Math 4030-001/Foundations of Algebra/Fall 2017

Foundations of the Foundations: Proofs

A **proof** is a demonstration of the truth of a mathematical statement. We already know what a mathematical statement is.

Definition 3.1: A demonstration is a series of sentences (a paragraph) with the following properties:

(1) Any assumptions in the paragraph are either statements that are known to be true or a single statement that we wish to prove is false (in a proof by contradiction),

(2) The truth of each new statement follows logically from earlier statements and assumptions.

This is still vague, so it's probably best to see some examples.

Proofs by Computation: These are proofs that involve checking an identity by a straightforward computation.

Example: The addition of rational numbers, defined by:

$$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$$

is an associative operation.

Proof. We need to check that for all triples of rational numbers,

$$\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) + \frac{m_3}{n_3} = \frac{m_1}{n_1} + \left(\frac{m_2}{n_2} + \frac{m_3}{n_3}\right)$$

First, expand the left side of the equation:

$$\begin{aligned} \left(\tfrac{m_1}{n_1} + \tfrac{m_2}{n_2}\right) + \tfrac{m_3}{n_3} &= \tfrac{m_1 n_2 + m_2 n_1}{n_1 n_2} + \tfrac{m_3}{n_3} \\ &= \tfrac{(m_1 n_2 + m_2 n_1) n_3 + m_3 (n_1 n_2)}{(n_1 n_2) n_3} \\ &= \tfrac{m_1 n_2 n_3 + n_1 m_2 n_3 + n_1 n_2 m_3}{n_1 n_2 n_3} \end{aligned}$$

then expand the right side of the equation:

$$\begin{aligned} \tfrac{m_1}{n_1} + \left(\tfrac{m_2}{n_2} + \tfrac{m_3}{n_3}\right) &= \tfrac{m_1}{n_1} + \tfrac{m_2 n_3 + m_3 n_2}{n_2 n_3} \\ &= \tfrac{m_1 (n_2 n_3) + (m_2 n_3 + m_3 n_2) n_1}{n_1 (n_2 n_3)} \\ &= \tfrac{m_1 n_2 n_3 + n_1 m_2 n_3 + n_1 n_2 m_3}{n_1 n_2 n_3} \end{aligned}$$

Since they are the same, it follows that addition is an associative. □

Remark. The associativity and commutativity of addition of **integers** were assumed and used in the last step of each expansion.

Proofs of Existence: These are proofs of the existence of something by exhibiting a single example.

Example. The integers are countably infinite, i.e. there is a bijection:

$$f : \mathbb{N} \to \mathbb{Z}$$

Proof. The function:

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even, and} \\ -\frac{(n-1)}{2} & \text{if } n \text{ is odd} \end{cases}$$

is a bijection from $\mathbb{N}$ to $\mathbb{Z}$. □

Remark. This is correct, but it may not get you full credit since you ought to provide some justification for the assertion that f is a bijection. For example, you may additionally explain why

$$f^{-1}(0) = 0, f^{-1}(n) = 2n \text{ and } f^{-1}(-n) = 2n + 1$$

to establish that f has an inverse function.

Example. Matrix multiplication is not commutative. That is,

$$(\exists \text{ matrix } A)(\exists \text{ matrix } B)\ (AB \neq BA)$$

To prove this, we need to exhibit a pair of matrices whose products differ when the order is switched.

Proof. The pair of matrices

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ satisfy}$$

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ but } BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Remark. The statement "matrix multiplication is commutative" isn't even technically mathematical, since the product AB is only defined when the number of columns of A matches the number of rows of B!

Example. There are real quadratic polynomials with no real roots. Written with quantifiers, this is the statement:

$$(\exists a \in \mathbb{R}^*)(\exists b \in \mathbb{R})(\exists c \in \mathbb{R})(\forall x \in \mathbb{R})\ ax^2 + bx + c \neq 0$$

Proof. Since $x^2 \geq 0$ for all real numbers, it follows that $x^2 + 1 \geq 1$ for all $x \in \mathbb{R}$. Therefore the polynomial $x^2 + 1$ has no real root. □

Remark. We get a much better proof assuming the quadratic formula. Whenever $b^2 - 4ac < 0$, then the two complex roots of $ax^2 + bx + c = 0$ have non-zero imaginary parts, so they are not real.

Proofs of Uniqueness. To prove that there is *at most* one thing with a desired property, start with two and then show that they are equal. *Note:* This is not a proof of existence!

Example. There is at most one additive identity among the integers.

Proof. Let a and b be additive integer identities. Then:

$$b + a = a \text{ because } b \text{ is an additive identity, and}$$

$$a + b = b \text{ because } a \text{ is an additive identity}$$

Therefore $a = b$ because addition of integers is commutative. □

Existence. 0 is the additive identity.

Example. There is at most one additive inverse of an integer.

Proof. Fix $a \in \mathbb{Z}$ and let b and c be additive inverses of a. Then:

$$b + (a + c) = b + 0 = b \text{ and } (b + a) + c = 0 + c = c$$

So $b = c$ by the associative law of addition. □

Existence. $-a$ is the additive inverse of a.

