Math 311 - Introduction to Proof and Abstract Mathematics
Group Assignment # 5 **Name:**_____
Due: Thursday, September 13th

Properties of Integers: Let a, b, and c be arbitrary integers.

Closure under $+$ and $\cdot$	$a+b$ and ab are also integers.
Associative properties	$(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.
Commutative properties	$a+b = b+a$ and $ab = ba$.
Distributive property	$a(b+c) = ab+ac$.
Identities	$0 \neq 1$, $a+0 = a$, $a \cdot 1 = a$, and $a \cdot 0 = 0$.
Additive inverses	$\forall a \exists!$ integer $-a = -1 \cdot a$ such that $a+(-a) = 0$.
Subtraction	$b-a$ is defined to equal $b+(-a)$.
No divisors of 0	If $ab = 0$ then $a = 0$ or $b = 0$.
Cancellation	If $ab = ac$ and $a \neq 0$, then $b = c$.
Transitive property of $<$	If $a < b$ and $b < c$, then $a < c$.
Trichotomy	Exactly one of $a < b$, $a = b$ or $a > b$ holds.
Order property 1	If $a < b$ then $a + c < b + c$.
Order property 2	If $c > 0$, then $a < b$ iff $ac < bc$.
Order property 3	If $c < 0$, then $a < b$ iff $ac > bc$.

1. Use the properties of integers to prove the second distributive property: $(a+b)c = ac+bc$.

Recall: n is **prime** if $n > 1$ and the only positive integer factors of n are 1 and n; i.e., n is prime if $n > 1$ and $(\forall a, b \in \mathbb{N})[n = ab \Rightarrow (a = 1 \text{ or } b = 1)]$.

Recall: An integer a **divides** an integer b, written $a|b$, if and only if there exists $n \in \mathbb{Z}$ such that $b = an$. In this case, we may also say that b *is divisible by* a.

Proposition 2.1.3 For all integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Proof: Let a, b, and c be integers satisfying $a|b$ and $b|c$. Using the definition of divisibility, there is an integer n such that $b = an$. Similarly, there is an integers m such that $c = mb$. Therefore, using the properties of equality and substitution, we have $c = mb = m(an)$. Using the associative property and commutativity of multiplication, $c = (ma)n = (am)n = a(mn)$. Notice that mn is an integer by Closure of the integers under multiplication. Therefore, again applying the definition of divisibility, $a|c$.

Properties of Real Numbers: Let a, b, and c be arbitrary real numbers.

Closure under $+$ and $\cdot$	$a+b$ and ab are also real numbers.
Associative properties	$(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.
Commutative properties	$a+b = b+a$ and $ab = ba$.
Distributive property	$a(b+c) = ab+ac$.
Identities	$0 \neq 1$, $a+0 = a$, $a \cdot 1 = a$, and $a \cdot 0 = 0$.
Additive inverses	$\forall a \exists!$ real number $-a = -1 \cdot a$ such that $a+(-a) = 0$.
Subtraction	$b-a$ is defined to equal $b+(-a)$.
Multiplicative Inverses	If $a \neq 0$ then $\exists!$ real number $a^{-1} = \frac{1}{a}$ such that $a\dot{a}^{-1} = a \cdot \frac{1}{a} = 1$.
Division	When $a \neq 0$ $\frac{b}{a}$ is defined to equal $b \cdot \frac{1}{a}$.
Cancellation	If $ab = ac$ and $a \neq 0$, then $b = c$.
Transitive property of $<$	If $a < b$ and $b < c$, then $a < c$.
Trichotomy	Exactly one of $a < b$, $a = b$ or $a > b$ holds.
Order property 1	If $a < b$ then $a + c < b + c$.
Order property 2	If $c > 0$, then $a < b$ iff $ac < bc$.
Order property 3	If $c < 0$, then $a < b$ iff $ac > bc$.

Note: The real numbers have one additional important property called the **Completeness Axiom** that we may take time to discuss later in the course.

