty$ provided we now assume $S_n < S_{n+1}$ for all $n$, $a = S_0$, and $S_n \uparrow b$ as $n \to \infty$.

Proof. This proof is very similar to the proof of Proposition 3.36 and so will be omitted.

3.4 The Decimal Representation of a Real Number

Lemma 3.38 (Geometric Series). Let $\alpha \in \mathbb{R}$ or $\alpha \in \mathbb{Q}$, $m, n \in \mathbb{Z}$ and $S := \sum_{k=n}^m \alpha^k$. Then

$$S = \begin{cases} 
  m - n + 1 & \text{if } \alpha = 1 \\
  \frac{\alpha^{m+1} - \alpha^n}{\alpha - 1} & \text{if } \alpha \neq 1.
\end{cases}$$

Proof. When $\alpha = 1$,

$$S = \sum_{k=n}^m 1^k = m - n + 1.$$ 

If $\alpha \neq 1$, then

$$\alpha S - S = \alpha^{m+1} - \alpha^n.$$ 

Solving for $S$ gives

$$S = \sum_{k=n}^m \alpha^k = \frac{\alpha^{m+1} - \alpha^n}{\alpha - 1} \text{ if } \alpha \neq 1. \quad (3.11)$$

Taking $\alpha = 10^{-1}$ in Eq. (3.11) implies
If we may associate the real number \( \frac{a_m - n}{10^{-m+n}} \) with \( \frac{1}{10 - n} \), \( \frac{1 - 10^{-m + n}}{10^{m - n} - 1} \) and in particular, for all \( M \geq n \),

\[
\lim_{m \to \infty} \sum_{k=n}^{m} 10^{-k} = \frac{1}{9} \left( \frac{1 - 10^{-m + n}}{10^{m - n} - 1} \right)
\]

\[
\text{Definition 3.39 (Decimal Numbers). Let } \mathbb{D} \text{ denote those sequences } \alpha \in \{0, 1, 2, \ldots, 9\}^\mathbb{N} \text{ with the following properties:}
\]

1. there exists \( N \in \mathbb{N} \) such that \( \alpha_n = 0 \) for all \( n \geq N \) and
2. \( \alpha_n \neq 0 \) for some \( n \in \mathbb{Z} \).

A decimal number is then an expression of the form

\[
\alpha_n \alpha_{n+1} \cdots \alpha_0 \alpha_1 \alpha_2 \alpha_3 \ldots
\]

For example

\[
52 + \sqrt{2} \approx 53.4142135623730950488016887240969807856967187537694807\ldots
\]

To every decimal number \( \alpha \in \mathbb{D} \) is the sequence \( a_n = a_n(\alpha) \) defined for \( n \in \mathbb{N} \) by

\[
a_n := \sum_{k=-\infty}^{n} \alpha_k 10^{-k}.
\]

Since for \( m > n \),

\[
|a_m - a_n| = \left| \sum_{k=n+1}^{m} \alpha_k 10^{-k} \right| \leq 9 \sum_{k=n+1}^{m} 10^{-k} \leq 9 \cdot \frac{1}{10^n} = \frac{1}{10^n},
\]

it follows that

\[
|a_m - a_n| \leq \frac{1}{10^{\min(m,n)}} \to 0 \text{ as } m, n \to \infty
\]

which shows \( \{a_n\}_{n=1}^{\infty} \) is a Cauchy sequence. Thus to every decimal number we may associate the real number

\[
a(\alpha) := \lim_{n \to \infty} a_n.
\]

**Theorem 3.40. If } x \geq 0 \text{ is a real number, there exists } \alpha \in \mathbb{D} \text{ such that } x = a(\alpha), \text{ i.e. all real numbers can be represented in decimal form.}

**Proof. If } x = 0 \text{, we can take } a_n = 0 \text{ for all } n \text{ so that } 0 = a(\alpha). \text{ So suppose that } x > 0 \text{ and let } p := \min \{\{n \in \mathbb{N} : x < n\}\}. \text{ Set } m = p - 1, \text{ then } m \leq x < m + 1. \text{ We then define } \alpha_k \text{ for } k \leq 0 \text{ so that } m = \alpha_N \cdots \alpha_0. \text{ We now construct } \alpha_k \text{ for } k \geq 1. \text{ For } k = 1 \text{ we write}

\[
[m, m+1) = \sum_{l=0}^{9} \left[ m + \frac{l}{10} \right]
\]

and then choose \( \alpha_1 = l \) if \( x \in [m + \frac{l}{10}, m + \frac{l+1}{10}) \). We then construct \( \alpha_2 \) using,

\[
[m + \alpha_1 \frac{1}{10}, m + \frac{\alpha_1 + 1}{10}) \sum_{l=0}^{9} \left[ m + \frac{\alpha_1 + l}{10}, m + \frac{\alpha_1 + l + 1}{10} \right]
\]

and set \( \alpha_2 = l \) for \( x \in [m + \frac{\alpha_1 + l}{10}, m + \frac{\alpha_1 + l + 1}{10}) \). Continuing this way inductively we construct \( \{\alpha_k\}_{k=1}^{\infty} \) such that

\[
x \in [m + \sum_{j=1}^{k} \frac{\alpha_j}{10^j}, m + \sum_{j=1}^{k-1} \frac{\alpha_j}{10^j} + \frac{\alpha_k + 1}{10^k}).
\]

It is now easy to see that \( x = a(\alpha) \).

**Remark 3.41. The representation of } x \geq 0 \text{ as a decimal number may not be unique. For example,

\[
0.99\overline{9} = \sum_{k=1}^{\infty} \frac{9}{10^k} = \frac{9}{9} \cdot \frac{1}{10} = 1.00.
\]

[Or note that]

\[
1 - 0.9\overline{\cdot} 0 = 0.\overline{0} = 0 \text{ as } n \to \infty.
\]

On the other hand if we agree to not allow a tail of repeated 9’s as an element of \( \mathbb{D} \), then the representation would be unique.

### 3.5 Summary of Key Facts about Real Numbers

1. The real numbers, \( \mathbb{R} \), is the unique (up to order preserving field isomorphism) ordered field with the least upper bound property or equivalently which is Cauchy complete.
2. Informally the real numbers are the rational numbers with the (irrational) hole filled in.
3. Monotone bounded sequence always converge in \( \mathbb{R} \).
4. A sequence converges in \( \mathbb{R} \) iff it is Cauchy.
5. Cauchy sequences are bounded.
6. \( \mathbb{N} \) is unbounded from above in \( \mathbb{R} \).
7. For all \( \varepsilon > 0 \) in \( \mathbb{R} \) there exists \( n \in \mathbb{N} \) such that \( \frac{1}{n} < \varepsilon \).
8. \( \mathbb{Q} \) and \( \mathbb{R} \setminus \mathbb{Q} \) is dense in \( \mathbb{R} \). In particular, between any two real numbers \( a < b \), there are infinitely many rational and irrational numbers.
9. Decimal numbers map (almost 1-1) into the real numbers by taking the limit of the truncated decimal number.
10. If \( a, b, \varepsilon \in \mathbb{R} \), then
   a) \( a \leq b \) by showing that \( a \leq b + \varepsilon \) for all \( \varepsilon > 0 \).
   b) \( a = b \) by proving \( a \leq b \) and \( b \leq a \) or
   c) \( a = b \) by showing \( |b - a| \leq \varepsilon \) for all \( \varepsilon > 0 \).
11. A number of standard limit theorems hold, see Theorem 3.13.
12. Unlike limits, \( \limsup \) and \( \liminf \) always exist. Moreover we have:
   \[ \liminf_{n \to \infty} a_n \leq \limsup_{n \to \infty} a_n \]
   with equality iff \( \lim_{n \to \infty} a_n \) exists in which case
   \[ \liminf_{n \to \infty} a_n = \lim_{n \to \infty} a_n = \limsup_{n \to \infty} a_n. \]
   We may allow the values of \( \pm \infty \) in these statements.
13. If \( b_k \colon= \{a_{n_k}\}_{k=1}^\infty \) is a convergent subsequence of \( \{a_n\} \), then
   \[ \liminf_{n \to \infty} a_n \leq \lim_{k \to \infty} b_k \leq \limsup_{n \to \infty} a_n \]
   and we may choose \( \{b_k\} \) so that \( \lim_{k \to \infty} b_k = \limsup_{n \to \infty} a_n \) or
   \( \lim_{k \to \infty} b_k = \liminf_{n \to \infty} a_n \).
14. Bounded sequences of real numbers always have convergence subsequences.
15. If \( S \subset \mathbb{R} \) and \( A \colon= \sup(S) \), then there exists \( \{a_n\}_{n=1}^\infty \subset S \) such that
   \( a_n \leq a_{n+1} \) for all \( n \) and \( \lim_{n \to \infty} a_n = \sup(S) \).
16. If \( S \subset \mathbb{R} \) and \( A \colon= \inf(S) \), then there exists \( \{a_n\}_{n=1}^\infty \subset S \) such that
   \( a_n \leq a_n \) for all \( n \) and \( \lim_{n \to \infty} a_n = \inf(S) \).

### 3.6 (Optional) Proofs of Theorem 3.6 and Theorem 3.3

In this section, we assume that \( \mathbb{R} \) is as describe in Theorem 3.6. The next exercise is relatively straightforward.

**Exercise 3.15.** Prove the following properties of \( \mathbb{R} \).

1. Show addition and multiplication in Theorem 3.6 are well defined.

2. Show \( (\mathbb{R}, +, \cdot) \) satisfies the axioms of a field. **Hint:** for constructing multiplicative inverses, make use of Proposition 3.42 below to conclude if \( \alpha \colon= \{a_n\}_{n=1}^\infty \in \mathbb{R} \) and \( a \neq 0 = i(0) \), then there exists \( N \in \mathbb{N} \) such that \( |a_n| \geq \frac{1}{N} \) for a.a. \( n \). By redefining the first few terms of \( a_n \) if necessary, you may assume that \( |a_n| \geq \frac{1}{N} \) for all \( n \) and then take
   \[ \alpha^{-1} = \left\{ a_n^{-1} \right\}_{n=1}^\infty. \]

3. Show \( i : \mathbb{Q} \to \mathbb{R} \) is injective homomorphism of fields.

To finish the proof of Theorem 3.6 we must show that \( P \) is an ordering on \( \mathbb{R} \) with the least upper bound property. This will be carried out in the remainder of this section.

**Proposition 3.42.** Suppose that \( \alpha \colon= \{a_n\}_{n=1}^\infty \) and \( \beta \colon= \{b_n\}_{n=1}^\infty \) are real numbers. Then precisely one of the following three cases can happen:

1. \( \lim_{n \to \infty} (a_n - b_n) = 0 \), i.e. \( \alpha = \beta \),
2. there exists \( \varepsilon = \frac{1}{N} > 0 \) such that \( a_n \geq b_n + \varepsilon \) for a.a. \( n \) in which case \( \alpha > \beta \),
3. there exists \( \varepsilon = \frac{1}{N} > 0 \) such that \( b_n \geq a_n + \varepsilon \) for a.a. \( n \) in which case \( \beta > \alpha \).

**Proof.** If case 1. does not hold then there exists \( \delta > 0 \) such that \( |a_n - b_n| \geq \delta \) for infinitely many \( n \). There are now two possibilities (which will turn out to me mutually exclusive;

   i) \( a_n - b_n \geq \delta \) i.o. \( n \),
   ii) \( b_n - a_n \geq \delta \) i.o. \( n \).

   Since \( \{a_n\} \) and \( \{b_n\} \) are Cauchy sequences, there exists \( N \in \mathbb{N} \) such that
   \[ |a_n - a_m| \geq \delta/3 \]
   and \( |b_n - b_m| \geq \delta/3 \) for all \( m, n \geq N \).

