Bloch's The Real Numbers and Real Analysis: Answer Book

Konstantin Lepa

Construction of the Real Numbers

1. Introduction

Definition 1.1.1. *Let S be a set. A* ***binary operation*** *on S is a function $S \times S \to S$. A* ***unary operation*** *on S is a function $S \to S$.*

2. Entry 1: Axioms for the Natural Numbers

Axiom 1.2.1 (Peano Postulates). *There exists a set $\mathbb{N}$ with an element $1 \in \mathbb{N}$ and a function $s : \mathbb{N} \to \mathbb{N}$ that satisfy the following three properties.*

(a) *There is no $n \in \mathbb{N}$ such that $s(n) = 1$.*
(b) *The function s is injective.*
(c) *Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.*

Definition 1.2.2. *The set of **natural numbers**, denoted $\mathbb{N}$, is the set the existence of which is given in the Peano Postulates.*

Lemma 1.2.3. *Let $a \in \mathbb{N}$. Suppose that $a \neq 1$. Then there is a unique $b \in \mathbb{N}$ such that $a = s(b)$.*

Theorem 1.2.4 (Definition by Recursion). *Let H be a set, let $e \in H$ and let $k : H \to H$ be a function. Then there is a unique function $f : \mathbb{N} \to H$ such that $f(1) = e$, and that $f \circ s = k \circ f$.*

Theorem 1.2.5. *There is a unique binary operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

(a) $n + 1 = s(n)$.
(b) $n + s(m) = s(n + m)$.

Theorem 1.2.6. *There is a unique binary operation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

(a) $n \cdot 1 = n$.
(b) $n \cdot s(m) = (n \cdot m) + n$.

Theorem 1.2.7. *Let $a, b, c \in \mathbb{N}$.*

(1) *If $a + c = b + c$, then $a = b$* *(Cancellation Law for Addition).*
(2) $(a + b) + c = a + (b + c)$ *(Associative Law for Addition).*
(3) $1 + a = s(a) = a + 1$.
(4) $a + b = b + a$ *(Commutative Law for Addition).*
(5) $a + b \neq 1$.
(6) $a + b \neq a$.
(7) $a \cdot 1 = a = 1 \cdot a$ *(Identity Law for Multiplication).*
(8) $(a + b)c = ac + bc$ *(Distributive Law).*
(9) $ab = ba$ *(Commutative Law for Multiplication).*
(10) $c(a + b) = ca + cb$ *(Distributive Law).*
(11) $(ab)c = a(bc)$ *(Associative Law for Multiplication).*
(12) *If $ac = bc$ then $a = b$* *(Cancellation Law for Multiplication).*
(13) *$ab = 1$ if and only if $a = 1 = b$.*

Definition 1.2.8. *The relation $<$ on $\mathbb{N}$ is defined by $a < b$ if and only if there is some $p \in \mathbb{N}$ such that $a + p = b$, for all $a, b \in \mathbb{N}$. The relation $\leq$ on $\mathbb{N}$ is defined by $a \leq b$ if and only if $a < b$ or $a = b$, for all $a, b \in \mathbb{N}$.*

Theorem 1.2.9. *Let $a, b, c, d \in \mathbb{N}$.*

(1) *$a \leq a$ and $a \nless a$ and $a < a + 1$.*
(2) $1 \leq a$.
(3) *If $a < b$ and $b < c$, then $a < c$; if $a \leq b$ and $b < c$, then $a < c$; if $a < b$ and $b \leq c$, then $a < c$; if $a \leq b$ and $b \leq c$, then $a \leq c$.*
(4) *$a < b$ if and only if $a + c < b + c$.*
(5) *$a < b$ if and only if $ac < bc$.*
(6) *Precisely one of $a < b$ or $a = b$ or $a > b$ holds* *(Trichotomy Law).*
(7) *$a \leq b$ or $b \leq a$.*
(8) *If $a \leq b$ and $b \leq a$, then $a = b$.*
(9) *It cannot be that $b < a < b + 1$.*
(10) *$a \leq b$ if and only if $a < b + 1$.*
(11) *$a < b$ if and only if $a + 1 \leq b$.*

Theorem 1.2.10 (Well-Ordering Principle). *Let $G \subseteq \mathbb{N}$ be a non-empty set. Then there is some $m \in G$ such that $m \leq g$ for all $g \in G$.*

Exercise 1.2.1 (Used in Theorem 1.2.6). Fill in the missing details in the proof of Theorem 1.2.6.

Proof. To prove uniqueness, suppose that there are two binary operations $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and $\odot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfy the two properties of the theorem. Let

$$G = \{x \in \mathbb{N} \mid n \cdot x = n \odot x \text{ for all } n \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will imply that $\cdot$ and $\odot$ are the same operation. Clearly, $G \subseteq \mathbb{N}$. Also, $1 \in G$ because $n \cdot 1 = n = n \odot 1$ for all $n \in \mathbb{N}$. Now let $g \in G$, and let $n \in \mathbb{N}$. By hypothesis on g, we have $n \cdot g = n \odot g$. Then,

$$n \cdot s(g) = (n \cdot g) + n = (n \odot g) + n = n \odot s(g).$$

Therefore $s(g) \in G$, and hence by Part (c) of the Peano Postulates it follows that $G = \mathbb{N}$.

Let $q \in \mathbb{N}$. Let $h_q : \mathbb{N} \to \mathbb{N}$ be defined by $h_q(m) = m+q$ for all $m \in \mathbb{N}$. Applying Theorem 1.2.4 to the set $\mathbb{N}$, the element $q \in \mathbb{N}$ and the function $h_q : \mathbb{N} \to \mathbb{N}$, implies that there is a unique function $g_q : \mathbb{N} \to \mathbb{N}$ such that $g_q(1) = q$ and $g_q \circ s = h_q \circ g_q$. Let $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $c \cdot d = g_c(d)$ for all $(c, d) \in \mathbb{N} \times \mathbb{N}$. Then $n \cdot 1 = g_n(1) = n$, which is Part (a), and

$$\begin{aligned} n \cdot s(m) &= g_n(s(m)) = (g_n \circ s)(m) = (h_n \circ g_n)(m) \\ &= h_n(g_n(m)) = h_n(n \cdot m) = (n \cdot m) + n, \end{aligned}$$

which is Part (b). □

Exercise 1.2.2 (Used in Theorem 1.2.7). Prove Theorem 1.2.7 (2) (3) (4) (7) (8) (9) (10) (11) (13).

Proof.

(2) Let

$$G = \{z \in \mathbb{N} \mid (x+y)+z = x+(y+z) \text{ for all } x, y \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Associative Law for Addition. Clearly $G \subseteq \mathbb{N}$. Using both parts of Theorem 1.2.5 we have

$$(a+b)+1 = s(a+b) = a+s(b) = a+(b+1).$$

Hence, $1 \in G$. Now let $c \in G$. By hypothesis on c, we know that $(a+b)+c = a+(b+c)$, so by Part (b) of Theorem 1.2.5 it follows that

$$\begin{aligned}(a+b)+s(c) &= s((a+b)+c) = s(a+(b+c))\\ &= a+s(b+c) = a+(b+s(c)).\end{aligned}$$

Therefore $s(c) \in G$, and hence $G = \mathbb{N}$ by Part (c) of the Peano Postulates.

(3) Let

$$G = \{1+n = s(n) \text{ for all } n \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply Part (3). Clearly $G \subseteq \mathbb{N}$, and $1 \in G$ because by Part (a) of Theorem 1.2.5 we have $1+1 = s(1)$. Now let $a \in G$. Using the Associative Law for Addition and Theorem 1.2.5, it then follows that

$$\begin{aligned}1+s(a) &= s(1+a) = s(a+1) = a+s(1)\\ &= a+(1+1) = (a+1)+1 = s(a)+1\\ &= s(s(a)).\end{aligned}$$

Therefore $s(a) \in G$, and hence $G = \mathbb{N}$ by Part (c) of the Peano Postulates.

(4) Let

$$G = \{x \in \mathbb{N} \mid x+y = y+x \text{ for all } y \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Commutative Law for Addition. Clearly $G \subseteq \mathbb{N}$. By Part (3) we also have $1+y = y+1$ for all $y \in \mathbb{N}$, so $1 \in G$. Now let $a \in G$. Then,

$$\begin{aligned}s(a)+b &= (a+1)+b && \text{(Part (a) of Theorem 1.2.5)}\\ &= a+(1+b) && \text{(Associative Law for Addition)}\\ &= (1+b)+a && \text{(Hypothesis on } a\text{)}\\ &= (b+1)+a && \text{(Part (3) of the theorem)}\\ &= b+(1+a) = b+(a+1) = b+s(a).\end{aligned}$$

Hence, $s(a) \in G$. We deduce that $G = \mathbb{N}$ by Part (c) of the Peano Postulates.

(7) Let

$$G = \{1 \cdot x = x \text{ for all x } \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Identity Law for Multiplication. Clearly $G \subseteq \mathbb{N}$. By Theorem 1.2.6 (a), it follows that $1 \cdot 1 = 1$, so $1 \in G$. Now let $a \in G$. Using Theorem 1.2.6 (b), hypothesis on a, and Theorem a, it then follows that

$$1 \cdot s(a) = 1 \cdot a + 1 = a + 1 = s(a).$$

Hence $s(a) \in G$, and by Part (c) of the Peano Postulates, we deduce that $G = \mathbb{N}$.

(8) Let

$$G = \{z \in \mathbb{N} \mid (x+y)z = xz + yz \text{ for all } x, y \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Distributive Law. Clearly $G \subseteq \mathbb{N}$. Also, by Theorem 1.2.6 (b), it follows that $(a+b) \cdot 1 = a+b = a \cdot 1 + b \cdot 1$, and as a result $1 \in G$. Now let $c \in G$. Then,

$$\begin{aligned}(a+b)s(c) &= (a+b)c + (a+b) && \text{(Part (b) of Theorem 1.2.6)}\\ &= (ac+bc)+(a+b) && \text{(Hypothesis on } c\text{)}\\ &= ac+(bc+(a+b)) && \text{(Associative Law for Addition)}\\ &= ac+((a+b)+bc) && \text{(Commutative Law for Addition)}\\ &= (ac+(a+b))+bc\\ &= ((ac+a)+b)+bc\\ &= (ac+a)+(b+bc)\\ &= (ac+a)+(bc+b)\\ &= as(c)+bs(c)\end{aligned}$$

Hence, $s(c) \in G$, and by Part (c) of the Peano Postulates, we can conclude that $G \in \mathbb{N}$.

(9) Let

$$G = \{x \in \mathbb{N} \mid xy = yx \text{ for all } y \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Commutative Law for Multiplication. Clearly $G \subseteq \mathbb{N}$. By the Identity Law for Multiplication, $1 \in G$. Now let $a \in G$. Then,

$$\begin{aligned}s(a)b &= (a+1)b && \text{(Part (a) of Theorem 1.2.5)}\\ &= ab+b && \text{(Distributive Law)}\\ &= ba+b && \text{(Hypothesis on } a\text{)}\\ &= bs(a).\end{aligned}$$

Hence, $s(a) \in G$, and we deduce that $G = \mathbb{N}$ because of Part (c) of the Peano Postulates.

(10) Using Part (8) (Distributive Law) and Part (9) (Commutative Law for Multiplication), it follows that

$$c(a+b) = (a+b)c = ac+bc = ca+cb.$$

(11) Let

$$G = \{z \in \mathbb{N} \mid (xy)z = x(yz) \text{ for all } x, y \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply the Associative Law for Multiplication. By Theorem 1.2.6 (a), it follows that $(ab) \cdot 1 = ab = a(b \cdot 1)$, and therefore $1 \in G$. Now let $a \in G$. Then,

$$\begin{aligned}(ab)s(c) &= (ab)c + ab && \text{(Part (b) of Theorem 1.2.6)}\\ &= a(bc)+ab && \text{(Hypothesis on } c\text{)}\\ &= a(bc+b) && \text{(Distributive Law)}\\ &= a(bs(c)).\end{aligned}$$

Hence $s(c) \in G$. By Part (c) of the Peano Postulates, it then follows that $G = \mathbb{N}$.

(13) Let $ab = 1$. Suppose to the contrary that either $a \neq 1$ or $b \neq 1$. Suppose, without loss of generality, that $a \neq 1$. By Lemma 1.2.3, there is some $p \in \mathbb{N}$ such that $a = s(p)$, so $ab = s(p)b$. Because of the Commutative Law for Multiplication and Theorem 1.2.6 (b), $s(p)b = bs(p) = bp + b = 1$, which is a contradiction to Part (5) of this theorem. Hence, $a = 1 = b$.

Now let $a = 1 = b$. By Theorem 1.2.6 (a), it then follows that $ab = 1 \cdot 1 = 1$. □

Exercise 1.2.3 (Used in Section 1.2). Let $a, b \in \mathbb{N}$. Suppose that $a < b$. Prove that there is a unique $p \in \mathbb{N}$ such that $a + p = b$.

Proof. Since $a < b$, Definition 1.2.8 immediately implies the existence part. For uniqueness, suppose that there are $p_1, p_2 \in \mathbb{N}$ such that $a+p_1 = b$ and $a+p_2 = b$, so $a+p_1 = a+p_2$. By the Commutative Law for Addition, it follows that $p_1+a = p_2+a$, and by the Cancellation Law for Addition, it follows that $p_1 = p_2$. □

Exercise 1.2.4 (Used in Theorem 1.2.9). Prove Theorem 1.2.9 (1) (3) (4) (5) (11).

Proof.

(1) As $a = a$, we have either $a < a$ or $a = a$, so $a \leq a$. Next suppose to the contrary that $a < a$. We can find some $p \in \mathbb{N}$ such that $a + p = a$, which is a contradiction to Theorem 1.2.9 (6). Hence, $a \not< a$. Finally, let $p = 1$. Then $a + p = a + 1$, and by Definition 1.2.8 we deduce that $a < a + 1$.

(3) Suppose that $a < b$ and $b < c$. We can choose some $p, q \in \mathbb{N}$ such that $a + p = b$ and $b + q = c$. Then $(a + p) + q = c$, and by the Associative Law for Addition we get $a + (p + q) = c$, which implies that $a < c$. Now suppose that $a \leq b$ and $b < c$. Then either $a < b$ or $a = b$. If $a < b$, then we already know that $a < c$. If $a = b$, then clearly $b = a < c$. A similar argument shows that if $a < b$ and $b \leq c$, then $a < c$. Finally, suppose that $a \leq b$ and $b \leq c$. This means either $a < b$ or $a = b$ and either $b < c$ or $b = c$. We have shown all cases above except the trivial case when we have $a = b = c$. Hence, either $a < c$ or $a = c$, or in other words $a \leq c$.

(4) Suppose that $a < b$. We can find some $p \in \mathbb{N}$ such that $a + p = b$. Then $(a + p) + c = b + c$. Using Theorem 1.2.9 (2) (4), we have

$$(a + p) + c = a + (p + c) = a + (c + p) = (a + c) + p.$$

Hence, $(a + c) + p = b + c$, which implies that $a + c < b + c$. It is possible to reverse these implications and deduce the argument.

(5) Let

$$G = \{z \in \mathbb{N} \mid \text{ if } x < y \text{ then } xz < yz\}.$$

We will prove that $G = \mathbb{N}$, which will imply this part of the theorem. Clearly $G \subseteq \mathbb{N}$. By Theorem 1.2.6 (a), it follows that if $a < b$ then $a = a \cdot 1 < b \cdot 1 = b$, and therefore $1 \in G$. Now let $c \in G$. Suppose that $a < b$. By hypothesis on c, it then follows that $ac < bc$. Using the Distributive Law, Part (4), and the Commutative Law for Addition, we have

$$a(c + 1) = ac + a < bc + a = a + bc < b + bc = bc + b = b(c + 1).$$

Therefore $a(c + 1) < b(c + 1)$, and hence $c + 1 \in G$. By Part (c) of the Peano Postulates, it follows that $G = \mathbb{N}$, or in other words if $a < b$ then $ac < bc$.

Now we will show that if $ac < bc$ then $a < b$. Suppose that $ac < bc$, and suppose to the contrary that $a \geq b$, which means either $a > b$ or $a = b$.

Case 1. $a = b$. Then $ac = bc$, which is a contradiction to the fact that $ac < bc$ because of the Trichotomy Law. Hence $a < b$.

Case 2. $a > b$. This means that $b < a$, and it then follows that $bc < ac$, again a contradiction. Hence $a < b$.

(11) Suppose that $a < b$, and suppose to the contrary that $b < a + 1$. By Part (4) it then follows that $a + 1 < b + 1$, so $b < a + 1 < b + 1$, which is a contradiction to Part (9) of this theorem. Hence, $a + 1 \leq b$.

Now suppose that $a + 1 \leq b$, and suppose to the contrary that $b \leq a$. Then by Part (3) we deduce that $a + 1 \leq a$, which means either $a + 1 < a$ or $a + 1 = a$. If $a + 1 < a$ then there is a contradiction to Parts (1) and (6) of this theorem. If $a + 1 = a$ then there is a contradiction to Theorem 1.2.7 (6). Hence, $a < b$. □

Exercise 1.2.5 (Used in Exercise 1.3.3). Let $a, b \in \mathbb{N}$. Prove that if $a + a = b + b$, then $a = b$.

Proof. Suppose that $a + a = b + b$. Using the Distributive Law and Theorem 1.2.6 (b), we have

$$a(1+1) = a \cdot 1 + a \cdot 1 = a + a = b + b = b \cdot 1 + b \cdot 1 = b(1+1).$$

Thus, $a(1+1) = b(1+1)$. Then by the Cancellation Law for Multiplication we deduce that $a = b$. □

Exercise 1.2.6. Let $b \in \mathbb{N}$. Prove that

$$\{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cup \{n \in \mathbb{N} \mid b+1 \leq n\} = \mathbb{N}$$
$$\{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cap \{n \in \mathbb{N} \mid b+1 \leq n\} = \emptyset.$$

Proof. Let

$$G = \{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cup \{n \in \mathbb{N} \mid b+1 \leq n\}.$$

We will prove that $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. By Theorem 1.2.9 (1) (2) it follows that $1 \leq 1 \leq b$. Hence, $1 \in G$. Now let $a \in G$. We consider the following three cases:

Case 1. $a < b$. By Theorem 1.2.9 (4) it then follows that $a+1 < b+1$, and by Definition 1.2.8 it follows that $a+1 \leq b$. Hence $a+1 \in G$.

Case 2. $a = b$. Then $a+1 = b+1$, so $a+1 \leq b+1$, and hence $a+1 \in G$.

Case 3. $a > b$. By Theorem 1.2.9 (4) we get $b+1 \leq a+1$. Hence $a+1 \in G$.

Thus, $a+1 \in G$, and by Part (c) of the Peano Postulates we deduce that $G = \mathbb{N}$.

Now let

$$M = \{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cap \{n \in \mathbb{N} \mid b+1 \leq n\}.$$

Suppose to the contrary that $M \neq \emptyset$. We can choose some $a \in M$ such that $1 \leq a \leq b$ and $b+1 \leq a$. Using Theorem 1.2.9 (10), we have $a < b+1$ and $b+1 < a+1$, or in other words $a < b+1 < a+1$, which is a contradiction to Theorem 1.2.9 (9). Therefore $M = \emptyset$. □

Exercise 1.2.7. Let $A \subseteq \mathbb{N}$ be a set. The set A is **closed** if $a \in A$ implies $a + 1 \in A$. Suppose that A is closed.

(1) Prove that if $a \in A$ and $n \in \mathbb{N}$, then $a + n \in A$.
(2) Prove that if $a \in A$, then $\{x \in \mathbb{N} \mid x \geq a\} \subseteq A$.

Proof of (1). Let

$$G = \{n \in \mathbb{N} \mid \text{ if } a \in A \text{ then } a + n \in A\}.$$

We will prove that $G = \mathbb{N}$, which will imply the desired result. Clearly $G \subseteq \mathbb{N}$. Because A is closed, we deduce that $1 \in G$. Now let $a \in A$ and $n \in G$. Then $a + n \in A$, and since A is closed, it follows that $(a + n) + 1 \in A$. Using the Associative Law for Addition, we obtain $(a + n) + 1 = a + (n + 1)$, and hence $n + 1 \in G$. Thus, by Part (c) of the Peano Postulates, we can conclude that $G = \mathbb{N}$. □

Proof of (2). Let $a \in A$, and suppose that $n \in \{x \in \mathbb{N} \mid x \geq a\}$. Then $a \leq n$, which means either $a < n$ or $a = n$. If $a = n$ then clearly $n \in A$. Now suppose that $a \neq n$, so $a < n$. According to Definition 1.2.8 there is some $k \in \mathbb{N}$ such that $a + k = n$. By Part (1) of this exercise, it follows that $a + k \in A$, or in other words $n \in A$. Since n was arbitrary, we can conclude that $\{x \in \mathbb{N} \mid x \geq a\} \subseteq A$. □

Exercise 1.2.8 (Used in Section 1.2). Suppose that the set $\mathbb{N}$ together with the element $1 \in \mathbb{N}$ and the function $s : \mathbb{N} \to \mathbb{N}$, and that the set $\mathbb{N}'$ together with the element $1' \in \mathbb{N}'$ and the function $s' : \mathbb{N}' \to \mathbb{N}'$, both satisfy the Peano Postulates. Prove that there is a bijective function $f : \mathbb{N} \to \mathbb{N}'$ such that $f(1) = 1'$ and $f \circ s = s' \circ f$. The existence of such a bijective function proves that the natural numbers are essentially unique.

The existence of the function f follows immediately from the existence part of Theorem 1.2.4; the trickier aspect of this exercise is to prove that f is bijective. To do that, find an inverse for f by using the existence part of Theorem 1.2.4 again, and then prove that the function you found is an inverse of f by using the uniqueness part of Theorem 1.2.4.

Proof. We will prove that f is a bijective function. Because the set $\mathbb{N}'$ together with the element $1' \in \mathbb{N}'$ and the function $s' : \mathbb{N}' \to \mathbb{N}'$ satisfies the Peano Postulates, we can imply Theorem 1.2.4 to the set $\mathbb{N}$, the element $1 \in \mathbb{N}$ and the function $s : \mathbb{N} \to \mathbb{N}$, to deduce that there is a unique function $g : \mathbb{N} \to \mathbb{N}'$ such that $g(1') = 1$ and $g \circ s' = s \circ g$.

Let

$$G = \{n \in \mathbb{N} \mid g(f(n)) = n\}.$$

We will show that $G = \mathbb{N}$, which will imply that $g(f(n)) = n$ for all $n \in \mathbb{N}$. Since $g(f(1)) = g(1') = 1$, it follows that $1 \in G$. Now let $n \in G$, which means that $g(f(n)) = n$. Then,

$$\begin{aligned} g(f(s(n))) &= (g \circ f \circ s)(n) = (g \circ (f \circ s))(n) = (g \circ (s' \circ f))(n) \\ &= (g \circ s' \circ f)(n) = (s \circ g \circ f)(n) = s(g(f(n))) \\ &= s(n). \end{aligned}$$

Hence, $s(n) \in G$, and by Part (c) of the Peano Postulates, it follows that $G = \mathbb{N}$. A similar argument shows that $f(g(n')) = n'$ for all $n' \in \mathbb{N}'$.

Now let $n \in \mathbb{N}$ and $n' \in \mathbb{N}'$. If $n' = f(n)$ then $g(n') = g(f(n)) = n$. Also, if $n = g(n')$ then $f(n) = f(g(n')) = n'$. Because of uniqueness of g, it then follows that g is an inverse of f, and we can conclude that f is bijective. □

Exercise 1.2.9 (Not in the book). Given any two of the three axioms of the Peano Postulates, find a structure that satisfies those two axioms, but not the third. Feel free to assume $\mathbb{R}$, $\mathbb{Z}$, or anything else for this problem.

Example 1. Suppose that $n \in \mathbb{N}$. Let $A = \{x \in \mathbb{N} \mid x \leq n\}$, and let $s : A \to A$ be a function that is defined by

$$s(x) = \begin{cases} x+1, & x < n \\ 1, & \text{otherwise.} \end{cases}$$

Then they satisfy the following two properties.

(a) The function s is injective.

(b) Let $G \subseteq A$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = A$.

But then $s(n) = 1$.

Example 2. Suppose that $n \in \mathbb{N}$. Let $A = \{x \in \mathbb{N} \mid x \leq n\}$, and let $s : A \to A$ be a function that is defined by

$$s(x) = \begin{cases} x+1, & x < n \\ x, & \text{otherwise.} \end{cases}$$

Then they satisfy the following two properties.

(a) There is no $n \in A$ such that $s(n) = 1$.

(b) Let $G \subseteq A$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = A$.

We can find some $m \in A$ such that $m + 1 = n$. Then $s(m) = n = s(n)$ and $m \neq n$, and hence s is not injective.

Example 3. Let $A = \mathbb{N}$, and let $s : A \to A$ be a function that is defined by $s(x) = x + 2$. Then they satisfy the following two properties.

(a) There is no $n \in A$ such that $s(n) = 1$.

(b) The function s is injective.

Let $G = \{a \in A \mid a \text{ is even }\}$. Clearly $G \subseteq A$ and $1 \in G$. Also, if $g \in G$ then $s(g) \in G$. But it is obvious that $G \neq A$.

Exercise 1.2.10 (Not in the book). Construct the exponentiation n^m and prove its basic properties.

Theorem 1.2.11 (Exponentiation). *There is a unique binary operation $\boxdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

(a) $n \boxdot 1 = n$.
(b) $n \boxdot s(m) = (n \boxdot m) \cdot n$.

The number $n \boxdot m$ is also denoted n^m.

Proof. To prove uniqueness, suppose that there are two binary operations $\boxdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and $\boxtimes : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfy the two properties of this theorem. Let

$$G = \{g \in \mathbb{N} \mid n \boxdot g = n \boxtimes g \text{ for all } n \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will imply that $\boxdot$ and $\boxtimes$ are the same opertion. Clearly $G \subseteq \mathbb{N}$. Because $n \boxdot 1 = n = n \boxtimes 1$ it follows that $1 \in G$. Now let $n \in \mathbb{N}$ and $g \in G$. This means that $n \boxdot g = n \boxtimes g$. Then,

$$n \boxdot s(g) = (n \boxdot g) \cdot n = (n \boxtimes g) \cdot n = n \boxtimes s(g).$$

Hence $s(g) \in G$, and by Part (c) of the Peano Postulates we can conclude that $G = \mathbb{N}$.

For existence, let $p \in \mathbb{N}$, and let $k_p : \mathbb{N} \to \mathbb{N}$ be defined by $k_p(n) = p \cdot n$ for all $n \in \mathbb{N}$. We can apply Theorem 1.2.4 to the set $\mathbb{N}$, the element $p \in \mathbb{N}$ and the function $k_p : \mathbb{N} \to \mathbb{N}$, to deduce that there is a unique function $f_p : \mathbb{N} \to \mathbb{N}$ such that $f_p(1) = p$ and $f_p \circ s = k_p \circ f_p$. Let $\boxdot : \mathbb{N} \to \mathbb{N}$ be defined by $c \boxdot d = f_c(d)$ for all $(c, d) \in \mathbb{N}$. Let $n, m \in \mathbb{N}$. It then follows that $n \boxdot 1 = f_n(1) = n$, which is Part (a), and also we have

$$\begin{aligned} n \boxdot s(m) &= f_n(s(m)) = (f_n \circ s)(m) = (k_n \circ f_n)(m) \\ &= k_n(f_n(m)) = k_n(n \boxdot m) = (n \boxdot m) \cdot n, \end{aligned}$$

which is Part (b). □

Theorem 1.2.12. *Let $a, b, c \in \mathbb{N}$.*

(1) $a^{b+c} = a^b a^c$.
(2) $a^{bc} = (a^b)^c$.
(3) $b^a c^a = (bc)^a$.

Proof.

(1) Let

$$G = \{y \in \mathbb{N} \mid a^{x+y} = a^x a^y \text{ for all } x \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply that $a^{b+c} = a^b a^c$. Clearly $G \in \mathbb{N}$. By Theorem 1.2.11 it follows that

$$a^{b+1} = a^{s(b)} = a^b a = a^b a^1,$$

and hence $1 \in G$. Now let $c \in G$, or in other words $a^{b+c} = a^b a^c$. By repeated use of the Associative and Commutative Laws for Addition and Associative Law for Multiplication we obtain

$$\begin{aligned} a^{b+s(c)} &= a^{b+(c+1)} = a^{b+(1+c)} = a^{(b+1)+c} = a^{s(b+c)} \\ &= a^{b+c} a = (a^b a^c) a = a^b (a^c a) = a^b a^{s(c)}, \end{aligned}$$

and hence $s(c) \in G$. Thus, by Part (c) of the Peano Postulates we can conclude that $G = \mathbb{N}$.

(2) Let

$$G = \{y \in \mathbb{N} \mid a^{xy} = (a^x)^y \text{ for all } x \in \mathbb{N}\}.$$

We will prove that $G = \mathbb{N}$, which will immediately imply that $a^{bc} = (a^b)^c$. Clearly $G \in \mathbb{N}$. By Part (a) of Theorem 1.2.11 we deduce that $a^{b \cdot 1} = a^b = (a^b)^1$, and hence $1 \in G$. Now let $c \in G$. This means that $a^{bc} = (a^b)^c$. Using the Distributive Law we obtain

$$a^{b \cdot s(c)} = a^{b(c+1)} = a^{bc+b} = a^{bc} a^b = (a^b)^c a^b = (a^b)^{s(c)}.$$

Therefore $s(c) \in G$, and hence by Part (c) of the Peano Postulates we can conclude that $G = \mathbb{N}$.

