Chapter 1. Rings, Fields, Orders and Cardinality

Introduction

Real analysis is similar to calculus, but with a strong emphasis placed on rigorous mathematical proofs. It is not possible to prove anything of interest without making some initial assumptions and, in this first chapter, we shall define rings and fields and ordered fields, and gather together and list all of the basic algebraic properties which hold in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ which are needed in mathematical proofs. We shall also briefly discuss cardinality.

In the second chapter, we shall prove some of the theorems, about limits, continuity and differentiation, whose proofs are normally omitted in calculus courses. We shall also introduce a few additional concepts, including Cauchy sequences and uniform continuity.

In the third chapter, we give a careful definition of the Riemann integral (which is usually described informally in calculus courses) and we prove many of the basic properties of the integral (which cannot be proven using only an informal definition of the integral).

The fourth chapter deals with sequences of functions and power series. We introduce the concept of uniform convergence (which is not usually mentioned in calculus courses) and prove various properties which allow us to show, for example, that power series can be differentiated and integrated term by term (a fact which is used often in calculus, physics and engineering, but which is not usually proven).

In the fifth chapter, we discuss various topological properties of sets in $\mathbb{R}^n$: we define open and closed sets, we study limit points and boundary points, and we study connected and compact sets. Then we discuss limits of sequences in $\mathbb{R}^n$ and limits and continuity of functions of several variables. We shall see that continuous functions preserve various properties of sets, for example, that continuous functions send connected sets to connected sets, and compact sets to compact sets.

In the sixth chapter, we study differentiation of function of several variables, and in the final chapter we study integration of functions of several variables.

Sets

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 $A\subsetneqq B$, when A is a **proper subset** of B, they 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

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

We say that A and B are **disjoint** when $A\cap B=\emptyset$. We also write $A^2=A\times A$.

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 Notation: We write $\mathbb{N} = \{0, 1, 2, \cdots\}$ for the set of **natural numbers** (which include the number 0), $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ for the set of **positive integers** $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ for the set of all **integers**, $\mathbb{Q}$ for the set of **rational numbers**, and $\mathbb{R}$ 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 will be discussed with some care in this chapter.

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

$$\begin{gathered}
(a, b) = \big\{x \in \mathbb{R} \big| a < x < b\big\}\ ,\ [a, b] = \big\{x \in \mathbb{R} \big| a \leq x \leq b\big\}\,, \\
(a, b] = \big\{x \in \mathbb{R} \big| a < x \leq b\big\}\ ,\ [a, b) = \big\{x \in \mathbb{R} \big| a \leq x < b\big\}\,, \\
(a, \infty) = \big\{x \in \mathbb{R} \big| a < x\big\}\ ,\ [a, \infty) = \big\{x \in \mathbb{R} \big| a \leq x\big\}\,, \\
(-\infty, b) = \big\{x \in \mathbb{R} \big| x \leq b\big\}\ ,\ (-\infty, b] = \big\{x \in \mathbb{R} \big| x \leq b\big\}\,, \\
(-\infty, \infty) = \mathbb{R}\,.
\end{gathered}$$

An **interval** in $\mathbb{R}$ is any set of one of the above forms. In the case that $a = b$ we have $(a, b) = [a, b) = (a, b] = \emptyset$ 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 Remark: In rigorous mathematics, most mathematical objects are defined to be sets. This includes objects that we do not normally think of as being sets, such as functions and sequences (a function is defined to be the set which we normally call its graph).

1.6 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 $\text{Domain}(r) = \big\{x \in A \big| xry \text{ for some } y \in B\big\}$ and $\text{Range}(r) = \big\{y \in B \big| xry \text{ for some } x \in A\big\}$. A **binary relation** on A is a relation on $A \times A$.

1.7 Example: The usual order relation $\leq$ on $\mathbb{R}$ is a binary relation on $\mathbb{R}$ (so $\leq\ \subseteq \mathbb{R}^2$). When x is less than or equal to y, we normally write $x \leq y$ rather than writing $(x, y) \in\ \leq$.

1.8 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 $f : A \to B$. When $f : A \to B$ 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 $f : A^2 \to A$ where $A^2 = A \times A$.

1.9 Example: The operation of addition of real numbers is a binary operation on $\mathbb{R}$ (so we have $+ \subseteq\ \mathbb{R}^2$). Given $x, y \in \mathbb{R}$, we usually write the sum $+(x, y)$ as $x + y$.

Rings and Fields

1.10 Definition: A **ring** (with identity) is a set R with distinct elements $0, 1 \in R$, called the **zero** and **identity** elements, and binary operations $+, \times : R^2 \to R$, called **addition** and **multiplication**, where for $a, b \in R$ we write $+(a, b)$ as $a + b$ and we write $\times(a, b)$ as $a \times b$ or $a \cdot b$ or ab, such that

R1. $+$ is associative: for all $a, b, c \in R$ we have $(a + b) + c = a + (b + c)$,
R2. $+$ is commutative: for all $a, b \in R$ we have $a + b = b + a$,
R3. 0 is an additive identity: for all $a \in R$ we have $a + 0 = a$,
R4. every $a \in R$ has an additive inverse: for all $a \in R$ there exists $b \in R$ such that $a + b = 0$,
R5. $\times$ is associative: for all $a, b, c \in R$ we have $(ab)c = a(bc)$,
R6. 1 is a multiplicative identity: for all $a \in R$ we have $a \cdot 1 = a = 1 \cdot a$, and
R7. $\times$ is distributive over $+$: for all $a, b, c \in R$ we have $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$.

A ring R is called **commutative** when

R8. $\times$ is commutative: for all $a, b \in R$ we have $ab = ba$.

A **field** is a commutative ring R in which

R9. every $0 \neq a \in R$ has an inverse: for all $0 \neq a \in R$ there exists $b \in R$ such that $ab = 1$.

