1. REAL AND COMPLEX NUMBERS

Numbers are at the heart of mathematics. By now you must be fairly familiar with them. Basic sets of numbers are:

- the natural numbers, \( \mathbb{N} = \{0, 1, 2, \cdots \} \);
- the integers (die Zahlen), \( \mathbb{Z} = \{ \cdots, -2, -1, 0, 1, 2, \cdots \} \);
- the rational numbers (quotients), \( \mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\} \);
- the real numbers, \( \mathbb{R} = (-\infty, \infty) \);
- the complex numbers, \( \mathbb{C} = \{ x + iy : x, y \in \mathbb{R} \} \).

Each of these sets is endowed with natural algebraic operations (like ‘addition’ and ‘multiplication’) and order relations (like ‘less than’) by which their elements are manipulated and compared. It is fairly clear how \( \mathbb{N}, \mathbb{Z}, \) and \( \mathbb{Q} \) are related through an increasingly richer algebraic structure. It is also fairly clear that \( \mathbb{R} \) and \( \mathbb{C} \) bear a similar relationship. What is less clear is the relationship between \( \mathbb{Q} \) and \( \mathbb{R} \). In particular, what are the properties that allow \( \mathbb{R} \) and not \( \mathbb{Q} \) to be identified with a ‘line’? In this section we review some of these issues.

1.1. Fields. The sets \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) endowed with their natural algebraic operations are each an example of a general algebraic structure known as a field.

Definition 1.1. A field is a set \( X \) equipped with two distinguished binary operations, called addition and multiplication, that satisfy the addition, multiplication, and distributive axioms presented below. Taken together, these axioms constitute the so-called field axioms.

Addition axioms. Addition maps any two \( x, y \in X \) to their sum \( x + y \in X \) such that:

- (i) \( x + y = y + x \) for every \( x, y \in X \), — commutativity;
• (ii) \((x + y) + z = x + (y + z)\) for every \(x, y, z \in X\), — associativity;
• (iii) there exists a \(0 \in X\), such that \(x + 0 = x\) for every \(x \in X\), — identity;
• (iv) for every \(x \in X\) there exists a \(-x \in X\), such that \(x + (-x) = 0\), — inverse.

Definition 1.2. A set \(X\) equipped with a distinguished binary operation that satisfies the addition axioms is called an Abelian group or a commutative group.

Remark: When working with Abelian groups, it is both convenient and common to write
\[
x - y, \quad x + y + z, \quad 2x, \quad 3x, \quad \cdots,
\]
rather than
\[
x + (-y), \quad x + (y + z), \quad x + x, \quad x + x + x, \quad \cdots.
\]

Examples: When addition has its usual meaning, the axioms for an Abelian groups clearly hold in \(\mathbb{Z}, \mathbb{Q}, \mathbb{R},\) and \(\mathbb{C}\), but not in \(\mathbb{N}\). They also hold in \(\mathbb{Z}_n \equiv \mathbb{Z}/(n\mathbb{Z})\) for every positive integer \(n\). (If you do not know this last example, do not worry. It is not critical in this course.)

The addition axioms immediately imply the following.

Proposition 1.1. • (a) If \(x, y, z \in X\) and \(x + y = x + z\) then \(y = z\).
• (b) If \(x, y \in X\) and \(x + y = x\) then \(y = 0\).
• (c) If \(x, y \in X\) and \(x + y = 0\) then \(y = -x\).
• (d) If \(x, y \in X\) then \((-x + y = (-x) + (-y))\).
• (e) If \(x \in X\) then \((-x) = x\).

Proof: Exercise.

Assertion (a) states that addition enjoys a so-called cancellation law. Assertion (b) states that there is a unique additive identity of the type assumed in (iii). This unique additive identity is called zero. All other elements of \(X\) are said to be nonzero. Assertion (c) states that for every \(x \in X\) there is a unique additive inverse of the type assumed in (iv). This unique additive inverse is called the negative of \(x\). The map defined for every \(x \in X\) by \(x \mapsto -x\) is called negation. Assertion (d) states that the negative of a sum is the sum of the negatives. Assertion (e) states that for every \(x \in X\) the negative of the negative of \(x\) is again \(x\).

Multiplication axioms. Multiplication maps any two \(x, y \in X\) to their product \(xy \in X\) such that:
• (i) \( xy = yx \) for every \( x, y \in X \), — commutativity;
• (ii) \((xy)z = x(yz)\) for every \( x, y, z \in X \), — associativity;
• (iii) there exists a nonzero \( 1 \in X \) such that \( x1 = x \) for every \( x \in X \), — identity;
• (iv) for every nonzero \( x \in X \) there exists a \( x^{-1} \in X \) such that \( xx^{-1} = 1 \), — inverse.

