MATH 300: CHAPTER 2- FORMAL PROOFS

TOM BENHAMOU
RUTGERS UNIVERSITY

The purpose of this lecture is to learn how to write formal proofs. We will also develop basic number theory, mostly to demonstrate formal proofs.

1. Formal Proofs

1.1. **Why do we need proofs?** Unlike day-to-day information, when a mathematical statement is being claimed, there must be some calculation/ argument establishing it. This is the true power of mathematics which makes it so convincing. It gives us the sensation that the truth of mathematical statements is absolute, and there is no room for interpretations.

What grants mathematics this ability is its high standard of precision and accuracy. This accuracy is well understood when considering calculations which we are already accustomed to. But what shall we do if the mathematical statement does not involve only calculations?

Proofs are designated exactly for that. They serve all mathematicians as a convincing tool, and as such a tool, proofs have a rigid structure, specific words which are used, which are all determined by the logical structure of the statement we intend to proof.

Given a statement which you believe (conjecture) to be true, the only acceptable way to establish your conjecture as a theorem (mathematical truth) is to provide a proof for it.

Remember! If you claim something, it is your responsibility to back up your claim with a formal proof.

1.2. **How to write a proof?** It takes some practice to understand how to write proofs, the students are encouraged to write down on their own as much proofs as possible, starting from proving trivial statements and gradually amplify the logical complexity of the statements.

Let us try and explain how to form proofs.

Rule 1: you should prove everything you claim in this course which is not a statement learned in the average American education system up to 8th grade.

Example 1.1. The statements

"the sum of two even numbers is even" or "for every x, $x < x + 1$"

Date: February 5, 2024.

do not require proofs. While “There are infinitely many prime numbers”, “for every $n > 2$, $2^n < n^n$” do require one.

Every statement you will encounter in this course can be formalized using the propositional and predicate calculus. There is no actual need to formalize each and every statement, instead, we should only focus on the logical structure of the statement.

Rule 2: The logical structure of a statement determines the structure of the proof.

For logical connectives, we use the truth table:

Example 1.2. Prove that: Either $2 > 17$ or Paris is the capital of France.

Proof. This is a disjunction $A \vee B$, where A is $2 > 17$ and B is ”Paris is the capital of France” (By rule 1 this is ok). Indeed B is true and therefore (by the truth table of $\vee$) $A \vee B$ is true. □

The structure of a proof for $A \wedge B$ and $\sim A$ is very similar. However, implications $A \Rightarrow B$ are a bit more involved, and we will discuss them in a separate section.

One part which is not mathematical but improves the readability of proofs is the declaration of what you are about to do. There are several commonly used such declarations which we will gather along the way.

Rule 3: Declare what you are about to do.

Example 1.3. Let us re-write the previous proof with some guiding declarations. Among the most common declarations is ”WTP” (want to prove). This is more of a psychological trick that helps us distill what we should do in the proof.

Proof. WTP $A \vee B$ where A is $2 > 17$ and B is ”Paris is the capital of France”. We will prove it by referring to the truth table (this is also a declaration), indeed B is true and therefore $A \vee B$ is true. □

Any given mathematical statement has two parts:

(1) The assumptions:
   (a) Assumptions stated in the theorem.
   (b) Assumptions inffered from the logical structure of the statement.
   (c) Assumptions that arise from some previous definition.
   (d) Previously proven statements under the same assumptions.
   (e) An equivalent statement to another assumption.
   (f) Axiom (will be discussed in the future).
(2) The conclusion: the new information that the statement introduces.

Rule 4: Assumptions can appear in a proof at any time.

Example 1.4. Prove the following statement: Suppose that $n \in \mathbb{N}$ is a number greater than 2, prove that $n^2 \geq 9$.

Proof. We assume that $n \in \mathbb{N}$ and $n > 2$ and WTP $n^2 \geq 9$. By the assumption that $n \in \mathbb{N}$, and by definition of $\mathbb{N}$, since $n > 2$ then $n \geq 3$. Then $n^2 = n \cdot n \geq 3 \cdot 3 = 9$. □

As we will see, not all statements have assumptions[1].

The last general rule we consider is called "modus ponens"

Rule 4: If P and $P \Rightarrow Q$ appeared in the proof then we can deduce Q.

