Research Methods in Mathematics
Lecture 3: Addition, multiplication and inequality

T. PERUTZ

Addition and multiplication

The definition of addition of done natural numbers is done inductively. We want to define $n+m$. We first define $n+1=S(n)$. Next, we define $n+S(1)=S(n+1)$. In general, if $n+m$ has already been defined, we set $n+S(m)=S(n+m)$.

Is this a valid definition? Yes: let $P(m)$ be the statement '$n+m$ has been defined'. Then, by induction, $P(m)$ is true for all natural numbers m.[1]

A first theorem—one we will not prove—is as follows:

Theorem 1 *For all natural numbers m, n and p, we have*

(1) $(m+n)+p=m+(n+p)$;

(2) $m+n=n+m$.

Because of (1), we can unambiguously write $m+n+p$ without specifying the brackets.

Next we come to multiplication. Again, we define mn by induction on n: we set $m1=1$ and $mS(n)=mn+n$.

Theorem 2 *For all natural numbers m, n and p, we have*

(1) $(mn)p=m(np)$;

(2) $m1=m$ *(this is true by definition!);*

(3) $mn=nm$.

There is also a result that relates addition to multiplication:

Theorem 3 *For all natural numbers m, n and p, we have $(m+n)p=mp+np$.*

The properties of addition and multiplication described by the three theorems are fundamental ones that will be shared by several number systems which appear in this course.

[1] You might ask: is the sentence '$n+m$ has been defined' something that should be legitimately considered a statement? What *is* a statement? Logicians attempt to answer this question, but we shall go no deeper into this particular rabbit-hole.

Inequality

Define a natural number m to be *greater than* n, and write $m > n$, if there is a natural number q such that $n + q = m$.

Theorem 4 *Let m and n be natural numbers. Then exactly one of the following three statements is true: (i) $m > n$; (ii) $n > m$; (iii) $m = n$.*

Proof For a given n, let $Q(n)$ be the statement that the theorem holds for all m. We prove $Q(n)$ by induction on n.

We start with $Q(1)$. We have to prove that exactly one of the following holds: $m > 1$; $1 > m$; or $m = 1$. Notice that $1 > m$ is never true, because if $1 = m + q$ then 1 is the successor of something, which it is not. So we must prove statement $P(m)$: that $m > 1$ or $m = 1$, but not both. This we prove by induction on m! If $m = 1$ then it is not true that $m > 1$ (because 1 is not a successor) so $P(1)$ is true. Assuming $P(m)$, we prove $P(S(m))$. So m is either equal to 1 or to $m + q$ for some q. Then $S(m)$ is equal either to $1 + 1$ or to $m + S(q)$; thus $S(m) > 1$. And $S(m) \neq 1$, as 1 is not a successor. This proves that the inductive step; so $P(m)$ is true for all m.

Now consider the inductive step. We know $Q(n)$ and we must prove $Q(S(n))$. If $n > m$ then certainly $S(n) > m$ too. If $n = m$ then $S(n) > m$. If $m > n$ then $m = n + q$, say. Either $q = 1$, in which case $m = S(n)$; or $q > 1$ (by $Q(1)$) in which case q is a successor $S(p)$, and $m = n + S(p) = S(n) + p$ so $m > S(n)$. So one of the three possibilities definitely holds.

Problem: complete the proof by showing inductively that it's impossible for two of the possibilities to hold simultaneously. □

Summary so far: The axioms for the natural numbers encode the concepts '1' and 'adding one'. They also encode the principle of mathematical induction. Granting that a system satisfying the axioms exists, one can deduce addition, multiplication, inequality, and the familiar properties of these structures.

Spivak reference: chapters 1–2.

The integers

Addition and multiplication of natural numbers have the following properties.

▷ SIX PROPERTIES OF $+$ AND $\times$:

$+$ is associative:	$(m+n)+p = m+(n+p)$
$+$ is commutative:	$m+n = n+m$
$\times$ is associative:	$(mn)p = m(np)$
1 is a unit:	$m1 = m$
$\times$ is commutative:	$mn = nm$
$\times$ distributes over $+$:	$(m+n)p = mp+np$.

We have also shown that for any two natural numbers n and m, exactly one of three possibilities holds: $m > n$, $n > m$, or $n = m$.

Inequality is related to subtraction. If $n > m$, one can define $n - m$ as the unique natural number q such that $n = m+q$. However, if $n = m$ or $m > n$, no such q exists and so one cannot sensibly define $n - m$.

The advantage of the *integers* is that subtraction is always possible. The integers are the numbers

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots.$$

Collectively, they are denoted by $\mathbb{Z}$.[2] For each natural number n, one also has an integer n and an integer $-n$. Every integer m is either 0, or there is a natural number n so that $m = n$, or one so that $m = -n$. Addition and multiplication are defined, and besides the six properties ▷, the following hold:

† TWO MORE PROPERTIES OF $+$ AND $\times$ IN $\mathbb{Z}$

- There is an integer 0 so that, for all integers a, one has $0 + a = a$.
- Given an integer a, there exists an integer $-a$ such that $a + (-a) = 0$.

Example 5 Another familiar fact is that $0a = 0$ for any a. Prove that this follows from the properties we have already listed.

A definition of the integers

How to *define* the integers, starting from the natural numbers?

Perhaps the neatest way is to use subtraction as the starting point of the definition. We define an integer to be represented by a pair (a, b) of natural numbers, which

[2] This letter is used because the German word for number is 'Zahl'.

we write as $a - b$. Two pairs $a - b$ and $a' - b'$ represent the same integer if there is some natural number c such that $a' = a + c$ and $b' = b + c$, or such that $a = a' + c$ and $b = b' + c$. Thus $(b + c) - (a + c) = b - a$. We can then define addition of integers by $(a - b) + (c - d) = (a + c) - (b - d)$, and multiplication by $(a - b)(c - d) = (ac + bd) - (bc + ad)$. You then have to check that all the properties, as listed above, are satisfied.