<h1 style="text-align: center">Examples of Proof: Sets</h1>

We discussed in class how to formally show that one set is a subset of another and how to show two sets are equal. Here are some examples.

In the first proof here, remember that it is important to use different dummy variables when talking about different sets or different elements of the same set. You don't want to accidently start by assuming that two elements are equal. Note that I discovered the relationship between m and n in my scratch work (I asked myself what needed to be true to make $4m + 1$ equal to $4n - 3$, setting them equal and solving I got $n = m + 1$).

Theorem Let $A = \{n : n = 4k + 1 \text{ for some } k \in \mathbb{Z}\}$ and $B = \{n : n = 4k - 3 \text{ for some } k \in \mathbb{Z}\}$. Prove $A = B$
Proof: We must show that $A \subseteq B$ and $B \subseteq A$.
First, we show that $A \subseteq B$.
Let $x \in A$. By definition of A, $x = 4m + 1$ for some $m \in \mathbb{Z}$. Letting $n = m + 1$, we check by substitution that $4n - 3 = 4(m + 1) - 3 = 4m + 4 - 3 = 4m + 1 = x$. Hence, $x = 4n - 3$ for some $n \in \mathbb{Z}$ (namely, $n = m + 1$). Thus, $x \in B$ and we have shown $A \subseteq B$.
Now we show that $B \subseteq A$.
Let $x \in B$. By definition of B, $x = 4n - 3$ for some $n \in \mathbb{Z}$. Letting $m = n - 1$, we check by substitution that $4m + 1 = 4(n - 1) + 1 = 4n - 4 + 1 = 4n - 3 = x$. Thus, $x = 4m + 1$ for some $m \in \mathbb{Z}$ (namely, $m = n - 1$). Ergo, $x \in A$ and we have shown $B \subset A$.
Therefore, $A = B$. $\square$

Here is another set equality proof (from class) about set operations.

Theorem For any sets A and B, $A - B = A \cap B^c$.
Proof: We must show $A - B \subseteq A \cap B^c$ and $A \cap B^c \subseteq A - B$. First, we show that $A - B \subseteq A \cap B^c$.
Let $x \in A - B$. By definition of set difference, $x \in A$ and $x \notin B$. By definition of complement, $x \notin B$ implies that $x \in B^c$. Hence, it is true that both, $x \in A$ and $x \in B^c$. By definition of intersection, $x \in A \cap B^c$.
Now we show that $A \cap B^c \subseteq A - B$.
Let $x \in A \cap B^c$. By definition of intersection, $x \in A$ and $x \in B^c$. By definition of complement, $x \in B^c$ implies that $x \notin B$. Hence, $x \in A$ and $x \notin B$. By definition of set difference, $x \in A - B$.
Thus, $A - B = A \cap B^c$. $\square$

Here are some basic subset proofs about set operations.

Theorem For any sets A and B, $A \cap B \subseteq A$.
Proof: Let $x \in A \cap B$. By definition of intersection, $x \in A$ and $x \in B$. Thus, in particular, $x \in A$ is true. $\square$

Theorem For any sets A and B, $B \subseteq A \cup B$.
Proof: Let $x \in B$. Thus, it is true that at least one of $x \in A$ or $x \in B$ is true. Since $x \in A$ or $x \in B$ is true, by definition of union, $x \in A \cup B$. $\square$

Theorem For any sets A and B, $A - B \subseteq A$.
Proof: Let $x \in A - B$. By definition of set difference, $x \in A$ and $x \notin B$. Thus, in particular, $x \in A$ is true. $\square$

Examples of Proofs: Inequalities

Here are some of the main inequality facts that I expect you to assume (facts 2 - 6 all hold with the less than or equal size ($\leq$) as well except as noted in 3):

1. If x is a real number, then either $x < 0$, $x > 0$, or $x = 0$.
   It is sometimes useful to do all three of these cases separately in a proof.

2. If $x < y$ and a is any real number, then $x + a < y + a$ and $x - a < y - a$.
   You can add or subtract from both sides of an inequality.

3. If $x < y$ and $w < z$, then $x + w < y + z$. *You can add two inequalities.*
   If $x < y$ and $w \leq z$, then $x + w < y + z$.
   This is the same fact as above, I am just noting that if one inequality is strict, then we can say the sum in strict.

4. If $x < y$ and a is a positive real number, then $ax < ay$.
   You can multiply by a positive constant and the inequality stays in the same direction.
   If $x < y$ and a is a negative real number, then $ax > ay$. *Multiplying by a negative constant changes the direction of the inequality.*

5. If $0 < x < y$ and $0 < w < z$, then $xw < yz$.
   You can multiply inequalities provided all the numbers are positive.

