Math 4030-001/Foundations of Algebra/Fall 2017

Numbers at the Foundations: The Natural Numbers

We start with the **Natural Numbers**. This is the set

$$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$$

of "counting" numbers together with their ordering:

$$1 < 2 < 3 < 4 < ...$$

Remark. A set with an ordering of its elements is called an *ordered set*.

There is one **axiom** of the set of natural numbers that we will adopt. An axiom is a statement that we may assume to be true without proof. It is, colloquially, a statement whose truth we hold to be self-evident.

The Well-Ordered Axiom: Every set of natural numbers except the empty set has a unique smallest element.

Examples are pretty obvious, since if we list the elements of $S \subset \mathbb{N}$ in order, the smallest element is the first in the list. For example, the first odd natural number is 1 and the first even natural number is 2.

Remarks. (a) The empty set fails because it has **no** elements!

(b) Plenty of subsets of natural numbers can have no *largest* element. In fact, a subset of $\mathbb{N}$ has a largest element if and only if it is finite.

From the well-ordered axiom we may prove the:

Principle of induction: If S is a subset of $\mathbb{N}$ satisfying:

(i) $1 \in S$ and

(ii) $(\forall n \in \mathbb{N})\ n \in S \Rightarrow n + 1 \in S$

then $S = \mathbb{N}$.

Proof: Let S sastify (i) and (ii) and consider the complement S^c. This is a set of natural numbers, so we may use the well-ordered axiom to conclude that either S^c is empty or S^c has a smallest element.

We now prove (a proof within a proof!) by contradiction that S^c has no smallest element. Suppose **p:** S^c has a smallest element. Call it $m \in S^c$. If $m = 1$, then we have a false statement, namely $1 \in S$ (because of (i)) and $1 \in S^c$. Otherwise $m > 1$ and (ii) is equivalent to:

$$(\forall n \in \mathbb{N})\ n + 1 \in S^c \Rightarrow n \in S^c$$

which says in particular that $m - 1 \in S^c$, which is also false because m was the smallest element of S^c. This proves S^c has no smallest element.

Now we return to the larger proof. We used the well-ordered axiom to conclude that S^c is empty or it has a smallest element and we also proved that S^c has **no** smallest element, so S^c is empty, i.e. $S = \mathbb{N}$. $\square$

Remark. The principle of induction is ubiquitous in mathematics. Any time you might be tempted to write the abbreviation "etc." or "..." in a proof or definition, you are probably using the principle of induction.

Examples. (a) The definition of the factorial for all natural numbers may be made by induction:

$$\text{(i) } 1! = 1 \quad \text{and} \quad \text{(ii) } (\forall n)\ (n+1)! = (n+1) \cdot n!$$

where (i) gives the definition of 1! and (ii) gives the definition of $(n+1)!$, provided that the definition of of $n!$ has first been given. In other words, this "algorithm" defines the factorial for a set S of natural numbers such that $1 \in S$ and $(\forall n \in \mathbb{N})\ n \in S \Rightarrow n+1 \in S$. By the principle of induction, this means $S = \mathbb{N}$. Of course, we usually write:

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 1$$

to mean the same thing (the product of the first n natural numbers).

(b) The sum of the first n integers has no "factorial-like" notation, but it is given by a formula that can be verified by induction.

$$(*)\ n + (n-1) + \cdots + 1 = \frac{(n+1)n}{2}$$

Proof. The set S of natural numbers for which $(*)$ is true satisfies:

(i) $1 \in S$:

$$1 = \frac{2 \cdot 1}{2}$$

(ii) $(\forall n \in \mathbb{N})\ n \in S \Rightarrow n+1 \in S$:

$$\text{Suppose } n + (n-1) + \cdots + 1 = \frac{(n+1)n}{2}. \text{ Then}$$

$$(n+1) + n + \cdots + 1 = (n+1) + \frac{(n+1)n}{2}$$

$$= (n+1) + \frac{n^2+n}{2} = \frac{2(n+1) + n^2 + n}{2} = \frac{n^2+3n+2}{2} = \frac{(n+2)(n+1)}{2}$$

$$= \frac{((n+1)+1)(n+1)}{2}$$

Therefore, by the principle of induction, $(*)$ is true **for all** n. $\square$

Remark. The expressions $1 \in S$ and$(\forall n \in \mathbb{N})\ n \in S \Rightarrow n+1 \in S$ above are not part of the demonstration of the proof, but are there to clarify for the reader what we are trying to prove.

