A fact about fields

Observation. $\{0\}$ is a field, with algebraic operations $0 \cdot 0 = 0 = 0 + 0$.

Proposition

If F is a field with more than one element, then $0 \neq 1$.

Proof. Find $x \in F$ different from 0. Then $0 = x \cdot 0 \neq x \cdot 1 = 1$, hence $0 \neq 1$. ■

Order

Definition: A relation $\leqslant$ on a set S is called linear (total) order if:

(O1) Totality: for $a, b \in S$, either $a \leqslant b$, or $b \leqslant a$.

(O2) Antisymmetry: if $a \leqslant b$ and $b \leqslant a$, then $a = b$.

(O3) Transitivity: if $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

We write $a < b$ if $a \leqslant b$, $a \neq b$.

Definition: A field F is called ordered if it is equipped with linear order $\leqslant$ s.t.:

(O4) If $a, b, c \in F$, and $a \leqslant b$, then $a + c \leqslant b + c$.

(O5) If $a, b, c \in F$, $a \leqslant b$, and $c \geqslant 0$, then $ac \leqslant bc$.

Examples of ordered fields. $(\mathbb{Q}, \leqslant)$, $(\mathbb{R}, \leqslant)$.
$\mathbb{C}$ is a field, but cannot be equipped with a linear order.

Properties of ordered fields

Theorem (Theorem 3.2 – p. 16 of text)

Suppose F is an ordered field, $a, b, c, \in F$. Then:

1. *If $a \leqslant b$, then $-b \leqslant -a$.*
2. *If $a \leqslant b$, and $c \leqslant 0$, then $bc \leqslant ac$.*
3. *If $0 \leqslant a$ and $0 \leqslant b$, then $0 \leqslant ab$.*
4. *$0 \leqslant a^2$ (for all $a \in F$).*
5. *$0 < 1$.*
6. *If $0 < a$, then $0 < a^{-1}$.*
7. *If $0 < a < b$, then $0 < b^{-1} < a^{-1}$.*

Proof of (iii). $b \geqslant 0$, hence, by (O5), $0 \cdot b \leqslant ab$. But, $0 \cdot b = 0$. ■

Fact. $\mathbb{C}$ is not an ordered field.

Proof. $\mathbb{C}$ is a field. Suppose, for the sake of contradiction, that $\leqslant$ determines a linear order on $\mathbb{C}$. Recall: $\iota^2 = -1$, where $\iota = \sqrt{-1}$. Then $-1 > 0$, hence $1 = -(-1) < -0 = 0$. However, $1 > 0$. ■

Absolute value

Definition (Absolute value – Def. 3.3, p. 17)

Suppose F is an ordered field, $a \in F$. Define
absolute value $|a| = \begin{cases} a & a \geqslant 0 \\ -a & a < 0 \end{cases}$.

Meaning: distance between 0 and a (imagine the real line).

Note: $|a| = |-a|$.

Definition (Distance – Def. 3.4, p. 17)

Suppose F is an ordered field, $a, b \in F$. Define the distance between a and b as $\mathrm{dist}(a, b) = |a - b|$.

Note: $\mathrm{dist}(a, b) = \mathrm{dist}(b, a)$.

Properties of absolute value

Theorem (Theorem 3.5, p. 17)

Suppose F is an ordered field, $a, b \in F$.

1. $|a| \geqslant 0$.
2. $|ab| = |a|\,|b|$.
3. $|a+b| \leqslant |a| + |b|$ *[sometimes called Triangle Inequality].*

Corollary (Triangle inequality – Cor. 3.6, p. 18)

For $a, b, c \in F$, $\mathrm{dist}(a, c) \leqslant \mathrm{dist}(a, b) + \mathrm{dist}(b, c)$.

