The Real Numbers and Real Analysis
Ethan Bloch

Noah Lewis

November 15, 2025

Contents

1 Construction of the Real Numbers 1
1.1 Axioms for the Natural Numbers . . . 1
1.2 Constructing the Integers . . . 7
1.3 Axioms for the Integers . . . 15
1.4 Constructing the Rational Numbers . . . 18
1.5 Dedekind Cuts . . . 25

1 Construction of the Real Numbers

1.1 Axioms for the Natural Numbers

Problem 1

Fill in the missing details in the proof of Theorem 1.2.6.

Proof. We must show the uniquness of the 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. $n \cdot s(m) = (n \cdot m) + n$.

Suppose there are two binary operations $\cdot$ and $\times$ on $\mathbb{N}$ that satisfy the two properties for all $n, m \in \mathbb{N}$. Let

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

We will prove that $G = \mathbb{N}$, which will imply that $\cdot$ and $\times$ are the same binary operation. It is clear that $G \subseteq \mathbb{N}$. By part (a) applied to each of $\cdot$ and $\times$ we see that $n \cdot 1 = n = n \times 1$ for all $n \in \mathbb{N}$ and hence $1 \in G$. Now let $q \in G$. Let $n \in \mathbb{N}$. Then $n \cdot q = n \times q$ by hypothesis on q. It then follows from part (b) that $n \cdot s(q) = (n \cdot q) + n = (n \times q) + n = n \times s(q)$. Hence $s(q) \in G$. By part (c) of the Peano Postulates we conclude that $G = \mathbb{N}$. ∎

Proof. We must show the two properties hold. Now, $n \cdot 1 = g_n(1) = n$, which is part (a), and $n \cdot s(m) = g_n(s(m)) = (g_n \circ s)(m) = (h_n \circ g_n)(m) = g_n(m) + n = (n \cdot m) + n$, which is part (b). ∎

Problem 2

Prove Theorem 1.2.7 (2) (3) (4) (7) (8) (9) (10) (11) (13).

Proof. Let $a, b, c \in \mathbb{N}$. We must show $(a+b)+c = a+(b+c)$. Consider the set

$$G = \{z \in \mathbb{N} \mid \text{if } x, y \in \mathbb{N} \text{ then } (x+y)+z = x+(y+z)\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Suppose $z \in G$. Consider

$$(x+y)+1 = s(x+y) = x+s(y) = x+(y+1)$$

Thus $1 \in G$. Futher let $x, y, z \in \mathbb{N}$, and consider

$$(x+y)+s(z) = s((x+y)+z)$$

By our hypothesis on z, $(x+y)+z = x+(y+z)$ so

$$s((x+y)+z) = s(x+(y+z)) = x+s(y+z) = x+(y+s(z))$$

So $s(z) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a \in \mathbb{N}$. We must show $1+a = s(a) = a+1$. Consider the set

$$G = \{a \in \mathbb{N} \mid 1+a = s(a) = a+1\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Let $a \in \mathbb{N}$ such that $a = 1$.

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

Thus $1 \in G$. Suppose $x \in \mathbb{N}$ and $x \in G$. By our hypothesis, $1+x = x+1$. Then

$$1+s(x) = s(1+x) = s(x+1) = s(x)+1$$

So $s(x) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a, b \in \mathbb{N}$. We must show $a+b = b+a$. Consider the set

$$G = \{x \in \mathbb{N} \mid \text{if } y \in \mathbb{N} \text{ then } x+y = y+x\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Let $x \in \mathbb{N}$. By Theorem 1.2.7 part (3), $1+x = x+1$. Thus $1 \in G$. Now suppose $x \in G$. Let $y \in \mathbb{N}$. First note by Theorem 1.2.7 part (2), $1+(x+y) = (1+x)+y$. Consider

$$y+s(x) = s(y+x) = s(x+y) \text{ hypothesis on } x = 1+(x+y) = (1+x)+y = s(x)+y$$

So $s(x) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a \in \mathbb{N}$. We must show $a \cdot 1 = a = 1 \cdot a$. Consider the set

$$G = \{x \in \mathbb{N} \mid x \cdot 1 = x = 1 \cdot x\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Consider

$$\begin{aligned} x \cdot 1 &= x && \text{Theorem 1.2.6 part (a)} \\ &= 1 \\ &= 1 \cdot 1 \\ &= x \cdot 1 \end{aligned}$$

Thus $1 \in G$. Consider

$$\begin{aligned} s(x) \cdot 1 &= s(x) && \text{Theorem 1.2.6 part (a)} \\ &= x+1 && \text{Theorem 1.2.5 part (a)} \\ &= x \cdot 1 + 1 && \text{Theorem 1.2.6 part (a)} \\ &= 1 \cdot x + 1 && \text{Induction hypothesis} \\ &= 1 \cdot s(x) && \text{Theorem 1.2.6 part (b)} \end{aligned}$$

So $s(x) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show $(a+b)c = ac + bc$. Consider the set

$$G = \{c \in \mathbb{N} \mid \text{if } a, b \in \mathbb{N} \text{ then } (a+b)c = ac + bc\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Let $a, b \in \mathbb{N}$. Then

$$\begin{aligned} (a+b)1 &= a + b && \text{(Theorem 1.2.6 part (a))} \\ &= a \cdot 1 + b \cdot 1 && \text{(Theorem 1.2.6 part (a))} \end{aligned}$$

Suppose $a, b, c \in \mathbb{N}$ and $c \in G$. Then

$$\begin{aligned} (a+b) \cdot s(c) &= ((a+b)c) + (a+b) && \text{(Theorem 1.2.6 part (a))} \\ &= (ac + bc + a + b) && \text{(Induction Hypothesis)} \\ &= (ac + a + bc + b) && \text{(Theorem 1.2.7 part (4))} \\ &= a \cdot s(c) + b \cdot s(c) && \text{(Theorem 1.2.5 part (a))} \end{aligned}$$

So $s(c) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a, b \in \mathbb{N}$. We must show $ab = ba$. Consider the set

$$G = \{a \in \mathbb{N} \mid \text{if } b \in \mathbb{N} \text{ then } ab = ba\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. By Theorem 1.2.7 part (7), $a \cdot 1 = 1 \cdot a$. Thus $1 \in G$. Suppose $a, b \in \mathbb{N}$ and $a \in G$.

$$\begin{aligned} s(a) \cdot b &= (a+1)b && \text{(Theorem 1.2.5 part (a))} \\ &= ab + 1b && \text{(Theorem 1.2.7 part (8))} \\ &= ab + b1 && \text{(Theorem 1.2.7 part (7))} \\ &= ab + b && \text{(Theorem 1.2.6 part (7))} \\ &= ba + b && \text{(Induction Hypothesis)} \\ &= b \cdot s(a) && \text{(Theorem 1.2.6 part (b))} \end{aligned}$$

So $s(a) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a, b \in \mathbb{N}$. We must show $c(a+b) = ca + cb$. By Theorem 1.2.7 part (9), $c(a+b) = (a+b)c$. By Theorem 1.2.7 part (8), $(a+b)c = ac + bc$. By Theorem 1.2.7 part (9), $ac + bc = ca + cb$. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show $(ab)c = a(bc)$. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show $(ab)c = a(bc)$. Consider the set

$$G = \{c \in \mathbb{N} \mid \text{if } a, b \in \mathbb{N} \text{ then } (ab)c = a(bc)\}$$

We will show $G = \mathbb{N}$. Clearly $G \subseteq \mathbb{N}$. We first show $1 \in G$. Let $a, b \in \mathbb{N}$. Then

$$(ab)1 = ab \text{ (Theorem 1.2.7 part (7))} \;\; = a(b \cdot 1) \text{ (Theorem 1.2.6 part (a))}$$

Thus $1 \in G$. Suppose $a, b, c \in \mathbb{N}$ and $c \in G$. Then

$$\begin{aligned} (ab) \cdot s(c) &= (ab)(c+1) && \text{(Theorem 1.2.5 part (a))} \\ &= (ab)c + (ab)1 && \text{(Theorem 1.2.7 part (10))} \\ &= a(bc) + (ab)1 && \text{(Induction Hypothesis)} \\ &= a(bc) + ab && \text{(Theorem 1.2.7 part (7))} \\ &= a(bc + b) && \text{(Theorem 1.2.7 part (8))} \\ &= a(bc + b \cdot 1) && \text{(Theorem 1.2.7 part (7))} \\ &= a(b(c+1)) && \text{(Theorem 1.2.7 part (8))} \\ &= a(b \cdot s(c)) && \text{(Theorem 1.2.5 part (a))} \end{aligned}$$

So $s(c) \in G$. Thus $G = \mathbb{N}$ by part (c) of the Peano Postulates. ∎

Proof. Let $a, b \in \mathbb{N}$. We must show $ab = 1$ if and only if $a = 1 = b$.

Suppose $ab = 1$. For contradiction, suppose $a \neq 1$ or $b \neq 1$. Suppose $a \neq 1$. By Lemma 1.2.3 there exists $c \in \mathbb{N}$ such that $s(c) = a$. Then

$$ab = s(c)b = (c+1)b \text{ (Theorem 1.2.5 part (a)) } = cb + b \text{ (Theorem 1.2.7 part (8)) } = 1$$

Contradicting Theorem 1.2.7 part (5). Suppose $b \neq 1$. By Lemma 1.2.3 there exists $c \in \mathbb{N}$ such that $s(c) = b$. Then

$$ab = a \cdot s(c) = a(c+1) \text{ (Theorem 1.2.5 part (a)) } = ac + a \text{ (Theorem 1.2.7 part (10)) } = 1$$

Contradicting Theorem 1.2.7 part (5).

Suppose $a = 1 = b$. Then $ab = a \cdot 1 = a = 1$ by Theorem 1.2.6 part (a). ∎

Problem 3

Let $a, b \in \mathbb{N}$. Suppose $a < b$. Prove that there is a unique $p \in \mathbb{N}$ such that $a + p = b$

Proof. We first prove uniqueness. Let $a, b \in \mathbb{N}$ such that $a < b$. Suppose $x, y \in \mathbb{N}$ such that $a + x = b$ and $a + y = b$. Then $a + x = a + y$. By Theorem 1.2.7 part (4), $x + a = y + a$. Then by Theorem 1.2.7 part (1), $x = y$.

We now prove existence. Since $a < b$, by definition of $<$ there exists $p \in \mathbb{N}$ such that $a + p = b$. ∎

Problem 4

Prove Theorem 1.2.9 (1) (3) (4) (5) (11).

Proof. Let $a \in \mathbb{N}$. We must show $a \leq a$, and $a \nless a$, and $a < a + 1$.

To show $a \leq a$, suppose for contradiction $a = a$. Thus $a \leq a$. To show $a \nless a$, first, suppose $a < a$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $a + p = a$ contradicting Theorem 1.2.7 part (6). To show $a < a + 1$ consider $s(a) = a + 1 = a + 1$ thus $a < a + 1$. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show 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 $a \leq c$.