(3) Let $G = \{x \in \mathbb{N} \mid b^x c^x = (bc)^x\}$. We will prove that $G = \mathbb{N}$, which will immediately imply that $b^a c^a = (bc)^a$. Clearly $G \in \mathbb{N}$. Because of Part (a) of Theorem 1.2.11 it follows that $b^1 c^1 = bc = (bc)^1$. Now let $a \in G$. Then $b^a c^a = (bc)^a$. Using Part (b) of Theorem 1.2.11 we deduce that $b^{s(a)} = b^a b$ and $c^{s(a)} = c^a c$. By repeated use of the Associative and Commutative Laws for Multiplication we obtain

$$\begin{aligned} b^{s(a)} c^{s(a)} &= (b^a b)(c^a c) = b^a (b c^a) c = b^a (c^a b) c \\ &= (b^a c^a)(bc) = (bc)^a (bc) = (bc)^{s(a)}. \end{aligned}$$

Hence $s(a) \in G$, and because of Part (c) of the Peano Postulates we can conclude that $G = \mathbb{N}$. □

3. Constructing the Integers

Definition 1.3.1. *The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is defined by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$, for all $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$.*

Lemma 1.3.2. *The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Definition 1.3.3. *The set of* ***integers****, denoted $\mathbb{Z}$, is the set of equivalence classes of $\mathbb{N} \times \mathbb{N}$ with respect to the equivalence relation $\sim$.*

The elements $\hat{0}, \hat{1} \in \mathbb{Z}$ are defined by $\hat{0} = [(1, 1)]$ and $\hat{1} = [(1+1, 1)]$. The binary operations $+$ and $\cdot$ on $\mathbb{Z}$ are defined by

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

for all $[(a, b)], [(c, d)] \in \mathbb{Z}$. The unary operation $-$ on $\mathbb{Z}$ is defined by $-[(a, b)] = [(b, a)]$ for all $[(a, b)] \in \mathbb{Z}$. The relation $<$ on $\mathbb{Z}$ is defined by $[(a, b)] < [(c, d)]$ if and only if $a + d < b + c$, for all $[(a, b)], [(c, d)] \in \mathbb{Z}$. The relation $\leq$ on $\mathbb{Z}$ is defined by $[(a, b)] \leq [(c, d)]$ if and only if $[(a, b)] < [(c, d)]$ or $[(a, b)] = [(c, d)]$, for all $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Lemma 1.3.4. *The binary operations $+$ and $\cdot$, the unary operation $-$, and the relation $<$, all on $\mathbb{Z}$, are well-defined.*

Theorem 1.3.5. *Let $x, y, z \in \mathbb{Z}$.*

(1) $(x + y) + z = x + (y + z)$ (Associative Law for Addition).
(2) $x + y = y + x$ (Commutative Law for Addition).
(3) $x + \hat{0} = x$ (Identity Law for Addition).
(4) $x + (-x) = \hat{0}$ (Inverses Law for Addition).
(5) $(xy)z = x(yz)$ (Associative Law for Multiplication).
(6) $xy = yx$ (Commutative Law for Multiplication).
(7) $x \cdot \hat{1} = x$ (Identity Law for Multiplication).
(8) $x(y + z) = xy + xz$ (Distributive Law).
(9) If $xy = \hat{0}$, then $x = \hat{0}$ or $y = \hat{0}$ (No Zero Divisors Law).
(10) Precisely one of $x < y$ or $x = y$ or $x > y$ holds (Trichotomy Law).
(11) If $x < y$ and $y < z$, then $x < z$ (Transitive Law).
(12) If $x < y$ then $x + z < y + z$ (Addition Law for Order).
(13) If $x < y$ and $z > \hat{0}$, then $xz < yz$ (Multiplication Law for Order).
(14) $\hat{0} \neq \hat{1}$ (Non-Triviality).

Definition 1.3.6. *Let $x \in \mathbb{Z}$. The number x is* ***positive*** *if $x > \hat{0}$, and the number x is* ***negative*** *if $x < \hat{0}$.*

Theorem 1.3.7. *Let $i : \mathbb{N} \to \mathbb{Z}$ be defined by $i(n) = [(n + 1, 1)]$ for all $n \in \mathbb{N}$.*

(1) The function $i : \mathbb{N} \to \mathbb{Z}$ is injective.
(2) $i(\mathbb{N}) = \{x \in \mathbb{Z} \mid x > \hat{0}\}$.
(3) $i(1) = \hat{1}$.
(4) Let $a, b \in \mathbb{N}$. Then
(a) $i(a + b) = i(a) + i(b)$;
(b) $i(ab) = i(a)i(b)$;
(c) $a < b$ if and only if $i(a) < i(b)$.

Theorem 1.3.8. *Let $x, y, z \in \mathbb{Z}$.*

(1) If $x + z = y + z$, then $x = y$ (Cancellation Law for Addition).
(2) $-(-x) = x$.
(3) $-(x + y) = (-x) + (-y)$.
(4) $x \cdot 0 = 0$.
(5) If $z \neq 0$ and if $xz = yz$, then $x = y$ (Cancellation Law for Multiplication).
(6) $(-x)y = -xy = x(-y)$.
(7) $xy = 1$ if and only if $x = 1 = y$ or $x = -1 = y$.
(8) $x > 0$ if and only if $-x < 0$, and $x < 0$ if and only if $-x > 0$.
(9) $0 < 1$.
(10) If $x \leq y$ and $y \leq x$, then $x = y$.
(11) If $x > 0$ and $y > 0$, then $xy > 0$. If $x > 0$ and $y < 0$, then $xy < 0$.

Theorem 1.3.9. *Let $x \in \mathbb{Z}$. Then there is no $y \in \mathbb{Z}$ such that $x < y < x + 1$.*

Exercise 1.3.2 (Used in Lemma 1.3.2). Complete the proof of Lemma 1.3.2. That is, prove that the relation $\sim$ is transitive.

Proof. Let $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$. We note that $a+b=b+a$, and hence $(a,b) \sim (a,b)$. Therefore $\sim$ is reflexive. Now suppose that $(a,b) \sim (c,d)$. Then $a+d=b+c$. Hence $c+b=d+a$, and therefore $(c,d) \sim (a,b)$. It follows that $\sim$ is symmetric.

Now let $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$, and suppose that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $a+d=b+c$ and $c+f=d+e$. By adding these two equations and doing some rearranging we obtain $(a+f)+(c+d)=(b+e)+(c+d)$. Canceling yields $a+f=b+e$, or in other words $(a,b) \sim (e,f)$. Hence, $\sim$ is transitive. □

Exercise 1.3.3 (Used in Lemma 1.3.4). Complete the proof of Lemma 1.3.4. That is, prove that $\cdot$ and $-$ for $\mathbb{Z}$ are well-defined. The proof for $\cdot$ is a bit more complicated than might be expected. [Use Exercise 1.2.5.]

Proof. Let $(a, b), (c, d), (x, y), (z, w) \in \mathbb{N} \times \mathbb{N}$. Suppose that $[(a, b)] = [(x, y)]$ and $[(c, d)] = [(z, w)]$.

By hypothesis we know that $(a, b) \sim (x, y)$ and $(c, d) \sim (z, w)$. Hence $a + y = b + x$ and $c + w = d + z$. By adding these two equations and doing some rearranging we obtain $(a + c) + (y + w) = (b + d) + (x + z)$, and we deduce that $[(a + c, b + d)] = [(x + z, y + w)]$. Therefore $+$ is well-defined.

Now suppose that $[(a, b)] < [(b, d)]$. Therefore $a+d < b+c$. Adding $b+x = a+y$ and $c+w = d+z$ to this inequality, we obtain $a+d+b+x+c+w < b+c+a+y+d+z$. Canceling yields $x+w < y+z$, and it follows that $[(x, y)] < [(y, w)]$. This process can be done backwards, and hence $[(x, y)] < [(y, w)]$ implies $[(a, b)] < [(b, d)]$. Therefore $[(a, b)] < [(b, d)]$ if and only if $[(x, y)] < [(y, w)]$, which means that $<$ is well-defined.

Next we will show that $-$ is well-defined, so

$$\begin{aligned} (a, b) \sim (x, y) &\iff a + y = b + x \\ &\iff x + b = y + a \\ &\iff (y, x) \sim (b, a) \\ &\iff (b, a) \sim (y, x) \\ &\iff [(b, a)] = [(y, x)]. \end{aligned}$$

Because $-$ is a function, it follows that

$$[(a, b)] = -[(b, a)] = -[(y, x)] = [(x, y)].$$

Hence, $-$ is well-defined.

We know that $a + y = b + x$, so $(a + y)c = (b + x)c$ and $(b + x)d = (a + y)d$. Having $c + w = d + z$ and by adding these two equations we obtain

$$\begin{gathered} (a + y)c + (b + x)d = (b + x)c + (a + y)d \\ \iff ac + yc + bd + xd = bc + xc + ad + yd \\ \iff (ac + bd) + yc + xd = (ad + bc) + xc + yd \\ \iff (ac + bd) + yc + xd + yw + xz = (ad + bc) + xc + yd + yw + xz \\ \iff (ac + bd) + y(c + w) + x(d + z) = (ad + bc) + (xz + yw) + xc + yd \\ \iff (ac + bd) + y(d + z) + x(c + w) = (ad + bc) + (xz + yw) + xc + yd \\ \iff (ac + bd) + yd + yz + xc + xw = (ad + bc) + (xz + yw) + xc + yd \\ \iff (ac + bd) + (xw + yz) + xc + yd = (ad + bc) + (xz + yw) + xc + yd \\ \iff (ac + bd) + (xw + yz) = (ad + bc) + (xz + yw) \\ \iff (ac + bd, xw + yz) \sim (ad + bc, xz + yw) \\ \iff [(ac + bd, ad + bc)] = [(xz + yw, xw + yz)] \\ \iff [(a, b)] \cdot [(c, d)] = [(x, y)] \cdot [(z, w)]. \end{gathered}$$

Hence, $\cdot$ is well-defined. □

Exercise 1.3.4 (Used in Theorem 1.3.5 and Theorem 1.3.7). Let $a, b \in \mathbb{N}$.

(1) Prove that $[(a, b)] = \hat{0}$ if and only if $a = b$.
(2) Prove that $[(a, b)] = \hat{1}$ if and only if $a = b + 1$.
(3) Prove that $[(a, b)] = [(n, 1)]$ for some $n \in \mathbb{N}$ such that $n \neq 1$ if and only if $a > b$ if and only if $[(a, b)] > \hat{0}$.
(4) Prove that $[(a, b)] = [(1, m)]$ for some $m \in \mathbb{N}$ such that $m \neq 1$ if and only if $a < b$ if and only if $[(a, b)] < \hat{0}$.

Proof of (1). Suppose that $[(a, b)] = \hat{0}$. Then,

$$[(a, b)] = \hat{0} \iff [(a, b)] = [(1, 1)] \iff (a, b) \sim (1, 1)$$
$$\iff a + 1 = b + 1 \iff a = b.$$

□

Proof of (2). Suppose that $[(a, b)] = \hat{1}$. Then,

$$[(a, b)] = \hat{1} \iff [(a, b)] = [(1 + 1, 1)] \iff (a, b) \sim (1 + 1, 1)$$
$$\iff a + 1 = b + 1 + 1 \iff a = b + 1.$$

□

Proof of (3). Suppose that $[(a, b)] = [(n, 1)]$ for some $n \in \mathbb{N}$ such that $n \neq 1$. Then $(a, b) \sim (n, 1)$, so $a + 1 = b + n$. Because $n \neq 1$, by Lemma 1.2.3 we can find some $k \in \mathbb{N}$ such that $n = k + 1$. Then $a + 1 = b + k + 1$, so $a = b + k$. By Definition 1.2.8, it then follows that $a > b$.

Now suppose that $a > b$. Then $a + 1 > b + 1$, and hence $[(a, b)] > [(1, 1)] = \hat{0}$.

Finally, suppose that $[(a, b)] > \hat{0} = [(1, 1)]$. Then $a + 1 > b + 1$. By Definition 1.2.8, there is some $k \in \mathbb{N}$ such that $a + 1 = b + 1 + k$. Let $n = 1 + k$. Then $n \neq 1$ and $a + 1 = b + n$, so $(a, b) \sim (n, 1)$, and hence $[(a, b)] = [(n, 1)]$. □

Proof of (4). Suppose that $[(a, b)] = [(1, m)]$ for some $m \in \mathbb{N}$ such that $m \neq 1$. Then $(a, b) \sim (1, m)$, so $a + m = b + 1$. Because $m \neq 1$, by Lemma 1.2.3 we can find some $k \in \mathbb{N}$ such that $m = k + 1$. Then $a + k + 1 = b + 1$, so $a + k = b$. By Definition 1.2.8, it then follows that $a < b$.

Now suppose that $a < b$. Then $a + 1 < b + 1$, and hence $[(a, b)] < [(1, 1)] = \hat{0}$.

Finally, suppose that $[(a, b)] < \hat{0} = [(1, 1)]$. Then $a + 1 < b + 1$. By Definition 1.2.8, there is some $k \in \mathbb{N}$ such that $a + 1 + k = b + 1$. Let $m = 1 + k$. Then $m \neq 1$ and $a + m = b + 1$, so $(a, b) \sim (1, m)$, and hence $[(a, b)] = [(1, m)]$. □

Exercise 1.3.5 (Used in Theorem 1.3.5). Prove Theorem 1.3.5 (1) (3) (4) (5) (6) (7) (8) (10) (11) (13) (14).

Proof. Suppose that $x = [(a,b)]$, that $y = [(c,d)]$ and that $z = [(e,f)]$, for some $a,b,c,d,e,f \in \mathbb{N}$.

(1) We have

$$\begin{aligned}(x+y)+z &= ([(a,b)]+[(c,d)])+[(e,f)] = [(a+c,b+d)]+[(e,f)]\\ &= [((a+c)+e,(b+d)+f)] = [(a+(c+e),b+(d+f))]\\ &= [(a,b)]+[(c+e,d+f)] = [(a,b)]+([(c,d)]+[(e,f)])\\ &= x+(y+z).\end{aligned}$$

(3) We have

$$\begin{aligned}(a+1)+b = (b+1)+a &\iff (a+1,b+1) \sim (a,b)\\ &\iff [(a+1,b+1)] = [(a,b)]\\ &\iff [(a,b)]+[(1,1)] = [(a,b)]\\ &\iff x+\hat{0} = x.\end{aligned}$$

(4) We have

$$\begin{aligned}x+(-x) &= [(a,b)]+(-[(a,b)]) = [(a,b)]+[(b,a)]\\ &= [(a+b,b+a)] = [(a+b,a+b)].\end{aligned}$$

By Exercise 1.3.4 (1), it then follows that $[(a+b,a+b)] = \hat{0}$, and hence $x+(-x) = \hat{0}$.

(5) We have

$$\begin{aligned}(xy)z &= ([(a,b)]\cdot[(c,d)])\cdot[(e,f)])\\ &= [(ac+bd,ad+bc)]\cdot[(e,f)]\\ &= [((ac+bd)e+(ad+bc)f,(ac+bd)f+(ad+bc)e)]\\ &= [(ace+bde+adf+bcf,acf+bdf+ade+bce)]\\ &= [(a(ce+df)+b(cf+de),a(cf+de)+b(ce+df))]\\ &= [(a,b)]\cdot[(ce+df,cf+de)]\\ &= [(a,b)]\cdot([(c,d)]\cdot[(e,f)]) = x(yz).\end{aligned}$$

(6) We have

$$\begin{aligned}xy &= [(a,b)]\cdot[(c,d)] = [(ac+bd,ad+bc)]\\ &= [(ca+db,da+cb)] = [(ca+db,cb+da)]\\ &= [(c,d)]\cdot[(a,b)]\\ &= yx.\end{aligned}$$

(7) By Exercise 1.3.4 (1) and Part (3) of this theorem, it follows that

$$\begin{aligned}x\cdot\hat{1} &= [(a,b)]\cdot[(1+1,1)] = [(a(1+1)+b\cdot 1,a\cdot 1+b(1+1))]\\ &= [(a+a+b,a+b+b)] = [(a+(a+b),b+(a+b))]\\ &= [(a,b)]+[(a+b,a+b)] = x+\hat{0} = x.\end{aligned}$$

(8) We have

$$\begin{aligned}x(y+z) &= [(a,b)]\cdot([(c,d)]+[(e,f)])\\ &= [(a,b)]\cdot[(c+e,d+f)]\\ &= [(a(c+e)+b(d+f),a(d+f)+b(c+e))]\\ &= [(ac+ae+bd+bf,ad+af+bc+be)]\\ &= [((ac+bd)+(ae+bf),(ad+bc)+(af+be))]\\ &= [(ac+bd,ad+bc)]+[(ae+bf,af+be)]\\ &= ([(a,b)]\cdot[(c,d)])+([(a,b)]\cdot[(e,f)])\\ &= xy+yz.\end{aligned}$$

(10) Suppose that $x = y$. Then $[(a,b)] = [(c,d)]$, so $(a,b) \sim (c,d)$, and as a result $a+d = b+c$. The Trichotomy Law of $\mathbb{N}$ implies that $a+d \not< b+c$ and $a+d \not> b+c$. Therefore $[(a,b)] \not< [(c,d)]$ and $[(a,b)] \not> [(c,d)]$. Thus, $x \not< y$ and $x \not> y$.

Now suppose that $x < y$. Then $[(a,b)] < [(c,d)]$, so $a+d < b+c$. Using the Trichotomy Law of $\mathbb{N}$ again, it follows that $a+d \neq b+c$ and $a+d \not> b+c$, so $[(a,b)] \neq [(c,d)]$ and $[(a,b)] \not> [(c,d)]$. Therefore $x \neq y$ and $x \not> y$.

A similar argument shows that if $x > y$ then $x \neq y$ and $x \not< y$. Thus, $x < y$ or $x = y$ or $x > y$.

Finally, suppose to the contrary that $x \not< y$ and $x \neq y$ and $x \not> y$. Then

$$[(a,b)] \not< [(c,d)] \text{ and } [(a,b)] \neq [(c,d)] \text{ and } [(a,b)] \not> [(c,d)].$$

This implies that

$$a+d \not< b+c \text{ and } a+d \neq b+c \text{ and } a+d \not> b+c,$$

which is a contradiction to the Trichotomy Law of $\mathbb{N}$. Hence, precisely one of $x < y$ or $x = y$ or $x > y$ holds.

(11) Suppose that $x < y$ and $y < z$. Then

$$[(a,b)] < [(c,d)] \text{ and } [(c,d)] < [(e,f)],$$

and we obtain

$$a+d < b+c \text{ and } c+f < d+e.$$

Adding f to the inequality $a+d < b+c$, we get $a+d+f < b+c+f$. Similarly, adding b to the inequality $c+f < d+e$, we get $b+c+f < b+d+e$. Then

$$a+d+f < b+c+f < b+d+e,$$

which implies that $a+d+f < b+d+e$, so $a+f < b+e$. Therefore $[(a,b)] < [(e,f)]$, and hence $x < z$.

(13) Because $z > \hat{0}$, by Exercise 1.3.4 (3) there is some $n \in \mathbb{N}$ such that $n \neq 1$ and $[(e,f)] = [(n,1)]$. Now we can choose some $m \in \mathbb{N}$ such that $n = m+1$ because of Lemma 1.2.3. By hypothesis we know that $x < y$, so $a+d < b+c$. Then $(a+d)m < (b+c)m$. Adding $(a+d)+(b+c)$ to both sides of this inequality, we obtain

$$\begin{aligned}&(a+d)m+(a+d)+(b+c) < (b+c)m+(a+d)+(b+c)\\ \iff\ &(a+d)(m+1)+(b+c) < (b+c)(m+1)+(a+d).\end{aligned}$$

Since $n = m+1$, we have

$$\begin{aligned}&(a+d)n+(b+c) < (b+c)n+(a+d)\\ \iff\ &an+dn+b+c < bn+cn+a+d\\ \iff\ &(an+b)+(c+dn) < (a+bn)+(cn+d)\\ \iff\ &[(an+b,a+bn)] < [(cn+d,c+dn)]\\ \iff\ &[(a,b)]\cdot[(n,1)] < [(c,d)]\cdot[(n,1)].\end{aligned}$$

Because $[(n,1)] = [(e,f)]$, it follows that $[(a,b)]\cdot[(e,f)] < [(c,d)]\cdot[(e,f)]$, and hence $xz < yz$.

(14) We have

$$\begin{aligned}(1+1)+1 &= 1+(1+1)\\ 1+1 &< 1+(1+1)\\ [(1,1)] &< [(1+1,1)]\\ \hat{0} &< \hat{1}.\end{aligned}$$

By the Trichotomy Law it then follows that $\hat{0} \neq \hat{1}$. □

Exercise 1.3.6 (Used in Theorem 1.3.7). Prove Theorem 1.3.7 (1) (3) (4 b) (4 c).

Proof.

(1) Suppose that $i(a) = i(b)$. It then follows that $[(a+1,1)] = [(b+1,1)]$, so $(a+1)+1 = 1+(b+1)$. Doing some rearranging, we get $a+(1+1) = b+(1+1)$, and canceling yields $a = b$. Hence, the function $i : \mathbb{N} \to \mathbb{Z}$ is injective.

(3) We have $i(1) = [(1+1,1)] = \hat{1}$.

(4 b) We have

$$\begin{aligned} i(a)i(b) &= [(a+1,1)] \cdot [(b+1,1)] \\ &= [((a+1)(b+1)+1, (a+1)+(b+1))] \\ &= [(ab+a+b+1+1, a+1+b+1)] \\ &= [((ab+1)+(a+b+1), 1+(a+b+1))] \\ &= [(ab+1,1)] + [(a+b+1, a+b+1)]. \end{aligned}$$

By Exercise 1.3.4 (1) we know that $[(a+b+1, a+b+1)] = \hat{0}$, so by the Identity Law for Addition of $\mathbb{Z}$, it then follows that $i(a)i(b) = [(ab+1,1)] + \hat{0} = [(ab+1,1)] = i(ab)$.

(4 c) Suppose that $a < b$. Then,

$$\begin{aligned} a < b &\iff a+(1+1) < b+(1+1) \\ &\iff (a+1)+1 = 1+(b+1) \\ &\iff [(a+1,1)] < [(b+1,1)] \\ &\iff i(a) < i(b). \end{aligned}$$

□

Exercise 1.3.7. Let $x, y, z \in \mathbb{Z}$.

(1) Prove that $x < y$ if and only if $-x > -y$.
(2) Prove that if $z < 0$, then $x < y$ if and only if $xz > yz$.

Proof of (1). Suppose that $y > x$. Adding $[(-x)] + [(-y)]$ to both sides of this inequality, we have $y+[(-x)+(-y)] > x+[(-x)+(-y)]$ because of the Addition Law for Order. By repeated use of the Associative and Commutative Laws for Addition we deduce that $(-x) + [y + (-y)] > (-y) + [x + (-x)]$. Now by the Inverse Law for Addition we see that $(-x) + 0 > (-y) + 0$, and because of Identity Law for Addition, we can conclude that $-x > -y$. This process can be done backwards, and hence $x < y$ if $-x > -y$. □

Proof of (2). Suppose that $z < 0$, and suppose that $x < y$. By Theorem 1.3.8 (8) we see that $-z > 0$. Then by the Multiplication Law for Order we deduce that $x(-z) < y(-z)$, and by Theorem 1.3.8 (6) it follows that $-xz < -yz$. But then $-(-xz) > -(-yz)$ because of Part (1) of this exercise, and by Theorem 1.3.8 (2) we can conclude that $xz > yz$. This process can be done backwards, and hence $x < y$ if $xz > yz$. □

Exercise 1.3.8 (Used in Exercise 1.5.9). Let $x \in \mathbb{Z}$. Prove that if $x > 0$ then $x \geq 1$. Prove that if $x < 0$ then $x \leq -1$.

Proof. Suppose that $x > 0$. Then by Theorem 1.3.9 we know that there is no $z \in \mathbb{Z}$ such that $0 < z < 0 + 1$, or in other words if $z > 0$ then $z \geq 0 + 1$. Because $x > 0$ we deduce that $x \geq 0 + 1$. But then by the Commutative and Identity Laws for Addition it follows that $0 + 1 = 1 + 0 = 1$, and hence $x \geq 1$. A similar argument shows that $x \geq 1$ implies $x > 0$, and also shows that $x < 0$ if and only if $x \leq -1$. □

Exercise 1.3.9.

(1) Prove that $1 < 2$.
(2) Let $x \in \mathbb{Z}$. Prove that $2x \neq 1$.

Proof of (1). By Theorem 1.3.8 (9) we know that $0 < 1$. Then by the Addition Law for Order we deduce that $0 + 1 < 1 + 1 = 2$, and by the Commutative and Identity Laws for Addition it follows that $0 + 1 = 1 + 0 = 1 < 2$, as required. □

Proof of (2). Suppose to the contrary that $2x = 1$. Then by Theorem 1.3.8 (7) there is either $x = 1 = 2$ or $x = -1 = 2$.

Case 1. $x = 1 = 2$. By Part (1) of this exercise we know that $1 < 2$, so $1 = 2$ and $1 < 2$, which is a contradiction to the Trichotomy Law. Hence, $2x \neq 1$.

Case 2. $x = -1 = 2$. By Theorem 1.3.8 (9) we have $0 < 1$, and because of the Addition Law for Order we get $0 + (-1) < 1 + (-1)$. Now applying the Commutative, Identity, and Inverses Laws for Addition we obtain $-1 < 0$. Also by Part (1) of this exercise we have $1 < 2$. Then $-1 < 0 < 1 < 2$, and by the Transitive Law $-1 < 2$. Since $-1 = 2$ and $-1 < 2$, there is a contradiction to the Trichotomy Law, and hence $2x \neq 1$.

□

Exercise 1.3.10 (Used in Section 1.3). Prove that the Well-Ordering Principle (Theorem 1.2.10), which was stated for $\mathbb{N}$ in Section 1.2, still holds when we think of $\mathbb{N}$ as the set of positive integers. That is, let $G \subseteq \{x \in \mathbb{Z} \mid x > 0\}$ be a non-empty set. Prove that there is some $m \in G$ such that $m \leq g$ for all $g \in G$. Use Theorem 1.3.7.

Proof. Let

$$\mathbb{N}_G = \{a \in \mathbb{N} \mid \text{there is some } g \in G \text{ such that } i(a) = g\}.$$

Then clearly $\mathbb{N}_G \subseteq \mathbb{N}$ and $G = i(\mathbb{N}_G)$. The nonemptiness of G implies the nonemptiness of $\mathbb{N}_G$, and by Well-Ordering Principle of $\mathbb{N}$ there is some $n_\circ \in \mathbb{N}_G$ such that $n_\circ \leq n$ for all $n \in \mathbb{N}_G$. Let $m = i(n_\circ)$, and let $g \in G$. By hypothesis on G we know that $G \subseteq \{x \in \mathbb{Z} \mid x > 0\}$, so by Theorem 1.3.7 (2) it follows that $G = i(\mathbb{N}_G) \subseteq i(\mathbb{N})$. We can choose some $n \in \mathbb{N}_G$ such that $i(n) = g$. Then $n_\circ \leq n$, and by Theorem 1.3.7 (4 c) we can conclude that $m = i(n_\circ) \leq i(n) = g$. □

Exercise 1.3.11 (Used in Theorem 1.3.8). Prove Theorem 1.3.8 (1) (3) (4) (5) (7) (10) (11).

Proof.

(1) Suppose that $x + z = y + z$. Adding $-z$ to both sides of this equation we obtain $x + z + (-z) = y + z + (-z)$. By the Associative Law for Addition we get $x + [z + (-z)] = y + [z + (-z)]$. Because of Inverses Law for Addition we see that $z + (-z) = 0$, so this implies that $x + 0 = y + 0$. But then by Identity Law for Addition we can conclude that $x = y$.

(3) By the Inverses Law for Addition we have $-(x+y)+(x+y) = 0$. Adding $(-x) + (-y)$ to both sides of this equation we obtain

$$-(x + y) + (x + y) + (-x) + (-y) = (-x) + (-y).$$

By repeated use of the Associative, Commutative, and Identity Laws for Addition it follows that

$$\begin{aligned} -(x + y) + (x + y) + (-x) + (-y) &= -(x + y) + [x + (-x)] + [y + (-y)] \\ &= -(x + y) + 0 + 0 \\ &= [-(x + y) + 0] + 0 = -(x + y) + 0 \\ &= -(x + y). \end{aligned}$$

Hence, $-(x + y) = (-x) + (-y)$.

(4) By the Identity Law for Addition we know that $0 + 0 = 0$, so using the Distributive Law we obtain

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0.$$

Adding $-(x \cdot 0)$ to both sides of the equation $x \cdot 0 + x \cdot 0 = x \cdot 0$ we get

$$x \cdot 0 + x \cdot 0 + [-(x \cdot 0)] = x \cdot 0 + [-(x \cdot 0)].$$

Now by the Associative Law for Addition we get

$$x \cdot 0 + (x \cdot 0 + ([-(x \cdot 0)])) = x \cdot 0 + [-(x \cdot 0)],$$

and by the Inverses Law for Addition we see that $x \cdot 0 + 0 = 0$. Finally, by the Identity Law for Addition it follows that $x \cdot 0 = 0$, as required.

(5) Suppose that $z \neq 0$ and $xz = yz$. Now suppose to the contrary that $x \neq y$, and suppose, without loss of generality, that $x < y$. If $z < 0$ then by Exercise 1.3.7 (2) it follows that $xz > yz$, which is a contradiction to the Trichotomy Law. If $z > 0$ then by the Multiplication Law for Order it follows that $xz < yz$, again a contradiction to the Trichotomy Law. Hence, $x = y$.

