1 Axioms for the natural numbers

Axiom. ***(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 is injective.

c. Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$ and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.

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

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

Theorem 2. *There is a unique binary operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

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

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

Theorem 3. *There is a unique binary operation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that satisfies the following two properties for all $n, m \in \mathbb{N}$.*

a. $n \cdot 1 = n$

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

Theorem 4. *Let $a, b, c \in \mathbb{N}$.*

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

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

Theorem 5. *Let $a, b, c, d \in \mathbb{N}$.*

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

Theorem 6. ***(Well-Ordering Principle).*** *Let $G \subseteq \mathbb{N}$ be a non-empty set. Then there is some $m \in G$ such that $m \leq g$ for all $g \in G$.*

Exercises

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

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

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

Then $G \subseteq N$. By part (a) applied to both $\cdot$ and $\times$ we see that $n \cdot 1 = 1 = n \times 1$ for all $n \in \mathbb{N}$, so $1 \in G$. Now let $q \in G$ and $n \in N$. Then $n \cdot q = n \times q$. Then it follows from part (b) that

$$n \cdot s(q) = (n \cdot q) + n = (n \times q) + n = n \times s(q).$$

Then $s(q) \in G$, and therefore we can conclude using part (c) of the Peano Postulates that $G = \mathbb{N}$.

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

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

2. $(a+b)+c = a+(b+c)$

   Proof. Let
   $$G = \{z \in \mathbb{N} : \text{ if } x, y \in \mathbb{N}, (x+y)+z = x+(y+z)\}.$$
   Then $(x+y)+1 = s(x+y) = x+s(y) = x+(y+1)$, so $1 \in G$. Now, let $z \in G$. Then
   $$\begin{aligned}(x+y)+s(z) &= (x+y)+(z+1)\\ &= ((x+y)+z)+1\\ &= (x+(y+z))+1\\ &= x+((y+z)+1)\\ &= x+(y+(z+1))\\ &= x+(y+s(z))\end{aligned}$$
   So if $z \in G$ then $s(z) \in G$, and therefore $G = \mathbb{N}$. □

3. $1+a = s(a) = a+1$.

   Proof. It follows from the definition of $+$, that $a+1 = s(a)$. Let $G = \{a \in N : 1+a = s(a)\}$. $1+1 = s(1)$, so $1 \in G$. Now, let $a \in G$. Then $(1+a)+1 = s(1+a) = 1+s(a) = 1+(1+a)$. So $s(a) \in G$, and therefore $G = \mathbb{N}$. □

4. $a+b = b+a$

   Proof. Let
   $$G = \{a \in \mathbb{N} : \text{ if } b \in \mathbb{N}, a+b = b+a\}.$$
   Let $b \in N$. It follows that $1+b = b+1$, so $1 \in G$. Now, let $a \in G$. Then
   $$(a+1)+b = (1+a)+b = 1+(a+b) = 1+(b+a) = (b+a)+1 = b+(a+1).$$
   So $s(a) \in G$, and therefore $G = \mathbb{N}$. □

7. $a \cdot 1 = a = 1 \cdot a$

   Proof. It follows from the definition of $\cdot$ that $a \cdot 1 = a$. Let $G = \{a \in \mathbb{N} : 1 \cdot a = a\}$. Since $1 \cdot 1 = 1$, we know that $1 \in G$. Let $a \in G$. Then
   $$1 \cdot s(a) = (1 \cdot a)+1 = a+1 = s(a).$$
   So $s(a) \in \mathbb{N}$, and therefore $G = \mathbb{N}$. □

8. $(a+b)c = ac+bc$