① Suppose $a < b$ and $b < c$. By definition of $<$, there exists $p_1, p_2 \in \mathbb{N}$ such that $a + p_1 = b$ and $b + p_2 = c$. Then $b + p_2 = (a + p_1) + p_2 = c$. By definition of $<$, $a < c$.

② Suppose $a \leq b$ and $b < c$. By definition of $\leq$, either $a = b$ or $a < b$. Suppose $a < b$. By ①, $a < c$. Suppose $a = b$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $b + p = c$. Then $b + p = a + p = c$. By definition of $<$, $a < c$.

③ Suppose $a < b$ and $b \leq c$. By definition of $\leq$, either $b = c$ or $b < c$. Suppose $b < c$. By ①, $a < c$. Suppose $b = c$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $a + p = b$. Then $b = a + p = c$ thus, by definition of $<$, $a < c$.

Suppose $a \leq b$ and $b \leq c$. There are four cases:

1. Suppose $a < b$ and $b < c$. By ①, $a < c$.
2. Suppose $a \leq b$ and $b < c$. By ②, $a < c$.
3. Suppose $a < b$ and $b \leq c$. By ③, $a < c$.
4. Suppose $a \leq b$ and $b \leq c$. There are four cases:
   (a) Suppose $a = b$ and $b < c$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $b + p = c$. Then $b + p = a + p = c$ so $a < c$.

(b) Suppose $a < b$ and $b < c$. By ①, $a < c$.

(c) Suppose $a = b$ and $b = c$. Clearly $a = b = c$ thus $a = c$.

(d) Suppose $a < b$ and $b = c$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $a + p = b$. Then $a + p = b = c$ so $a < c$.

Thus either $a < c$ or $a = c$ thus, by definition of $\leq$, $a \leq c$. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show if $a < b$ if and only if $a + c < b + c$.

Suppose $a < b$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $a + p = b$. By Theorem 1.2.7 part (1), $(a + p) + c = b + c$. By Theorem 1.2.7 part (2), $a + (p + c) = b + c$. By Theorem 1.2.7 part (4), $a + (c + p) = b + c$. By Theorem 1.2.7 part (2), $(a + c) + p = b + c$. Thus by definition of $<$, $a + c < b + c$.

Suppose $a + c < b + c$. There exists $p \in \mathbb{N}$ such that $(a + c) + p = b + c$. By Theorem 1.2.7 part (4), $p + (a + c) = b + c$. By Theorem 1.2.7 part (2), $(p + a) + c = b + c$. By Theorem 1.2.7 part (1), $p + a = b$ so, by Theorem 1.2.7 part (4), $a + p = b$. Thus by definition of $<$, $a < b$. ∎

Proof. Let $a, b, c \in \mathbb{N}$. We must show $a < b$ if and only if $ac < bc$.

Suppose $a < b$. For contradiction, suppose $ac \geq bc$. By definition of $\geq$, either $ac = bc$ or $ac > bc$.

Suppose $ac = bc$. By Theorem 1.2.7 part (12), $a = b$. But $a = b < b$ contradicting Theorem 1.2.9 part (1).

Suppose $ac > bc$. By definition of $<$, there exists $p_1, p_2 \in \mathbb{N}$ such that $a + p_1 = b$ and $bc + p_2 = ac$. Then $bc + p_2 = (a + p_1)c + p_2 = ac + p_1 c + p_2$ (by Theorem 1.2.8 part (8) for distributivity) $= ac$. By definition of $<$, $ac < ac$ contradicting Theorem 1.2.9 part (1).

Suppose $ac < bc$. For contradiction, suppose $a \geq b$. By definition of $\geq$, either $a = b$ or $a > b$

Suppose $a = b$. Then $ac = bc < bc$ which contradicts Theorem 1.2.9 part (1).

Suppose $a > b$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $b + p = a$. Then, by Theorem 1.2.8 part (8), $ac = (b + p)c = bc + pc$. By definition of $<$, $bc < ac$. ∎

Proof. Let $a, b \in \mathbb{N}$. We must show $a < b$ if and only if $a + 1 \leq b$.

Suppose $a < b$. For contradiction, suppose $a + 1 > b$. By definition of $<$, there exists $p_2 \in \mathbb{N}$ such that $a + p_2 = b$. Since $a + 1 > b$, there exists $p_1 \in \mathbb{N}$ such that $b + p_1 = a + 1$. Then $b + p_1 = (a + p_2) + p_1 = a + 1$. By Theorem 1.2.7 part (4), $p_1 + (a + p_2) = 1 + a$. By Theorem 1.2.7 part (4), $p_1 + (p_2 + a) = 1 + a$. By Theorem 1.2.7 part (2), $(p_1 + p_2) + a = 1 + a$. By Theorem 1.2.7 part (1), $p_1 + p_2 = 1$ contradicting Theorem 1.2.7 part (5).

Suppose $a + 1 \leq b$. By definition of $\leq$, either $a + 1 = b$ or $a + 1 < b$.

Suppose $a + 1 = b$. By definition of $<$, $a < b$.

Suppose $a + 1 < b$. For contradiction, suppose $a \geq b$. By definition of $\geq$, either $a = b$ or $a > b$. Suppose $a = b$, then $a + 1 = b + 1 > b$ contradicting Theorem 1.2.7 part (6). Suppose $a > b$. By definition of $<$, there exists $p_1, p_2 \in \mathbb{N}$ such that $(a + 1) + p_1 = b$ and $b + p_2 = a$. Then $(a + 1) + p_1 = ((b + p_2) + 1) + p_1 = b$. By definition of $<$, $b < b$ contradicting Theorem 1.2.9 part (1). ∎

Problem 5

Let $a, b \in \mathbb{N}$. Prove that if $a + a = b + b$, then $a = b$.

Proof. Suppose $a + a = b + b$. First, by Theorem 1.2.6 part (a), $a + a = a \cdot 1 + a \cdot 1$. Then, by Theorem 1.2.7 part (10), $a \cdot 1 + a \cdot 1 = a(1 + 1) = a \cdot 2$. Similarly $b + b = b \cdot 2$. Then, by Theorem 1.2.7 part (12), since $a \cdot 2 = b \cdot 2$, $a = b$. ∎

Problem 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 $A = \{n \in \mathbb{N} \mid 1 \leq n \leq b\}$ and $B = \{n \in \mathbb{N} \mid b+1 \leq n\}$. It is clear that $A \subseteq \mathbb{N}$ and $B \subseteq \mathbb{N}$. Thus $A \cup B \subseteq \mathbb{N}$. Now let x be an arbitrary element in $\mathbb{N}$. By Theorem 1.2.9 part (6), either $x < b$, $x = b$, or $x > b$. Suppose $x < b$. Then $x \in A$, so $x \in A \cup B$. Suppose $x = b$. Then $x \in A$, so $x \in A \cup B$. Suppose $x > b$. Then $x \in B$, so $x \in A \cup B$. Therefore $\mathbb{N} \subseteq A \cup B$. It follows that $A \cup B = \mathbb{N}$.

Suppose $A \cap B \neq \emptyset$. Let $x \in A \cap B$. Then $1 \leq x \leq b$ and $b+1 \leq x$. By Theorem 1.2.9 part (3), $b+1 \leq x \leq b$ contradicting Theorem 1.2.9 part (9). ∎

Problem 7

Let $A \subseteq N$ be a set. The set A is **closed** if $a \in A$ implies $a+1 \in A$. Suppose 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. If $A = \emptyset$ then clearly the implication vacuously holds. Suppose $A \neq \emptyset$. Consider the set

$$G = \{x \in \mathbb{N} \mid a + x \in A\}.$$

We will show $G = \mathbb{N}$, proving our implication. Now, since $a \in A$ and A is closed, $a+1 \in A$, thus $1 \in G$. Suppose $x \in \mathbb{N}$ and $x \in G$. Then consider $a + s(x) = a + (x+1)$. By Theorem 1.2.7 part (2), $a + (x+1) = (a+x)+1$. By our hypothesis, $a + x \in A$. But since A is closed, $(a+x)+1 \in A$. Thus $s(x) \in G$. By the part (c) of the Peano Postulates, we conclude that $G = \mathbb{N}$. ∎

Proof. Suppose $a \in A$. Let $x \in \mathbb{N}$ such that $x \geq a$. Either $x = a$ or $a < x$. Suppose $x = a$, then trivially $x = a \in A$. Suppose $a < x$. By definition of $<$, there exists $p \in \mathbb{N}$ such that $a + p = x$. By the previous proof, $a + p = x \in A$. ∎

Problem 8

Suppose that the set $\mathbb{N}$ together with the element $1 \in \mathbb{N}$ and the function $s : \mathbb{N} \to \mathbb{N}$, and 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.

Proof. We can apply Theorem 1.2.4 to the set $\mathbb{N}'$, the element $1'$ and the function $s' : \mathbb{N}' \to \mathbb{N}'$, to deduce that there is a unique function $f : \mathbb{N} \to \mathbb{N}'$ such that $f \circ s = s' \circ f$ and $f(1) = 1'$.

We can apply Theorem 1.2.4 again, to the set $\mathbb{N}$, the element 1 and the function $s : \mathbb{N} \to \mathbb{N}$, to deduce that there is a unique function $f' : \mathbb{N}' \to \mathbb{N}$ such that $f' \circ s' = s \circ f'$ and $f'(1') = 1$.

Now we must show f' is the inverse of f.

Consider $f' \circ f$. Let $x \in \mathbb{N}$.

Base case: $x = 1$.

$$(f' \circ f)(x) = f'(f(1)) = f'(1') = 1 = x$$

Inductive step: Suppose $x > 1$. By Lemma 1.2.3 there exists $y \in \mathbb{N}$ such that $s(y) = x$. Suppose for $y \in \mathbb{N}$ such that $y < x$, $(f' \circ f)(y) = y$. Then

$$\begin{aligned}
(f' \circ f)(x) &= f'(f(s(y))) \\
&= f'(s'(f(y))) && \text{(by } f \circ s = s' \circ f\text{)} \\
&= s(f'(f(y))) && \text{(by } f' \circ s' = s \circ f'\text{)} \\
&= s(y) && y < x \\
&= x
\end{aligned}$$

Consider $f \circ f'$. Let $x' \in \mathbb{N}'$.

