E. Try to prove Thm 2.7.1 by induction on \( b \). Where do you first get stuck? If you could somehow overcome that problem, where would you get stuck next?

**Ans E.** We are told for each \( b \) to let \( P(b) \) be the claim: for all nonnegative integers \( a, c \) we have \( a(b+c) = ab + ac \). But then there is already trouble proving \( P(0) \): \( a(0 + c) = a0 + ac \). By the def of + we can reduce the LHS to \( ac \), but we cannot reduce the RHS until we know that \( a0 = 0 \). Unfortunately, the def of multiplication merely says that \( 0a = 0 \).

Now, just as all addition facts can be proved before any multiplication facts, it may be that the fact that multiplication commutes can be proved before proving that multiplication distributes over addition (although we proceed in the opposite order in [FM] below). If so, in the current proof of distributivity we could say \( a0 + ac = 0 + ac = ac \), the last equality by the def of +. That would finish \( P(0) \).

Even so, there will be more problems in the inductive step, \( P(b) \implies P(b+1) \). We want \( a((b+1)+c) = a(b+1) + ac \). Starting with the LHS, we can say \( a((b+1)+c) = a((b+c)+1) \) (def of + applied to \( (b+1) + c \)), but now we are really in trouble, because to expand \( a((b+c)+1) \) we need \( P(b+c) \), which is a later case of \( P \).

EE. From the definition of addition, justify that \( 0 + 0 = 0 \).

**Ans EE.** The basis case \( P(0) \) of the definition of addition is that \( 0 + n = n \) for all integers \( n \). The particular instance \( n = 0 \) is that \( 0 + 0 = 0 \). (This would be a proof even if we didn’t know that both sides simplify to 0.)

F. Using Definition 2.7.2, prove that \( 0 + n = n + 0 \) for all natural numbers \( n \).

**Ans F.** For each \( n \), let \( P(n) \) be the claim that \( 0+n = n+0 \). We will prove \( P(n) \) for all natural numbers \( n \) by induction (i.e., for all nonnegative integers \( n \)).

Basis, \( P(0) \): This says that \( 0 + 0 = 0 + 0 \), which is surely true since both sides are the same. (This would be a proof even if we didn’t know that both sides simplify to 0.)

\[
P(n) \implies P(n+1):
\]

\[
0 + (n+1) = n + 1 \quad \text{[basis case of def of +]}
\]
\[
= (0+n) + 1 \quad \text{[ditto, applied to \( n \)]}
\]
\[
= (n+0) + 1 \quad \text{[\( P(n) \)]}
\]
\[
= (n+1) + 0 \quad \text{[def of \( (n+1) + m \) with \( m = 0 \)]}
\]
FA. Here are the steps of an inductive proof that natural number addition is associative. Your job is to figure out where we are at each line (basis? inductive step?) and what the justification is for that line.

1) \( 0 + (b + c) = b + c \)
2) \( = (0 + b) + c. \)
3) \( (a + 1) + (b + c) = [a + (b + c)] + 1 \)
4) \( = a + [(b + c) + 1] \)
5) \( = a + [(b + 1) + c] \)
6) \( = [a + (b + 1)] + c \)
7) \( = [(a + b) + 1] + c \)
8) \( = [(a + 1) + b] + c. \)

Ans FA. First, we are doing induction on \( P(a) \): \( a + (b + c) = (a + b) + c \) for all nonnegative integers \( b, c \).

The only thing we assume about addition is the inductive definition.

Basis, \( P(0) \):

1) \( 0 + (b + c) = b + c \) \[ def of + in case 0 + n with n = b + c \]
2) \( = (0 + b) + c. \) \[ ditto with n = b \]

\( P(a) \Rightarrow P(a+1) \):

3) \( (a + 1) + (b + c) = [a + (b + c)] + 1 \) \[ inductive def of + \]
4) \( = a + [(b + c) + 1] \) \[ P(a) with b \leftarrow b + c, c \leftarrow 1 \]
5) \( = a + [(b + 1) + c] \) \[ inductive def of + applied to b + 1 \]
6) \( = [a + (b + 1)] + c \) \[ P(a) with b \leftarrow b + 1 \]
7) \( = [(a + b) + 1] + c \) \[ P(a) applied within brackets \]
8) \( = [(a + 1) + b] + c. \) \[ def of + applied within brackets \]

FC. Combine the cases \( m = 0 \) and \( m = 1 \) of the definition of \( m + n \) and conclude that \( 1 + n = n + 1 \).

In other words, the first two cases of Definition 2.7.2 imply commutativity for \( m = 1 \), so it’s not surprising we could prove commutativity in general by induction.

Ans FC.

\( 0 + n = n. \) \[ basis case of def of + \]
\( 1 + n = (0 + n) + 1 \) \[ inductive part of def of + with m = 0 \]
\( = n + 1. \) \[ substitute basis case \]

FE. Critique the following claim about Def 2.7.2. “Even if it is assumed we already understand what \( n + 1 \) means for any natural number \( n \), the definition still doesn’t make sense. In order to understand the 2nd display, we need to know what \( m + n \) means for any \( m \) and \( n \), that is, we already have to understand all about addition.”
Ans FE. The 2nd display referred to is
\[(m+1) + n = (m+n) + 1.\] (2)

The use of \(m+n\) on the right is a previous case, since the definition is by induction on \(m\) (and thus \(n\) arbitrary). In a recursive definition, we are allowed to jump into the middle, assume we already know what the previous case means, in order to define the next case. This assumption is warranted because it is justified once we start from the basis case and work upwards forever, defining all cases one at a time.

