

Chapter 1: Sets, Fields and Orders

1.1 Definition: For sets A and B , we use the following notation. We write $x \in A$ when x is an **element** of the set A . We denote the **empty set**, that is the set with no elements, by \emptyset . We write $A = B$ when the sets A and B are **equal**, that is when A and B have the same elements. We write $A \subseteq B$ (some books write $A \subset B$) when A is a **subset** of B , that is when every element of A is also an element of B . We write $A \subset B$, or for emphasis $A \subsetneq B$, when A is a **proper subset** of B , that is when $A \subseteq B$ but $A \neq B$. We denote the **union** of A and B by $A \cup B$, the **intersection** of A and B by $A \cap B$, the set A **remove** B by $A \setminus B$ and the **product** of A and B by $A \times B$, that is

$$\begin{aligned} A \cup B &= \{x \mid x \in A \text{ or } x \in B\}, \\ A \cap B &= \{x \mid x \in A \text{ and } x \in B\}, \\ A \setminus B &= \{x \mid x \in A \mid x \notin B\}, \text{ and} \\ A \times B &= \{(a, b) \mid a \in A \text{ and } b \in B\}. \end{aligned}$$

We say that A and B are **disjoint** when $A \cap B = \emptyset$.

1.2 Theorem: (*Properties of Sets*) Let $A, B, C \subseteq X$. Then

- (1) (*Idempotence*) $A \cup A = A$, $A \cap A = A$,
- (2) (*Identity*) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, $A \cup X = X$, $A \cap X = A$,
- (3) (*Associativity*) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$,
- (4) (*Commutativity*) $A \cup B = B \cup A$ and $A \cap B = B \cap A$,
- (5) (*Distributivity*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
- (6) (*De Morgan's Laws*) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Proof: The proof is left as an exercise.

1.3 Definition: We write $\mathbf{N} = \{0, 1, 2, \dots\}$ for the set of **natural numbers** (which we take to include the number 0), $\mathbf{Z} = \{0, \pm 1, \pm 2, \dots\}$ for the set of **integers**, \mathbf{Q} for the set of **rational numbers** and we write \mathbf{R} for the set of **real numbers**. We assume familiarity with the algebraic operations $+$, $-$, \cdot , \div and with the order relations $<$, \leq , $>$, \geq on these sets. Some of the fundamental properties of these operations and order relations are discussed in this chapter.

1.4 Definition: For $a, b \in \mathbf{R}$ with $a \leq b$ we write

$$\begin{aligned} (a, b) &= \{x \in \mathbf{R} \mid a < x < b\}, \quad [a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}, \\ (a, b] &= \{x \in \mathbf{R} \mid a < x \leq b\}, \quad [a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}, \\ (a, \infty) &= \{x \in \mathbf{R} \mid a < x\}, \quad [a, \infty) = \{x \in \mathbf{R} \mid a \leq x\}, \\ (-\infty, b) &= \{x \in \mathbf{R} \mid x < b\}, \quad (-\infty, b] = \{x \in \mathbf{R} \mid x \leq b\}, \\ (-\infty, \infty) &= \mathbf{R}. \end{aligned}$$

An **interval** in \mathbf{R} is any set of one of the above forms. In the case that $a = b$ we have $(a, b) = [a, b) = (a, b] = [a, b] = \emptyset$ and $[a, b] = \{a\}$, and these intervals are called **degenerate** intervals. The intervals \emptyset , (a, b) , (a, ∞) , $(-\infty, b)$ and $(-\infty, \infty)$ are called **open** intervals. The intervals \emptyset , $[a, b]$, $[a, \infty)$, $(-\infty, b]$ and $(-\infty, \infty)$ are called **closed** intervals.

1.5 Definition: Let A and B be sets. A **relation** on $A \times B$ is a subset $r \subseteq A \times B$. When r is a relation on $A \times B$ and $a \in A$ and $b \in B$, we say that a and b are **related** under r and we write arb when $(a, b) \in r$. The **domain** and **range** of the relation r are the sets $\text{Domain}(r) = \{x \in A \mid xry \text{ for some } y \in B\}$ and $\text{Range}(r) = \{y \in B \mid xry \text{ for some } x \in A\}$.