   If case i) holds, we may choose an \( m \geq N \) such that \( a_m - b_m \geq \delta \) and so for \( n \geq N \) we find,
   \[ \delta \leq a_m - b_m = a_m - a_n + a_n - b_n + b_n - b_m \]
   \[ \leq |a_m - a_n| + a_n - b_n + |b_n - b_m| \]
   \[ = \delta/3 + a_n - b_n + \delta/3 \]
   from which it follows that \( a_n - b_n \geq \varepsilon \colon= \delta/3 \) for all \( n \geq N \) and we are in case 2. Similarly if case ii) holds then we are in fact in case 3. of the proposition. \( \blacksquare \)

**Corollary 3.43.** Suppose that \( \alpha \colon= \{a_n\}_{n=1}^\infty \) and \( \beta \colon= \{b_n\}_{n=1}^\infty \) are real numbers, then \( \alpha \geq \beta \) iff for all \( N \in \mathbb{N} \),

\[ a_n - b_n \geq \frac{1}{N} \]

for a.a. \( n \).

\[ (3.12) \]
Alternatively put, \( \alpha \geq \beta \) iff for all \( N \in \mathbb{N} \),
\[
    b_n \leq a_n + \frac{1}{N} \quad \text{for a.a. } n.
\]

**Proof.** If \( \alpha = \beta \), then \( \lim_{n \to \infty} (a_n - b_n) = 0 \) and therefore Eq. (3.12) holds. If \( \alpha > \beta \), then in fact \( a_n - b_n \geq \varepsilon > 0 \geq -1/N \) for a.a. \( n \).

Conversely, if \( \alpha < \beta \), then there exists \( \varepsilon > 0 \) such that \( b_n \geq a_n + \varepsilon \) for a.a. \( n \). Thus if Eq. (3.12) were to also hold we could conclude for each \( N \in \mathbb{N} \) that
\[
    a_n \geq b_n - \frac{1}{N} \geq a_n + \varepsilon - \frac{1}{N} \quad \text{for a.a. } n.
\]

This leads to a contradiction as soon as we choose \( N \) so large as to make \( 1/N < \varepsilon \). Thus if Eq. (3.12) holds we must have \( \alpha \geq \beta \).

**Proposition 3.44.** Suppose that \( \lambda \in \mathbb{R} \), \( \{a_n\}_{n=1}^{\infty} \) be a Cauchy sequence in \( \mathbb{Q} \), and \( \alpha := \lim_{n \to \infty} a_n \). If \( \lambda \leq i(a_k) \) for all \( k \) then \( \lambda \leq \alpha \). Similarly if \( i(a_k) \leq \lambda \) for all \( k \) then \( \alpha \leq \lambda \).

**Proof.** Let \( \lambda = \lim_{n \to \infty} a_n \) and suppose that \( \lambda \leq i(a_n) \) for all \( n \). For sake of contradiction, suppose that \( \lambda > \alpha \), i.e. there exists an \( n \in \mathbb{N} \) such that \( a_n \geq \lambda + \frac{1}{N} \) for a.a. \( n \). The assumption that \( \lambda \leq i(a_k) \) implies that \( \lambda \leq a_k + \frac{1}{N} \) for a.a. \( n \). Because \( \{a_k\} \) is Cauchy, we may conclude there exists \( M \in \mathbb{N} \) such that
\[
    \lambda \leq a_k + \frac{1}{2N} \quad \text{for all } n,k \geq M.
\]

By making \( M \) even larger if necessary, we may assume that \( \lambda_n \geq a_n + \frac{1}{N} \) for all \( n \geq M \) as well. From these two inequalities with \( k = n \geq M \) we learn
\[
    a_n + \frac{1}{N} \leq \lambda_n \leq a_n + \frac{1}{2N} \implies \frac{1}{2N} \geq \frac{1}{N}
\]
and we have reached the desired contradiction. The fact that \( i(a_k) \leq \lambda \) for all \( k \) implies \( \alpha \leq \lambda \) is proved similarly. Alternatively if \( i(a_k) \leq \lambda \) then \( -\lambda \leq i(-a_k) \) which implies \( -\lambda \leq -\alpha \), i.e. \( \alpha \leq \lambda \).

With these results in hand, let us now show that \( \mathbb{R} \) as defined in Theorem 3.6 has the least upper bound property.

**Proof of the least upper bound property.** So suppose that \( \Lambda \subset \mathbb{R} \) is a non empty set which is bounded from above. For each \( m \in \mathbb{N} \), let \( k_m \in \mathbb{Z} \) be the smallest integer such that \( i(a_m) := i(b_{k_m}) \) is an upper bound for \( \Lambda \). Since, for all \( n \geq m \), \( a_m - 2^{-m} \leq a_n \leq a_m \), we may conclude that
\[
    |a_n - a_m| \leq 2^{-\min(n,m)} \to 0 \quad \text{as } n,m \to \infty.
\]
This shows \( \{a_n\}_{n=1}^{\infty} \) is Cauchy and hence we defined an element \( \alpha := \lim_{n \to \infty} a_n \) \( \in \mathbb{R} \). We now will show \( \alpha = \sup \Lambda \).

3.6 (Optional) Proofs of Theorem 3.6 and Theorem 3.3

If \( \lambda \in \Lambda \), then \( \lambda \leq i(a_n) \) for all \( n \) and so by Proposition 3.44 we conclude that \( \lambda \leq \alpha \), i.e. \( \alpha \) is an upper bound for \( \Lambda \). Now suppose that \( \beta \) is another upper bound for \( \Lambda \). As \( i(a_n - 2^{-n}) \) is not an upper bound for \( \Lambda \) there exists \( \lambda \in \Lambda \) such that
\[
    i(a_n - 2^{-n}) < \lambda \leq \beta.
\]

So by another application of Proposition 3.44 we learn that
\[
    \alpha = \lim_{n \to \infty} a_n = \lim_{n \to \infty} (a_n - 2^{-n}) \leq \beta.
\]

This shows that \( \alpha \) is in fact the least upper bound for \( \Lambda \).

**Theorem 3.45 (Real numbers are unique).** Suppose that \( \mathbb{F} \) and \( \mathbb{G} \) are two complete ordered fields. Then there is a unique order preserving isomorphism, \( \varphi : \mathbb{F} \to \mathbb{G} \).

**Sketch.** Suppose that \( \varphi : \mathbb{F} \to \mathbb{G} \) is an order preserving homomorphism. The usual arguments show that any homomorphism, \( \varphi : \mathbb{F} \to \mathbb{G} \) must satisfy \( \varphi(q \cdot 1_F) = q \cdot 1_G \). We know that \( \{q \cdot 1_F : q \in \mathbb{Q}\} \) and \( \{q \cdot 1_G : q \in \mathbb{Q}\} \) are dense copies of \( \mathbb{Q} \) inside of \( \mathbb{F} \) and \( \mathbb{G} \) respectively. Now for general \( a \in \mathbb{F} \) choose \( q_n, p_n \in \mathbb{Q} \) such that \( q_n \cdot 1_F \uparrow a \) and \( p_n \cdot 1_F \downarrow a \). Since \( \varphi \) is order preserving we must have \( q_n \cdot 1_G = \varphi(q_n \cdot 1_F) \) is increasing and \( p_n \cdot 1_G = \varphi(p_n \cdot 1_F) \) is decreasing. Moreover, since \( p_n \cdot 1_F \to 0 \) we must have \( \lim_{n \to \infty} \varphi(q_n \cdot 1_F) = \lim_{n \to \infty} \varphi(p_n \cdot 1_F) \). Since \( \varphi(q_n \cdot 1_F) \leq \varphi(a) \leq \varphi(p_n \cdot 1_F) \) for all \( n \) it then follows that \( \varphi(a) = \lim_{n \to \infty} q_n \cdot 1_G = \lim_{n \to \infty} p_n \cdot 1_G \) and we have shown \( \varphi \) is uniquely determined.

For the converse, if \( q_n \in \mathbb{Q} \) we know that
\[
    |q_n \cdot 1_F - q_m \cdot 1_F| = |q_n - q_m| \cdot 1_F \text{ and }
    |q_n \cdot 1_G - q_m \cdot 1_G| = |q_n - q_m| \cdot 1_G.
\]
Thus if \( \{q_n \cdot 1_F\}_{n=1}^{\infty} \) is convergent in \( \mathbb{F} \) iff \( \{q_n \cdot 1_G\}_{n=1}^{\infty} \) is convergent in \( \mathbb{G} \). Thus for any \( a \in \mathbb{F} \) we choose \( q_n \in \mathbb{Q} \) such that \( q_n \cdot 1_F \uparrow a \) and then define \( \varphi(a) := \lim_{n \to \infty} q_n \cdot 1_G \). One now checks that this formula is well defined (independent of the choice of \( q_n \) \( \subset \mathbb{Q} \) that \( q_n \cdot 1_F \uparrow a \)) and defines an order preserving isomorphism. For example, if \( a \leq b \) we may choose \( q_n \subset \mathbb{Q} \) and \( p_n \subset \mathbb{Q} \) such that \( q_n \cdot 1_F \uparrow a \) and \( p_n \cdot 1_F \downarrow b \). Then \( q_n \cdot 1_G \leq p_n \cdot 1_G \) for all \( n \) and letting \( n \to \infty \) shows,
\[
    \varphi(a) = \lim_{n \to \infty} q_n \cdot 1_G \leq \lim_{n \to \infty} p_n \cdot 1_G = \varphi(b).
\]

The other properties of \( \varphi \) are proved similarly.
Algebraic Properties of Complex Numbers

Definition 4.1 (Complex Numbers). Let \( \mathbb{C} = \mathbb{R}^2 \) equipped with multiplication rule
\[
(a, b)(c, d) \equiv (ac - bd, bc + ad)
\]
and the usual rule for vector addition. As is standard we will write \( 0 = (0, 0), \)
\( 1 = (1, 0) \) and \( i = (0, 1) \) so that every element \( z \in \mathbb{C} \) may be written as \( z = x + yi \) which in the future will be written simply as \( z = x + iy \). If \( z = x + iy \),
let \( \text{Re} \; z = x \) and \( \text{Im} \; z = y \).

Writing \( z = a + ib \) and \( w = c + id \), the multiplication rule in Eq. (4.1) becomes
\[
(a + ib)(c + id) \equiv (ac - bd) + i(bc + ad)
\]
and in particular \( 1^2 = 1 \) and \( i^2 = -1 \).

Proposition 4.2. The complex numbers \( \mathbb{C} \) with the above multiplication rule satisfies the usual definitions of a field – see Definition 2.1. For example \( z^2 \) and in particular \( 1 \) has a multiplicative inverse given by
\[
z^{-1} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}.
\]
Moreover \( \mathbb{R} \) as sub-field under the identification
\[
\mathbb{R} \ni a \rightarrow a1 + 0i = (a, 0) \in \mathbb{C}.
\]

Proof. Suppose \( z = a + ib \neq 0 \), we wish to find \( w = c + id \) such that \( zw = 1 \) and this happens by Eq. (4.2) iff
\[
ac - bd = 1 \quad \text{and} \quad \quad \text{bc} + ad = 0.
\]
Solving these equations as follows
\[
a(4.4) \quad \quad \quad \rightarrow \quad (a^2 + b^2) \; c = a \quad \rightarrow \quad \text{Re} \; w = c = \frac{a}{a^2 + b^2}
\]
\[
b(4.5) \quad \quad \quad \rightarrow \quad (a^2 + b^2) \; d = -b \quad \rightarrow \quad \text{Im} \; w = d = -\frac{b}{a^2 + b^2}.
\]
gives implies the result in Eq. (4.3).

