Math 300: Worked Examples
Northwestern, Spring 2013

This is a collection of examples and proofs worked out in detail. I also try to give a sense of the thought process you might go through in trying to come up with some of these proofs. Remember that a large part of learning how to form rigorous mathematical arguments (i.e. proofs) is having seen numerous examples written out so that you become comfortable with the techniques to use and when to try to use the. So, reading as many proofs as possible is a good thing. Let me know if there's anything specific you'd like to see on here.

Primes and Divisibility

Claim. *If p is a prime number, then $\sqrt{p}$ is irrational.*

Thoughts. To say that a number is rational is to say that we can write it as $\frac{a}{b}$ for some integers a and b with b nonzero. Thus to say that a number is irrational is to say that it is not possible to write it in this form. The trouble with trying to prove this claim directly is that it is not so easy to show directly that something *can't* be done. In general, when trying to show that something can't be done it will likely be much simpler to assume it can be done and show that something goes wrong. This is what a proof by contradiction is all about.

So, knowing that we might want to try a proof by contradiction, the next question is: what is the contradiction we should be aiming for, and how do we get there? This is where the real work is involved, and there is not one answer which works in all situations. In other words, the contradiction we aim for will likely change from problem to problem. Often times, we simply start trying to work things out and in the course of doing so realize at some a point a possible contradiction we could aim for, and then rework our arguments. In this case, we start with

$$\sqrt{p} = \frac{a}{b},$$

i.e. what it would mean for $\sqrt{p}$ to be rational, and start playing around knowing that at some point we will have to use the fact that p is prime. Here we immediately get

$$p = \frac{a^2}{b^2}, \text{ and then } pb^2 = a^2.$$

Notice that now we have something to work with, and in particular this equation says that a^2 is divisible by p. Notice this is not something we assumed at the beginning, but rather is a consequence of our work so far. In this case this is the point where p being prime is useful, since this will imply that a itself is also divisible by p; we state this fact as a lemma below. Again, we now have something further to work with, since this means we can write a as $a = pk$ for some integer k. We continue on, playing around with our equations more until we show that b would also have to be divisible by p.

To sum up, assuming that $\sqrt{p} = \frac{a}{b}$, we can show that both a and b would have to be divisible by p. At this point we realize that we can make the contradiction work out by making the right choice of a and b at the beginning. Here then is our final proof, after the statement of a brief lemma we will use.

Lemma. *Let p be a prime number. If p divides the product ab of integers a and b, then p divides a or p divides b. In particular, if p divides a^2, then p divides a.*

I invite you to think about why this is true, and how you might try to prove it. As a hint, consider the prime factorizations of a and b.

Proof of Claim. By way of contradiction, suppose that $\sqrt{p}$ is rational. Then there exist positive integers a and b with $b \neq 0$ such that a and b have no common factors other than 1 and $\sqrt{p} = \frac{a}{b}$. Then

$$p = \frac{a^2}{b^2}, \text{ so } pb^2 = a^2.$$

Hence p divides a^2, so since p is prime p divides a as well. Thus there exists an integer k such that $a = kp$. Substituting this into the expression above gives

$$pb^2 = k^2p^2, \text{ so } b^2 = k^2p.$$

Therefore p divides b^2, so p divides b as well since p is prime. This means that p is a common factor of a and b, contradicting the choice of a and b as having no common factors larger than 1. We conclude that $\sqrt{p}$ is irrational as claimed. □

One final comment here: if we had not chosen a and b with no common factors other than 1 at the beginning there is another contradiction we can derive. After we've shown that b is also divisible by p, we know we can write b as $b = \ell p$ for some integer ℓ. Then substituting $a = kp$ and $b = \ell p$ into our original expression for $\sqrt{p}$ we get

$$\sqrt{p} = \frac{a}{b} = \frac{kp}{\ell p} = \frac{k}{\ell}.$$

The point is that here k is smaller than a and ℓ is smaller than b, so we've shown that if we can write $\sqrt{p}$ as a fraction of positive integers, we can rewrite it as a fraction of *smaller* positive integers as well. Repeating the same argument would produce even smaller positive integers whose fraction was $\sqrt{p}$, and so on. This leads to a contradiction: since positive integers cannot be smaller than 1, it is not possible to keep on producing smaller and smaller positive integers whose fraction was still $\sqrt{p}$ as the above argument would suggest.