(7) By Part (9) of this theorem we know that $0 < 1$, so by the Addition Law for Order we deduce that $0 + a < 1 + a$ for all $a \in \mathbb{Z}$. By the Commutative and Identity Laws for Addition we obtain $a < a + 1$ for all $a \in \mathbb{Z}$.

Suppose that $xy = 1$, and suppose to the contrary that either $x \neq 1$ or $y \neq 1$. Without loss of generality, suppose that $x \neq 1$. Then either $x < 1$ or $x > 1$. Suppose that $x < 1$. Using the Identity and Commutative Laws for Addition we obtain $x < 1 = 1 + 0 = 0 + 1$, and by the Well-Ordering Principle we deduce that $x \leq 0$, or in other words either $x < 0$ or $x = 0$. If $x = 0$, then using the Commutative Law for Multiplication we get $xy = 0 \cdot y = y \cdot 0 = 1$, which contradicts Part (4) of this theorem. Hence, $x \neq 0$. A similar argument shows that $y \neq 0$. Next since $x \neq 0$, we have

$$\begin{aligned} x < 0 &\iff x < 1 + (-1) && \text{(Inverses Law for Addition)} \\ &\iff x < (-1) + 1 && \text{(Commutative Law for Addition)} \\ &\iff x \leq -1 && \text{(Well-Ordering Principle)} \\ &\iff -x \geq -(-1) && \text{(Part (1) of Exercise 1.3.7)} \\ &\iff -x \geq 1 && \text{(Part (2) of this theorem).} \end{aligned}$$

We also know that $-x < (-x) + 1$, so $1 \leq -x < (-x) + 1$, and by the Transitive Law we get $1 < (-x) + 1$. If $y > 0$ then

$$\begin{aligned} & 1 \leq -x < (-x) + 1 \\ &\iff 1 < (-x) + 1 && \text{(Transitive Law)} \\ &\iff y \cdot 1 < y[(-x) + 1] && \text{(Multiplication Law for Order)} \\ &\iff y \cdot 1 < y(-x) + y \cdot 1 && \text{(Distributive Law)} \\ &\iff y \cdot 1 < y[-(x \cdot 1)] + y \cdot 1 && \text{(Identity Law for Multiplication)} \\ &\iff y \cdot 1 < -[y(x \cdot 1)] + y \cdot 1 && \text{(Part (6) of this theorem)} \\ &\iff y < (-yx) + y && \text{(Identity Law for Multiplication)} \\ &\iff y < (-1) + y && \text{(Hypothesis on } xy\text{)} \\ &\iff y + 1 < (-1) + y + 1 && \text{(Addition Law for Order)} \\ &\iff y + 1 < y + 1 + (-1) && \text{(Commutative Law for Addition)} \\ &\iff y + 1 < y + [1 + (-1)] && \text{(Associative Law for Addition)} \\ &\iff y + 1 < y + 0 && \text{(Inverses Law for Addition)} \\ &\iff y + 1 < y && \text{(Identity Law for Addition),} \end{aligned}$$

which is a contradiction to the Trichotomy Law because $a < a + 1$ for all $a \in \mathbb{Z}$. If $y < 0$ then

$$\begin{aligned} & 1 \leq -x < (-x) + 1 \\ &\iff y[(-x) + 1] < y(-x) < y \cdot 1 && \text{(Multiplication Law for Order)} \\ &\iff y(-x) + y \cdot 1 < y(-x) < y \cdot 1 && \text{(Distributive Law)} \\ &\iff y[-(x \cdot 1)] + y \cdot 1 < y(-x) < y \cdot 1 && \text{(Identity Law for Multiplication)} \\ &\iff [-y(x \cdot 1)] + y \cdot 1 < -yx < y \cdot 1 && \text{(Part (6) of this theorem)} \\ &\iff (-yx) + y < -xy < y && \text{(Identity Law for Multiplication)} \\ &\iff (-1) + y < -xy < y && \text{(Hypothesis on } xy\text{)} \\ &\iff (-1) + y + 1 < -xy < y + 1 && \text{(Addition Law for Order)} \\ &\iff y + 1 + (-1) < -xy < y + 1 && \text{(Commutative Law for Addition)} \\ &\iff y + [1 + (-1)] < -xy < y + 1 && \text{(Associative Law for Addition)} \\ &\iff y + 0 < -xy < y + 1 && \text{(Inverses Law for Addition)} \\ &\iff y < -xy < y + 1 && \text{(Identity Law for Addition),} \end{aligned}$$

which is a contradiction to the Well-Ordering Principle. Hence, if $x < 1$ then $x = 1 = y$. If $x > 1$, then it follows that $1 < x < x + 1$, so a similar argument leads to a contradiction, and hence $x = 1 = y$. Thus, we can conclude that if $xy = 1$ then either $x = 1 = y$ or $x = -1 = y$.

Now suppose that either $x = 1 = y$ or $x = -1 = y$. If $x = 1 = y$ then $xy = 1 \cdot 1 = 1$ because of the Identity Law for Multiplication. Suppose that $x = -1 = y$. Then $xy = (-1) \cdot (-1)$. Using Part (6) of this theorem we have $(-1) \cdot (-1) = -[(-1) \cdot 1]$, and by the Identity Law for Multiplication it follows that $(-1) \cdot 1 = -1$, so $xy = -(-1)$. Finally, by Part (2) of this theorem we deduce that $xy = 1$.

(10) Taking the contrapositive, suppose that $x \neq y$. Then by the Trichotomy Law we deduce that either $x > y$ or $y > x$, as required.

(11) Suppose that $x > 0$ and $y > 0$. By the Addition Law for Order it follows that $x + 1 > 1$. Using the Multiplication Law for Order we obtain $(x + 1)y > 1 \cdot y$. Because of the Distributive Law we get $y(x + 1) = yx + y$, and by the Commutative Law for Multiplication we know that $yx = xy$ and $1 \cdot y = y \cdot 1$, so $xy + y > y \cdot 1$. Also, we know that $y \cdot 1 = y$ because of the Identity Law for Multiplication. Thus, $xy + y > y$. Using the Inverses and Commutative Laws for Addition we deduce that $y = y + 0 = 0 + y$, so $xy + y > 0 + y$. Finally, by the Cancellation Law for Addition we can conclude that $xy > 0$. A similar argument shows that if $x < 0$ and $y < 0$ then $xy < 0$. □

4. Entry 2: Axioms for the Integers

Definition 1.4.1. *An* ***ordered integral domain*** *is a set R with elements $0, 1 \in R$, binary operations $+$ and $\cdot$, a unary operation $-$ and a relation $<$, which satisfy the following properties. Let $x, y, z \in R$.*

(a) $(x + y) + z = x + (y + z)$ *(Associative Law for Addition).*
(b) $x + y = y + x$ *(Commutative Law for Addition).*
(c) $x + 0 = x$ *(Identity Law for Addition).*
(d) $x + (-x) = 0$ *(Inverses Law for Addition).*
(e) $(xy)z = x(yz)$ *(Associative Law for Multiplication).*
(f) $xy = yx$ *(Commutative Law for Multiplication).*
(g) $x \cdot 1 = x$ *(Identity Law for Multiplication).*
(h) $x(y + z) = xy + xz$ *(Distributive Law).*
(i) *If $xy = 0$, then $x = 0$ or $y = 0$ (No Zero Divisors Law).*
(j) *Precisely one of $x < y$ or $x = y$ or $x > y$ holds (Trichotomy Law).*
(k) *If $x < y$ and $y < z$, then $x < z$ (Transitive Law).*
(l) *If $x < y$ then $x + z < y + z$ (Addition Law for Order).*
(m) *If $x < y$ and $z > 0$, then $xz < yz$ (Multiplication Law for Order).*
(n) $0 \neq 1$ *(Non-Triviality).*

Definition 1.4.2. *Let R be an ordered integral domain, and let $A \subseteq R$ be a set.*

(1) *The relation $\leq$ on R is defined by $a \leq b$ if and only if $a < b$ or $a = b$, for all $a, b \in R$.*
(2) *The set A has a* ***least element*** *if there is some $a \in A$ such that $a \leq x$ for all $x \in A$.*

Definition 1.4.3. *Let R be an ordered integral domain. The ordered integral domain R satisfies the* ***Well-Ordering Principle*** *if every non-empty subset of $\{x \in R \mid x > 0\}$ has a least element.*

Axiom 1.4.4 (Axiom for the Integers). *There exists an ordered integral domain $\mathbb{Z}$ that satisfies the Well-Ordering Principle.*

Lemma 1.4.5. *Let $x, y, z \in \mathbb{Z}$.*

(1) *If $x + z = y + z$, then $x = y$ (Cancellation Law for Addition).*
(2) $-(-x) = x$.
(3) $-(x + y) = (-x) + (-y)$.
(4) $x \cdot 0 = 0$.
(5) *If $z \neq 0$ and if $xz = yz$, then $x = y$ (Cancellation Law for Multiplication).*
(6) $(-x)y = -xy = x(-y)$.
(7) *$xy = 1$ if and only if $x = 1 = y$ or $x = -1 = y$.*
(8) *$x > 0$ if and only if $-x < 0$, and $x < 0$ if and only if $-x > 0$.*
(9) $0 < 1$.
(10) *If $x \leq y$ and $y \leq x$, then $x = y$.*
(11) *If $x > 0$ and $y > 0$, then $xy > 0$. If $x > 0$ and $y < 0$, then $xy < 0$.*

Theorem 1.4.6. *Let $x \in \mathbb{Z}$. Then there is no $y \in \mathbb{Z}$ such that $x < y < x + 1$.*

Definition 1.4.7.

(1) *Let $x \in \mathbb{Z}$. The number x is positive if $x > 0$, and the number x is negative if $x < 0$.*
(2) *The set of natural numbers, denoted $\mathbb{N}$, is defined by*

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}.$$

Theorem 1.4.8 (Peano Postulates). *Let $s : \mathbb{N} \to \mathbb{N}$ be defined by $s(n) = n + 1$ for all $n \in \mathbb{N}$.*

(a) *There is no $n \in \mathbb{N}$ such that $s(n) = 1$.*
(b) *The function s is injective.*
(c) *Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.*

Lemma 1.4.9 (Not in the book). *Let $a, b \in \mathbb{Z}$. Suppose that $a < b$. Then there is some $k \in \mathbb{N}$ such that $a + k = b$.*

Proof. Let $k = b + (-a)$. By the Addition Law for Order we have $b + (-a) > a + (-a)$, and by the Inverses Law for Addition we deduce that $k = b + (-a) > 0$. Hence, $k \in \mathbb{N}$. Now adding a to both sides of the equation $k = b + (-a)$ we obtain $k + a = b + (-a) + a$. Using the Associative and Commutative Laws for Addition it follows that $a + k = b + [a + (-a)]$, and hence by the Inverses and Identity Laws for Addition we see that $a + k = b$. □

Exercise 1.4.2 (Used in Section 1.4). Let $n \in \mathbb{N}$. Prove that $n + 1 \in \mathbb{N}$.

Proof. Suppose that $n \in \mathbb{N}$. Then $n \in \mathbb{Z}$ and $n > 0$. Using the Addition Law for Order we obtain $n + 1 > 0 + 1$. By the Commutative and Identity Laws for Addition we deduce that $n + 1 > 1$. Also, we know by Part (9) of Lemma 1.4.5 that $0 < 1$. Then applying the Transitive Law we get $n + 1 > 0$, and hence by the definition of $\mathbb{N}$ we see that $n + 1 \in \mathbb{N}$. □

Exercise 1.4.3 (Used in Exercise 1.4.8). Let $x, y \in \mathbb{Z}$. Prove that $x \leq y$ if and only if $-x \geq -y$.

Proof. Suppose that $x \leq y$, which means that either $x = y$ or $x < y$. Suppose that $x = y$. Then $x(-1) = y(-1)$, and by Part (6) of Lemma 1.4.5 we obtain $-(x \cdot 1) = -(y \cdot 1)$. Hence by the Identity Law for Multiplication we see that $-x = -y$.

Now suppose that $x < y$, or in other words $y > x$. Then by the Addition Law for Order we deduce that $y+(-x)+(-y) > x+(-x)+(-y)$. Using the Commutative and Associative Laws for Addition we get $(-x) + [y + (-y)] > (-y) + [x + (-x)]$. But then by the Inverses and Identity Laws for Addition we can conclude that $-x > -y$.

Thus, $-x \geq -y$. This process can be done backwards, and hence $x \leq y$ if and only if $-x \geq -y$. □

Exercise 1.4.4 (Used in Exercise 1.4.6, Exercise 1.4.8 and Exercise 1.5.9). Prove that $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 1\}$.

Proof. We will prove that $x > 0$ if and only if $x \geq 1$ for all $x \in \mathbb{Z}$, which will imply that $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 1\}$. Let $x \in \mathbb{Z}$, and suppose that $x > 0$. Then by the Well-Ordering Principle it follows that $x \geq 0 + 1$, and hence by the Commutative and Identity Laws for Addition we can conclude that $x \geq 1$. Now suppose that $x \geq 1$, which means that either $x = 1$ or $x > 1$. Because of Lemma 1.4.5 (9) we know that $0 < 1$, so if $x = 1$ then clearly $x > 0$. But if $x > 1$ then $0 < 1 < x$, and by the Transitive Law we deduce that $x > 0$.

□

Exercise 1.4.5. Let $a, b \in \mathbb{Z}$. Prove that if $a < b$, then $a + 1 \leq b$.

Proof. If $a < b$ then by the Well-Ordering Principle it follows that $a + 1 \leq b$. □

Exercise 1.4.6 (Used in Theorem 2.5.4). Let $n \in \mathbb{N}$. Suppose that $n \neq 1$. Prove that there is some $b \in \mathbb{N}$ such that $b + 1 = n$. [Use Exercise 1.4.4.]

Proof. Let $b = n+(-1)$. By Exercise 1.4.4 we know that $n \geq 1$, and because $n \neq 1$ it implies that $n > 1$. By the Addition Law for Order it follows that $n + (-1) > 1 + (-1)$, and by the Inverses Law for Addition we deduce that $n + (-1) > 0$, so $b > 0$. Hence, $b \in \mathbb{N}$.

We have $b + 1 = n + (-1) + 1$. By the Commutative and Inverses Laws for Addition we see that $(-1) + 1 = 1 + (-1) = 0$. Then applying the Associative Law for Addition we deduce that $n + [(-1) + 1] = n + 0$, and hence by the Identity Law for Addition we can conclude that $b + 1 = n$. □

Exercise 1.4.7 (Used in Section 1.4). Let $\mathbb{Z}[x]$ denote the set of polynomials with integer coefficients and variable x. This set has binary operations $+$ and $\cdot$ as usual for polynomials. The relation $<$, called the **dictionary order** on $\mathbb{Z}[x]$, is defined by $f < g$ if and only if either the degree of f is less than the degree of g, or if the degrees of f and g are equal and if $f \neq g$ and if the highest degree coefficient which differs for f and g is smaller for f, for all $f, g \in \mathbb{Z}[x]$. Let $0, 1 \in \mathbb{Z}[x]$ be the polynomials that are constantly 0 and 1, respectively.

(1) Prove that $\mathbb{Z}[x]$, with $+$, $\cdot$, $<$, 0 and 1 as defined above, is an ordered integral domain.
(2) Let $f \in \mathbb{Z}[x]$. Prove that there is no $g \in \mathbb{Z}[x]$ such that $f < g < f + 1$.
(3) Prove that $\mathbb{Z}[x]$ does not satisfy the Well-Ordering Principle.

Definition 1.4.10. *The set of* ***polynomials with variable*** x*, denoted* $\mathbb{Z}[x]$*, is the set of infinite sequences with integer coefficients in ascending order of degrees.*

The elements $\widetilde{0}, \widetilde{1} \in \mathbb{Z}[x]$ *are defined by* $\widetilde{0} = (0, 0, 0, \ldots)$ *and* $\widetilde{1} = (1, 0, 0, \ldots)$. *The binary operations* $+$ *and* $\cdot$ *on* $\mathbb{Z}[x]$ *are defined by*

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0,\ a_1 + b_1,\ a_2 + b_2,\ \ldots)$$
$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

for all $(a_0, a_1, a_2, \ldots), (b_0, b_1, b_2, \ldots) \in \mathbb{Z}[x]$ *where* $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ *for all* $n \in \mathbb{Z}^+$. *The unary operation* $-$ *on* $\mathbb{Z}[x]$ *is defined by* $-(a_0, a_1, a_2, \ldots) = (-a_0, -a_1, -a_2, \ldots)$.

The sequence $(a_0, a_1, a_2, \ldots)$ *is also denoted* $(a_n)_{n=0}^{\infty}$.

Definition 1.4.11. *Let* R *be an ordered integral domain, and let* $A \subseteq R$ *be a set. The set* A *has a* ***greatest element*** *if there is some* $a \in A$ *such that* $a \geq x$ *for all* $x \in A$.

Definition 1.4.12. *The* ***degree*** *of* $a \in \mathbb{Z}[x]$*, denoted* $\deg(a)$*, is either* 0 *if* $a = \widetilde{0}$ *or the greatest integer* $n \in \mathbb{Z}^+$ *such that* $a_n \neq 0$.

Definition 1.4.13. *The relation* $<$*, called the* ***dictionary order*** *on* $\mathbb{Z}[x]$*, is defined by* $a < b$ *if and only if either* $\deg(a) < \deg(b)$ *or* $\deg(a) = \deg(b)$ *and there is the greatest* $n \leq \deg(a) = \deg(b)$ *such that* $a_n < b_n$ *for all* $a, b \in \mathbb{Z}[x]$.

Proof of (1). Let $a, b, c \in \mathbb{Z}[x]$. We will prove that $\mathbb{Z}[x]$ satisfies the following properties, which will imply that $\mathbb{Z}[x]$ is an ordered integral domain.

(1) $(a + b) + c = a + (b + c)$ (Associative Law for Addition).
(2) $a + b = b + a$ (Commutative Law for Addition).
(3) $a + \widetilde{0} = a$ (Identity Law for Addition).
(4) $a + (-a) = \widetilde{0}$ (Inverses Law for Addition).
(5) $(ab)c = a(bc)$ (Associative Law for Multiplication).
(6) $ab = ba$ (Commutative Law for Multiplication).
(7) $a \cdot \widetilde{1} = a$ (Identity Law for Multiplication).
(8) $a(b + c) = ab + ac$ (Distributive Law).
(9) If $ab = \widetilde{0}$, then $a = \widetilde{0}$ or $b = \widetilde{0}$ (No Zero Divisors Law).
(10) Precisely one of $a < b$ or $a = b$ or $a > b$ holds (Trichotomy Law).
(11) If $a < b$ and $b < c$, then $a < c$ (Transitive Law).
(12) If $a < b$ then $a + c < b + c$ (Addition Law for Order).
(13) If $a < b$ and $c > \widetilde{0}$, then $ac < bc$ (Multiplication Law for Order).
(14) $\widetilde{0} \neq \widetilde{1}$ (Non-Triviality).

(1) Using the Associative Law for Addition for the integers we obtain

$$\begin{aligned}(a + b) + c &= [(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots)] + (c_0, c_1, c_2, \ldots)\\ &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) + (c_0, c_1, c_2, \ldots)\\ &= ([a_0 + b_0] + c_0,\ [a_1 + b_1] + c_1,\ [a_2 + b_2] + c_2,\ \ldots)\\ &= (a_0 + [b_0 + c_0],\ a_1 + [b_1 + c_1],\ a_2 + [b_2 + c_2],\ \ldots)\\ &= (a_0, a_1, a_2, \ldots) + (b_0 + c_0, b_1 + c_1, b_2 + c_2, \ldots)\\ &= (a_0, a_1, a_2, \ldots) + [(b_0, b_1, b_2, \ldots) + (c_0, c_1, c_2, \ldots)]\\ &= a + (b + c).\end{aligned}$$

(2) Using the Commutative Law for Addition for the integers we obtain

$$\begin{aligned}a + b &= (a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots)\\ &= (a_0 + b_0,\ a_1 + b_1,\ a_2 + b_2,\ \ldots)\\ &= (b_0 + a_0,\ b_1 + a_1,\ b_2 + a_2,\ \ldots)\\ &= (b_0, b_1, b_2, \ldots) + (a_0, a_1, a_2, \ldots)\\ &= b + a.\end{aligned}$$

(3) Using the Identity Law for Addition for the integers it follows that

$$\begin{aligned}a + \widetilde{0} &= (a_0, a_1, a_2, \ldots) + (0, 0, 0, \ldots)\\ &= (a_0 + 0,\ a_1 + 0,\ a_2 + 0,\ \ldots)\\ &= (a_0, a_1, a_2, \ldots) = a.\end{aligned}$$

(4) Using the Inverses Law for Addition for the integers we get

$$\begin{aligned}a + (-a) &= (a_0, a_1, a_2, \ldots) + [-(a_0, a_1, a_2, \ldots)]\\ &= (a_0, a_1, a_2, \ldots) + (-a_0, -a_1, -a_2, \ldots)\\ &= (a_0 + [-a_0],\ a_1 + [-a_1],\ a_2 + [-a_2],\ \ldots)\\ &= (0, 0, 0, \ldots) = \widetilde{0}.\end{aligned}$$

(5) Using the Distributive Law for the integers we obtain

$$\begin{aligned}(ab)c &= \left(\sum_{i=0}^{n} (ab)_i c_{n-i}\right)_{n=0}^{\infty} = \left(\sum_{i=0}^{n}\sum_{j=0}^{i} a_j b_{i-j} c_{n-i}\right)_{n=0}^{\infty}\\ &= \left(\sum_{j=0}^{n}\sum_{i=j}^{n} a_j b_{i-j} c_{n-i}\right)_{n=0}^{\infty} = \left(\sum_{j=0}^{n} a_j \sum_{i=j}^{n} b_{i-j} c_{n-i}\right)_{n=0}^{\infty}\\ &= \left(\sum_{j=0}^{n} a_j \sum_{k=0}^{n-j} b_k c_{n-j-k}\right)_{n=0}^{\infty} = \left(\sum_{j=0}^{n} a_j (bc)_{n-j}\right)_{n=0}^{\infty}\\ &= a(bc).\end{aligned}$$

(6) Using the Commutative Law for Multiplication for the integers we get

$$ab = \left(\sum_{i=0}^{n} a_i b_{n-i}\right)_{n=0}^{\infty} = \left(\sum_{j=0}^{n} a_{n-j} b_j\right)_{n=0}^{\infty} = \left(\sum_{j=0}^{n} b_j a_{n-j}\right)_{n=0}^{\infty} = ba.$$

(7) By the definition of $\widetilde{1}$ we know that $\widetilde{1}_0 = 1$ and if $n \neq 0$ then $\widetilde{1}_n = 0$. Using Lemma 1.4.5 (4) and the Identity and Commutative Laws for Addition for the integers it then follows that

$$\begin{aligned}a \cdot \widetilde{1} &= \left(\sum_{i=0}^{n} (a_i \cdot \widetilde{1}_{n-i})\right)_{n=0}^{\infty} = \left(\sum_{i=0}^{n-1} (a_i \cdot \widetilde{1}_{n-i}) + a_n \cdot \widetilde{1}_0\right)_{n=0}^{\infty}\\ &= \left(\sum_{i=0}^{n-1} (a_i \cdot 0) + a_n \cdot 1\right)_{n=0}^{\infty} = \left(\sum_{i=0}^{n-1} 0 + a_n\right)_{n=0}^{\infty}\\ &= (0 + a_n)_{n=0}^{\infty} = (a_n + 0)_{n=0}^{\infty} = (a_n)_{n=0}^{\infty} = a.\end{aligned}$$

(8) Using the Distributive Law for the integers we obtain

$$\begin{aligned}a(b + c) &= \left(\sum_{i=0}^{n} a_i (b + c)_{n-i}\right)_{n=0}^{\infty} = \left(\sum_{i=0}^{n} a_i (b_{n-i} + c_{n-i})\right)_{n=0}^{\infty}\\ &= \left(\sum_{i=0}^{n} (a_i b_{n-i} + a_i c_{n-i})\right)_{n=0}^{\infty} = \left(\sum_{i=0}^{n} a_i b_{n-i} + \sum_{i=0}^{n} a_i c_{n-i}\right)_{n=0}^{\infty}\\ &= \left(\sum_{i=0}^{n} a_i b_{n-i}\right)_{n=0}^{\infty} + \left(\sum_{i=0}^{n} a_i c_{n-i}\right)_{n=0}^{\infty} = ab + ac.\end{aligned}$$

(9) Suppose that $ab = \widetilde{0}$, and suppose to the contrary that $a \neq \widetilde{0}$ and $b \neq \widetilde{0}$. By the definition of polynomial we know that there is some $p, q \in \mathbb{Z}^+$ such that a_p and b_q are greatest nonzero elements of a and b, respectively. This implies $a_x = 0 = b_y$ for all $x > p$ and $y > q$. Then,

$$\begin{aligned}\sum_{i=0}^{p+q} a_i b_{p+q-i} &= \sum_{i=0}^{p-1} a_i b_{p+q-i} + a_p b_q + \sum_{i=p+1}^{p+q-i} a_i b_{p+q-i}\\ &= \sum_{i=0}^{p-1} a_i \cdot 0 + a_p b_q + \sum_{i=p+1}^{p+q-i} 0 \cdot b_{p+q-i}.\end{aligned}$$

By the Commutative Law for Multiplication for the integers we observe that

$$\sum_{i=p+1}^{p+q-i} 0 \cdot b_{p+q-i} = \sum_{i=p+1}^{p+q-i} b_{p+q-i} \cdot 0,$$

and from the Identity Law for Multiplication and the Identity Law for Addition for the integers we deduce that

$$\sum_{i=0}^{p-1} a_i \cdot 0 = \sum_{i=0}^{p-1} 0 = 0 = \sum_{i=p+1}^{p+q-i} 0 = \sum_{i=p+1}^{p+q-i} b_{p+q-i} \cdot 0.$$

Finally, by repeated use of the Commutative and Identity Laws for Addition for the integers we obtain

$$\sum_{i=0}^{p+q} a_i b_{p+q-i} = 0 + a_p b_q + 0 = (a_p b_q + 0) + 0 = a_p b_q + 0 = a_p b_q.$$

Since $a_p \neq 0$ and $b_q \neq 0$, the No Zero Divisors Law for the integers implies that $a_p b_q \neq 0$. Hence, $\sum_{i=0}^{p+q} a_i b_{p+q-i} \neq 0$. But then $(\sum_{i=0}^{n} a_i b_{n-i})_{n=0}^{\infty} \neq \widetilde{0}$, which is a contradiction to the fact that $ab = \widetilde{0}$. Hence, there is either $a = \widetilde{0}$ or $b = \widetilde{0}$.

(10) Suppose that $a = b$. Then $(a_n)_{n=0}^{\infty} = (b_n)_{n=0}^{\infty}$. Because of the Trichotomy Law for the integers we deduce that $a_n \nless b_n$ and $a_n \ngtr b_n$ for all $n \in \mathbb{Z}^+$. Hence, $a \nless b$ and $a \ngtr b$.

Now let $n = \deg(a)$ and $m = \deg(b)$. Without loss of generality, suppose that $a < b$. Suppose that $n < m$. By the Trichotomy Law for the integers it follows that $n \neq m$ and $n \ngtr m$, and hence by the definition of dictionary order we can conclude that $a \neq b$ and $a \ngtr b$. We consider the following two cases.

Case 1. $n < m$. By the Trichotomy Law for the integers it follows that $n \neq m$ and $n \ngtr m$, and hence by the definition of dictionary order we can conclude that $a \neq b$ and $a \ngtr b$.

Case 2. $n \ngtr m$. Then $n = m$ and there is the greatest $p \leq n = m$ such that $a_p < b_p$. By the Trichotomy Law for the integers we see that $a_p \neq b_p$ and $a_p \ngtr b_p$. Hence by the definition of dictionary order we have shown that $a \neq b$ and $a \ngtr b$.

Finally, suppose to the contrary that $a \neq b$ and $a \nless b$ and $a \ngtr b$. Then $n \nless m$ and $n \neq m$ and $n \ngtr m$, which is a contradiction to the Trichotomy Law for the integers. Hence, precisely one of $a < b$ or $a = b$ or $a > b$ holds.

(11) Let p, q, and r be the degrees of a, b, and c, respectively. If $p < q$ and $q < r$, then by the Trichotomy Law for the integers we get $p < r$, and hence $a < c$. Suppose that $p = q = r$. There is the greatest $s \leq p = q = r$ and $t \leq p = q = r$ such that $a_s < b_s$ and $b_t < c_t$. We consider the following three cases.

Case 1. $s < t$. Then $a_s < b_s = c_s$, and hence $a < c$.

Case 2. $s > t$. Then $a_t = b_t < c_t$, and hence $a < c$.

Case 3. $s = t$. Then $a_s < b_s < c_s$, and by the Trichotomy Law for the integers we deduce that $a_s < c_s$. Hence, $a < c$.

Now suppose, without loss of generality, that $p < q$ and $q = r$. Then clearly $p < r$, and as a result $a < c$.

(12) Let $d_a, d_b, d_c, d_{a+c}, d_{b+c} \in \mathbb{Z}^+$ be the degrees of $a, b, c, a + c, b + c \in \mathbb{Z}[x]$, respectively. We note that $d_{a+c} = \max(d_a, d_c)$ and $d_{b+c} = \max(d_b, d_c)$. Suppose that $d_a = d_b$. Then $\max(d_a, d_c) = \max(d_b, d_c)$, and then $d_{a+c} = d_{b+c}$. Also, we observe that there is the greatest $p \leq d_a = d_b$ such that $a_p < b_p$. By Addition Law for Order for the integers it follows that $a_p + c_p < b_p + c_p$. Hence, $a + c < b + c$.