Base case: $x' = 1'$.

$$(f \circ f')(x') = f(f'(1')) = f(1) = 1' = x'$$

Inductive step: Suppose $x' > 1'$. By Lemma 1.2.3 there exists $y' \in \mathbb{N}'$ such that $s'(y') = x'$. Suppose for $y' \in \mathbb{N}'$ such that $y' < x'$, $(f \circ f')(y') = y'$. Then

$$\begin{aligned}
(f \circ f')(x') &= f(f'(s'(y'))) \\
&= f(s(f'(y'))) && \text{(by } f' \circ s' = s \circ f'\text{)} \\
&= s'(f(f'(y'))) && \text{(by } f \circ s = s' \circ f\text{)} \\
&= s'(y') && \text{(induction hypothesis)} \\
&= x'
\end{aligned}$$

Since $(f' \circ f)(x) = x$ and $(f \circ f')(x') = x'$, we conclude that f' is the inverse of f. Thus f is bijective. ∎

Extra Problem

Show the Peano axioms are independent. That is, for any two Peano axioms, find a structure that satisfies them but not the third. You may assume the regular math of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Axiom 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 $G \subseteq \mathbb{N}$. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.*

Proof. (**a., b.**) Let $s : \mathbb{N} \to \mathbb{N}$ be defined by $s(x) = x + 2$. Let $G = \{x \mid \exists k \in \mathbb{Z}, x = 2k + 1\}$. Clearly s is injective, $1 \in G$, and $G \subseteq \mathbb{N}$. But $G \neq \mathbb{N}$, and if $g \in G$ then $s(g) = g + 2 \in G$. Clearly **a., b.** hold while **c.** does not hold.

(**a., c.**) Let $M = \{1, p\}$ and let $s : M \to M$ be defined by $s(1) = p$ and $s(p) = p$. Clearly **a., c.** hold while **b.** does not hold.

(**b., c.**) Let $M = \{1, p\}$ and let $s : M \to M$ be defined by $s(1) = p$ and $s(p) = 1$. Clearly **b., c** hold while **a.** does not hold. ∎

1.2 Constructing the Integers

Problem 2

Complete the proof of Lemma 1.3.2. That is, prove that the relation $\sim$ is transitive.

Proof. Let $(a,b),(c,d),(e,f) \in \mathbb{N}\times\mathbb{N}$. Assume $(a,b)\sim(c,d)$ and $(c,d)\sim(e,f)$. By definition of $\sim$, $a+d=b+c$ and $c+f=d+e$. Then taking sums shows $a+d+c+f=b+c+d+e$. Cancelling terms $a+f=b+e$. Thus, by definition of $\sim$, $(a,b)\sim(f,e)$. Since $\sim$ is symmetric, $(a,b)\sim(e,f)$. ∎

Problem 3

Test 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 $(a,b)\sim(c,d)$ and $(x,y)\sim(z,w)$. So $a+d=b+c$ and $x+w=y+z$. We compute the following equations.

1. $ax+aw=ay+az$. Multiply $x+w=y+z$ by a.
2. $by+bz=bx+bw$. Multiply $y+z=x+w$ by b.
3. $cx+cw=cy+cz$. Multiply $x+w=y+z$ by c.
4. $dy+dz=dx+dw$. Multiply $y+z=x+w$ by d.

Then taking sums.

$$ax+aw+by+bz+cx+cw+dy+dz=ay+az+bx+bw+cy+cz+dx+dw$$

Grouping terms.

$$ax+by+cw+dz+(aw+bz+cx+dy)=ay+bx+cz+dw+(az+bw+cy+dx)$$

We can complete the proof by ignoring bloch's hint because it doesn't help dumasses like me and cheating by showing $aw+bz+cx+dy=az+bw+cy+dx$.

$$\begin{aligned}
&\big([(aw+1,aw)]+[(bz+1,bz)]+[(cx+1,cx)]+[(dy+1,dy)]\big)\\
&\quad-\big([(az+1,az)]+[(bw+1,bw)]+[(cy+1,cy)]+[(dx+1,dx)]\big)\\
&=[(aw+1,aw)]+[(bz+1,bz)]+[(cx+1,cx)]+[(dy+1,dy)]\\
&\quad+[(az,az+1)]+[(bw,bw+1)]+[(cy,cy+1)]+[(dx,dx+1)]\\
&=[(aw+bz+cx+dy+az+bw+cy+dx+4,\ aw+bz+cx+dy+az+bw+cy+dx+4)]\\
&=[(1,1)]=0
\end{aligned}$$

Thus $ax+by+cw+dz=ay+bx+cz+dw$. Then it follows that

$$(ax+by,ay+bx)\sim(cz+dw,cw+dz)$$

Then from the definition of $\cdot$

$$(a,b)\cdot(x,y)\sim(c,d)\cdot(z,w)$$

∎

Proof. Let $(a,b),(c,d),(x,y),(z,w) \in \mathbb{N}\times\mathbb{N}$. Suppose $(a,b)\sim(c,d)$ and $(x,y)\sim(z,w)$. So $a+d=b+c$ and $x+w=y+z$. Summing shows $a+y+d+z=b+x+c+w$. Which is to say $(a+y,b+x)\sim(c+w,d+z)$. Therefore $(a,b)+(y,x)\sim(c,d)+(w,z)$. It then follows that $(a,b)-(x,y)\sim(c,d)-(z,w)$. Thus $-$ is well defined. ∎

Problem 4

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

Proof. Suppose $[(a, b)] = \hat{0}$. Thus $(a, b) \sim (1, 1)$. Therefore $a + 1 = b + 1$. It follows that $a = b$.

Suppose $a = b$. Then $a + 1 = b + 1$ Therefore $(a, b) \sim (1, 1)$. It follows that $[(a, b)] = \hat{0}$. ∎

Proof. Suppose $[(a, b)] = \hat{1}$. Thus $(a, b) \sim (1 + 1, 1)$. Therefore $a + 1 = b + (1 + 1)$. It follows that $a = b + 1$.

Suppose $a = b + 1$. Thus $a + 1 = b + (1 + 1)$. Thus $(a, b) \sim (1 + 1, 1)$. It follows that $[(a, b)] = \hat{1}$. ∎

Proof. (① →②) Suppose $[(a, b)] = [(n, 1)]$ for some $n \in \mathbb{N}$ such that $n \neq 1$. Thus $a+1 = b+n$. Since $n \neq 1$, $n > 1$. There exists $p \in \mathbb{N}$ such that $s(p) = n$. Then $a + 1 = b + s(p) = b + p + 1$. It follows that $a = b + p$. Thus $b < a$.

(② →①) Suppose $a > b$. There exists $p \in \mathbb{N}$ such that $a = b + p$. Then $a + 1 = b + p + 1$. It follows that $a + 1 = b + s(p)$. Let $n = s(p)$. Therefore $[(a, b)] = [(n, 1)]$ for some $n \in \mathbb{N}$ such that $n \neq 1$.

(② →③) Suppose $a > b$. There exists $p \in \mathbb{N}$ such that $a = b + p$. Then $a + 1 = b + 1 + p$. Therefore $[(a, b)] > \hat{0}$.

(③ →②) Suppose $[(a, b)] > \hat{0}$. It follows that $a + 1 > b + 1$. Thus there exists p such that $a + 1 = b + 1 + p$. Therefore $a = b + p$ and it follows that $a > b$. ∎

Proof. (① →②) Suppose $[(a, b)] = [(1, m)]$ for some $m \in \mathbb{N}$ such that $m \neq 1$. Then $a + m = b + 1$. Since $m \neq 1$, $m > 1$. There exists $p \in \mathbb{N}$ such that $s(p) = m$. Then $a + s(p) = b + 1 \implies a + p + 1 = b + 1$. It follows that $a = b - p$. Thus $a < b$.

(② →①) Suppose $a < b$. There exists $p \in \mathbb{N}$ such that $b = a + p$ with $p \neq 0$. Then $b + 1 = a + p + 1 = a + s(p)$. Let $m = s(p)$. Then $m \neq 1$. Therefore $[(a, b)] = [(1, m)]$ for some $m \in \mathbb{N}$ with $m \neq 1$.

(② →③) Suppose $a < b$. Then there exists $p \in \mathbb{N}$ such that $b = a + p$. Then $b + 1 = a + 1 + p$. Therefore $[(a, b)] < \hat{0}$.

(③ →②) Suppose $[(a, b)] < \hat{0}$. It follows that $b + 1 > a + 1$. Thus there exists $p \in \mathbb{N}$ such that $b + 1 = a + 1 + p$. Therefore $b = a + p$, so $a < b$. ∎

Problem 5

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

Proof. Let $x, y, z \in \mathbb{Z}$. We must show $(x + y) + z = z + (x + y)$. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = (x_1, x_2)$, $y = (y_1, y_2)$ and $z = (z_1, z_2)$. Then

$$
\begin{aligned}
(x + y) + z &= ([(x_1, x_2)] + [(y_1, y_2)]) + [(z_1, z_2)] \\
&= [(x_1 + y_1), (x_2 + y_2)] + [(z_1, z_2)] \\
&= [((x_1 + y_1) + z_1), ((x_2 + y_2) + z_2)] \\
&= [(x_1 + (y_1 + z_1)), (x_2 + (y_2 + z_2))] \\
&= [(x_1, x_2)] + [(y_1 + z_1), (y_2 + z_2)] \\
&= [(x_1, x_2)] + ([y_1, y_2] + [z_1, z_2]) \\
&= x + (y + z)
\end{aligned}
$$

∎

Proof. We must show $x + \hat{0} = x$. Let $(x_1, x_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)]$. Then $x + \hat{0} = [(x_1, x_2)] + [(1, 1)] = [(x_1 + 1, x_2 + 1)]$. Now $x_1 + x_2 + 1 = x_1 + x_2 + 1$ and rearranging shows $(x_1 + 1) + x_2 = (x_2 + 1) + x_1$. From which it follows $(x_1 + 1, x_2 + 1) \sim (x_1, x_2)$. Thus

$$[(x_1 + 1, x_2 + 1)] = [(x_1, x_2)] = x$$

∎

Proof. Let $x \in \mathbb{N}$ We must show $x + (-x) = \hat{0}$. Let $(x_1, x_2) \in \mathbb{N}$ such that $x = [(x_1, x_2)]$. Then

$$x + (-x) = [(x_1, x_2)] + (-[(x_1, x_2)]) = [(x_1, x_2)] + [(x_2, x_1)] = [(x_1 + x_2, x_2 + x_1)]$$

Now it is clearly $x_1 + x_2 + 1 = x_1 + x_2 + 1$ and rearranging shows $(x_1 + x_2) + 1 = (x_2 + x_1) + 1$. Thus $(x_1 + x_2, x_2 + x_1) \sim (1, 1)$. Then

$$[(x_1 + x_2, x_2 + x_1)] = [(1, 1)] = \hat{0}$$

∎

Proof. Let $x, y, z \in \mathbb{Z}$. We must show $(xy)z = x(yz)$. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)], z = [(z_1, z_2)]$. Then

$$\begin{aligned}
(xy)z &= ([(x_1, x_2)] \cdot [(y_1, y_2)]) \cdot [(z_1, z_2)] \\
&= [(x_1 y_1 + x_2 y_2, x_1 y_2 + x_2 y_1)] \cdot [(z_1, z_2)] \\
&= [((x_1 y_1 + x_2 y_2) z_1 + (x_1 y_2 + x_2 y_1) z_2, (x_1 y_1 + x_2 y_2) z_2 + (x_1 y_2 + x_2 y_1) z_1)] \\
&= [(x_1 y_1 z_1 + x_2 y_2 z_1 + x_1 y_2 z_2 + x_2 y_1 z_2, x_1 y_1 z_2 + x_2 y_2 z_2 + x_1 y_2 z_1 + x_2 y_1 z_1)] \\
&= [(x_1(y_1 z_1 + y_2 z_2) + x_2(y_2 z_1 + y_1 z_2), x_1(y_1 z_2 + y_2 z_1) + x_2(y_2 z_2 + y_1 z_1))] \\
&= [(x_1, x_2)] \cdot [(y_1 z_1 + y_2 z_2, y_1 z_2 + y_2 z_1)] \\
&= [(x_1, x_2)] \cdot ([(y_1, y_2)] \cdot [(z_1, z_2)]) \\
&= x \cdot (yz)
\end{aligned}$$