**Distributive axiom.** Addition and multiplication are related by:

• (i) \( x(y + z) = xy + xz \) for every \( x, y, z \in X \), — distributivity.

These combined with the addition axioms constitute the field axioms.

**Remark:** When working with fields, it is both convenient and common to write

\[ x/y, \ yz, \ x^2, \ x^3, \ldots, \]

rather than

\[ xy^{-1}, \ yz, \ xx, \ xxx, \ldots. \]

**Examples:** When addition and multiplication have their usual meaning, the field axioms clearly hold in \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C}, \) but not in \( \mathbb{N} \) or \( \mathbb{Z}. \) They also hold in \( \mathbb{Z}_n \) when \( n \) is prime.

The multiplication axioms immediately imply the following.

**Proposition 1.2.**

• (a) If \( x, y, z \in X, \ x \neq 0, \) and \( xy = xz \) then \( y = z. \)
• (b) If \( x, y \in X, \ x \neq 0, \) and \( xy = x \) then \( y = 1. \)
• (c) If \( x, y \in X, \ x \neq 0, \) and \( xy = 1 \) then \( y = x^{-1}. \)
• (d) If \( x, y \in X, \ x \neq 0, \ y \neq 0, \) and \( xy \neq 0 \) then \( (xy)^{-1} = x^{-1}y^{-1}. \)
• (e) If \( x \in X \) and \( x \neq 0 \) then \( (x^{-1})^{-1} = x. \)

**Proof:** Exercise.

Assertion (a) states that multiplication enjoys a so-called cancellation law. Assertion (b) states that there is a unique multiplicative identity of the type assumed in (iii). This unique multiplicative identity is called one. Assertion (c) states that for every nonzero \( x \in X \) there is a unique multiplicative inverse of the type assumed in (iv). This unique multiplicative inverse is called the reciprocal of \( x. \) The map defined for every nonzero \( x \in X \) by \( x \mapsto x^{-1} \) is called reciprocation. Assertion (d) states that the reciprocal of a product is the product of the reciprocals. Assertion (e) states that for every nonzero \( x \in X \) the reciprocal of the reciprocal of \( x \) is again \( x. \)

The field axioms imply the following.

**Proposition 1.3.** Let \( X \) be a field.
• (a) If \( x \in X \) then \( x0 = 0 \).
• (b) If \( x, y \in X \) and \( xy = 0 \) then \( x = 0 \) or \( y = 0 \).
• (c) If \( x, y \in X \) then \( (-x)y = -(xy) = x(-y) \).
• (d) If \( x \in X \) and \( x \neq 0 \) then \( (-x)^{-1} = -x^{-1} \).

**Proof:** Exercise.

Assertion (a) states that the product of anything with zero is zero. In particular, it shows that zero cannot have a multiplicative inverse. Hence, an element has a multiplicative inverse if and only if it is nonzero. Assertion (b) states that if a product is zero, at least one of its factors must be zero. This should be compared with (d) of Proposition 2.2. Assertions (c) and (d) state how negation, multiplication, and reciprocation relate.

1.2. **Ordered Sets.** The sets \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \) and \( \mathbb{R} \) endowed with their natural order relation are each an example of a general structure known as an ordered set.

**Definition 1.3.** An ordered set \((X, <)\) is a set \( X \) equipped with a distinguished binary relation “\(<\)”, called an order, that satisfies the order axioms presented below.

**Order axioms.** A binary relation “\(<\)” on a set \( X \) is called an order whenever:

- (i) if \( x, y, z \in X \) then \( x < y \) and \( y < z \) implies \( x < z \), — transitivity;
- (ii) if \( x, y \in X \) then exactly one of \( x < y \), \( x = y \), or \( y < x \) is true, — trichotomy.

**Remark:** When working with ordered sets, it is both convenient and common to use the notation

\[
x > y, \quad x \leq y, \quad x \geq y,
\]

to mean

\[
y < x, \quad x < y \text{ or } x = y, \quad y < x \text{ or } x = y.
\]

Another common notational shorthand is

\[
x < y < z, \quad x < y \leq z, \quad \cdots,
\]

to mean

\[
x < y \text{ and } y < z, \quad y < x \text{ and } x \leq y, \quad \cdots.
\]

**Examples:** When “\(<\)” has its usual meaning of “less than”, the order axioms clearly hold in \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \) and \( \mathbb{R} \).
Definition 1.4. Let $(X, <)$ be an ordered set. A point $x \in X$ is an upper bound (a lower bound) of a set $S \subseteq X$ whenever $y \leq x$ ($x \leq y$) for every $y \in S$. If $S \subseteq X$ has an upper bound (a lower bound) then $S$ is said to be bounded above (bounded below). A set $S \subseteq X$ that is both bounded above and bounded below is said to be bounded.