Basic Assumption 1: $\mathbb{Z}$ and $\mathbb{R}$ are sets, there are distinct elements $0, 1 \in \mathbb{Z}$, and there are binary operations $+, \times$ on $\mathbb{R}$ which make $\mathbb{R}$ a field, and which restrict to give binary operations on $\mathbb{Z}$ making $\mathbb{Z}$ a commutative ring.

1.11 Example: There are many other examples of rings and fields. Here are a few:

The set $\mathbb{Q}$ of rational numbers (defined below) and the set $\mathbb{C}$ of complex numbers are fields.
The sets $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ are commutative rings.
The sets $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[i] = \{a+ib \mid a, b \in \mathbb{Q}\}$ are fields.

When $n \in \mathbb{Z}$ with $n \geq 2$, the set $\mathbb{Z}_n$ of integers modulo n is a ring using addition and multiplication modulo n. The ring $\mathbb{Z}_n$ is a field if and only if n is a prime number.

When R is a ring and $n \in \mathbb{Z}$ with $n \geq 2$, the set $M_n(R)$ of $n \times n$ matrices with entries in R, is a non-commutative ring using matrix addition and matrix multiplication.

1.12 Definition: Let R be a ring. For $a, b \in R$, if $ab = 1$ then we say that a is a **left inverse** of b and that b is a **right inverse** of a, and if we have both $ab = 1$ and $ba = 1$ then we say that a is an **inverse** of b and that b is an **inverse** of a. For $a \in R$, if there exists $b \in R$ such that $ab = ba = 1$ then we say that a is **invertible** or that a is a **unit**.

1.13 Example: In $\mathbb{Z}$, the numbers 1 and -1 are the only units, and each is equal to its own inverse. In a field, every nonzero element is a unit (by R9). In $\mathbb{Z}[\sqrt{2}]$, the elements $a = 3 + 2\sqrt{2}$ and $b = 3 - 2\sqrt{2}$ are inverses of each other. In $\mathbb{Z}_6$ the only units are 1 and 5, and each is equal to its own inverse. In $\mathbb{Z}_7$ (which is a field) we have $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ and $6^{-1} = 6$. In $M_2(\mathbb{Z})$, the matrices $A = \left(\begin{smallmatrix} 1 & 3 \\ 2 & 5 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} -5 & 3 \\ 2 & -1 \end{smallmatrix}\right)$ are inverses of each other.

1.14 Definition: Let R be a ring. For $a, b \in R$, if $a \neq 0$ and $b \neq 0$ and $ab = 0$ then we say that a and b are **zero divisors**. A commutative ring with no zero divisors is called an **integral domain**.

1.15 Example: In $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$ and $4 \cdot 3 = 0$, and so 2, 3 and 4 are zero divisors. In $M_2(\mathbb{Z})$, for $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 6 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 2 & -4 \\ -1 & 2 \end{smallmatrix}\right)$ we have $AB = O$, so A and B are zero divisors.

1.16 Theorem: *(Uniqueness of Identity and Inverse) Let R be a ring. Then*
(1) the additive identity 0 is unique in the sense that if $e \in R$ has the property that $a+e=a$ for all $a \in R$ then $e=0$,
(2) the additive inverse of $a \in G$ is unique in the sense that for all $a,b,c \in G$ if $a+b=0$ and $a+c=0$ then $b=c$,
(3) the multiplicative identity 1 is unique in the sense that if $u \in R$ has the property that $au=ua=a$ for all $a \in G$ then $u=1$, and
(4) if $a \in R$ has an inverse, then it is unique in the sense that for all $a,b,c \in G$ if $ab=ba=1$ and $ac=ca=1$ then $b=c$.

Proof: Let us prove Part (1). Let $e \in R$ and suppose that $a+e=a$ for all $a \in R$. Then

$$\begin{aligned} e &= e+0 \ \text{, by R3,} \\ &= 0+e \ \text{, by R2,} \\ &= 0 \ \text{, since } a+e=a \text{ for all } a \in R \text{ so in particular } 0+e=0. \end{aligned}$$

Let us prove Part (2). Let $a,b,c \in R$ and suppose that $a+b=0$ and $a+c=0$. Then

$$\begin{aligned} b &= b+0 \text{ , by R3,} \\ &= 0+b \text{ , by R2,} \\ &= (a+c)+b \text{ , since } a+c=0, \\ &= (c+a)+b \text{ , by R2,} \\ &= c+(a+b) \text{ , by R1,} \\ &= c+0 \text{ , since } a+b=0, \\ &= c \text{ , by R3.} \end{aligned}$$

The proof of Parts (3) and (4) is left as an exercise.

1.17 Notation: Let R be a ring. For $a \in R$ we denote the unique additive inverse of $a \in R$ by $-a$, and for $a,b \in R$ we write $b-a$ for $b+(-a)$. When $a \in R$ is invertible, we denote its unique multiplicative inverse by a^{-1}. When F is a field and $a \neq 0$ we also write a^{-1} as $\frac{1}{a}$, and when $a,b \in F$ with $a \neq 0$, we write $b \div a = b/a = \frac{b}{a} = b\,a^{-1}$.

1.18 Theorem: *(Properties of Rings) Let R be a ring. Let $a,b,c,d \in R$.*
(1) If $a+b=a+c$ then $b=c$.
(2) If $a+b=a$ then $b=0$.
(3) If $a+b=0$ then $b=-a$.
(4) $a \cdot 0 = 0 = 0 \cdot a$.
(5) $-(-a)=a$.
(6) $(-a)b=-(ab)=a(-b)$.
(7) $(-a)(-b)=ab$.
(8) $(-1)a=-a$.
(9) $a(b-c)=ab-ac$ and $(a-b)c=ac-bc$.
(10) If $ab=1$ and $bc=1$ then b is invertible and $a=c=b^{-1}$.
(11) If a and b are invertible then so is ab and we have $(ab)^{-1}=b^{-1}a^{-1}$.
(12) If $ab=ac$, or if $ba=ca$, then either $a=0$, or $b=c$, or a is a zero divisor,
(13) If a is a unit then a is not a zero divisor.
(14) If R is a field and $b,d \neq 0$ then

$$-\left(\tfrac{a}{b}\right) = \tfrac{-a}{b} \ , \ \tfrac{a}{b} \pm \tfrac{c}{d} = \tfrac{ad \pm bc}{bd} \ , \ \tfrac{a}{b} \cdot \tfrac{c}{d} = \tfrac{ac}{bd} \text{ and, if } a \neq 0 \text{ then } \left(\tfrac{a}{b}\right)^{-1} = \tfrac{b}{a}.$$