Remark. Of course no number other than 0 can be an additive identity, and of course $-a$ is the only additive inverse to a. But the point is that uniqueness can be concluded without thinking about the details of addition of integers (and therefore can be applied in other situations).

Example. Left and right inverses of a matrix A are the same matrix.

Proof. Let A be a square matrix and let B and C satisfy:

$$BA = I \text{ and } AC = I$$

Then

$$B = B(AC) = (BA)C = C \quad \square$$

Remark. We assumed the associative law for multiplication of matrices, which can be established with an ugly proof by computation, or else by reinterpreting matrices as *transformations* of a vector space. We will talk about this later.

Existence? Nope. Not every matrix is invertible.

Proofs by Contradiction. To prove $\neg p$, we may instead prove:

$$(p \Rightarrow q) \wedge (\neg q)$$

because this compound statement is true **only when** p is false, as you can see with a truth table. In practical terms, this means that if we assume p and use it in a demonstration to deduce a statement q that is false, then p must have been false to begin with!

Example. $\neg$ **p:** $\sqrt{2}$ is not a rational number.

Proof: Assume **p:** $\sqrt{2}$ is a rational number. Then

$$\sqrt{2} = \frac{m}{n}$$

for natural numbers m and n with no common factors. We then get:

$$2 = \frac{m^2}{n^2} \quad \text{and} \quad 2n^2 = m^2$$

by squaring both sides, from which we conclude that m is even. Letting $m = 2k$, we get $2n^2 = 4k^2$ and $n^2 = 2k^2$, so n is also even. Thus:

q: The numbers m and n with no common factors are both even.

This is clearly a false statement!

Remark. We assumed that rational numbers can be put in *lowest terms*, in which the numerator and denominator have no common factors. This is actually a pretty sophisticated assumption. We also assumed that if m^2 is even, then m is even, which is much less sophisticated.

Example. $\neg$**p** : The open interval $(0, 1) \subset \mathbb{R}$ is not countably infinite.

Proof. Assume **p** and let $f : \mathbb{N} \to (0, 1)$ be a bijective function. Since every real number $r \in (0, 1)$ can be expressed as a binary decimal:

$$0.a_1a_2a_3a_4...., \quad a_i \in \{0, 1\}$$

we may consider the list of values of the function f:

$$\begin{aligned} f(1) &= 0.a_{1,1}a_{1,2}a_{1,3}a_{1,4}... \\ f(2) &= 0.a_{2,1}a_{2,2}a_{2,3}a_{2,4}... \\ f(3) &= 0.a_{3,1}a_{3,2}a_{3,3}a_{3,4}... \\ f(4) &= 0.a_{4,1}a_{4,2}a_{4,3}a_{4,4}... \\ &\vdots \end{aligned}$$

But this list **leaves out** a binary decimal, namely the decimal:

$$0.b_1b_2b_3....$$

that "switches the bit" of each $a_{i,i}$, turning each $a_{i,i} = 0$ into $b_i = 1$ and each $a_{i,i} = 1$ into $b_i = 0$. Because of this,

q: The bijection f is not onto. False! $\square$

Proof by Pigeonholing. This is a surprisingly useful idea, in which we use the fact that a function $f : A \to B$ of finite sets cannot be one-to-one if $|A| > |B|$. That is, if A is a set of pigeons and B is a set of holes and there are more pigeons than holes, then more than one pigeon must go in some hole.

Example. Decimal expansions of rational numbers eventually repeat.

Proof. The decimal expansion of m/n is obtained by long division. This is a recursive procedure, in which one digit at a time is produced:

(Initialize) Divide m by n to get a quotient q and remainder $r < n$.

(Loop)

(i) If $r = 0$, stop. The decimal terminates (with repeating zeroes).

(ii) Divide $10r$ by n. The quotient is the next digit (write it down) and reset r to be the remainder. Return to the loop.

The pigeonhole principle comes into play as follows. At some point in the loop, the same remainder (which is between 1 and $n-1$) must occur for a second time. In fact, this has to happen within the first n iterations of the loop. At that point, the decimal repeats. □

Remark. The assumption made here is that every pair of natural numbers m and n satisfy an equation:

$$m = nq + r$$

where q is the quotient and r is a remainder, satisfying $r < n$. This is a medium-sophisticated assumption, which is, of course, *long division.*

Exercises 1.3. Prove each of the following.

3.1. Let $i^2 = -1$ and define multiplication of complex numbers by:

$$(a + bi)(c + di) = (ac - bd) + i(ad + bc)$$

Prove that

$$(a + bi)\left(\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}\right) = 1$$

provided that $a^2 + b^2 \neq 0$.

3.2. Prove that if $|A| > 3$, then there are two permutations of A that do not commute. (Hint: Start with $A_3 = \{1, 2, 3\}$.)

3.3. (a) Prove that the polynomial $x^2 + x + 1$ has no real roots.

(b) Prove that there is exactly one real cube root of 1.

3.4. Prove that the square of an odd number is odd.

3.5. Prove that there is no real fourth root of -1.

3.6. Interlude. Convert the following to *binary* repeating decimals:
(a) 1/2 (b) 1/3 (c) 1/4 (d) 1/5 (e) 1/6 (f) 1/7 (g) 1/8

3.7. Create your own math question that uses the pigeonhole principle. Try to make it interesting :-)