1.6 Definition: Let A and B be sets. A **function** from A to B is a relation f on $A \times B$ with the property that for every $x \in A$ there exists a unique element $y \in B$ such that xfy . When f is a function from A to B , we write $f : A \rightarrow B$. When $f : A \rightarrow B$ and $x \in A$ we denote the unique element $y \in B$ for which xfy by $f(x)$. Note that $\text{Domain}(f) = A$ and $\text{Range}(f) \subseteq B$. A **binary operation** on A is a function $f : A \times A \rightarrow A$.

1.7 Definition: A **field** is a set F with two distinct elements $0, 1 \in F$ and two binary operations $+$ and \cdot such that

- (1) (Additive Associativity) for all $x, y, z \in F$ we have $(x + y) + z = x + (y + z)$,
- (2) (Additive Commutativity) for all $x, y \in F$ we have $x + y = y + x$,
- (3) (Additive Identity) for all $x \in F$ we have $0 + x = x$,
- (4) (Additive Inverse) for all $x \in F$ there exists a unique $y \in F$ such that $x + y = 0$,
- (5) (Multiplicative Associativity) for all $x, y, z \in F$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- (6) (Multiplicative Commutativity) for all $x, y \in F$ we have $x \cdot y = y \cdot x$,
- (7) (Multiplicative Identity) for all $x \in F$ we have $1 \cdot x = x$,
- (8) (Multiplicative Inverse) for all $0 \neq x \in F$ there exists a unique $y \in F$ such that $x \cdot y = 1$.
- (9) (Distributivity) for all $x, y, z \in F$ we have $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

1.8 Theorem: \mathbf{Q} and \mathbf{R} are fields.

Proof: We omit the proof, but we remark that \mathbf{Z} is not a field because it does not satisfy Property (8).

1.9 Notation: Let F be a field and let $a, b \in F$. We denote the unique additive inverse of a by $-a$ and we write $a - b = a + (-b)$. We usually write $a \cdot b$ simply as ab , and, when $a \neq 0$, we denote the unique multiplicative inverse of a by a^{-1} and we write $b \div a = \frac{b}{a} = b a^{-1}$.

1.10 Theorem: Let F be a field. Then for all $x, y, z \in F$ we have

- (1) (Additive Cancellation) if $x + y = x + z$ then $y = z$,
- (2) (Uniqueness of Additive Identity) if $x + y = x$ then $y = 0$,
- (3) (Multiplicative Cancellation) if $xy = xz$ then either $x = 0$ or $y = z$,
- (4) (Uniqueness of Multiplicative Identity) if $xy = x$ then $y = 1$,
- (5) (No Zero Divisors) if $xy = 0$ then $x = 0$ or $y = 0$.

Proof: The proof is left as an exercise.

1.11 Theorem: (Properties of Fields) Let F be a field. Then for all $x, y \in F$ we have $0 \cdot x = 0$, $-(-x) = x$, $-(x + y) = -x - y$, $(-1)x = -x$, $(-x)y = -(xy)$, $(-x)(-y) = xy$, $(a^{-1})^{-1} = a$, $(ab)^{-1} = a^{-1}b^{-1}$ and $(-a)^{-1} = -a^{-1}$.

Proof: The proof is left as an exercise.

1.12 Definition: An **order** on a set X is a binary relation \leq on X such that

- (1) (Totality) for all $x, y \in X$, either $x \leq y$ or $y \leq x$,
- (2) (Antisymmetry) for all $x, y \in X$, if $x \leq y$ and $y \leq x$ then $x = y$, and
- (3) (Transitivity) for all $x, y, z \in X$, if $x < y$ and $y < z$ then $x < z$.

An **ordered set** is a set X with an order \leq .

1.13 Theorem: Each of \mathbf{N} , \mathbf{Z} , \mathbf{Q} and \mathbf{R} is an ordered set using its standard order \leq . Under the inclusions $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$ the orders coincide (so that for example when $a, b \in \mathbf{N}$ we have $a \leq b$ in \mathbf{N} if and only if $a \leq b$ in \mathbf{R}).