Proof: We give a few sample proofs. To prove Part (1), suppose that $a+b=a+c$. Let $d=-a$ so that $a+d=0$ (we can do this by R4). Then

$$\begin{aligned} b &= b+0 \text{ , by R3,} \\ &= b+(a+d) \text{ , since } a+d=0, \\ &= (b+a)+d \text{ , by R1,} \\ &= (a+b)+d \text{ , by R2,} \\ &= (a+c)+d \text{ , since } a+b=a+c, \\ &= (c+a)+d \text{ , by R2,} \\ &= c+(a+d) \text{ , by R1,} \\ &= c+0 \text{ , since } a+d=0, \\ &= c \text{ , by R3.} \end{aligned}$$

To prove Part (2), suppose that $a+b=a$. Since $a+b=a$ and $a=a+0$ (by R3), we have $a+b=a+0$, and so $b=0$ by Part (1).

To prove Part (3), suppose that $a+b=0$. Since $a+b=0$ and $0=a+(-a)$, we have $a+b=a+(-a)$, and so $b=-a$ by Part (1).

To prove Part (4), note that since $0=0+0$ (by R3) we have $0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$ (by R7). Since $0\cdot a+0\cdot a=0\cdot a$ it follows that $0\cdot a=0$, by Part (1). Similarly, $a\cdot 0=0$.

To prove Part (5), note that $(-a)+a=a+(-a)=0$ so $a=-(-a)$ by Part (3).

To prove Part (8), note that

$$\begin{aligned} a+(-1)a &= 1\cdot a+(-1)a \text{ , by R6,} \\ &= (1+(-1))\cdot a \text{ , by R7,} \\ &= 0\cdot a \text{ , since } 1+(-1)=0, \\ &= 0 \text{ , by Part (4).} \end{aligned}$$

Since $a+(-1)a=0$ we have $(-1)a=-a$ by Part (3).

To prove Part (10), suppose $ab=1$ and $bc=1$. Then $a=a\cdot 1=a(bc)=(ab)c=1\cdot c=c$.

To prove the addition formula in Part (14), suppose R is a field and $b,d\neq 0$. Note that b and d are invertible by $R9$, and we have

$$\begin{aligned} \tfrac{a}{b}+\tfrac{c}{d} &= ab^{-1}+cd^{-1} \text{ , using Notation 1.17} \\ &= (ab^{-1})(dd^{-1})+(cd^{-1})(bb^{-1}) \text{ , by R6 since } dd^{-1}=1 \text{ and } bb^{-1}=1 \\ &= (ad)(d^{-1}b^{-1})+(bc)(d^{-1}b^{-1}) \text{ , by R5 and R8 used several times} \\ &= (ad+bc)(bd)^{-1} \text{ , by R7 and since } d^{-1}b^{-1}=(bd)^{-1} \text{ by Part 11} \\ &= \tfrac{ad+bc}{bd} \text{ , using Notation 1.17.} \end{aligned}$$

1.19 Definition: The set $\mathbb{Q}$ of **rational numbers** is defined to be

$$\mathbb{Q}=\left\{\tfrac{a}{b}\,\middle|\,a,b\in\mathbb{Z} \text{ with } b\neq 0\right\}.$$

1.20 Theorem: *The set $\mathbb{Q}$ is a field using the (restriction of) the operations used in $\mathbb{R}$.*

Proof: This follows mainly from Part (14) of the previous theorem.

Ordered Fields

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

O1. (Totality) for all $x, y \in X$, either $x \leq y$ or $y \leq x$,
O2. (Antisymmetry) for all $x, y \in X$, if $x \leq y$ and $y \leq x$ then $x = y$, and
O3. (Transitivity) for all $x, y, z \in X$, if $x \leq y$ and $y \leq z$ then $x \leq z$.

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

1.22 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 $y < x$.

1.23 Theorem: *Let $\leq$ be an order on a set X. Then*
(1) for all $x, y \in X$, we have $x \leq y \iff \big(x < y$ or $x = y\big)$,
(2) for all $x, y \in X$ exactly one of the following 3 statements holds:

$$x = y,\ x < y \text{ or } y < x.$$

(3) for all $x, y, z \in X$, if $x < y$ and $y < z$ then $x < z$.

Solution: We shall only prove Parts (1) and (2). Let $x, y \in X$. By the definition of $<$, to prove Part (1) we need to show that $x \leq y \iff \big((x \leq y \text{ and } x \neq y) \text{ or } x = y\big)$. Suppose first that $x \leq y$. Note that either $x = y$ or $x \neq y$. If $x = y$ then the statement $\big((x \leq y \text{ and } x \neq y) \text{ or } x = y\big)$ is true. If $x \neq y$ then we have $(x \leq y \text{ and } x \neq y)$ and so again the statement $\big((x \leq y \text{ and } x \neq y) \text{ or } x = y\big)$ is true. This completes the proof that $x \leq y \Longrightarrow \big((x \leq y \text{ and } x \neq y) \text{ or } x = y\big)$. Suppose, conversely, that either $(x \leq y \text{ and } x \neq y)$ or $x = y$. If $x \leq y$ and $x \neq y$ then of course $x \leq y$. Suppose that $x = y$. By applying O1 in the case that $y = x$, we find that $(x \leq x \text{ or } x \leq x)$ or, more simply, $x \leq x$. Since $x = y$ and $x \leq x$ if follows (by substitution) that $x \leq y$. This completes the proof that $\big((x \leq y \text{ and } x \neq y) \text{ or } x = y\big) \Longrightarrow x \leq y$.