Probably the most painful thing to check directly is the associative law, namely that \( z_1z_2z_3 = z_1[z_2z_3] \) for all \( z_1, z_2, z_3 \in \mathbb{C} \). This is equivalent to showing for all \( a, b, u, v, x, y \in \mathbb{R} \) that
\[
[(a + ib)(u + iv)](x + iy) = (a + ib)[(u + iv)(x + iy)].
\]
We do this by working out both sides as follows;
\[
LHS = [(au - bv) + i(au + bv)](x + iy) = (au - bv)x - (av + bu)y + i[(av + bu)x + (au - bv)y];
\]
\[
RHS = (a + ib)[(ux - vy) + i(uy + vx)] = a(ux - vy) - b(uy + vx) + i[b(ux - vy) + a(uy + vx)].
\]
The reader should now easily see that both of these expressions are in fact equal. The remaining axioms of a field are checked similarly. \( \blacksquare \)

Notation 4.3 We will write \( 1/z \) for \( z^{-1} \) and \( w/z \) to mean \( z^{-1} \cdot w \).

Notation 4.4 (Conjugation and Modulous) If \( z = a + ib \) with \( a, b \in \mathbb{R} \) let \( \bar{z} = a - ib \) and
\[
|z|^2 \equiv z\bar{z} = a^2 + b^2.
\]
Notice that
\[
\text{Re} \; z = \frac{1}{2} (z + \bar{z}) \quad \text{and} \quad \text{Im} \; z = \frac{1}{2i} (z - \bar{z}).
\]

Proposition 4.5. Complex conjugation and the modulus operators satisfy:
1. \( \bar{\bar{z}} = z \),
2. \( \overline{zw} = \bar{z}\bar{w} \) and \( \bar{z} + \bar{w} = \bar{z + w} \),
3. \( |z| = |\bar{z}| \),
4. \( |zw| = |z||w| \) and in particular \( |z^n| = |z|^n \) for all \( n \in \mathbb{N} \),
5. \( \text{Re} \; z \leq |z| \) and \( |\text{Im} \; z| \leq |z| \),
6. \( |z + w| \leq |z| + |w| \).
7. If \( z = 0 \) iff \( |z| = 0 \).
8. If \( z \neq 0 \) then
\[
    z^{-1} := \frac{\bar{z}}{|z|^2}
\]
(also written as \( \frac{1}{z} \)) is the inverse of \( z \).
9. \(|z^{-1}| = |z|^{-1}\) and more generally \(|z^n| = |z|^n\) for all \( n \in \mathbb{Z} \).

**Proof.** 1. and 3. are geometrically obvious as well as easily verified.
2. Say \( z = a + ib \) and \( w = c + id \), then \( \bar{z}w \) is the same as \( zw \) with \( b \) replaced by \(-b\) and \( d \) replaced by \(-d\), and looking at Eq. 4.5 we see that
\[
    \bar{z}w = (ac - bd) - i(bc + ad) = \overline{zw}.
\]

4. \(|zw|^2 = zw\bar{w} = \bar{z}w\bar{w} = |z|^2|w|^2\) as real numbers and hence \(|zw| = |z||w|\).
5. Geometrically obvious or also follows from
\[
    |z| = \sqrt{|\text{Re}\, z|^2 + |\text{Im}\, z|^2}.
\]
6. This is the triangle inequality which may be understood geometrically or by the computation
\[
    |z + w|^2 = (z + w)(\bar{z} + \bar{w}) = |z|^2 + |w|^2 + \bar{z}\bar{w} + \bar{z}w
= |z|^2 + |w|^2 + 2\overline{w} \Re\, (\bar{z}w) \leq |z|^2 + |w|^2 + 2|z||w|
= ((|z| + |w|)^2.
\]
7. Obvious.
8. Follows from Eq. 4.5. Alternatively if \( \rho = \rho + i0 > 0 \) is a real number then \( \rho^{-1} = \rho^{-1} + i0 \) as is easily verified since \( \mathbb{R} \) is a sub-field of \( \mathbb{C} \). Thus since \( \bar{z}z = |z|^2 \) we find
\[
    \frac{1}{|z|^2} \bar{z}z = \frac{1}{|z|^2} |z|^2 = 1 \implies z^{-1} = \frac{1}{|z|^2} \bar{z} = \frac{\Re\, z}{|z|^2} - \frac{i}{|z|^2} \Im\, z.
\]
9. \(|z|^{-1} = \left| \frac{\bar{z}}{|z|^2} \right| = \left| \frac{1}{|z|^2} \right| |\bar{z}| = \frac{1}{|z|}.

**Corollary 4.6.** If \( w, z \in \mathbb{C} \), then
\[
    |z| - |w| \leq |z - w|.
\]

**Proof.** Just copy the proof of Lemma 4.6.

**Lemma 4.7.** For complex number \( u, v, w, z \in \mathbb{C} \) with \( v \neq 0 \neq z \), we have
\[
    \frac{1}{u/v} = \frac{1}{uv}, \text{ i.e. } u^{-1}v^{-1} = (uv)^{-1}
\]
\[
    \frac{u \cdot v}{v \cdot z} = \frac{uv}{vz}
\]
and
\[
    \frac{u + w}{v + z} = \frac{u + w}{vz}.
\]

**Proof.** For the first item, it suffices to check that
\[
    (uv)(u^{-1}v^{-1}) = u^{-1}u = 1.
\]
The rest follow using
\[
    \frac{uv}{vz} = \frac{uv}{z} = \frac{u}{v} + \frac{w}{z} = \frac{zu}{vz} + \frac{vw}{vz} = (vz)^{-1} (zu + vw) = \frac{uz + vw}{vz}.
\]

### 4.1 A Matrix Perspective (Optional)

Here is a way to understand some of the basic properties of \( \mathbb{C} \) using your knowledge of linear algebra. Let \( M_z : \mathbb{C} \rightarrow \mathbb{C} \) denote multiplication by \( z = a + ib \).

We now identify \( \mathbb{C} \) with \( \mathbb{R}^2 \) by
\[
    \mathbb{C} \ni c + id \cong \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{R}^2.
\]

Using this identification, the product formula
\[
    zw = (ac - bd) + i (bc + ad),
\]
becomes
\[
    M_z w = \begin{pmatrix} ac - bd \\ bc + ad \end{pmatrix} = \begin{pmatrix} a - b \\ b \ a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix}
\]
so that
\[
    M_z = \begin{pmatrix} a - b \\ b \ a \end{pmatrix} = aI + bJ
\]
where
\[
    J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
\]

We now have the following simple observations:
1. \( J^2 = -I \) and \( J^{tr} = -J \),
2. \( M_z M_w = M_w M_z \) because \( J \) and \( I \) commute,
3. we have
\[
M_z M_w = (a I + b J) (c I + d J) = (ac - bd) I + (ad + bc) J = M_{zw},
\]
4. the associativity of complex multiplication follows from the associativity properties of matrix multiplication,
5. \( M_{z}^{tr} = a I - b J = M_{z} \) and in particular
6. \( M_{zw}^{tr} = (M_z M_w)^{tr} = M_w^{tr} M_z^{tr} = M_{w} M_{z} = M_{wz} \),
7. \( M_{z}^{tr} M_{z} = M_{zz} = M_{zz} \) for \( |z|^{2} = \det (M_{z}) \),
8. \( |w z| = \det (M_{wz}) = \det (M_{w} M_{z}) = \det (M_{w}) \det (M_{z}) = |w| |z| \),
9. \( M_z \) is invertible iff \( \det (M_z) \neq 0 \) which happens iff \( |z|^{2} \neq 0 \) and in this case we know from basic linear algebra that
\[
M_{z}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \frac{1}{|z|^{2}} M_{z}^{tr} = M_{|z|^{2} z},
\]
10. With this notation we have \( M_z M_w = M_{zw} \) and since \( I \) and \( J \) commute it follows that \( zw = wz \). Moreover, since matrix multiplication is associative so is complex multiplication. Also notice that \( M_z \) is invertible iff \( \det M_z = a^2 + b^2 = |z|^2 \neq 0 \) in which case
\[
M_{z}^{-1} = \frac{1}{|z|^{2}} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = M_{z/|z|^2},
\]
as we have already seen above.
Limits, Continuity, and Compactness in \( \mathbb{C} \)

**Definition 5.1.** A sequence \( \{z_n\}_{n=1}^{\infty} \subset \mathbb{C} \) is **Cauchy** if \(|z_n - z_m| \to 0\) as \( m, n \to \infty \) and is **convergent** to \( z \in \mathbb{C} \) if \(|z - z_n| \to 0\) as \( n \to \infty \). As usual if \( \{z_n\}_{n=1}^{\infty} \) converges to \( z \) we will write \( z_n \to z \) as \( n \to \infty \) or \( z = \lim_{n \to \infty} z_n \).

**Theorem 5.2.** The complex numbers are complete, i.e., all Cauchy sequences are convergent.

**Proof.** This follows from the completeness of real numbers and the easily proved observations that if \( z_n = a_n + ib_n \in \mathbb{C} \), then
1. \( \{z_n\}_{n=1}^{\infty} \subset \mathbb{C} \) is Cauchy iff \( \{a_n\}_{n=1}^{\infty} \subset \mathbb{R} \) and \( \{b_n\}_{n=1}^{\infty} \subset \mathbb{R} \) are Cauchy and
2. \( z_n \to z = a + ib \) as \( n \to \infty \) iff \( a_n \to a \) and \( b_n \to b \) as \( n \to \infty \).

The complex numbers satisfy all the same limit theorems as the real numbers.

**Exercise 5.2.** Show the following functions are continuous on \( \mathbb{C} \):
1. \( f(z) = c \) for all \( z \in \mathbb{C} \) where \( c \in \mathbb{C} \) is a constant.
2. \( f(z) = |z| \).
3. \( f(z) = z \) and \( f(z) = \bar{z} \).
4. \( f(z) = \Re z \) and \( f(z) = \Im z \).
5. \( f(z) = \sum_{m,n=0}^{\infty} a_{m,n} z^m \bar{z}^n \) where \( a_{m,n} \in \mathbb{C} \).

**Exercise 5.3.** Suppose that \( X \) and \( Y \) are subsets of \( \mathbb{C} \) and \( f : X \to \mathbb{C} \) and \( g : Y \to \mathbb{C} \) are functions such that \( f(z) \in Y \) for all \( z \in X \). In this case, we may define the composite function, \( g \circ f : X \to \mathbb{C} \), by \( g \circ f(z) := g(f(z)) \). Show \( g \circ f \) is continuous if both \( f \) and \( g \) are continuous.

**Theorem 5.5.** Suppose that \( f : X \to \mathbb{C} \) is a function, then \( f \) is continuous at \( x \in X \) iff for all \( \varepsilon > 0 \) there exists \( \delta = \delta(\varepsilon) > 0 \) such that \(|f(x) - f(y)| \leq \varepsilon \) for all \( y \) such that \(|y - x| \leq \delta \).

**Proof.** (\( \Rightarrow \)) Suppose that \( \{z_n\} \subset \mathbb{C} \) such that \( z_n \to z \) in \( X \). For each \( \delta > 0 \) there exists \( N = N(\delta) \) such that \(|z_n - z| \leq \delta\) for all \( n \geq N \). Therefore \(|f(z_n) - f(z)| \leq \varepsilon \) for all \( n \geq N = N(\delta(\varepsilon)) \) and therefore \( \lim_{n \to \infty} f(z_n) = f(z) \).

(\( \Leftarrow \)) If there exists \( \varepsilon > 0 \) such that for all \( \delta > 0 \) there exists \( z_\delta \in X \) with \(|z_\delta - z| \leq \delta \) with \(|f(z_\delta) - f(z)| \geq \varepsilon \), then taking \( z_n := z_1/n \), we learn that \( \lim_{n \to \infty} f(z_n) \neq f(z) \).