Now suppose that $d_a < d_b$. We consider the following three cases.

Case 1. $d_a < d_b < d_c$. Then $\max(d_a, d_c) = d_c$ and $\max(d_b, d_c) = d_c$, and then $d_{a+c} = d_{b+c}$. Let $p = d_b$. Because $d_a < d_b$ we see that $p \leq d_{a+c} = d_{b+c}$ is the greatest element of $\mathbb{Z}^+$ such that $a_p < b_p$. By Addition Law for Order for the integers it follows that $a_p + c_p < b_p + c_p$, and hence $a + c < b + c$.

Case 2. $d_c \leq d_a < d_b$. Then $\max(d_a, d_c) = d_a$ and $\max(d_b, d_c) = d_b$, and then $d_{a+c} < d_{b+c}$. Hence $a + c < b + c$.

Case 3. $d_a < d_c \leq d_b$. A similar argument shows that $a + c < b + c$.

(13) We note that $\deg(ab) = \deg(a) + \deg(b)$ for all $a, b \in \mathbb{Z}[x]$. Suppose that $a < b$ and $c > \widetilde{0}$. Suppose further that $\deg(a) < \deg(b)$. Because $c > \widetilde{0}$ it follows that $\deg(c) > 0$. We then deduce from the Addition Law for Order for the integers that $\deg(a) + \deg(c) < \deg(b) + \deg(c)$. Then $\deg(ac) < \deg(bc)$, and hence $ac < bc$.

Now suppose that $\deg(a) = \deg(b)$. Then there is the greatest $p \leq \deg(a) = \deg(b)$ such that $a_p < b_p$. Then $\deg(ac) = \deg(bc)$, and because $c > \widetilde{0}$ we have $p \leq \deg(ac) = \deg(bc)$. Also, by the Multiplication Law for Order for the integers we see that $a_p c_p < b_p c_p$, and hence $ac < bc$.

(14) Because $\widetilde{0}_0 \neq \widetilde{1}_0$ we can conclude that $\widetilde{0} \neq \widetilde{1}$. □

Proof of (2). Suppose to the contrary that $g \in \mathbb{Z}[x]$ such that $f < g < f + \widetilde{1}$. Suppose that $\deg(f) < \deg(g) < \deg(f + \widetilde{1})$. We can notice that $\deg(f + \widetilde{1}) = \deg(f)$, so $\deg(f) < \deg(g)$ and $\deg(g) < \deg(f)$, which is a contradiction to Trichotomy Law for the integers. Hence, either $f \nless g$ or $g \nless f + \widetilde{1}$.

Now suppose that $\deg(f) = \deg(g) = \deg(f + \widetilde{1})$. Then there is the greatest

$$p \leq \deg(f) = \deg(g) = \deg(f + \widetilde{1})$$

such that

$$f_p < g_p < (f + \widetilde{1})_p = f_p + \widetilde{1}_p.$$

If $p = 0$ then $f_0 < g_0 < f_0 + 1$, which is a contradiction to Theorem 1.4.6. But if $p > 0$ then $f_p < g_p$ and $g_p < f_p$, which is a contradiction to the Trichotomy Law for the integers. Hence, either $f \nless g$ or $g \nless f + \widetilde{1}$.

Finally, suppose that either

$$\deg(f) < \deg(g) = \deg(f + \widetilde{1}) \text{ or } \deg(f) = \deg(g) < \deg(f + \widetilde{1}).$$

But we know that $\deg(f) = \deg(f + \widetilde{1})$, so this implies that either $\deg(f) < \deg(g)$ and $\deg(f) = \deg(g)$ or $\deg(f) = \deg(g)$ and $\deg(g) < \deg(f)$, which is a contradiction to the Trichotomy Law for the integers. Hence, either $f \nless g$ or $g \nless f + \widetilde{1}$. □

Proof of (3). Let $A = \{a \in \mathbb{Z}[x] \mid \deg(a) = 1\}$. Clearly, A is nonempty, and since $\deg(0) = 0$ we see that $a > \widetilde{0}$ for all $a \in A$. Suppose to the contrary that there is some $a' \in A$ such that $a' \leq a$ for all $a \in A$. Because $\deg(a) = 1$ for all $a \in A$, there is the greatest $p \in \mathbb{Z}^+$ such that $a'_p \leq a_p$ for all $a \in A$. Let $b = a' + [(-a'_p) + (-a'_p)]x$, and as a result $b_p = a'_p + [(-a'_p) + (-a'_p)]$. By repeated use of the Inverses and Identity Laws for Addition for the integers we obtain $b_p = -a'_p$. Then $\deg(b_p) = 1$, and hence $b \in A$. By Transitive Law for the integers, $-a'_p < 0 < a_p$ implies $-a'_p = b_p < a'_p$. From the Trichotomy Law for the integers we then deduce that $a' \nleq b$, which is a contradiction to the fact that $a' \leq a$ for all $a \in A$. Hence, $\mathbb{Z}[x]$ does not satisfy the Well-Ordering Principle. □

Lemma 1.4.9 (Not in the book). *Let $a, b \in \mathbb{Z}$. Suppose that $a < b$. Then there is some $k \in \mathbb{N}$ such that $a + k = b$.*

Exercise 1.4.8. Let $a \in \mathbb{Z}$.

(1) Let $G \subseteq \{x \in \mathbb{Z} \mid x \geq a\}$ be a set. Suppose that $a \in G$, and that if $g \in G$ then $g + 1 \in G$. Prove that $G = \{x \in \mathbb{Z} \mid x \geq a\}$. [Use Exercise 1.4.4.]

(2) Let $H \subseteq \{x \in \mathbb{Z} \mid x \leq a\}$ be a set. Suppose that $a \in H$, and that if $h \in H$ then $h + (-1) \in H$. Prove that $H = \{x \in \mathbb{Z} \mid x \leq a\}$. [Use Exercise 1.4.3.]

Proof of (1). Let $y \in \mathbb{Z}$, and suppose that $y \geq a$. If $y = a$, then clearly $y \in G$. Now suppose that $y \neq a$, so $y > a$. Then according to Lemma 1.4.9 we can choose some $k \in \mathbb{N}$ such that $y = a + k$.

Let $I = \{n \in \mathbb{N} \mid a + n \in G\}$. Clearly $I \subseteq \mathbb{N}$. Because $a \in G$ it follows that $a + 1 \in G$, and therefore $1 \in I$. Now suppose that $n \in I$, which means that $a + n \in G$. Then $(a + n) + 1 \in G$. By the Associative Law for Addition we have $a + (n + 1) \in G$. Hence $n + 1 \in I$, and using Part (c) of the Peano Postulates we deduce that $I = \mathbb{N}$. Hence, $y = a + k \in G$. □

Proof of (2). Let $y \in \mathbb{Z}$, and suppose that $y \leq a$. By Exercise 1.4.3 it follows that $-y \geq -a$, which means that either $-y = -a$ or $-y > -a$. Suppose that $-y = -a$. Then by the Identity Law for Multiplication we have $-(y \cdot 1) = -(a \cdot 1)$. By Lemma 1.4.5 (6) and the Cancellation Law for Multiplication we deduce that $y = a$. Hence, $y \in H$.

Now suppose that $-y > -a$. It follows from Lemma 1.4.9 that there is some $k \in \mathbb{N}$ such that $-y = (-a) + k$. Multiplying both sides of this equation by -1 we obtain $(-1)(-y) = (-1)[(-a) + k]$. According to Lemma 1.4.5 (6) and the Commutative Law for Multiplication we obtain $[-(-y)] \cdot 1 = [-(-a)] \cdot 1 + (-k) \cdot 1$, and by Lemma 1.4.5 (2) and the Identity Law for Multiplication we see that $y = a + (-k)$.

Let $I = \{n \in \mathbb{N} \mid a + (-n) \in H\}$. Clearly $I \subseteq H$. Because $a \in G$ it follows that $a + (-1) \in G$, and therefore $1 \in I$. Now suppose that $n \in I$. Then $a + (-n) \in H$, so $[a + (-n)] + (-1) \in H$. Using the Associative Law for Addition we get $a + [(-n) + (-1)]$, and using Part (3) of Lemma 1.4.5 we get $a + [-(n+1)] \in H$. Thus, $n + 1 \in I$, and by Part (c) of the Peano Postulates we deduce that $I = \mathbb{N}$. Hence, $y = a + (-k) \in H$. □

5. Constructing the Rational Numbers

Definition 1.5.1. *Let $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. The relation $\asymp$ on $\mathbb{Z} \times \mathbb{Z}^*$ is defined by $(x, y) \asymp (z, w)$ if and only if $xw = yz$, for all $(x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}^*$.*

Lemma 1.5.2. *The relation $\asymp$ is an equivalence relation.*

Definition 1.5.3. *The set of* ***rational numbers****, denoted $\mathbb{Q}$, is the set of equivalence classes of $\mathbb{Z} \times \mathbb{Z}^*$ with respect to the equivalence relation $\asymp$.*

The elements $\overline{0}, \overline{1} \in \mathbb{Q}$ are defined by $\overline{0} = [(0, 1)]$ and $\overline{1} = [(1, 1)]$. Let $\mathbb{Q}^* = \mathbb{Q} - \{\overline{0}\}$. The binary operations $+$ and $\cdot$ on $\mathbb{Q}$ are defined by

$$[(x, y)] + [(z, w)] = [(xw + yz, yw)]$$
$$[(x, y)] \cdot [(z, w)] = [(xz, yw)]$$

for all $[(x, y)], [(z, w)] \in \mathbb{Q}$. The unary operation $-$ on $\mathbb{Q}$ is defined by $-[(x, y)] = [(-x, y)]$ for all $[(x, y)] \in \mathbb{Q}$. The unary operation $^{-1}$ on $\mathbb{Q}^*$ is defined by $[(x, y)]^{-1} = [(y, x)]$ for all $[(x, y)] \in \mathbb{Q}^*$. The relation $<$ on $\mathbb{Q}$ is defined by $[(x, y)] < [(z, w)]$ if and only if either $xw < yz$ when $y > 0$ and $w > 0$ or when $y < 0$ and $w < 0$, and $xw > yz$ when $y > 0$ and $w < 0$ or when $y < 0$ and $w > 0$, for all $[(x, y)], [(z, w)] \in \mathbb{Q}$. The relation $\leq$ on $\mathbb{Q}$ is defined by $[(x, y)] \leq [(z, w)]$ if and only if $[(x, y)] < [(z, w)]$ or $[(x, y)] = [(z, w)]$, for all $[(x, y)], [(z, w)] \in \mathbb{Q}$.

Lemma 1.5.4. *The binary operations $+$ and $\cdot$, the unary operations $-$ and $^{-1}$, and the relation $<$, all on $\mathbb{Q}$, are well-defined.*

Theorem 1.5.5. *Let $r, s, t \in \mathbb{Q}$.*

(1) $(r + s) + t = r + (s + t)$ (Associative Law for Addition).

(2) $r + s = s + r$ (Commutative Law for Addition).

(3) $r + \overline{0} = r$ (Identity Law for Addition).

(4) $r + (-r) = \overline{0}$ (Inverses Law for Addition).

(5) $(rs)t = r(st)$ (Associative Law for Multiplication).

(6) $rs = sr$ (Commutative Law for Multiplication).

(7) $r \cdot \overline{1} = r$ (Identity Law for Multiplication).

(8) If $r \neq \overline{0}$, then $r \cdot r^{-1} = \overline{1}$ (Inverses Law for Multiplication).

(9) $r(s + t) = rs + rt$ (Distributive Law).

(10) Precisely one of $r < s$ or $r = s$ or $r > s$ holds (Trichotomy Law).

(11) If $r < s$ and $s < t$, then $r < t$ (Transitive Law).

(12) If $r < s$ then $r + t < s + t$ (Addition Law for Order).

(13) If $r < s$ and $t > \overline{0}$, then $rt < st$ (Multiplication Law for Order).

(14) $\overline{0} \neq \overline{1}$ (Non-Triviality).

Theorem 1.5.6. *Let $i : \mathbb{Z} \to \mathbb{Q}$ be defined by $i(x) = [(x, 1)]$ for all $x \in \mathbb{Z}$.*

(1) The function $i : \mathbb{Z} \to \mathbb{Q}$ is injective.

(2) $i(0) = \overline{0}$ and $i(1) = \overline{1}$.

(3) Let $x, y \in \mathbb{Z}$. Then

(a) $i(x + y) = i(x) + i(y)$;

(b) $i(-x) = -i(x)$;

(c) $i(xy) = i(x)i(y)$;

(d) $x < y$ if and only if $i(x) < i(y)$.

(4) For each $r \in \mathbb{Q}$ there are $x, y \in \mathbb{Z}$ such that $y \neq 0$ and $r = i(x)(i(y))^{-1}$.

Definition 1.5.7. *The binary operation $-$ on $\mathbb{Q}$ is defined by $r - s = r + (-s)$ for all $r, s \in \mathbb{Q}$. The binary operation $\div : \mathbb{Q} \times \mathbb{Q}^* \to \mathbb{Q}$ is defined by $r \div s = rs^{-1}$ for all $(r, s) \in \mathbb{Q} \times \mathbb{Q}^*$; we also let $0 \div s = 0 \cdot s^{-1} = 0$ for all $s \in \mathbb{Q}^*$. The number $r \div s$ is also denoted $\frac{r}{s}$.*

Lemma 1.5.8. *Let $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$.*

(1) $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

(2) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

(3) $-\frac{a}{b} = \frac{-a}{b}$.

(4) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

(5) If $a \neq 0$, then $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

(6) If $b > 0$ and $d > 0$, or if $b < 0$ and $d < 0$, then $\frac{a}{b} < \frac{c}{d}$ if and only if $ad < bc$; if $b > 0$ and $d < 0$, or if $b < 0$ and $d > 0$, then $\frac{a}{b} < \frac{c}{d}$ if and only if $ad > bc$.

Lemma 1.5.9 (Not in the book). *Let*

$$P = \{(x, y) \in \mathbb{Q} \mid \textit{there is either } x > 0 \textit{ and } y > 0 \textit{ or } x < 0 \textit{ and } y < 0\}.$$

Let $r, s \in \mathbb{Q}$.

(1) $r < s$ *if and only if* $(-r) + s \in P$.

(2) if $r, s \in P$*, then* $r + s \in P$ *and* $rs \in P$.

(3) if $r \in \mathbb{Q}^*$*, then precisely one of* $r \in P$ *or* $-r \in P$ *holds.*

Proof. Suppose that $r = [(x, y)]$ and that $s = [(z, w)]$.

(1) Suppose that $r < s$. Then $[(x, y)] < [(z, w)]$. We consider the following two cases.

Case 1. There is either $y > 0$ and $w > 0$ or $y < 0$ and $w < 0$. Without loss of generality, suppose that $y > 0$ and $w > 0$. Then $xw < yz$. Adding $-xw$ to both sides of this inequality we obtain

$$yz + (-xw) > xw + (-xw) = 0,$$

so $(-xw) + yz > 0$. Also, $y > 0$ and $w > 0$ imply $yw > 0$. Hence,

$$[([-xw] + yz, yw)] = (-r) + s \in P.$$

Case 2. There is either $y < 0$ and $w > 0$ or $y > 0$ and $w < 0$. A similar argument shows that $(-xw) + yz < 0$ and $yw < 0$, and hence

$$[([-xw] + yz, yw)] = (-r) + s \in P.$$

Now suppose that $(-r) + s \in P$, which means that $[([-xw] + yz, yw)] \in P$. From the definition of P this implies the following two cases.

Case 1. $(-xw)+yz > 0$ and $yw > 0$. Adding xw to the inequality $(-xw)+yz > 0$ and doing some rearranging we obtain $xw < yz$. Next suppose to the contrary that either $y > 0$ and $w < 0$ or $y < 0$ and $w > 0$, or in other words there is either $y > 0$ and $-w > 0$ or $-y > 0$ and $w > 0$. Then

$$y(-w) = (-y)w = -yw > 0,$$

so $yw < 0$, which is a contradiction to hypothesis on yw. Hence either $y > 0$ and $w > 0$ or $y < 0$ and $w < 0$. By Definition 1.5.3 we can conclude that $[(x, y)] = r < s = [(z, w)]$.

Case 2. $(-xw) + yz < 0$ and $yw < 0$. A similar argument shows that $r < s$.

(2) Suppose that $r, s \in P$, which means that $[(x, y)] \in P$ and $[(z, w)] \in P$. We consider the following four cases.

Case 1. $x > 0$, $y > 0$, $z > 0$, and $w > 0$. Then $xw > 0$, $yz > 0$, $xz > 0$, and $yw > 0$, and as a result $xw+yz > 0$. Hence, $r+s = [(xw+yz, yw)] \in P$ and $rs = [(xz, yw)] \in P$.

Case 2. $x < 0$, $y < 0$, $z < 0$, and $w < 0$. Then $-x > 0$, $-y > 0$, $-z > 0$, and $-w > 0$. Because $(-a)(-b) = ab$ for all $a, b \in \mathbb{Z}$ this case is similar to the previous case. Hence, $r + s \in P$ and $rs \in P$.

Case 3. $x > 0, y > 0, z < 0$, and $w < 0$. Then $xw < 0, yz < 0, xz < 0$ and $yw < 0$. It then follows that $xw+yz < 0$. Hence, $r+s = [(xw+yz, yw)] \in P$ and $rs = [(xz, yw)] \in P$.

Case 4. $x < 0$, $y < 0$, $z > 0$, and $w > 0$. A similar argument shows that $r + s \in P$ and $rs \in P$.

(3) Suppose that $r \in \mathbb{Q}^*$, or in other words $r \in \mathbb{Q}$ and $r \neq 0$. Suppose that $r \notin P$. Then either $x > 0$ and $y < 0$ or $x < 0$ and $y > 0$. It then follows either $-x < 0$ and $y < 0$ or $-x > 0$ and $y > 0$. Hence, $[(-x, y)] = -r \in P$.

Now suppose to the contrary that $r \in P$ and $-r \in P$. Because $r \in P$ there is either $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$. Without loss of generality, suppose that $x > 0$ and $y > 0$. Because $-r \in P$ we consider the following two cases.

Case 1. $-x > 0$ and $y > 0$. Then $-x > 0$ implies $x < 0$, which is a contradiction to the fact that $x > 0$. Hence, $-r \notin P$.

Case 2. $-x < 0$ and $y < 0$. Then there is a contradiction to the fact that $y > 0$, and hence $-r \notin P$.

Thus, we can conclude that precisely one of $r \in P$ or $-r \in P$ holds. □

Lemma 1.5.10 (Not in the book). *Let $r, s \in \mathbb{Q}$. Then $(-r)+(-s) = -(r+s)$.*

Proof. By the Inverses Law for Addition we know that $(r+s)+[-(r+s)] = \overline{0}$. Adding $(-r)+(-s)$ to both sides of this equation we obtain

$$(r+s)+[-(r+s)]+(-r)+(-s) = (-r)+(-s).$$

Then by repeated use of the Associative, Commutative, Inverses, and Identity Laws for Addition we can conclude that $-(r+s) = (-r)+(-s)$. □

Exercise 1.5.1 (Used in Lemma 1.5.2). Complete the proof of Lemma 1.5.2. That is, prove that the relation $\asymp$ is reflexive and symmetric.

Proof. Let $(x, y), (z, w), (u, v) \in \mathbb{Z}\times\mathbb{Z}^*$. Suppose that $(x, y) \asymp (z, w)$ and $(z, w) \asymp (u, v)$. Then $xw = yz$ and $zv = wu$. It follows that $(xw)v = (yz)v$ and $y(zv) = y(wu)$, which implies that $(xv)w = (yz)v$ and $(yz)v = (yu)w$, and hence $(xv)w = (yu)w$. We know that $w \neq 0$, and therefore we deduce that $xv = yu$. It follows that $(x, y) \asymp (u, v)$. Therefore $\asymp$ is transitive. Since $xy = yx$, it follows that $(x, y) \asymp (x, y)$, and hence $\asymp$ is reflexive. Now to see that $\asymp$ is symmetric, suppose that $(x, y) \asymp (z, w)$. Then $xw = yz$. This implies that $yz = xw$, which implies that $zy = wx$. Hence, $(z, w) \asymp (x, y)$. □

Lemma 1.5.9 (Not in the book). *Let*

$$P = \{(x, y) \in \mathbb{Q} \mid \textit{there is either } x > 0 \textit{ and } y > 0 \textit{ or } x < 0 \textit{ and } y < 0\}.$$

Let $r, s \in \mathbb{Q}$.

(1) $r < s$ *if and only if* $(-r) + s \in P$.
(2) *if* $r, s \in P$, *then* $r + s \in P$ *and* $rs \in P$.
(3) *if* $r \in \mathbb{Q}^*$, *then precisely one of* $r \in P$ *or* $-r \in P$ *holds.*

Exercise 1.5.2 (Used in Lemma 1.5.4). Complete the proof of Lemma 1.5.4. That is, prove that the binary operation $+$, the unary operation $^{-1}$ and the relation $<$, all on $\mathbb{Q}$, are well-defined.

Proof. Let $(x, y), (z, w), (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$. Suppose that $[(x, y)] = [(a, b)]$ and that $[(z, w)] = [(c, d)]$.

By hypothesis we know that $(x, y) \asymp (a, b)$ and $(z, w) \asymp (c, d)$. Hence $xb = ya$ and $zd = wc$. By multiplying these two equations and doing some rearranging we obtain $(xz)(bd) = (yw)(ac)$, and this implies that $[(xz, yw)] = [(ac, bd)]$. Therefore $\cdot$ is well-defined. Also, from $xb = ya$ we deduce that $(-x)b = y(-a)$, and hence $[(-x, y)] = [(-a, b)]$. Therefore $-$ is well-defined.

Multiplying the equation $xb = ya$ by wd we get $(xb)(wd) = (ya)(wd)$, and multiplying the equation $zd = wc$ by yb we get $(zd)(yb) = (wc)(yb)$. By adding these two equations we obtain $(xb)(wd) + (zd)(yb) = (ya)(wd) + (wc)(yb)$, and doing some rearranging we have $(xw + yz)(bd) = (ad + bc)(yw)$, which implies that $[(xw + yz, yw)] = [(ad + bc, bd)]$. Therefore $+$ is well-defined. From $xb = ya$ it follows that $ya = xb$, so $[(y, x)] = [(b, a)]$. Hence, $^{-1}$ is well-defined.

To see that $<$ is well-defined, suppose that $[(x, y)] < [(z, w)]$. From Part (2) of Lemma 1.5.9 it follows that $[(-x, y)] + [(z, w)] \in P$, so $[([-xw] + yz, yw)] \in P$. Then there is either $(-xw) + yz > 0$ and $yw > 0$ or $(-xw) + yz < 0$ and $yw < 0$. Without loss of generality, suppose that $(-xw) + yz > 0$ and $yw > 0$. Adding xw to both sides of the inequality $(-xw) + yz > 0$ we get

$$xw + (-xw) + yz = 0 + yz > xw + 0,$$

and as a result $xw < yz$. We know that $bd = yw > 0$, so multiplying both sides of the inequality $xw < yz$ by bd and doing some rearranging we obtain $(xb)(wd) < (zd)(yb)$. Because $xb = ya$ and $zd = wc$ we have $(ya)(wd) < (wc)(yb)$. Doing some rearranging again we get $(ad)(yw) < (bc)(yw)$. We have $y \neq 0$ and $w \neq 0$, so canceling yields $ad < bc$, and hence $[(a, b)] < [(c, d)]$. □

Lemma 1.5.9 (Not in the book). *Let*

$$P = \{(x, y) \in \mathbb{Q} \mid \textit{there is either } x > 0 \textit{ and } y > 0 \textit{ or } x < 0 \textit{ and } y < 0\}.$$

Let $r, s \in \mathbb{Q}$.

(1) $r < s$ *if and only if* $(-r) + s \in P$.
(2) if $r, s \in P$, *then* $r + s \in P$ *and* $rs \in P$.
(3) if $r \in \mathbb{Q}^*$, *then precisely one of* $r \in P$ *or* $-r \in P$ *holds.*

Exercise 1.5.3 (Used in Theorem 1.5.5 and Theorem 1.5.6). Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^*$.

(1) Prove that $[(x, y)] = \overline{0}$ if and only if $x = 0$.
(2) Prove that $[(x, y)] = \overline{1}$ if and only if $x = y$.
(3) Prove that $\overline{0} < [(x, y)]$ if and only if $0 < xy$.

Proof of (1). Suppose that $[(x, y)] = \overline{0}$. Then,

$$\begin{aligned} [(x, y)] = \overline{0} &\iff [(x, y)] = [(0, 1)] \\ &\iff (x, y) \asymp (0, 1) \\ &\iff x \cdot 1 = y \cdot 0 \\ &\iff x = 0. \end{aligned}$$

□

Proof of (2). Suppose that $[(x, y)] = \overline{1}$. Then,

$$\begin{aligned} [(x, y)] = \overline{1} &\iff [(x, y)] = [(1, 1)] \\ &\iff (x, y) \asymp (1, 1) \\ &\iff x \cdot 1 = y \cdot 1 \\ &\iff x = y. \end{aligned}$$

□

Proof of (3). Suppose that $\overline{0} < [(x, y)]$. Using Part (1) of Lemma 1.5.9 we have

$$\begin{aligned} \overline{0} < [(x, y)] &\iff [(0, 1)] < [(x, y)] \\ &\iff (-[(0, 1)]) + [(x, y)] \in P \\ &\iff [(-0, 1)] + [(x, y)] \in P \\ &\iff [(0, 1)] + [(x, y)] \in P \\ &\iff [(0 \cdot y + x \cdot 1, 1 \cdot y)] \in P \\ &\iff [(y \cdot 0 + x \cdot 1, y \cdot 1)] \in P \\ &\iff [(0 + x, y)] \in P \\ &\iff [(x, y)] \in P. \end{aligned}$$

This implies that there is either $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$. If $x > 0$ and $y > 0$ then clearly $0 < xy$. Now suppose that $x < 0$ and $y < 0$. Then $-x > 0$ and $-y > 0$, and we can conclude that $0 < (-x)(-y) = -(-xy) = xy$. This process can be done backwards, and hence $\overline{0} < [(x, y)]$ if and only if $0 < xy$. □

Lemma 1.5.9 (Not in the book). *Let*

$$P = \{(x, y) \in \mathbb{Q} \mid \textit{there is either } x > 0 \textit{ and } y > 0 \textit{ or } x < 0 \textit{ and } y < 0\}.$$

Let $r, s \in \mathbb{Q}$.

(1) $r < s$ if and only if $(-r) + s \in P$.
(2) if $r, s \in P$, then $r + s \in P$ and $rs \in P$.
(3) if $r \in \mathbb{Q}^*$, then precisely one of $r \in P$ or $-r \in P$ holds.

Lemma 1.5.10 (Not in the book). *Let $r, s \in \mathbb{Q}$. Then $(-r) + (-s) = -(r + s)$.*

Exercise 1.5.4 (Used in Theorem 1.5.5). Prove Theorem 1.5.5 (1) (2) (3) (5) (6) (8) (9) (11) (12) (14).

Proof. Suppose that $r = [(x, y)]$, that $s = [(z, w)]$ and that $t = [(u, v)]$ for some $x, z, u \in \mathbb{Z}$ and $y, w, v \in \mathbb{Z}^*$.

(1) We have

$$\begin{aligned}
(r + s) + t &= ([(x, y)] + [(z, w)]) + [(u, v)] \\
&= [(xw + yz, yw)] + [(u, v)] \\
&= [((xw + yz)v + (yw)u, (yw)v)] \\
&= [((xw)v + (yz)v + (yw)u, (yw)v) \\
&= [(x(wv) + y(zv) + y(wu), y(wv))] \\
&= [(x(wv) + y(zv + wu), y(wv))] \\
&= [(x, y)] + [(zv + wu, wv)] \\
&= [(x, y)] + ([(z, w)] + [(u, v)]) \\
&= r + (s + t).
\end{aligned}$$

(2) We have

$$\begin{aligned}
r + s &= [(x, y)] + [(z, w)] \\
&= [(xw + yz, yw)] = [(yz + xw, yw)] \\
&= [(zy + wx, wy)] = s + r.
\end{aligned}$$

(3) We have

$$\begin{aligned}
r + \overline{0} &= [(x, y)] + [(0, 1)] \\
&= [(x \cdot 1 + y \cdot 0, y \cdot 1)] = [(x + 0, y)] \\
&= [(x, y)] = r.
\end{aligned}$$

(5) We have

$$\begin{aligned}
(rs)t &= ([(x, y)] \cdot [(z, w)]) \cdot [(u, v)] \\
&= [(xz, yw)] \cdot [(u, v)] = [((xz)u, (yw)v)] \\
&= [(x(zu), y(wv))] = [(x, y)] \cdot [(zu, wv)] \\
&= [(x, y)] \cdot ([z, w] \cdot [(u, v)]) = r(st).
\end{aligned}$$

(6) We have

$$\begin{aligned}
rs &= [(x, y)] \cdot [(z, w)] \\
&= [(xz, yw)] \cdot [(zx, wy)] \\
&= [(z, w)] \cdot [(x, y)] = sr.
\end{aligned}$$

(8) Suppose that $r \neq \overline{0}$, which means that $r \in \mathbb{Q}^*$. Then,

$$\begin{aligned}
r \cdot r^{-1} &= [(x, y)] \cdot [(x, y)]^{-1} = [(x, y)] \cdot [(y, x)] \\
&= [(xy, yx)] = [(xy, xy)] = \overline{1},
\end{aligned}$$

where the last equality holds by Exercise 1.5.3 (2).