Definition 1.5. Let $(X, <)$ be an ordered set, and let $S \subseteq X$ be bounded above. A point $x \in X$ is a least upper bound or supremum of $S$ whenever:

1. $x$ is an upper bound of $S$;
2. if $y \in X$ is also an upper bound of $S$ then $x \leq y$.

We similarly define a greatest lower bound or infimum of $S$.

If a supremum or infimum of $S$ exists then it must be unique. The supremum of $S$ is denoted $\sup\{S\}$ or $\sup\{z : z \in S\}$, while the infimum is denoted $\inf\{S\}$ or $\inf\{z : z \in S\}$.

The notions of supremum and infimum should not be confused with those of maximum and minimum.

Definition 1.6. Let $(X, <)$ be an ordered set, and let $S \subseteq X$. A point $x \in S$ is a maximum (minimum) of $S$ whenever $x$ is an upper (lower) bound of $S$.

If a maximum or minimum of $S$ exists then it must be unique. The maximum of $S$ is denoted $\max\{S\}$ or $\max\{z : z \in S\}$, while the infimum is denoted $\min\{S\}$ or $\min\{z : z \in S\}$. Moreover, if a maximum (minimum) of $S$ exists then

$$\sup\{S\} = \max\{S\} \quad (\inf\{S\} = \min\{S\}).$$

Examples: Any bounded open interval $(a, b)$ in $\mathbb{R}$ has no maximum or minimum, yet $\sup(a, b) = b$ and $\inf\{(a, b)\} = a$. For any bounded closed interval $[a, b]$ in $\mathbb{R}$ one has $\max[a, b] = b$ and $\min[a, b] = a$. The same is true if these intervals are restricted to elements of $\mathbb{Q}$.

What will distinguish $\mathbb{R}$ from $\mathbb{Q}$ is the following property.

Definition 1.7. Let $(X, <)$ be an ordered set. Then $X$ is said to have the least upper bound property whenever every nonempty subset of $X$ with an upper bound has a least upper bound.

Remark: It may seem we should also define a “greatest lower bound property”, but the next proposition shows that this is unnecessary because it is exactly the same property.
**Proposition 1.4.** Let \((X, <)\) be an ordered set. Let \(X\) have the least upper bound property. Then every nonempty subset of \(X\) with a lower bound has a greatest lower bound.

**Proof:** Let \(S \subset X\) be a nonempty set with a lower bound. Let \(L \subset X\) be the set of all lower bounds of \(S\). It is nonempty and bounded above by any element of \(S\). Therefore \(\sup\{L\}\) exists. It is easy to check that \(\sup\{L\} = \inf\{S\}\). \(\square\)

**Examples:** When “<” has its usual meaning of “less than”, the sets \(\mathbb{N}\) and \(\mathbb{Z}\) have the least upper bound property, while the set \(\mathbb{Q}\) does not. To see the latter case, consider the set 

\[ S = \{ r \in \mathbb{Q} : r^2 \leq 2 \}. \]

First show that there is no \(r \in \mathbb{Q}\) such that \(r^2 = 2\). Then show that if \(q \in S\) and \(q > 0\) then there exists a \(p \in S\) with \(p > q\), so there is no upper bound within \(S\). It follows that \(q \in \mathbb{Q}\) is an upper bound for \(S\) if and only if \(q > 0\) and \(q^2 > 2\). Finally, we show that for every such \(q\) there exists such a \(p\) with \(p < q\). What we are looking for here is a better rational approximation from above of \(\sqrt{2}\). This can be done by taking one iteration of Newton’s method and applied to \(x^2 - 2 = 0\). Set

\[ p = q - \frac{q^2 - 2}{2q} = \frac{q^2 + 2}{2q}. \]

A picture alone should convince you this is a suitable \(p\). Indeed, it is clear from the above that \(p < q\) and that \(p > 0\). A skeptic only needs to check that \(p^2 > 2\). We confirm this fact by the calculation

\[ p^2 - 2 = \frac{q^4 + 4q^2 + 4}{4q^2} - 2 = \frac{q^4 - 4q^2 + 4}{4q^2} = \left(\frac{q^2 - 2}{2q}\right)^2 > 0. \]

1.3. **Ordered Fields.** The sets \(\mathbb{Q}\) and \(\mathbb{R}\) endowed with their natural algebraic operations and order relation are each an example of a general algebraic structure known as an ordered field.