**Exercise 5.4 (Continuity).** Let \( X \) be a non-empty subset of \( \mathbb{C} \) and \( f : X \to \mathbb{C} \) be a function. We say \( f \) is **continuous at** \( z \in X \) if
\[
\lim_{n \to \infty} f(z_n) = f(z) \quad \text{for all } \{z_n\}_{n=1}^{\infty} \subset X \text{ with } \lim_{n \to \infty} z_n = z.
\]
We say \( f \) is **continuous on** \( X \) if it is continuous at all points in \( X \).

**Exercise 5.1.** Suppose that \( X \) is a subset of \( \mathbb{C} \) and \( f,g : X \to \mathbb{C} \) are two continuous functions on \( X \). Show:
1. \( f + g \) is continuous,
2. \( f \cdot g \) is continuous,
3. \( f/g \) is continuous provided \( g(z) \neq 0 \) for all \( z \in X \). In particular, \( 1/z \) is continuous on \( \mathbb{C} \setminus \{0\} \).
Lemma 5.8. We refer to

Indeed, just check that

Moreover, show that

Exercise 5.5 (Differentiability of \(x^{1/m}\)). Show for each \(m \in \mathbb{N}\) that the function 

is closed. Indeed, just check that

Exercise 5.6 (Intermediate value theorem). Suppose that \(-\infty < a < b < \infty\) and \(f : [a, b] \to \mathbb{R}\) is a continuous function such that \(f(a) < 0\) and \(f(b) > 0\). Let \(S := \{t \in [a, b] : f(t) \leq 0\}\) and let \(c := \sup(S)\). Show \(c \in (a, b)\) and \(f(c) = 0\).

5.1 Closed and open subsets

Definition 5.7. A subset \(A \subseteq \mathbb{C}\) is closed if it is closed under taking limits, i.e. for all sequences \((z_n)_{n=1}^{\infty}\) in \(A\) which are convergent in \(\mathbb{C}\), satisfy \(\lim_{n \to \infty} z_n \in A\).

Lemma 5.8. If \(f : \mathbb{C} \to \mathbb{R}\) is a continuous function and \(k \in \mathbb{R}\), then the following sets are closed,

\[ A := \{z \in \mathbb{C} : f(z) \leq k\} , \quad B := \{z \in \mathbb{C} : f(z) = k\} , \quad \text{and} \quad C := \{z \in \mathbb{C} : f(z) \geq k\} \]

are closed.

Proof. The proof that \(A, B,\) and \(C\) are closed all go the same way so let me just check that \(A\) is closed. To this end, suppose that \((z_n)_{n=1}^{\infty}\) is a sequence in \(A\) such that \(z := \lim_{n \to \infty} z_n\) exists in \(\mathbb{C}\). Since \(z_n \in A\), \(f(z_n) \leq k\) and therefore,

\[ k \geq \lim_{n \to \infty} f(z_n) = f(z) \]

wherein the last equality we have used the definition of \(f\) being continuous. By definition of \(A\) it then follows that \(z \in A\) and so we have checked that \(A\) is closed. \(\blacksquare\)

Example 5.9 (Closed Balls). For \(z \in \mathbb{C}\) and \(\rho > 0\), then the ball

is closed. Indeed, just check that \(f(w) = |w - z|\) is continuous and then apply Lemma 5.8. We refer to \(C_z(\rho)\) as the closed ball in \(\mathbb{C}\) centered at \(z\) with radius \(\rho\). Notice that \(\{z\} = C_z(0)\) is a closed set for all \(z \in \mathbb{C}\).

Exercise 5.9. Show that \(B_z(\rho)\) is open in \(\mathbb{C}\) for all \(z \in \mathbb{C}\) and \(\rho > 0\).

Exercise 5.10. Let \(U\) be a subset of \(\mathbb{C}\). Show the following are equivalent;

1. \(U\) is open,
2. for all \(z \in U\) there exists \(\rho > 0\) such that \(B_z(\rho) \subseteq U\).
3. \(U\) can be written as a union of open balls.

Exercise 5.11. Show \(U := \mathbb{C} \setminus \{z_0\}\) is open for any \(z_0 \in \mathbb{C}\). More generally, show that \(U := \mathbb{C} \setminus S\) is open for all whenever \(S\) is a finite subset of \(\mathbb{C}\).
5.2 Compactness

Definition 5.15. As subset $K \subset \mathbb{C}$ is *(sequentially) compact* if every sequence $\{z_n\}_{n=1}^{\infty} \subset K$ has a convergent subsequence, $\{w_k := z_{n_k}\}_{k=1}^{\infty}$ such that $\lim_{k \to \infty} w_k = K$.

Example 5.16. Suppose that $F \subset \mathbb{C}$ is an unbounded set, i.e., for all $n \in \mathbb{N}$ there exists $z_n \in F$ such that $|z_n| \geq n$. The sequence $\{z_n\}_{n=1}^{\infty}$ and all of its subsequences are unbounded and therefore not Cauchy in $\mathbb{C}$ and hence not convergent in $\mathbb{C}$. This shows that compact sets must be bounded.

Example 5.17. Suppose that $F \subset \mathbb{C}$ is not closed. Then there exists $\{z_n\}_{n=1}^{\infty} \subset F$ such that $z := \lim_{n \to \infty} z_n \notin F$. Moreover, although every subsequence of $\{z_n\}_{n=1}^{\infty}$ is convergent, they all still converge to $z \notin F$. This shows that a compact set must be closed.

Lemma 5.18 (Bolzano–Weierstrass property). Every bounded sequence, $\{z_n\}_{n=1}^{\infty} \subset \mathbb{C}$, has a convergent subsequence.

Proof. By assumption there exists $M < \infty$ such that $|z_n| \leq M$ for all $n \in \mathbb{N}$. Writing $z_n = a_n + ib_n$ with $a_n, b_n \in \mathbb{R}$ we may conclude that $|a_n|, |b_n| \leq M$. According to Corollary 5.31 there exists an increasing function $N \ni k \to n_k \in \mathbb{N}$ such that $\lim_{k \to \infty} a_{n_k} = A$ exists. Similarly, we can apply Corollary 5.31 again to find an increasing function $N \ni l \to k_l \in \mathbb{N}$ such that $\lim_{l \to \infty} b_{n_{k_l}} = B$ exists. We now let $w_l := z_{n_{k_l}}$ for $l \in \mathbb{N}$. Then $\{w_l\}_{l=1}^{\infty}$ is a subsequence of $\{z_n\}_{n=1}^{\infty}$ which is convergent to $A + iB \in \mathbb{C}$. Indeed,

$$|w_l - (A + iB)| = |a_{n_{k_l}} - A + i(b_{n_{k_l}} - B)| \leq |a_{n_{k_l}} - A| + |b_{n_{k_l}} - B| \to 0$$

as $l \to \infty$.

Theorem 5.19 (Bolzano–Weierstrass / Heine–Borel theorem). As subset $K \subset \mathbb{C}$ is compact if and only if it is closed and bounded.

Proof. In light of Examples 5.16 and 5.17 we are left to show that closed and bounded sets are compact. So let $K \subset \mathbb{C}$ be a closed and bounded set and $\{z_n\}_{n=1}^{\infty}$ be any sequence in $K$. According to Lemma 5.18 below, $\{z_n\}_{n=1}^{\infty}$ has a convergent subsequence, $\{w_k := z_{n_k}\}_{k=1}^{\infty}$. Since $w_k \in K$ for all $k$ and $K$ is closed it necessarily follows that $\lim_{k \to \infty} w_k \in K$ which shows $K$ is compact.

Exercise 5.12 (Extreme value theorem). Let $K$ be compact subset of $\mathbb{C}$ and $f : K \to \mathbb{R}$ be a continuous function. Show $-\infty < \inf f \leq \sup f < \infty$ and there exists $a, b \in K$ such that $f(a) = \inf f$ and $f(b) = \sup f$. Hint: first show there exists $\{z_n\}_{n=1}^{\infty} \subset K$ such that $f(z_n) \uparrow \sup f$ as $n \to \infty$.

Exercise 5.13 (Uniform Continuity). Let $K$ be compact subset of $\mathbb{C}$ and $f : K \to \mathbb{C}$ be a continuous function. Show that $f$ is uniformly continuous, i.e. if $\varepsilon > 0$ there exists $\delta > 0$ such that $|f(z) - f(w)| < \varepsilon$ if $w, z \in K$ with $|w - z| < \delta$. Hint: prove the contrapositive.

Exercise 5.14. If $K \subset \mathbb{C}$ is compact and $C \subset K$ is closed, then $C$ is compact.

Exercise 5.15. If $K \subset \mathbb{R}$ is compact then $\sup (K) \in K$.

Exercise 5.16. If $K \subset \mathbb{C}$ is compact and $f : K \to \mathbb{C}$ is continuous, then $f(K)$ is compact. In particular, for $C \subset K$ closed, we have $f(C)$ is closed and in fact compact in $\mathbb{C}$.

Exercise 5.17. Let $f : [a, b] \to [c, d]$ be a strictly increasing continuous function such that $f(a) = c$ and $f(b) = d$. Then $f$ is bijective and $g := f^{-1} : [c, d] \to [a, b]$ is continuous.

5.3 Uniform Convergence

Definition 5.20 (Uniform Convergence). Let $D$ be a subset of $\mathbb{C}$, $f : D \to \mathbb{C}$ and, for each $n \in \mathbb{N}$, $f_n : D \to \mathbb{C}$ be functions. We say that $f_n \to f$ uniformly if

$$\delta_n := \sup_{z \in D} |f(z) - f_n(z)| \to 0$$

as $n \to \infty$.

The next theorem is a basic fact about uniform convergence which does not hold in general for pointwise convergence. The proof of this theorem is a bit subtle but well worth mastering as the method will arise over and over again.

Theorem 5.21 (Uniform Convergence Preserves Continuity). If $\{f_n\}_{n=1}^{\infty}$ are continuous functions from $D \subset \mathbb{C}$ to $\mathbb{C}$ such that $f_n \to f : D \to \mathbb{C}$ uniformly, then $f$ is continuous.

Proof. We must show $\lim_{k \to \infty} f(z_k) = f(z)$ whenever $\{z_k\}_{k=1}^{\infty} \subset D$ is a convergent sequence such that $z := \lim_k z_k \in D$. So assume we are given such a sequence $\{z_k\}_{k=1}^{\infty}$. Then for any $n \in \mathbb{N}$ we have,

$$|f(z) - f(z_k)| = ||f(z) - f_n(z)| + |f_n(z) - f_n(z_k)| + |f_n(z_k) - f(z_k)||$$

$$\leq |f(z) - f_n(z)| + |f_n(z) - f_n(z_k)| + |f_n(z_k) - f(z_k)|$$

$$\leq \delta_n + |f_n(z) - f_n(z_k)| + \delta_n = |f_n(z) - f_n(z_k)| + 2\delta_n$$

Therefore,

$$\limsup_{k \to \infty} |f(z) - f(z_k)| \leq \limsup_{k \to \infty} |f_n(z) - f_n(z_k)| + 2\delta_n = 2\delta_n$$
wherein we have used the continuity of $f_n$ for the last equality. Thus we have shown
\[
\limsup_{k \to \infty} |f(z) - f(z_k)| \leq 2\delta_n
\]
which upon passing to the limit as $n \to \infty$ shows \(\limsup_{k \to \infty} |f(z) - f(z_k)| = 0\). This suffices to show \(\lim_{k \to \infty} f(z_k) = f(z)\). \qed
Set Operations and Countability

Let \( \mathbb{N} \) denote the positive integers, \( \mathbb{N}_0 := \mathbb{N} \cup \{0\} \) be the non-negative integers and \( \mathbb{Z} = \mathbb{N}_0 \cup (-\mathbb{N}) \) – the positive and negative integers including 0, \( \mathbb{Q} \) the rational numbers, \( \mathbb{R} \) the real numbers (see Chapter ?? below), and \( \mathbb{C} \) the complex numbers. We will also use \( \mathbb{F} \) to stand for either of the fields \( \mathbb{R} \) or \( \mathbb{C} \).