Theorem 2.1.5 Let $n \in \mathbb{Z}^+$ (that is, suppose n is a positive integer)

(1) Assume n is even. Then every $x \in \mathbb{R}$ with $x \geq 0$ has a real "nth root"; i.e., when $x \geq 0$, there is a unique non-negative real number denoted by $x^{\frac{1}{n}} = \sqrt[n]{x}$ which satisfies $\left(x^{\frac{1}{n}}\right)^n = x$. Furthermore, for any $x \in \mathbb{R}$, $(x^n)^{\frac{1}{n}} = |x|$.

(2) Assume n is odd. Then every $x \in \mathbb{R}$ has a real "nth root"; i.e., when $x \geq 0$, there is a unique real number denoted by $x^{\frac{1}{n}} = \sqrt[n]{x}$ which satisfies $\left(x^{\frac{1}{n}}\right)^n = x$. Furthermore, for any $x \in \mathbb{R}$, $(x^n)^{\frac{1}{n}} = x$.

Note: We will accept this theorem without proof (although doing so does make me a little sad).

Proposition 2.1.6: For all $a, b \in \mathbb{R}$ with $a < b < 0$, $a^2 > b^2$.

Proof: Let $a, b \in \mathbb{R}$ with $a < b < 0$. If we multiply this inequality by a, since $a < 0$, by Order property (3) of real numbers, we have $a \cdot a > a \cdot b > a \cdot 0$ or, simplifying, $a^2 > ab > 0$. Similarly, if we multiply the original inequality by b, since $b < 0$, by Order property (3) of real numbers, we have $b \cdot a > b \cdot b > b \cdot 0$ or, simplifying, $ba = ab > b^2 > 0$. Since we have $a^2 > ab$ and $ab > b^2$ using the transitive property of $<$ gives $a^2 > b^2$. $\square$.

2. Use the properties of real numbers to prove that if $0 < a < b$, then $a^2 < b^2$.

Counterexamples:

To **disprove** a statement of the form $(\forall x)P(x)$ (i.e. to show that it is false)
• Find a specific element a in the universe such that $P(a)$ is **false**.
• That is, identify a specific element of the universe a and demonstrate that $P(a)$ is false for that element.
• Such an element is called a **counterexample**.

To **disprove** that a statement of the form $(\exists x)P(x)$ (i.e. to show that it is false)
• Begin by stating "Let x be an arbitrary (but now *fixed*) element of the universe."
• Use definitions and established mathematical principles to demonstrate that $P(x)$ is **false**.
• That is, demonstrate that $P(a)$ is false for every element in the universe.

3. Explain, in your own words, why a single counterexample is sufficient to **disprove** a universally quantified statement.

4. Explain, in your own words, why, in order to **disprove** a existentially quantified statement, one must show that the statement is **never** true.

Proof by Cases: Sometimes, it is difficult or unpleasant to find a single argument to prove a general (universal) statement. In this situation, one nice way around this obstacle is to divide the universe into two or more subsets and to provide separate arguments that prove the statement holds in each subset. This method of proof is called *proof by cases* (or **the method of exhaustion**).

Note: One nice way to get a sense of how to prove each case (and what cases to use) it is often useful to work through a few examples. However, unless we are in a finite universe, we will not be able to prove the full statement by looking at specific examples. We are merely looking for patterns that we can adapt for use in a more formal proof. This idea is especially important when we are given a statement to "Prove or Disprove" as we will need to decide whether or not we believe the statement is true or false.

5. Prove that for any integer n, $n^2 + n$ is even. [Hint: split into two cases. Case 1 - suppose n is even. Case 2 - suppose n is odd]

6. Prove or Disprove each of the following statements.

   (a) For all integers a, b, c, if $a|(b + c)$ then $a|b$ or $a|c$.

   (b) For all real numbers x and y, if $x < y$, then $x < \frac{x+y}{2} < y$.

Proving Biconditional Statements: Logically speaking, a biconditional statement is two conditional statements combined together into a single statement. With this in mind, to prove a biconditional statement of the form $P \Leftrightarrow Q$, we will generally combine two separate proofs. A proof that $P \Rightarrow Q$ and a proof that $Q \Rightarrow P$.

7. Prove that for any integers n, n is even if and only if n^2 is even.