Chapter 3. Rings, Fields, and Orders

3.1 Remark: In this chapter (and the next) we shall gather together and list all of the basic algebraic properties which hold in $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ which are needed in mathematical proofs. In addition to the sets $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$, there are many other algebraic systems (involving sets of mathematical objects along with operations, such as addition and multiplication, which act on these objects) which are studied and used in mathematics. For example, we can add and multiply two functions together, or we can add and multiply two matrices together. Some of the algebraic properties which hold in $\mathbf{Z}$ or in $\mathbf{R}$ also hold in some of these other algebraic systems. Rings and fields, as defined below, are algebraic systems with operations which satisfy some familiar algebraic properties.

3.2 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 $ab = 1$.

3.3 Theorem: $\mathbf{Z}$ *is a commutative ring and* $\mathbf{Q}$ *and* $\mathbf{R}$ *are fields with* $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$.

Proof: We accept this axiomatically, without proof.

3.4 Exercise: Show that the set $\mathbf{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbf{Z}\right\}$ is a commutative ring and that the set $\mathbf{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbf{Q}\right\}$ is a field.

3.5 Example: Let n be a positive integer. There is a ring, denoted by $\mathbf{Z}_n$, which is called the ring of **integers modulo** n. Later, we shall define $\mathbf{Z}_n$ precisely but, for now, we provide an informal description. We let $\mathbf{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and, for $a, b \in \mathbf{Z}_n$, we define the sum $a + b \in \mathbf{Z}_n$ to be the remainder when the integer $a + b \in \mathbf{Z}$ is divided by n, and we define the product $ab \in \mathbf{Z}_n$ to be the remainder when the integer ab is divided by n. For example, in $\mathbf{Z}_6$ addition and multiplication are given by the following tables.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

3.6 Example: There is a field, denoted by $\mathbf{C}$, which is called the **field of complex numbers**. Later we shall study the field $\mathbf{C}$ in more detail but, for now, we provide a brief introduction. We define $\mathbf{C} = \mathbf{R}^2 = \big\{(x,y)\big| x \in \mathbf{R}, y \in \mathbf{R}\big\}$. In $\mathbf{C}$, we write $0 = (0,0)$, $1 = (1,0)$ and $i = (0,1)$ and for $x, y \in \mathbf{R}$ we write $x = (x,0)$, $iy = (0,y)$ and $x+iy = (x,y)$. For $a, b, c, d \in \mathbf{R}$ we define

$$\begin{aligned}(a+ib) + (c+id) &= (a+c) + i(b+d),\\ (a+ib)\cdot(c+id) &= (ac-bd) + i(ad+bc).\end{aligned}$$

Note that in $\mathbf{C}$ we have $i^2 = -1$ and for $0 \le a \in \mathbf{R}$ we have $\left(i\sqrt{a}\right)^2 = -a$.

3.7 Exercise: Show that the set $\mathbf{Z}[i] = \big\{a+ib\big|a,b \in \mathbf{Z}\big\}$ is a commutative ring and that the set $\mathbf{Q}(i) = \big\{a+ib\big|a,b \in \mathbf{Q}\big\}$ is a field.

3.8 Example: For sets R and S, we write R^S for the set of all functions $f : S \to R$. When R is a ring, the set R^S is a ring with addition and multiplication defined, for $x \in S$, by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. The zero and identity elements are the constant function 0 (given by $0(x) = 0$ for all $x \in S$) and the constant function 1 (given by $1(x) = 1$ for all $x \in S$.

3.9 Example: When R is a set and $n \in \mathbf{Z}^+ = \{1, 2, 3, \cdots\}$, we define $R^n = R^{\{1,2,\cdots,n\}}$, which is the set of all functions $a : \{1, 2, \cdots, n\} \to R$. An element of R^n is called an **n-tuple** with entries in R. We write $a = (a_1, a_2, \cdots, a_n)$ to indicate that a is the n-tuple $a : \{1, 2, \cdots, n\} \to R$ given by $a(k) = a_k \in R$ for each index $k \in \{1, 2, \cdots, n\}$. The elements $a_k \in R$ are called the **entries** of the n-tuple a. We have

$$R^n = \big\{(a_1, a_2, \cdots, a_n)\big|\text{ each } a_k \in R\big\}.$$

When R is a ring, R^n is a ring with addition and multiplication given by $(a+b)_k = a_k + b_k$ and $(ab)_k = a_k b_k$ and with 0 and 1 given by $0 = (0, 0, \cdots, 0)$ and $1 = (1, 1, \cdots, 1)$.