**Notation 6.1** Given two sets \( X \) and \( Y \), let \( Y^X \) denote the collection of all functions \( f : X \to Y \). If \( X = \mathbb{N} \), we will say that \( f \in Y^\mathbb{N} \) is a sequence with values in \( Y \) and often write \( f_n \) for \( f(n) \) and express \( f \) as \( \{f_n\}_{n=1}^\infty \). If \( X = \{1, 2, \ldots, N\} \), we will write \( Y^N \) in place of \( Y^{\{1, 2, \ldots, N\}} \) and denote \( f \in Y^N \) by \( f = (f_1, f_2, \ldots, f_N) \) where \( f_n = f(n) \).

**Notation 6.2** More generally if \( \{X_\alpha : \alpha \in A\} \) is a collection of non-empty sets, let \( X_A = \prod_{\alpha \in A} X_\alpha \) and \( \pi_\alpha : X_A \to X_\alpha \) be the canonical projection map defined by \( \pi_\alpha(x) = x_\alpha \). If \( X_\alpha = X \) for some fixed space \( X \), then we will write \( \prod_{\alpha \in A} X_\alpha \) as \( X^A \) rather than \( X_A \).

Recall that an element \( x \in X_A \) is a “choice function,” i.e. an assignment \( x_\alpha := x(\alpha) \in X_\alpha \) for each \( \alpha \in A \). The axiom of choice (see Appendix ??) states that \( X_A \neq \emptyset \) provided that \( X_\alpha \neq \emptyset \) for each \( \alpha \in A \).

**Notation 6.3** Given a set \( X \), let \( 2^X \) denote the **power set** of \( X \) – the collection of all subsets of \( X \) including the empty set.

The reason for writing the power set of \( X \) as \( 2^X \) is that if we think of 2 meaning \( \{0, 1\} \), then an element of \( a \in 2^X = \{0, 1\}^X \) is completely determined by the set

\[
A := \{x \in X : a(x) = 1\} \subseteq X.
\]

In this way elements in \( \{0, 1\}^X \) are in one to one correspondence with subsets of \( X \).

For \( A \in 2^X \) let

\[
A^c := X \setminus A = \{x \in X : x \notin A\}
\]

and more generally if \( A, B \subseteq X \) let

\[
B \setminus A := \{x \in B : x \notin A\} = A \cap B^c.
\]

We also define the symmetric difference of \( A \) and \( B \) by

\[
A \triangle B := (B \setminus A) \cup (A \setminus B).
\]

As usual if \( \{A_\alpha\}_{\alpha \in I} \) is an indexed collection of subsets of \( X \) we define the union and the intersection of this collection by

\[
\cup_{\alpha \in I} A_\alpha := \{x \in X : \exists \alpha \in I \exists x \in A_\alpha\} \quad \text{and} \quad \cap_{\alpha \in I} A_\alpha := \{x \in X : x \in A_\alpha \forall \alpha \in I\}.
\]

**Notation 6.4** We will also write \( \prod_{\alpha \in I} A_\alpha \) for \( \cup_{\alpha \in I} A_\alpha \) in the case that \( \{A_\alpha\}_{\alpha \in I} \) are pairwise disjoint, i.e. \( A_\alpha \cap A_\beta = \emptyset \) if \( \alpha \neq \beta \).

Notice that \( \cup \) is closely related to \( \exists \) and \( \cap \) is closely related to \( \forall \). For example let \( \{A_n\}_{n=1}^\infty \) be a sequence of subsets from \( X \) and define

\[
\{A_n \ i.o.\} := \{x \in X : \# \{n : x \in A_n\} = \infty\} \quad \text{and} \quad \{A_n \ a.a.\} := \{x \in X : x \in A_n \forall n \text{ sufficiently large}\}.
\]

(One should read \( \{A_n \ i.o.\} \) as \( A_n \) infinitely often and \( \{A_n \ a.a.\} \) as \( A_n \) almost always.) Then \( x \in \{A_n \ i.o.\} \) iff

\[
\forall N \in \mathbb{N} \exists n \geq N \exists x \in A_n
\]

and this may be expressed as

\[
\{A_n \ i.o.\} = \cap_{n=1}^\infty \cup_{n \geq N} A_n.
\]

Similarly, \( x \in \{A_n \ a.a.\} \) iff

\[
\exists N \in \mathbb{N} \exists n \geq N \forall x \in A_n
\]

which may be written as

\[
\{A_n \ a.a.\} = \cup_{n=1}^\infty \cap_{n \geq N} A_n.
\]

**Definition 6.5.** A set \( X \) is said to be **countable** if is empty or there is an injective function \( f : X \to \mathbb{N} \), otherwise \( X \) is said to be **uncountable**.

**Lemma 6.6 (Basic Properties of Countable Sets).**
1. If \( A \subseteq X \) is a subset of a countable set \( X \) then \( A \) is countable.
2. Any infinite subset \( A \subseteq \mathbb{N} \) is in one to one correspondence with \( \mathbb{N} \).
3. A non-empty set \( X \) is countable iff there exists a surjective map, \( g : N \to X \).
4. If \( X \) and \( Y \) are countable then \( X \times Y \) is countable.
5. Suppose for each \( m \in \mathbb{N} \) that \( A_m \) is a countable subset of a set \( X \), then 
\( A = \bigcup_{m=1}^{\infty} A_m \) is countable. In short, the countable union of countable sets is still countable.
6. If \( X \) is an infinite set and \( Y \) is a set with at least two elements, then \( Y^X \) is uncountable. In particular \( 2^X \) is uncountable for any infinite set \( X \).

**Proof.** 1. If \( f : X \to N \) is an injective map then so is the restriction, \( f|A \), of \( f \) to the subset \( A \).
2. Let \( f(1) = \min A \) and define \( f \) inductively by 
\[
f(n + 1) = \min (A \setminus \{f(1), \ldots, f(n)\}).
\]
Since \( A \) is infinite the process continues indefinitely. The function \( f : N \to A \) defined this way is a bijection.
3. If \( g : N \to \mathbb{N} \) is a surjective map, let 
\[
f(x) = \min g^{-1}([x]) = \min \{n \in \mathbb{N} : f(n) = x\}.
\]
Then \( f : X \to \mathbb{N} \) is injective which combined with item 2. (taking \( A = f(X) \)) shows \( X \) is countable. Conversely if \( f : X \to \mathbb{N} \) is injective let \( x_0 \in X \) be a fixed point and define \( g : N \to X \) by 
\[
g(n) = f^{-1}(n) \quad \text{for } n \in f(X) \text{ and } g(n) = x_0 \quad \text{otherwise}.
\]
4. Let us first construct a bijection, \( h \), from \( N \) to \( N \times N \). To do this put the elements of \( N \times N \) into an array of the form
\[
\begin{pmatrix}
(1,1) & (1,2) & (1,3) & \ldots \\
(2,1) & (2,2) & (2,3) & \ldots \\
(3,1) & (3,2) & (3,3) & \ldots \\
& \vdots & \vdots & \ddots
\end{pmatrix}
\]
and then “count” these elements by counting the sets \( \{(i,j) : i+j=k\} \) one at a time. For example let \( h(1) = (1,1), \ h(2) = (2,1), \ h(3) = (1,2), \ h(4) = (3,1), \ h(5) = (2,2), \ h(6) = (1,3) \) and so on. If \( f : N \to X \) and \( g : N \to Y \) are surjective functions, then the function \( (f \times g) \circ h : N \to X \times Y \) is surjective where \( (f \times g) (m,n) := (f(m),g(n)) \) for all \((m,n) \in \mathbb{N} \times \mathbb{N} \).
5. If \( A = \emptyset \) then \( A \) is countable by definition so we may assume \( A \neq \emptyset \). With out loss of generality we may assume \( A_1 \neq \emptyset \) and by replacing \( A_m \) by \( A_1 \) if necessary we may also assume \( A_m \neq \emptyset \) for all \( m \). For each \( m \in \mathbb{N} \) let \( a_m : N \to A_m \) be a surjective function and then define \( f : N \times N \to \bigcup_{m=1}^{\infty} A_m \) by 
\[
f(m,n) := a_m(n). \quad \text{The function } f \text{ is surjective and hence so is the composition, } f \circ h : N \to \bigcup_{m=1}^{\infty} A_m, \text{ where } h : N \to N \times N \text{ is the bijection defined above.}
\]
6. Let us begin by showing \( 2^N = \{0,1\}^N \) is uncountable. For sake of contradiction suppose \( f : N \to \{0,1\}^N \) is a surjection and write \( f(n) = (f_1(n), f_2(n), f_3(n), \ldots) \). Now define \( a \in \{0,1\}^N \) by \( a_n := 1 - f_n(n) \). By construction \( f_n(n) \neq a_n \) for all \( n \) and so \( a \notin f(N) \). This contradicts the assumption that \( f \) is surjective and shows \( 2^N \) is uncountable. For the general case, since \( Y_0^X \subset Y^X \) for any subset \( Y_0 \subset Y \), if \( Y_0^X \) is uncountable then so is \( Y^X \). In this way we may assume \( Y_0 \) is a two point set which may as well be \( Y_0 = \{0,1\} \). Moreover, since \( X \) is an infinite set we may find an injective map \( i : N \to X \) and use this to set up an injection, \( i : 2^N \to 2^X \) by setting \( i(A) := \{x_n : n \in \mathbb{N}\} \subset X \) for all \( A \subset \mathbb{N} \). If \( 2^X \) were countable we could find a surjective map \( f : 2^X \to N \) in which case \( f \circ i : 2^N \to N \) would be surjective as well. However this is impossible since we have already seen that \( 2^N \) is uncountable.

**Corollary 6.7.** The set \( \{0,1\} : 0 < a < 1 \) is uncountable while \( \mathbb{Q} \cap (0,1) \) is countable.

**Proof.** From Section 3.4 the set \( \{0,1,2,\ldots,8\}^N \) can be mapped injectively into \( (0,1) \) and therefore it follows from Lemma 6.6 that \( (0,1) \) is uncountable. For each \( m \in \mathbb{N} \), let \( A_m := \{n \in \mathbb{N} : n < m\} \). Since \( \mathbb{Q} \cap (0,1) = \bigcup_{m=1}^{\infty} A_m \) and \( # (A_m) < \infty \) for all \( m \), another application of Lemma 6.6 shows \( \mathbb{Q} \cap (0,1) \) is countable.

We end this section with some notation which will be used frequently in the sequel.

**Notation 6.8.** If \( f : X \to Y \) is a function and \( \mathcal{E} \subset 2^X \) let 
\[
f^{-1}(\mathcal{E}) := \{f^{-1}(E) : E \in \mathcal{E}\}.
\]
If \( \mathcal{G} \subset 2^X \), let 
\[
f_\mathcal{G} := \{A \in 2^X : f^{-1}(A) \in \mathcal{G}\}.
\]

**Definition 6.9.** Let \( \mathcal{E} \subset 2^X \) be a collection of sets, \( A \subset X, \ i_A : A \to X \) be the inclusion map \( i_A(x) = x \) for all \( x \in A \) and 
\[
\mathcal{E}_A = i_A^{-1}(\mathcal{E}) := \{A \cap E : E \in \mathcal{E}\}.
\]

### 6.1 Exercises

Let \( f : X \to Y \) be a function and \( \{A_i\}_{i \in I} \) be an indexed family of subsets of \( Y \), verify the following assertions.
Exercise 6.1. $(\cap_{i \in I} A_i)^c = \cup_{i \in I} A_i^c$.