Proof: We omit the proof.

1.14 Notation: When \leq is an order on X , we write $x < y$ when $x \leq y$ and $x \neq y$, we write $x \geq y$ when $y \leq x$ and we write $x > y$ when $y < x$.

1.15 Definition: An **ordered field** is a field F with an order \leq such that for all $x, y, z \in F$

- (1) if $x \leq y$ then $x + z \leq y + z$, and
- (2) if $0 \leq x$ and $0 \leq y$ then $0 \leq xy$.

When F is an ordered field and $x \in F$ we say that x is **positive** when $x > 0$, we say x is **negative** when $x < 0$, we say x is **nonpositive** when $x \leq 0$, and we say x is **nonnegative** when $x \geq 0$.

1.16 Theorem: \mathbf{Q} and \mathbf{R} are ordered fields.

Proof: We omit the proof.

1.17 Theorem: (Properties of Ordered Fields) Let F be an ordered field. Then for all $x, y, z \in F$

- (1) if $x > 0$ then $-x < 0$, and if $x < 0$ then $-x > 0$,
- (2) if $x > 0$ and $y < z$ then $xy < xz$,
- (3) if $x < 0$ and $y < z$ then $xy > xz$,
- (4) if $x \neq 0$ then $x^2 > 0$, and in particular $1 > 0$, and
- (5) if $0 < x < y$ then $0 < \frac{1}{y} < \frac{1}{x}$.

Proof: The proof is left as an exercise.

1.18 Definition: Let F be an ordered field. For $a \in F$ we define the **absolute value** of a to be

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

1.19 Theorem: (Properties of Absolute Value) Let F be an ordered field. For all $x, y \in F$

- (1) (Positive Definiteness) $|x| \geq 0$ with $|x| = 0 \iff x = 0$,
- (2) (Symmetry) $|x - y| = |y - x|$,
- (3) (Multiplicativeness) $|xy| = |x| |y|$
- (4) (Triangle Inequality) $||x| - |y|| \leq |x + y| \leq |x| + |y|$, and
- (5) (Approximation) for $a, b \in F$ with $b \geq 0$ we have $|x - a| \leq b \iff a - b \leq x \leq a + b$.

Proof: The proof is left as an exercise.

1.20 Theorem: (Induction Principle) Let $m \in \mathbf{Z}$. Let $F(n)$ be a statement about n . Suppose that

- (1) $F(m)$ is true, and
- (2) for all $k \in \mathbf{Z}$ with $k \geq m$, if $F(k)$ is true then $F(k+1)$ is true.

Then $F(n)$ is true for all $n \in \mathbf{Z}$ with $n \geq m$.

Proof: We omit the proof.

1.21 Theorem: (Basic Order Properties in \mathbf{Z})

- (1) for $n \in \mathbf{Z}$ we have $n \in \mathbf{N}$ if and only if $n \geq 0$,
- (2) for all $k, n \in \mathbf{Z}$ we have $k \leq n$ if and only if $k < n + 1$.

Proof: We omit the proof.

1.22 Theorem: (Strong Induction Principle) Let $m \in \mathbf{Z}$. Let $F(n)$ be a statement about n . Suppose that for all $n \in \mathbf{Z}$ with $n \geq m$, if $F(k)$ is true for all $k \in \mathbf{Z}$ with $m \leq k < n$ then $F(n)$ is true. Then $F(n)$ is true for all $n \in \mathbf{Z}$ with $n \geq m$.