For a set R, we let $R^\infty = R^{\{1,2,3,\cdots\}}$, which is the set of all functions $a : \mathbf{Z}^+ \to R$. An element of R^∞ is called a **sequence** with entries in R. We write $a = (a_k)_{k\ge1} = (a_1, a_2, a_3, \cdots)$ to indicate that a is the sequence given by $a(k) = a_k$ for all $k \in \mathbf{Z}^+$. The elements $a_k \in R$ are called the **entries** of the sequence a. Thus we have

$$R^\infty = \big\{(a_1, a_2, a_3, \cdots)\big|\text{ each } a_k \in R\big\}.$$

When R is a ring, R^∞ is a ring with addition and multiplication given by $(a+b)_k = a_k + b_k$ and $(ab)_k = a_k b_k$ and with 0 and 1 given by $0 = (0, 0, 0, \cdots)$ and $1 = (1, 1, 1, \cdots)$.

More generally, given a set R, a **sequence** with entries in R is a function of the form $a : \{m, m+1, m+2, \cdots\} \to R$ for some $m \in \mathbf{Z}$, and we write $a = (a_n)_{n\ge m}$ to indicate that a is the sequence with $a(k) = a_k$ for all $k \ge m$.

3.10 Remark: In foundational mathematics, as outlined briefly in Appendix 1, the sets $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are constructed using the ZFC axioms. In this procedure, the natural numbers are defined to be the sets $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$ and in general, $n = \{0, 1, 2, \cdots, n-1\}$. In foundational mathematics, the sets R^n and R^∞ are usually defined (slightly differently than we defined them above) by $R^n = R^{\{0,1,\cdots,n-1\}}$ and $R^\infty = R^{\mathbf{N}} = R^{\{0,1,2,\cdots\}}$.

3.11 Example: Let R be a ring. A **formal power series** in the variable x with coefficients in R is an expression of the form

$$f = f(x) = \sum_{k\geq 0} c_k x^k = \sum_{k=0}^{\infty} c_k x^k = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots$$

with each $c_k \in R$ The elements $c_k \in R$ are called the **coefficients** of f. The set of all formal power series in x with coefficients in R is denoted by $R[[x]]$. The set $R[[x]]$ is a ring with addition and multiplication defined as follows: for $f(x) = \sum_{k\geq 0} a_k x^k$ and $g(x) = \sum_{k\geq 0} b_k x^k$, we define $(f+g)(x) = \sum_{k\geq 0} (a_k + b_k)x^k$ and $(fg)(x) = \sum_{n\geq 0} c_n x^n$, where $c_n = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + \cdots a_n b_0$. A **polynomial** in the variable x with coefficients in R is a formal power series with only finitely many nonzero coefficients, that is a power series of the form

$$f = f(x) = \sum_{k\geq 0} c_k x^k = \sum_{k=0}^{n} c_k x^k = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

for some $n \in \mathbf{N}$, where each $c_k \in R$ and $c_k = 0$ for all $k > n$. In this case, if $c_n \neq 0$ then we say that n is the **degree** of the polynomial f and we write $\deg(f) = n$. The set of all polynomials in x with coefficients in R is denoted by $R[x]$, and it is a ring using the same operations used in $R[[x]]$.

3.12 Remark: In foundational mathematics, the above definition would not be considered to be rigorous, because all mathematical objects must be defined to be sets (which can be constructed using the ZFC axioms). The above definition states that a formal power series is an "expression " of a certain form, but it does not define what such an expression actually is, as a set. To be rigorous, the power series which we denoted by $f(x) = \sum_{k=1}^{\infty} c_k x^k$ would be defined to be *equal* to the function $c \in R^{\mathbf{N}}$ which is given by $c(k) = c_k$. Using this definition, the variable symbol x is irrelevant and we have $R[[x]] = R[[y]]$. Also note that, using this definition, the sets $R[[x]]$ and $R^{\mathbf{N}}$ are *equal*, but the multiplication operation used in $R[[x]]$ is not equal to the multiplication operation used in $\mathbf{R}^{\mathbf{N}}$.