Exercise 6.2. Suppose that $B \subset Y$, show that $B \setminus (\cup_{i \in I} A_i) = \cap_{i \in I} (B \setminus A_i)$.

Exercise 6.3. $f^{-1}(\cup_{i \in I} A_i) = \cup_{i \in I} f^{-1}(A_i)$.

Exercise 6.4. $f^{-1}(\cap_{i \in I} A_i) = \cap_{i \in I} f^{-1}(A_i)$.

Exercise 6.5. Find a counterexample which shows that $f(C \cap D) = f(C) \cap f(D)$ need not hold.

**Definition 6.10 (Algebraic Numbers).** A real number, $x \in \mathbb{R}$, is called algebraic number, if there is an $n \in \mathbb{N}$, a polynomial, $p(t) = \sum_{k=0}^{n} a_k t^k$ with $a_k \in \mathbb{Q}$, such that $a_n = 1$, and $p(x) = 0$. [That is to say, $x \in \mathbb{R}$ is algebraic if it is the root of a non-trivial polynomial with coefficients from $\mathbb{Q}$.]

Note that for all $q \in \mathbb{Q}$, $p(t) := t - q$ satisfies $p(q) = 0$. Hence all rational numbers are algebraic. But there are many more algebraic numbers, for example $y^{1/n}$ is algebraic for all $y \geq 0$ and $n \in \mathbb{N}$.

Exercise 6.6. Show that the set of algebraic numbers is countable. [Hint: any polynomial of degree $n$ has at most $n$ – real roots.] In particular, “most” irrational numbers are not algebraic numbers, i.e. there is still any uncountable number of non-algebraic numbers.
Appendix: Notation and Logic

The following abbreviations along with their negations are used throughout these notes.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Negation</th>
</tr>
</thead>
<tbody>
<tr>
<td>∀</td>
<td>for all</td>
<td>∃</td>
</tr>
<tr>
<td>∃</td>
<td>there exists</td>
<td>∀</td>
</tr>
<tr>
<td>∈, or “space” then</td>
<td>∋</td>
<td>∈, or “space”</td>
</tr>
<tr>
<td>∋</td>
<td>such that</td>
<td>∈</td>
</tr>
<tr>
<td>a.a.</td>
<td>almost all</td>
<td>i.o.</td>
</tr>
<tr>
<td>i.o.</td>
<td>infinitely often</td>
<td>a.a.</td>
</tr>
<tr>
<td>=</td>
<td>equals</td>
<td>≠</td>
</tr>
<tr>
<td>≠</td>
<td>not equals</td>
<td>=</td>
</tr>
<tr>
<td>≤</td>
<td>less than or equal</td>
<td>&gt;</td>
</tr>
<tr>
<td>&gt;</td>
<td>greater than</td>
<td>≤</td>
</tr>
</tbody>
</table>

Here are some examples.

1. \( a_n = b_n \) i.o. \( n \) ⇐⇒ \# \( \{ n : a_n = b_n \} \) = \( \infty \). The negation of \# \( \{ n : a_n = b_n \} \) = \( \infty \) is \# \( \{ n : a_n = b_n \} \) < \( \infty \) ⇐⇒ \( a_n \neq b_n \) for a.a. \( n \).

2. \( \lim_{n \to \infty} a_n = L \) is by definition the statement;
\[ \forall \varepsilon > 0 \exists N \in \mathbb{N} \exists \forall n \geq N, \ |L - a_n| \leq \varepsilon. \]
This may also be written as
\[ \forall \varepsilon > 0, \ |L - a_n| \leq \varepsilon \text{ for a.a. } n. \]

3. The negation of the previous statement is \( \lim_{n \to \infty} a_n \neq L \) which translates to
\[ \exists \varepsilon > 0 \exists N \in \mathbb{N}, \exists \forall n \geq N \exists |L - a_n| > \varepsilon. \]
This last statement is also equivalent to;
\[ \exists \varepsilon > 0 \exists |L - a_n| > \varepsilon \text{ i.o. } n. \]
It is sometimes useful to reformulate this last statement as; there exists \( \varepsilon > 0 \) and an increasing function \( \mathbb{N} \ni k \to n_k \in \mathbb{N} \) such that
\[ |L - a_{n_k}| > \varepsilon \text{ for all } k \in \mathbb{N}. \]
Appendix: More Set Theoretic Properties (highly optional)

B.1 Appendix: Zorn’s Lemma and the Hausdorff Maximal Principle (optional)

**Definition B.1.** A partial order \( \leq \) on \( X \) is a relation with following properties:

1. If \( x \leq y \) and \( y \leq z \) then \( x \leq z \).
2. If \( x \leq y \) and \( y \leq x \) then \( x = y \).
3. \( x \leq x \) for all \( x \in X \).

**Example B.2.** Let \( Y \) be a set and \( X = 2^Y \). There are two natural partial orders on \( X \):

1. Ordered by inclusion, \( A \subseteq B \) is \( A \subset B \) and
2. Ordered by reverse inclusion, \( A \subseteq B \) if \( B \subseteq A \).

**Definition B.3.** Let \( (X, \leq) \) be a partially ordered set we say \( X \) is linearly or totally ordered if for all \( x, y \in X \) either \( x \leq y \) or \( y \leq x \). The real numbers \( \mathbb{R} \) with the usual order \( \leq \) is a typical example.

**Definition B.4.** Let \( (X, \leq) \) be a partial ordered set. We say \( x \in X \) is a maximal element if for all \( y \in X \) such that \( y \geq x \) implies \( y = x \), i.e. there is no element larger than \( x \). An upper bound for a subset \( E \) of \( X \) is an element \( x \in X \) such that \( x \geq y \) for all \( y \in E \).

**Example B.5.** Let

\[
X = \{ a = \{1 \}, b = \{1, 2 \}, c = \{3 \}, d = \{2, 4 \}, e = \{2 \} \}
\]

ordered by set inclusion. Then \( b \) and \( d \) are maximal elements despite that fact that \( b \not\subseteq d \) and \( d \not\subseteq b \). We also have:

1. If \( E = \{a, c, e\} \), then \( E \) has no upper bound.
2. If \( E = \{a, e\} \), then \( b \) is an upper bound.
3. If \( E = \{e\} \), then \( b \) and \( d \) are upper bounds.

**Theorem B.6.** The following are equivalent.

1. The axioms of choice: to each collection, \( \{X_\alpha\}_{\alpha \in A} \), of non-empty sets there exists a "choice function," \( x: A \to \prod_{\alpha \in A} X_\alpha \) such that \( x(\alpha) \in X_\alpha \) for all \( \alpha \in A \), i.e. \( \prod_{\alpha \in A} X_\alpha \neq \emptyset \).

2. **The Hausdorff Maximal Principle**: Every partially ordered set has a maximal (relative to the inclusion order) linearly ordered subset.

3. **Zorn’s Lemma**: If \( X \) is partially ordered set such that every linearly ordered subset of \( X \) has an upper bound, then \( X \) has a maximal element.

**Proof.** (\( 2 \Rightarrow 3 \)) Let \( X \) be a partially ordered subset as in 3 and let \( F = \{E \subset X : E \text{ is linearly ordered}\} \) which we equip with the inclusion partial ordering. By 2, there exist a maximal element \( E \in F \). By assumption, the linearly ordered set \( E \) has an upper bound \( x \in X \). The element \( x \) is maximal, for if \( y \in Y \) and \( y \geq x \), then \( E \cup \{y\} \) is still a linearly ordered set containing \( E \). So by maximality of \( E \), \( E = E \cup \{y\} \), i.e. \( y \in E \) and therefore \( y \leq x \) showing which combined with \( y \geq x \) implies that \( y = x \).

(\( 3 \Rightarrow 1 \)) Let \( \{X_\alpha\}_{\alpha \in A} \) be a collection of non-empty sets, we must show \( \prod_{\alpha \in A} X_\alpha \) is not empty. Let \( G \) denote the collection of functions \( g: D(g) \to \prod_{\alpha \in A} X_\alpha \) such that \( D(g) \) is a subset of \( A \), and for all \( \alpha \in D(g) \), \( g(\alpha) \in X_\alpha \). Notice that \( G \) is not empty, for we may let \( \alpha_0 \in A \) and \( x_0 \in X_\alpha \) and then set \( D(g) = \{\alpha_0\} \) and \( g(\alpha_0) = x_0 \) to construct an element of \( G \). We now put a partial order on \( G \) as follows. We say that \( f \leq g \) for \( f, g \in G \) provided that \( D(f) \subseteq D(g) \) and \( f = g|_{D(f)} \). If \( \Phi \subset G \) is a linearly ordered set, let \( D(h) = \bigcup_{g \in \Phi} D(g) \) and for \( \alpha \in D(g) \) let \( h(\alpha) = g(\alpha) \). Then \( h \in G \) is a upper bound for \( \Phi \). So by Zorn’s

1. If \( X \) is a countable set we may prove Zorn’s Lemma by induction. Let \( \{x_n\}_{n=1}^\infty \) be an enumeration of \( X \), and define \( E_0 \subset X \) inductively as follows. For \( n = 1 \) let \( E_1 = \{x_1\} \), and if \( E_n \) have been chosen, let \( E_{n+1} = E_n \cup \{x_{n+1}\} \) if \( x_{n+1} \) is an upper bound for \( E_n \) otherwise let \( E_{n+1} = E_n \). The set \( E = \bigcup_{n=1}^\infty E_n \) is a linearly ordered (you check) subset of \( X \) and hence by assumption \( E \) has an upper bound, \( x \in X \). I claim that his element is maximal, for if there exists \( y = x_m \in X \) such that \( y \geq x \), then \( x_m \) would be an upper bound for \( E_{m-1} \) and therefore \( y = x_m \in E_m \subset E \). That is to say if \( y \geq x \), then \( y \in E \) and hence \( y \leq x \), so \( y = x \). (Hence we may view Zorn’s lemma as a “jazzy” up version of induction.)

2. Similarly one may show that \( 3 \Rightarrow 2 \). Let \( F = \{E \subset X : E \text{ is linearly ordered}\} \) and order \( F \) by inclusion. If \( M \subset F \) is linearly ordered, let \( E = \bigcup M = \bigcup_{A \in M} A \). If \( x, y \in E \) then \( x \in A \) and \( y \in B \) for some \( A, B \subset M \). Now \( M \) is linearly ordered by set inclusion so \( A \subset B \) or \( B \subset A \) i.e. \( x, y \in A \) or \( x, y \in B \). Since \( A \) and \( B \) are linearly order we must have either \( x \leq y \) or \( y \leq x \), that is to say \( E \) is linearly ordered. Hence by 3, there exists a maximal element \( E \in F \) which is the assertion in 2.
Lemma there exists a maximal element \( h \in \mathcal{G} \). To finish the proof we need only show that \( D(h) = A \). If this were not the case, then let \( \alpha_0 \in A \setminus D(h) \) and \( x_0 \in X_{\alpha_0} \). We may now define \( D(\tilde{h}) = D(h) \cup \{ \alpha_0 \} \) and
\[
\tilde{h}(\alpha) = \begin{cases} 
 h(\alpha) & \text{if } \alpha \in D(h) \\
 x_0 & \text{if } \alpha = \alpha_0.
\end{cases}
\]

Then \( h \leq \tilde{h} \) while \( h \neq \tilde{h} \) violating the fact that \( h \) was a maximal element.