Let us prove Part (2). First we show that at least one of the 3 statement holds. We need to show that either $(x = y \text{ or } x < y)$ or $y < x$. By Part (1), this is equivalent to showing that either $x \leq y$ or $y < x$. Suppose that $y \not< x$. By the definition of $y < x$ we are supposing that it is not the case that $(y \leq x \text{ and } y \neq x)$ or, equivalently, we are supposing that either $y \not\leq x$ or $y = x$. In the case that $y \not\leq x$, it follows by O1 that $x \leq y$. In the case that $y = x$ we already showed above that $x \leq y$. This completes the proof that at least 1 of the 3 statements holds. It is not possible to have $x = y$ and $x < y$ because, by definition, when $x < y$ we have $x \neq y$. Similarly it is not possible to have $x = y$ and $y < x$. Suppose, for a contradiction, that $x < y$ and $y < x$. Since $x < y$ we have $x \leq y$ (by the definition of $x < y$). Since $y < x$ we have $y \leq x$ (by definition). Since $x \leq y$ and $y \leq x$ we have $x = y$ by O2. But since $x < y$ we have $x \neq y$ (by definition) and this gives the desired contradiction.

1.24 Definition: An **ordered field** is a field F with an order $\leq$ such that

O4. (Compatibility with $+$) for all $x, y, z \in F$, if $x \leq y$ then $x + z \leq y + z$, and

O5. (Compatibility with $\times$) for all $x, y \in F$, 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 $x \geq 0$.

Basic Assumption 2: The field $\mathbb{R}$ is an ordered field using its usual order relation $\leq$.

1.25 Note: Any subset of $\mathbb{R}$ is an ordered set using the order relation $\leq$. Any field F, which is a subset of $\mathbb{R}$ and uses the same operations, is an ordered field using $\leq$.

1.26 Definition: We define the sets $\mathbb{N} = \big\{n\in\mathbb{Z}\,\big|\,n \geq 0\big\}$ and $\mathbb{Z}^+ = \big\{n\in\mathbb{Z}\,\big|\,n \geq 1\big\}$.

1.27 Note: We have $\mathbb{N} \subseteq \mathbb{Z}^+ \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. These are all ordered sets, and $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields.

1.28 Example: There are many ordered fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{R}$, for example $F=\mathbb{Q}[\sqrt{2}]$.

1.29 Theorem: *(Properties of Ordered Fields) Let F be an ordered field. Then for all $x, y, z \in F$*
(1) if $x \geq 0$ then $-x \leq 0$, and if $x \leq 0$ then $-x \geq 0$,
(2) if $x \geq 0$ and $y \leq z$ then $xy \leq xz$,
(3) if $x \leq 0$ and $y \leq z$ then $xz \leq xy$,
(4) $0 \leq x^2$,
(5) we have $0 < 1$ and $-1 < 0$, and
(6) if $0 < x$ then $0 < \frac{1}{x}$ and if $0 < x \leq y$ then $0 < \frac{1}{y} \leq \frac{1}{x}$.

Proof: We shall provide two proofs for each of the first two parts. The first proof will be brief, using standard mathematical language, and will use some of the properties from Definition 1.10 and Theorem 1.18 implicitly. The second proof will be more detailed, indicating explicitly which property is being used at each step of the proof. Then we provide brief proofs for each of the remaining parts.

For the first proof of Part (1), let $x \in F$. If $x \geq 0$, that is if $0 \leq x$, then by O4 we have $0+(-x) \leq x+(-x)$ hence $-x \leq 0$, and if $x \leq 0$ then by O4 we have $x+(-x) \leq 0+(-x)$ hence $0 \leq -x$.

We now repeat the above prof of Part (1) adding additional detail. Let $x \in F$ be arbitrary. Let $u = -x$ so that $x + u = 0$ (using R4 and the Notation 1.17). First suppose that $x \geq 0$, which means that $0 \leq x$ by Notation 1.22. Then

$$\begin{aligned}
0 + u \leq x + u &\text{ , by O4,} \\
0 + u \leq 0 &\text{ , since } x + u = 0, \\
u + 0 \leq 0 &\text{ , since } 0 + u = u + 0 \text{ by R2,} \\
u \leq 0 &\text{ , since } u + 0 = u \text{ by R3,} \\
-x \leq 0 &\text{ , since } u = -x.
\end{aligned}$$

Next suppose that $x \leq 0$. Then

$$\begin{aligned}
x + u \leq 0 + u &\text{ , by O4,} \\
0 \leq 0 + u &\text{ , since } x + u = 0, \\
0 \leq u + 0 &\text{ , since } 0 + u = u + 0 \text{ by R2,} \\
0 \leq u &\text{ , since } u + 0 = u \text{ by R3.} \\
u \geq 0 &\text{ , by Notation 1.22,} \\
-x \geq 0 &\text{ , since } u = -x.
\end{aligned}$$

To prove Part (2), let $x, y, z \in F$ and suppose that $0 \leq x$ and $y \leq z$. Since $y \leq z$, by O4 we have $y + (-y) \leq z + (-y)$, hence $0 \leq z - y$. Since $0 \leq x$ and $0 \leq z - y$, by O5 we have $0 \leq x(z - y)$, and hence by Theorem 1.18 Part (9) we have $0 \leq xz - xy$. By O4 it follows that $0 + xy \leq (xz - xy) + xy$. Thus

$$xy = xy + 0 = 0 + xy \leq (xz - xy) + xy = xz + (-xy + xy) = xz + 0 = xz.$$

We now provide a second proof of Part (2), adding additional detail to the above proof. Also, we shall avoid using Part (9) of Theorem 1.18, since we did not prove it. Instead, we shall use Part (4) which we did prove.

