Mathematics 4300 – Foundations of Algebra – Fall 1999

6. Fundamental Theorems. The Binomial Theorem. We return now to the natural numbers, in order to investigate the principle of induction. This will lead to our first "fundamental" theorem, the binomial theorem.

Definition: A **statement** is a sentence which is true or false (but not both).

Examples: (a) $1 < 2$. (True)

(b) All integers are even. (False)

(c) There are infinitely many twin primes.
(We don't know which it is, but this is either true or false!)

Not Examples: (a) $x < 2$ (Not a statement until we say what x is).

(b) This sentence is false. (Is it true? False?)

Definition: An **axiom** is a statement that we all agree is true because:

(a) It is "obvious" and

(b) It is not possible to deduce it from other axioms.

Axioms are the building blocks of mathematical proofs. There is a some subjectivity (surprise!) about what constitutes an axiom in mathematics. What is obvious to one person may not be so obvious to another. But over the years, certain axioms (such as most of Euclid's axioms of geometry) have been generally accepted. In the case of number systems, there are two which go back to the ancients.

The Archimedean Axiom: Given any real number r, there is a natural number n such that $n > r$.

(Obvious, no? We tend to use this without thinking.)

The Smallest Element Axiom: (Also called the Well-Ordering Principle). Every subset of $\mathbf{N}$ except the empty set has a smallest element.

I.e. Given $S \subseteq \mathbf{N}$, there is an $s_0 \in S$ such that $s_0 < s$ for all **other** $s \in S$.

(We have to leave out the empty set because it has **no** elements.)

From the smallest element axiom, we **deduce** the:

Principle of Mathematical Induction: Suppose T is a subset of the set of natural numbers, with the following two properties:

(a) $1 \in T$, and

(b) whenever $n \in T$, then $n+1 \in T$ also.

Then $T = \mathbf{N}$.

Proof: Suppose we are given T with properties (a) and (b). We want to conclude that $T = \mathbf{N}$. To do this, consider the complement:

$$S = \mathbf{N} - T = \{n \in \mathbf{N} \mid n \notin T\}$$

I claim that $S = \emptyset$. Otherwise, S would have a smallest element (axiom!) which we'll call s_0. Is it possible that $s_0 = 1$? No, because $1 \in T$ by (a). Is it possible that $s_0 > 1$? No again, because then we would have $s_0 - 1 \in T$ (remember that s_0 is smallest element of S) and then $s_0 \in T$ by (b). So there are no possibilities for s_0! But that means the $S = \emptyset$, so that $T = \mathbf{N}$.

The rest of this lecture is devoted to some of the consequences of the principle of mathematical induction.

Definitions by Induction: Suppose we define a function $f(n)$ by defining:

(a) $f(1)$, and

(b) $f(n+1)$, supposing that $f(n)$ is already defined.

then the **domain** of f is a subset of $\mathbf{N}$ satisfying (a) and (b) of the principle of mathematical induction, so the domain must be set of all natural numbers!

Most definitions of functions of the natural numbers are made this way.

Powers: If r is a number, then the nth power r^n is defined by:

(a) $r^1 = r$, and

(b) $r^{n+1} = r(r^n)$.

Remark: In the earlier sections, I would have written: $r^n = r \cdot ... \cdot r$ The principle of mathematical induction can be thought of as the **meaning** of those dots, or of the word "etcetera", which we also used earlier.

While we are at it, let's define:

Negative Powers: $r^{-n} = (\frac{1}{r})^n$ (this does not work for $r = 0$, of course)

The Zero Power: $r^0 = 1$ (this is OK even when $r = 0$).

Factorials: The factorial $n!$ is defined by the following:

(a) $1! = 1$, and

(b) $(n+1)! = (n+1)(n!)$.

(We may also define $0! = 1$.)

Factorials are an essential tool for counting things. One of the most important properties of the factorials is attributed to Pascal:

Definition:

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

(this makes sense whenever $n \geq m$ and $m \geq 0$)

Pascal's Formula: If $n > m$ and $m > 0$, then:

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$$

(we need $n > m$ and $m > 0$ for the right side of the equation to make sense)

Proof: This is just a formula for the sum of two rational numbers!

$$\begin{aligned}
\binom{n}{m} + \binom{n}{m-1} &= \frac{n!}{m!(n-m)!} + \frac{n!}{(m-1)!(n-m+1)!} \\
&= \frac{n-m+1}{n-m+1} \cdot \frac{n!}{m!(n-m)!} + \frac{m}{m} \cdot \frac{n!}{(m-1)!(n-m+1)!} \\
&= \frac{(n-m+1)n!}{m!(n-m+1)!} + \frac{(m)n!}{m!(n-m+1)!} \\
&= \frac{(n-m+1+m)n!}{m!(n-m+1)!} = \frac{(n+1)!}{m!(n-m+1)!} \\
&= \binom{n+1}{m}
\end{aligned}$$

Remarks: Before trying to go through the proof of something like Pascal's formula, you should fool around with the definition to get a feel for things!