3.13 Example: Let R be a ring and let $m, n \in \mathbf{Z}^+$. An $m \times n$ **matrix** with entries in R is an expression of the form

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

with each $a_{k,l} \in R$. The element $a_{k,l}$ is called the (k,l) entry of A, and we write $A_{k,l} = a_{k,l}$. The set of all $m \times n$ matrices with entries in R is denoted by $M_{m\times n}(R)$. We define the sum and product of two matrices as follows. For $A, B \in M_{m\times n}(R)$, we define $A+B \in M_{m\times n}(R)$ to be the matrix with entries $(A+B)_{k,l} = A_{k,l} + B_{k,l}$. For $A \in M_{m\times p}(R)$ and $B \in M_{p\times n}(R)$ we define $AB \in M_{m\times n}(R)$ to be the matrix with entries $(AB)_{k,l} = \sum_{j=1}^{p} A_{k,j} B_{j,l}$. When R is a ring and $n \in \mathbf{Z}^+$, the set of square matrices $M_n(R) = M_{n\times n}(R)$ is a non-commutative ring using these operations. The zero element is the **zero matrix** O with entries $O_{k,l} = 0$ for all k, l, and the identity element is the **identity matrix** I with entries $I_{k,k} = 1$ and $I_{k,l} = 0$ when $k \neq l$. The ring $M_n(R)$ plays an important role in linear algebra.

3.14 Definition: Let R be a ring. For $a, b \in R$, if $ab = ba = 1$ 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**.

3.15 Example: In $\mathbf{Z}$, the numbers 1 and -1 are invertible, and each is equal to its own inverse. In a field, every nonzero element is invertible (by R9). In $\mathbf{Z}[\sqrt{2}]$, the elements $a = 3 + 2\sqrt{2}$ and $b = 3 - 2\sqrt{2}$ are inverses of each other. The multiplication table in Example 3.5 shows that the only invertible elements in $\mathbf{Z}_6$ are 1 and 5, and each is equal to its own inverse. In $\mathbf{Z}_7$, every nonzero element is invertible, indeed we have $1 \cdot 1 = 1$, $2 \cdot 4 = 4 \cdot 2 = 1$, $3 \cdot 5 = 5 \cdot 3 = 1$ and $6 \cdot 6 = 1$. Verify that in $\mathbf{Z}[[x]]$, the power series $f(x) = 1 - x$ and $g(x) = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + x^3 + \cdots$ are inverses. Verify that in $M_2(\mathbf{Z})$, the matrices $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$ and $B = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}$ are inverses.

3.16 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

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

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.

3.17 Exercise: Convert the proof of Part (1) of the above theorem into a derivation of valid arguments to show that

$$\big\{\forall x\, \forall y\ x+y = y+x\,,\ \forall x\ x+0 = x\big\} \models \forall u\big(\forall x\ x+u = x \rightarrow u = 0\big).$$

3.18 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 $b \div a = b/a = \frac{b}{a} = b\,a^{-1}$.

3.19 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**.

3.20 Theorem: *(Properties of Rings) Let R be a ring. Then for all $a, b, c \in R$,*

(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) $a \cdot 0 = 0 = 0 \cdot a$ for all $a \in R$,
(5) $-(-a) = a$ for all $a \in R$,
(6) $(-a)b = -(ab) = a(-b)$ for all $a, b \in R$,
(7) $(-a)(-b) = ab$ for all $a, b \in R$,
(8) $(-1)a = -a$ for all $a \in R$,
(9) $a(b - c) = ab - ac$ and $(a - b)c = ac - bc$ for all $a, b, c \in R$,
(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 a is a zero divisor, or $b = c$,
(13) if a is a unit then a is not a zero divisor, and
(14) if R is contained in a field (and uses the same operations) then R has no zero divisors.

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).

3.21 Example: In $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ there are no zero divisors. In $\mathbf{Z}_6$ we have $2 \cdot 3 = 0$ so 2 and 3 are zero divisors. In $\mathbf{Z}^2$, given $0 \neq a, b \in \mathbf{Z}$ we have $(a, 0) \cdot (0, b) = (0, 0)$ and so $(a, 0)$ and $(0, b)$ are zero divisors. In $M_2(\mathbf{Z})$, for $A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix}$ we have $AB = O$ and so A and B are zero divisors.

3.22 Definition: A commutative ring with no zero divisors is called an **integral domain**.

3.23 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 $\leq$.

3.24 Theorem: *Each of* $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ *and* $\mathbf{R}$ *is an ordered set using its standard order* $\leq$ *with* $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$ *(and 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 accept the truth of this theorem axiomatically, without proof.

3.25 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 $y < x$.

3.26 Theorem: *Let* $\leq$ *be an order on a set* X*. Then*

(1) for all $x, y \in X$*, we have* $x \leq y \iff \big(x < y \text{ or } x = y\big)$,
(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.

3.27 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 $x \geq 0$.

3.28 Theorem: R *is an ordered field.*

Proof: We accept this axiomatically, without proof.

3.29 Corollary: *Any field F, which is a subset of* **R** *and uses the same operations and the same order, is an ordered field.*

3.30 Example: Q and $\mathbf{Q}[\sqrt{2}]$ are ordered fields.

3.31 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 3.2 and Theorem 3.20 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 $0 \leq x$ then by O4 we have $0 + (-x) \leq x + (-x)$ hence $-x \leq 0$.