∎

Proof. Let $x, y \in \mathbb{N}$. We must show $xy = yx$. Let $(x_1, x_2), (y_1, y_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)]$. Then

$$\begin{aligned}
xy &= [(x_1, x_2)] \cdot [(y_1, y_2)] \\
&= [(x_1 y_1 + x_2 y_2, x_1 y_2 + x_2 y_1)] \\
&= [(x_2 y_2 + x_1 y_1, x_2 y_1 + x_1 y_2)] \\
&= [(y_1, y_2)] \cdot [(x_1, x_2)] \\
&= yx
\end{aligned}$$

∎

Proof. Let $x \in \mathbb{Z}$. We must show $x \cdot \hat{1} = x$. Let $(x_1, x_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)]$. Then

$$x \cdot \hat{1} = [(x_1, x_2)] \cdot [(1 + 1, 1)] = [(x_1(1 + 1) + x_2 \cdot 1, x_1 \cdot 1 + x_2 \cdot 1)] = [(2x_1 + x_2, x_1 + x_2)]$$

Now $2x_1 + 2x_2 = 2x_1 + 2x_2$. It follows that $(2x_1 + x_2, x_1 + x_2) \sim (x_1, x_2)$. Therefore

$$[(2x_1 + x_2, x_1 + x_2)] = [(x_1, x_2)] = x$$

∎

Proof. Let $x, y, z \in \mathbb{Z}$. We must show $x(y+z) = xy + xz$. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)], z = [(z_1, z_2)]$.

$$\begin{aligned}
x(y+z) &= [(x_1, x_2)] \cdot ([(y_1, y_2)] + [(z_1, z_2)]) \\
&= [(x_1, x_2)] \cdot [(y_1 + z_1, y_2 + z_2)] \\
&= [(x_1(y_1 + z_1) + x_2(y_2 + z_2),\ x_1(y_2 + z_2) + x_2(y_1 + z_1))] \\
&= [(x_1y_1 + x_1z_1 + x_2y_2 + x_2z_2,\ x_1y_2 + x_1z_2 + x_2y_1 + x_2z_1)] \\
&= [(x_1y_1 + x_2y_2,\ x_1y_2 + x_2y_1) + (x_1z_1 + x_2z_2,\ x_1z_2 + x_2z_1)] \\
&= xy + xz.
\end{aligned}$$

∎

Proof. Let $x, y \in \mathbb{Z}$. We must show precisely one of $x < y$, $x = y$, or $x > y$ holds. Let $(x_1, x_2), (y_1, y_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)]$.

We first show no two hold simultaneously.

Suppose $x < y$ and $x > y$. Then $x_1 + y_2 < x_2 + y_1$ and $x_1 + y_2 > x_2 + y_1$, which is a contradiction.

Suppose $x < y$ and $x = y$. Then $x_1 + y_2 < x_2 + y_1$ and $x_1 + y_2 = x_2 + y_1$, which is a contradiction.

Suppose $x > y$ and $x = y$. Then $x_1 + y_2 > x_2 + y_1$ and $x_1 + y_2 = x_2 + y_1$, which is a contradiction.

Thus no two hold simultaneously.

We now show at least one holds. We know either $x_1 + y_2 < x_2 + y_1$, $x_1 + y_2 = x_2 + y_1$, or $x_1 + y_2 > x_2 + y_1$. Thus at least one of $x < y$, $x = y$, or $x > y$ holds. ∎

Proof. Let $x, y, z \in \mathbb{Z}$. We must show if $x < y$ then $x + z < y + z$. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)], z = [(z_1, z_2)]$. Suppose $x < y$. Then $x_1 + y_2 < x_2 + y_1$. There exists $p \in \mathbb{N}$ such that $x_1 + y_2 + p = x_2 + y_1$. It follows that $x_1 + y_2 + p + z_1 + z_2 = x_2 + y_1 + z_1 + z_2$. Rearranging terms $(x_1 + z_1) + (y_2 + z_2) + p = (x_2 + z_2) + (y_1 + z_1)$. Thus $(x_1 + z_1) + (y_2 + z_2) < (x_2 + z_2) + (y_1 + z_1)$. Then

$$[(x_1 + z_1, x_2 + z_2)] < [(y_1 + z_1, y_2 + z_2)] \iff [(x_1, x_2)] + [(z_1, z_2)] < [(y_1, y_2)]$$

Therefore $x + z < y + z$. ∎

Proof. Let $x, y, z \in \mathbb{Z}$. We must show if $x < y$ and $z > \hat{0}$, then $xz < yz$. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)], y = [(y_1, y_2)], z = [(z_1, z_2)]$.

Suppose $x < y$ and $z > \hat{0}$. Then $x_1 + y_2 < x_2 + y_1$ and $z_1 > z_2$. Since $z_1 > z_2$, there exists $q \in \mathbb{N}$ such that $z_1 = z_2 + q$. From $x_1 + y_2 < x_2 + y_1$ there exists $p \in \mathbb{N}$ such that $x_1 + y_2 + p = x_2 + y_1$. From $x_1 + y_2 + p = x_2 + y_1$ multiply by z_1, $x_1z_1 + y_2z_1 + pz_1 = x_2z_1 + y_1z_1$. From $x_1 + y_2 + p = x_2 + y_1$ multiply by z_2, $x_1z_2 + y_2z_2 + pz_2 = x_2z_2 + y_1z_2$. Taking sums

$$(x_1z_1 + x_2z_2) + (y_1z_2 + y_2z_1) + pz_1 = (x_2z_1 + x_1z_2) + (y_2z_1 + y_1z_2)$$

Rearranging terms gives

$$(x_1z_1 + x_2z_2) + pz_1 < (x_2z_1 + x_1z_2)$$

Thus $(x_1z_1 + x_2z_2) < (x_2z_1 + x_1z_2)$. Then

$$[(x_1z_1 + x_2z_2, x_2z_1 + x_1z_2)] < [(y_1z_1 + y_2z_2, y_2z_1 + y_1z_2)] \iff [(x_1, x_2)] \cdot [(z_1, z_2)] < [(y_1, y_2)] \cdot [(z_1, z_2)]$$

Therefore $xz < yz$. ∎

Proof. We must show $\hat{0} \neq \hat{1}$. For contradiction suppose $\hat{0} = \hat{1}$. Then $(1, 1) \sim (1 + 1, 1)$ then $1 + 1 = 1 + 1 + 1$ Let $p \in \mathbb{N}$ such that $p = 1 + 1$. It follows that $p + 1 = p$ which is a contradiction. ∎

Problem 6

Prove Theorem 1.3.7 (1) (3) (4(*b*)) (4(*c*)).

Theorem 1. *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* $i(a) < i(b)$.

Proof. We must show $i : \mathbb{N} \to \mathbb{Z}$ is injective. Let $x_1, x_2 \in \mathbb{N}$ such that $i(x_1) = i(x_2)$. We must show $x_1 = x_2$. Now, $[(x_1 + 1, 1)] = [(x_2 + 1, 1)]$. Thus $(x_1 + 1) + 1 = 1 + (x_2 + 1)$ and cancelling terms shows that $x_1 = x_2$. ∎

Proof. We must show $i(1) = \hat{1}$. Now, $i(1) = [(1 + 1, 1)] = \hat{1}$. ∎

Proof. We must show $i(ab) = i(a)i(b)$. Now $i(ab) = [(ab + 1, 1)]$. We know that $ab + a + b + 3 = ab + a + b + 3$ which is equivalent to $ab+1+a+1+b+1 = 1+(ab+a+b+1)+1$. Rearranging terms $(ab+1)+((a+1)+(b+1)) = 1+((a+1)(b+1)+1)$. Thus $(ab+1, 1) \sim ((a+1)(b+1)+1, (a+1)+(b+1))$. Then $[(ab+1, 1)] = [((a+1)(b+1)+1, (a+1)+(b+1))]$ and $[((a+1)(b+1)+1, (a+1)+(b+1))] = [(a+1, 1)] \cdot [(b+1, 1)]$. It follows that $[(a+1, 1)] \cdot [(b+1, 1)] = i(a)i(b)$. ∎

Proof. We must show $a < b$ if and only if $i(a) < i(b)$.

Suppose $a < b$. It follows that $(a + 1) + 1 < 1 + (b + 1)$. Thus $[(a + 1, 1)] < [(b + 1, 1)]$.

Suppose $i(a) < i(b)$. Then $[(a + 1, 1)] < [(b + 1, 1)]$. It follows that $(a + 1) + 1 < 1 + (b + 1)$. Cancelling terms shows $a < b$. ∎

Problem 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. Suppose $x < y$ then

$$\begin{aligned}
x < y &\iff x + ((-x) + (-y)) < y + ((-x) + (-y)) && \text{by Theorem 1.3.5 part (12)} \\
&\iff x + ((-x) + (-y)) < y + ((-y) + (-x)) && \text{by Theorem 1.3.5 part (2)} \\
&\iff (x + (-x)) + (-y) < (y + (-y)) + (-x) && \text{by Theorem 1.3.5 part (1)} \\
&\iff 0 + (-y) < 0 + (-x) && \text{by Theorem 1.3.5 part (4)} \\
&\iff (-y) + 0 < (-x) + 0 && \text{by Theorem 1.3.5 part (2)} \\
&\iff -y < -x && \text{by Theorem 1.3.5 (4)}
\end{aligned}$$

Suppose $-y < -x$ then

$$\begin{aligned}
-y < -x &\iff (-y) + (x + y) < (-x) + (x + y) && \text{by Theorem 1.3.5 part (12)}\\
&\iff (-y) + (y + x) < (-x) + (x + y) && \text{by Theorem 1.3.5 part (2)}\\
&\iff ((-y) + y) + x < ((-x) + x) + y && \text{by Theorem 1.3.5 part (1)}\\
&\iff 0 + x < 0 + y && \text{by Theorem 1.3.5 part (4)}\\
&\iff x + 0 < y + 0 && \text{by Theorem 1.3.5 part (2)}\\
&\iff x < y && \text{by Theorem 1.3.5 part (4)}
\end{aligned}$$

∎

Proof. Suppose $z < 0$. It follows that $-z > 0$.