Claim. *Let $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$, then a or b is even.*

Thoughts. There are two possible problems in trying to prove this directly. One is that the conclusion we are trying to reach requires one of two things to be true, and we may not know which is actually true beforehand. In other words, how exactly do you directly prove that one of two things can happen? This can be avoided by using the following fact:

$$(P \implies Q \vee R) \text{ is equivalent to } (P \wedge \neg Q \implies R).$$

Work out the truth tables for each to convince yourselves that these implications mean the same thing. Intuitively this makes sense: think of the conclusion of the first implication as saying "either Q is true, or if Q is false then R must be true." To prove this we might say: "if Q is true there is nothing to show, so we assume instead that Q is false. In this case we need to show that R is true," which is precisely the statement of the rewritten implication.

The point is that the implication in the claim can be equivalently rephrased as "If $a^2 + b^2 = c^2$ and a is odd, then b is even." This is a bit better since now we only have *one* thing to show in our conclusion, and as an added benefit we have an additional hypothesis, namely that a is odd. This is good: the more hypotheses you have and the fewer conclusions you have, the easier it should

be to produce a proof. In this case however, we're stuck since there's really no way to go from $a^2 + b^2 = c^2$ and a odd to showing that b is even. The trouble is that although we can solve for b as

$$b = \sqrt{c^2 - a^2},$$

there's not much we can do at this point to conclude that b would have to be even as a result of a being odd, since there's no way we can "undo" the square root.

So, this suggests we should rephrase our original implication in another way, and the standard things to try are either contradiction or contrapositive. Both of these are possible, and we give both proofs below. The idea in either is to take the new assumption that a and b are both odd, and use this to figure out what type of integer $a^2 + b^2$ would have to be. Comparing this to the possibilities for c^2 ends up giving us our contradiction, or ends up proving the contrapositive if we proceed via that method instead.

Proof of Claim. By way of contradiction, suppose that $a^2 + b^2 = c^2$ and that both a and b are odd. Then there exist $k, \ell \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\ell+1$. Substituting into the above equation gives

$$(2k+1)^2 + (2\ell+1)^2 = c^2, \text{ or } 4(k^2 + \ell^2 + k + \ell) + 2 = c^2.$$

In particular then, c^2 is even so c is even as well. Hence we can write c as $c = 2m$ for some $m \in \mathbb{Z}$. However, this means that $c^2 = 4m^2$ so that 4 divides c^2. This is a contradiction, since previously we had

$$4(k^2 + \ell^2 + k + \ell) + 2 = c^2,$$

which implies that c^2 is not a multiple of 4. We thus conclude that if $a^2 + b^2 = c^2$, at least one of a or b is even as claimed. □

Alternate Proof. By way of contrapositive, suppose that both a and b are odd. We must show that $a^2 + b^2 \neq c^2$. Since a and b are odd, there exist $k, \ell \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\ell+1$. Then

$$a^2 + b^2 = (2k+1)^2 + (2\ell+1)^2 = 4(k^2 + \ell^2 + k + \ell) + 2,$$

so that $a^2 + b^2$ is an even integer which is not divisible by 4.

Now, there are two possibilities for c: either c is odd or c is even. If c is odd, then c^2 is odd and we cannot have $a^2 + b^2 = c^2$ since the left side is even. If c is even, then writing c as $c = 2k$ for some $k \in \mathbb{Z}$ gives $c^2 = 4k^2$ so that c^2 is divisible by 4. Thus again we cannot have $a^2 + b^2 = c^2$ since the left side is not divisible by 4. We conclude that $a^2 + b^2 \neq c^2$ as was to be shown. □

Claim. *There are infinitely many prime numbers.*

This is not all that an important fact for us since we won't do much if anything with prime numbers; indeed, this fact is given in Chapter 5 of our book, which we won't cover fully. Nonetheless, it is a good example which everyone should see at some point in their lives. This is an old argument of Euclid's, dating back to Ancient Greece. We give two versions (which are really the same): one phrased as a direct proof and one as a proof by contradiction. Notice how relatively simple the idea really is.

Proof. Suppose that $p_1, \ldots, p_n$ is a finite list of prime numbers and set

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $N > 1$ is an integer there exists a prime q dividing N. Now, if q was one of the primes $p_1, \ldots, p_n$, q would divide their product and hence would divide

$$1 = N - p_1 p_2 \cdots p_n$$

as well. This is not possible, so q cannot be among the primes $p_1, \ldots, p_n$. Thus given any finite list of primes we can always produce another prime not in that list, so the number of primes must be infinite. □

Alternate Proof. By way of contradiction, suppose that there are finitely many prime numbers. Call them $p_1, \ldots, p_n$ and set

