Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2022

Solutions to Assignment #5
Multiplication

Please give your complete reasoning in your solution. Recall that, unless stated otherwise on a given assignment, you are permitted to work together and look things up, so long as you write up your solution by yourself and acknowledge all sources and help that you ended up using.

Early in the term, and again more recently, we defined multiplication on the natural numbers from addition as follows:

- Let $n \cdot 0 = 0$ for all $n \in \mathbb{N}$.
- Given that $n \cdot k$ has been defined, let $n \cdot S(k) = (n \cdot k) + n$, where S is the successor function.

1. Show that multiplication of natural numbers is associative, that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, $c \in \mathbb{N}$. *[2]*

SOLUTION. To keep each step as simple as we can, it is convenient to first show that the left distributive law for multiplication over addition, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, holds for all x, y, $z \in \mathbb{N}$. We do this by induction on $z \in \mathbb{Z}$:

Base Step. $(z = 0)$ By the definitions of $\cdot$ and $+$ on the natural numbers, $x \cdot (y + 0) = x \cdot y = (x \cdot y) + 0 = (x \cdot y) + (y \cdot 0)$.

Inductive Hypothesis. $(z \leq n)$ Assume that for all x, y, $z \in \mathbb{N}$ with $z \leq n$, we have $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Inductive Step. $(z = n + 1 = S(n))$ Here we go:

$$\begin{aligned} x \cdot (y + z) &= x \cdot (y + S(n)) = x \cdot S(y + n) \quad \text{by the definition of } + \\ &= (x \cdot (y + n)) + x \quad \text{by the definition of } \cdot \\ &= ((x \cdot y) + (x \cdot n)) + x \quad \text{by the Inductive Hypothesis} \\ &= (x \cdot y) + ((x \cdot n) + x) \quad \text{by the associativity of } + \\ &= (x \cdot y) + (x \cdot S(n)) \quad \text{by the definition of } \cdot \\ &= (x \cdot y) + (x \cdot z) \end{aligned}$$

It follows by induction that the left distributive law is true for the natural numbers.

We now proceed to show that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, $\in \mathbb{N}$ by induction on c.

Base Step. ($c = 0$) By the definition of multiplication, $a \cdot (b \cdot 0) = a \cdot 0 = 0 = (a \cdot b) \cdot 0$ for all a, $b \in \mathbb{N}$.

Inductive Hypothesis. ($c \leq k$) Assume that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, $c \in \mathbb{N}$ with $c \leq k$.

Inductive Step. ($c = k + 1 = S(k)$) Here we go:

$$\begin{aligned}(a \cdot b) \cdot c = (a \cdot b) \cdot S(k) &= ((a \cdot b) \cdot k) + (a \cdot b) \quad \text{by the definition of } \cdot \\ &= (a \cdot (b \cdot k)) + (a \cdot b) \quad \text{by the Inductive Hypothesis} \\ &= a \cdot ((b \cdot k) + b) \quad \text{by the left distributive law} \\ &= a \cdot (b \cdot S(k)) \quad \text{by the definition of } \cdot \\ &= a \cdot (b \cdot c)\end{aligned}$$

Thus, by induction, multiplication of natural numbers is associative. ■

2. Show that multiplication of matural numbers is commutative, that is, $a \cdot b = b \cdot a$ for all a, $b \in \mathbb{N}$. *[3]*

Note. For **1** and **2** the proofs done in class that addition of natural numbers is associative and commutative, respectively, are useful models for how to proceed.

Solution. *Per* the note above, we will follow the proof done in class that $+$ is associative as far as possible. We will show that $a \cdot b = b \cdot a$ for all a, $b \in \mathbb{N}$ by induction on b, with subsidiary inductions at the base steps.

Base Step One. ($b = 0$) We show $a \cdot 0 = 0 = 0 \cdot a$ by induction on a.

Base Step. ($a = 0$) By the definition of $\cdot$, $0 \cdot 0 = 0 = 0 \cdot 0$.