Proof: Let $G(n)$ be the statement “ $F(k)$ is true for all $m \leq k < n$ ”. Note that $G(m)$ is true vacuously since there are no elements k with $m \leq k < m$. Let $n \in \mathbf{Z}$ with $n \geq m$ and suppose, inductively, that $G(n)$ is true, in other words that $F(k)$ is true for all $m \leq k < n$. It follows from the hypothesis of the theorem that $F(n)$ is true, and so we have $F(k)$ true for all $k \in \mathbf{Z}$ with $m \leq k \leq n$. By the Basic Order Property (2), it follows that $F(k)$ is true for all $k \in \mathbf{Z}$ with $m \leq k < n + 1$, or equivalently that $G(n + 1)$ is true. By the Induction Principle, it follows that $G(n)$ is true for all $n \in \mathbf{Z}$ with $n \geq m$. Let $n \in \mathbf{Z}$ with $n \geq m$. Since $G(n)$ is true, we know that $F(k)$ is true for all $k \in \mathbf{Z}$ with $m \leq k < n$. By the hypothesis of the theorem, it follows that $F(n)$ is true. Thus $F(n)$ is true for all $n \in \mathbf{Z}$ with $n \geq m$.

1.23 Example: Let $a_0 = 0$ and $a_1 = 1$ and for $n \geq 2$ let $a_n = a_{n-1} + 6a_{n-2}$. Show that $a_n = \frac{1}{5}(3^n - (-2)^n)$ for all $n \geq 0$.

Solution: We claim that $a_n = \frac{1}{5}(3^n - (-2)^n)$ for all $n \geq 0$. When $n = 0$ we have $a_n = a_0 = 0$ and $\frac{1}{5}(3^n - (-2)^n) = \frac{1}{5}(3^0 - (-2)^0) = 0$, so the claim is true when $n = 0$. When $n = 1$ we have $a_n = a_1 = 1$ and $\frac{1}{5}(3^n - (-2)^n) = \frac{1}{5}(3 - (-2)) = 1$, so the claim is true when $n = 1$. Let $n \geq 2$ and suppose the claim is true for all $k < n$. In particular we suppose the claim is true for $n-1$ and $n-2$, that is we suppose $a_{n-1} = \frac{1}{5}(3^{n-1} - (-2)^{n-1})$ and $a_{n-2} = \frac{1}{5}(3^{n-2} - (-2)^{n-2})$. Then

$$\begin{aligned}
 a_n &= a_{n-1} + 6a_{n-2} \\
 &= \frac{1}{5}(3^{n-1} - (-2)^{n-1}) + \frac{6}{5}(3^{n-2} - (-2)^{n-2}) \\
 &= \left(\frac{1}{5} \cdot 3^{n-1} + \frac{6}{5} \cdot 3^{n-2}\right) - \left(\frac{1}{5}(-2)^{n-1} + \frac{6}{5}(-2)^{n-2}\right) \\
 &= \left(\frac{3}{5} \cdot 3^{n-2} + \frac{6}{5} \cdot 3^{n-2}\right) - \left(-\frac{2}{5}(-2)^{n-2} + \frac{6}{5}(-2)^{n-2}\right) \\
 &= \frac{9}{5} \cdot 3^{n-2} - \frac{4}{5}(-2)^{n-2} = \frac{1}{5} \cdot 3^n - \frac{1}{5}(-2)^n \\
 &= \frac{1}{5}(3^n - (-2)^n) = \frac{1}{5}(3^n - (-2)^n).
 \end{aligned}$$

By Strong Induction, we have $a_n = \frac{1}{5}(3^n - (-2)^n)$ for all $n \geq 0$.

1.24 Definition: Let X be an ordered set and let $A \subseteq X$. We say that A is **bounded above** (in X) when there exists an element $b \in X$ such that $x \leq b$ for all $x \in A$, and in this case we say that b is an **upper bound** for A (in X).

We say that A is **bounded below** (in X) when there exists an element $a \in X$ such that $a \leq x$ for all $x \in A$, and in this case we say that a is a **lower bound** for A (in X). We say that A is **bounded** (in X) when A is bounded above and bounded below.

1.25 Definition: Let X be an ordered set and let $A \subseteq X$. We say that A has a **supremum** (or a **least upper bound**) (in X) when there exists an element $b \in X$ such that b is an upper bound for A with $b \leq c$ for every upper bound $c \in X$ for A , and in this case we say that b is the **supremum** (or the **least upper bound**) of A (in X) (note that if the supremum exists then it is unique by antisymmetry) and we write $b = \sup A$. When the supremum $b = \sup A$ exists and we have $b \in A$, then we also say that b is the **maximum element** of A and we write $b = \max A$.