Recall that the nth **power** is defined by repeated multiplication, which can be reinterpreted as a definition by induction:

Definition 4.1. Given a natural number m, let:

$$\text{(i) } m^1 = m \text{ and } \text{(ii) } (\forall n)\ m^{n+1} = m^n \cdot m$$

to obtain a definition of m^n for all natural numbers n.

Remark. This defines an *operation* on pairs of natural numbers that is neither associative nor commutative:

$$(2^3)^2 = 64 \text{ and } 2^{(3^2)} = 512$$

$$2^3 = 8 \text{ and } 3^2 = 9$$

(two proofs of existence).

The power does distribute with multiplication, though.

$$(mk)^n = m^n k^n$$

may be proved by induction as follows:

(i) $(mk)^1 = mk = m^1 k^1$

(ii) $(\forall n)$ if $(mk)^n = m^n k^n$, then

$(mk)^{n+1} = (mk)^n (mk) = (m^n k^n)(mk) = (m^n m)(k^n k) = m^{n+1} k^{n+1}$

Therefore the identity holds for all natural numbers n. □

Remark. In part (ii) of this proof, we have assumed the associative and commutative laws of the operation of multiplication.

Exponential Properties. (a) $m^{k+n} = m^k \cdot m^n$ (b) $(m^k)^n = m^{kn}$

Proof. We will prove both of these by induction.

(a) For each fixed value of m and k,

(i) $m^{k+1} = m^k m = m^k m^1$.

(ii) $(\forall n)$ if $m^{k+n} = m^k m^n$, then

$$m^{k+n+1} = m^{k+n} m = m^k m^n m = m^k m^{n+1}$$

(b) (i) $(m^k)^1 = m^k = m^{k \cdot 1}$.

(ii) $(\forall n)$ if $(m^k)^n = m^{kn}$, then

$(m^k)^{n+1} = (m^k)^n \cdot m^k = m^{kn} \cdot m^k = m^{kn+k} = m^{k(n+1)}$ □

Remark. Inside the proof of (b) part (ii), the truth of (a) was assumed. This is allowed since (a) was proved before (b). If the proof of (a) had also assumed the truth of (b) (which it didn't!), the logic would have been circular and invalid. Beware of circular logic!

Since multiplication is also defined by repeated addition we could backtrack and define multiplication as repeated addition by induction.

Definition 4.2. Given a natural number m, let:

$$\text{(i) } m \cdot 1 = m \quad \text{and} \quad \text{(ii) } (\forall n)\ m(n+1) = mn + m$$

to define mn for all natural numbers n.

Remark. Multiplication bears the same relationship to addition that exponentiation bears to multiplication. From that point of view it is a bit surprising that multiplication is associative and commutative! After all, exponentiation is neither.

Proofs of Commutativity and Associativity of Multiplication.

(a) The number mn can be interpreted as the number of dots in an $m \times n$ array in the plane. There is a *symmetry* of the plane exchanging x and y coordinates under which $m \times n$ arrays of dots are exchanged with $n \times m$ arrays of dots. So they have the same number of dots.

(b) The number of dots in an $m \times n \times k$ grid in three-space agrees with both $(mn)k$ and $m(nk)$ since the $m \times n \times k$ grid may be viewed either as k copies of the $m \times n$ array in the xy-plane or else as m copies of the $n \times k$ grid in the yz-plane.

Remark. These new sorts of proofs appeal to geometry and symmetry. One might instead choose to prove commutativity and associativity by induction, to keep the algebra "free" of geometric intuition.

We may backtrack further and define addition by induction:

Definition 4.3. Given a natural number m, let:

(i) $m+1 =$ the number after m and (ii) $(\forall n)\ m+(n+1) = (m+n)+1$

to define $m + n$ for all natural numbers n.

