The Real Numbers and Real Analysis
Ethan Bloch

Noah Lewis

November 8, 2025

Contents

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 $bc + p_2 = (a + p_1)c + p_2 = ac + p_1c + p_2$ (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

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 $x + w = y + z$.

Therefore, $(a, b) \cdot (x, y) \sim (c, d) \cdot (z, w)$, and multiplication is well-defined. ∎

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 $x + \hat{0} = [(x_1, x_2)] + [(1, 1)] = [(x_1 + 1, x_2 + 1)]$. Then $(1, 1) \sim (x_1 + 1, x_2 + 1)$ implies $x_2 + 1 + 1 = x_1 + 1 + 1$. Cancelling terms shows $x_1 = x_2$. ∎

Problem 6

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

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 $xz > yz$.

Problem 8

Let $x \in \mathbb{Z}$. Prove that if $x > 0$ then $x \geq 1$. Prove that if $x < 0$ then $x \leq -1$.

Problem 9

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

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.

Problem 11

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