You should also always fool around doing calculations with small values (which I have arranged suggestively below):

$$\binom{1}{0} = 1, \binom{1}{1} = 1$$
$$\binom{2}{0} = 1, \binom{2}{1} = 2, \binom{2}{2} = 1$$
$$\binom{3}{0} = 1, \binom{3}{1} = 3, \binom{3}{2} = 3, \binom{3}{3} = 1$$
$$\binom{4}{0} = 1, \binom{4}{1} = 4, \binom{4}{2} = 6, \binom{4}{3} = 4, \binom{4}{4} = 1$$

which for one thing tells us that these rational numbers are look like they are always going to be integers(!) and for another, if we leave out all the extra notation we get "Pascal's triangle" (arranged suggestively, as above):

$$\begin{array}{c} 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ \text{etc} \end{array}$$

which has the wonderful property that every number is the sum of the two numbers above it! But this is exactly what Pascal's formula tells us!!

Since we've already guessed it, let's prove:

Proposition: $\binom{n}{m}$ is always a natural number.

Proof: I want to prove this in the spirit of the branch of mathematics known as "combinatorics" which is devoted to counting things. Namely, I want to count the number of subsets of $S = \{1, 2, 3, ..., n\}$ with exactly m elements.

For example, the subsets of $\{1, 2, 3, 4\}$ with exactly 2 elements are:

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$$

and there are exactly 6 of these.

To choose such a subset, we need to pick m elements out of S. There are:

(i) n possibilities for the first choice,

(ii) $n-1$ possibilities for the second choice,

(iii) $n-2$ possibilities for the third choice,

$$\vdots$$

(m) $n-m+1$ possibilities for the mth choice

giving us $n(n-1)...(n-m+1)$ ways in all to choose a subset. On the other hand, if we are given $T = \{n_1, n_2, ..., n_m\} \subset S$, then we could have chosen T in lots of different ways. Namely, we could have chosen:

(i) One of the $n_1, ..., n_m$ first (m possibilities),

(ii) One of the remaining ones second ($m-1$ possibilities),

$$\vdots$$

(m) The last one (only one choice!)

meaning that **each T was chosen $m!$ times.** This means that the actual number of subsets with m elements is the number of ways of choosing a subset divided by the number of times a subset gets chosen, which is:

$$\frac{n(n-1)...(n-m+1)}{m!} = \frac{n(n-1)...(n-m+1)(m-n)!}{m!(n-m)!} = \binom{n}{m}$$

Thus $\binom{n}{m}$ is a natural number because it counts subsets

Enough with the factorials for the moment:

Proofs by Induction: Suppose $P(n)$ is a sentence with variable n which becomes a statement whenever n is replaced by a natural number. Suppose we prove the following two **statements**:

(a) $P(1)$, and

(b) $P(n+1)$ is true whenever $P(n)$ is true.

Then all natural numbers make $P(n)$ a true statement, because the principle of induction tells us that the set of n which make $P(n)$ true must be the entire set of natural numbers!

Remark: The sentence (b) really is a statement, though it may not look it. It is false if $P(1)$ is true but $P(2)$ is false, or if $P(2)$ is true but $P(3)$ is false, etc. And it is true otherwise!

Now for some examples of this powerful proof technique:

Sums of natural numbers. We want to prove the formula:

$$P(n): \quad 1+2+3+...+n = \binom{n+1}{2}$$

(Let's write down the first few to convince ourselves this may be true:)

$P(1): 1 = \binom{2}{2}$

$P(2): 1+2 = \binom{3}{2} = 3$

$P(3): 1+2+3 = \binom{4}{2} = 6$

So it looks OK. Now for the proof. Notice first that:

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

so we can make this substitution whenever we want.

(a) $P(1)$. This is the obvious equality $1 = \binom{2}{2}$.

