Transition to Mathematical Proofs
Chapter 7 - Peano Arithmetic Assignment Solutions

Theorem 1 (Commutativity)**.** *For all $a, b \in \mathbb{N}$, the following hold:*

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

Theorem 2 (Associativity)**.** *For all $a, b, c \in \mathbb{N}$, the following hold:*

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

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Theorem 3 (Distributivity)**.** *For all $a, b, c \in \mathbb{N}$, the following holds:*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Question 1. Let $a, b, c \in \mathbb{N}$. Show that if $a + b = a + c$, then $b = c$.

Proof 1. Suppose for $a, b, c \in \mathbb{N}$ we have that $a + b = a + c$. We will show that $b = c$. We proceed by induction on a. That is, we show that the subset $A \subset \mathbb{N}$, where

$$A = \{a \in \mathbb{N} : \forall b, c \in \mathbb{N}, a + b = a + c \Rightarrow b = c\},$$

is equal to $\mathbb{N}$. If $a = 0$, then we have:

$$0 + b = 0 + c.$$

By commutativity, we turn this into:

$$b + 0 = c + 0.$$

By the definition of addition, this reduces to $b = c$, as desired. Now suppose for some $a \in \mathbb{N}$ that for all $b, c \in \mathbb{N}$, we have that $a + b = a + c$ implies $b = c$ (for our inductive assumption). We show that $S(a) + b = S(a) + c$ implies that $b = c$.

Notice that it will suffice to show that $S(a) + b = S(a) + c$ implies that $a + b = a + c$, and our inductive assumption will give that $b = c$, completing the proof. Starting with $S(a) + b = S(a) + c$, we proceed as follows:

$$S(a) + b = S(a) + c$$

$$b + S(a) = c + S(a)$$

$$S(b + a) = S(c + a)$$

$$b + a = c + a$$

$$a + b = a + c.$$

The second and fifth lines follow from commutativity, the third line from the definition of addition, and the fourth line from injectivity of the successor function (Axiom 8). Hence our inductive assumption implies $b = c$. Because $0 \in A$, and $a \in A$ implies $S(a) \in A$, we have that A is an inductive set. Thus, the induction axiom (Axiom 9) gives that $\mathbb{N} \subset A$, so $\mathbb{N} = A$, as desired.

□

Question 2. Let $a \in \mathbb{N}$.

(a) Show that $a + a = 2 \cdot a$. Remember that the symbol "2" means the successor of 1, which is the successor of 0.

(b) Show that the n-fold sum $a + \ldots + a = n \cdot a$.

Proof 2a. Recall from the chapter notes that for all $a \in \mathbb{N}$, we have $a \cdot 1 = a$. Recall also that $1 = S(0)$. Thus,

$$a + a = a + a \cdot 1 = a \cdot S(1)$$

where the second equality follows from the recursive part of the definition of multiplication. Now, $S(1) = 2$, and so another application of commutativity yields the final result:

$$a \cdot S(1) = a \cdot 2 = 2 \cdot a.$$

Hence $a + a = 2 \cdot a$.

□

Proof 2b. Let $a \in \mathbb{N}$ be arbitrary. We proceed by induction on n. The case of $n = 0$ is vacuous, and $n = 1$ is covered in the chapter. Suppose for some $n \in \mathbb{N}$ that the assertion holds, that is, $a + \ldots + a = n \cdot a$. Adding a to both sides, we obtain:

$$a + (a + \ldots + a) = a + n \cdot a.$$

By associativity, we may rewrite the left-hand side without parentheses. Recall also that $a = a \cdot 1 = 1 \cdot a$ by commutativity and the chapter notes. We now have

$$a + \ldots + a = 1 \cdot a + n \cdot a,$$

with $n + 1$ summands on the left-hand side. Now, by distributivity, we may simplify the right-hand side to $(1 + n) \cdot a$, which by commutativity is $(n + 1) \cdot a$. But by definition, $n + 1 = S(n)$, so

$$a + \ldots + a = S(n) \cdot a$$

with $n + 1$ summands. Now, the set $A \subset \mathbb{N}$ of numbers for which the above assertion holds contains 0 and all successors. Thus A is inductive, and so by Axiom 9, $\mathbb{N} \subset A$, which means $A = \mathbb{N}$, as desired.

□

Question 3. In this question, we will explore one way to define the standard ordering "$\leq$" on the natural numbers, and prove some important properties about it. Let $a, b \in \mathbb{N}$. Define $a \leq b$ if and only if there exists some $c \in \mathbb{N}$ such that $a + c = b$.

(a) Let $a, b, c \in \mathbb{N}$ such that $c \neq 0$ and $a = b \cdot c$. Prove that $b \leq a$.

(b) Let $a \in \mathbb{N}$. Prove that $a \leq a$. You may recall this is known as the *reflexive* property.

(c) Let $a, b, c \in \mathbb{N}$. Prove that if $a \leq b$ and $b \leq c$, then $a \leq c$. You may also recall this is known as the *transitive* property.

(d) Let $a, b \in \mathbb{N}$. Prove that if $a \leq b$ and $b \leq a$, then $a = b$. This property is called *antisymmetry*, and is where $\leq$ differs from an equivalence relation (which instead has *symmetry*).

Proof 3a. First, notice that by the discussion beneath Axiom 9, every nonzero number is a successor to some other number. We know $c \neq 0$, so for some $d \in \mathbb{N}$, we have that $S(d) = c$. Thus $a = b \cdot c$ is the same as $a = b \cdot S(d)$. By the definition of multiplication, this implies $a = b + b \cdot d$, whence $b \leq a$.

□

Proof 3b. Notice $a + 0 = a$ by definition of addition. Thus $a \leq a$.

□

Proof 3c. Suppose $a \leq b$ and $b \leq c$. Let $d, e \in \mathbb{N}$ such that $a + d = b$ and $b + e = c$. Substituting the first equation into the second for b, we have $(a + d) + e = c$. By associativity, we have $a + (d + e) = c$, whence $a \leq c$.

□

Proof 3d. Suppose $a \leq b$ and $b \leq a$. Then $\exists b, c \in \mathbb{N}$ such that $a + c = b$ and $b + d = a$. Substituting the first equation into the second for b, we arrive at:

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

By associativity, we have $a + (c + d) = a$, and by definition of addition, we have

$$a + (c + d) = a + 0.$$

Using Problem 1, we can cancel the a's to get $c + d = 0$. Now suppose for a contradiction that $d \neq 0$. Then for some $e \in \mathbb{N}$, $S(e) = d$ (as in 3a). Using $c + d = 0$, we get $c + S(e) = 0$, which by the definition of addition results in $S(c + e) = 0$. By Axiom 7, this is necessarily false. Hence $d = 0$. But $b + d = a$, giving $b + 0 = a$, or identically $b = a$ as desired.

□