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $N > 1$ is an integer there exists a prime q dividing N. Now, since $p_1, \ldots, p_n$ is the list of all possible prime numbers, q must be one of them. This implies that q divides $p_1 \cdots p_n$ and hence that q divides

$$1 = N - p_1 p_2 \cdots p_n.$$

This is a contradiction since 1 is not divisible by any prime, so we conclude that the number of primes is in fact infinite. □

Set Theory and Functions

Claim. *Let A and B be sets. Then $A \subseteq B$ if and only if $A \cap B = A$.*

Thoughts. If you read what this is saying out loud in words or draw a Venn diagram, it seems kind of obvious. And indeed it is: the point however is to write out a precise proof of this which makes no reference to what A and B might explicitly be. First we assume $A \subseteq B$ and show that $A \cap B = A$. To do so we must show that $A \cap B \subseteq A$ and $A \subseteq A \cap B$. To show $A \subseteq A \cap B$ for instance, we take $x \in A$ and show that $x \in A \cap B$, and to show this we must show that $x \in A$ and $x \in B$. Note that so far all we've done is unwind definitions, and indeed examples like this are good in that, while tedious at times, they force you to understand how to work with definitions and how to structure arguments. At this point, $x \in A$ since we are assuming that $x \in A$ to start with, and $x \in B$ comes from our original assumption that $A \subseteq B$. The rest of the proof is just as straightforward, and amounts to unwinding definitions.

Proof. Suppose that $A \subseteq B$; we must show that $A \cap B = A$. In order to do so we must show that each side is a subset of the other. First, if $x \in A \cap B$ then $x \in A$ and $x \in B$. Since $x \in A$, we conclude that $A \cap B \subseteq A$. Now let $x \in A$. Since $A \subseteq B$, $x \in B$. Thus $x \in A$ and $x \in B$ so $x \in A \cap B$ and hence $A \subseteq A \cap B$. Therefore $A \cap B = A$.

Conversely, suppose that $A \cap B = A$ and let $x \in A$. We must show that $x \in B$. Since $x \in A$ and $A = A \cap B$, we have $x \in A \cap B$. Hence $x \in A$ implies that $x \in B$, as was to be shown. Thus $A \subseteq B$ as claimed. □

Claim. *Let A and B be sets and $S \subseteq A$ And $T \subseteq B$. Then $S \times T \subseteq A \times B$.*

Thoughts. Another simple element chase which involves unraveling definitions. More interesting here is the fact that not every subset of a Cartesian product is of the form described in this claim. For instance, the subset

$$D := \{(x, x) \in \mathbb{R}^2 \mid x \in [0, 1]\}$$

of $[0,1] \times [0,1]$—i.e. the "main diagonal" of a unit square—is not of the form

$$(\text{subset of } [0,1]) \times (\text{subset of } [0,1]).$$

Suppose that it were, say $D = S \times T$ for some $S, T \subseteq [0,1]$. Since $(1/2, 1/2)$ and $(3/4, 3/4)$ are both in D, we would have $(1/2, 1/2) \in S \times T$ and $(3/4, 3/4) \in S \times T$. But then we would have $1/2 \in S$ and $3/4 \in T$ so that $(1/2, 3/4)$ would be in $S \times T$. However $(1/2, 3/4) \notin D$, contradicting $D = S \times T$.

Proof of Claim. Let $(s,t) \in S \times T$. Then $s \in S$ and $t \in T$ by the definition of a Cartesian product. Since $S \subseteq A$, $s \in A$ and since $T \subseteq B$, $t \in B$. Thus $(s,t) \in A \times B$ again by definition of a Cartesian product, so we conclude that $S \times T \subseteq A \times B$. □

Claim. *Let A and B be sets and let $\mathcal{P}(A)$ and $\mathcal{P}(B)$ denote their power sets. Then $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.*

Thoughts. This is another set-theoretic proof that boils down to unraveling definitions. The tricky concept is that of a power set and what it means for one set to be an *element* of (as opposed to subset of) another. If $S \in \mathcal{P}(A \cap B)$, we want to show that $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$, meaning $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$. However, to say that S is an element of a power set just means that S is a subset of the thing we are taking the power set of. So, the previous statement really says:

$$\text{If } S \text{ is a subset of } A \cap B, \text{ then } S \text{ is a subset of } A \text{ and } S \text{ is a subset of } B.$$

Maybe this is simpler to think about now that it is not phrased in terms of power sets.