(9) Using Exercise 1.5.3 (2) we note that $[(y, y)] = \overline{1}$. By Part (7) of this theorem we know that $r(s + t) = r(s + t) \cdot \overline{1}$. Then,

$$\begin{aligned}
r(s + t) &= r(s + t) \cdot \overline{1} \\
&= [(x, y)] \cdot ([(z, w)] + [(u, v)]) \cdot [(y, y)] \\
&= [(x, y)] \cdot [(zv + wu, wv)] \cdot [(y, y)] \\
&= [(x(zv + wu), y(wv))] \cdot [(y, y)] \\
&= [(x(zv + wu)y, y(wv)y)] \\
&= [([x(zv) + x(wu)]y, y(wv)y)] \\
&= [(x(zv)y + x(wu)y, y(wv)y)] \\
&= [(xzvy + xwuy, ywvy)] \\
&= [(xzyv + ywxu, ywyv)] \\
&= [([xz][yv] + [yw][xu], [yw][yv])] \\
&= [(xz, yw)] + [(xu, yv)] \\
&= rs + rt.
\end{aligned}$$

(11) Suppose that $r < s$ and $s < t$. According to Part (1) of Lemma 1.5.9 we see that $(-r) + s \in P$ and $(-s) + t \in P$, so using Part (2) of Lemma 1.5.9 we deduce that $(-r) + s + (-s) + t \in P$. Then by repeated use of the Associative, Inverses, and Identity Laws for Addition we obtain $(-r) + t \in P$. Hence, $r < t$.

(12) Suppose that $r < s$. By Part (1) of Lemma 1.5.9 we know that $(-r)+s \in P$, and using the Identity and Inverses Laws for Addition we observe that

$$(-r) + s = (-r) + s + \overline{0} = (-r) + s + t + (-t) \in P.$$

By repeated use of the Associative and Commutative for Addition we obtain

$$([-r] + [-t]) + (s + t) \in P.$$

By Lemma 1.5.10 we see that $(-r) + (-t) = -(r + t)$. Then $[-(r + t)] + (s + t) \in P$, and hence $r + t < s + t$.

(14) Suppose to the contrary that $\overline{0} = \overline{1}$. Then $[(0, 1)] = [(1, 1)]$, which means that $(0, 1) \asymp (1, 1)$. But then $0 \cdot 1 = 1 \cdot 1$, and by the Identity Law for Multiplication it follows that $0 = 1$, which contradicts Non-Triviality for integer numbers. Hence, $\overline{0} \neq \overline{1}$. □

Exercise 1.5.5 (Used in Theorem 1.5.6). Prove Theorem 1.5.6 (1) (2) (3).

Proof.

(1) Let $a, b \in \mathbb{Z}$, and suppose that $i(a) = i(b)$. From the definition of $i : \mathbb{Z} \to \mathbb{Q}$, it follows that $[(a, 1)] = [(b, 1)]$, which means that $(a, 1) \asymp (b, 1)$. Then $a \cdot 1 = 1 \cdot b$, and hence $a = b$.

(2) By the definition of $i : \mathbb{Z} \to \mathbb{Q}$ we have $i(0) = [(0, 1)]$ and $i(1) = [(1, 1)]$, and from Definition 1.5.3 we obtain $i(0) = \overline{0}$ and $i(1) = \overline{1}$, as required.

(3 a) We have

$$\begin{aligned} i(x + y) &= [(x + y, 1)] = [(x \cdot 1 + 1 \cdot y, 1 \cdot 1)] \\ &= [(x, 1)] + [(y, 1)] = i(x) + i(y). \end{aligned}$$

(3 b) We have

$$i(-x) = [(-x, 1)] = -[(x, 1)] = -i(x).$$

(3 c) We have

$$i(xy) = [(xy, 1)] = [(xy, 1 \cdot 1)] = [(x, 1)] \cdot [(y, 1)] = i(x)i(y).$$

(3 d) Suppose that $x < y$. From Lemma 1.4.5 (9) we know that $1 > 0$, so $x \cdot 1 < y \cdot 1$. Then $x \cdot 1 < 1 \cdot y$, which means that $[(x, 1)] < [(y, 1)]$, or in other words $i(x) < i(y)$. This process can be done backwards, and hence $x < y$ if and only if $i(x) < i(y)$. □

Exercise 1.5.6 (Used in Exercise 1.6.2, Theorem 1.7.6 and Exercise 1.7.3). Let $r, s, p, q \in \mathbb{Q}$.

(1) Prove that $-1 < 0 < 1$.
(2) Prove that if $r < s$ then $-s < -r$.
(3) Prove that $r \cdot 0 = 0$.
(4) Prove that if $r > 0$ and $s > 0$, then $r + s > 0$ and $rs > 0$.
(5) Prove that if $r > 0$, then $\frac{1}{r} > 0$.
(6) Prove that if $0 < r < s$, then $\frac{1}{s} < \frac{1}{r}$.
(7) Prove that if $0 < r < p$ and $0 < s < q$, then $rs < pq$.

Proof of (1). From Lemma 1.4.5 (9) we know that $0 < 1$ for $0, 1 \in \mathbb{Z}$. Adding -1 to this inequality we obtain $-1 < 1 + (-1) = 0$, so $-1 < 0 < 1$ for $-1, 0, 1 \in \mathbb{Z}$. By Theorem 1.5.6 (3 d) it follows that $i(-1) < i(0) < i(1)$. Because of Theorem 1.5.6 (3 b) we see that $i(-1) = -i(1)$, and hence by Theorem 1.5.6 (2) we deduce that $-1 < 0 < 1$. □

Proof of (2). Suppose that $r < s$. By the Addition Law for Order we obtain

$$r + [(-r) + (-s)] < s + [(-r) + (-s)].$$

By repeated use of the Associative and Commutative Laws for Addition we deduce that

$$(-s) + [r + (-r)] < (-r) + [s + (-s)].$$

Because of the Inverses Law for Addition we see that $r + (-r) = 0$ and $s + (-s) = 0$, so $(-s) + 0 < (-r) + 0$, and hence by the Identity Law for Addition we can conclude that $-s < -r$. □

Proof of (3). Let $r = \frac{x}{y}$ for $x, y \in \mathbb{Z}$. Then $r \cdot 0 = \frac{x}{y} \cdot \frac{0}{1}$. By Lemma 1.5.8 (4) we obtain

$$\frac{x}{y} \cdot \frac{0}{1} = \frac{x \cdot 0}{y \cdot 1} = \frac{0}{y},$$

and from Definition 1.5.7 we see that $\frac{0}{y} = 0$. Hence, $r \cdot 0 = 0$.

□

Proof of (4). Suppose that $r > 0$ and $s > 0$. By the Addition Law for Order we obtain $r + s > 0 + s$. Using the Commutative and Identity we observe that $0 + s = s + 0 = s$, so $r + s > s$. By hypothesis on s and the Transitive Law we deduce that $r + s > 0$.

Now using the Multiplication Law for Order we get $rs > 0 \cdot s$. From Part (3) of this exercise and the Commutative Law for Multiplication we see that $0 \cdot s = s \cdot 0 = 0$, and hence $rs > 0$. □

Proof of (5). Suppose that $r > 0$. By Part (1) of this exercise we know that $0 < 1$. From the Multiplication Law for Order it follows that $0 \cdot r < 1 \cdot r$. Because of the Commutative Law for Multiplication we see that $1 \cdot r = r \cdot 1$, so $0 \cdot r < r \cdot 1$. But then from hypothesis on r and the Lemma 1.5.8 (6) we deduce that $\frac{0}{r} < \frac{1}{r}$. Finally, by Definition 1.5.7 we observe that $\frac{0}{r} = 0$, and hence $\frac{1}{r} > 0$. □

Proof of (6). Suppose that $0 < r < s$. From the Transitive Law we see that $s > 0$. By Part (5) of this exercise we deduce that $r^{-1} > 0$ and $s^{-1} > 0$. By repeated use of the Multiplication Law for Order we obtain $rr^{-1}s^{-1} < sr^{-1}s^{-1}$. From the Commutative Law for Multiplication we observe that $sr^{-1} = r^{-1}s$, so using the Associative and Inverses Laws for Multiplication we get $1 \cdot s^{-1} < r^{-1} \cdot 1$. Finally, by the Commutative and Identity Laws for Multiplication we can conclude that $\frac{1}{s} < \frac{1}{r}$. □

Proof of (7). Suppose that $0 < r < p$ and $0 < s < q$. We note that $p > 0$ because of the Transitive Law. Now we obtain $rs < ps$ and $sp < qp$ according to the Multiplication Law for Order. From the Commutative Law for Multiplication we deduce that $ps < pq$. But then $rs < ps < pq$, and hence by the Transitive Law we can conclude that $rs < pq$. □

Exercise 1.5.7.

(1) Prove that $1 < 2$.

(2) Let $s, t \in \mathbb{Q}$. Suppose that $s < t$. Prove that $\frac{s+t}{2} \in \mathbb{Q}$, and that $s < \frac{s+t}{2} < t$.

Proof of (1). By Exercise 1.5.6 (1) we have $0 < 1$. Because of the Addition Law for Order we obtain $0 + 1 < 1 + 1 = 2$. Using the Commutative and Identity Laws for Addition we see that $0 + 1 = 1 + 0 = 1$, and hence $1 < 2$. □

Proof of (2). By Exercise 1.5.6 (1) and Part (1) of this exercise we know that $0 < 1 < 2$, so using the Transitive Law we deduce that $2 > 0$, and as a result $2 \in \mathbb{Q}^*$. Hence, $\frac{s+t}{2} \in \mathbb{Q}$.

It follows from Exercise 1.5.6 (5) that $2^{-1} > 0$, and from the Multiplication Law for Order we can conclude that $s \cdot 2^{-1} < t \cdot 2^{-1}$.

From the Addition Law for Order we get $s \cdot 2^{-1} + s \cdot 2^{-1} < t \cdot 2^{-1} + s \cdot 2^{-1}$. Because of the Identity Law for Multiplication we observe that $s \cdot 2^{-1} + s \cdot 2^{-1} = (s \cdot 2^{-1}) \cdot 1 + (s \cdot 2^{-1}) \cdot 1$. Also, from the Associative Law for Addition and the Commutative Law for Multiplication we observe that $t \cdot 2^{-1} + s \cdot 2^{-1} = 2^{-1} \cdot s + 2^{-1} \cdot t$, so using the Distributive Law we deduce that $s \cdot 2^{-1}(1+1) = s \cdot 2^{-1} \cdot 2 < 2^{-1}(s+t) = (s+t)2^{-1}$. From the Commutative and Inverses Laws for Multiplication it follows that $2^{-1} \cdot 2 = 2 \cdot 2^{-1} = 1$. By the Associative and Identity Laws for Multiplication it follows that $s \cdot 2^{-1} \cdot 2 = s \cdot (2^{-1} \cdot 2) = s \cdot 1 = s$. Hence, $s < \frac{s+t}{2}$.

By the Addition Law for Order we obtain $s \cdot 2^{-1} + t \cdot 2^{-1} < t \cdot 2^{-1} + t \cdot 2^{-1}$. From the Commutative Law for Multiplication and the Distributive Law we deduce that $(s+t)2^{-1} < t(1+1)2^{-1} = t \cdot 2 \cdot 2^{-1}$. We already know that $2 \cdot 2^{-1} = 1$, so using the Associative and Identity Laws for Multiplication we get $t \cdot 2 \cdot 2^{-1} = t(2 \cdot 2^{-1}) = t \cdot 1 = t$. Hence, $s < \frac{s+t}{2} < t$. □

Exercise 1.5.8. Let $r \in \mathbb{Q}$. Suppose that $r > 0$.

(1) Prove that if $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ such that $b \neq 0$, then either $a > 0$ and $b > 0$, or $a < 0$ and $b < 0$.
(2) Prove that $r = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ such that $m > 0$ and $n > 0$.

Proof of (1). Suppose that $r = \frac{a}{b}$ for some $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Because of Exercise 1.5.6 (1) we know that $1 > 0$, and we note that $\frac{0}{1} = 0$ according to Definition 1.5.7. Taking into account Lemma 1.5.8 (6) we consider the following two cases.

Case 1. $b < 0$. Then $\frac{0}{1} < \frac{a}{b}$ implies $0 \cdot b > 1 \cdot a$, and hence $a < 0$.
Case 2. $b > 0$. Then $\frac{0}{1} < \frac{a}{b}$ implies $0 \cdot b < 1 \cdot a$, and hence $a > 0$.

□

Proof of (2). From Definition 1.5.7 and Theorem 1.5.6 (4) we observe that there is $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ such that $r = \frac{a}{b}$. By Part (1) of this exercise we deduce that a and b are either both positive or both negative. If a and b are both positive, then we will clearly reach the desired result. Now suppose that $a < 0$ and $b < 0$. Let $m = -a$ and $n = -b$, which means that m and n are both positive. Using Exercise 1.5.3 (2) we can notice that $1 = \frac{-1}{-1}$. Then,

$$r = \frac{a}{b} = \frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{-1}{-1} = \frac{a(-1)}{b(-1)} = \frac{-a}{-b} = \frac{m}{n},$$

as required.

□

Exercise 1.5.9 (Used in Lemma 1.6.9 and Exercise 1.6.2). Let $r, s \in \mathbb{Q}$.

(1) Suppose that $r > 0$ and $s > 0$. Prove that there is some $n \in \mathbb{N}$ such that $s < nr$.

[Use Exercise 1.5.6, 1.5.8, and either Exercise 1.3.8 or 1.4.4.]

(2) Suppose that $r > 0$. Prove that there is some $m \in \mathbb{N}$ such that $\frac{1}{m} < r$.

(3) For each $x \in \mathbb{Q}$, let x^2 denote $x \cdot x$. Suppose that $r > 0$ and $s > 0$. Prove that if $r^2 < s$, then there is some $k \in \mathbb{N}$ such that $\left(r + \frac{1}{k}\right)^2 < s$.

Proof of (1). Using Exercise 1.5.8 (2) we then deduce that $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}^+ - \{0\}$. Then $ad > 0$ and $bc > 0$ because of Exercise 1.5.6 (4), and then $ad \geq 1$ and $bc \geq 1$ because of Exercise 1.3.8. This means that $bc \in \mathbb{N}$ according to Exercise 1.4.4.

By Exercise 1.5.6 (1) we know that $0 < 1$, so we obtain $bc < bc + 1$. Let $n = bc + 1$. Then $n \in \mathbb{N}$ and $bc < n$. If $ad = 1$ then $bc < n \cdot 1 = n(ad)$, and by Lemma 1.5.8 (1) we have $s = \frac{c}{d} < n \cdot \frac{a}{b} = nr$, as required. Now suppose that $ad > 1$. From Exercise 1.5.6 (7) it then follows that $1 \cdot bc < ad(bc+1)$, so $bc < n(ad)$. Using Lemma 1.5.8 (1) we see that $\frac{c}{d} < n \cdot \frac{a}{b}$, and hence $s < nr$. □

Proof of (2). Because of Exercise 1.5.8 (2) we have $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ such that $a > 0$ and $b > 0$. We know that $a, b \in \mathbb{Q}$, so using Part (1) of this exercise we can find some $m \in \mathbb{N}$ such that $b < ma$. Then $1 \cdot b < ma$, and hence by Lemma 1.5.8 (1) we deduce that $\frac{1}{m} < \frac{a}{b} = r$. □

Proof of (3). Suppose that $r^2 < s$. Then $s - r^2 > 0$. From Exercise 1.5.6 (1) we know that $1 > 0$. By repeated use of Exercise 1.5.6 (4) we see that $r + r + 1 = 2r + 1 > 0$. It then follows from Exercise 1.5.6 (5) that $\frac{1}{2r+1} > 0$, and hence by Exercise 1.5.6 (4) we deduce that $\frac{s-r^2}{2r+1} > 0$.

By Part (2) of this exercise we can find some $k \in \mathbb{N}$ such that $\frac{1}{k} < \frac{s-r^2}{2r+1}$. We note that $k \in \mathbb{Z}$ and $\frac{1}{k} > 0$ according to Exercise 1.4.4 and Exercise 1.5.6 (5). Because of Lemma 1.5.8 (6) we have $1 \cdot (2r+1) = 2r + 1 < k(s - r^2)$. Multiplying both sides of this inequality by $\frac{1}{k}$ it follows that

$$\frac{1}{k}(2r+1) = 2r\frac{1}{k} + \frac{1}{k} < s - r^2 = \frac{1}{k}k(s - r^2).$$

By Exercise 1.3.8 we observe that $k \geq 1$, so $k^2 \geq k$. Using Exercise 1.5.6 (6) we get $\frac{1}{k^2} = \left(\frac{1}{k}\right)^2 \leq \frac{1}{k}$. Then

$$2r\frac{1}{k} + \left(\frac{1}{k}\right)^2 \leq 2r\frac{1}{k} + \frac{1}{k} < s - r^2,$$

and then $2r\frac{1}{k} + \left(\frac{1}{k}\right)^2 < s - r^2$. Finally, adding r^2 to this inequality and doing some rearranging we obtain

$$r^2 + 2\frac{1}{k}r + \left(\frac{1}{k}\right)^2 = \left(r + \frac{1}{k}\right)^2 < s,$$

as required. □

6. Dedekind Cuts

Definition 1.6.1. *Let $A \subseteq \mathbb{Q}$ be a set. The set A is a* ***Dedekind cut*** *if the following three properties hold.*

(a) $A \neq \emptyset$ *and* $A \neq \mathbb{Q}$.
(b) *Let* $x \in A$. *If* $y \in \mathbb{Q}$ *and* $y \geq x$, *then* $y \in A$.
(c) *Let* $x \in A$. *Then there is some* $y \in A$ *such that* $y < x$.

Lemma 1.6.2. *Let* $r \in \mathbb{Q}$. *Then the set*

$$\{x \in \mathbb{Q} \mid x > r\}$$

is a Dedekind cut.

Definition 1.6.4. *Let* $r \in \mathbb{Q}$. *The* ***rational cut*** *at* r, *denoted* D_r, *is the Dedekind cut*

$$D_r = \{x \in \mathbb{Q} \mid x > r\}.$$

An ***irrational cut*** *is a Dedekind cut that is not a rational cut at any rational number.*

Lemma 1.6.5. *Let* $A \subseteq \mathbb{Q}$ *be a Dedekind cut.*

(1) $\mathbb{Q} - A = \{x \in \mathbb{Q} \mid x < a$ *for all* $a \in A\}$.
(2) *Let* $x \in \mathbb{Q} - A$. *If* $y \in \mathbb{Q}$ *and* $y \leq x$, *then* $y \in \mathbb{Q} - A$.

Lemma 1.6.6. *Let* $A, B \subseteq \mathbb{Q}$ *be Dedekind cuts. Then precisely one of* $A \subsetneq B$ *or* $A = B$ *or* $B \subsetneq A$ *holds.*

Lemma 1.6.7. *Let* A *be a non-empty family of subsets of* $\mathbb{Q}$. *Suppose that* X *is a Dedekind cut for all* $X \in A$. *If* $\bigcup_{X \in A} X \neq \mathbb{Q}$, *then* $\bigcup_{X \in A} X$ *is a Dedekind cut.*

Lemma 1.6.8. *Let* $A, B \subseteq \mathbb{Q}$ *be Dedekind cuts.*

(1) *The set*

$$\{r \in \mathbb{Q} \mid r = a + b \text{ for some } a \in A \text{ and } b \in B\}$$

is a Dedekind cut.

(2) *The set*

$$\{r \in \mathbb{Q} \mid -r < c \text{ for some } c \in \mathbb{Q} - A\}$$

is a Dedekind cut.

(3) *Suppose that* $0 \in \mathbb{Q} - A$ *and* $0 \in \mathbb{Q} - B$. *The set*

$$\{r \in \mathbb{Q} \mid r = ab \text{ for some } a \in A \text{ and } b \in B\}$$

is a Dedekind cut.

(4) *Suppose that there is some* $q \in \mathbb{Q} - A$ *such that* $q > 0$. *The set*

$$\{r \in \mathbb{Q} \mid r > 0 \text{ and } \frac{1}{r} < c \text{ for some } c \in \mathbb{Q} - A\}$$

is a Dedekind cut.

Lemma 1.6.9. *Let* $A \subseteq \mathbb{Q}$ *be a Dedekind cut. Let* $y \in \mathbb{Q}$.

(1) *Suppose that* $y > 0$. *Then there are* $u \in A$ *and* $v \in \mathbb{Q} - A$ *such that* $y = u - v$, *and* $v < e$ *for some* $e \in \mathbb{Q} - A$.
(2) *Suppose that* $y > 1$, *and that there is some* $q \in \mathbb{Q} - A$ *such that* $q > 0$. *Then there are* $r \in A$ *and* $s \in \mathbb{Q} - A$ *such that* $s > 0$, *and* $y > \frac{r}{s}$, *and* $s < g$ *for some* $g \in \mathbb{Q} - A$.

Exercise 1.6.1. Let $A, B \subseteq \mathbb{Q}$ be Dedekind cuts. Suppose that $A \subsetneq B$. Prove that $B - A$ has more than one element. If you are familiar with the cardinality of sets, prove that $B - A$ is countably infinite.

Proof. Because of Part (a) of the definition of Dedekind cuts we see that $A \neq \emptyset$ and $B \neq \emptyset$, so since $A \neq B$ we then deduce that $B - A \neq \emptyset$. There is some $x \in \mathbb{Q}$ such that $x \in B$ and $x \notin A$. By Part (c) of the definition of Dedekind cuts we can find some $y \in B$ such that $y < x$. Suppose to the contrary that $y \notin B - A$. Then $y \in A$. Because of Part (b) of the definition of Dedekind cuts, $x > y$ implies $x \in A$, which is a contradiction to the fact that $x \in B - A$. Hence $y \in B - A$, and since $x, y \in B - A$ we can conclude that $B - A$ has more than one element. □

Exercise 1.6.2. Let

$$T = \{x \in \mathbb{Q} \mid x > 0 \text{ and } x^2 > 2\}.$$

(1) Prove that T is a Dedekind cut.
(2) Prove that if $T = D_r$ for some $r \in \mathbb{Q}$, then $r^2 = 2$.
[Use Exercise 1.5.6, Exercise 1.5.7 and Exercise 1.5.9 (3).]

Proof of (1). Clearly $T \subseteq \mathbb{Q}$. Now we will show that T satisfies the three parts of the definition of Dedekind cuts.

(a) We note that $0, 1 \in \mathbb{Q}$. By Exercise 1.5.7 (1) we have $1 < 2$, which means that $1 \notin T$, and hence $T \neq \mathbb{Q}$. To see that $T \neq \emptyset$, we will prove that $2 \in T$. We have $2^2 = (1+1)^2 = 1+2+1 = 2+(1+1) = 2+2$. From Exercise 1.5.6 (1) we know that $0 < 1$, so $0 < 2$. Then $2+2 > 2+0 = 2$, and as a result $2^2 > 2$. Hence, $2 \in T$.

(b) Let $x \in T$, and let $y \in \mathbb{Q}$. Suppose that $y \geq x$. By hypothesis on x we know that $x > 0$ and $x^2 > 2$. Then $y > 0$ and $y^2 \geq xy$. We also see that $2 < x^2 < xy$, and as a result we can conclude that $y^2 > 2$. Hence, $y \in T$.

(c) Let $x \in T$. Then $x > 0$ and $x^2 > 2$. Suppose to the contrary that $x \leq 1$. If $x = 1$ then using Exercise 1.5.7 (1) we get $x^2 = 1^2 = 1 < 2$, which is a contradiction. If $x < 1$ then from Exercise 1.5.6 (7) we obtain $x^2 < 1$, which is a contradiction again. Hence, $x > 1$.

Let $y = \frac{1}{2}x + 1$. By Exercise 1.5.7 (2) it follows that $2 < \frac{1}{2}x + 1 = \frac{2+x}{2} < x$, so $y < x$. We have

$$\left(\frac{1}{2}x + 1\right)^2 = \frac{1}{4}x^2 + x + 1.$$

By Exercise 1.5.6 (4) we deduce that $\frac{1}{4}x^2 > 0$. Because $x > 1$ we see that $x + 1 > 1 + 1 = 2$, or in other words $x + 1 - 2 > 0$. Using Exercise 1.5.6 (4) again, we get $\frac{1}{4}x^2 + (x + 1 - 2) > 0$. But then $\frac{1}{4}x^2 + x + 1 > 2$, and then $y^2 > 2$. Hence, $y \in T$. □

Proof of (2). Suppose that $T = D_r$ for some $r \in \mathbb{Q}$, and suppose to the contrary that $r^2 \neq 2$. There is either $r^2 < 2$ or $r^2 > 2$.

Case 1. $r^2 < 2$. Because of Exercise 1.5.9 (3) we can find some $k \in \mathbb{N}$ such that $\left(r + \frac{1}{k}\right)^2 < 2$. From Exercise 1.5.6 (5) it follows that $\frac{1}{k} > 0$. Then $r + \frac{1}{k} > r$, which means that $r + \frac{1}{k} \in D_r$. But then $r + \frac{1}{k} \in T$, and as a result $\left(r + \frac{1}{k}\right)^2 > 2$, which is a contradiction.

Case 2. $r^2 > 2$. Since $x > 0$ and $x > r$ for all $x \in T = D_r$, we deduce that $r > 0$, and then $r \in T$. But this implies that $r \in D_r$, which is a contradiction because $r \not> r$.

Because we have reached a contradiction in the both cases, we can conclude that $r^2 = 2$. □

Exercise 1.6.3 (Used in Lemma 1.6.8). Prove Lemma 1.6.8 (3).

Proof. Let

$$P = \{r \in \mathbb{Q} \mid r = ab \text{ for some } a \in A \text{ and } b \in B\}.$$

We will show that P satisfies the three parts of the definition of Dedekind cuts.

(a) Clearly $0 \notin P$, so $P \neq \mathbb{Q}$. We know that $A \neq \emptyset$ and $B \neq \emptyset$. Then there is some $a \in A$ and $b \in B$, and then $ab \in P$. Hence, $P \neq \emptyset$.

(b) Let $x \in A$, and let $y \in \mathbb{Q}$. Suppose that $y \geq x$. We know that $x = ab$ for some $a \in A$ and $b \in B$. Then $y = \left(\frac{ya}{x}\right) b$. Because $y \geq x$ and $x \neq 0$ we have $\frac{ya}{x} \geq a$, which means that $\frac{ya}{x} \in A$, and hence $y \in P$.

(c) Let $x \in P$. Applying Part (c) of the definition of Dedekind cuts to A, we see that there is some $a_\circ \in A$ such that $a_\circ < a$. Then $a_\circ b \in P$ and $a_\circ b < ab = x$, as required. □

Exercise 1.6.4 (Used in Lemma 1.7.4). Let $A \subseteq \mathbb{Q}$ be a Dedekind cut, and let $r \in \mathbb{Q}$.

(1) Prove that $A \subsetneq D_r$ if and only if there is some $q \in \mathbb{Q} - A$ such that $r < q$.

(2) Prove that $A \subseteq D_r$ if and only if $r \in \mathbb{Q} - A$ if and only if $r < a$ for all $a \in A$.

Proof of (1). Suppose that $A \subsetneq D_r$. Then there is some $q \in D_r$ such that $q \notin A$, which implies that $q \in \mathbb{Q} - A$ and $r < q$.