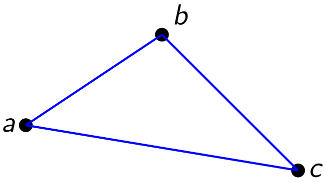
Proof. $\mathrm{dist}(a, c) = |a - c| = |(a - b) + (b - c)| \leqslant |a - b| + |b - c|$
$= \mathrm{dist}(a, b) + \mathrm{dist}(b, c)$. ∎

Geometric meaning of the triangle inequality

Corollary (Triangle inequality – Cor. 3.6, p. 18)

For $a, b, c \in F$, $\mathrm{dist}(a, c) \leqslant \mathrm{dist}(a, b) + \mathrm{dist}(b, c)$.

In a triangle, the length of one side cannot exceed the total length of the other two.



Proof: $|a + b| \leqslant |a| + |b|$**.** $a \leqslant |a|$ and $b \leqslant |b|$, so $a + b \leqslant |a| + |b|$.
Similarly, $(-a) + (-b) \leqslant |-a| + |-b| = |a| + |b|$.
But $(-a) + (-b) = -(a + b)$, hence $-(a + b) \leqslant |a| + |b|$.
$|a + b|$ equals either $a + b$ or $-(a + b)$, hence $|a + b| \leqslant |a| + |b|$. ∎

Section 4: Upper bound, maximum, etc.

Definition

Suppose $S \subset \mathbb{R}$, $S \neq \emptyset$.

- x is an upper bound for S if $x \geqslant s\ \forall s \in S$.
- S is bounded above if it has an upper bound.
- x is the maximum of S ($\max S$) if x is an upper bound, and $x \in S$.
- Lower bound, minimum are defined similarly.
- S is bounded if it is bounded both above and below.

Observation. $\max S$ is unique. If $x, y \in S$ are upper bounds for S, then $x = y$. Indeed, then $x \leqslant y$, and $y \leqslant x$, so $x = y$.

Examples. **1.** $A = \{1, 3, 5, 7, 11\}$. $\max A = 11$. x is an upper bound for A iff $x \geqslant 11$. $\min A = 1$. x is a lower bound for A iff $x \leqslant 1$.

Every finite set has max and min. For infinite sets, things are different.

2. $B = (-\infty, 0)$ is not bounded below. x is an upper bound for B iff $x \geqslant 0$. B has no maximum. 0 is the least (smallest) upper bound.

Completeness axiom (p. 23)

Axiom (Completeness axiom)

If $S \subset \mathbb{R}$ is non-empty and bounded above, then it has (unique) least upper bound, or supremum, denoted by $\sup S$.

We are not constructing $\mathbb{R}$ in this course; rather, we are describing properties of $\mathbb{R}$.

Remark. The supremum is unique. Indeed, aiming at a contradiction, suppose x, y are different least upper bounds for S. $\leqslant$ determines a linear order on $\mathbb{R}$ (any two elements are comparable), hence either $x < y$, or $y < x$. If $x < y$, then y is not a least upper bound. Similarly, if $y < x$, then x is not a least upper bound. Either way, a contradiction! ■

Notation (Section 5). If $S \neq \emptyset$ is not bounded above, we let $\sup S = \infty$.

Completeness makes real numbers special

There are many ordered fields, $\mathbb{R}$, $\mathbb{Q}$, ...

Completeness fails for $\mathbb{Q}$. Let $S = \{r \in \mathbb{Q} : r > 0, r^2 < 2\}$ (in other words, $S = \{r \in \mathbb{Q} : 0 < r < \sqrt{2}\}$). Then no $u \in \mathbb{Q}$ can be the supremum of S.

- If $u < \sqrt{2}$, then (by denseness of rationals, to be discussed) $\exists v \in (u, \sqrt{2}) \cap \mathbb{Q}$, so $v \in S$; so u is not an upper bound.
- If $u > \sqrt{2}$, then (by denseness of rationals again) $\exists v \in (\sqrt{2}, u) \cap \mathbb{Q}$, so v is an upper bound on S; so u is not the least upper bound.

Theorem (Characterization of reals)

The set of reals is the unique complete ordered field.

Consequences of completeness axiom

Proposition (Definition 4.3 + Corollary 4.5)

If $S \subset \mathbb{R}$ is non-empty and bounded below, then it has (unique) greatest lower bound, or infimum, denoted by $\inf S$.