Let $x, y, z \in F$ be arbitrary. Suppose that $x \geq 0$, that is $0 \leq x$, and suppose that $y \leq z$. Let $u = -y$ so that $y + u = 0$ (using R4 and Notation 1.17). Then

$$\begin{aligned}
y + u \leq z + u &\text{ , since } y \leq z, \text{ by O4,} \\
0 \leq z + u &\text{ , since } y + u = 0, \\
0 \leq x(z + u) &\text{ , since } 0 \leq x \text{ and } 0 \leq z + u, \text{ by O5,} \\
0 \leq xz + xu &\text{ , by R7,} \\
0 + xy \leq (xz + xu) + xy &\text{ , by O4,} \\
0 + xy \leq xz + (xu + xy) &\text{ , by R1,} \\
0 + xy \leq xz + x(u + y) &\text{ , by R7,} \\
0 + xy \leq xz + x(y + u) &\text{ , by R2,} \\
0 + xy \leq xz + x \cdot 0 &\text{ , since } y + u = 0, \\
0 + xy \leq xz + 0 &\text{ , by Theorem 1.18 Part (4),} \\
0 + xy \leq xz &\text{ , by R3,} \\
xy + 0 \leq xz &\text{ , by R2,} \\
xy \leq xz &\text{ , by R3.}
\end{aligned}$$

To prove Part (3), let $x, y, z \in F$ and suppose that $x \leq 0$ and $y \leq z$. Since $x \leq 0$ we have $0 \leq -x$ by Part (1). Since $y \leq z$, by O4 we have $y - y \leq z - y$, that is $0 \leq z - y$. Since $0 \leq -x$ and $0 \leq z - y$, by O5 we have $0 \leq (-x)(z - y)$. Using some properties of rings, it follows that $0 \leq xy - xz$ hence, by O4, $0 + xz \leq (xy - xz) + xz$, and hence $xz \leq xy$.

We prove Part (4) by considering two cases. Let $x \in F$ be arbitrary. By O1 we know that either $x \leq 0$ or $0 \leq x$. If $0 \leq x$ then by O5 we have $0 \leq x \cdot x$, that is $0 \leq x^2$. If $x \leq 0$ then by Part (1) we have $0 \leq -x$ and so, by O5, we have $0 \leq (-x)(-x)$ hence, by Part (7) of Theorem 1.18, we have $0 \leq x \cdot x$, that is $0 \leq x^2$. In either case we find that $0 \leq x^2$, as required.

By Part (4) we have $0 \leq 1^2 = 1$. Since $0 \leq 1$ and $0 \neq 1$, we have $0 < 1$. We leave the proof that $-1 < 0$ as an exercise.

To prove Part (6), let $x, y \in F$ with $0 < x \leq y$. Suppose, for a contradiction, that $\frac{1}{x} \leq 0$. Since $0 \leq x$ and $\frac{1}{x} \leq 0$ it follows from Part (2) that $x \cdot \frac{1}{x} \leq x \cdot 0$, and hence $1 \leq 0$. But we know from Part (4) that $0 < 1$ and so we have the desired contradiction. Since it is not the case that $\frac{1}{x} \leq 0$ we must have $0 < \frac{1}{x}$ by O1 and O2. Since $0 \leq x$ and $x \leq y$ we have $0 \leq y$ by O3. If we had $y = 0$ then we would have $y = 0 < x$ and $x \leq y$ which is not possible by O1 and O2. Since $0 \leq y$ and $y \neq 0$ we have $0 < y$. As above, since $0 < y$ we have $0 < \frac{1}{y}$. It remains to show that $\frac{1}{y} \leq \frac{1}{x}$. If $x = y$ then $\frac{1}{x} = \frac{1}{y}$. Suppose that $x < y$. If we had $\frac{1}{x} \leq \frac{1}{y}$ then, since $0 \leq x$ and $0 \leq y$, it would follow from O5 that $\frac{1}{x}\,xy \leq \frac{1}{y}\,xy$, so that $y \leq x$, which contradicts the fact that $x < y$. Thus $\frac{1}{y} < \frac{1}{x}$.

1.30 Note: The various properties of ordered fields, which were stated in terms of the order relation $\leq$, have analogous counterparts involving the strict order relation $<$. As an exercise, verify that the following properties hold when F is an ordered field and $x, y, z \in F$.

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

1.31 Note: It is not possible to define an order $\leq$ on $\mathbb{C}$ which makes $\mathbb{C}$ into an ordered field because if $\mathbb{C}$ was an ordered field then since $0 < 1$ we would have $-1 < 0$ (by Part 3) but since $-1 = i^2$ we would also have $-1 > 0$ (by Part 6).

Also, when p is a prime number so that $\mathbb{Z}_p$ is a field, it is not possible to define an order $\leq$ on $\mathbb{Z}_p$ which makes it an ordered field, because if $\mathbb{Z}_p$ was an ordered field then we would have $0 < 1 < 1 + 1 < \cdots < 1 + 1 + \cdots 1 = 0$ (the sum of p copies of 1 is equal to 0).

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

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

1.33 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) $\big||x| - |y|\big| \leq |x + y| \leq |x| + |y|$, 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.

Basic Assumption 3: (The Discreteness Property of $\mathbb{Z}$) There does not exist $k \in \mathbb{Z}$ with $0 < k < 1$. Equivalently, for all $n \in \mathbb{Z}$ there does not exist $k \in \mathbb{Z}$ with $n < k < n + 1$.