We say that A has an **infimum** (or a **greatest lower bound**) (in X) when there exists an element $a \in X$ such that a is a lower bound for A with $c \leq a$ for every lower bound c for A , and in this case we say that a is the **infimum** (or the **greatest lower bound**) of A (in X) and we write $a = \inf A$. When $a = \inf A \in A$ we also say that a is the **minimum element** of A and we write $a = \min A$.

1.26 Example: Let $A = (0, \infty)$ and $B = [1, \sqrt{2})$. The set A is bounded below but not bounded above. The numbers -1 and 0 are both lower bounds for A and we have $\inf A = 0$. The set A has no minimum element and no maximum element. The set B is bounded above and below. The numbers 0 and 1 are both lower bounds for B and the numbers $\sqrt{2}$ and 3 are both upper bounds for B . We have $\inf B = 1$ and $\sup B = \sqrt{2}$. The set B has a minimum element, namely $\min B = \inf B = 1$, but B has no maximum element.

1.27 Theorem: (*Completeness Properties of \mathbf{R}*)

- (1) Every nonempty subset of \mathbf{R} which is bounded above in \mathbf{R} has a supremum in \mathbf{R} .
- (2) Every nonempty subset of \mathbf{R} which is bounded below in \mathbf{R} has an infimum in \mathbf{R} .

Proof: We omit the proof.

1.28 Theorem: (*Approximation Property of Supremum and Infimum*) Let $\emptyset \neq A \subseteq \mathbf{R}$.

- (1) If $b = \sup A$ then for all $0 < \epsilon \in \mathbf{R}$ there exists $x \in A$ with $b - \epsilon < x \leq b$, and
- (2) if $a = \inf A$ then for all $0 < \epsilon \in \mathbf{R}$ there exists $x \in A$ with $a \leq x < a + \epsilon$.

Proof: Let $b = \sup A$. Let $\epsilon > 0$. Suppose, for a contradiction, that there is no element $x \in A$ with $b - \epsilon < x$, or equivalently that for all $x \in A$ we have $b - \epsilon \geq x$. Let $c = b - \epsilon$. Note that c is an upper bound for A since $x \leq b - \epsilon = c$ for all $x \in A$. Since $b = \sup A$ and c is an upper bound for A we have $b \leq c$. But since $\epsilon > 0$ we have $b > b - \epsilon = c$ giving the desired contradiction. This proves that there exists $x \in A$ with $b - \epsilon < x$. Choose such an element $x \in A$. Since $b = \sup A$ we know that b is an upper bound for A and hence $b \geq x$. Thus we have $b - \epsilon < x \leq b$, as required.

1.29 Theorem: (Well-Ordering Properties of \mathbf{Z} in \mathbf{R})

- (1) Every nonempty subset of \mathbf{Z} which is bounded above in \mathbf{R} has a maximum element.
- (2) Every nonempty subset of \mathbf{Z} which is bounded below in \mathbf{R} has a minimum element, in particular every nonempty subset of \mathbf{N} has a minimum element.

Proof: We prove Part (1). Let A be a nonempty subset of \mathbf{Z} which is bounded in \mathbf{R} . By Completeness, A has a supremum in \mathbf{R} . Let $n = \sup A$. We must show that $n \in A$. Suppose, for a contradiction, that $n \notin A$. By the Approximation Property (using $\epsilon = 1$), we can choose $a \in A$ with $n - 1 < a \leq n$. Note that $a \neq n$ since $a \in A$ and $n \notin A$ and so we have $a < n$. By the Approximation Property again (using $\epsilon = n - a$) we can choose $b \in A$ with $a < b \leq n$. Since $a < b$ we have $b - a > 0$. Since $n - 1 < a$ and $b \leq n$ we have $1 = n - (n - 1) > b - a$. But then we have $b - a \in \mathbf{Z}$ with $0 < b - a < 1$ which contradicts the Basic Order Properties of \mathbf{Z} (since $b - a < 1 \implies b - a \leq 0$). Thus $n \in A$ so A has a maximum element.