Notation. If $S \neq \emptyset$ is not bounded below, we let $\inf S = -\infty$.

Proposition (Archimedean Property – p 25)

If $a, b \in \mathbb{R}$, $a > 0$, $b > 0$, then $\exists\, n \in \mathbb{N}$ s.t. $na > b$.

Corollary

For $x > 0$, $\exists\, m, k \in \mathbb{N}$ s.t. $\frac{1}{k} < x < m$.

Proof. (1) Use Archimedean Property with $a = x$, $b = 1$. Find $k \in \mathbb{N}$ s.t. $kx > 1 \Leftrightarrow x > \frac{1}{k}$.

(2) Use Archimedean Property with $a = 1$, $b = x$. Find $m \in \mathbb{N}$ s.t. $m > x$.

■

Proof of Archimedean Property

Lemma

$\mathbb{N}$ *is not bounded above.*

Proof. Suppose, for the sake of contradiction, that $\mathbb{N}$ is bounded above. Let $x = \sup \mathbb{N}$. $x - 1$ is not an upper bound for $\mathbb{N}$, hence $\exists n \in \mathbb{N}$ with $n > x - 1$. Then $x < n + 1 \in \mathbb{N}$, contradiction! ■

Proof of Archimedean Property. To arrive at a contradiction, suppose Archimedean Property fails: there exist $a, b > 0$ so that $na \leqslant b \; \forall \; n \in \mathbb{N}$. Then $n \leqslant a^{-1}b \; \forall \; n \in \mathbb{N}$. IOW $a^{-1}b$ is an upper bound for $\mathbb{N}$, which does not exist! ■

Denseness of $\mathbb{Q}$ (Theorem 4.7)

Theorem (Denseness of $\mathbb{Q}$)

$\mathbb{Q}$ is dense in $\mathbb{R}$ – in other words, if $a, b \in \mathbb{R}$, $a < b$, then $\exists r \in \mathbb{Q} \cap (a, b)$.

Remark

In fact, (a, b) contains infinitely many rational points. Indeed, find $r_1 \in (a, b) \cap \mathbb{Q}$. Find an interval $(a_1, b_1) \subset (a, b) \setminus \{r_1\}$. Find $r_2 \in (a_1, b_1) \cap \mathbb{Q}$, and an interval $(a_2, b_2) \subset (a_1, b_1) \setminus \{r_2\}$. Proceeding further in the same manner, we find distinct rational numbers $r_1, r_2, \ldots \in (a, b)$.

Denseness of $\mathbb{Q}$ (Theorem 4.7)

Theorem (Denseness of $\mathbb{Q}$)

$\mathbb{Q}$ is dense in $\mathbb{R}$ – in other words, if $a, b \in \mathbb{R}$, $a < b$, then $\exists r \in \mathbb{Q} \cap (a, b)$.

Lemma. If $x, y \in \mathbb{R}$, $y - x > 1$, then $(x, y) \cap \mathbb{Z} \neq \emptyset$.

Proof of Lemma. Need to find $m \in \mathbb{Z}$, $x < m < y$. Use Archimedean property to pick $k \in \mathbb{N}$ with $k > |x| + |y|$.
Then $S = \{n \in \mathbb{Z} : |n| \leqslant k, n > x\}$ is a non-empty (since $k \in S$) *finite* set, hence it has a *minimum* m. This m works for us. Indeed, $m > x$. Want: $m < y$. If $m \geqslant y$, then $k \geqslant m > m - 1 \geqslant y - 1 > x$, so $m - 1 \in S$, which contradicts the minimality of m. ∎

Proof of denseness of $\mathbb{Q}$. Need to show that, if $a, b \in \mathbb{R}$, $a < b$, then $(a, b) \cap \mathbb{Q} \neq \emptyset$.
Use Arcimedean Property to find $n \in \mathbb{N}$ s.t. $n(b - a) > 1$.
Then $nb - na > 1$, hence, by Lemma, $\exists\, m \in \mathbb{Z} \cap (na, nb)$.
Conclude: $\dfrac{m}{n} \in (a, b)$. ∎