1.34 Example: Prove that for all $k, l \in \mathbb{Z}$, if $kl = 1$ then either $k = l = 1$ or $k = l = -1$.

Solution: Let $k, l \in \mathbb{Z}$ and suppose that $kl = 1$. By Theorem 1.23 Part (2), applied several times, exactly 1 of the following 7 possibilities holds: $k < -1$, $k = -1$, $-1 < k < 0$, $k = 0$, $0 < k < 1$, $k = 1$ or $1 < k$. Note that $k \neq 0$ since if we had $k = 0$ then we would have $1 = kl = 0 \cdot l = 0$. Also, we cannot have $-1 < k < 0$ or $0 < k < 1$ by the Discreteness Property, so we are left with the following 4 possibilities: $k < -1$, $k = -1$, $k = 1$ or $1 < k$. Suppose, for a contradiction, that $1 < k$. By Theorem 1.29 Part (5) we have $0 < 1 < k$, so by Note 1.30 Part (7) we have $0 < \frac{1}{k} < \frac{1}{1}$. This implies that $0 < l < 1$ $\big($because $kl = 1$ so that $l = \frac{1}{k}$ and $1 \cdot 1 = 1$ so that $\frac{1}{1} = 1\big)$, but this is not possible by the Discreteness Property. Similarly, if we had $k < -1$ then we would have $\frac{1}{-1} < \frac{1}{k} < 0$ and hence $-1 < l < 0$, which is impossible by Discreteness. Thus we have eliminated 5 of the 7 possibilities leaving only the 2 possibilities $k = \pm 1$. Finally note that when $k = 1$ we have $1 = kl = 1 \cdot l = l$ and when $k = -1$ we have $1 = kl = (-1)l = -l$.

Upper and Lower Bounds

1.35 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.

We say that A has a **maximum** element when there exists $b \in A$ with $b \geq x$ for every $x \in A$. In this case, the maximum element $b \in A$ is unique, and we write $b = \max A$. We say that A has a **supremum** (or a **least upper bound**) (in X) when there exists $b \in X$ such that b is an upper bound for A with $b \leq c$ for every upper bound $c \in X$ for A. In this case, the supremum (or least upper bound) $b \in F$ is unique, and we write $b = \sup A$. Verify that when A has a supremum $b = \sup A \in F$, if $b \in A$ then $b = \max A$ and if $b \notin A$ that A has no maximum element.

We say that a has a **minimum** element when there exists $a \in A$ with $a \leq x$ for every $x \in A$, and in this case we write $a = \min A$. We say that A has an **infimum** (or a **greatest lower bound**) (in X) when there exists $a \in X$ 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 write $a = \inf A$. Verify that when $a = \inf A \in F$, if $a \in A$ then $a = \min A$ and if $a \notin A$ then A has no minimum.

1.36 Example: Let $A = (0, \infty) = \{x \in \mathbb{R} \,|\, 0 < x\}$ and $B = [1, \sqrt{2}) = \{x \in \mathbb{R} \,|\, 1 \leq x < \sqrt{2}\}$. 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.

1.37 Theorem: *(Approximation Property of Supremum and Infimum) Let F be an ordered field, let $\emptyset \neq A \subseteq F$, and let $b \in F$. Then*

(1) $b = \sup A \iff \big(\forall\, x \in A\ x \leq b \ \text{ and } \ \forall\, 0 < \epsilon \in F\ \exists\, x \in A\ b - \epsilon < x\big)$.

(2) $b = \ \inf A \iff \big(\forall\, x \in A\ b \leq x \ \text{ and } \ \forall\, 0 < \epsilon \in F\ \exists\, x \in A\ x < b + \epsilon\big)$.

Proof: We prove Party 1. Suppose that $b = \sup A$. Since b is an upper bound for A, we have $b \geq x$ for every $x \in A$. It remains to prove that $\forall 0 < \epsilon \in F\ \exists\, x \in A\ b - \epsilon < x$. Suppose not. Then we can choose $\epsilon > 0$ such that for all $x \in A$ we have $b - \epsilon \geq x$. But then $b - \epsilon$ is an upper bound for A, and since $b - \epsilon < b$, this contradicts the fact that b is the smallest upper bound for A.

Suppose, conversely, that $\forall\, x \in A\ x \leq b$ and $\forall\, 0 < \epsilon \in F\ \exists\, x \in A\ b - \epsilon < x$. The fact that $\forall\, x \in A\ x \leq b$ means that b is an upper bound for A. It remains to prove that if c is any upper bound for A then $b \leq c$. Let $c \in F$ and suppose that $b > c$. From the assumption $\forall\, 0 < \epsilon \in F\ \exists\, x \in A\ b - \epsilon < x$, taking $\epsilon = b - c > 0$, we can choose $x \in A$ such that $b - (b - c) < x$, that is $c < x$, so c is not an upper bound for A.

Basic Assumption 4: (The Least Upper, and Greatest Lower Bound Properties of $\mathbb{R}$) Every nonempty subset of $\mathbb{R}$ which is bounded above in $\mathbb{R}$ has a supremum in $\mathbb{R}$. Equivalently, every nonempty subset of $\mathbb{R}$ which is bounded below in $\mathbb{R}$ has an infimum in $\mathbb{R}$.

Summary of all Basic Assumptions: We assume that $\mathbb{R}$ is an ordered field with the least upper bound property, and $\mathbb{Z}$ is a subring of $\mathbb{R}$, with the discreteness property.

1.38 Theorem: *(Well-Ordering Properties of $\mathbb{Z}$ in $\mathbb{R}$)*

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

Proof: We prove Part (1). Let A be a nonempty subset of $\mathbb{Z}$ which is bounded above in $\mathbb{R}$. By the Least Upper Bound Property, A has a supremum in $\mathbb{R}$. 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 $b - a \in \mathbb{Z}$ with $0 < b - a < 1$ which contradicts the Discreteness Property of $\mathbb{Z}$. Thus $n \in A$ so A has a maximum element.

1.39 Theorem: *(Floor and Ceiling Properties of $\mathbb{Z}$ in R)*

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

Proof: We prove Part (1). First we prove uniqueness. Let $x \in \mathbb{R}$ and suppose that $n, m \in \mathbb{Z}$ 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 $x \in \mathbb{R}$. First let us consider the case that $x \geq 0$. Let $A = \{k \in \mathbb{Z} \,|\, k \leq x\}$. Note that $A \neq \emptyset$ because $0 \in A$ and A is bounded above in $\mathbb{R}$ by x. By The Well-Ordering Property of $\mathbb{Z}$ in $\mathbb{R}$, A has a maximum element. Let $n = \max A$. Since $n \in A$ we have $n \in \mathbb{Z}$ 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 $n \in \mathbb{Z}$ with $x - 1 < n \leq x$, as required.