6. If $x < y$ and $y < z$, then $x < z$. *This is called the transitive property.*

7. If x is a real number, then $x^2 \geq 0$. *The square of a real number is not negative.*

Below is the first proof we ever did in lecture. Remember that in our scratch work, we found that the conclusion was equivalent to a known fact from above. Then we wrote our proof starting from this known fact.

Theorem (*The AGM Inequality, Part 1*) If x and y are real numbers, then $2xy \leq x^2 + y^2$.
Proof: Let x and y be real numbers.
Since the square of a real number can't be negative, we have $0 \leq (x - y)^2$ (this is fact 7 listed above). By expanding the square, we get $0 \leq x^2 - 2xy + y^2$. Adding $2xy$ to both sides of the inequality gives $2xy \leq x^2 + y^2$ (this is allowed by fact 2 listed above). $\square$

Illustrating a Counterexample The statement: 'If x is a real number, then $x \leq x^2$' is a false statement. Here is one counterexample: Let $x = \frac{1}{2}$, so that $x^2 = \frac{1}{4}$. But $x = \frac{1}{2} > \frac{1}{4} = x^2$, so this is a counterexample (the hypothesis is true and the conclusion is false).
After thinking about the example above and trying a few more examples, you probably realized that it is true that $x \leq x^2$, when $x \geq 1$ and when $x \leq 0$. Let's prove this.

Theorem If x is a real number and $x \leq 0$ or $x \geq 1$, then $x \leq x^2$.
Proof: Let x be a real number. We prove the two separate cases: $x \leq 0$ or $x \geq 1$.
CASE 1: Assume $x \leq 0$. By fact 7, $0 \leq x^2$. Since we have $x \leq 0$ and $0 \leq x^2$, by the transitive property, $x \leq x^2$.
CASE 2: Assume $x \geq 1$. Since x is a positive number, we can multiply both sides of this inequality by x (by fact 4 above) to get $x^2 \geq x$ which is the same as $x \leq x^2$.
In all cases of the hypothesis, we have shown that $x \leq x^2$. $\square$

Here are some more inequality proofs, some of which you will see in lecture. Note that the proof below would also work with $\leq$ in place of $<$ everywhere.

Theorem If $0 < a < b$, then $a^2 < ab < b^2$.
Proof: Assume $0 < a < b$.
Since $a < b$ and $a > 0$, by fact 4, we can multiply the first inequality by a to get $a^2 < ab$.
Since $a < b$ and $b > a > 0$, by fact 4 again, we can multiply the first inequality by b to get $ab < b^2$.
Hence, $a^2 < ab < b^2$. $\square$

Corollary If $0 < c < d$, then $\sqrt{c} < \sqrt{d}$.

Proof: Assume $0 < c < d$. If, on the contrary, $\sqrt{c} \geq \sqrt{d}$, then the theorem above implies that $\sqrt{c}^2 \geq \sqrt{d}^2$, so $c \geq d$. By assumption, this cannot be the case, so $\sqrt{c} < \sqrt{d}$. $\square$

The proof of this corollary illustrates an important technique called 'proof by contradiction'. The idea is to assume the hypothesis, then assume the conclusion is false. If these assumptions always lead to a contradiction, then the conclusion must be true. We will talk a lot more about this in chapter 2, but you are welcome to use this idea now if you want to try it.

Examples of Proofs: Absolute Values

The absolute value function is one that you should have some familiarity, but is also a function that students sometimes misunderstand. An important observation is the absolute value is a function that performs different operations based on two cases $x < 0$ or $x \geq 0$. Thus, most proofs and problems that involve using the absolute value function require a look at cases.

Definition If x is a real number, then the absolute value of x is defined by $|x| = \begin{cases} -x & \text{, if } x < 0; \\ x & \text{, if } x \geq 0. \end{cases}$

In other words, the number is left alone if $x \geq 0$ and the sign is flipped if $x < 0$. So negatives are never output by this function. Because of this fact, some students get confused about how $|x| = -x$ sometimes, but remember this is only the case if x is already negative (so $-x$ is positive). Let's do some proofs with the absolute value.

Theorem If x is a real number, then $|x|^2 = x^2$.

Proof: Let x be a real number. We prove the two separate cases: $x < 0$ or $x \geq 0$.
CASE 1: Assume $x < 0$. By the definition of absolute value, $|x| = -x$. Squaring both sides gives $|x|^2 = (-x)^2$. Since $(-x)^2 = x^2$ for any real number (see Prop. 1.43(e) in the book), we have $|x|^2 = x^2$.
CASE 2: Assume $x \geq 0$. By the definition of absolute value, $|x| = x$. Squaring both sides gives $|x|^2 = x^2$.
In all cases, $|x|^2 = x^2$. $\square$

Theorem If x is a real number, then $x \leq |x|$.