**Definition 1.8.** A set \(X\) that is both a field and an ordered set is called an ordered field whenever:

- (i) if \(x, y, z \in X\) then \(x < y\) implies \(x + z < y + z\);
- (ii) if \(x, y \in X\) then \(0 < x\) and \(0 < y\) implies \(0 < xy\).

If \(x > 0\) (\(x < 0\), \(x \geq 0\), \(x \leq 0\)) then we say \(x\) is positive (negative, nonnegative, nonpositive). The set of all positive (negative) elements of \(X\) is denoted \(X^+\) (\(X^-\)).

**Examples:** When addition, multiplication, and “<” have their usual meanings, the sets \(\mathbb{Q}\) and \(\mathbb{R}\) are ordered fields.
Proposition 1.5. Let $X$ be an ordered field.

- (a) If $x > 0$ then $-x < 0$, and vice versa.
- (b) If $x > 0$ and $y < z$ then $y < x + z$ and $xy < xz$.
- (c) If $x < 0$ and $y < z$ then $x + y < z$ and $xy > xz$.
- (d) If $x \neq 0$ then $x^2 > 0$.
- (e) If $0 < x < y$ then $0 < y^{-1} < x^{-1}$.

Proof: Exercise.

The above proposition shows that $X^+$ satisfies the following.

- (i) If $x, y \in X^+$ then $x + y \in X^+$ and $xy \in X^+$.
- (ii) For every $x \in X$ exactly one of $x \in X^+$, $-x \in X^+$, or $x = 0$ is true.

These so-called positivity properties alone characterize the order relation on the field $X$.

Proposition 1.6. Let $X$ be a field. Let $X^+ \subset X$ satisfy the above positivity properties. Define the binary relation $<$ on $X$ by

$$x < y \quad \text{means} \quad y - x \in X^+.$$  

Then $(X, <)$ is an ordered field.

Proof: Exercise.

Proposition 1.6 implies that we could have defined an ordered field as a field $X$ that has a subset $X^+$ satisfying the positivity properties. In this case the positivity properties become the positivity axioms, and the order axioms become order properties. This is the approach taken in Fitzpatrick’s book.

Definition 1.9. Let $X$ be an ordered field. The absolute value function on $X$ is defined by

$$|x| = \begin{cases} 
  x & \text{if } x > 0 \\
  0 & \text{if } x = 0 \\
  -x & \text{if } x < 0 
\end{cases}.$$  

Proposition 1.7. Let $X$ be an ordered field. Then for every $x, y \in X$

- (a) $|x| \geq 0$,
- (b) $|x| = 0$ if and only if $x = 0$,
- (c) $|x + y| \leq |x| + |y|$,
- (d) $|xy| \leq |x||y|$,
- (e) $|x - y| \leq |x - y|$.

Proof: Exercise.
1.4. **Real Numbers.** The main theorem of this section, which we state without proof, is the following.

**Theorem 1.1.** There exists a unique (up to an isomorphism) ordered field with the least upper bound property that contains $\mathbb{Q}$ (up to an isomorphism) as a subfield.

**Proof:** Proofs of this theorem are quite long and technical. You can find a proof of all but the uniqueness in the book by W. Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, New York, 1976. That proof is based on a construction due to Dedekind using so-called Dedekind cuts. Later in this course we will sketch another proof of all but the uniqueness that is based on a construction due to Cantor using Cauchy sequences. Both Dedekind and Cantor published their constructions in 1872.

**Definition 1.10.** The real numbers are defined to be the unique ordered field with the least upper bound property whose existence is guaranteed by Theorem 1.1. This field is denoted $\mathbb{R}$.

**Remark:** The least upper bound property that sets $\mathbb{R}$ apart from $\mathbb{Q}$. As we will see, it is why $\mathbb{R}$ can be identified with a line.

Important properties of $\mathbb{R}$ are given in the following.

**Proposition 1.8.**

- If $x, y \in \mathbb{R}$ and $x > 0$ then there exists $n \in \mathbb{Z}^+$ such that $nx > y$.
- If $x \in \mathbb{R}$ then there exists a unique $m \in \mathbb{Z}$ such that $m \in (x - 1, x]$.
- If $x, y \in \mathbb{R}$ and $x < y$ then there exists $q \in \mathbb{Q}$ such that $x < q < y$.