(1 \( \Rightarrow \) 2) Let \((X, \leq)\) be a partially ordered set. Let \( \mathcal{F} \) be the collection of linearly ordered subsets of \( X \) which we order by set inclusion. Given \( x_0 \in X \), \( \{ x_0 \} \in \mathcal{F} \) is linearly ordered set so that \( \mathcal{F} \neq \emptyset \). Fix an element \( P_0 \in \mathcal{F} \). If \( P_0 \) is not maximal there exists \( P_1 \in \mathcal{F} \) such that \( P_0 \subset P_1 \). In particular we may choose \( x \notin P_0 \) such that \( P_0 \cup \{ x \} \in \mathcal{F} \). The idea now is to keep repeating this process of adding points \( x \in X \) until we construct a maximal element \( P \) of \( \mathcal{F} \). We now have to take care of some details. We may assume with out loss of generality that \( \tilde{F} = \{ P \in \mathcal{F} : P \) is not maximal \} is a non-empty set. For \( P \in \tilde{F} \), let \( P^* = \{ x \in X : P \cup \{ x \} \in \mathcal{F} \} \). As the above argument shows, \( P^* \neq \emptyset \) for all \( P \in \tilde{F} \). Using the axiom of choice, there exists \( f \in \prod_{P \in \mathcal{F}} P^* \).

We now define \( g : \mathcal{F} \to \mathcal{F} \) by
\[
g(P) = \begin{cases} 
P & \text{if } P \text{ is maximal} \\
P \cup \{ f(x) \} & \text{if } P \text{ is not maximal.}
\end{cases}
\]

(B.1)

The proof is completed by Lemma B.7 below which shows that \( g \) must have a fixed point \( P \in \mathcal{F} \). This fixed point is maximal by construction of \( g \).

**Lemma B.7.** The function \( g : \mathcal{F} \to \mathcal{F} \) defined in Eq. (B.1) has a fixed point.

**Proof.** The idea of the proof is as follows. Let \( P_1 \in \mathcal{F} \) be chosen arbitrarily. Notice that \( \Phi = \{ g^{(n)}(P_0) \} \) is a linearly ordered set and it is therefore easily verified that \( P_1 = \bigcup_{n=0}^{\infty} g^{(n)}(P_0) \in \mathcal{F} \). Similarly we may repeat the process to construct \( P_2 = \bigcup_{n=0}^{\infty} g^{(n)}(P_1) \in \mathcal{F} \) and \( P_3 = \bigcup_{n=0}^{\infty} g^{(n)}(P_2) \in \mathcal{F} \), etc. etc. Then take \( P_\infty = \bigcup_{n=0}^{\infty} P_n \) and start again with \( P_0 \) replaced by \( P_\infty \). Then keep going this way until eventually the sets stop increasing in size, in which case we have found our fixed point. The problem with this strategy is that we may never win. (This is very reminiscent of constructing measurable sets and the way out is to use measure theoretic like arguments.)

Let us now start the formal proof. Again let \( P_0 \in \mathcal{F} \) and let \( \mathcal{F}_1 = \{ P \in \mathcal{F} : P_0 \subset P \} \). Notice that \( \mathcal{F}_1 \) has the following properties:

1. \( P_0 \in \mathcal{F}_1 \).
2. If \( \Phi \subset \mathcal{F}_1 \) is a totally ordered (by set inclusion) subset then \( \cup \Phi \in \mathcal{F}_1 \).
3. If \( P \in \mathcal{F}_1 \) then \( g(P) \in \mathcal{F}_1 \).

Let us call a general subset \( \mathcal{F}' \subset \mathcal{F} \) satisfying these three conditions a tower and let
\[
\mathcal{F}_0 = \cap \{ \mathcal{F} : \mathcal{F}' \text{ is a tower} \}.
\]

Standard arguments show that \( \mathcal{F}_0 \) is still a tower and clearly is the smallest tower containing \( P_0 \). (Morally speaking \( \mathcal{F}_0 \) consists of all of the sets we were trying to constructed in the “idea section” of the proof.) We now claim that \( \mathcal{F}_0 \) is a linearly ordered subset of \( \mathcal{F} \). To prove this let \( \Gamma \subset \mathcal{F}_0 \) be the linearly ordered set
\[
\Gamma = \{ C \in \mathcal{F}_0 : \text{ for all } A \in \mathcal{F}_0 \text{ either } A \subset C \text{ or } C \subset A \}.
\]

Shortly we will show that \( \Gamma \subset \mathcal{F}_0 \) is a tower and hence that \( \mathcal{F}_0 = \Gamma \). That is to say \( \mathcal{F}_0 \) is linearly ordered. Assuming this for the moment let us finish the proof.

Let \( P \equiv \cup \mathcal{F}_0 \) which is in \( \mathcal{F}_0 \) by property 2 and is clearly the largest element in \( \mathcal{F}_0 \). By 3, it now follows that \( P \subset g(P) \in \mathcal{F}_0 \) and by maximality of \( P \), we have \( g(P) = P \), the desired fixed point. So to finish the proof, we must show that \( \Gamma \) is a tower. First off it is clear that \( P_0 \in \Gamma \) so in particular \( \Gamma \) is not empty. For each \( C \in \Gamma \) let
\[
\Phi_C := \{ A \in \mathcal{F}_0 : \text{ either } A \subset C \text{ or } g(C) \subset A \}.
\]

We will begin by showing that \( \Phi_C \subset \mathcal{F}_0 \) is a tower and therefore that \( \Phi_C = \mathcal{F}_0 \).

1. \( P_0 \in \Phi_C \) since \( P_0 \subset C \) for all \( C \in \Gamma \subset \mathcal{F}_0 \).
2. If \( \Phi \subset \Phi_C \subset \mathcal{F}_0 \) is totally ordered by set inclusion, then \( A_\Phi := \cup \Phi \in \mathcal{F}_0 \). We must show \( A_\Phi \subset \Phi_C \), that is \( A_\Phi \subset C \) or \( C \subset A_\Phi \). Now if \( A \subset C \) for all \( A \in \Phi \), then \( A_\Phi \subset C \) and hence \( A_\Phi \in \Phi_C \) on the other hand if there is some \( A \in \Phi \) such that \( g(C) \subset A \) then clearly \( g(C) \subset A_\Phi \) and again \( A_\Phi \in \Phi_C \). Given \( A \in \Phi_C \) we must show \( g(A) \in \Phi_C \), i.e. that
\[
g(A) \subset C \text{ or } g(C) \subset g(A). \tag{B.2}
\]

There are three cases to consider: either \( A \subset C \), \( A = C \), or \( g(C) \subset A \). In the case \( A = C \), \( g(C) = g(A) \subset A \) and if \( g(C) \subset A \) then \( g(C) \subset A \subset g(A) \) and Eq. (B.2) holds in either of these cases. So assume that \( A \subset C \). Since \( C \in \Gamma \), either \( g(A) \subset C \) (in which case we are done) or \( C \subset g(A) \). Hence we may assume that
\[
A \subset C \subset g(A).
\]

Now if \( C \) were a proper subset of \( g(A) \) it would then follow that \( g(A) \setminus A \) would consist of at least two points which contradicts the definition of \( g \). Hence we
must have \( g(A) = C \subset C \) and again Eq. \([B.2]\) holds, so \( \Phi_C \) is a tower. It is now easy to show \( \Gamma \) is a tower. It is again clear that \( P_0 \in \Gamma \) and Property 2. may be checked for \( \Gamma \) in the same way as it was done for \( \Phi_C \) above. For Property 3., if \( C \in \Gamma \) we may use \( \Phi_C = \Phi_0 \) to conclude for all \( A \in \Phi_0 \), either \( A \subset C \subset g(C) \) or \( g(C) \subset A \), i.e. \( g(C) \in \Gamma \). Thus \( \Gamma \) is a tower and we are done.

### B.2 Cardinality

In mathematics, the essence of counting a set and finding a result \( n \), is that it establishes a one to one correspondence (or bijection) of the set with the set of numbers \( \{1, 2, \ldots, n\} \). A fundamental fact, which can be proved by mathematical induction, is that no bijection can exist between \( \{1, 2, \ldots, n\} \) and \( \{1, 2, \ldots, m\} \) unless \( n = m \); this fact (together with the fact that two bijections can be composed to give another bijection) ensures that counting the same set in different ways can never result in different numbers (unless an error is made). This is the fundamental mathematical theorem that gives counting its purpose; however you count a (finite) set, the answer is the same. In a broader context, the theorem is an example of a theorem in the mathematical field of (finite) combinatorics—hence (finite) combinatorics is sometimes referred to as "the mathematics of counting."

Many sets that arise in mathematics do not allow a bijection to be established with \( \{1, 2, \ldots, n\} \) for any natural number \( n \); these are called infinite sets, while those sets for which such a bijection does exist (for some \( n \)) are called finite sets. Infinite sets cannot be counted in the usual sense; for one thing, the mathematical theorems which underlie this usual sense for finite sets are false for infinite sets. Furthermore, different definitions of the concepts in terms of which these theorems are stated, while equivalent for finite sets, are inequivalent in the context of infinite sets.

The notion of counting may be extended to them in the sense of establishing (the existence of) a bijection with some well understood set. For instance, if a set can be brought into bijection with the set of all natural numbers, then it is called "countably infinite." This kind of counting differs in a fundamental way from counting of finite sets, in that adding new elements to a set does not necessarily increase its size, because the possibility of a bijection with the original set is not excluded. For instance, the set of all integers (including negative numbers) can be brought into bijection with the set of natural numbers, and even seemingly much larger sets like that of all finite sequences of rational numbers are still (only) countably infinite. Nevertheless there are sets, such as the set of real numbers, that can be shown to be "too large" to admit a bijection with the natural numbers, and these sets are called "uncountable." Sets for which there exists a bijection between them are said to have the same cardinality, and in the most general sense counting a set can be taken to mean determining its cardinality. Beyond the cardinalities given by each of the natural numbers, there is an infinite hierarchy of infinite cardinalities, although only very few such cardinalities occur in ordinary mathematics (that is, outside set theory that explicitly studies possible cardinalities).

Counting, mostly of finite sets, has various applications in mathematics. One important principle is that if two sets \( X \) and \( Y \) have the same finite number of elements, and a function \( f : X \to Y \) is known to be injective, then it is also surjective, and vice versa. A related fact is known as the pigeonhole principle, which states that if two sets \( X \) and \( Y \) have finite numbers of elements \( n \) and \( m \) with \( n > m \), then any map \( f : X \to Y \) is not injective (so there exist two distinct elements of \( X \) that \( f \) sends to the same element of \( Y \)); this follows from the former principle, since if \( f \) were injective, then so would its restriction to a strict subset \( S \) of \( X \) with \( m \) elements, which restriction would then be surjective, contradicting the fact that for \( x \) in \( X \) outside \( S \), \( f(x) \) cannot be in the image of the restriction. Similar counting arguments can prove the existence of certain objects without explicitly providing an example. In the case of infinite sets this can even apply in situations where it is impossible to give an example; for instance there must exists real numbers that are not computable numbers, because the latter set is only countably infinite, but by definition a non-computable number cannot be precisely specified.

The domain of enumerative combinatorics deals with computing the number of elements of finite sets, without actually counting them; the latter usually being impossible because infinite families of finite sets are considered at once, such as the set of permutations of \( \{1, 2, \ldots, n\} \) for any natural number \( n \).

### B.3 Formalities of Counting

**Definition B.8.** We say \( \text{card} (X) \leq \text{card} (Y) \) if there exists an injective map, \( f : X \to Y \) and \( \text{card} (Y) \geq \text{card} (X) \) if there exists a surjective map \( g : Y \to X \). We say \( \text{card} (X) = \text{card} (Y) \) if there exists a bijections, \( f : X \to Y \).