Proof. Let $S \in \mathcal{P}(A \cap B)$. We want to show that $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$, or in other words that $S \subseteq A$ and $S \subseteq B$. To this end, let $s \in S$. Since $S \in \mathcal{P}(A \cap B)$, $S \subseteq A \cap B$. Hence $s \in A \cap B$ so $s \in A$ and $s \in B$. Since $s \in S$ implies $s \in A$, S is a subset of A, and since $s \in S$ implies $s \in B$, S is a subset of B. Thus $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$ so $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Therefore $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

Conversely, let $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$. We want to show that $S \in \mathcal{P}(A \cap B)$. To this end let $s \in S$. Since $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$, $S \subseteq A$ and $S \subseteq B$. Thus $s \in A$ and $s \in B$, so $s \in A \cap B$ and hence $s \in S$ implies $s \in A \cap B$. This means that $S \subseteq A \cap B$, so $S \in \mathcal{P}(A \cap B)$, showing that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ as needed. □

Claim. *For any $k \in \mathbb{N}$ let $k\mathbb{Z}$ denote the set of integer multiples of k. Then*

$$\bigcap_{k \in \mathbb{N}} \mathcal{P}(k\mathbb{Z}) = \{\emptyset, \{0\}\}.$$

Thoughts. This is a tricky one, but in the end (as usual) is all about unwinding definitions. Forget about what we are asked to show the intersection actually equals: the first question is, how would we even guess what the intersection should be if we weren't given that information beforehand? Let's figure out what it means for something to be in this intersection.

Saying that $A \in \bigcap_{k \in \mathbb{N}} \mathcal{P}(k\mathbb{Z})$ means that

$$\text{For all } k \in \mathbb{N}, A \in \mathcal{P}(k\mathbb{Z}).$$

To say that $A \in \mathcal{P}(k\mathbb{Z})$ simply means that $A \subseteq k\mathbb{Z}$, so $A \in \bigcap_{k \in \mathbb{N}} \mathcal{P}(k\mathbb{Z})$ means that

$$\text{For all } k \in \mathbb{N}, \ A \subseteq k\mathbb{Z}.$$

Now, $A \subseteq k\mathbb{Z}$ means that anything in A is also in $k\mathbb{Z}$, so since $k\mathbb{Z}$ is the set of all integer multiples of k we get that $A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$ means

$$\text{If } x \in A, \text{ then } x \text{ is an integer multiple of } k \text{ for all } k \in \mathbb{N}.$$

Note that this final statement says nothing about power sets and should be easier to digest than $A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$ itself. The point is that we are looking for sets A with the property that any element of it is a multiple of k for every possible $k \in \mathbb{N}$. But the only integer which is a multiple of every $k \in \mathbb{N}$ is 0, so the condition on says that simply "If there is something in A, then that something equals 0." Thus either A is empty or A contains only 0, which precisely gives the statement in the claim as to what this intersection equals.

All the ideas of our proof are written out above, and now all that is left is to organize it well. Again, the key in the above discussion is that we have to use definitions and what we know about mathematical statements to figure out precisely what it is we are supposed to show.

Proof of Claim. We must show that $\bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}) \subseteq \{\emptyset, \{0\}\}$ and that $\{\emptyset, \{0\}\} \subseteq \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$; we start with the second containment. First, $\emptyset \subseteq k\mathbb{Z}$ for all $k \in \mathbb{N}$ since $\emptyset$ is a subset of any set. Thus $\emptyset \in \mathcal{P}(k\mathbb{Z})$ for all $k \in \mathbb{N}$ and hence

$$\emptyset \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}).$$

Next, for any $k \in \mathbb{N}$, 0 is a multiple of k so $0 \in k\mathbb{Z}$ for any $k \in \mathbb{N}$. Thus $\{0\} \subseteq k\mathbb{Z}$ for all $k \in \mathbb{N}$, and hence $\{0\} \in \mathcal{P}(k\mathbb{Z})$ for all $k \in \mathbb{N}$. This means that

$$\{0\} \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}),$$

and putting this together with the previous fact that $\emptyset$ is in this intersection as well, we conclude that

$$\{\emptyset, \{0\}\} \subseteq \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}).$$

Now, for the other containment, let $A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$. We must show that $A \in \{\emptyset, \{0\}\}$, which requires us to show that $A = \emptyset$ or $A = \{0\}$. Now, since $A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$ we have that

$$A \in \mathcal{P}(k\mathbb{Z}) \text{ for all } k \in \mathbb{N}, \text{ and hence that } A \subseteq k\mathbb{Z} \text{ for all } k \in \mathbb{N}.$$