**Remark.** The first assertion above is called the *Archimedean property* of $\mathbb{R}$, the second is a statement about the distribution of the integers, while the third asserts that $\mathbb{Q}$ is *dense* in $\mathbb{R}$ — i.e. that between any two reals lies a rational.

**Proof.** Suppose the first assertion is false. Then $y$ is an upper bound for the set $S = \{nx : n \in \mathbb{N}\}$. By the least upper bound property $S$ has a supremum. Let $z = \sup\{S\}$. Because $x > 0$ one has that $z - x < z$. Hence, $z - x$ is not an upper bound for $S$ because $z = \sup\{S\}$. This implies there exists some $n \in \mathbb{N}$ such that $z - x < nx$. But then $z < (n + 1)x$, which contradicts the fact $z$ is an upper bound of $S$. Therefore the first assertion holds.

To prove the second assertion, by the first assertion there exists $k, l \in \mathbb{Z}^+$ such that $-x < k$ and $x < l$. It follows that $-k < x < l$. 

One can then argue that there exists some \( m \in \mathbb{Z} \) such that
\[
-k \leq m \leq l \quad \text{and} \quad m - 1 < x \leq m.
\]
This step is left as an exercise.

To prove the third assertion, because \( y - x > 0 \), by the first assertion there exists \( n \in \mathbb{Z}^+ \) such that \( n(y - x) > 1 \). Then by the second assertion there exists a unique \( m \in (nx, nx + 1] \). Combining these facts yields
\[
x < m - 1 < x + n(y - x) = ny.
\]
Because \( n \) is nonzero, we conclude that
\[
x < m < y.
\]

\[ \square \]

1.5. Extended Real Numbers. It is often convenient to extend the real numbers \( \mathbb{R} \) by appending two elements designated \(-\infty\) and \(\infty\). This enlarged set is called the extended real numbers and is denoted by \( \mathbb{R}^{ex} \).

The order \(<\) on \( \mathbb{R} \) is extended to \( \mathbb{R}^{ex} \) by defining
\[
-\infty < x < \infty \quad \text{for every} \quad x \in \mathbb{R}.
\]
Interval notation thereby extends naturally to \( \mathbb{R}^{ex} \). In particular, one has \( \mathbb{R}^{ex} = [-\infty, \infty] \). The ordered set \( (\mathbb{R}^{ex}, <) \) has the property that \( \infty \) (\(-\infty\)) is an upper (lower) bound for every subset of \( \mathbb{R}^{ex} \). It also has the least upper bound property. Indeed, every nonempty \( S \subset \mathbb{R}^{ex} \) has a supremum given by
\[
\sup\{S\} = \begin{cases} 
\infty & \text{if either} \ S \cap \mathbb{R} \text{has no upper bound in} \ \mathbb{R} \text{or} \ \infty \in S, \\
-\infty & \text{if} \ S = \{-\infty\}, \\
\sup\{S \cap \mathbb{R}\} & \text{otherwise}.
\end{cases}
\]
In particular, every nonempty \( S \subset \mathbb{R} \) that has no upper bound in \( \mathbb{R} \) (and therefore no supremum in \( \mathbb{R} \)) has \( \sup\{S\} = \infty \) in \( \mathbb{R}^{ex} \). Similar statements hold for lower bounds and infimums.

The operations of addition and multiplication on \( R \) cannot be extended so as to make \( \mathbb{R}^{ex} \) into a field. It is however natural to extend addition by defining for every \( x \in \mathbb{R} \)
\[
x + \infty = \infty + x = \infty, \quad x - \infty = -\infty + x = -\infty,
\]
and by defining
\[
\infty + \infty = \infty, \quad -\infty - \infty = -\infty,
\]
while leaving $\infty - \infty$ and $-\infty + \infty$ undefined. Similarly, it is natural to extend multiplication by defining for every nonzero $x \in \mathbb{R}$

$$x \infty = \infty x = \begin{cases} 
\infty & \text{if } x > 0 \\
-\infty & \text{if } x < 0 
\end{cases},$$

$$x (-\infty) = (-\infty) x = \begin{cases} 
-\infty & \text{if } x > 0 \\
\infty & \text{if } x < 0 
\end{cases},$$

and by defining

$$\infty \infty = (-\infty) (-\infty) = \infty, \quad \infty (-\infty) = (-\infty) \infty = -\infty,$$

while leaving $0 \infty$, $\infty 0$, $0 (-\infty)$, and $(-\infty) 0$ undefined.