Now suppose that $r < q$ for some $q \in \mathbb{Q} - A$. This means that $q \in \mathbb{Q}$ and $q \notin A$. Then by the definition of D_r we deduce that $q \in D_r$, and as a result $D_r - A \neq \emptyset$. Hence $D_r \nsubseteq A$, and hence by Lemma 1.6.6 we conclude that $A \subsetneq D_r$. □

Proof of (2). Lemma 1.6.5 (1) implies that $r \in \mathbb{Q} - A$ if and only if $r < a$ for all $a \in A$. From the definition of D_r we see that $r \notin D_r$, and if $A \subseteq D_r$ then $r \in \mathbb{Q} - A$. If $r \in \mathbb{Q} - A$, or in other words $r < a$ for all $a \in A$, then using the definition of D_r again we obtain $a \in D_r$, which means that $A \subseteq D_r$. □

7. Constructing the Real Numbers

Definition 1.7.1. *The set of **real numbers**, denoted* $\mathbb{R}$*, is defined by*

$$\mathbb{R} = \{A \subseteq \mathbb{Q} \mid A \text{ is a Dedekind cut } \}.$$

Definition 1.7.2. *The relation* $<$ *on* $\mathbb{R}$ *is defined by* $A < B$ *if and only if* $A \supsetneq B$*, for all* $A, B \in \mathbb{R}$*. The relation* $\leq$ *on* $\mathbb{R}$ *is defined by* $A \leq B$ *if and only if* $A \supseteq B$*, for all* $A, B \in \mathbb{R}$*.*

Definition 1.7.3. *The binary operation* $+$ *on* $\mathbb{R}$ *is defined by*

$$A + B = \{r \in \mathbb{Q} \mid r = a + b \text{ for some } a \in A \text{ and } b \in B\}$$

for all $A, B \in \mathbb{R}$*. The unary operation* $-$ *on* $\mathbb{R}$ *is defined by*

$$-A = \{r \in \mathbb{Q} \mid -r < c \text{ for some } c \in \mathbb{Q} - A\}$$

for all $A \in \mathbb{R}$*.*

Lemma 1.7.4. *Let* $A \in \mathbb{R}$*, and let* $r \in \mathbb{Q}$*.*

(1) $A > D_r$ *if and only if there is some* $q \in \mathbb{Q} - A$ *such that* $q > r$*.*
(2) $A \geq D_r$ *if and only if* $r \in \mathbb{Q} - A$ *if and only if* $a > r$ *for all* $a \in A$*.*
(3) *If* $A < D_0$ *then* $-A \geq D_0$*.*

Definition 1.7.5. *The binary operation* $\cdot$ *on* $\mathbb{R}$ *is defined by*

$$A \cdot B = \begin{cases} \{r \in \mathbb{Q} \mid r = ab \text{ for some } a \in A \text{ and } b \in B\}, & \text{if } A \geq D_0 \text{ and } B \geq D_0 \\ -[(-A) \cdot B], & \text{if } A < D_0 \text{ and } B \geq D_0 \\ -[A \cdot (-B)], & \text{if } A \geq D_0 \text{ and } B < D_0 \\ (-A) \cdot (-B), & \text{if } A < D_0 \text{ and } B < D_0. \end{cases}$$

The unary operation $^{-1}$ *on* $\mathbb{R} - \{D_0\}$ *is defined by*

$$A^{-1} = \begin{cases} \{r \in \mathbb{Q} \mid r > 0 \text{ and } \frac{1}{r} < c \text{ for some } c \in \mathbb{Q} - A\}, & \text{if } A > D_0 \\ -(-A)^{-1}, & \text{if } A < D_0. \end{cases}$$

Theorem 1.7.6. *Let* $A, B, C \in \mathbb{R}$*.*

(1) $(A + B) + C = A + (B + C)$ *(Associative Law for Addition).*
(2) $A + B = B + A$ *(Commutative Law for Addition).*
(3) $A + D_0 = A$ *(Identity Law for Addition).*
(4) $A + (-A) = D_0$ *(Inverses Law for Addition).*
(5) $(AB)C = A(BC)$ *(Associative Law for Multiplication).*
(6) $AB = BA$ *(Commutative Law for Multiplication).*
(7) $A \cdot D_1 = A$ *(Identity Law for Multiplication).*
(8) *If* $A \neq D_0$*, then* $AA^{-1} = D_1$ *(Inverses Law for Multiplication).*
(9) $A(B + C) = AB + AC$ *(Distributive Law).*
(10) *Precisely one of* $A < B$ *or* $A = B$ *or* $A > B$ *holds (Trichotomy Law).*
(11) *If* $A < B$ *and* $B < C$*, then* $A < C$ *(Transitive Law).*
(12) *If* $A < B$ *then* $A + C < B + C$ *(Addition Law for Order).*
(13) *If* $A < B$ *and* $C > D_0$*, then* $AC < BC$ *(Multiplication Law for Order).*
(14) $D_0 < D_1$ *(Non-Triviality).*

Definition 1.7.7. *Let* $A \subseteq \mathbb{R}$ *be a set.*

(1) *The set* A *is **bounded above** if there is some* $M \in \mathbb{R}$ *such that* $X \leq M$ *for all* $X \in A$*. The number* M *is called an **upper bound** of* A*.*
(2) *The set* A *is **bounded below** if there is some* $P \in \mathbb{R}$ *such that* $X \geq P$ *for all* $X \in A$*. The number* P *is called a **lower bound** of* A*.*
(3) *The set* A *is **bounded** if it is bounded above and bounded below.*
(4) *Let* $M \in \mathbb{R}$*. The number* M *is a **least upper bound** (also called a **supremum**) of* A *if* M *is an upper bound of* A*, and if* $M \leq T$ *for all upper bounds* T *of* A*.*
(5) *Let* $P \in \mathbb{R}$*. The number* P *is a **greatest lower bound** (also called an **infimum**) of* A *if* P *is a lower bound of* A*, and if* $P \geq V$ *for all lower bounds* V *of* A*.*

Theorem 1.7.8 (Greatest Lower Bound Property). *Let* $A \subseteq \mathbb{R}$ *be a set. If* A *is non-empty and bounded below, then* A *has a greatest lower bound.*

Theorem 1.7.9 (Least Upper Bound Property). *Let* $A \subseteq \mathbb{R}$ *be a set. If* A *is nonempty and bounded above, then* A *has a least upper bound.*

Theorem 1.7.10. *Let* $i : \mathbb{Q} \to \mathbb{R}$ *be defined by* $i(r) = D_r$ *for all* $r \in \mathbb{R}$*.*

(1) *The function* $i : \mathbb{Q} \to \mathbb{R}$ *is injective.*
(2) $i(0) = D_0$ *and* $i(1) = D_1$*.*
(3) *Let* $r, s \in \mathbb{Q}$*. Then*
  (a) $i(r + s) = i(r) + i(s)$*;*
  (b) $i(-r) = -i(r)$*;*
  (c) $i(rs) = i(r)i(s)$*;*
  (d) *if* $r \neq 0$ *then* $i(r^{-1}) = [i(r)]^{-1}$*;*
  (e) $r < s$ *if and only if* $i(r) < i(s)$*.*

Exercise 1.7.1 (Used in Exercise 1.7.7). Let $r \in \mathbb{Q}$.

(1) Prove that $D_{-r} = -D_r$, using only Definition 1.6.4 and Definition 1.7.3.
(2) Prove that $D_{r^{-1}} = [D_r]^{-1}$, using only Definition 1.7.5 and Definition 1.7.3.

Proof of (1). Let $x \in \mathbb{Q}$. By the definition of D_{-r} we see that $-x < r$. Because $r \notin D_r$ we get $r \in \mathbb{Q} - D_r$, and by the definition of $-D_r$ we deduce that $x \in -D_r$. Hence, $D_{-r} \subseteq -D_r$. This process can be done backwards, and hence $D_{-r} = -D_r$. □

Proof of (2). We note that $r \neq 0$ because of the definition of $^{-1}$ on $\mathbb{R} - \{D_0\}$. Suppose that $D_r > D_0$. Let $x \in \mathbb{Q}$. From the definition of $D_{r^{-1}}$ we observe that $x > r^{-1} = \frac{1}{r}$. Since $D_r > D_0$, from Lemma 1.7.4 (2) we see that $0 \in \mathbb{Q} - D_0$ implies $r > 0$. Then $x > 0$ and $\frac{1}{x} < r$. Hence, $x \in [D_r]^{-1}$. Thus, $D_{r^{-1}} \subseteq [D_r]^{-1}$, and because this process can be done backwards we deduce that $D_{r^{-1}} = [D_r]^{-1}$. Since r was arbitrary, we can conclude that $D_{q^{-1}} = [D_q]^{-1}$ if $D_q > D_0$ for all $q \in \mathbb{Q}$.

Now suppose that $D_r < D_0$. By Lemma 1.7.4 (3) it follows that $-D_r > D_0$. From Part (1) of this exercise we know that $-D_q = D_{-q}$ for all $q \in \mathbb{Q}$, so $D_{-r} > D_0$. Then

$$D_{r^{-1}} = D_{-[-(r^{-1})]} = -D_{-(-r^{-1})} = -D_{(-r)^{-1}} = -[D_{-r}]^{-1} = -(-D_r)^{-1} = [D_r]^{-1},$$

as required. □

Exercise 1.7.2 (Used in Theorem 1.7.6). Let $A, B \in \mathbb{R}$. Suppose that $A > D_0$ and $B > D_0$. For this exercise, you may use only results prior to Theorem 1.7.6.

(1) Prove that $AB > D_0$.
(2) Prove that $A^{-1} > D_0$.

Proof of (1). Because $D_0 - A \neq \emptyset$ and $D_0 - B \neq \emptyset$, it follows from the definition of AB that $AB \neq D_0$. Now let $r \in AB$. Then $r = ab$ for some $a \in A$ and $b \in B$. Since $A > D_0$ and $B > D_0$, we deduce that $a > 0$ and $b > 0$. But then $r = ab > 0$. Hence $AB \subsetneq D_0$, or in other words $AB > D_0$. □

Proof of (2). We note that $A^{-1} \neq D_0$ by the definition of A^{-1}. Let $r \in A^{-1}$. Then $r > 0$, and as a result $r \in D_0$. Hence $A^{-1} \subsetneq D_0$, or in other words $A^{-1} > D_0$. □

Exercise 1.7.3 (Used in Theorem 1.7.6). Prove Theorem 1.7.6 (14). For this exercise, you may use only results prior to Theorem 1.7.6.

[Use Exercise 1.5.6 (1).]

Proof. We note that $D_0 \neq D_1$ because $1 \in D_0$ and $1 \notin D_1$. Let $x \in D_0$. Then $x > 1$. From Exercise 1.5.6 (1) we see that $x > 1 > 0$. Then $x > 0$, and as a result $x \in D_0$. Hence $D_1 \subsetneq D_0$, or in other words $D_0 < D_1$. □

Exercise 1.7.4 (Used in Theorem 1.7.6, Exercise 1.7.5 and Exercise 1.7.6). For this exercise, use only the properties of real numbers stated in Theorem 1.7.6 (1) (2) (3) (4) (10) (11) (12) (14); it is not necessary to use the definition of real numbers as Dedekind cuts. Let $A, B \in \mathbb{R}$.

(1) Prove that $A > D_0$ if and only if $-A < D_0$, and that $A < D_0$ if and only if $-A > D_0$.
(2) Prove that $-(-A) = A$.
(3) Prove that $-(A + B) = (-A) + (-B)$.
(4) Prove that if $A > D_0$ and $B > D_0$, then $A+B > D_0$, and that if $A < D_0$ and $B < D_0$, then $A + B < D_0$.
(5) Prove that $A = (-B) + (A + B) = B + [A + (-B)]$ and $-A = B + [-(B + A)]$.

Proof of (1). Suppose that $A > D_0$. Let $x \in D_0$. By the definition of D_0, we see that $-x < 0$. From Lemma 1.7.4 (2) it follows that $0 \in \mathbb{Q} - A$, and hence $x \in -A$, which means that $D_0 \subseteq -A$. Because $D_0 - A \neq \emptyset$ we can find some $c \in D_0$ such that $c \notin A$. Then $c \in \mathbb{Q} - A$ and $0 = -0 < c$, and as a result $0 \in -A$. But we know that $0 \notin D_0$, so $-A \neq D_0$, and hence $-A < D_0$.

Now we will prove that if $-A < D_0$, then $A > D_0$. Taking the contrapositive, suppose that $A \leq D_0$. If $A < D_0$ then from Lemma 1.7.4 (3) we deduce that $-A \geq D_0$. Suppose further that $A = D_0$. Then,

$$\begin{aligned} -A &= \{r \in \mathbb{Q} \mid -r < c \text{ for some } c \in \mathbb{Q} - A\} \\ &= \{r \in \mathbb{Q} \mid -r < 0 \text{ where } 0 \in \mathbb{Q} - D_0 = \mathbb{Q} - A\} \\ &= -D_0. \end{aligned}$$

Using Exercise 1.7.1 (1) we obtain $-A = -D_0 = D_{-0} = D_0$, and hence $-A \geq D_0$.

A similar argument shows that $A < D_0$ if and only if $-A > D_0$. □

Proof of (2). By the Inverses Law for Addition we know that $A + (-A) = D_0$. Then,

$$\begin{aligned} D_0 &= A + (-A) \\ &\iff D_0 + (-(-A)) = A + (-A) + (-(-A)) \\ &\iff D_0 + (-(-A)) = A + [(-A) + (-(-A))] \\ &\qquad \text{(Associative Law for Addition)} \\ &\iff D_0 + (-(-A)) = A + D_0 \\ &\qquad \text{(Inverses Law for Addition)} \\ &\iff (-(-A)) + D_0 = A + D_0 \\ &\qquad \text{(Commutative Law for Addition)} \\ &\iff -(-A) = A, \end{aligned}$$

as required. □

Proof of (3). By the Identity Law for Addition we observe that $D_0 = D_0 + D_0$. From the Inverses Law for Addition we deduce that $(A + B) + [-(A + B)] = D_0$, that $A + (-A) = D_0$, and that $B + (-B) = D_0$. Then,

$$(A + B) + [-(A + B)] = [A + (-A)] + [B + (-B)].$$

By repeated use of the Associative and Commutative Laws for Addition we obtain

$$[-(A + B)] + (A + B) = (-A) + (-B) + (A + B).$$

Adding $-(A+B)$ to both sides of this equation and using the Associtative, Inverses and Identity Laws for Addition it follows that

$$-(A + B) = (-A) + (-B),$$

as required. □

Proof of (4). Suppose that $A > D_0$ and $B > D_0$. From the Addition Law for Order we deduce that $A + B > D_0 + B$. By the Commutative and Identity Laws for Addition we see that $D_0 + B = B + D_0 = B$. Then $A + B > B > D_0$, and hence by the Transitive Law $A + B > D_0$. A similar argument shows that if $A < D_0$ and $B < D_0$, then $A + B < D_0$. □

Proof of (5). By the Identity Law for Addition we observe that $A = A + D_0$. Then,

$$\begin{aligned} A = A + D_0 &= A + [B + (-B)] && \text{(Inverses Law for Addition)} \\ &= (A + B) + (-B) && \text{(Associative Law for Addition)} \\ &= (-B) + (A + B) && \text{(Commutative Law for Addition)} \\ &= [(-B) + A] + B && \text{(Associative Law for Addition)} \\ &= B + [A + (-B)] && \text{(Commutative Law for Addition).} \end{aligned}$$

Similarly, by the Identity Law for Addition we observe that $-A = (-A) + D_0$. Then,

$$\begin{aligned} -A = (-A) + D_0 &= D_0 + (-A) && \text{(Commutative Law for Addition)} \\ &= [B + (-B)] + (-A) && \text{(Inverses Law for Addition)} \\ &= B + [(-B) + (-A)] && \text{(Associative Law for Addition)} \\ &= B + [-(B + A)] && \text{(Part (3) of this exercise).} \end{aligned}$$

□

Exercise 1.7.5 (Used in Theorem 1.7.6). Prove Theorem 1.7.6 (5) (7). For this exercise, you may use only Parts (1), (2), (3), (4), (10), (11), (12) and (14) of the theorem, and anything prior to the theorem.

[Use Exercise 1.7.4.]

Proof.

(5) Let $X, Y, Z \in \mathbb{R}$, and suppose that $X \geq D_0$ and $Y \geq D_0$ and $Z \geq D_0$. By the definition of multiplication for the real numbers, it then follows that

$$\begin{aligned}(XY)Z &= \{r \in \mathbb{Q} \mid r = (xy)z \text{ for some } x \in X \text{ and } y \in Y \text{ and } z \in Z\} \\ &= \{r \in \mathbb{Q} \mid r = x(yz) \text{ for some } x \in X \text{ and } y \in Y \text{ and } z \in Z\} \\ &= X(YZ).\end{aligned}$$

Suppose that $X \geq D_0$ and $Y < D_0$. From Exercise 1.7.4 (2) it follows that $X(-Y) = -[-X(-Y)] = -XY$. By Exercise 1.7.4 (1) and Exercise 1.7.2 (1) we deduce that $X(-Y) = -XY > D_0$ and $XY < D_0$. A similar argument shows that if $X < D_0$ and $Y \geq D_0$ then $(-X)Y = -XY > D_0$ and $XY < D_0$.

Now we will prove that $(AB)C = A(BC)$. We consider the following cases.

Case 1. $A \geq D_0$ and $B \geq D_0$.

Case 1 a. $C \geq D_0$. Clearly, $(AB)C = A(BC)$.

Case 1 b. $C < D_0$. Then $-C < D_0$, and then

$$\begin{aligned}(AB)C &= -[(AB)\cdot(-C)] = -[A\cdot(B[-C])] \\ &= -[A\cdot(-BC)] = A(BC).\end{aligned}$$

Case 2. $A < D_0$ and $B \geq D_0$. Then $-A > D_0$ and $AB < D_0$.

Case 2 a. $C \geq D_0$. It then follows that

$$\begin{aligned}(AB)C &= -[(-AB)\cdot C] = -[([-A]B)\cdot C] \\ &= -[(-A)\cdot(BC)] = A(BC).\end{aligned}$$

Case 2 b. $C < D_0$. Then $-C > D_0$, and then

$$\begin{aligned}(AB)C &= (-AB)\cdot(-C) = ([-A]B)\cdot(-C) \\ &= (-A)\cdot(B[-C]) = (-A)\cdot(-BC) = A(BC).\end{aligned}$$

Case 3. $A \geq D_0$ and $B < D_0$. By a similar argument as Case 2, we deduce that $(AB)C = A(BC)$.

Case 4. $A < D_0$ and $B < D_0$. It then follows that $-A > D_0$ and $-B > D_0$, and then $AB = (-A)(-B) > D_0$.

Case 4 a. $C \geq D_0$. Then

$$\begin{aligned}(AB)C &= ([-A][-B])\cdot C = (-A)\cdot([-B]C) \\ &= (-A)\cdot(-BC) = A(BC).\end{aligned}$$

Case 4 b. $C < D_0$. Then $-C > D_0$, and then

$$\begin{aligned}(AB)C &= -[([-A][-B])\cdot(-C)] \\ &= -[(-A)\cdot([-B][-C])] \\ &= -[(-A)\cdot(BC)] = A(BC).\end{aligned}$$

(7) We note that $D_1 > D_0$ because of the Non-Triviality. Suppose that $A \geq D_0$. To see that $A \cdot D_1 \subseteq A$, suppose that $x = ad_1 \in A \cdot D_1$ for some $a \in A$ and $d_1 \in D_1$. From Lemma 1.6.5 (2) it follows that $a > 0$, and from the definition of D_1 it follows that $d_1 > 1$. Then $ad_1 > a$. Applying Part (b) of the definition of Dedekind cuts to A, we deduce that $x = ad_1 \in A$. Hence, $A \cdot D_1 \subseteq A$.

To see that $A \subseteq A \cdot D_1$, suppose that $x \in A$. By Part (c) of the definition of Dedekind cuts we can find some $y \in A$ such that $y < x$. Let $d = xy^{-1}$. Then $d > 1$, and as a result $d \in D_1$. We then deduce that

$$x = x \cdot 1 = x(yy^{-1}) = (xy)y^{-1} = (yx)y^{-1} = y(xy^{-1}) = yd.$$

Therefore $x \in A \cdot D_1$, or in other words $A \subseteq A \cdot D_1$. Thus, we have shown that if $A \geq D_0$ then $A \cdot D_1 = A$.

Now suppose that $A < D_0$. By Exercise 1.7.4 (1) we see that $-A \geq D_0$. Using Exercise 1.7.4 (2) and the case we have already proved, we obtain

$$A \cdot D_1 = -[(-A)D_1] = -(-A) = A.$$

□

Exercise 1.7.6 (Used in Theorem 1.7.6). Prove the remaining four cases in the proof of Theorem 1.7.6 (9).

[Use Exercise 1.7.4.]

Proof. First, suppose that $A < D_0$ and $B \geq D_0$ and $C \geq D_0$. Then $-A > D_0$, and then

$$\begin{aligned} A(B+C) &= -[(-A)(B+C)] = -[(-A)B + (-A)C] = -[(-[AB]) + (-[AC])] \\ &= -[-(AB+AC)] = AB + AC. \end{aligned}$$

Second, suppose that $A < D_0$ and $B < D_0$ and $C \geq D_0$. Then $-A > D_0$ and $-B > D_0$. If $B + C \geq D_0$, then

$$\begin{aligned} AB + AC &= (-A)(-B) + (-[(-A)([-B] + [B+C])]) \\ &= (-A)(-B) + (-[(-A)(-B)]) + (-[(-A)(B+C)]) \\ &= D_0 + (-[(-A)(B+C)]) \\ &= (-[(-A)(B+C)]) + D_0 \\ &= -[(-A)(B+C)] = A(B+C). \end{aligned}$$

If $B + C < D_0$, then $-(B+C) > D_0$ and

$$\begin{aligned} AB + AC &= (-A)(-B) + (-[(-A)C]) \\ &= (-A)([-(B+C)] + C) + (-[(-A)C]) \\ &= (-A)[-(B+C)] + (-A)C + (-[(-A)C]) \\ &= (-A)[-(B+C)] + D_0 \\ &= (-A)[-(B+C)] = A(B+C). \end{aligned}$$

Third, suppose that $A < D_0$ and $B \geq D_0$ and $C < D_0$. This case is just like the previous case, and we omit details.

Fourth, suppose that $A < D_0$ and $B < D_0$ and $C < D_0$. Then $B + C < D_0$, and $-A > D_0$ and $-B > D_0$ and $-C > D_0$ and $-(B+C) > D_0$. Then,

$$\begin{aligned} A(B+C) &= (-A)[-(B+C)] = (-A)[(-B) + (-C)] \\ &= (-A)(-B) + (-A)(-C) = AB + AC. \end{aligned}$$

□

Exercise 1.7.7 (Used in Theorem 1.7.10). Prove Theorem 1.7.10.
[Use Exercise 1.7.1.]

Proof.

(1) Let $x, y \in \mathbb{Q}$, and suppose that $i(x) = i(y)$. Then $D_x = D_y$. This implies $r > x$ and $r > y$ for all $r \in D_x = D_y$. Suppose to the contrary that $x \neq y$. This means that $x < y$ or $x > y$. If $x < y$ then $y \in D_x$, and as a result $y \in D_y$, which is a contradiction to the definition of D_y. Similarly, if $x > y$ then $x \in D_y$, and as a result $x \in D_x$, which is a contradiction to the definition of D_x. Hence, $x = y$.

(2) Clearly, by the definition of $i : \mathbb{Q} \to \mathbb{R}$ we have $i(0) = D_0$ and $i(1) = D_1$.

(3 a) We will prove that $D_{r+s} = D_r + D_s$, which will imply that $i(r + s) = i(r) + i(s)$. Suppose that $x \in D_{r+s}$. Then $x > r + s$. Let $a = \frac{x+r-s}{2}$ and $b = \frac{x+s-r}{2}$. We observe that

$$a = \frac{x + r - s}{2} > \frac{(r + s) + r - s}{2} = r$$

and that

$$b = \frac{x + s - r}{2} > \frac{(r + s) + s - r}{2} = s.$$

It then follows that $a \in D_r$ and $b \in D_s$. We deduce that

$$a + b = \frac{x + r - s}{2} + \frac{x + s - r}{2} = x.$$

Hence $x \in D_r + D_s$, and therefore $D_{r+s} \subseteq D_r + D_s$.

Now suppose that $x \in D_r + D_s$. We can choose some $a \in D_r$ and $b \in D_s$ such that $x = a + b$. Then $a > r$ and $b > s$. We see that $a + b > r + b$ and that $b + r > s + r$. Then $x = a + b > r + s$. Hence $x \in D_{r+s}$, and therefore $D_r + D_s \subseteq D_{r+s}$.

(3 b) By Exercise 1.7.1 (1) we know that $D_{-r} = -D_r$, so $i(-r) = -i(r)$, as required.

(3 c) We will prove that $D_{rs} = D_r D_s$, which will imply that $i(rs) = i(r)i(s)$. Suppose that $D_r \geq D_0$ and $D_s \geq D_0$. If $D_s = D_0$ then

$$D_{rs} = D_{r \cdot 0} = D_0 = D_r D_0 = D_r D_s.$$

A similar argument shows that if $D_r = D_0$ then $D_{rs} = D_r D_s$. Next suppose that $D_r > D_0$ and $D_s > D_0$. By Lemma 1.7.4 (2) it follows that $r > 0$ and $s > 0$. Suppose further that $x \in D_{rs}$. Then $x > rs$. By Part (c) of the definition of Dedekind cuts applied to D_{rs} we can find some $y \in D_{rs}$ such that $y < x$. We note that

$$\begin{aligned} y > rs &\iff x - (x - y) > rs \\ &\iff x > rs + (x - y) \\ &\iff x > r\left(s + (x - y)r^{-1}\right) \\ &\iff \frac{x}{s + (x - y)r^{-1}} > r. \end{aligned}$$

By Exercises 1.5.6 (5) and 1.5.6 (4) we have $(x - y)r^{-1} > 0$, so $s + (x - y)r^{-1} > s$. Let

$$a = \frac{x}{s + (x - y)r^{-1}} \text{ and } b = s + (x - y)r^{-1}.$$

Then $a \in D_r$ and $b \in D_s$. We also observe that

$$ab = \frac{x}{s + (x - y)r^{-1}} \left(s + (x - y)r^{-1}\right) = x.$$

Hence $x \in D_r + D_s$, and therefore $D_{rs} \subseteq D_r D_s$.

To see that $D_r D_s \subseteq D_{rs}$, suppose that $x \in D_r D_s$. We can find some $a \in D_r$ and $b \in D_s$ such that $x = ab$. Then $a > r$ and $b > s$. It follows from Lemma 1.7.4 (2) and Exercise 1.5.6 (7) that $0 < rs < ab$, and hence $x \in D_{rs}$, which implies $D_r D_s \subseteq D_{rs}$. Thus, we have shown that if $D_r \geq D_0$ and $D_s \geq D_0$ then $D_{rs} = D_r D_s$.

Now we will prove the remaining three cases. First, suppose that $D_r < D_0$ and $D_s \geq D_0$. By Exercise 1.7.4 (1) we see that $-D_r > D_0$. Using Exercises 1.7.1 (1) and 1.7.4 (2) we obtain

$$D_{rs} = -(-D_{rs}) = -D_{-(rs)} = -D_{(-r)s} = -(D_{-r} D_s) = -[(-D_r)D_s] = D_r D_s.$$

Second, suppose that $D_r \geq D_0$ and $D_s < D_0$. This case is just like the previous case, and we omit details.

Third, suppose that $D_r < D_0$ and $D_s < D_0$. Then $-D_r > D_0$ and $-D_s > D_0$, and we deduce that

$$D_{rs} = D_{-(-rs)} = D_{(-r)(-s)} = D_{-r} D_{-s} = (-D_r)(-D_s) = D_r D_s.$$

(3 d) Suppose that $r \neq 0$. By Exercise 1.7.1 (2) it follows that $D_{r^{-1}} = [D_r]^{-1}$, so $i(r^{-1}) = [i(r)]^{-1}$, as required.

(3 e) Suppose that $r < s$. Then $s - r > 0$. From Lemma 1.7.4 (1) we see that $D_{s-r} > D_0$. Then,

$$\begin{aligned} & D_0 < D_{s-r} \\ \iff\ & D_0 < D_{s+(-r)} \\ \iff\ & D_0 < D_s + D_{-r} && \text{(Part (3 a) of this exercise)} \\ \iff\ & D_0 < D_s + (-D_r) && \text{(Part (1) of Exercise 1.7.1)} \\ \iff\ & D_0 + D_r < [D_s + (-D_r)] + D_r && \text{(Addition Law for Order)} \\ \iff\ & D_0 + D_r < D_s + [(-D_r) + D_r] && \text{(Associative Law for Addition)} \\ \iff\ & D_r + D_0 < D_s + [D_r + (-D_r)] && \text{(Commutative Law for Addition)} \\ \iff\ & D_r + D_0 < D_s + D_0 && \text{(Inverses Law for Addition)} \\ \iff\ & D_r < D_s && \text{(Identity Law for Addition).} \end{aligned}$$

□

Properties of the Real Numbers

2. Entry 3: Axioms for the Real Numbers

Definition 2.2.1. *Let $x, y, z \in \curvearrowleft$.*

(a) $(x + y) + z = x + (y + z)$ *(Associative Law for Addition).*
(b) $x + y = y + x$ *(Commutative Law for Addition).*
(c) $x + 0 = x$ *(Identity Law for Addition).*
(d) $x + (-x) = 0$ *(Inverses Law for Addition).*
(e) $(xy)z = x(yz)$ *(Associative Law for Multiplication).*
(f) $xy = yx$ *(Commutative Law for Multiplication).*
(g) $x \cdot 1 = x$ *(Identity Law for Multiplication).*
(h) *If* $x \neq 0$*, then* $x \cdot x^{-1} = 1$ *(Inverses Law for Multiplication).*
(i) $x(y + z) = xy + xz$ *(Distributive Law).*
(j) *Precisely one of* $x < y$ *or* $x = y$ *or* $x > y$ *holds* *(Trichotomy Law).*
(k) *If* $x < y$ *and* $y < z$*, then* $x < z$ *(Transitive Law).*
(l) *If* $x < y$ *then* $x + z < y + z$ *(Addition Law for Order).*
(m) *If* $x < y$ *and* $z > 0$*, then* $xz < yz$ *(Multiplication Law for Order).*
(n) $0 \neq 1$ *(Non-Triviality).*

Definition 2.2.2. *Let F be an ordered field, and let $A \subseteq F$ be a set.*

(1) *The set A is **bounded above** if there is some $M \in \mathbb{R}$ such that $X \leq M$ for all $X \in A$. The number M is called an **upper bound** of A.*
(2) *The set A is **bounded below** if there is some $P \in \mathbb{R}$ such that $X \geq P$ for all $X \in A$. The number P is called a **lower bound** of A.*
(3) *The set A is **bounded** if it is bounded above and bounded below.*
(4) *Let $M \in \mathbb{R}$. The number M is a **least upper bound** (also called a **supremum**) of A if M is an upper bound of A, and if $M \leq T$ for all upper bounds T of A.*
(5) *Let $P \in \mathbb{R}$. The number P is a **greatest lower bound** (also called an **infimum**) of A if P is a lower bound of A, and if $P \geq V$ for all lower bounds V of A.*

Definition 2.2.3. *Let F be an ordered field. The ordered field F satisfies the **Least Upper Bound Property** if every non-empty subset of F that is bounded above has a least upper bound.*

Axiom 2.2.4 (Axiom for the Real Numbers). *There exists an ordered field $\mathbb{R}$ that satisfies the Least Upper Bound Property.*

3. Algebraic Properties of the Real Numbers

Definition 2.3.1.