Thus for any $x \in A$, $x \in k\mathbb{Z}$ for all $k \in \mathbb{N}$. Since the only integer which is a multiple of k for every $k \in \mathbb{N}$ is 0, this means that for any $x \in A$, $x = 0$. Therefore either A is empty, or A consists only of $\{0\}$. Hence

$$\text{if } A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}), \text{ then } A = \emptyset \text{ or } A = \{0\},$$

so if $A \in \bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z})$, then $A \in \{\emptyset, \{0\}\}$. We conclude that $\bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}) \subseteq \{\emptyset, \{0\}\}$, and hence $\bigcap_{k\in\mathbb{N}} \mathcal{P}(k\mathbb{Z}) = \{\emptyset, \{0\}\}$ as claimed. □

Claim. *Let A be any set, and let $\{0,1\}^A$ denote the set of functions $A \to \{0,1\}$. Then there exists a bijection between $\mathcal{P}(A)$ and $\{0,1\}^A$.*

Thoughts. First, the notation B^A for the set of functions from A to B is very standard even though it might seem kind of strange. There are reasons for this, but they go a little beyond the scope of this course. The claim is that there is a way to associate to any subset of A a function from

A to $\{0,1\}$, and this association gives a one-to-one correspondence between subsets of A and such functions.

Here is the key idea: a subset of A is determined by specifying which elements of A are in it and which elements of A aren't in it. To those elements in the subset, we define the corresponding function by sending those to 1, and for the elements not in the subset the function will send them to 0. So, the function we associate to a subset of A "picks out" the subset as the set of elements it sends to 1.

Proof. We construct a function $F : \mathcal{P}(A) \to \{0,1\}^A$ as follows. For $S \subseteq A$ let $f_S : A \to \{0,1\}$ be the function defined by

$$f_S(a) = \begin{cases} 1 & \text{if } a \in S \\ 0 & \text{if } a \notin S. \end{cases}$$

Then define F by setting $F(S) = f_S$. We claim that F is bijective. To show this, we could directly show that F is injective and surjective, but instead we show that F is invertible by constructing an explicit inverse function. Our claim then follows since a function is invertible if and only if it is bijective.

Define $F^{-1} : \{0,1\}^A \to \mathcal{P}(A)$ as follows. For a given function $f : A \to \{0,1\}$ define $F^{-1}(f)$ to be the subset of A given by the inverse image $f^{-1}(\{1\})$ of $\{1\}$ under f; that is:

$$F^{-1}(f) = f^{-1}(\{1\}) \text{ for any } f \in \{0,1\}^A.$$

To check that F^{-1} is indeed the inverse of F we show that $FF^{-1} = id_{\{0,1\}^A}$ and $F^{-1}F = id_{\mathcal{P}(A)}$.

First suppose that $S \in \mathcal{P}(A)$. Then $F(S) = f_S$ and $F^{-1}(f_S) = f_S^{-1}(\{1\})$. Since the elements of A which f_S sends to 1 are precisely those in S, we see that $f_S^{-1}(\{1\}) = S$. Thus

$$(F^{-1}F)(S) = F^{-1}(F(S)) = F^{-1}(f_S) = f_S^{-1}(\{1\}) = S \text{ for any } S \in \mathcal{P}(A),$$

so $F^{-1}F = id_{\mathcal{P}(A)}$. Next let $f : A \to \{0,1\}$ be any function. Then $S := f^{-1}(\{1\})$ is a subset of A, and $F(S) = f_S$ is the function sending things in S to 1 and everything else to 0. However, since $S = f^{-1}(\{1\})$ the things in S are precisely the things which f sends to 1 so f_S and f both sends things in S to 1 and both send things not in S to 0. Thus $f_S = f$ so

$$(FF^{-1})(f) = F(F^{-1}(f)) = F(f^{-1}(\{1\}) = f \text{ for any } f \in \{0,1\}^A.$$

This means that $FF^{-1} = id_{\{0,1\}^A}$, so F^{-1} is the inverse of F as claimed. We conclude that F is invertible. □

Note that this fact gives another way to prove that the power set of a set with n elements has 2^n elements. If A is finite with n elements, the existence of the above bijection implies that $\mathcal{P}(A)$ has as many things in it as does $\{0,1\}^A$. To count the number of functions $A \to \{0,1\}$, note that for each element of A there are 2 choices for where it can be sent. Since this is true for each of the n elements of A, there are

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{n \text{ times}} = 2^n$$

such functions $A \to \{0,1\}$. Thus if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Binary Operations and Equivalence Relations

Claim. *Define the binary operation $*$ on $\mathbb{R}$ by $a * b := a + b + ab$ for all $a, b \in \mathbb{R}$. This operation is associative, commutative, has an identity element, and every number except -1 has an inverse.*

Thoughts. The first two parts of this—checking associativity and commutativity—are routine checks which just involve fully computing some expressions. For example, to check associativity we have to compute $(a * b) * c$ and $a * (b * c)$ and see that both give the same thing.