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 from 3.18). First suppose that $x \geq 0$, which means that $0 \leq x$ by Notation 3.27. 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

$$\begin{aligned} x + u &\leq 0 + u \text{ , by O4,} \\ 0 &\leq 0 + u \text{ , since } x + u = 0, \\ 0 &\leq u + 0 \text{ , since } 0 + u = u + 0 \text{ by R2,} \\ 0 &\leq u \text{ , since } u + 0 = u \text{ by R3.} \\ u &\geq 0 \text{ , by Notation 3.27,} \\ -x &\geq 0 \text{ , since } u = -x. \end{aligned}$$

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 3.20 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 3.20, 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 3.18). Then

$$\begin{aligned}
y + u &\leq z + u \text{ , since } y \leq z, \text{ by O4,} \\
0 &\leq z + u \text{ , since } y + u = 0, \\
0 &\leq x(z + u) \text{ , since } 0 \leq x \text{ and } 0 \leq z + u, \text{ by O5,} \\
0 &\leq xz + xu \text{ , by R7,} \\
0 + xy &\leq (xz + xu) + xy \text{ , by O4,} \\
0 + xy &\leq xz + (xu + xy) \text{ , by R1,} \\
0 + xy &\leq xz + x(u + y) \text{ , by R7,} \\
0 + xy &\leq xz + x(y + u) \text{ , by R2,} \\
0 + xy &\leq xz + x \cdot 0 \text{ , since } y + u = 0, \\
0 + xy &\leq xz + 0 \text{ , by Theorem 3.20 Part (4),} \\
0 + xy &\leq xz \text{ , by R3,} \\
xy + 0 &\leq xz \text{ , by R2,} \\
xy &\leq xz \text{ , by R3.}
\end{aligned}$$

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 3.20, 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 $\frac{1}{y} < \frac{1}{x}$.

3.32 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 $\frac{1}{y} < \frac{1}{x} < 0$.

3.33 Note: Note that it is not possible to define an order $\leq$ on $\mathbf{C}$ which makes $\mathbf{C}$ into an ordered field because if $\mathbf{C}$ 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).

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

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

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

(1) (Positive Definiteness) $|x| \geq 0$ with $|x| = 0 \Longleftrightarrow x = 0$,
(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 $|x - a| \leq b \Longleftrightarrow a - b \leq x \leq a + b$.

Proof: The proof is left as an exercise.

3.36 Theorem: *(Basic Order Properties of $\mathbf{Z}$)*

(1) For all $n \in \mathbf{Z}$ 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 $k < n + 1$. Equivalently, for all $n \in \mathbf{Z}$ there does not exist $k \in \mathbf{Z}$ with $n < k < n + 1$.

Proof: This theorem is accepted as true axiomatically, without proof.

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

Solution: Let $k, l \in \mathbf{Z}$ and suppose that $kl = 1$. By Theorem 3.26 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 hove $1 = kl = 0 \cdot l = 0$. Also, we cannot have $-1 < k < 0$ or $0 < k < 1$ by Theorem 3.36 Part (2), 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 3.31 Part (5) we have $0 < 1 < k$, so by Note 3.32 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 Theorem 3.36 Part (2). 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 Theorem 3.36 Part (2). 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 $1 = kl = (-1)l = -l$.

3.38 Remark: At this stage we have have either proven, or accepted axiomatically, all of the algebraic properties of $\mathbf{Z}$ which were used in our proof in Example 2.31 at the end of the previous chapter.

3.39 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.

3.40 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 $a = \min A$.

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

3.42 Theorem: *(Least Upper Bound and Greatest Lower Bound 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 accept this axiomatically, without proof.

3.43 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: We prove Part (1). 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.

3.44 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 Theorem 3.39, 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 $\mathbf{Z}$. Thus $n \in A$ so A has a maximum element.

3.45 Theorem: *(Floor and Ceiling Properties of* $\mathbf{Z}$ *in* 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 $A = \{k \in \mathbf{Z} \,|\, k \leq x\}$. 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 $x - 1 \geq n \Longrightarrow x \geq n + 1 \Longrightarrow n + 1 \in A \Longrightarrow n \neq \max A$. 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).

3.46 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 $f : \mathbf{R} \to \mathbf{Z}$ given by $f(x) = \lfloor x \rfloor$ is called the **floor function**.

3.47 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 $m = \lfloor x \rfloor - 1 \leq x - 1 < x$.

3.48 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 $a < q < b$.