**Proposition B.9.** We have \( \text{card} (X) \leq \text{card} (Y) \) iff \( \text{card} (Y) \geq \text{card} (X) \).

**Proof.** If \( f : X \to Y \) is an injective map, define \( g : Y \to X \) by \( g(y) = f^{-1} \) and \( g|_{f(X)} = x_0 \in X \) chosen arbitrarily. Then \( g : Y \to X \) is surjective.

If \( g : Y \to X \) is a surjective map, then \( Y_x := g^{-1}(\{x\}) \neq \emptyset \) for all \( x \in X \) and so by the axiom of choice there exists \( x \in \prod_{x \in X} Y_x \). Thus \( f : X \to Y \) such that \( f(x) \in Y_x \) for all \( x \). As the \( Y_x \) are pairwise disjoint, it follows that \( f \) is injective.

**Theorem B.10 (Schröder-Bernstein Theorem).** If \( \text{card} (X) \leq \text{card} (Y) \) and \( \text{card} (Y) \leq \text{card} (X) \), then \( \text{card} (X) = \text{card} (Y) \). Stated more explicitly; if there exists injective maps \( f : X \to Y \) and \( g : Y \to X \), then there exists a bijective map, \( h : X \to Y \).
We continue this process of inverse iterates as long as it is possible, i.e. we can construct $y_{n+1}$ if $x_n \in g(Y)$ and $x_{n+1} \in f(X)$. There are now three possibilities:

1. ancestor $(x)$ has infinite length so the process never gets stuck in which case we say $x \in X_\infty$, read as start in $X$ and end never get stuck.
2. ancestor $(x)$ is finite and the last term in the sequence is in $X$, in which case we say $x \in X_X$ (read as start in $X$ and end in (get stuck in) $X$).
3. ancestor $(x)$ is finite and the last term in the sequence is in $Y$, in which case we say $x \in X_Y$ (read as start in $X$ and end in (get stuck in) $Y$).

In this way we partition $X$ into three disjoint sets, $X_\infty, X_X,$ and $X_Y$. Similarly we may partition $Y$ into $Y_\infty, Y_Y,$ and $Y_Y$. Let us now observe that,

1. $f(X_\infty) = Y_\infty$. Indeed if $x \in X_\infty$ then ancestor $(f(x)) = (x, \text{ancestor}(x))$ is an infinite sequence, i.e. $f(x) \in Y_\infty$. Moreover if $y \in Y_\infty$, then ancestor $(y) = (y, \text{ancestor}(x))$ where $f(x) = y$ so that $x \in X_\infty$ and $y \in f(X_\infty)$. Thus we have shown $f : X_\infty \rightarrow Y_\infty$ is a bijection, i.e. $\text{card}(X_\infty) = \text{card}(Y_\infty)$.
2. $f(X_X) = Y_X$. Indeed if $x \in X_X$ then again ancestor $(f(x)) = (x, \text{ancestor}(x))$ which ends in $X$ so that $f(x) \in Y_X$. Moreover if $y \in Y_X$, then ancestor $(y) = (y, \text{ancestor}(x))$ where $f(x) = y$ so that ancestor $(x)$ ends in $X$, i.e. $y \in f(X_X)$. Thus we have shown $f : X_X \rightarrow Y_X$ is a bijection, i.e. $\text{card}(X_X) = \text{card}(Y_X)$.
3. By the same argument as in item 2, it follow that $g : Y_Y \rightarrow X_Y$ is a bijection, i.e. $\text{card}(X_Y) = \text{card}(Y_Y)$.

The last three statement implies $\text{card}(X) = \text{card}(Y)$. We may in fact define a bijection, $h : X \rightarrow Y$, by

$$h(x) = \begin{cases} f(x) & \text{if } x \in X_\infty \cup X_X \\ g_{\mid Y_Y}^{-1}(x) & \text{if } x \in X_Y \end{cases}.$$  

**Definition B.11.** We say $\text{card}(X) < \text{card}(Y)$ if $\text{card}(X) \leq \text{card}(Y)$ and $\text{card}(X) \neq \text{card}(Y)$, i.e. $\text{card}(X) < \text{card}(Y)$ if there exists an injective map, $f : X \rightarrow Y,$ but not bijective map exists. Similarly we say $\text{card}(Y) > \text{card}(X)$ if $\text{card}(Y) \geq \text{card}(X)$ and $\text{card}(Y) \neq \text{card}(X)$, i.e. $\text{card}(Y) > \text{card}(X)$ if there exists a surjective map $g : Y \rightarrow X$ but no bijective map exists.

**Proposition B.12.** For any non-empty set $X$, $\text{card}(X) < \text{card}(2^X)$.

**Proof.** Define $f : X \rightarrow 2^X$ by $f(x) = \{x\}$. Then $f$ is an injective map and hence $\text{card}(X) \leq \text{card}(2^X)$. Now suppose that $g : X \rightarrow 2^X$ is any map. Let $X_0 = \{x \in X : x \notin g(x)\} \subset X$. I claim that $X_0 \notin g(X)$.

Indeed suppose there exists $x_0 \in X$ such that $g(x_0) = X_0$. If $x_0 \in X_0$, then $x_0 \notin g(x_0) = X_0$ which is impossible. Similarly if $x_0 \notin X_0 = g(x_0)$ then $x_0 \in X_0$ and again we have reached a contradiction. Thus we must conclude that $X_0 \notin g(X)$. Thus there are no surjective maps, $g : X \rightarrow 2^X$ so that $\text{card}(X) \neq \text{card}(2^X)$.

**Proposition B.13.** If $\text{card}(X) < \text{card}(Y)$ and $\text{card}(Y) \leq \text{card}(Z)$, then $\text{card}(X) < \text{card}(Z)$.

**Proof.** If there exists an injective map, $f : Z \rightarrow X$ then composing this with and injective map, $g : X \rightarrow Y$ gives an injective map, $g \circ f : Z \rightarrow X$ and therefore $\text{card}(Z) \leq \text{card}(X)$. But this would imply that $\text{card}(X) = \text{card}(Z)$.

**Definition B.14.** Let $A_n := \{1, 2, \ldots, n\}$ for all $n \in \mathbb{N}$ and write $n$ for $\text{card}(A_n)$.

**Proposition B.15.** We have $\text{card}(A_m) < \text{card}(A_n)$ for all $m < n$. Moreover if $\emptyset \neq X \subset A_n$ then card $(X) = \text{card}(A_k)$ for some $k < n$.

**Proof.** If $A_1 \rightarrow A_2$, then either $f(1) = 1$ or $f(1) = 2$. In either case $f$ is injective but not bijective so that card $(A_2) < \text{card}(A_1)$. Let $S_n$ be the statement that card $(A_k) < \text{card}(A_l)$ for all $1 \leq k < l \leq n$ and for any proper subset $X \subset A_n$ we have card $(X) = \text{card}(A_m)$ for some $m < n$. Then we have just shown that $S_2$ is true. So suppose that $S_n$ is now true. As $f : A_k \rightarrow A_1$ defined by $f(m) = m$ for all $m \in A_k$ is a injection when $k < l$ we always have card $(A_k) \leq \text{card}(A_l)$. Now suppose that card $(A_k) = \text{card}(A_{n+1})$ for some $k \leq n$. Then there exists a bijection, $f : A_{n+1} \rightarrow A_k$. In this case $f(A_n)$ is a proper subset of $A_k$ and therefore card $(f(A_n)) < \text{card}(A_k)$ but on the other hand card $(f(A_n)) = \text{card}(A_n) \geq \text{card}(A_k)$ which is a contradiction. So no such bijection can exists and we have shown card $(A_k) < \text{card}(A_{n+1})$ for all $k \leq n$. Finally suppose that $X \subset A_{n+1}$ is proper subset. If $X \subset A_n$ then card $(X) = \text{card}(A_k)$ for some $k \leq n$ by the induction hypothesis. On the other hand if $n + 1 \in X$, let $X' := X \setminus \{n + 1\} \subseteq A_n$. Therefore by the induction hypothesis card $(X') = \text{card}(A_k)$ for some $k < n$. It is then clear that card $(X) = \text{card}(A_{k+1})$ where $k + 1 < n$, indeed we map $X := X' \cup \{n + 1\} \rightarrow A_k \cup \{k + 1\} = A_{k+1}$.

**Example B.16.** card $(A_n \setminus \{k\}) = n - 1$ for $k \in A_n$. Indeed, let $f : A_{n-1} \rightarrow A_n \setminus \{k\}$ be defined by
\[ f(x) = \begin{cases} 
  x & \text{if } x < k \\
  x + 1 & \text{if } x \geq k 
\end{cases} \]

Then \( f \) is the desired bijection. More generally if \( X \subset Y \) and \( \text{card}(X) = m < n = \text{card}(Y) \), then \( \text{card}(Y \setminus X) = n - m \) and if \( X \) and \( Y \) are finite disjoint sets then \( \text{card}(X \cup Y) = \text{card}(X) + \text{card}(Y) \). Similarly, \( \text{card}(X \times Y) = \text{card}(X) \cdot \text{card}(Y) \).

**Proposition B.17.** If \( f : A_n \to A_n \) is a map, then the following are equivalent,

1. \( f \) is injective,
2. \( f \) is surjective,
3. \( f \) is bijective.

Moreover \( \text{card}(\text{Bijec}(A_n)) = n! \).

**Proof.** If \( n = 1 \), the only map \( f : A_1 \to A_1 \) is \( f(1) = 1 \). So in this case there is nothing to prove. So now suppose the proposition holds for level \( n \) and \( f : A_{n+1} \to A_{n+1} \) is a given map.

If \( f : A_{n+1} \to A_{n+1} \) is an injective map and \( f(A_{n+1}) \) is a proper subset of \( A_{n+1} \), then \( \text{card}(A_{n+1}) < \text{card}(f(A_{n+1})) = \text{card}(A_{n+1}) \) which is absurd. Thus \( f \) is injective implies \( f \) is surjective.

Conversely suppose that \( f : A_{n+1} \to A_{n+1} \) is surjective. Let \( g : A_{n+1} \to A_{n+1} \) be a right inverse, i.e. \( f \circ g = \text{id} \), which is necessarily injective, see the proof of Proposition [B.9] By the previous paragraph we know that \( g \) is necessarily surjective and therefore \( f = g^{-1} \) is a bijection.

It now only remains to prove \( \text{card}(\text{Bijec}(A_n)) = n! \) which we again do by induction. For \( n = 1 \) the result is clear. So suppose it holds at level \( n \). If \( f : A_{n+1} \to A_{n+1} \) is a bijection. Given \( 1 \leq k \leq n+1 \) let

\[ \text{Bij}_k(A_{n+1}) := \{ f \in \text{Bij}(A_{n+1}) : f(n+1) = k \}. \]

For \( f \in \text{Bij}_k(A_{n+1}) \), we have \( f : A_n \to A_{n+1} \setminus \{k\} \cong A_n \) is a bijection. Thus \( \text{Bij}_k(A_{n+1}) \cong \text{Bij}(A_n) \) and

\[ \text{Bij}(A_{n+1}) = \sum_{k=1}^{n+1} \text{Bij}_k(A_{n+1}) \]

we have

\[ \text{card}(\text{Bij}(A_{n+1})) = \sum_{k=1}^{n+1} \text{card}(\text{Bij}_k(A_{n+1})) \]

\[ = \sum_{k=1}^{n+1} \text{card}(\text{Bij}(A_n)) = \sum_{k=1}^{n+1} n! \]

\[ = (n + 1) n! = (n + 1)!. \]

\[ \blacksquare \]
References
