Math 215 - Introduction to Advanced Mathematics

Direct Proofs

Fall 2017

Mathematical statements that we want to prove take the form

$$A \implies B$$

which we read as "A implies B" or "If A, then B." A (the *hypothesis*) and B (the *conclusion*) are themselves mathematical statements like "$p|a$" or "S is a subset of T" or whatever. A **direct proof** of $A \implies B$ is a series of statements beginning with A and ending with B where each statement follows logically from the ones before it.

1 Wiggles the Cat

Here is a stupid example of a direct proof. Assume that the following things are true.

Fact 1.1. *If Wiggles the Cat is mad, then he is a dentist.*

Fact 1.2. *Every dentist has a secret.*

Fact 1.3. *If any cat has a secret, then it may come to dinner.*

Then we can prove the following proposition.

Proposition 1.4. *If Wiggles the Cat is mad, then he may come to dinner.*

Proof. To prove this statement, we'll start by assuming the hypothesis ("Wiggles the Cat is mad") is true, and use logical steps to arrive at the desired conclusion ("he may come to dinner").

1. Assume that Wiggles the Cat is mad.
2. Then by Fact 1.1 it follows that he is a dentist.
3. Since Wiggles is a dentist, then by Fact 1.2, he has a secret.
4. Since Wiggles has a secret and since he is a cat, then by Fact 1.3, he may come to dinner.

□

2 If and Only If Statements

The statement

$$A \iff B$$

reads "A if and only if B" and all it means is that A implies B and B also implies A. If you are asked to prove an "if and only if" statement, then you're being asked to prove two different statements, $A \implies B$ and $B \implies A$.

When you use previous propositions and theorems in a proof that you're writing you should think of the ones that are "if and only if" statements as two-way streets for whatever logical drive you're wanting to take. This is in contrast to any $A \implies B$ theorem that you may want to use which is a one-way street that let's you go from A to B, but not the other way around.

3 Definitions

Definitions in math are there to summarize information. For instance,

- The **intersection** of two sets S and T as $S \cap T = \{x : x \in S \text{ and } x \in T\}$,
- A function $f : S \to T$ is **surjective** if for every $t \in T$, there exists an $s \in S$ such that $f(s) = t$,
- For integers a and b we say that $a|b$ (a **divides** b) if and only if there exists some $k \in \mathbb{Z}$ such that $ak = b$.

are all definitions that give us shorthand for important ideas. Now we can talk about $S \cap T$ rather than describing what we mean with $\{x : x \in S \text{ and } x \in T\}$ whenever we need to use the concept of an intersection.

When we use definitions in proofs, we basically treat them like they are if and only if statements. In fact, the third example above is already written like one. But this does not mean that definitions can be proven or disproved. For example, why is it true that $a|b$ if and only if there exists some $k \in \mathbb{Z}$ such that $ak = b$? Because that's what I defined "$a|b$" to stand for! Before that it was nothing, just empty symbols.

In a proof, we treat definitions as two-way streets for taking logical steps if we need to. If you're at a step and you know that some function $f : S \to T$ is surjective, then you may logically conclude that for every $t \in T$, there exists an $s \in S$ such that $f(s) = t$ and no one can stop you. Conversely, if you have some function $f : S \to T$ for which you know that for every $t \in T$, there exists an $s \in S$ such that $f(s) = t$, then you may conclude that it's surjective.

Of course, the first definition defines an object (as opposed to a characteristic of an object like surjective or a relationship between two objects like $a|b$), and it wouldn't make much sense to treat it as an if and only if statement as we wrote it. However, anytime $S \cap T$ shows up, you can replace it with the set $\{x : x \in S \text{ and } x \in T\}$ and vice versa.

4 Some Direct Proofs

Proposition 4.1. *Let a, b, and c be integers. If $a|b$, then $a|bc$.*

Proof. 1. Assume that $a|b$.

2. Then by definition, there exists some $k \in \mathbb{Z}$ such that $ak = b$.

3. Since we can multiply two sides of an equation with the same thing (an outside assumption, but a reasonable one), then this implies that $akc = bc$.

4. Since $kc \in \mathbb{Z}$ and since $a(kc) = bc$, then by definition $a|bc$.

□

Definition Let a be an integer. We say that a is **even** if $2|a$. Otherwise, a is **odd**.

Proposition 4.2. *If x is an even integer, then x^2 is an even integer.*

Proof. 1. Let x be an even integer.

2. By definition of even, $2|x$.

3. By definition of divides, there exists some $k \in \mathbb{Z}$ such that $2k = x$.

4. Therefore, $x^2 = 4k^2$.

5. So $x^2 = 2(2k^2)$.

6. Since $2k^2$ is an integer, then by definition $2|x^2$.

7. Hence, by definition x^2 is even.

□

Definition Let $f : X \to Y$ and $g : Y \to Z$ be functions. Then the **composite** $g \circ f$ is the function defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

Proposition 4.3. *If $f : X \to Y$ and $g : Y \to Z$ are surjective functions, then $g \circ f : X \to Z$ is surjective.*

Before starting the proof of this let's think about what we need to show. We need to start with the fact that $f : X \to Y$ and $g : Y \to Z$ are surjective functions, and then we need to end up concluding that $g \circ f : X \to Z$ is surjective. By the definition of surjective, $g \circ f : X \to Z$ is surjective if and only if for every $z \in Z$, there exists some $x \in X$ such that $(g \circ f)(x) = z$.

Ok, so take some random $z \in Z$. Our goal is to show that something in X maps to it. So now we should probably take a closer look at our function $g \circ f$. By definition of

composite, we know that it is defined by taking each $x \in X$ and sending it to $g(f(x))$. So if $g \circ f$ is surjective, then there had better be some $x \in X$ for which $z = g(f(x))$ (where z is the random element we fixed).

Is there such an x? We're all done with unpacking the definitions for what we want to show, but we haven't thought about what the hypothesis is saying yet. It tells us that f and g are both surjective. I want to show that something goes to z, and I can see from the definition of surjective that g must send something to z. Of course, the thing it sends is from Y which is not what we want, but it's a step in the right direction maybe. Let's call the thing that get's sent y. So now we know that $g(y) = z$.

Now the only fact that we haven't used is that f is also surjective. So let's think about it. Everything in Y gets something sent to it from X through f. Hey, that means some element gets mapped to y and then would get mapped to z when we threw g into the mix! That's enough to get the proof started:

Proof.

1. Let $f : X \to Y$ and $g : Y \to Z$ be surjective functions.
2. Let $z \in Z$. Since g is surjective, there exists some $y \in Y$ such that $g(y) = z$.
3. Since f is surjective, we know that there exists some $x \in X$ such that $f(x) = y$.
4. Therefore, $g(f(x)) = g(y) = z$.
5. Since z was a arbitrary element of Z, then we've just shown that $g \circ f$ is surjective.

□