Suppose $x < y$. By Theorem 1.3.5 part 13,2 it follows that $x(-z) < y(-z) \iff -zx < -zy$. By the previous problem, $zy > zx$. By Theorem 1.3.5 part 2, $xz > yz$,

Suppose $xz > yz$. By the previous problem, $-xz < -yz$. By Theorem 1.3.5 part 2, $x(-z) < y(-z)$. By Theorem 1.3.5 part 13, $x < y$. ∎

Problem 8

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 $x > 0$. For contradiction suppose $x < 1$. Then $0 < x < 1$ and it follows that $1 < x + 1 < 2$. Let i be the bijective function in Theorem 1.3.7. It follows that $i(1) < i(x + 1) < i(2) = i(1) + i(1)$. contradicting Theorem 1.2.9 part 9. ∎

Proof. Suppose $x < 0$. For contradiction suppose $x > -1$. Then $-1 < x < 0$ and it follows that $1 < x + 2 < 2$. Let i be the bijective function in Theorem 1.3.7. It follows that $i(1) < i(x + 2) < i(2) = i(1) + i(1)$, contradicting Theorem 1.2.9 part 9. ∎

Problem 9

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

Proof. For contradiction suppose $1 \geq 2$. Either $1 = 2$ or $1 > 2$.

Suppose $1 = 2$. Let i be the bijective function in Theorem 1.3.7. Then $i(1) = i(2) = i(1) + i(1)$, which contradicts Theorem 1.2.7 part 6.

Suppose $1 > 2$. Then $i(1) > i(1) + i(1)$. There exists $p \in \mathbb{N}$ such that $i(1) = p + i(1) + i(1)$. This also contradicts Theorem 1.2.7 part 6.

It follows that $1 < 2$. ∎

Proof. For contradiction suppose $2x = 1$ Let $(x_1, x_2) \in \mathbb{N} \times \mathbb{N}$ such that $x = [(x_1, x_2)]$. Then $[(3, 1)] \cdot [(x_1, x_2)] = [(1 + 1, 1)] \iff [(3x_1 + x_2, 3x_2 + x_1)] = [(1 + 1, 1)]$ It follows that $3x_1 + x_2 + 1 = 3x_2 + x_1 + 1$. Cancelling terms shows $x_1 = x_2$. So $(x_1, x_2) \sim (1, 1)$ thus $2 \cdot \hat{0} = 0 \neq 1$. ∎

Problem 10

Prove that the Well-Order 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 $G \subseteq \{x \in \mathbb{Z} \mid x > 0\}$ such that $G \neq \emptyset$. Let i be the bijective function in Theorem 1.3.7. By Theorem 1.2.10, since $i^{-1}(G) \subseteq \mathbb{N}$ there exists $n \in i^{-1}(G)$ such that for all $x \in i^{-1}(G)$, $n \leq x$. It follows that for all $x \in G$, $i(n) \leq x$ ∎

Problem 11

Prove Theorem 1.3.8 (1) (3) (4) (5) (7) (10) (11).

Proof. We must show if $x + z = y + z$ then $x = y$. Suppose $x + z = y + z$. Then

$$\begin{aligned}
& x + z = y + z \\
\iff & (x + z) + (-z) = (y + z) + (-z) \\
\iff & x + (z + (-z)) = y + (z + (-z)) && \text{by Theorem 1.3.5 part (1)} \\
\iff & x + 0 = y + z && \text{by Theorem 1.3.5 part (4)} \\
\iff & x = y && \text{by Theorem 1.3.5 part (3)}
\end{aligned}$$

∎

Proof. We must show $-(x + y) = (-x) + (-y)$. Then

$$\begin{aligned}
& -(x + y) = (-x) + (-y) \\
\iff & -(x + y) + (x + y) = (-x) + (-y) + (x + y) \\
\iff & (x + y) + (-(x + y)) = (-x) + (x + y) + (-y) && \text{by Theorem 1.3.5 part (2)} \\
\iff & (x + y) + (-(x + y)) = (-x) + x + (y + (-y)) && \text{by Theorem 1.3.5 part (5)} \\
\iff & (x + y) + (-(x + y)) = x + (-x) + (y + (-y)) && \text{by Theorem 1.3.5 part (2)} \\
\iff & 0 = 0 + 0 && \text{by Theorem 1.3.5 part (4)} \\
\iff & 0 = 0 && \text{by Theorem 1.3.5 part (4)}
\end{aligned}$$

∎

Proof. We must show $x \cdot 0 = 0$.

$$\begin{aligned}
& (x \cdot 0) + (x \cdot 0) = x(0 + 0) && \text{by Theorem 1.3.5 part (8)} \\
\iff & (x \cdot 0) + (x \cdot 0) = x \cdot 0 && \text{by Theorem 1.3.5 part (3)} \\
\iff & (x \cdot 0) + (x \cdot 0) + (-(x \cdot 0)) = x \cdot 0 + (-(x \cdot 0)) \\
\iff & (x \cdot 0) + \big((x \cdot 0) + (-(x \cdot 0))\big) = x \cdot 0 + (-(x \cdot 0)) && \text{by Theorem 1.3.5 part (1)} \\
\iff & (x \cdot 0) + 0 = 0 && \text{by Theorem 1.3.5 part (4)} \\
\iff & x \cdot 0 = 0 && \text{by Theorem 1.3.5 part (3)}
\end{aligned}$$

∎

Proof. We must show that if $z \neq 0$ and $xz = yz$, then $x = y$. Suppose $z \neq 0$ and $xz = yz$. Then

$$\begin{aligned}
xz = yz \iff & xz - yz = 0 \\
\iff & (x - y)z = 0.
\end{aligned}$$

Since $z \neq 0$, it follows that $x + (-y) = 0$, so $x = y$. ∎

Proof. We must show $xy = 1$ if and only if $x = 1 = y$ or $x = -1 = y$.

$(\rightarrow)$ Suppose $xy = 1$. For contradiction, suppose $x \neq 1, y \neq 1$, and $x \neq -1, y \neq -1$.

To make things easier, we first show $x \neq 0, y \neq 0$. If $x = 0$ then $xy = 0y$ and from the 1.3.8 (4) it follows that $0y = 0$ contradicting that $xy = 1$. Similarly $y \neq 0$.

1. $x > 1, y > 1$.
2. $x < 1, y < 1$ so $x < 0, y < 0$.
3. $x > 1, y < 1$ so $y < 0$.
4. $x < 1, y > 1$ so $x < 0$.

Suppose $x > 1, y > 1$. Since $1 > 0$ it follows that $y > 0$ by Transitive Law. Since $1 < x$ and $y > 0$ it follows that $1 \cdot y < xy$. Then from Identity Law for Multiplication it follows that $y < xy$ showing $y < 1$ which is a contradiction.

Suppose $x < 0$ and $y < 0$. Since $-x > 0$ and $-y > 0$, we have $(-x)(-y) = xy$. But $xy = 1$, so $(-x)(-y) = 1$. For contradiction suppose $-x \neq 1$. Then either $-x > 1$ or $-x < 1$. Suppose $-x > 1$. Since $-y > 0$ it follows that $1 \cdot (-y) < (-x)(-y) = 1$. Then from Identity Law for Multiplication it follows that $-y < 1$. But $-y \in \mathbb{Z}$ and $-y > 0$ thus $-y \in \mathbb{N}$ contradicting that 1 is the lower bound of $\mathbb{N}$. Suppose $-x < 1$. So $-x \leq 0$. Suppose $-x = 0$. Thus $x = 0$ which is a contradiction. Thus $-x < 0$. Since $-y > 0$ it follows that $(-x)(-y) < 0 \cdot (-y)$. From which it follows that $1 < 0$ which is a contradiction.

Suppose $x > 1$ and $y < 0$. Since $1 < x$ and $y < 0$ it follows that $1 \cdot y > xy$. Then from Identity Law for Multiplication it follows that $y > xy$. But $xy = 1$ so $y > 1$ which contradicts $y < 1$.

Suppose $x < 0$ and $y > 1$. Since $1 < y$ and $x < 0$ it follows that $x \cdot 1 > xy$. Then from Identity Law for Multiplication it follows that $x > xy$. But $xy = 1$ so $x > 1$ which contradicts $x < 1$.

$(\leftarrow)$ Suppose $x = 1 = y$ or $x = -1 = y$. Suppose $x = 1 = y$. Then $xy = 1 \cdot 1 = 1$. Suppose $x = -1 = y$. Then $xy = (-1)(-1)$. Then by 1.3.8 (6), $(-1)(-1) = 1(-(-1))$. and by 1.3.8 (2), $1(-(-1)) = 1 \cdot 1 = 1$. Thus $xy = 1$. ∎

Proof. We must show if $x \leq y$ and $y \leq x$, then $x = y$. Suppose $x \leq y$ and $y \leq x$. For contradiction suppose $x \neq y$. Then either $x < y$ or $x > y$. Suppose $x < y$. This contradicts $y \leq x$. Suppose $x > y$. This contradicts $x \leq y$. Thus $x = y$. ∎

Proof. We must show that if $x > 0$ and $y > 0$, then $xy > 0$, and if $x > 0$ and $y < 0$, then $xy < 0$.

Suppose $x, y > 0$ and for contradiction $xy \leq 0$. Either $xy = 0$ or $xy < 0$. Suppose $xy = 0$ and it follows that $x = 0$ or $y = 0$ contradicting $x, y > 0$. Suppose $xy < 0$. It follows that $-xy > 0$. Thus $x(-y) > x \cdot 0$. Since $x > 0$ it follows that $-y > 0$ (Problem 7). Then $y < 0$ which is a contradiciton.

Suppose $x > 0$ and $y < 0$ and for contradiction $xy \geq 0$. Either $xy = 0$ or $xy > 0$. Suppose $xy = 0$ and it follows that $x = 0$ or $y = 0$ contradicting $x > 0, y < 0$. Suppose $xy > 0$. Since $-y > 0$ and $x > 0$ it follows that $x(-y) > 0$. Thus $-xy > 0$ and it follows that $xy < 0$. ∎

1.3 Axioms for the Integers

Problem 2

Let $n \in \mathbb{N}$. Prove that $n + 1 \in \mathbb{N}$.

Proof. Since $n \in \mathbb{N}$, $n \in \mathbb{Z}$ and $n > 0$. By Addition Law for Order, $n + 1 > 1$. By 1.4.5 (9), $n + 1 > 1 > 0$. By Transitive Law, $n + 1 > 0$. Since $n + 1 \in \mathbb{Z}$ and $n + 1 > 0$, by definition of $\mathbb{N}$, $n + 1 \in \mathbb{N}$. ∎

Problem 3

Let $x, y \in \mathbb{Z}$. Prove that $x \leq y$ if and only if $-x \geq -y$.

