In Example 1 of Section 2.3, we asserted that the proof of the distributive law, \( a(b+c) = ab + ac \), involves induction. We now prove this law. Such basis facts are part of the foundations of mathematics. Since the usual purpose of the study of foundations is to be absolutely certain of such facts, you should now watch us with an especially critical eye, to see if you have any objections to our proof.

One can't prove anything about multiplication unless multiplication is first defined. Here's the first place induction plays a role: we use an inductive definition. Multiplication involves two factors; our definition involves induction on the first.

**Definition 2.7.1.** Multiplication of natural numbers is defined by

\[
0 \cdot n = 0, \\
(m+1)n = mn + n
\]

**Theorem 2.7.1.** For all natural numbers \( a, b, c \),

\[ a(b + c) = ab + ac. \]

Proof: By induction on \( a \). In other words, we let \( P(a) \) be the claim that \( a(b+c) = ab + ac \) for all natural numbers \( b \) and \( c \). (Note: here is one of those cases where a multiple induction can be avoided, but it makes a difference which one variable you choose to induct on [E].)

Basis. \( P(0) \) is true because

\[
0(b + c) = 0 \\
= 0 + 0 \\
= 0 \cdot b + 0 \cdot c. \quad [\text{def. of mult. used twice}]
\]

Inductive Step. Assume \( P(a) \) and prove \( P(a+1) \). Starting with the LHS of \( P(a + 1) \) we have
\[(a + 1)(b + c) = a(b + c) + (b + c) \quad \text{[def. of mult.]}\]
\[= (ab + ac) + (b + c) \quad \text{[P(a)]}\]
\[= (ab + b) + (ac + c) \quad \text{[rearrange terms]}\]
\[= (a + 1)b + (a + 1)c \quad \text{[def. of mult. used twice]}\]

Thus we have \(P(a+1)\), completing the proof.

By now you should have two sorts of objections. On the one hand, we have proved too little: We have worked with the natural numbers; what about the other integers, the rational numbers, the real numbers, the complex numbers? On the other hand, we have assumed too much: what’s this justification above by “rearrange terms”? If we are trying to prove something so basic as the distributive law, what allows us to use the associative and commutative laws? Even something as basic as \(0 = 0 + 0\) in the basis step demands further proof [EE].

We agree with your objections! If our goal here were to obtain absolute certainly about the distributive law, we would hardly be done. However, our goal is merely to illustrate the use of induction in justifying the basic laws of arithmetic and algebra. True, we have proved too little, but the extension of the proof to those other number systems does not involve induction. (It could use induction in the case of the integers, since we could do induction on \(-1, -2, \ldots\), but since these numbers are a mirror image of the positive integers, it is easier not to use induction again. As for the other number systems mentioned, they don’t have the property that you can get to them all but starting at one of them and repeatedly adding 1 — a point we will return to below.)

As for assuming too much, you must at least concede that our reasoning was not circular. We did not assume the distributive law, which is about both multiplication and addition. Indeed, every “suspect” thing we assumed is a fact about addition alone. Remember, we jumped into the middle of the foundations problem to give an illustration. It is quite possible that these suspect facts could have been proved earlier in the process.

Indeed, they can be — also by induction. To illustrate this we carry the foundations process a little farther back and outline the proof that addition of natural numbers is commutative: \(m + n = n + m\). Naturally enough, to begin with this requires a
**Definition 2.7.2.** For natural numbers \( m \) and \( n \), their sum \( m + n \) is defined by

\[
0 + n = n, \\
(m+1) + n = (m+n) + 1.
\]

**Theorem 2.7.2.** Addition of natural numbers is commutative, that is,

\[ m + n = n + m. \]

Proof: We do induction on \( m \), i.e., let \( P(m) \) be the statement that \( m+n = n+m \) for all natural numbers \( n \).

Basis. \( P(0) \) states: \( 0 + n = n + 0 \) for all \( n \). We know that \( 0 + n = n \) from the definition of addition. But although everybody knows that \( n + 0 = n \) too, that’s not part of what we have been told. In other words, 0 has been defined to be a “left identity” but the fact that it is a “right identity” is going to have to be another theorem, one we need to prove before Thm 2.7.2. It can be done, and it’s not too hard — it’s another induction [F].

Inductive Step. Assuming \( P(m) \), we write down the LHS of \( P(m+1) \) and see what we can do:

\[
(m+1) + n = (m+n) + 1 \quad \text{[def. of add.]} \\
= (n+m) + 1 \quad \text{[} P(m) \text{]} \\
= n + (m+1) \quad \text{[Associative Law]}
\]

Having reached the RHS of \( P(m+1) \), we are done. \[]

Of course, this is only a proof assuming that natural number addition is associative. So once again we have identified yet another standard property which must be proved earlier. This one is pretty tricky; [FA] steps you through it.

At this point it should be plausible that there is some order in which all the basic properties of natural numbers can be proved (using induction) so that no proof depends on a property that isn’t proved until later. Not only is it plausible, it’s true — but it took a number of famous mathematicians around the beginning of the century many years of work to show it! (Much of the work involves even deeper foundations — reducing numbers to sets and sets to logic.)
There is one final matter about foundations which deserves comments. There is a problem with Def. 2.7.2. Although it purports to be a definition of addition, we can’t even make sense of its 2nd display unless we already understand what $n + 1$ means. And once we understand what it means, there are a whole sequence of special names. Thus, along with this general definition, we need a whole set of particular definitions —

1+1 is given the name 2,
2+1 is given the name 3,
3+1 is given the name 4,

and so on. Another way to put this is: the natural numbers come with a successor function as part of their definition (where the successor of 1 is 2, and so on), and the first step in defining addition is to define $n + 1$ to mean the successor of $n$. 

Problems

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?

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

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

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) \( = [(a+1)+b] + c. \)

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.

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.”

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?
**FL.** From the definition of multiplication of positive integers, prove

a) \(1 \cdot n = n\),  
b) \(2 \cdot n = n + n\)

**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.

a) Assume also that \(n0 = 0\) and \(n \cdot 1 = n\). (Where do you need these?)

b) Don’t assume \(n0 = 0\) and \(n \cdot 1 = n\). That is, prove these from the other assumptions before starting the proof of commutativity.

**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:

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

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

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

**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 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?