Proof: Let x be a real number. We prove the two separate cases: $x < 0$ or $x \geq 0$.
CASE 1: Assume $x < 0$. By the definition of absolute value, $|x| = -x > 0$. Since we have $x < 0$ and $0 < |x|$, by the transitive property, $x < |x|$ (in which case it is also true, though less specific, to say that $x \leq |x|$.
CASE 2: Assume $x \geq 0$. By the definition of absolute value, $|x| = x$. In which case it is also true, though less specific as before, to say that $x \leq |x|$.
In all cases, $x \leq |x|$. $\square$

A useful observation about absolute values and inequalities is that $|x| < 5$ is the same as saying $-5 < x < 5$. If you are working with inequalities and absolute values, it might be wise to rewrite the inequality in this way.

Theorem If $|x + 2| < 10$ and $x > 0$, then $|x - 5| < 5$.

Proof: Assume $|x + 2| < 10$ and $x > 0$. Rewriting the first inequality without the absolute value, we have $-10 < x + 2 < 10$. By subtracting two from, we obtain $-12 < x < 8$. Hence, noting both assumptions, we have $0 < x < 8$. Subtracting five, we obtain $-5 < x - 5 < 3$. Since $x - 5 < 3$ and $3 < 5$, we have $x - 5 < 5$ (by the transitive property). Thus, $-5 < x - 5 < 5$ which is equivalent to $|x - 5| < 5$. $\square$

Here we prove several things about the rational numbers which you probably already believe to be true, but it is a chance for you to see several direct proofs. Remember, a direct proof starts with the hypothesis and ends with the conclusion. In the middle we use logical deductions from known facts and definitions. For all the proofs below we are essentially just unwinding the definition of a rational number.

Definition A *rational number* is any number, x, that can be written in the form $x = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

Theorem If x and y are rational numbers, then xy is a rational number.
Proof: Assume x and y are rational numbers.
By the definition of a rational number, $x = \frac{a}{b}$ and $y = \frac{c}{d}$ for some integers a, b, c, and d where b and d are not zero. By substitution, $xy = \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$. Since $p = ac$ and $q = bd$ are integers and $q = bd$ is not zero, we have shown that xy can be written in the form $\frac{p}{q}$ for some integers p and q. Hence, xy is a rational number. $\square$

You can see that we couldn't use the symbols a and b for both x and y as that would assume that x and y are the same.

Theorem If x and y are rational numbers, then $x + y$ is a rational number.
Proof: Assume x and y are rational numbers.
By the definition of a rational number, $x = \frac{a}{b}$ and $y = \frac{c}{d}$ for some integers a, b, c, and d where b and d are not zero. By substitution, $x + y = \frac{a}{b} + \frac{c}{d}$. Getting a common denominator we have $x + y = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$. Since $p = ad + bc$ and $q = bd$ are integers and $q = bd$ is not zero, we have shown that xy can be written in the form $\frac{p}{q}$ for some integers p and q. Hence $x + y$ is a rational number. $\square$

Theorem If x and y are rational numbers and $y \neq 0$, then x/y is a rational number.
Proof: Assume x and y are rational numbers and $y \neq 0$.
By the definition of a rational number, $x = \frac{a}{b}$ and $y = \frac{c}{d}$ for some integers a, b, c, and d where b and d are not zero. Since $y = \frac{c}{d}$ can't be zero by assumption, c must also be nonzero. By substitution, $x/y = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$. Since $p = ad$ and $q = bc$ are integers and $q = bc$ is not zero, we have shown that xy can be written in the form $\frac{p}{q}$ for some integers p and q. Hence x/y is a rational number. $\square$

The next two proofs illustrate how mathematicians try to generalize theorems.

Theorem If x is a rational numbers, then x^2 is a rational number.
Proof: Assume x is a rational number.
By the definition of a rational number, $x = \frac{a}{b}$ for some integers a and b where b is not zero. By substitution, $x^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$. Since $p = a^2$ and $q = b^2$ are integers and $q = b^2$ is not zero, we have shown that xy can be written in the form $\frac{p}{q}$ for some integers p and q. Hence, x^2 is a rational number. $\square$

Theorem If x is a rational numbers and n is a natural number, then x^n is a rational number.
Proof: Assume x is a rational number.
By the definition of being rational, $x = \frac{a}{b}$ for some integers a and b where b is not zero. By substitution, $x^n = \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$. Since $p = a^n$ and $q = b^n$ are integers and $q = b^n$ is not zero, we have shown that xy can be written in the form $\frac{p}{q}$ for some integers p and q. Hence, x^n is a rational number. $\square$

Most of the facts above don't hold true in general for *irrational* numbers. For example, $x = \sqrt{2}$ is irrational (we will prove this later in the quarter), how $x^2 = \sqrt{2}^2 = 2 = \frac{2}{1}$ is a rational number. So the square of an irrational number may or may not be irrational. The sum of two irrational number can be rational and the product of two irrational number can be rational (you may see if you can find counterexamples).