(1) *The binary operation* $-$ *on* $\mathbb{R}$ *is defined by* $a - b = a + (-b)$ *for all* $a, b \in \mathbb{R}$. *The binary operation* $\div$ *on* $\mathbb{R} - \{0\}$ *is defined by* $a \div b = ab^{-1}$ *for all* $a, b \in \mathbb{R} - \{0\}$*; we also let* $0 \div s = 0 \cdot s^{-1} = 0$ *for all* $s \in \mathbb{R} - \{0\}$. *The number* $a \div b$ *is also denoted* $\frac{a}{b}$.

(2) *Let* $a \in \mathbb{R}$. *The square of* a*, denoted* a^2*, is defined by* $a^2 = a \cdot a$.

(3) *The relation* $\leq$ *on* $\mathbb{R}$ *is defined by* $x \leq y$ *if and only if* $x < y$ *or* $x = y$*, for all* $x, y \in \mathbb{R}$.

(4) *The number* $2 \in \mathbb{R}$ *is defined by* $2 = 1 + 1$.

Lemma 2.3.2. *Let* $a, b, c \in \mathbb{R}$.

(1) *If* $a + c = b + c$ *then* $a = b$ *(Cancellation Law for Addition).*
(2) *If* $a + b = a$ *then* $b = 0$.
(3) *If* $a + b = 0$ *then* $b = -a$.
(4) $-(a + b) = (-a) + (-b)$.
(5) $-0 = 0$.
(6) *If* $ac = bc$ *and* $c \neq 0$*, then* $a = b$ *(Cancellation Law for Multiplication).*
(7) $0 \cdot a = 0 = a \cdot 0$.
(8) *If* $ab = a$ *and* $a \neq 0$*, then* $b = 1$.
(9) *If* $ab = 1$ *then* $b = a^{-1}$.
(10) *If* $a \neq 0$ *and* $b \neq 0$*, then* $(ab)^{-1} = a^{-1}b^{-1}$.
(11) $(-1) \cdot a = -a$.
(12) $(-a)b = -ab = a(-b)$.
(13) $-(-a) = a$.
(14) $(-1)^2 = 1$ *and* $1^{-1} = 1$.
(15) *If* $ab = 0$*, then* $a = 0$ *or* $b = 0$ *(No Zero Divisors Law).*
(16) *If* $a \neq 0$ *then* $(a^{-1})^{-1} = a$.
(17) *If* $a \neq 0$ *then* $(-a)^{-1} = -a^{-1}$.

Lemma 2.3.3. *Let* $a, b, c, d \in \mathbb{R}$.

(1) *If* $a \leq b$ *and* $b \leq a$*, then* $a = b$.
(2) *If* $a \leq b$ *and* $b \leq c$*, then* $a \leq c$. *If* $a \leq b$ *and* $b < c$*, then* $a < c$. *If* $a < b$ *and* $b \leq c$*, then* $a < c$.
(3) *If* $a \leq b$ *then* $a + c \leq b + c$.
(4) *If* $a < b$ *and* $c < d$*, then* $a + c < b + d$*; if* $a \leq b$ *and* $c \leq d$*, then* $a + c \leq b + d$.
(5) $a > 0$ *if and only if* $-a < 0$*, and* $a < 0$ *if and only if* $-a > 0$*; also* $a \geq 0$ *if and only if* $-a \leq 0$*, and* $a \leq 0$ *if and only if* $-a \geq 0$.
(6) $a < b$ *if and only if* $b - a > 0$ *if and only if* $-b < -a$. *Also* $a \leq b$ *if and only if* $b - a \geq 0$ *if and only if* $-b \leq -a$.
(7) *If* $a \neq 0$ *then* $a^2 > 0$.
(8) $-1 < 0 < 1$.
(9) $a < a + 1$.
(10) *If* $a \leq b$ *and* $c > 0$*, then* $ac \leq bc$.
(11) *If* $0 \leq a < b$ *and* $0 \leq c < d$*, then* $ac < bd$*; if* $0 \leq a \leq b$ *and* $0 \leq c \leq d$*, then* $ac \leq bd$.
(12) *If* $a < b$ *and* $c < 0$*, then* $ac > bc$.
(13) *If* $a > 0$ *then* $a^{-1} > 0$.
(14) *If* $a > 0$ *and* $b > 0$*, then* $a < b$ *if and only if* $b^{-1} < a^{-1}$ *if and only if* $a^2 < b^2$.

Definition 2.3.4. *Let* $a \in \mathbb{R}$. *The number* a *is* ***positive*** *if* $a > 0$*; the number* a *is* ***negative*** *if* $a < 0$*; and the number* a *is* ***non-negative*** *if* $a \geq 0$.

Lemma 2.3.5. *Let* $a, b \in \mathbb{R}$.

(1) *If* $a > 0$ *and* $b > 0$*, then* $a + b > 0$. *If* $a > 0$ *and* $b \geq 0$*, then* $a + b > 0$. *If* $a \geq 0$ *and* $b \geq 0$*, then* $a + b \geq 0$.
(2) *If* $a < 0$ *and* $b < 0$*, then* $a + b < 0$. *If* $a < 0$ *and* $b \leq 0$*, then* $a + b < 0$. *If* $a \leq 0$ *and* $b \leq 0$*, then* $a + b \leq 0$.
(3) *If* $a > 0$ *and* $b > 0$*, then* $ab > 0$. *If* $a > 0$ *and* $b \geq 0$*, then* $ab \geq 0$. *If* $a \geq 0$ *and* $b \geq 0$*, then* $ab \geq 0$.
(4) *If* $a < 0$ *and* $b < 0$*, then* $ab > 0$. *If* $a < 0$ *and* $b \leq 0$*, then* $ab \geq 0$. *If* $a \leq 0$ *and* $b \leq 0$*, then* $ab \geq 0$.
(5) *If* $a < 0$ *and* $b > 0$*, then* $ab < 0$. *If* $a < 0$ *and* $b \geq 0$*, then* $ab \leq 0$. *If* $a \leq 0$ *and* $b > 0$*, then* $ab \leq 0$. *If* $a \leq 0$ *and* $b \geq 0$*, then* $ab \leq 0$.

Definition 2.3.6. *An* ***open bounded interval*** *is a set of the form*

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\},$$

where $a, b \in \mathbb{R}$ *and* $a \leq b$. *A* ***closed bounded interval*** *is a set of the form*

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\},$$

where $a, b \in \mathbb{R}$ *and* $a \leq b$. *A* ***half-open interval*** *is a set of the form*

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\} \quad \text{or} \quad (a, b] = \{x \in \mathbb{R} \mid a < x \leq b\},$$

where $a, b \in \mathbb{R}$ *and* $a \leq b$. *An* ***open unbounded interval*** *is a set of the form*

$$(a, \infty) = \{x \in \mathbb{R} \mid a < x\} \quad \text{or} \quad (-\infty, b) = \{x \in \mathbb{R} \mid x < b\} \quad \text{or} \quad (-\infty, \infty) = \mathbb{R},$$

where $a, b \in \mathbb{R}$. *A* ***closed unbounded interval*** *is a set of the form*

$$[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\} \quad \text{or} \quad (-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\},$$

where $a, b \in \mathbb{R}$.

An ***open interval*** *is either an open bounded interval or an open unbounded interval. A* ***closed interval*** *is either a closed bounded interval or a closed unbounded interval. A* ***right unbounded interval*** *is any interval of the form* $(a, \infty), [a, \infty)$ *or* $(-\infty, \infty)$. *A* ***left unbounded interval*** *is any interval of the form* $(-\infty, b), (-\infty, b]$ *or* $(-\infty, \infty)$. *A* ***non-degenerate interval*** *is any interval of the form* $(a, b), (a, b], [a, b)$ *or* $[a, b]$ *where* $a < b$*, or any unbounded interval. The number* a *in intervals of the form* $[a, b), [a, b]$ *or* $[a, \infty)$ *is called the* ***left endpoint*** *of the interval. The number* b *in intervals of the form* $(a, b], [a, b]$ *or* $(-\infty, b]$ *is called the* ***right endpoint*** *of the interval. An* ***endpoint*** *of an interval is either a left endpoint or a right endpoint. The* ***interior*** *of an interval is everything in the interval other than its endpoints (if it has any).*

Lemma 2.3.7. *Let* $I \subseteq \mathbb{R}$ *be an interval.*

(1) *If* $x, y \in I$ *and* $x \leq y$*, then* $[x, y] \subseteq I$.
(2) *If* I *is an open interval, and if* $x \in I$*, then there is some* $\delta > 0$ *such that* $[x - \delta, x + \delta] \subseteq I$.

Definition 2.3.8. *Let* $a \in \mathbb{R}$. *The* ***absolute value*** *of* a*, denoted* $|a|$*, is defined by*

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

Lemma 2.3.9. *Let* $a, b \in \mathbb{R}$.

(1) $|a| \geq 0$*, and* $|a| = 0$ *if and only if* $a = 0$.
(2) $-|a| \leq a \leq |a|$.
(3) $|a| = |b|$ *if and only if* $a = b$ *or* $a = -b$.
(4) $|a| < b$ *if and only if* $-b < a < b$*, and* $|a| \leq b$ *if and only if* $-b \leq a \leq b$.
(5) $|ab| = |a| \cdot |b|$.
(6) $|a + b| \leq |a| + |b|$ *(Triangle Inequality).*
(7) $||a| - |b|| \leq |a + b|$ *and* $||a| - |b|| \leq |a - b|$.

Lemma 2.3.10. *Let* $a \in \mathbb{R}$.

(1) $a \leq 0$ *if and only if* $a < \varepsilon$ *for all* $\varepsilon > 0$.
(2) $a \geq 0$ *if and only if* $a > -\varepsilon$ *for all* $\varepsilon > 0$.
(3) $a = 0$ *if and only if* $|a| < \varepsilon$ *for all* $\varepsilon > 0$.

Exercise 2.3.1 (Used in Lemma 2.3.2). Prove Lemma 2.3.2 (2) (3) (4) (6) (8) (10) (12) (13) (14) (16) (17).

Proof.

(2) Suppose that $a + b = a$. Then,

$$\begin{aligned}
a + b = a &\iff (a+b) + (-a) = a + (-a) \\
&\iff (b+a) + (-a) = a + (-a) && \text{(Commutative Law for Addition)} \\
&\iff b + (a + [-a]) = a + (-a) && \text{(Associative Law for Addition)} \\
&\iff b + 0 = 0 && \text{(Inverses Law for Addition)} \\
&\iff b = 0 && \text{(Identity Law for Addition).}
\end{aligned}$$

(3) Suppose that $a + b = 0$. Then,

$$\begin{aligned}
a + b = 0 &\iff (a+b) + (-a) = 0 + (-a) \\
&\iff (b+a) + (-a) = (-a) + 0 && \text{(Commutative Law for Addition)} \\
&\iff b + (a + [-a]) = (-a) + 0 && \text{(Associative Law for Addition)} \\
&\iff b + 0 = (-a) + 0 && \text{(Inverses Law for Addition)} \\
&\iff b = -a && \text{(Identity Law for Addition).}
\end{aligned}$$

(4) By the Inverses Law for Addition we observe that $(a+b)+[-(a+b)] = 0$. Adding $(-a) + (-b)$ to both sides of this equation we obtain

$$[(a+b) + (-[a+b])] + [(-a) + (-b)] = 0 + [(-a) + (-b)].$$

By repeated use of the Associative and Commutative Laws for Addition we deduce that

$$[([-(a+b)] + [a + (-a)]) + (b + [-b])] = [(-a) + (-b)] + 0.$$

From the Inverses Law for Addition we see that $a + (-a) = 0$ and $b + (-b) = 0$. Then,

$$[([-(a+b)] + 0) + 0] = [(-a) + (-b)] + 0.$$

Hence by repeated use of the Inverses Law for Addition we can conclude that

$$-(a+b) = (-a) + (-b).$$

(6) Suppose that $ac = bc$ and $c \neq 0$. Then,

$$\begin{aligned}
ac = bc &\iff (ac)c^{-1} = (bc)c^{-1} \\
&\iff a(cc^{-1}) = b(cc^{-1}) && \text{(Associative Law for Multiplication)} \\
&\iff a \cdot 1 = b \cdot 1 && \text{(Inverses Law for Multiplication)} \\
&\iff a = b && \text{(Identity Law for Multiplication).}
\end{aligned}$$

(8) Suppose that $ab = a$ and $a \neq 0$. Then,

$$\begin{aligned}
ab = a &\iff (ab)a^{-1} = aa^{-1} \\
&\iff (ba)a^{-1} = aa^{-1} && \text{(Commutative Law for Multiplication)} \\
&\iff b(aa^{-1}) = aa^{-1} && \text{(Associative Law for Multiplication)} \\
&\iff b \cdot 1 = 1 && \text{(Inverses Law for Multiplication)} \\
&\iff b = 1 && \text{(Identity Law for Multiplication).}
\end{aligned}$$

(10) Suppose that $a \neq 0$ and $b \neq 0$. From the Inverses Law for Multiplication we observe that $(ab)(ab)^{-1} = 1$. Then,

$$\begin{aligned}
&(ab)(ab)^{-1} = 1 \\
&\iff (ab)(ba) = 1 && \text{(Commutative Law for Multiplication)} \\
&\iff [(ab)^{-1}b]a = 1 && \text{(Associative Law for Multiplication)} \\
&\iff ([(ab)^{-1}b]a)a^{-1} = 1 \cdot a^{-1} \\
&\iff [(ab)^{-1}b][aa^{-1}] = 1 \cdot a^{-1} && \text{(Associative Law for Multiplication)} \\
&\iff [(ab)^{-1}b] \cdot 1 = 1 \cdot a^{-1} && \text{(Inverses Law for Multiplication)} \\
&\iff [(ab)^{-1}b] \cdot 1 = a^{-1} \cdot 1 && \text{(Commutative Law for Multiplication)} \\
&\iff (ab)^{-1}b = a^{-1} && \text{(Identity Law for Multiplication)} \\
&\iff [(ab)^{-1}b]b^{-1} = a^{-1}b^{-1} \\
&\iff (ab)^{-1}(bb^{-1}) = a^{-1}b^{-1} && \text{(Associative Law for Multiplication)} \\
&\iff (ab)^{-1} \cdot 1 = a^{-1}b^{-1} && \text{(Inverses Law for Multiplication)} \\
&\iff (ab)^{-1} = a^{-1}b^{-1} && \text{(Identity Law for Multiplication).}
\end{aligned}$$

(12) By Part (11) of this lemma and the Associative Law for Multiplication, we deduce that

$$(-a)b = [(-1)a]b = (-1)(ab) = -ab.$$

Using the Commutative Law for Multiplication additionally, we deduce that

$$a(-b) = a[(-1)b] = [a(-1)]b = [(-1)a]b = (-a)b.$$

Hence, $(-a)b = -ab = a(-b)$.

(13) From the Inverses Law for Addition we see that $(-a) + (-[-a]) = 0$. Then,

$$\begin{aligned}
&(-a) + (-[-a]) = 0 \\
&\iff [(-a) + (-[-a])] + a = 0 + a \\
&\iff [(-[-a]) + (-a)] + a = a + 0 && \text{(Commutative Law for Addition)} \\
&\iff [-(-a)] + [(-a) + a] = a + 0 && \text{(Associative Law for Addition)} \\
&\iff [-(-a)] + [a + (-a)] = a + 0 && \text{(Commutative Law for Addition)} \\
&\iff [-(-a)] + 0 = a + 0 && \text{(Inverses Law for Addition)} \\
&\iff -(-a) = a && \text{(Identity Law for Addition).}
\end{aligned}$$

(14) Using Parts (12) (13) of this lemma and the Identity Law for Addition we obtain

$$(-1)^2 = (-1)(-1) = -[1 \cdot (-1)] = -(-[1 \cdot 1]) = -(-1) = 1.$$

By the Identity, Commutative and Inverses Laws for Multiplication we deduce that

$$1^{-1} = 1^{-1} \cdot 1 = 1 \cdot 1^{-1} = 1.$$

(16) Let $x \in \mathbb{R}$, and suppose that $x \neq 0$. From the Identity Law for Multiplication we obtain $xx^{-1} = 1$. Suppose to the contrary that $x^{-1} = 0$. Then by Part (7) of this lemma we observe that $x \cdot 0 = xx^{-1} = 0$, which is a contradiction. Hence, $x^{-1} \neq 0$.

Suppose that $a \neq 0$. From the Inverses Law for Multiplication we see that $a^{-1}(a^{-1})^{-1} = 1$. Then,

$$\begin{aligned}
&a^{-1}(a^{-1})^{-1} = 1 \\
&\iff [a^{-1}(a^{-1})^{-1}]a = 1 \cdot a \\
&\iff [(a^{-1})^{-1}a^{-1}]a = a \cdot 1 && \text{(Commutative Law for Multiplication)} \\
&\iff (a^{-1})^{-1}(a^{-1}a) = a \cdot 1 && \text{(Associative Law for Multiplication)} \\
&\iff (a^{-1})^{-1}(aa^{-1}) = a \cdot 1 && \text{(Commutative Law for Multiplication)} \\
&\iff (a^{-1})^{-1} \cdot 1 = a \cdot 1 && \text{(Inverses Law for Multiplication)} \\
&\iff (a^{-1})^{-1} = a && \text{(Identity Law for Multiplication).}
\end{aligned}$$

(17) Let $x \in \mathbb{R}$, and suppose that $x \neq 0$. From the Identity Law for Multiplication we obtain $xx^{-1} = 1$. By Part (13) of this lemma we know that $x = -(-x)$. Using Part (5) of this lemma we deduce that $x = -(-x) = -0 = 0$, which is a contradiction. Hence, $-x \neq 0$.

Suppose that $a \neq 0$. Suppose to the contrary that $-a = 0$. From the Inverses Law for Multiplication we see that $(-1)(-1)^{-1} = 1$. Then,

$$\begin{aligned}
&(-1)(-1)^{-1} = 1 \\
&\iff [(-1)(-1)^{-1}](-1) = 1 \cdot (-1) \\
&\iff [(-1)^{-1}(-1)](-1) = (-1) \cdot 1 && \text{(Commutative Law for Multiplication)} \\
&\iff (-1)^{-1}[(-1)(-1)] = (-1) \cdot 1 && \text{(Associative Law for Multiplication)} \\
&\iff (-1)^{-1} \cdot 1 = (-1) \cdot 1 && \text{(Part (14) of this lemma)} \\
&\iff (-1)^{-1} = (-1) && \text{(Identity Law for Multiplication)} \\
&\iff (-1)^{-1}a^{-1} = (-1)a^{-1} \\
&\iff [(-1)a]^{-1} = (-1)a^{-1} && \text{(Part (10) of this lemma)} \\
&\iff [a(-1)]^{-1} = a^{-1}(-1) && \text{(Commutative Law for Multiplication)} \\
&\iff [-(a \cdot 1)]^{-1} = -[a^{-1} \cdot 1] && \text{(Part (12) of this lemma)} \\
&\iff (-a)^{-1} = -a^{-1} && \text{(Identity Law for Multiplication).}
\end{aligned}$$

□

Exercise 2.3.2 (Used in Lemma 2.3.3). Prove Lemma 2.3.3 (2) (4) (6) (9) (10) (13) (14).

Proof.

(2) Suppose that $a \leq b$ and $b \leq c$. We consider the following four cases. First, if $a < b$ and $b < c$, then by the Transitive Law it follows that $a < c$, and hence $a \leq c$. Second, if $a = b$ and $b = c$, then $a = c$, and hence $a \leq c$. Third, if $a < b$ and $b = c$, then $a < c$, and hence $a \leq c$. Fourth, if $a = b$ and $b < c$, then $a < c$, and hence $a \leq c$.

(4) Suppose that $a < b$ and $c < d$. By the Addition Law for Order we deduce that $a + c < b + c$ and that $c + b < d + b$. From the Commutative Law for Addition we observe that $b + c < b + d$, and hence by the Transitive Law we conclude that $a + c < b + d$. A similar argument shows that if $a \leq b$ and $c \leq d$, then $a + c \leq b + d$.

(6) First, suppose that $a < b$. Then,

$$\begin{aligned} b > a &\iff b + (-a) > a + (-a) && \text{(Addition Law for Order)}\\ &\iff b - a > 0 && \text{(Identity Law for Addition).} \end{aligned}$$

Second, suppose that $b - a > 0$. Then,

$$\begin{aligned} &0 < b + (-a)\\ &\iff 0 + (-b) < [b + (-a)] + (-b) && \text{(Addition Law for Order)}\\ &\iff (-b) + 0 < [(-a) + b] + (-b) && \text{(Commutative Law for Addition)}\\ &\iff (-b) + 0 < (-a) + [b + (-b)] && \text{(Associative Law for Addition)}\\ &\iff (-b) + 0 < (-a) + 0 && \text{(Inverses Law for Addition)}\\ &\iff -b < -a && \text{(Identity Law for Addition).} \end{aligned}$$

Third, suppose that $-b < -a$. Then,

$$\begin{aligned} &-b < -a\\ &\iff (-b) + (b + a) < (-a) + (b + a) && \text{(Addition Law for Order)}\\ &\iff [(-b) + b] + a < (-a) + (b + a) && \text{(Associative Law for Addition)}\\ &\iff a + [b + (-b)] < (b + a) + (-a) && \text{(Commutative Law for Addition)}\\ &\iff a + [b + (-b)] < b + [a + (-a)] && \text{(Associative Law for Addition)}\\ &\iff a + 0 < b + 0 && \text{(Inverses Law for Addition)}\\ &\iff a < b && \text{(Identity Law for Addition).} \end{aligned}$$

Thus, $a < b$ if and only if $b - a > 0$ if and only if $-b < -a$. A similar argument shows that $a \leq b$ if and only if $b - a \geq 0$ if and only if $-b \leq -a$.

(9) By Part (8) of this lemma we know that $0 < 1$. Then,

$$\begin{aligned} 0 < 1 &\iff 0 + a < 1 + a && \text{(Addition Law for Order)}\\ &\iff a + 0 < a + 1 && \text{(Commutative Law for Addition)}\\ &\iff a < a + 1 && \text{(Identity Law for Addition).} \end{aligned}$$

(10) Suppose that $a \leq b$ and $c > 0$. If $a = b$, then $ac = bc$, and hence $ac \leq bc$. If $a < b$, then by the Multiplication Law for Order we deduce that $ac < bc$, and hence $ac \leq bc$.

(13) Suppose that $a > 0$. Then by the Trichotomy Law it follows that $a \neq 0$, and then by Inverses Law for Multiplication it follows that $aa^{-1} = 1$. Suppose to the contrary that $a^{-1} \leq 0$, which means that either $a^{-1} = 0$ or $a^{-1} < 0$. Suppose that $a^{-1} = 0$. We then deduce from Lemma 2.3.2 (7) that $0 = a \cdot 0 = a \cdot a^{-1}$, which is a contradiction.

Now suppose that $a^{-1} < 0$. Then,

$$\begin{aligned} a^{-1} < 0 &\iff -a^{-1} > 0 && \text{(Part (5) of this lemma)}\\ &\iff a(-a^{-1}) > 0 && \text{(Part (10) of this lemma)}\\ &\iff -(aa^{-1}) > 0 && \text{(Part (12) of Lemma 2.3.2)}\\ &\iff -1 > 0 && \text{(Inverses Law for Multiplication).} \end{aligned}$$

From Part (8) of this lemma we know that $-1 < 0$. Thus, we have $-1 > 0$ and $-1 < 0$, which is a contradiction to the Trichotomy Law. Hence, $a^{-1} > 0$.

(14) Suppose that $a > 0$ and $b > 0$. Suppose further that $a < b$. By Part (13) of this lemma we see that $a^{-1} > 0$ and $b^{-1} > 0$. From Part (10) of this lemma we observe that $a^{-1}b^{-1} > 0$. Then,

$$\begin{aligned} a < b &\iff a(a^{-1}b^{-1}) < b(a^{-1}b^{-1}) && \text{(Multiplication Law for Order)}\\ &\iff a(a^{-1}b^{-1}) < (a^{-1}b^{-1})b && \text{(Commutative Law for Multiplication)}\\ &\iff (aa^{-1})b^{-1} < a^{-1}(b^{-1}b) && \text{(Associative Law for Multiplication)}\\ &\iff b^{-1}(aa^{-1}) < a^{-1}(bb^{-1}) && \text{(Commutative Law for Multiplication)}\\ &\iff b^{-1} \cdot 1 < a^{-1} \cdot 1 && \text{(Inverses Law for Multiplication)}\\ &\iff b^{-1} < a^{-1} && \text{(Identity Law for Multiplication).} \end{aligned}$$

Now suppose that $b^{-1} < a^{-1}$. By Parts (7) (10) of this lemma we know that $a^2 > 0$ and $ba^2 > 0$. Then,

$$\begin{aligned} &b^{-1} < a^{-1}\\ &\iff b^{-1}(ba^2) < a^{-1}(ba^2) = a^{-1}(baa) && \text{(Multiplication Law for Order)}\\ &\iff b^{-1}(ba^2) < (baa)a^{-1} && \text{(Commutative Law for Multiplication)}\\ &\iff (b^{-1}b)a^2 < (ba)(aa^{-1}) && \text{(Associative Law for Multiplication)}\\ &\iff a^2(bb^{-1}) < (ab)(aa^{-1}) && \text{(Commutative Law for Multiplication)}\\ &\iff a^2 \cdot 1 < (ab) \cdot 1 && \text{(Inverses Law for Multiplication)}\\ &\iff a^2 < ab && \text{(Identity Law for Multiplication).} \end{aligned}$$

A similar argument shows that $b^2 > 0$ and $ab^2 > 0$ and $ab < b^2$. Thus, $a^2 < ab < b^2$, and from the Transitive Law it follows that $a^2 < b^2$.

Finally, suppose that $a^2 < b^2$. Suppose to the contrary that $a \geq b$. By the Multiplication Law for Order we observe that $ab \geq bb = b^2$ and that $a^2 = aa \geq ab$. From the Transitive Law we see that $a^2 \geq b^2$, which is a contradiction to the fact that $a^2 < b^2$ because of the Trichotomy Law. Hence, $a < b$. □

Exercise 2.3.3. For any $a \in \mathbb{R}$, let a^3 denote $a \cdot a \cdot a$.

Let $x, y \in \mathbb{R}$.

(1) Prove that if $x < y$, then $x^3 < y^3$.

(2) Prove that there are $c, d \in \mathbb{R}$ such that $c^3 < x < d^3$.

Proof of (1). Suppose that $x < y$. Suppose that $x = 0$. Then $y > 0$. By repeated use of Lemma 2.3.3 (10) we deduce that $y^3 > 0^3$. From Lemma 2.3.2 (7) we observe that $0^2 = 0 \cdot 0$ and that $x^3 = 0^3 = 0^2 \cdot 0 = 0$. Hence, $x^3 < y^3$. A similar argument shows that if $y = 0$, then $x^3 < y^3$.

Now suppose that $x \neq 0$ and $y \neq 0$. Because of Lemma 2.3.3 (7) it follows that $x^2 > 0$ and $y^2 > 0$. From Lemma 2.3.3 (10) we obtain

$$x(xx) < y(xx) \quad \text{and} \quad x(yy) < y(yy) \quad \text{and} \quad x(xy) < y(xy).$$

Using the Associative and Commutative Laws for Multiplication we then deduce that

$$x^3 < yx^2 < xy^2 < y^3.$$

Hence by Transitive Law we conclude that $x^3 < y^3$. □

Proof of (2). We note that $0 = 0^3$ according to Part (7) of Lemma 2.3.2. We consider the following three cases. First, suppose that $x = 0$. We then deduce from Lemma 2.3.3 (8) that $-1 < x < 1$.

Second, suppose that $x > 0$. It then follows from the Addition Law for Order that $x + 1 > 0 + 1$. Because of the Commutative and Identity Laws for Addition, we deduce that $x + 1 > 1$. Using the Multiplication Law for Order we observe that $(x + 1)^2 > x + 1$ and that $(x + 1)^3 > (x + 1)^2$. By Lemma 2.3.3 (8) it follows that $x < x + 1$, and hence by the Transitive Law we conclude that $0^3 < x < (x + 1)^3$.

Third, suppose that $x < 0$. By a similar argument, we obtain $(x - 1)^3 < x < 0^3$.

□

Exercise 2.3.4 (Used in Lemma 2.3.5). Prove Lemma 2.3.5 (2) (3) (4).

Proof.

(2) First, suppose that $a < 0$ and $b < 0$. Then by Lemma 2.3.3 (4) and the Identity Law for Addition we see that $a + b < 0 + 0 = 0$.

Second, suppose that $a < 0$ and $b \leq 0$. There are now two subcases. First, suppose that $b < 0$. Then by the previous paragraph we know that $a + b < 0$. Second, suppose that $b = 0$. Then by the Identity Law for Addition we see that $a + b = a + 0 = a > 0$.

Third, suppose that $a \leq 0$ and $b \leq 0$. There are now two subcases. First, suppose that $a < 0$. Then by the previous paragraph we know that $a+b < 0$, which implies that $a+b \leq 0$. Second, suppose that $a = 0$. Then by the Commutative and Identity Laws for Addition we see that $a + b = 0 + b = b + 0 = b \leq 0$.

(3) First, suppose that $a > 0$ and $b > 0$. By the Multiplication Law for Order and Lemma 2.3.2 (7) we deduce that $ab > 0 \cdot b = 0$.

Second, suppose that $a > 0$ and $b \geq 0$ There are now two subcases. First suppose that $b > 0$. Then by the previous case we know that $ab > 0$, which implies that $ab \geq 0$. Second, suppose that $b = 0$. Then by Lemma 2.3.2 (7) we see that $ab = 0 \cdot 0 = 0$, and hence $ab \leq 0$.

The proofs of other two parts are similar, and we omit the details.

(4) This part is just like the previous part, and we omit details. □

Exercise 2.3.5 (Used in Exercise 2.3.6 and Exercise 2.8.9).

