MTH 505: Number Theory — Spring 2017
Homework 1 — Drew Armstrong

1.1. From $(\mathbb{N}, \sigma, 0)$ to $(\mathbb{N}, +, \cdot, 0, 1)$. Recall Peano's four axioms for the natural numbers:

(P1) There exists a special element called $0 \in \mathbb{N}$.

(P2) The element 0 is not the successor of any number, i.e.,

$$\forall n \in \mathbb{N}, \sigma(n) \neq 0.$$

(P3) Every number has a unique successor, i.e.,

$$\forall m, n \in \mathbb{N}, (\sigma(m) = \sigma(n)) \Rightarrow (m = n).$$

(P4) *The Induction Principle.* If a set of natural numbers $S \subseteq \mathbb{N}$ contains 0 and is closed under succession, then we must have $S = \mathbb{N}$. In other words, if we have

- $0 \in S$,
- $\forall n \in \mathbb{N}, (n \in S) \Rightarrow (\sigma(n) \in S)$,

then it follows that $S = \mathbb{N}$.

It is strange that these axioms do not tell us how to *add* or *multiply* numbers. In this problem you will investige the steps involved when unpacking Peano's axioms into the structure $(\mathbb{N}, +, \cdot, 0, 1)$.

(a) **Lemma.** If $n \in \mathbb{N}$ and $n \neq 0$, show that there exists a unique $m \in \mathbb{N}$ such that $\sigma(m) = n$. We call this m the *predecessor* of n.

This lemma allows us to define the binary operations $+, \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ recursively, as follows:

$$a + 0 := a, \tag{1}$$
$$a + \sigma(b) := \sigma(a + b), \tag{2}$$
$$a \cdot 0 := 0, \tag{3}$$
$$a \cdot \sigma(b) := (a \cdot b) + a. \tag{4}$$

Now you will prove that $+$ and $\cdot$ have the desired properties. It is important to prove the following results in the suggested order or you might get stuck. Induction is your **only tool**, so for each problem you should define a certain set of natural numbers $S \subseteq \mathbb{N}$ and then prove that $S = \mathbb{N}$. For example, in part (a) you should fix $a, b \in \mathbb{N}$ and then let $S \subseteq \mathbb{N}$ be the set of $c \in \mathbb{N}$ such that $a + (b + c) = (a + b) + c$.

(b) **Associativity of Addition.** Show that for all $a, b, c \in \mathbb{N}$ we have $a+(b+c) = (a+b)+c$.

(c) **Lemma.** Show that $a + 0 = 0 + a$ and $a + \sigma(0) = \sigma(0) + a$ for all $a \in \mathbb{N}$.

(d) **Commutativity of Addition.** Show that for all $a, b \in \mathbb{N}$ we have $a + b = b + a$.

(e) **Distributive Law.** Show that for all $a, b, c \in \mathbb{N}$ we have $a(b + c) = ab + ac$.

(f) **Associativity of Multiplication.** Show that for all $a, b, c \in \mathbb{N}$ we have $a(bc) = (ab)c$.

(g) **Lemma.** Show that for all $a, b \in \mathbb{N}$ we have $\sigma(a)b = ab + b$. [Hint: Induction on b.]

(h) **Commutativity of Multiplication.** Show that for all $a, b \in \mathbb{N}$ we have $ab = ba$. [Hint: Prove the base case by induction, then use Lemma (g).]

1.2. From $(\mathbb{N}, +, \cdot, 0, 1)$ to $(\mathbb{Z}, +, \cdot, 0, 1)$. The integers are obtained from the natural numbers by "formally adjoining additive inverses". This problem will investigate the steps involved. Let $(\mathbb{N}, +, \cdot, 0, 1)$ be the structure obtained from Problem 1.1. You can ignore the successor function now and just write $n + 1$ instead of $\sigma(n)$. Let $\mathbb{Z}$ denote the set of ordered pairs of natural numbers:

$$\mathbb{Z} = \{[a, b] : a, b \in \mathbb{N}\}.$$

(a) Prove that the following rule defines an equivalence relation on $\mathbb{Z}$:

$$[a, b] \sim [c, d] \quad \Longleftrightarrow \quad a + d = c + b.$$

Intuition: We think of the pair $[a, b]$ as the fictional number "$a - b$".

(b) Prove that the following binary operations on $\mathbb{Z}$ are well-defined on equivalence classes:

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

(c) Prove that each of the operations $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is commutative and associative, and also that $\cdot$ distributes over $+$.

(d) Finally, explain how to view $(\mathbb{N}, +, \cdot, 0, 1)$ as subsystem of $(\mathbb{Z}, +, \cdot, 0, 1)$ and show that each element of $\mathbb{N}$ now has an *additive inverse* in the larger system.

1.3. From $(\mathbb{Z}, +, \cdot, 0, 1)$ to $(\mathbb{Q}, +, \cdot, 0, 1)$. The rational numbers are obtained from the natural numbers by "formally adjoining multiplicative inverses". This problem will investigate the steps involved. Let $(\mathbb{Z}, +, \cdot, 0, 1)$ be the structure obtained from Problem 1.2. But now we will forget the language of ordered pairs and we will just write $n \in \mathbb{Z}$ for integers. Let $\mathbb{Q}$ denote the set of **ordered pairs of integers** in which the second entry is **nonzero**:

$$\mathbb{Q} := \{[a, b] : a, b \in \mathbb{Z}, b \neq 0\}.$$

(a) Prove that the following rule defines an equivalence relation on $\mathbb{Q}$:

$$[a, b] \sim [c, d] \quad \Longleftrightarrow \quad ad = bc.$$

Intuition: We think of the pair $[a, b]$ as the fictional number "a/b".

(b) Prove that the following binary operations on $\mathbb{Q}$ are well-defined on equivalence classes:

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

Hence we obtain two binary operations $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.

(c) **(Optional)** Prove that each of the operations $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is commutative and associative, and also that $\cdot$ distributes over $+$.

(d) Finally, explain how to view $(\mathbb{Z}, +, \cdot, 0, 1)$ as subsystem of $(\mathbb{Q}, +, \cdot, 0, 1)$ and show that each **nonzero** element of $\mathbb{Z}$ now has an *multiplicative inverse* in the larger system.