FG. There are two places in Def 2.7.2 where adding 1 after a number is assumed to be already understood: in \(m + 1\) on the LHS of the 2nd display, and in \((m+n) + 1\) on the RHS. Does the RHS instance cause the same problem as the LHS instance, or is it all right as part of the recursivity of the definition?

Ans FG. The successor function (that is, adding 1 as opposed to adding an arbitrary nonnegative integer \(n\)) has to be assumed understood for all nonnegative integers before Def. 2.7.2 makes sense.

FL. From the definition of multiplication of positive integers, prove
\[\begin{align*}
a) \quad 1 \cdot n &= n, \\
b) \quad 2 \cdot n &= n + n
\end{align*}\]

Ans FL. For reference, we repeat and label the two parts of the definition of multiplication:
\[\begin{align*}
0n &= 0, \quad (1) \\
(m+1)n &= mn + n \quad (2)
\end{align*}\]

Also remember that we are assuming that all facts about addition alone (not addition mixed with multiplication) have already been proved earlier in the development.
\[\begin{align*}
a) \quad 1n &= 0n + n \\
&= 0 + n \\
&= n. \\
&\quad \text{[(2) with } m = 0] \\
&\quad \text{[(1)]} \\
&\quad \text{[addition fact]}
\end{align*}\]
\[\begin{align*}
b) \quad 2n &= 1n + n \\
&= n + n. \\
&\quad \text{[(2) with } m = 1] \\
&\quad \text{[part a]}
\end{align*}\]

FM. Prove that multiplication of natural numbers is commutative. You may assume all standard facts about addition of natural numbers. From the text, you may also assume the definition of multiplication and the fact that multiplication is distributive.
\[\begin{align*}
a) \quad \text{Assume also that } n \cdot 0 &= 0 \text{ and } n \cdot 1 &= n. \quad (\text{Where do you need these?})
\end{align*}\]
\[\begin{align*}
b) \quad \text{Don’t assume } n \cdot 0 &= 0 \text{ and } n \cdot 1 &= n. \quad \text{That is, prove these from the other assumptions before starting the proof of commutativity.}
\end{align*}\]

Ans FM. We continue to refer to the parts of the definition of multiplication as (1) and (2) as in the solution to [FL].
a) For each $m$, let $P(m)$ be the statement that for all nonnegative integers $n$, we have $mn = nm$. We prove commutativity of nonnegative integers under multiplication by proving $P(m)$ for all $m \geq 0$. (In other words, we have two variables $m, n$ and we do induction on $m$.)

$P(0)$: $0 \cdot n = 0 = n \cdot 0$.

$P(m) \Rightarrow P(m+1):$

\[(m+1)n = mn + n \quad [\text{(2)}] \]
\[= nm + n \quad [P(m)] \]
\[= nm + n \cdot 1 \quad \text{[told we could assume]} \]
\[= n(m+1). \quad \text{[distributive law]} \]

b) First we prove $n \cdot 0 = 0$.

For $n = 0$, we want to verify that $0 \cdot 0 = 0$; this is true by (1). For the inductive step,

\[(n+1) \cdot 0 = n \cdot 0 + 0 \quad [\text{(2)}] \]
\[= 0 + 0 \quad \text{[previous case]} \]
\[= 0. \quad \text{[addition fact]} \]

Next is an inductive proof that $n \cdot 1 = n$. The basis, $n = 0$ is true by (1) with $n$ there $= 1$. For $P(n) \Rightarrow P(n+1)$, we have

\[(n+1) \cdot 1 = n \cdot 1 + 1 \quad [\text{(2) with } m = n \text{ and } n = 1] \]
\[= n + 1. \quad [P(n)] \]

The main proof of $mn = nm$ proceeds exactly as before, except where we made assumptions before we now refer to the proofs.

FP. Assuming we have proved that multiplication of natural numbers commutes ($mn = nm$) and continuing to assume we know all about addition, prove the right-distribution law:

\[(p + q)n = pn + qn. \]

Ans FP.

\[(p + q)n = n(p + q) \quad \text{[mult commutes]} \]
\[= np + nq \quad \text{[left distribution (proved earlier)]} \]
\[= pn + qn. \quad \text{[mult commutes (twice)]} \]

FR. Assuming the result of Problem FP and everything assumed in FP, prove the “foil theorem” (first, outer, inner, last):

\[(a + b)(p + q) = ap + aq + bp + bq. \]
Ans FR.

\[(a + b)(p + q) = a(p + q) + b(p + q) \quad \text{[right distrib with } n = p + q]\]
\[= ap + aq + bp + bq \quad \text{[left distrib twice]}\]

FX. In the discussion of the definition of addition for the natural numbers, we noted that one has to start by defining the successor for every number — 1 follows 0, 2 follows 1, and so on. Unfortunately, this naming of all the natural numbers requires infinitely many definitions, and there isn’t enough room on the page. We need a definition schema, that is, a precise but generic description of these definitions. One way to get it would be to provide a recursive definition of the set of desired definitions! Another way would be to write an algorithm which can, on demand, produce any one of the definitions.

Write such an algorithm. Given the name of a natural number (in decimal digits), it should return the name of its successor.

Is this closely related to some problem discussed earlier in the book?