Next consider the case that $x < 0$. If $x \in \mathbb{Z}$ we can take $n = x$. Suppose that $x \notin \mathbb{Z}$. We have $-x > 0$ so, by the previous paragraph, we can choose $m \in \mathbb{Z}$ with $-x - 1 < m \leq -x$. Since $m \in \mathbb{Z}$ but $x \notin \mathbb{Z}$ 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).

1.40 Definition: For $x \in \mathbb{R}$, the unique $n \in \mathbb{Z}$ with $x - 1 < n \leq x$ is called the **floor** of x, and we write $n = \lfloor x \rfloor$. The function $f : \mathbb{R} \to \mathbb{Z}$ given by $f(x) = \lfloor x \rfloor$ is called the **floor function**. The unique $m \in \mathbb{Z}$ with $x \leq m < x + 1$ is called the **ceiling** of x, and we write $m = \lceil x \rceil$. The function $f : \mathbb{R} \to \mathbb{Z}$ given by $f(x) = \lceil x \rceil$ is called the **ceiling function**.

1.41 Theorem: *(Archimedean Property of $\mathbb{Z}$ in $\mathbb{R}$)*

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

Proof: Let $x \in \mathbb{R}$. 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 $m = \lfloor x \rfloor - 1 \leq x - 1 < x$.

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

Proof: Let $a, b \in \mathbb{R}$ with $a < b$. By the Archimedean Property, we can choose $n \in \mathbb{Z}$ 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 $a < q < b$.

Mathematical Induction

1.43 Theorem: *(Induction Principle) Let $m \in \mathbb{Z}$. Let $F(n)$ be a statement about n. Suppose that $F(m)$ is true, and suppose that for all $k \in \mathbb{Z}$ with $k > m$, if $F(k-1)$ is true then $F(k)$ is true. Then $F(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq m$.*

Proof: Let $S = \big\{k\in\mathbb{Z}\big|k\geq m \text{ and } F(k) \text{ is false}\big\}$. To prove that $F(n)$ is true for all $n \geq m$, we shall prove that $S = \emptyset$. Suppose, for a contradiction, that $S \neq \emptyset$. Since $S \neq \emptyset$ and S is bounded below by m, it follows from the Well-Ordering Property of $\mathbb{Z}$ that S has a minimum element. Let $k = \min(S)$. Since $k \in S$ it follows that $k \geq m$ and $F(k)$ is false. Since $F(m)$ is true and $F(k)$ is false, it follows that $k \neq m$, so we have $k > m$. We claim that $F(k-1)$ is true. Suppose, for a contradiction, that $F(k-1)$ is false. Since $k-1 \geq m$ and $F(k-1)$ is false, it follows that $k-1 \in S$. Since $k = \min(S)$ and $k-1 \in S$, we have $k \leq k-1$ giving the desired contradiction (to the assumption that $F(k-1)$ is false). Thus $F(k-1)$ is true, as claimed. Since $k > m$ and $F(k-1)$ is true, it follows by the hypothesis in the statement of the theorem that $F(k)$ is true. But, as mentioned earlier, since $k \in S$ we know that $F(k)$ is false, so we have obtained the desired contradiction (to the assumption that $S \neq \emptyset$). Thus $S = \emptyset$, as required.

1.44 Note: It follows, from the above theorem, that in order to prove that $F(n)$ is true for all $n \geq m$, we can do the following:

1. Prove that $F(m)$ is true (this is called proving the **base case**).
2. Let $n > m$ and suppose that $F(n-1)$ is true (this is called the **induction hypothesis**).
3. Prove that $F(n)$ is true.

1.45 Theorem: *(Strong Induction Principle) Let $m\in\mathbb{Z}$. Let $F(n)$ be a statement about n. Suppose that for all $n \in \mathbb{Z}$ with $n \geq m$, if $F(k)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$ then $F(n)$ is true. Then $F(n)$ is true for all $n \in \mathbb{Z}$ 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 $n \in \mathbb{Z}$ 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 $k \in \mathbb{Z}$ with $m \leq k \leq n$. By the Discreteness Property of $\mathbb{Z}$, it follows that $F(k)$ is true for all $k \in \mathbb{Z}$ 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 $n \in \mathbb{Z}$ with $n \geq m$. Let $n \in \mathbb{Z}$ with $n \geq m$. Since $G(n)$ is true, we know that $F(k)$ is true for all $k \in \mathbb{Z}$ 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 $n \in \mathbb{Z}$ with $n \geq m$.

1.46 Note: In order to prove that $F(n)$ is true for all $n \geq m$, we can do the following:

1. Let $n \geq m$ and suppose that $F(k)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$.
2. Prove that $F(n)$ is true.

Although strong induction, used as above, does not require the proof that $F(m)$ is true (the base case), there are situations in which one ore more base cases must be verified to make this method of proof valid. For example, if a sequence $(x_n)_{n\geq 1}$ is defined by specifying the values of x_1 and x_2 and by giving a recursion formula for x_n in terms of x_{n-1} and x_{n-2} for all $n \geq 3$, then in order to prove that x_n satisfies the closed-form formula $x_n = f(n)$ for all $n \geq 1$ it suffices to prove that $x_1 = f(1)$ and $x_2 = f(2)$ (two base cases) and to prove that for all $n \geq 3$, if $x_{n-1} = f(n-1)$ and $x_{n-2} = f(x_{n-2})$ then $x_n = f(n)$.

1.47 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 $a_n = \frac{1}{5}\big(3^n - (-2)^n\big)$ for all $n \geq 0$.