Proof. $(\rightarrow)$ Suppose $x \leq y$. Then

$$\begin{aligned}
x \leq y &\iff x + ((-x) + (-y)) \leq y + ((-x) + (-y)) && \\
&\iff (x + (-x)) + (-y) \leq y + ((-x) + (-y)) && \text{1.4.1 (a)} \\
&\iff (x + (-x)) + (-y) \leq y + ((-y) + (-x)) && \text{1.4.1 (b)} \\
&\iff (x + (-x)) + (-y) \leq (y + (-y)) + (-x) && \text{1.4.1 (a)} \\
&\iff 0 + (-y) \leq 0 + (-x) && \text{1.4.1 (d)} \\
&\iff -y + 0 \leq -x + 0 && \text{1.4.1 (b)} \\
&\iff -y \leq -x && \text{1.4.1 (c)}
\end{aligned}$$

$(\leftarrow)$ Suppose $-x \geq -y$. Then

$$\begin{aligned}
-x \geq -y &\iff -x + (x + y) \geq -y + (x + y) && \\
&\iff (-x + x) + y \geq -y + (x + y) && \text{1.4.1 (a)} \\
&\iff (-x + x) + y \geq -y + (y + x) && \text{1.4.1 (b)} \\
&\iff (-x + x) + y \geq (-y + y) + x && \text{1.4.1 (a)} \\
&\iff (x + (-x)) + y \geq (y + (-y)) + x && \text{1.4.1 (b)} \\
&\iff 0 + y \geq 0 + x && \text{1.4.1 (d)} \\
&\iff y + 0 \geq x + 0 && \text{1.4.1 (b)} \\
&\iff y \geq x && \text{1.4.1 (c)}
\end{aligned}$$

∎

Problem 4

Prove that $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 1\}$.

Proof. Let $x \in \mathbb{N}$. By definition $x \in \mathbb{Z}$ and $x > 0$. For contradiction, suppose $x < 1$. Then $0 < x < 1$ contradicting 1.4.6. Thus $x \geq 1$. It follows that $x \in \{x \in \mathbb{Z} \mid x \geq 1\}$. Therefore $\mathbb{N} \subseteq \{x \in \mathbb{Z} \mid x \geq 1\}$.

Let $x \in \{x \in \mathbb{Z} \mid x \geq 1\}$. Either $x = 1$ or $x > 1$. In either case $x > 0$. Thus $x \in \mathbb{N}$. Therefore $\{x \in \mathbb{Z} \mid x \geq 1\} \subseteq \mathbb{N}$.

It follows that $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 1\}$. ∎

Problem 5

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

Proof. Suppose $a < b$. For contradiciton suppose $a + 1 > b$. Then $a + 1 > b > a$ contradicting 1.4.6. ∎

Problem 6

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. (**Base Case**) Suppose $n = 2$. Then $s(1) = 1 + 1 = 2$.

(**Induction Step**) Suppose the theorem holds for some $n \in \mathbb{N}$ such that $n \neq 1$. Consider $n + 1 = s(n)$. By our hypothesis there exists $b \in \mathbb{N}$ such that $s(b) = n$. Thus $n + 1 = s(s(b)) = s(b) + 1$. Thus proving our theorem. ∎

Problem 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 $G = \{x \in \mathbb{Z} \mid x \geq a\}$.
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 $H = \{x \in \mathbb{Z} \mid x \leq a\}$.

Proof. We must show for a fixed $a \in \mathbb{Z}$, $\{x \in \mathbb{Z} \mid x \geq a\} \subseteq G$. Now, $x \geq a \iff x + (-a) \geq 0 \iff x + (-a) + 1 \geq 1$. So we need to show $\{x \in \mathbb{Z} \mid x + (-a) + 1 \geq 1\} \subseteq G$. Which is equivalent to $\{x \in \mathbb{Z} \mid x + (-a) + 1 \in \mathbb{N}\}$.

(**Base Case**) Let $x = a$. Then $x + (-a) + 1 = a + (-a) + 1 = 1 \in \mathbb{N}$. Thus $x = a \in G$.

(**Induction Step**) Suppose for some $x \in \mathbb{Z}$ that $x + (-a) + 1 \in \mathbb{N}$ and $x \in G$. Then consider $x + 1$. We have

$$(x + 1) + (-a) + 1 = (x + (-a) + 1) + 1 \in \mathbb{N}.$$

By the definition of G, since $x \in G$, we have $x + 1 \in G$.

Thus $G = \{x \in \mathbb{Z} \mid x \geq a\}$. ∎

Proof. We must show for a fixed $a \in \mathbb{Z}$, $\{x \in \mathbb{Z} \mid x \leq a\} \subseteq H$. Now, $x \leq a \iff a - x \geq 0 \iff a - x + 1 \geq 1$. So we need to show $\{x \in \mathbb{Z} \mid a - x + 1 \geq 1\} \subseteq H$. Which is equivalent to $\{x \in \mathbb{Z} \mid a - x + 1 \in \mathbb{N}\}$.

(**Base Case**) Let $x = a$. Then $a - x + 1 = a - a + 1 = 1 \in \mathbb{N}$. Thus $x = a \in H$.

(**Induction Step**) Suppose for some $x \in \mathbb{Z}$ that $a - x + 1 \in \mathbb{N}$ and $x \in H$. Then consider $x - 1$. We have

$$a - (x - 1) + 1 = (a - x + 1) + 1 \in \mathbb{N}.$$

By the definition of H, since $x \in H$, it follows that $x - 1 \in H$.

Thus $H = \{x \in \mathbb{Z} \mid x \leq a\}$. ∎

Extra Problem

There is a "unique" ordered integral domain that satisfies Axiom 1.4.4. Formulate this rigorously and prove it.

Theorem 2. *Let A and A' be ordered integral domains satisfying Axiom 1.4.4. Let $0, 1 \in A$ and $0', 1' \in A'$ such that $0 < 1$ and $0' < 1'$ and for all $x \in A$, $x + 0 = x$ and for all $x' \in B$, $x' + 0' = x'$. Then there exists a bijective function*

$$i : A \to B$$

such that $i(1) = 1'$ and for all $x, y \in A$ the following equations and relation holds.

1. $i(x + y) = i(x) + i(y)$.
2. $i(x - y) = i(x) - i(y)$.
3. $i(x \cdot y) = i(x) \cdot i(y)$.
4. $x < y \iff i(x) < i(y)$.

Proof. We can apply the recursive construction to the set B, the element $1' \in B$, and the function $s(x) = x + 1'$ on B, to deduce that there is a unique function $i : A \to B$ such that $i(x+1) = i(x) + 1'$ for all $x \in A$ and $i(1) = 1'$.

Similarly, we can construct a function $i' : B \to A$ such that $i'(y + 1') = i'(y) + 1$ for all $y \in B$ and $i'(1') = 1$.

Now we show that i' is the inverse of i.

Consider $i' \circ i$. Let $x \in A$.

Base case: $x = 1$.

$$(i' \circ i)(1) = i'(i(1)) = i'(1') = 1 = x$$

Inductive step: Suppose $x > 1$. By the properties of the domain, there exists $y \in A$ such that $y + 1 = x$. Suppose for $y \in A$ with $y < x$ we have $(i' \circ i)(y) = y$. Then

$$\begin{aligned}
(i' \circ i)(x) &= i'(i(y + 1)) \\
&= i'(i(y) + 1') \\
&= i'(i(y)) + 1 \\
&= y + 1 && \text{(induction hypothesis)} \\
&= x
\end{aligned}$$

Now consider $i \circ i'$. Let $y \in B$.

Base case: $y = 1'$.

$$(i \circ i')(1') = i(i'(1')) = i(1) = 1' = y$$

Inductive step: Suppose $y > 1'$. By the properties of the domain, there exists $y_0 \in B$ such that $y_0 + 1' = y$. Suppose for $y_0 < y$ we have $(i \circ i')(y_0) = y_0$. Then

$$\begin{aligned}
(i \circ i')(y) &= i(i'(y_0 + 1')) \\
&= i(i'(y_0) + 1) \\
&= i(i'(y_0)) + 1' \\
&= y_0 + 1' && \text{(induction hypothesis)} \\
&= y
\end{aligned}$$

Since $(i' \circ i)(x) = x$ and $(i \circ i')(y) = y$, we conclude that i' is the inverse of i. Thus i is bijective.

Finally, we check that i preserves all operations:

- Addition: By construction, $i(x + 1) = i(x) + 1'$; using induction on sums $x + y$, we get $i(x + y) = i(x) + i(y)$ for all $x, y \in A$.
- Subtraction: $i(x - y) = i(x) - i(y)$ follows from the additive inverse and induction.
- Multiplication: Using induction on y, $i(x \cdot 1) = i(x) \cdot 1'$ and $i(x \cdot (y+1)) = i(x \cdot y) + i(x)$, giving $i(x \cdot y) = i(x) \cdot i(y)$.
- Order: By definition, $x < y \iff \exists z \neq 0$ with $x + z = y$; using preservation of addition and $i(0) = 0'$, we have $i(x) < i(y) \iff x < y$.

∎

1.4 Constructing the Rational Numbers

Problem 1

Complete the proof of Lemma 1.5.2. That is, prove that the relation $\asymp$ is reflexive and symmetric.

Proof. Let $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}^*$.

We must show $(a,b) \asymp (a,b)$. But $ab = ab$ thus $(a,b) \asymp (a,b)$.

Suppose $(a,b) \asymp (c,d)$. We must show $(c,d) \asymp (a,b)$. But $ad = bc \iff cb = da$ thus $(c,d) \asymp (a,b)$. ∎

Redefining <

Let $[(a,b)] \in \mathbb{Q}$. Define $[(a,b)]$ to be in P iff both $a,b > 0$ or both $a,b < 0$.

1. If $[(a,b)] = [(c,d)]$ then $[(a,b)]$ in P iff $[(c,d)]$ in P.
2. Define $x < y$ if and only if $y - x$ in P.
3. Show $x < y$ if and only if Definition 1.5.3 is satisfied (this simplifies the proof of $<$ being well-defined).
4. Show that if x, y in P, then $x + y$ and xy in P.
5. Show that for any nonzero x in $\mathbb{Q}$, exactly one of x, $-x$ is in P.

Proof. Let $(x_1,x_2),(y_1,y_2) \in \mathbb{Q} \times \mathbb{Q}^*$ and let $x, y \in \mathbb{Q}$ such that $x = [(x_1,x_2)]$ and $y = [(y_1,y_2)]$. We first show $x < y$ if and only if Definition 1.5.3 is satisfied. Definition 1.5.3 states $<$ on $\mathbb{Q}$ is defined by

$$\begin{aligned}
[(x_1,x_2)] < [(y_1,y_2)] \iff & (x_2 > 0 \land y_2 > 0 \land x_1y_2 < y_1x_2) && ① \\
& \lor (x_2 < 0 \land y_2 < 0 \land x_1y_2 < y_1x_2) && ② \\
& \lor (x_2 > 0 \land y_2 < 0 \land x_1y_2 > y_1x_2) && ③ \\
& \lor (x_2 < 0 \land y_2 > 0 \land x_1y_2 > y_1x_2) && ④
\end{aligned}$$

$(\longrightarrow)$ Suppose $x < y$. It follows that $y - x \in P$. Then

$$[(y_1,y_2)] - [(x_1,x_2)] = [(y_1,y_2)] + [(-x_1,x_2)] = [(y_1x_2 - x_1y_2, y_2x_2)] \in P$$

There are two cases. Either $(y_1x_2 - x_1y_2),(y_2x_2) > 0$ or or $(y_1x_2 - x_1y_2),(y_2x_2) < 0$.