Proofs of the Commutativity and Associativity of Addition.

(a) The number $m+n$ can be interpreted as the number of elements in the disjoint union of a set with m elements and a set with n elements. Since the union is a commutative operation, $m + n = n + n$.

(b) The number of elements in the disjoint union of three sets with m, n and k elements agrees with both $(m + n) + k$ and $m + (n + k)$.

Remark. One could also prove these by induction.

Now that we have settled the operations of arithmetic of natural numbers, we can get on to divisibility and more consequences of the well-ordered axiom.

Definition 4.4. (a) We say n **divides** m (or n is a **factor** of m) if

$$m = nk \text{ for some } k \in \mathbb{N}$$

We write $n|m$ to mean "n divides m."

(b) $p > 1$ is **prime** if the only numbers that divide p are 1 and p.

Remark. Since 1 divides **all** natural numbers and dividing by 1 is an uninteresting operation, we do not consider 1 to be a prime number. The primes under 50 are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$.

The Factorization Theorem. Every natural number $n > 1$ is the product of finitely many prime numbers.

Proof. Let S be the set of numbers that are greater than 1 and are **not** a product of finitely many prime numbers. Then either $S = \emptyset$ (and the Theorem is proved) or else by the well-ordered axiom S has a unique smallest element. Let's assume this and call this element m.

Since m is not a finite product of primes, m is in **not** itself prime. Thus m has a factor other than 1 and m. Call the factor n and write:

$$m = nk$$

Then $1 < n < m$ and $1 < k < m$. Since each of them is smaller than m and m is the smallest element of S, it follows that n and k are both products of finitely many primes. But if:

$$n = p_1 \cdots p_a \text{ and } k = q_1 \cdots q_b \text{ then } m = nk = (p_1 \cdots p_a)(q_1 \cdots q_b)$$

is therefore **not** and element of S, which is a contradiction. So our assumption is false. There is no such m, and S is empty. □

Remark. We have not yet proved **unique** factorization as a product of primes. In other words, we have only proved that $n = p_1 \cdots p_a$, but we haven't proven that n can't be a product of **other** primes as well. We will prove this in the next section. This is enough, however, for:

Theorem (Euclid). There are infinitely many primes.

Proof. Assume there are finitely many primes and list them:

$$p_1, p_2, ..., p_n$$

Now consider the natural number $m = p_1 \cdot p_2 \cdots p_n + 1$.

Since each $p_i > 1$, it follows that each p_i does **not** divide m, which nevertheless must have a finite prime factorization by the Theorem. Thus there are primes **other than** $p_1, ..., p_n$ appearing as factors of m. This contradicts the assumption that there are finitely many primes, and therefore there must be infinitely many primes. □

Example. If we thought 2 and 7 were the only primes, we'd take:

$$2 * 7 + 1 = 15 = 3 * 5$$

to get two more primes, namely 3 and 5. Then we could take:

$$2 * 3 * 5 * 7 + 1 = 211$$

and without knowing whether 211 is prime or not (it is!) we could conclude that there are primes other than $2, 3, 5$ and 7. Then:

$$2 * 3 * 5 * 7 * 211 + 1$$

factors into new primes, and we can proceed indefinitely, generating ever more primes each time. Notice we do not claim that this procedure generates **all** the primes. It simply generates infinitely many of them.

Exercises 4.

4.1. Prove that the sum of the first n odd numbers is n^2.

4.2. Prove that the sum of the first n perfect squares is:

$$\frac{(2n+1)(n+1)n}{6}$$

4.3. Prove the distributive law by induction. Given m and k, prove:

$$(m+k)n = mn + kn \text{ for all } n$$

Model your proof on the proof that $(mk)^n = m^k n^k$.

4.4. Give a geometric proof of the distributive law.

4.5. Find all the primes between 51 and 100.

4.6. Factorize all the numbers from 2 to 100.
(Use exponents. For example, $72 = 2^3 * 3^2$.)

4.7. Factorize 1001.

4.8. There was an assumption in the proof of Euclid's Theorem. Namely, if a prime p divides m we assumed it does not divide $m + 1$. Prove this.