2. Proving existential statements and Imprications

As we have seen in the previous section, the general structure of a proof of a logical connective is simple, one should prove that one of the truth assignments that turns the logical connective T holds (namely one of the rows in the truth table). For implications, this is more involved and requires clarification. Let us just focus on proving implication, as this is a very common proof structure. Recall that $P \Rightarrow Q$ is true if either P is false or P is true and Q is true. Hence there are two ways to proof an implication:

(1) (99.9% of the cases) assume that the antecedent P holds true and deduce that the consequent Q follows.

(2) (0.1% of the cases) Prove that the implication is *vacuous*, namely that the antecedent P is false.

Proof structure of implication $P \Rightarrow Q$:
Assume P.
...
Therefore, Q.
Thus $P \Rightarrow Q$.

In 99.9% of the cases, to prove an existential statement of the form $\exists x(p(x))$, one should:

(1) provide a specific *witness* x_0.

(2) Prove that $p(x_0)$ holds.

Proof structure for $\exists x(p(x))$:
Define/Let/Consider $x_0 = ...$
WTP $p(x_0)$
(proof of $p(x_0)$)
Thus $\exists x(p(x_0))$.

2.1. **Some basic definitions in Number Theory.**

Definition 2.1. An integer $n \in \mathbb{Z}$ is said to be *divisible* by m if there exists an integer $k \in \mathbb{Z}$ such that $n = k \cdot m$.

Definition 2.2. An *even* integer is any integer n which is divisible by 2. An *odd* integer is any integer which is not even.

[1] Except for the axioms.

Remark 2.3. An even number is of the from $2k$ where k is an integer. An odd number is of the form $2k+1$.

Example 2.4. Prove the following implications:

(1) Let x be an integer. if x is odd, then $x+1$ is even.

Proof. Suppose that x is odd (this is step 1). WTP $x+1$ is even. Since x is odd, $x = 2k+1$ where k is some integer [2]. Therefore,

$$x+1 = (2k+1)+1 = 2k+2 = 2(k+1).$$

It follows that $x+1$ is 2 times the integer[3] $k+1$ and hence, by definition, $x+1$ is even. Thus if x is odd then $x+1$ is even. □

(2) Let x, y be real numbers. Show that if $x < -1$ and $y > 2$ then the distance of the point (x, y) from the points $(1, 0)$ is greater than 7.

Proof. Suppose that $x < -1$ and $y > 2$. WTP the distance between (x, y) and $(1, -1)$ is greater than 4. The distance is defined by

$$d = \sqrt{(x-1)^2 + (y-(-1))^2} = \sqrt{(x-1)^2 + (y+2)^2}$$

Since $x < -1$, $x - 1 < -1 - 1 = -2$ and therefore $(x-1)^2 > (-2)^2 = 4$. Also since $y > 2$, $y + 2 > 2 + 2 = 4$ and therefore $(y+2)^2 > 4^2 = 16$. Hence

$$d > \sqrt{4+16} = \sqrt{20} > \sqrt{16} = 4$$

□

(3) If n is an even integer then n^2 is also even.

Proof. Suppose that[4] n is even. We want to prove that n^2 is even. By our assumption that n is even there is an integer k such that $n = 2k$. Substituting n by $2k$ we get,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Since $2k^2$ is an integer, we conclude that[5] n^2 is divisible by 2 and therefor an even number. □

(4) If n, m are odd integers then $n \cdot m$ is also odd.

Proof. Suppose that n, m are odd integers, then there are integers l, k such that

$$n = 2k+1, \quad m = 2l+1$$

Hence

$$nm = (2k+1)(2l+1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$$

Since $z = 2kl + k + l$ is an integer, $nm = 2z + 1$ and therefore an odd number. □

[2] This is equivalent by the previous remark.

[3] Here we use the basic fact that if k is an integer then $k+1$ is an integer.

[4] The structure of an implication is to first assume the antecedent and to prove the consequent.

[5] By the definition of divisibility.

Example 2.5. Prove the following statements:

(1) There is a natural number n such that $n^2 + 2n + 1$ is divisible by 4.
(2) There is x such that $x^2 < 0 \vee 6 > 5$.
(3) $\exists x(x + 1 = 0)$
(4) $(\exists x(x^2 < 0)) \vee (\exists x(x^2 > 0))$.
(5) $\exists x(x > 0 \Rightarrow 0 = 1)$.
(6) $\sim [(\exists x(x > 0)) \Rightarrow 0 = 1]$.