(Case 1) Suppose $(y_1x_2 - x_1y_2),(y_2x_2) < 0$. Since $y_2x_2 > 0$ either $y_2, x_2 > 0$ or $y_2x_2 < 0$. So, suppose $y_2, x_2 > 0$ we see ① holds. Similarly, suppose $y_2, x_2 < 0$ we see ② holds.

(Case 2) Suppose $(y_1x_2 - x_1y_2),(y_2x_2) < 0$. Since $y_2x_2 < 0$ either $y_2 > 0$ and $x_2 < 0$ or $y_2 < 0$ and $x_2 > 0$. So, suppose $y_2 > 0, x_2 < 0$ we see ③ holds. Similarly, suppose $y_2 < 0, x_2 > 0$ we see ④ holds.

So we have shown if $x < y$ then one case of Definition 1.5.3 holds.

$(\longleftarrow)$ Suppose $[(x_1,x_2)] < [(y_1,y_2)]$ then one of ①, ②, ③, ④ holds.

Case ①: $x_2 > 0$, $y_2 > 0$, and $x_1y_2 < y_1x_2$. Then $y_1x_2 - x_1y_2 > 0$ and $y_2x_2 > 0$, so $[(y_1x_2 - x_1y_2, y_2x_2)] \in P$. Thus $y - x \in P$ and therefore $x < y$.

Case ②: $x_2 < 0$, $y_2 < 0$, and $x_1y_2 < y_1x_2$. Then $y_1x_2 - x_1y_2 > 0$ and $y_2x_2 > 0$, so $[(y_1x_2 - x_1y_2, y_2x_2)] \in P$. Thus $y - x \in P$ and therefore $x < y$.

Case ③: $x_2 > 0$, $y_2 < 0$, and $x_1y_2 > y_1x_2$. Then $y_1x_2 - x_1y_2 < 0$ and $y_2x_2 < 0$, so $[(y_1x_2 - x_1y_2, y_2x_2)] \in P$. Thus $y - x \in P$ and therefore $x < y$.

Case ④: $x_2 < 0$, $y_2 > 0$, and $x_1y_2 > y_1x_2$. Then $y_1x_2 - x_1y_2 < 0$ and $y_2x_2 < 0$, so $[(y_1x_2 - x_1y_2, y_2x_2)] \in P$. Thus $y - x \in P$ and therefore $x < y$.

Thus proving our theorem. ∎

Proof. Let $x, y \in \mathbb{Z}$. Suppose $x, y \in P$. Let $[(x_1,x_2)] = x$ and $[(y_1,y_2)] = y$ such that $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. By definition of $+$, $x + y = [(x_1y_2 + y_1x_2, x_2y_2)]$. There are four cases.

Case $(x_1, x_2, y_1, y_2 > 0)$ Now, $y_1 > 0$ and since $x_2 > 0$, $y_1x_2 > 0 \cdot x_2 \iff y_1x_2 > 0$. Similarly $x_1y_2 > 0$. Then $y_1x_2 + x_1y_2 > 0 + x_1y_2 \iff y_1x_2 + x_1y_2 > x_1y_2 > 0$. Thus $x_1y_2 + y_1x_2 > 0$. Now, $x_2 > 0$ and since $y_2 > 0$, $x_2y_2 > 0 \cdot x_2 \iff x_2y_2 > 0$. Since $x_1y_2 + y_1x_2 > 0$ and $x_2y_2 > 0$, it follows that $x + y > 0$.

Case $(x_1, x_2, y_1, y_2 < 0)$ Now, $y_1 < 0$ and since $x_2 < 0$, $y_1x_2 < 0 \cdot x_2 \iff y_1x_2 > 0$. Similarly $x_1y_2 < 0 \cdot y_2 \iff x_1y_2 > 0$. Then $y_1x_2 + x_1y_2 > 0 + x_1y_2 \iff y_1x_2 + x_1y_2 > x_1y_2 > 0$. Now, $x_2 < 0$ and since $y_2 < 0$, $x_2y_2 < 0 \cdot x_2 \iff x_2y_2 > 0$. Since $x_1y_2 + y_1x_2 > 0$ and $x_2y_2 > 0$, it follows that $x + y > 0$.

Case $(x_1, x_2 > 0, y_1, y_2 < 0)$ Now, $y_1 < 0$ and since $x_2 > 0$, $y_1x_2 < 0 \cdot x_2 \iff y_1x_2 < 0$. Similarly, $x_1y_2 > 0 \cdot y_2 \iff x_1y_2 < 0$. Then $y_1x_2 + x_1y_2 < 0 + x_1y_2 \iff y_1x_2 + x_1y_2 < x_1y_2 < 0$. Now, $x_2 > 0$ and $y_2 < 0$, so $x_2y_2 > 0 \cdot y_2 \iff x_2y_2 < 0$. Since $y_1x_2 + x_1y_2 < 0$ and $x_2y_2 < 0$, it follows that $x + y > 0$.

Case $(x_1, x_2 < 0, y_1, y_2 > 0)$ Now, $y_1 > 0$ and $x_2 < 0$, so $y_1x_2 < 0 \cdot x_2 \iff y_1x_2 < 0$. Similarly, $x_1y_2 < 0 \cdot y_2 \iff x_1y_2 < 0$. Then $y_1x_2 + x_1y_2 < 0 + x_1y_2 \iff y_1x_2 + x_1y_2 < x_1y_2 < 0$. Now, $x_2 < 0$ and $y_2 > 0$, so $x_2y_2 < 0 \cdot y_2 \iff x_2y_2 < 0$. Since $y_1x_2 + x_1y_2 < 0$ and $x_2y_2 < 0$, it follows that $x + y > 0$. ∎

Proof. Let $x, y \in \mathbb{Z}$. Suppose $x, y \in P$. Let $[(x_1, x_2)] = x$ and $[(y_1, y_2)] = y$ such that $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. By definition of $\cdot$, $xy = [(x_1y_1, x_2y_2)]$. There are four cases.

Case $(x_1, x_2, y_1, y_2 > 0)$ Since $x_1 > 0$ and $y_1 > 0$ it follows that $x_1y_1 > 0$. Since $x_2 > 0$ and $y_2 > 0$ it follows that $x_2y_2 > 0$. Therefore $xy = [(x_1y_1, x_2y_2)] \in P$.

Case $(x_1, x_2, y_1, y_2 < 0)$ Since $x_1 < 0$ and $y_1 < 0$ it follows that $x_1y_1 > 0$. Since $x_2 < 0$ and $y_2 < 0$ it follows that $x_2y_2 > 0$. Therefore $xy = [(x_1y_1, x_2y_2)] \in P$.

Case $(x_1, x_2 > 0, y_1, y_2 < 0)$ Since $x_1 > 0$ and $y_1 < 0$ it follows that $x_1y_1 < 0$. Since $x_2 > 0$ and $y_2 < 0$ it follows that $x_2y_2 < 0$. Therefore $xy = [(x_1y_1, x_2y_2)] \in P$.

Case $(x_1, x_2 < 0, y_1, y_2 > 0)$ Since $x_1 < 0$ and $y_1 > 0$ it follows that $x_1y_1 < 0$. Since $x_2 < 0$ and $y_2 > 0$ it follows that $x_2y_2 < 0$. Therefore $xy = [(x_1y_1, x_2y_2)] \in P$. ∎

Proof. Let $x \in \mathbb{Q}$ such that $x \neq 0$. Let $x = [(x_1, x_2)]$ such that $x_1, x_2 \in \mathbb{Z}$. We want to show that exactly one of x or $-x$ is in P. Consider $-x = [(-x_1, x_2)]$. There are four cases.

Case $(x_1, x_2 > 0)$ Then $x \in P$ by definition. For $-x = [(-x_1, x_2)]$, so $-x_1 < 0$ and $x_2 > 0$, so $-x \notin P$. Thus exactly one of x or $-x$ is in P.

Case $(x_1, x_2 < 0)$ Then $x \in P$ by definition. For $-x = [(-x_1, x_2)]$, so $-x_1 > 0$ and $x_2 < 0$, so $-x \notin P$. Thus exactly one of x or $-x$ is in P.

Case $(x_1 > 0, x_2 < 0)$ Then $x \notin P$ by definition. For $-x = [(-x_1, x_2)]$, so $-x_1 < 0$ and $x_2 < 0$, so $-x \in P$. Thus exactly one of x or $-x$ is in P.

Case $(x_1 < 0, x_2 > 0)$ Then $x \notin P$ by definition. For $-x = [(-x_1, x_2)]$, so $-x_1 > 0$ and $x_2 > 0$, so $-x \in P$. Thus exactly one of x or $-x$ is in P. ∎

Problem 2

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

Proof. Let $(a, b), (c, d), (x, y), (z, w) \in \mathbb{Q} \times \mathbb{Q}^*$. Suppose $(a, b) \asymp (c, d)$ and $(x, y) \asymp (z, w)$. Thus $ad = bc$ and $xw = zy$.

Then

$$\begin{aligned} &[(a,b)] + [(x,y)] = [(c,d)] + [(z,w)] \\ \iff &(ay+bx,by) \asymp (cw+dz,dw) \\ \iff &(ay+bx)dw = (cw+dz)by \\ \iff &adyw + bxdw = cbyw + dzby. \end{aligned}$$

Since $ad = bc$ and $xw = zy$ it follows that $bcyw + bzyd = bcyw + bdzy$ which holds. Thus $(ay+bx,by) \asymp (cw+dz,dw)$.

Suppose $a \neq 0$ and $c \neq 0$. $[(a,b)]^{-1} = [(b,a)]$ and $[(c,d)]^{-1} = [(d,c)]$. Then $(b,a) \asymp (d,c) \iff bc = da$ which holds. Thus $[(a,b)]^{-1} = [(b,a)] = [(d,c)] = [(c,d)]^{-1}$

Suppose $[(a,b)] < [(x,y)]$. Then $[(a,b)] - [(x,y)] \in P$. But $[(a,b)] = [(c,d)]$ and $[(x,y)] = [(z,w)]$ so $[(c,d)] - [(z,w)] \in P$. It follows that $[(c,d)] < [(z,w)]$. ∎

Problem 3

Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^*$.

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

Proof. Suppose $[(x,y)] = \bar{0}$. Then $[(x,y)] = [(0,1)]$. It follows that $x \cdot 1 = y \cdot 0$. Thus $x = 0$.

Suppose $x = 0$. Then $x \cdot 1 = y \cdot 0$ It follows that $[(x,y)] = [(0,1)]$. Thus $[(x,y)] = \bar{0}$. ∎

Proof. Suppose $[(x,y)] = \bar{1}$. Then $[(x,y)] = [(1,1)]$. It follows that $x \cdot 1 = y \cdot 1$. Thus $x = y$.