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

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

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

1.48 Note: Suppose that we choose k of n objects, When the objects are chosen with replacement (so that repetition is allowed) and the order of the chosen objects matters (so the chosen objects form an ordered k-tuple), the number of ways to choose k of n objects is equal to n^k (since we have n choices for each of the k objects). For example, the number of ways to roll 3 six-sided dice is equal to $6^3 = 216$.

When the objects are chosen without replacement (so that the k chosen objects are distinct) and the order matters, the number of ways to choose k of n objects is equal to $n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$ (since we have n choices for the first object and $n-1$ choices for the second object and so on). In particular, the number of ways to arrange n objects in order (to form an ordered n-tuple) is equal to $n!$.

When the objects are chosen without replacement and the order does not matter (so the chosen objects form a k-element set), the number of ways to choose k of n objects is equal to $\frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$ (since each k-element set can be ordered in $k!$ ways to form $k!$ ordered k-tuples, and there are $\frac{n!}{(n-k)!}$ such ordered k-tuples). For example, the number of 4-element subsets of the set $\{1,2,3,4,5,6,7\}$ is equal to $\frac{7!}{4!3!} = \frac{7\cdot 6\cdot 5\cdot 4}{4\cdot 3\cdot 2\cdot 1} = 7\cdot 5 = 35$.

1.49 Definition: For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$, we define the **binomial coefficient** $\binom{n}{k}$, read as "n choose k", by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

1.50 Theorem: *(Pascal's Triangle) For $k, n \in \mathbb{N}$ with $0 \leq k \leq n$ we have*

$$\binom{n}{0} = \binom{n}{n} = 1\,,\ \binom{n}{k} = \binom{n}{n-k} \text{ and } \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Proof: The formulas $\binom{n}{0} = \binom{n}{n} = 1$ and $\binom{n}{k} = \binom{n}{n-k}$ are immediate from the definition of $\binom{n}{k}$ (since $0! = 1$) and we have

$$\begin{aligned} \binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{(k+1)n!}{(k+1)!(n-k)!} + \frac{(n-k)n!}{(k+1)!(n-k)!} \\ &= \frac{(k+1+n-k)n!}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} = \binom{n+1}{k+1}. \end{aligned}$$

1.51 Exercise: Make a table displaying the values $\binom{n}{k}$ for $0 \leq k \leq n \leq 10$. The table forms a triangle of positive integers in which each entry is obtained by adding two of the entries above.

1.52 Notation: Let R be a ring and let $a \in R$. For $k \in \mathbb{Z}^+$ we write $ka = a + a + \cdots + a$ with k terms in the sum, and we write $(-k)a = k(-a)$, and we write $a^k = a \cdot a \cdot \ldots \cdot a$ with k terms in the product. For $0 \in \mathbb{Z}$ we write $0a = 0$ and $a^0 = 1$. When $a \in R$ is a unit, for $k \in \mathbb{Z}^+$ we write $a^{-k} = (a^{-1})^k$.

1.53 Exercise: Let R be a ring and let $a, b \in R$. Show that for all $k, l \in \mathbb{Z}$ we have $(-k)a = -(ka)$, $(k+l)a = ka + la$ and $(ka)(lb) = (kl)(ab)$. Show that for all $k, l \in \mathbb{Z}^+$ we have $a^{k+l} = a^k a^l$. Show that if $ab = ba$ then for all $k, l \in \mathbb{Z}^+$ we have $(ab)^k = a^k b^k$. Show that if a is a unit, then for all $k, l \in \mathbb{Z}$ we have $a^{-k} = (a^k)^{-1}$ and $a^{k+l} = a^k a^l$.

1.54 Theorem: *(Binomial Theorem) Let R be a ring, let $a, b \in R$ with $ab = ba$, and let $n \in \mathbb{N}$. Then*

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a\, b^{n-1} + \binom{n}{n} b^n.\end{aligned}$$

Proof: We shall prove, by induction, that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ for all $n \geq 0$.

When $n = 0$ we have $\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{0}{0} a^0 b^0 = 1 = (a+b)^0 = (a+b)^n$.

When $n = 1$ we have $\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1 = (a+b)^n$.

Let $n \geq 1$ and suppose, inductively that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$. Then

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= (a+b)\Big(\binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a\, b^{n-1} + \binom{n}{n} b^n \Big) \\ &= \binom{n}{0} a^{n+1} + \binom{n}{1} a^n b + \binom{n}{2} a^{n-1} b^2 + \cdots + \binom{n}{n-1} a^2\, b^{n-1} + \binom{n}{n} a\, b^n \\ &\qquad + \binom{n}{0} a^n b + \binom{n}{1} a^{n-1} b^2 + \cdots + \binom{n}{n-2} a^2 b^{n-1} + \binom{n}{n-1} a\, b^n + \binom{n}{n} b^{n+1} \\ &= a^{n+1} + \Big(\binom{n}{0} + \binom{n}{1}\Big) a^n b + \Big(\binom{n}{1} + \binom{n}{2}\Big) a^{n-1} b + \cdots \\ &\qquad + \Big(\binom{n}{n-2} + \binom{n}{n-1}\Big) a^2 b^{n-1} + \Big(\binom{n}{n-1} + \binom{n}{n}\Big) a\, b^n + b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} + \binom{n+1}{1} a^n b + \binom{n+1}{2} a^{n-1} b^2 + \cdots + \binom{n+1}{n-1} a^2\, b^n + \binom{n+1}{n+1} a\, b^n \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k+1} a^{n+1-k} b^k\end{aligned}$$

as required, since $\binom{n}{0} = 1 = \binom{n+1}{0}$ and $\binom{n}{n} = 1 = \binom{n+1}{n+1}$ and $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ for all k with $0 \leq k \leq n$. By induction, we have $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ for all $n \geq 0$.

Finally note that, by interchanging a and b, we also have $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Cardinality

I may include some notes on cardinality later. For now, refer to Chapter 9 in Appendix 2, if you are interested.