Checking for the existence of an identity and inverses is more interesting. An identity should be a real number x which sastisfies $a * x = a$ and $x * a = a$ for all $a \in \mathbb{R}$, but since $*$ is actually commutative just satisfying $a * x = a$ for all $a \in \mathbb{R}$ is enough. Using the definition of $*$ this becomes

$$a + x + ax = a \text{ for all } a \in \mathbb{R}.$$

To find the identity x, note that this equation (after subtracting a from both sides) is the same as

$$x + ax = 0, \text{ or } x(1 + a) = 0 \text{ for all } a \in \mathbb{R}.$$

In order for this to be true for every single a, we need $x = 0$. Thus, the claim is that $0 \in \mathbb{R}$ is the required identity for $*$, and this is what we will show in the proof below.

Finding the inverse of an element $a \in \mathbb{R}$ is done via a similar process. The inverse of a should be some $b \in \mathbb{R}$ satisfying $a * b = 0$ (0 since we've already determined that 0 should be the identity) and $b * a = 0$. Again, satisfying $a * b = 0$ is enough due to commutativity of $*$. Thus we need b to satisfy

$$a + b + ab = 0,$$

and we simply have to solve this for b. We get that $b = -\frac{a}{1+a}$, which we now see only makes sense for $a \neq -1$. In the proof below we show that this choice for b indeed satisfies the required property of an inverse. Note that all the work which went into finding the identity and inverses was done here in our "scratch work", and we don't reproduce all this work in the the presented proof.

Proof of Claim. First we check associativity of $*$. Let $a, b, c \in \mathbb{R}$. Then

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ab + bc + abc\end{aligned}$$

and

$$\begin{aligned}a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc.\end{aligned}$$

Comparing these two expressions shows that $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathbb{R}$, so $*$ is associative. Since

$$a * b = a + b + ab = b + a + ba = b * a \text{ for all } a, b \in \mathbb{R},$$

the operation $*$ is commutative.

Now, we claim that 0 is an identity for $*$. Indeed, for any $a \in \mathbb{R}$ we have

$$a * 0 = a + 0 + a(0) = a$$

and $0 * a = a$ immediately follows from the commutativity of $*$. Thus $a * 0 = a = 0 * a$ for all $a \in \mathbb{R}$, so 0 is the identity for $*$. Finally, suppose that $a \in \mathbb{R}$ and that $a \neq 1$. Then $-\frac{a}{a+1}$ is a real number and

$$\begin{aligned}\left(-\frac{a}{a+1}\right) * a = a * \left(-\frac{a}{a+1}\right) &= a + \left(-\frac{a}{a+1}\right) + a\left(-\frac{a}{a+1}\right) \\ &= a - \frac{a}{a+1} - \frac{a^2}{a+1} \\ &= \frac{a(a+1) - a - a^2}{a+1} \\ &= \frac{a^2 + a - a - a^2}{a+1} \\ &= 0.\end{aligned}$$

Hence for $a \neq -1$, $-\frac{a}{a+1}$ satisfies the required property to be the inverse of a under $*$, so any real number which is not -1 has an inverse as claimed. □

Claim. *Let n be a positive integer. Define the relation R on $\mathbb{Z}$ by aRb if $a - b$ is divisible by n. Then R is an equivalence relation which has n equivalence classes.*

Thoughts. The first part of this, checking that R is an equivalence relation, is done by verifying that the three properties required of an equivalence relation are satisfied. The only tricky one might be checking that R is transitive, where from the assumptions that $a - b$ and $b - c$ are multiples of k we must show that $a - c$ is also a multiple of k. We get this by adding together $a - b$ and $b - c$, but if nothing else note that we could do the following: if $a - b = nk$ and $b - c = n\ell$ for some integer k and ℓ, we can get an expression for $a - c$ by solving for c in the second equation and then substituting the result in for c in $a - c$.

Trickier is determining the equivalence classes. In general, it will be useful to try to figure out what an equivalence class looks like first. That is, given some a, can we determine precisely what elements a is equivalent to? In this case we can do so explicitly using the fact that for b to be equivalent to a, $b - a = nk$ for some $k \in \mathbb{Z}$ and this gives a way to express b in terms of a. Here we have to use the following special property of the integers:

> For any $x \in \mathbb{Z}$, there exist unique integers q and r with $0 \leq r < n - 1$ such that $x = qn + r$.