Induction Hypothesis. ($a \leq k$) Assume that for all $a \in \mathbb{N}$ with $a \leq k$, we have $a \cdot 0 = 0 = 0 \cdot a$.

Inductive Step. ($a = k + 1 = S(k)$) Here we go:

$$\begin{aligned}0 \cdot a = 0 \cdot S(k) &= (0 \cdot a) + 0 \quad \text{by the definition of } \cdot \\ &= (a \cdot 0) + 0 \quad \text{by the Inductive Hypothesis} \\ &= 0 + 0 \quad \text{by the definition of } \cdot \\ &= 0 \quad \text{by the definition of } + \\ &= a \cdot 0 \quad \text{by the definition of } \cdot\end{aligned}$$

It follows by induction that $a \cdot 0 = 0 = 0 \cdot a$ for all $a \in \mathbb{N}$.

Base Step Two. ($b = 1 = S(0)$) We show $a \cdot 1 = a \cdot S(0) = a = S(0) \cdot a = 1 \cdot a$ for $a \in \mathbb{N}$ by induction on a.

> *Base Step.* ($a = 0$) $0 \cdot 1 = 0 \cdot S(0) = 0 = S(0) \cdot 0 = 1 \cdot 0$ by Base Step One above.
>
> *Induction Hypothesis.* ($a \leq n$) Assume that for all $a \in \mathbb{N}$ with $a \leq n$ we have $a \cdot 1 = a \cdot S(0) = a = S(0) \cdot a = 1 \cdot a$.
>
> *Inductive Step.* ($a = n + 1 = S(n)$) Here we go:
>
> $$\begin{aligned} a \cdot 1 = S(n) \cdot S(0) &= (S(n) \cdot 0) + S(n) \quad \text{by the definition of } \cdot \\ &= 0 + S(n) \quad \text{by the definition of } \cdot \\ &= S(n) + 0 \quad \text{by the commutativity of } + \\ &= S(n) = a \quad \text{by the definition of } + \\ &= S(n + 0) \quad \text{by the definition of } + \\ &= n + S(0) \quad \text{by the definition of } + \\ &= (n + 0) + S(0) \quad \text{by the definition of } + \\ &= (0 + n) + S(0) \quad \text{by the commutativity of } + \\ &= ((n \cdot 0) + n) + S(0) \quad \text{by the definition of } \cdot \\ &= (n \cdot S(0)) + S(0) \quad \text{by the definition of } \cdot \\ &= (S(0) \cdot n) + S(0) \quad \text{by the Induction Hypothesis} \\ &= S(0) \cdot S(n) \quad \text{by the definition of } \cdot \end{aligned}$$
>
> It follows by induction that $a \cdot 1 = a \cdot S(0) = a = S(0) \cdot a = 1 \cdot a$ for all $a \in \mathbb{N}$.

Induction Hypothesis. ($b \leq m$) Assume that $a \cdot b = b \cdot a$ for all a, $b \in \mathbb{N}$ with $b \leq m$.

Inductive Step. ($b = m + 1 = S(m)$) Here we go:

$$\begin{aligned} a \cdot b = a \cdot S(m) &= (a \cdot m) + a \quad \text{by the definition of } \cdot \\ &= (a \cdot m) + (a \cdot S(0)) \quad \text{by part of Base Step Two} \\ &= a \cdot (m + S(0)) \quad \text{by the left distributive law (see } \mathbf{1} \text{ above)} \\ &= a \cdot S(m) \quad \text{by the definition of } + \\ &= a \cdot b \end{aligned}$$

It follows by induction that $a \cdot b = b \cdot a$ for all a, $b \in \mathbb{N}$. Note that one consequence is that the right distributive law now follows from the left distributive law.■

3. Define exponentiation of natural numbers (with 0^0 set to 1) and prove what algebraic properties you can about it. *[3]*

Hint: Exponentiation is to multiplication as multiplication is to addition, more or less. However, exponentiation is neither associative nor commutative, though it has some basic algebraic properties that are useful and you should already be familiar with using.