Suppose $x = y$. Then $x \cdot 1 = y \cdot 1$. It follows that $[(x,y)] = [(1,1)]$. Thus $[(x,y)] = \bar{1}$. ∎

Proof. Suppose $\bar{0} < [(x,y)]$. By definition, $[(x,y)] - \bar{0} \in P$. But $\bar{0} = [(0,1)]$, so

$$[(x,y)] - [(0,1)] = [(x \cdot 1 - 0 \cdot y, y \cdot 1)] = [(x,y)] \in P$$

Thus either $x,y > 0$ or $x,y < 0$, so in either case $xy > 0$.

Suppose $xy > 0$. Then either $x,y > 0$ or $x,y < 0$. Thus $[(x,y)] \in P$, so $\bar{0} < [(x,y)]$. ∎

Problem 4

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

Proof. Let $r,s,t \in \mathbb{Q}$. We must show $(r+s)+t = r+(s+t)$. Let $(r_1,r_2),(s_1,s_2),(t_1,t_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Then

$$\begin{aligned} (r+s)+t &= ([(r_1,r_2)] + [(s_1,s_2)]) + [(t_1,t_2)] \\ &= [(r_1s_2 + r_2s_1, r_2s_2)] + [(t_1,t_2)] \\ &= [((r_1s_2 + r_2s_1)t_2 + t_1(r_2s_2), r_2s_2t_2)] \\ &= [(r_1s_2t_2 + r_2s_1t_2 + t_1r_2s_2, r_2s_2t_2)] \\ &= [(r_1s_2t_2 + (r_2s_1t_2 + t_1r_2s_2), r_2s_2t_2)] \\ &= [(r_1s_2t_2 + r_2(s_1t_2 + s_2t_1), r_2s_2t_2)] \\ &= [(r_1,r_2)] + [(s_1t_2 + s_2t_1, s_2t_2)] \\ &= [(r_1,r_2)] + ([(s_1,s_2)] + [(t_1,t_2)]) \\ &= r + (s+t) \end{aligned}$$

∎

Proof. Let $r, s \in \mathbb{Q}$. We must show $r + s = s + r$. Let $(r_1, r_2), (s_1, s_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Then

$$\begin{aligned}
r + s &= [(r_1, r_2)] + [(s_1, s_2)] \\
&= [(r_1 s_2 + s_1 r_2, r_2 s_2)] \\
&= [(s_1 r_2 + r_1 s_2, s_2 r_2)] \\
&= [(s_1, s_2)] + [(r_1, r_2)] \\
&= s + r
\end{aligned}$$

∎

Proof. Let $r \in \mathbb{Q}$. We must show $r + \bar{0} = r$. Let $(r_1, r_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Then

$$\begin{aligned}
r + \bar{0} = &= [(r_1, r_2)] + [(0, 1)] \\
&= [(r_1 \cdot 1 + 0 \cdot r_2, r_2 \cdot 1)] \\
&= [(r_1, r_2)] \\
&= r
\end{aligned}$$

∎

Proof. Let $r, s, t \in \mathbb{Q}$. We must show $(rs)t = r(st)$. Let $(r_1, r_2), (s_1, s_2), (t_1, t_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Then

$$\begin{aligned}
(rs)t &= ([(r_1, r_2)] \cdot [(s_1, s_2)]) \cdot [(t_1, t_2)] \\
&= [(r_1 s_1, r_2 s_2)] \cdot [(t_1, t_2)] \\
&= [(r_1 s_1 t_1, r_2 s_2 t_2)] \\
&= [(r_1, r_2)] \cdot [(s_1 t_1, s_2 t_2)] \\
&= [(r_1, r_2)] \cdot ([(s_1, s_2)] \cdot [(t_1, t_2)]) \\
&= r(st)
\end{aligned}$$

∎

Proof. Let $r, s \in \mathbb{Q}$. We must show $rs = sr$. Let $(r_1, r_2), (s_1, s_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Then

$$\begin{aligned}
rs &= [(r_1, r_2)] \cdot [(s_1, s_2)] \\
&= [(r_1 s_1, r_2 s_2)] \\
&= [(s_1 r_1, s_2 r_2)] \\
&= [(s_1, s_2)] \cdot [(r_1, r_2)] \\
&= sr
\end{aligned}$$

∎

Proof. Let $r \in \mathbb{Q}$. We must show if $r \neq \bar{0}$, then $r \cdot r^{-1} = \bar{1}$. Let $(r_1, r_2) \in \mathbb{Z} \times \mathbb{Z}^*$. Suppose $r \neq \bar{0}$. Then

$$\begin{aligned}
r \cdot r^{-1} &= [(r_1, r_2)] \cdot [(r_1, r_2)]^{-1} \\
&= [(r_1, r_2)] \cdot [(r_2, r_1)] && r \neq \bar{0} \implies r_1 \neq 0 \implies r_1 \in \mathbb{Z}^* \\
&= [(r_1 r_2, r_2 r_1)] \\
&= \bar{1} && \text{Problem 3 b}
\end{aligned}$$

∎

Proof. Let $r, s, t \in \mathbb{Q}$. We must show $r(s+t) = rs + rt$. Let $(r_1, r_2), (s_1, s_2), (t_1, t_2) \in \mathbb{Z} \times \mathbb{Z}^*$.

$$\begin{aligned}
r(s+t) &= [(r_1, r_2)]([(s_1, s_2)] + [(t_1, t_2)]) \\
&= [(r_1, r_2)]([s_1t_2 + t_1s_2, s_2t_2]) \\
&= [(r_1(s_1t_2 + t_1s_2), r_2(s_2t_2))] \\
&= [(r_1s_1t_2 + r_1t_1s_2, r_2s_2t_2)] \\
&= [(r_1s_1, r_2s_2)] + [(r_1t_1, r_2t_2)] \\
&= rs + rt.
\end{aligned}$$

∎

Proof. Let $r, s, t \in \mathbb{Q}$. We must show if $r < s$ and $s < t$, then $r < t$. Suppose $r < s$ and $s < t$. It follows that $s - r \in P$ and $t - s \in P$. It follows that $(s - r) + (t - s) = t - r \in P$. Thus $r < t$. ∎

Proof. Let $r, s, t \in \mathbb{Q}$. We must show if $r < s$ then $r + t < s + t$. Supose $r < s$. Then $s - r = s - r + 0 = s - r + t + (-t) = (s+t) - (r+t) \in P$. Thus $r + t < s + t$. ∎

Proof. We must show $\bar{0} \neq \bar{1}$. Suppose $\bar{0} = \bar{1}$. Then $[(0,1)] = [(1,1)] \iff 0 \cdot 1 = 1 \cdot 1 \iff 0 = 1$ which is a contradiction. Thus $\bar{0} \neq \bar{1}$. ∎

Problem 5

Prove Theorem 1.5.6 (1) (2) (3).

Theorem 3. *Let $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ be defined by $i(x) = [(x, 1)]$ for all $x \in \mathbb{Z}$.*

1. *Then function $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ is injective.*
2. $i(0) = \bar{0}$ *and* $i(1) = \bar{1}$.
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 $r = i(x)(i(y))^{-1}$.*

Proof. Let $x, y \in \mathbb{Z}$. Suppose $i(x) = i(y)$. Thus $[(x, 1)] = [(y, 1)]$ so $(x, 1) \asymp (y, 1)$. It follows that $x \cdot 1 = y \cdot 1$. From the Identity Law for Multiplication $x = y$. Thus i is injective. ∎

Proof. Notice $i(0) = [(0, 1)] = \bar{0}$ and $i(1) = [(1, 1)] = \bar{1}$. ∎

Proof. Let $x, y \in \mathbb{Z}$. Then

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

Similarly

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

Similarly

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

Finally suppose $x < y$. Then $i(y-x) = [(y-x,1)] \in P$ since $y - x \in P$ and $1 \in P$. Thus

$$[(y-x,1)] = [(y \cdot 1 - x \cdot 1, 1 \cdot 1)] = [(y,1)] - [(x,1)] = i(y) - i(x) \in P$$

It follows that $i(x) < i(y)$. ∎

Problem 6

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 $\frac{1}{s} < \frac{1}{s}$.
7. Prove that if $0 < r < p$ and $0 < s < q$, then $rs < pq$.

Problem 7

1. Prove that $1 < 2$.
2. Let $s, t \in \mathbb{Q}$. Suppose $s < t$. Prove that $\frac{s+t}{2} \in \mathbb{Q}$, and that $s < \frac{s+t}{2} < t$.

Proof. By Problem 6 Part 1, $0 < 1$. By Addition Law for Order, $0 + 1 < 1 + 1 \iff 1 < 2$. ∎

Proof. Now $\frac{1}{2} \in \mathbb{Q}$. Since $\mathbb{Q}$ is closed under multiplication and addition $(s+t) \cdot \frac{1}{2} = (s+t)2^{-1} = \frac{s+t}{2} \in \mathbb{Q}$.

We now show $\frac{s+t}{2} < t$. First, notice $t - \frac{s+t}{2} = \frac{t}{1} + \frac{-(s+t)}{2} = \frac{2t+(-(s+t))1}{2 \cdot 1}$. Clearly $2 \in P$ and $2t + (-(s+t))1 = 2t - s - t = t - s$. Since $s < t$ it follows that $t - s \in P$. Thus $t - \frac{s+t}{2} \in P$. Therefore $\frac{s+t}{2} < t$.

We now show $\frac{s+t}{2} > s$. First, notice $\frac{s+t}{2} - s = \frac{s+t}{2} + \frac{-s}{1} = \frac{(s+t)1+(-2)s}{2 \cdot 1}$. Clearly $2 \in P$ and $(s+t)1 + (-2)s = t - s$. Since $s < t$ it follows that $t - s \in P$. Thus $\frac{s+t}{2} - s \in P$. Therefore $\frac{s+t}{2} > s$.

It follows that $s < \frac{s+t}{2} < t$. ∎

Problem 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. Suppose $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ such that $b \neq 0$. Since $r > 0$ it follows that $a, b \in P$ or $a, b \notin P$. Suppose $a, b \in P$. Then $a = a - 0 \in P$ and $b = b - 0 \in P$. Thus $a > 0$ and $b > 0$. Suppose $a, b \notin P$. Then $a = a - 0 \notin P$ and $b = b - 0 \notin P$. Thus $-(a-0) = -a + 0 = 0 - a \in P$ and $-(b-0) = -b + 0 = 0 - b \in P$. Thus $0 > a$ and $0 > b$. ∎

Proof. Suppose $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. By part (1), either $a, b > 0$ or $a, b < 0$. If $a, b > 0$, let $m = a$ and $n = b$. Suppose $a, b < 0$. Then $-a > 0$ and $-b > 0$. Also, $(-a)(-b) = -(-ab) = ab$ so $(a, b) \asymp (-a, -b)$. Thus let $m = -a$ and $n = -b$. ∎

Problem 9

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

1. Suppose $r > 0$ and $s > 0$. Prove that there is some $n \in \mathbb{N}$ such that $s < nr$.
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 $r^2 < p$, then there is some $k \in \mathbb{N}$ such that $(r + \frac{1}{k})^2 < p$.

1.5 Dedekind Cuts