Think of r as the "remainder" you get when dividing x by n; this doesn't quite work for negative x but it goes a long way toward giving the correct intuition.

Proof. First, for any $a \in \mathbb{Z}$, $a - a = 0$ is divisible by n. Thus aRa for any $a \in \mathbb{Z}$ so R is reflexive. Now, suppose that aRb. Then $a - b$ is divisible by n so

$$a - b = nk \text{ for some } k \in \mathbb{Z}.$$

This gives $b - a = -nk = n(-k)$, so $b - a$ is also divisible by n. Hence aRb implies bRa so R is symmetric.

Finally, suppose that aRb and bRc. Then $a - b$ is divisible by n and $b - c$ is divisible by n, so

$$a - b = nk \text{ and } b - c = n\ell \text{ for some } k, \ell \in \mathbb{Z}.$$

This gives

$$a - c = (a - b) + (b - c) = nk + n\ell = n(k + \ell),$$

so $a - c$ is also divisible by n. Hence aRb and bRc implies aRc so R is transitive. Since R is reflexive, symmetric, and transitive, R is an equivalence relation as claimed.

We now determine the equivalence classes. As usual we denote this equivalence relation by $\sim$ from now on. For each $a \in \mathbb{Z}$, the equivalence class $[a]$ of a is the set of all things which are equivalent to a:

$$[a] := \{b \in \mathbb{Z} \mid b \sim a\}.$$

In this case, $b \sim a$ means that $b - a$ is divisible by n, so $b - a = nk$ for some $k \in \mathbb{Z}$. Rewriting this gives $b = nk + a$, so we conclude that b is in the equivalence class of a precisely when we can express it as a multiple of n plus a:

$$[a] = \{kn + a \mid k \in \mathbb{Z}\}.$$

We claim that $[0], [1], [2], \ldots, [n-1]$ are all the equivalence classes. Indeed, any integer $b \in \mathbb{Z}$ can be written as $b = nk + r$ with $k \in \mathbb{Z}$ and $0 \leq r < n$ in a unique way (r is the "remainder" term), so any $b \in \mathbb{Z}$ will be in the equivalence class of such an r. In particular, the multiples of n are in the equivalence class $[0]$, the integers which are 1 more than a multiple of n are in $[1]$, those which are 2 more than a multiple of n are in $[2]$, and so on. This gives $[0], [1], [2], \ldots, [n-1]$ as the equivalence classes since these are the only possible "remainder" terms, and there are n of these as claimed. □

Cardinality

Claim. *A real number α is said to be algebraic if there exists a polynomial $p(x)$ with integer coefficients such that $p(\alpha) = 0$. The set $\mathbb{A}$ of algebraic numbers is countable.*

Thoughts. A polynomial is an expression of the form $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, and to say that this has integer coefficients means that $a_1, a_2, \ldots, a_n$ are all integers. There are two key points here: any such polynomial is completely determined by its coefficients, which we can view all together as an element of $\mathbb{Z}^{n+1}$:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mapsto (a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1},$$

and any such polynomial has at most n roots. Since $\mathbb{Z}^m$ is countable for each m, the set of polynomials of fixed degree m with integer coefficients will then be countable, and the set of all polynomials with integer coefficients can be expressed as the union of these as the degree m ranges through all possible (countable) values. This will give a way to express the set of algebraic numbers $\mathbb{A}$ as a countable union of finite sets, from which the claim will follow.

Proof. Fix $n \in \mathbb{Z}_{\geq 0}$ and consider the set P_n of polynomials of degree at most n with integer coefficients:

$$P_n = \{a_n x^n + \cdots + a_1 x + a_0 \mid \text{ each } a_i \text{ is in } \mathbb{Z}\}.$$

The function $P_n \to \mathbb{Z}^{n+1}$ given by

$$a_n x^n + \cdots + a_1 x + a_0 \mapsto (a_n, \ldots, a_1, a_0)$$

is a bijection, so P_n has the same cardinality as $\mathbb{Z}^{n+1}$. Since $\mathbb{Z}^{n+1}$ is countable, P_n is countable as well. Now, let P denote the set of all polynomials with integer coefficients. This can be expressed as the union of all the P_n:

$$P = \bigcup_{n=0}^{\infty} P_n.$$

Since this is the union of countably many countable sets, it is countable itself.