SOLUTION. Setting $0^0 = 1$ makes it a little easier to state the definition because you don't have to make an exception for 0:

- For all $n \in \mathbb{N}$, let $n^0 = 1 = S(0)$.
- Given that n^k has been defined, let $n^{S(k)} = n^{(k+1)} = \left(n^k\right) \cdot n$.

Note that one side effect of the second part of the definition is that $0^k = 0$ for all $k > 0$.

The most familiar algebraic properties of exponentiation are the rules $\left(a^b\right)\cdot(a^c) = a^{(b+c)}$ and $\left(a^b\right)^c = a^{(b\cdot c)}$, which we shall verify for all a, b, $c \in \mathbb{N}$.

i. We show that $\left(a^b\right) \cdot (a^c) = a^{(b+c)}$ for all a, b, $c \in \mathbb{N}$ by induction on c:

Base Step. ($c = 0$) Recall, from Base Step Two of **2** above, that $n \cdot 1 = n \cdot S(0) = n$ for all $n \in \mathbb{N}$. Then:

$$\begin{aligned} \left(a^b\right) \cdot \left(a^0\right) &= \left(a^b\right) \cdot 1 \quad \text{by the definition of } x^y \\ &= a^b \quad \text{by part of Base Step Two in } \mathbf{2} \\ &= a^{(b+0)} \quad \text{by the definition of } + \end{aligned}$$

Inductive Hypothesis. ($c \le k$) Assume that $\left(a^b\right) \cdot (a^c) = a^{(b+c)}$ for all a, b, $c \in \mathbb{N}$ with $c \le k$.

Inductive Step. ($c = k + 1 = S(k)$) Here goes:

$$\begin{aligned} \left(a^b\right) \cdot (a^c) &= \left(a^b\right) \cdot \left(a^{k+1}\right) \\ &= \left(a^b\right) \cdot \left(\left(a^k\right) \cdot a\right) \quad \text{by the definition of } x^y \\ &= \left(\left(a^b\right) \cdot \left(a^k\right)\right) \cdot a \quad \text{by the commutatitivity of } \cdot \\ &= \left(a^{(b+k)}\right) \cdot a \quad \text{by the Inductive Hypothesis} \\ &= a^{((b+k)+1)} \quad \text{by the definition of } x^y \\ &= a^{(b+(k+1))} \quad \text{by the associativity of } + \\ &= a^{(b+c)} \end{aligned}$$

It follows by induction that $\left(a^b\right) \cdot (a^c) = a^{(b+c)}$ for all a, b, $c \in \mathbb{N}$.

ii. We show that $\left(a^b\right)^c = a^{(b \cdot c)}$ for all a, b, $c \in \mathbb{N}$ by induction on c:

Base Step. $(c = 0)$ Here we are:

$$\begin{aligned} \left(a^b\right)^0 &= 1 \quad \text{by the definition of } x^y \\ &= a^0 \quad \text{by the definition of } x^y \\ &= a^{(b \cdot 0)} \quad \text{by the definition of } \cdot \end{aligned}$$

Inductive Hypothesis. $(c \leq k)$ Assume that $\left(a^b\right)^c = a^{(b \cdot c)}$ for all a, b, $c \in \mathbb{N}$ with $c \leq k$.

Inductive Step. $(c = k + 1 = S(k))$ Here goes:

$$\begin{aligned} \left(a^b\right)^c = \left(a^b\right)^{(k+1)} &= \left(\left(a^b\right)^k\right) \cdot \left(a^b\right) \quad \text{by the definition of } x^y \\ &= \left(a^{(b \cdot k)}\right) \cdot \left(a^b\right) \quad \text{by the Inductive Hypothesis} \\ &= a^{((b \cdot k)+b)} \quad \text{by part } i \text{ above} \\ &= a^{(b \cdot S(k))} \quad \text{by the definition of } \cdot \\ &= a^{(b \cdot c)} \end{aligned}$$

It follows by induction that $\left(a^b\right)^c = a^{(b \cdot c)}$ for all a, b, $c \in \mathbb{N}$.

And that will do! ■