(b) Assuming $P(n): \quad 1+2+3+...+n = \frac{(n+1)n}{2}$, then:

$$\begin{aligned} 1+2+...+n+(n+1) &= \tfrac{(n+1)n}{2} + (n+1) \\ &= \tfrac{n^2+n}{2} + \tfrac{2n+2}{2} \\ &= \tfrac{n^2+3n+2}{2} \\ &= \tfrac{(n+2)(n+1)}{2} \end{aligned}$$

which is exactly $P(n+1)$. So we've proved (b)! And that finishes the proof.

The Binomial Theorem: Suppose r and s are numbers. Then:

$$(r+s)^n = r^n + \binom{n}{1} r^{n-1}s + ... + \binom{n}{m} r^{n-m}s^m + ... + \binom{n}{n-1} rs^{n-1} + s^n$$

Again, let's write down the first few to convince ourselves:

$P(1) : (r+s)^1 = r+s.$

$P(2) : (r+s)^2 = r^2 + \binom{2}{1} rs + s^2 = r^2 + 2rs + s^2$

$P(3) : (r+s)^3 = r^3 + \binom{3}{1} r^2 s + \binom{3}{2} rs^2 + s^3 = r^3 + 3r^2 s + 3rs^2 + s^3$

Proof: (a) $P(1)$ is obvious! $r+s = r+s$.

(b) Assuming $P(n)$, we multiply both sides by $r+s$ to get:

$$(r+s)^{n+1} =$$

$$(r+s)\left(r^n + \binom{n}{1} r^{n-1}s ... + \binom{n}{m} r^{n-m}s^m + ... + \binom{n}{n-1} rs^{n-1} + s^n\right)$$

which by the distributive law is:

$$r\left(r^n + ... + \binom{n}{m} r^{n-m}s^m + ... + s^n\right) +$$
$$s\left(r^n + ... + \binom{n}{m} r^{n-m}s^m + ... + s^n\right)$$

which after multiplying through becomes:

$$\begin{array}{ccccccc} r^{n+1}+ & nr^n s+ & ... & +\binom{n}{m} r^{n-m+1}s^m + & ...+ & rs^n + & \\ & r^n s + & ... & +\binom{n}{m-1} r^{n-m+1}s^m + & ... & nrs^n + & s^{n+1} \end{array}$$

which is equal to:

$$r^{n+1} + (n+1)r^n s + ... + \left(\binom{n}{m} + \binom{n}{m-1}\right) r^{n-m+1}s^m + ... + s^{n+1}$$

Now for the key point! Pascal's formula tells us that this is:

$$r^{n+1} + (n+1)r^n s + ... + \binom{n+1}{m} r^{n+1-m}s^m + ... + (n+1)rs^n + s^{n+1}$$

which is exactly $P(n+1)$. Whew! The proof is done!

Final Remarks: The binomial theorem is quite practical! It tells us that if we want to calculate $(r+s)^n$, we need to go down to the nth row of Pascal's triangle and use those natural numbers as coefficients. For example:

$$(r+s)^4 = r^4 + 4r^3 s + 6r^2 s^2 + 4rs^3 + s^4$$

Thus the natural numbers $\binom{n}{m}$ are exactly the numbers which appear as coefficients in $(r+s)^n$. This is why we call them **binomial coefficients**.

Exercises:

6.1. Using the definition by induction of r^n, prove that:

$$(rs)^n = r^n s^n$$

6.2. Prove by induction that:

$$1 + 3 + 5 + ... + (2n - 1) = n^2$$

6.3. Prove the geometric series formula for all $r \neq 1$:

$$1 + r + r^2 + ... + r^n = \frac{r^{n+1} - 1}{r - 1}$$

6.4. Calculate $(1 + 2i)^{11}$ using the binomial theorem.

The principle of complete mathematical induction says:

Fix a natural number m, and suppose $T \subseteq \mathbf{N}$ has the following properties.

(a) $1, 2, ..., m \in T$, and

(b) whenever $1, 2, 3, ..., n$ are in T and $n \geq m$, then $n + 1 \in T$ also.

Then $T = \mathbf{N}$.

6.5. (a) Prove the principle of complete mathematical induction. Model your proof on the proof of the principle of mathematical induction.

(b) Explain what a definition by complete mathematical induction is.

(c) The **Fibonacci sequence** is: $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$.

Thus the first few terms are:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

Explain why this is a definition by complete induction. (What is m?)

(d) Explain what a proof by complete induction is.

(e) Prove by complete induction that:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$