Finally, since P is countable, there is some listing of its elements:

$$p_1(x), p_2(x), p_3(x), \ldots$$

which includes all possible polynomials with integer coefficients. For each i, $p_i(x)$ only has finitely many roots. Thus $\mathbb{A}$, which can be expressed as

$$\mathbb{A} = \bigcup_{i=1}^{\infty} \{\text{roots of } p_i(x)\},$$

is the union of countably many finite sets, and so is countable as well as claimed. □

Claim. $\mathbb{R}^2$ *and* $\mathbb{R}$ *have the same cardinality.*

Proof. We first show that $(0,1) \times (0,1)$ and $(0,1)$ have the same cardinality. Define the function $f : (0,1) \times (0,1) \to (0,1)$ by

$$f(0.x_1x_2x_3\ldots, 0.y_1y_2y_3\ldots) = 0.x_1y_1x_2y_2x_3y_3\ldots,$$

where we represent a number in $(0,1)$ in terms of its decimal expansion. This function is invertible since it has inverse $f^{-1} : (0,1) \to (0,1) \times (0,1)$ given by

$$f^{-1}(0.a_1a_2a_3a_4\ldots) = (0.a_1a_3a_5\ldots, 0.a_2a_4a_6\ldots).$$

Thus f is bijective so $(0,1) \times (0,1)$ and $(0,1)$ have the same cardinality.

Now, since $(0,1)$ and $\mathbb{R}$ have the same cardinality, there is a bijective function $g : (0,1) \to \mathbb{R}$. Then the function $(0,1) \times (0,1) \to \mathbb{R} \times \mathbb{R}$ defined by

$$(x, y) \mapsto (g(x), g(y))$$

is bijective, so $(0,1) \times (0,1)$ and $\mathbb{R}^2$ have the same cardinality. Putting it all together, $\mathbb{R}^2$ has the same cardinality as $(0,1) \times (0,1)$, which has the same cardinality as $(0,1)$, which has the same cardinality as $\mathbb{R}$, so $\mathbb{R}^2$ and $\mathbb{R}$ have the same cardinality. □

Claim. *The set of functions from* $\mathbb{R}$ *to* $\mathbb{R}$ *has the same cardinality as the power set of* $\mathbb{R}$.

Proof. Let $F(\mathbb{R})$ denote the set of functions from $\mathbb{R}$ to $\mathbb{R}$ and let $\mathcal{P}(\mathbb{R})$ denote the power set of $\mathbb{R}$. We construct injections $F(\mathbb{R}) \to \mathcal{P}(\mathbb{R})$ and $\mathcal{P}(\mathbb{R}) \to F(\mathbb{R})$, and then the Schroeder-Bernstein Theorem will imply that $F(\mathbb{R})$ and $\mathcal{P}(R)$ have the same cardinality.

First, let $f \in F(\mathbb{R})$. The graph of f is the subset $\operatorname{gr} f$ of $\mathbb{R}^2$ defined by

$$\operatorname{gr} f := \{(x, f(x)) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}.$$

If two functions f and g have the same graph, then for any $x \in \mathbb{R}$ we have

$$(x, f(x)) = (x, g(x)), \text{ so } f(x) = g(x).$$

Hence if f and g have the same graph then $f(x) = g(x)$ for all $x \in \mathbb{R}$, so f and g are the same function. This means that the map $F(\mathbb{R}) \to \mathcal{P}(\mathbb{R}^2)$ defined by $f \mapsto \text{gr } f$ is injective. Since $\mathbb{R}^2$ and $\mathbb{R}$ have the same cardinality, a problem on the last homework assignment implies that $\mathcal{P}(\mathbb{R}^2)$ and $\mathcal{P}(\mathbb{R})$ have the cardinality. Thus there exists a bijection $\mathcal{P}(\mathbb{R}^2) \to \mathcal{P}(\mathbb{R})$, and composing $F(\mathbb{R}) \to \mathcal{P}(\mathbb{R}^2)$ with this gives an injection $F(\mathbb{R}) \to \mathcal{P}(\mathbb{R})$.

Now let $S \in \mathcal{P}(\mathbb{R})$. Define the function $f_S : \mathbb{R} \to \mathbb{R}$ by

$$f_S(a) = \begin{cases} 1 & \text{if } a \in S \\ 0 & \text{if } a \notin S. \end{cases}$$

A previous claim on this handout implies that the map $\mathcal{P}(\mathbb{R}) \to F(\mathbb{R})$ defined by $S \mapsto f_S$ is injective. Hence we conclude by the Schroeder-Bernstein Theorem that $F(\mathbb{R})$ and $\mathcal{P}(\mathbb{R})$ have the same cardinality as claimed. $\square$