1.30 Theorem: (Floor and Ceiling Properties of \mathbf{Z} in \mathbf{R})

- (1) (Floor Property) For every $x \in \mathbf{R}$ there exists a unique $n \in \mathbf{Z}$ with $x - 1 < n \leq x$.
- (2) (Ceiling Property) For every $x \in \mathbf{R}$ there exists a unique $m \in \mathbf{Z}$ with $x \leq m < x + 1$.

Proof: We prove Part (1). First we prove uniqueness. Let $x \in \mathbf{R}$ and suppose that $n, m \in \mathbf{Z}$ with $x - 1 < n \leq x$ and $x - 1 < m \leq x$. Since $x - 1 < n$ we have $x < n + 1$. Since $m \leq x$ and $x < n + 1$ we have $m < n + 1$ hence $m \leq n$. Similarly, we have $n \leq m$. Since $n \leq m$ and $m \leq n$, we have $n = m$. This proves uniqueness.

Next we prove existence. Let $x \in \mathbf{R}$. First let us consider the case that $x \geq 0$. Let $A = \{k \in \mathbf{Z} \mid k \leq x\}$. Note that $A \neq \emptyset$ because $0 \in A$ and A is bounded above in \mathbf{R} by x . By The Well-Ordering Property of \mathbf{Z} in \mathbf{R} , A has a maximum element. Let $n = \max A$. Since $n \in A$ we have $n \in \mathbf{Z}$ and $n \leq x$. Also note that $x - 1 < n$ since $x - 1 \geq n \implies x \geq n + 1 \implies n + 1 \in A \implies n \neq \max A$. Thus for $n = \max A$ we have $n \in \mathbf{Z}$ with $x - 1 < n \leq x$, as required.

Next consider the case that $x < 0$. If $x \in \mathbf{Z}$ we can take $n = x$. Suppose that $x \notin \mathbf{Z}$. We have $-x > 0$ so, by the previous paragraph, we can choose $m \in \mathbf{Z}$ with $-x - 1 < m \leq -x$. Since $m \in \mathbf{Z}$ but $x \notin \mathbf{Z}$ we have $m \neq -x$ so that $-x - 1 < m < -x$ and hence $x < -m < x + 1$. Thus we can take $n = -m - 1$ to get $x - 1 < n < x$. This completes the proof of Part (1).

1.31 Definition: Given $x \in \mathbf{R}$ we define the **floor** of x to be the unique $n \in \mathbf{Z}$ with $x - 1 < n \leq x$ and we denote the floor of x by $\lfloor x \rfloor$. The function $f : \mathbf{R} \rightarrow \mathbf{Z}$ given by $f(x) = \lfloor x \rfloor$ is called the **floor function**.

1.32 Theorem: (Archimedean Properties of \mathbf{Z} in \mathbf{R})

- (1) For every $x \in \mathbf{R}$ there exists $n \in \mathbf{Z}$ with $n > x$.
- (2) For every $x \in \mathbf{R}$ there exists $m \in \mathbf{Z}$ with $m < x$.

Proof: Let $x \in \mathbf{R}$. Let $n = \lfloor x \rfloor + 1$ and $m = \lfloor x \rfloor - 1$. Since $x - 1 < \lfloor x \rfloor$ we have $x < \lfloor x \rfloor + 1 = n$ and since $\lfloor x \rfloor \leq x$ we have $m = \lfloor x \rfloor - 1 \leq x - 1 < x$.

1.33 Theorem: (Density of \mathbf{Q} in \mathbf{R}) For all $a, b \in \mathbf{R}$ with $a < b$ there exists $q \in \mathbf{Q}$ with $a < q < b$.

Proof: Let $a, b \in \mathbf{R}$ with $a < b$. By the Archimedean Property, we can choose $n \in \mathbf{Z}$ with $n > \frac{1}{b-a} > 0$. Then $n(b-a) > 1$ and so $nb > na + 1$. Let $k = \lfloor na + 1 \rfloor$. Then we have $na < k \leq na + 1 < nb$ hence $a < \frac{k}{n} < b$. Thus we can take $q = \frac{k}{n}$ to get $a < q < b$.