(1) Prove that $1 < 2$.
(2) Prove that $0 < \frac{1}{2} < 1$.
(3) Prove that if $a, b \in \mathbb{R}$ and $a < b$, then $a < \frac{a+b}{2} < b$.

Proof of (1). By Lemma 2.3.3 (8) we know that $1 > 0$. From the Addition Law for Order we obtain $0+1 < 1+1 = 2$, and hence by the Commutative and Identity Laws for Addition, we conclude that $1 < 2$. □

Proof of (2). By Lemma 2.3.3 (8) and Part (1) of this exercise we know that $0 < 1 < 2$. Using the Transitive Law we deduce that $2 > 0$. By the Trichotomy Law we see that $2 \neq 0$. It follows from the Multiplication Law for Order that $0 \cdot 2^{-1} < 1 \cdot 2^{-1} < 2 \cdot 2^{-1}$. By the Commutative Law for Multiplication it implies that $2^{-1} \cdot 0 < 2^{-1} \cdot 1 < 2 \cdot 2^{-1}$. Lemma 2.3.2 (7) implies $2^{-1} \cdot 0 = 0$. The Identity Law for Multiplication implies that $2^{-1} \cdot 1 = 2^{-1}$. The Inverses Law for Multiplication implies that $2 \cdot 2^{-1} = 1$. Hence, $0 < \frac{1}{2} < 1$. □

Proof of (3). Let $a, b \in \mathbb{R}$, and suppose that $a < b$. By the Multiplication Law for Order and Commutative Law for Addition we observe that $a+a < a+b < b+b$. By the Trichotomy Law and Part (1) of this exercise we deduce that $2 \neq 0$. Then,

$$
\begin{aligned}
& a + a < a + b < b + b \\
& \iff a \cdot 1 + a \cdot 1 < a + b < b \cdot 1 + b \cdot 1 \\
& \qquad \text{(Identity Law for Multiplication)} \\
& \iff a(1+1) < a + b < b(1+1) \\
& \qquad \text{(Distributive Law)} \\
& \iff a \cdot 2 < a + b < b \cdot 2 \\
& \iff (a \cdot 2)2^{-1} < (a+b)2^{-1} < (b \cdot 2)2^{-1} \\
& \qquad \text{(Multiplication Law for Order)} \\
& \iff a(2 \cdot 2^{-1}) < (a+b)2^{-1} < b(2 \cdot 2^{-1}) \\
& \qquad \text{(Associative Law for Multiplication)} \\
& \iff a \cdot 1 < (a+b)2^{-1} < b \cdot 1 \\
& \qquad \text{(Inverses Law for Multiplication)} \\
& \iff a < (a+b)2^{-1} < b \\
& \qquad \text{(Identity Law for Multiplication).}
\end{aligned}
$$

□

Exercise 2.3.6 (Used in Lemma 2.3.7). Prove Lemma 2.3.7. [Use Exercise 2.3.5 (3).]

Proof.

(1) Let $x, y \in I$, and suppose that $x \leq y$. Suppose further that $p \in [x, y]$. Then $x \leq p \leq y$. Without loss of generality, suppose that $I = (z, w)$ for some $z, w \in \mathbb{R}$. Then $z < x \leq p \leq y < w$, and as a result $z < p < w$. Hence $p \in I$, and therefore $[x, y] \subseteq I$.

(2) Suppose that I is an open interval. Let $x \in I$. There are now four cases. First, suppose that $I = (p, q)$ for some $p, q \in \mathbb{R}$. Then $p < x < q$. From Exercise 2.3.5 (3) we observe that

$$p < \frac{p+x}{2} < x < \frac{x+q}{2} < q.$$

Without loss of generality, suppose that $x - p < q - x$. Then $p > 2x - q$. Let $\delta = \frac{x-p}{2}$. Because $x > p$ it follows that $\delta > 0$, and hence $x - \delta < x + \delta$. We deduce that

$$p < x - \delta = x - \frac{x-p}{2} = \frac{p+x}{2} < x < q.$$

Hence $x - \delta \in I$. We also deduce that

$$p < x < x + \delta = x + \frac{x-p}{2} = \frac{3x-p}{2} < \frac{3x-(2x-q)}{2} = \frac{x+q}{2} < q.$$

Hence $x + \delta \in I$. Using Part (1) of this lemma we can conclude that $[x - \delta, x + \delta] \subseteq I$.

Second, suppose that $I = (p, \infty)$ for some $p \in \mathbb{R}$. Then $x > p$. Let $\delta = \frac{x-p}{2}$. Then by the previous paragraph we deduce that $\delta > 0$ and $x - \delta < x + \delta$ and $x - \delta \in I$. But since $p < x + \delta$ we also deduce that $x + \delta \in I$, and hence by Part (1) of this lemma it follows that $[x - \delta, x + \delta] \subseteq I$.

Third, suppose that $I = (-\infty, q)$ for some $q \in \mathbb{R}$. This case is just like the previous case, and we omit details.

Fourth, suppose that $I = (-\infty, \infty)$. Let $\delta = 1$. Then $\delta > 0$ and $x - 1 < x + 1$. Because $I = \mathbb{R}$ we obtain $x - 1, x + 1 \in I$. Finally, Part (1) of this lemma implies that $[x - \delta, x + \delta] \subseteq I$. □

Exercise 2.3.7 (Used in Lemma 2.3.9). Prove Lemma 2.3.9 (1) (3) (7).

Proof.

(1) First, suppose that $a \geq 0$. Then $|a| = a \geq 0$. If $|a| = 0$, then $|a| = a = 0$, and if $a = 0$, then $0 = a = |a|$.

Second, suppose that $a < 0$. Then $-a > 0$ and $|a| = -a$. Hence, $|a| \geq 0$. If $|a| = 0$, then $|a| = -a = -0 = 0$, and if $a = 0$, then $0 = -0 = -a = |a|$.

(3) Suppose that $|a| = |b|$. We consider the following four cases.

Case 1. $a \geq 0$ and $b \geq 0$. Then $|a| = a$ and $|b| = b$. Hence, $a = b$.

Case 2. $a < 0$ and $b \geq 0$. Then $|a| = -a$ and $|b| = b$, so $-a = b$, and as a result $a = -b$.

Case 3. $a \geq 0$ and $b < 0$. A similar arguments shows that $a = -b$.

Case 4. $a < 0$ and $b < 0$. Then $|a| = -a$ and $|b| = -b$, so $-a = -b$, and as a result $a = b$.

Thus, there is either $a = b$ or $a = -b$.

Now suppose that there is either $a = b$ or $a = -b$. First, suppose that $a = b$, or in other words $-a = -b$. Then there is either $a \geq 0$ and $b \geq 0$ or $a < 0$ and $b < 0$, so there is either $|a| = a$ and $|b| = b$ or $|a| = -a$ and $|b| = -b$. Hence, $|a| = |b|$. Second, suppose that $a = -b$, or in other words $-a = b$. Then there is either $a \geq 0$ and $b < 0$ or $a < 0$ and $b \geq 0$, so there is either $|a| = a$ and $|b| = -b$ or $|a| = -a$ and $|b| = b$. Hence, $|a| = |b|$.

(7) Suppose that $|a| - |b| \geq 0$. Using the Triangle Inequility we deduce that

$$\begin{aligned} |b| = |(a+b) + (-a)| \leq |a+b| + |-a| = |a+b| + |a| \\ \iff |b| \leq |a+b| + |a| \\ \iff |b| - |a| \leq |a+b| \\ \iff -(|a| - |b|) \leq |a+b| \\ \iff |a| - |b| \geq -|a+b| \end{aligned}$$

and that

$$\begin{aligned} |a| = |(a+b) + (-b)| \leq |a+b| + |-b| = |a+b| + |b| \\ \iff |a| - |b| \leq |a+b|. \end{aligned}$$

Thus, $-|a+b| \leq |a| - |b| \leq |a+b|$. By Part (4) of this lemma we then deduce that $||a| - |b|| \leq |a+b|$. A similar argument shows that $||a| - |b|| \leq |a-b|$. □

Exercise 2.3.8 (Used throughout). Let $I \subseteq \mathbb{R}$ be an open interval, let $c \in I$ and let $\delta > 0$. Prove that there is some $x \in I - \{c\}$ such that $|x - c| < \delta$.

[Use Exercise 2.3.5 (3).]

Proof. Using Lemma 2.3.7 (2) we can find some $\delta_c > 0$ such that $[c-\delta_c, c+\delta_c] \subseteq I$. Suppose that $\delta_c < \delta$. Let $x = c + \delta_c$. Clearly, $x \in I - \{c\}$. We observe that $-\delta < \delta_c < \delta$, and by Lemma 2.3.9 (4) we deduce that $|\delta_c| < \delta$. Then,

$$|x - c| = |(c + \delta_c) - c| = |\delta_c| < \delta.$$

Now suppose that $\delta_c \geq \delta$. Let $x = c + \frac{\delta}{2}$. From Exercise 2.3.5 (3) it follows that $0 < \frac{\delta}{2} < \delta < \delta_c$. Then $x \neq c$ and $c - \delta < x < c + \delta_c$, and hence $x \in I - \{c\}$. Because $-\delta < 0$ we obtain $-\delta < \frac{\delta}{2} < \delta$, and by Lemma 2.3.9 (4) we deduce that $\left|\frac{\delta}{2}\right| < \delta$. Then,

$$|x - c| = \left|\left(c + \frac{\delta}{2}\right) - c\right| = \left|\frac{\delta}{2}\right| < \delta.$$

□

Exercise 2.3.9 (Used in Theorem 10.4.4 and Exercise 10.4.4). Let $a \in \mathbb{R}$, let $R \in (0, \infty)$ and let $x \in (a - R, a + R)$. Prove that there is some $P \in (0, R)$ such that $x \in (a - P, a + P)$.

Proof. Because $x \in (a - R, a + R)$ we obtain $a - R < x < a + R$, or in other words $-R < x - a < R$, which means that $x - a \in (-R, R)$. Because of Lemma 2.3.7 (2) we can find some $\delta > 0$ such that

$$[(x - a) - \delta,\ (x - a) + \delta] \subseteq (-R, R).$$

Suppose that $x - a \geq 0$. Let $P = (x - a) + \delta$. It then follows that $0 < P < R$, and as a result $-R < -P < 0$. Hence, $P \in (0, R)$. Because of hypothesis on $x - a$ we see that $-P < x - a < P$, or in other words $a - P < x < a + P$, and hence $x \in (a - P, a + P)$. A similar argument shows that if $x - a < 0$ then $x \in (a - P, a + P)$ where $P = (x - a) - \delta \in (0, R)$. □

Exercise 2.3.11 (Used throughout). Let $A \subseteq \mathbb{R}$ be a set. Prove that A is bounded if and only if there is some $M \in \mathbb{R}$ such that $M > 0$ and that $|x| \leq M$ for all $x \in A$.

Proof. Suppose that A is bounded. According to Definition 2.2.2 this means that A is bounded below and above, so there is some $L, U \in \mathbb{R}$ such that $L \leq x \leq U$ for all $x \in A$. Let $M = |L| + |U|$. Clearly, $M \in \mathbb{R}$. From Lemma 2.3.9 (1) we see that $|L| \geq 0$ and $|U| \geq 0$, and hence $M > 0$. We also deduce that $|L| \leq M$ and $|U| \leq M$, and because of Lemma 2.3.9 (4) we observe that $-M \leq L \leq M$ and $-M \leq U \leq M$. Then $-M \leq x \leq M$ for all $x \in A$, and hence $|x| \leq M$ for all $x \in A$.

Now suppose that there is some $M \in \mathbb{R}$ such that $M > 0$ and $|x| \leq M$ for all $x \in A$. From Lemma 2.3.9 (4) we deduce that $-M \leq x \leq M$ for all $x \in A$. By Definition 2.2.2 it follows that $-M$ is a lower bound of A and M is an upper bound of A. Hence, A is bounded. □

Exercise 2.3.12 (Used in Lemma 2.3.10). Prove Lemma 2.3.10 (2).

Proof. Suppose that $a \geq 0$, and let $\varepsilon > 0$. Then $-\varepsilon < 0$, and then $\varepsilon < 0 \leq a$. Hence, $a > -\varepsilon$.

Now suppose that $a > -\varepsilon$ for all $\varepsilon > 0$. Suppose to the contrary that $a < 0$. Then $-a > 0$, and then $a > -(-a) = a$, which is a contradiction to the fact that $a = a$. Hence, $a \geq 0$. □

Exercise 2.3.13 (Used in Exercise 2.5.15). Let $a, b, x, y \in \mathbb{R}$. Suppose that $a \leq x \leq b$ and $a \leq y \leq b$. Prove that $|x - y| \leq b - a$.

Proof. We deduce that

$$x - b \leq 0 = b - b \quad \text{and} \quad a - a = 0 \leq y - a.$$

Then $x - b \leq y - a$, and then $x - y \leq b - a$. Similarly, we also deduce that

$$a - a = 0 \leq x - a \quad \text{and} \quad y - b \leq 0 = b - b.$$

Then $y - b \leq x - a$, and then $x - y \geq a - b = -(b - a)$. Thus, $-(b - a) \leq x - y \leq b - a$, and by Lemma 2.3.9 (4) we can conclude that $|x - y| \leq b - a$. □

4. Finding the Natural Numbers, the Integers and the Rational Numbers in the Real Numbers

Definition 2.4.1. *Let $S \subseteq \mathbb{R}$ be a set. The set S is* ***inductive*** *if it satisfies the following two properties.*

(a) $1 \in S$.
(b) If $a \in S$, then $a + 1 \in S$.

Definition 2.4.2. *The set of* ***natural numbers****, denoted $\mathbb{N}$, is the intersection of all inductive subsets of $\mathbb{R}$.*

Lemma 2.4.3.

(1) $\mathbb{N}$ is inductive.
(2) If $A \subseteq \mathbb{R}$ and A is inductive, then $\mathbb{N} \subseteq A$.
(3) If $n \in \mathbb{N}$ then $n \geq 1$.

Theorem 2.4.4 (Peano Postulates). *Let $s : \mathbb{N} \to \mathbb{N}$ be defined by $s(n) = n + 1$ for all $n \in \mathbb{N}$*

(a) There is no $n \in \mathbb{N}$ such that $s(n) = 1$.
(b) The function s is injective.
(c) Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.

Lemma 2.4.5. *Let $a, b \in \mathbb{N}$. Then $a + b \in \mathbb{N}$ and $ab \in \mathbb{N}$.*

Theorem 2.4.6 (Well-Ordering Principle). *Let $G \subseteq \mathbb{N}$ be a non-empty set. Then there is some $m \in G$ such that $m \leq g$ for all $g \in G$.*

Definition 2.4.7. *Let*

$$-\mathbb{N} = \{x \in \mathbb{R} \mid x = -n \text{ for some } n \in \mathbb{N}\}.$$

The set of ***integers****, denoted $\mathbb{Z}$, is defined by*

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}.$$

Lemma 2.4.8.

(1) $\mathbb{N} \subseteq \mathbb{Z}$.
(2) $a \in \mathbb{N}$ if and only if $a \in \mathbb{Z}$ and $a > 0$.
(3) The three sets $-\mathbb{N}$, $\{0\}$ and $\mathbb{N}$ are mutually disjoint.

Lemma 2.4.9. *Let $a, b \in \mathbb{Z}$. Then $a + b \in \mathbb{Z}$, and $ab \in \mathbb{Z}$, and $-a \in \mathbb{Z}$.*

Theorem 2.4.10. *Let $a, b \in \mathbb{Z}$.*

(1) If $a < b$ then $a + 1 \leq b$.
(2) There is no $c \in \mathbb{Z}$ such that $a < c < a + 1$.
(3) If $|a - b| < 1$ then $a = b$.

Definition 2.4.11. *The set of* ***rational numbers****, denoted $\mathbb{Q}$, is defined by*

$$\mathbb{Q} = \{x \in \mathbb{R} \mid x = \frac{a}{b} \text{ for some } a, b \in \mathbb{Z} \text{ such that } b \neq 0\}.$$

The set of ***irrational numbers*** *is the set $\mathbb{R} - \mathbb{Q}$.*

Lemma 2.4.12.

(1) $\mathbb{Z} \subseteq \mathbb{Q}$.
(2) $q \in \mathbb{Q}$ and $q > 0$ if and only if $q = \frac{a}{b}$ for some $a, b \in \mathbb{N}$.

Lemma 2.4.13. *Let $a, b, c, d \in \mathbb{Z}$. Suppose that $b \neq 0$ and $d \neq 0$.*

(1) $\frac{a}{b} = 0$ if and only if $a = 0$.
(2) $\frac{a}{b} = 1$ if and only if $a = b$.
(3) $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.
(4) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
(5) $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.
(6) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
(7) If $a \neq 0$, then $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Corollary 2.4.14. *Let $a, b \in \mathbb{Q}$. Then $a + b \in \mathbb{Q}$ and $ab \in \mathbb{Q}$, and $-a \in \mathbb{Q}$, and if $a \neq 0$ then $a^{-1} \in \mathbb{Q}$.*

Lemma 2.4.15 (Not in the book). *Let $q \in \mathbb{Q}$. Then there is some $n \in \mathbb{N}$ such that $q < n$.*

Proof. Suppose to the contrary that $q \geq n$ for all $n \in \mathbb{N}$. From Lemma 2.4.3 (2) we know that $\mathbb{N}$ is inductive, so $1 \in \mathbb{N}$. By hypothesis on q, we have $q \geq 1 > 0$. We then deduce that $q \notin -\mathbb{N} \subseteq \mathbb{Z}$, which is a contradiction to Lemma 2.4.12 (1). Hence, there is some $n \in \mathbb{N}$ such that $q < n$. □

Exercise 2.4.1 (Used in Lemma 2.4.9). Let $a, b \in \mathbb{N}$. Prove that $a > b$ if and only if $a - b \in \mathbb{N}$ if and only if there is some $d \in \mathbb{N}$ such that $b + d = a$.

Proof. Suppose that $a > b$. By Lemma 2.4.8 (1) we know that $a, b \in \mathbb{Z}$. Then,

$$a - b = a + (-b) > b + (-b) = 0 \quad \text{and} \quad a - b \in \mathbb{Z}.$$

Using Lemma 2.4.8 (2) it follows that $a - b \in \mathbb{N}$. This process can be done backwards, and hence $a > b$ if and only if $a - b \in \mathbb{N}$.

Now suppose that $a > b$. Then $a - b \in \mathbb{N}$. Let $d = a - b$. We then deduce that $d \in \mathbb{N}$ and $b + d = b + (a - b) = a$. Finally, suppose that there is some $d \in \mathbb{N}$ such that $b + d = a$. By Lemma 2.4.8 (2) we have $a, b, d \in \mathbb{Z}$. Then,

$$\begin{aligned} d &= d + 0 = d + (b + (-b)) = (d + b) + (-b) \\ &= (b + d) + (-b) = a + (-b) \\ &= a - b. \end{aligned}$$

Because $d \in \mathbb{N}$, we conclude that $a - b \in \mathbb{N}$, or in other words $a > b$. □

Exercise 2.4.3 (Used in Theorem 2.5.4 and Exercise 2.5.13). Let $n \in \mathbb{N}$. Suppose that $n \neq 1$. Prove that there is some $b \in \mathbb{N}$ such that $b + 1 = n$.

Proof. From Lemma 2.4.8 (2) we know that $n \in \mathbb{Z}$ and $n > 0$. By Theorem 2.4.10 it follows that $0 + 1 \leq n$, and because $n \neq 1$ we obtain $n > 1$. Let $b = n - 1$. We have

$$b = n - 1 = n + (-1) > 1 + (-1) = 0,$$

and hence by Lemma 2.4.8 (2) we get $b \in \mathbb{N}$. Finally, we deduce that

$$\begin{aligned} b + 1 &= (n - 1) + 1 = (n + (-1)) + 1 \\ &= n + ((-1) + 1) = n + (1 + (-1)) \\ &= n + 0 = n. \end{aligned}$$

□

Exercise 2.4.4. Let $a, b \in \mathbb{Z}$. Prove that if $ab = 1$, then $a = 1$ and $b = 1$, or $a = -1$ and $b = -1$.

Proof. Suppose that $ab = 1$. By Lemma 2.4.12 (1) and the definition of rational numbers we see that $a, b \in \mathbb{Q} \subseteq \mathbb{R}$. From Lemma 2.3.5 we deduce that either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.

First, suppose that $a > 0$ and $b > 0$. By Theorem 2.4.10 (1) it follows that $a \geq 1$ and $b \geq 1$. Suppose to the contrary that either $a \neq 1$ or $b \neq 1$. Without loss of generality, suppose that $a \neq 1$, so $a > 1$. If $b = 1$, then $ab = a \cdot 1 = a > 1$, which is a contradiciton. If $b > 1$, then $ab > 1$, which is again a contradiction. Hence, $a = b = 1$.

Second, suppose that $a < 0$ and $b < 0$. Then $-a > 0$ and $-b > 0$. This part is just like the previous paragraph, and hence $-a = -b = 1$, or in other words $a = b = -1$. □

Exercise 2.4.5 (Used in Section 2.6 and Exercise 2.6.12). Prove that there is no $n \in \mathbb{Z}$ such that $n^2 = 2$.

Proof. Suppose to the contrary that there is some $n \in \mathbb{Z}$ such that $n^2 = 2$. Clearly $n \neq 0$. By Lemma 2.4.12 (1) and the definition of rational numbers we see that $n \in \mathbb{Q} \subseteq \mathbb{R}$. We note that $|n| \cdot |n| = n^2$, and because $n \in \mathbb{Z}$ we have $|n| \in \mathbb{Z}$ also. Let $m = 1$. We deduce that

$$1 = m^2 < n^2 < (m+1)^2 = 4.$$

Using Lemma 2.3.9 (1) we observe that $|n| > 0$. From Lemma 2.3.3 (14) it follows that $m < |n| < m + 1$, which is a contradiction to Lemma 2.4.10 (2). Hence, there is no $n \in \mathbb{Z}$ such that $n^2 = 2$. □

Exercise 2.4.6 (Used in Theorem 2.6.13). Let $q \in \mathbb{Q}$ and $x \in \mathbb{R} - \mathbb{Q}$.

(1) Prove that $q + x \in \mathbb{R} - \mathbb{Q}$.
(2) Prove that if $q \neq 0$ then $qx \in \mathbb{R} - \mathbb{Q}$.

Proof of (1). We note that $\mathbb{Q} \subseteq \mathbb{R}$ because of the definition of rational numbers. Suppose to the contrary that $q + x \in \mathbb{Q}$. Let $c = q + x$. From Corollary 2.4.14 we observe that $-q \in \mathbb{Q}$ and that $c - q \in \mathbb{Q}$. We then deduce that

$$c - q = (q + x) - q = (x + q) - q = x + (q - q) = x + 0 = x,$$

and as a result $x \in \mathbb{Q}$, which is a contradiction to hypothesis on x. Hence, we can conclude that $q + x \in \mathbb{R} - \mathbb{Q}$. □

Proof of (2). We note that $\mathbb{Q} \subseteq \mathbb{R}$ because of the definition of rational numbers. Suppose that $q \neq 0$, and suppose to the contrary that $qx \in \mathbb{Q}$. Let $c = qx$. From Corollary 2.4.14 we observe that $q^{-1} \in \mathbb{Q}$ and that $cq^{-1} \in \mathbb{Q}$. We then deduce that

$$cq^{-1} = (qx)q^{-1} = (xq)q^{-1} = x(qq^{-1}) = x \cdot 1 = x,$$

and as a result $x \in \mathbb{Q}$, which is a contradiction to hypothesis on x. Hence, we can conclude that $qx \in \mathbb{R} - \mathbb{Q}$. □

Exercise 2.4.7 (Used in Lemma 2.4.12). Prove Lemma 2.4.12 (2).

Proof. Suppose that $q \in \mathbb{Q}$ and $q > 0$. By the definition of rational numbers we know that $q = \frac{a}{b}$ for some $x, y \in \mathbb{Z}$ such that $y \neq 0$. From Lemma 2.3.5 we deduce that either $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$. First, suppose that $x > 0$ and $y > 0$. Let $a = x$ and $b = y$. By Lemma 2.4.8 (2) it follows that $a, b \in \mathbb{N}$. Second, suppose that $x < 0$ and $y < 0$. Let $a = -x$ and $b = -y$. Then $a > 0$ and $b > 0$, and using Lemma 2.4.8 (2) again we can conclude that $a, b \in \mathbb{N}$.

Now suppose that $q = \frac{a}{b}$ for some $a, b \in \mathbb{N}$. From Lemma 2.4.8 (2) we observe that $a, b \in \mathbb{Z}$ and $a > 0$ and $b > 0$. We then deduce that $b \neq 0$, and using the definition of rational numbers we can conclude that $q \in \mathbb{Q}$ and $q > 0$. □

Exercise 2.4.8 (Used in Lemma 2.4.13). Prove Lemma 2.4.13 (2) (3) (5) (6).

Proof.

(2) If $\frac{a}{b} = 1$, then $ab^{-1} = 1$, and therefore

$$a = (bb^{-1})a = b(b^{-1}a) = b(ab^{-1}) = b \cdot 1 = b.$$

If $a = b$, then $\frac{a}{b} = ab^{-1} = bb^{-1} = 1$.

(3) Suppose that $\frac{a}{b} = \frac{c}{d}$. Then $ab^{-1} = cd^{-1}$, and then

$$\begin{aligned} ad &= ad(b^{-1}b) = a(b^{-1}b)d = (ab^{-1})(bd) \\ &= (cd^{-1})(bd) = (bd)(d^{-1}c) = b(dd^{-1})c = bc. \end{aligned}$$

Now suppose that $ad = bc$. Then

$$\begin{aligned} \frac{a}{b} &= ab^{-1} = a(dd^{-1})b^{-1} = (ad)(d^{-1}b^{-1}) \\ &= (bc)(d^{-1}b^{-1}) = c(bb^{-1})d^{-1} = cd^{-1} = \frac{c}{d}. \end{aligned}$$

(5) We have $-(ab^{-1}) = (-a)b^{-1} = a(-b^{-1})$, or in other words

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

(6) We compute

$$\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1} = \frac{ac}{bd}.$$

□

Exercise 2.4.9 (Used in Theorem 2.7.1). Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Prove that $\frac{a}{b} < \frac{c}{d}$ if and only if either $cb - ad > 0$ and $bd > 0$, or $cb - ad < 0$ and $bd < 0$.

Proof. Suppose that $\frac{a}{b} < \frac{c}{d}$. Then $ab^{-1} < cd^{-1}$. There is either $bd > 0$ or $bd < 0$. If $bd > 0$, then

$$\begin{aligned} ad &= a(bb^{-1})d = (ab^{-1})(bd) \\ &< (cd^{-1})(bd) = c(d^{-1}d)b = cb, \end{aligned}$$

and as a result $cb - ad > 0$. If $bd < 0$, then $ad = (ab^{-1})(bd) > (cd^{-1})(bd) = cb$, and as a result $cb - ad < 0$.

Now suppose that either $cb - ad > 0$ and $bd > 0$, or $cb - ad < 0$ and $bd < 0$. If $cb - ad > 0$ and $bd > 0$, then $ad < cb$ and $(bd)^{-1} > 0$, and therefore

$$\begin{aligned} \frac{a}{b} &= ab^{-1} = a(dd^{-1})b^{-1} = (ad)(b^{-1}d^{-1}) = (ad)(bd)^{-1} \\ &< (cb)(bd)^{-1} = (cb)(b^{-1}d^{-1}) = c(bb^{-1})d^{-1} = cd^{-1} = \frac{c}{d}. \end{aligned}$$

If $cb - ad < 0$ and $bd < 0$, then $ad > cb$ and $(bd)^{-1} < 0$, and therefore $\frac{a}{b} = (ad)(bd)^{-1} < (cb)(bd)^{-1} = \frac{c}{d}$. □

Lemma 2.4.15 (Not in the book). *Let $q \in \mathbb{Q}$. Then there is some $n \in \mathbb{N}$ such that $q < n$.*

Exercise 2.4.10 (Used in Section 3.5). Let $a, b \in \mathbb{Q}$. Suppose that $a > 0$. Prove that there is some $n \in \mathbb{N}$ such that $b < na$. Use only the material in Sections 2.3 and 2.4; do not use the Least Upper Bound Property.

Proof. We note that $a \neq 0$ because $a > 0$. By Corollary 2.4.14 we observe that $a^{-1} \in \mathbb{Q}$ and that $ba^{-1} \in \mathbb{Q}$. From Lemma 2.4.15 we see that there is some $n \in \mathbb{N}$ such that $ba^{-1} < n$, so $(ba^{-1})a < na$. Then

$$(ba^{-1})a = b(a^{-1}a) = b < na,$$

as required. □

5. Induction and Recursion in Practice

Theorem 2.5.4 (Principle of Mathematical Induction—Variant). *TBD*

Exercise 2.5.13. TBD

Proof. TBD □

Exercise 2.5.15. TBD

Proof. TBD □

6. The Least Upper Bound Property and Its Consequences

Theorem 2.6.13. *TBD*

Exercise 2.6.12. TBD

Proof. TBD □

7. Uniqueness of the Real Numbers

Theorem 2.7.1 (Uniqueness of the Real Numbers). *TBD*

8. Decimal Expansion of Real Numbers

Exercise 2.8.9. TBD

Proof. TBD □

Limits and Continuity

5. Two Important Theorems

Sequences and Series of Functions

4. Functions as Power Series

Theorem 10.4.4. *TBD*

Exercise 10.4.4. TBD

Proof. TBD □

Bibliography

[1] Ethan D. Bloch, **The Real Numbers and Real Analysis**, 1st ed., Springer, 2011.