To provide the witness inside a proof (the first step of an existential proof) one should use the word "define" or "set" to declare his intention.

(1) Claim: There is a natural number n such that $n^2 + 2n + 1$ is divisible by 4.

Proof. Define[6] $n = 3$, then[7] $3^2 + 2 \cdot 3 + 1 = 16$ which is divisible by 4 [8] □

(2) Claim: There is x such that $x^2 < 0 \vee 1 + x > 5$.

Proof. Set $x = 7$. We need to prove that $(7^2 < 0) \vee (1 + 7 > 5)$. This is true[9] since $1 + 7 = 8 > 5$ □

(3) Claim: $\exists x(x + 1 = 0)$.

Proof. Define $x = -1$, then $-1 + 1 = 0$. □

(4) Claim: $(\exists x(x^2 - 1 < 0)) \wedge (\exists x(x^2 - 1 > 0))$.

Proof. We prove separately that [10]:

a. Claim: $\exists x(x^2 - 1 < 0)$.
Proof. Define $x = 0$, then $0^2 - 1 = -1 < 0$. □
b. Claim: $\exists x(x^2 - 1 > 0)$.
Proof. Define $x = 2$ then $2^2 - 1 = 3 > 0$. □

Hence we proved the $\wedge$-statement. □

(5) Claim: $\exists x(x > 0 \Rightarrow 0 = 1)$.

Proof. Define $x = -1$, we want to prove that $-1 > 0 \Rightarrow 0 = 1$ holds, but $-1 > 0$ is false, hence the implication is true vacuously. □

(6) Claim: $\sim [(\exists x(x > 0)) \Rightarrow 0 = 1]$.

[6] We use the same variable letter "n" as in the claim, this is the first step in an existential proof

[7] This is the second step of the proof of an existential statement.

[8] the fact that 16 is divisible by 4 does not require a proof, but as a practice, one should **prove** it using the previous definition.

[9] By the truth table of the logical connective $\vee$, to prove $\alpha \vee \beta$ it suffices to prove either α or to prove β. In our case it did not matter that $7^2 < 0$ is false since we proved the other.

[10] Note here that before it is an existential statement, it is a $\wedge$-statement. By the truth table, in order to prove $\alpha \wedge \beta$, we should prove both α and β.

Remark 2.6. Notice the difference between the previous example which can also be written as $\exists x(x > 0 \Rightarrow 0 = 1)$ and the current on $(\exists x(x > 0)) \Rightarrow 0 = 1$.

Proof. To disprove the claim we want to prove that $\sim ((\exists x(x > 0)) \Rightarrow 0 = 1)$ By the low of negation of implication $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$. Hence we want to prove that $(\exists x(x > 0)) \wedge \sim (0 = 1)$. To prove this $\wedge$-statement, we prove each statement separately. $\sim (0 = 1)$ is clear.

Claim: $\exists x(x > 0)$.

Proof. Define $x = 1$, then $x > 0$. □

□

Theorem 2.7. *Let a, b, c be integers. If a divides b and b divides c, then a divides c.*

Proof. Let a, b, c be integers.

Suppose that a divided b and b divides c. WTP a divides c.

By the assumption, there are integers k, l such that

$$b = al \text{ and } c = bk.$$

Substituting b we get $c = bk = (al)k = a(lk)$. Since the multiplication of integers is an integer, then lk is an integer. Hence there is an integer m (namely $m = lk$) such that $c = am$ and therefore a divides c. Thus, if a divides b and b divides c then a divides c.

□

2.2. **Applying theorems.** Usually theorems are formulated in the most general form. However, when we would like to *apply* a theorem, we will do it for a specific case which falls under the assumptions of the theorem.

Example 2.8. Claim: If $n = 10k + 5$ where k is an integer, namely that the units digit of n is 5, then $n^2 = k(k + 1) \cdot 100 + 25$.

Before proving the claim, let us see how to apply it. Pick your favorite integer with unit digit 5, say $n = 95$. Then, by the claim, since $95 = 10 \cdot 9 + 5$, we have $k = 9$ and $95^2 = 9 \cdot 10 \cdot 100 + 25 = 9025$.

Proof. Suppose that $n = 10k + 5$. We want to prove that $n^2 = k(k+1)100 + 25$. Substituting n, we have

$$n^2 = (10k+5)^2 = (10k)^2 + 10k \cdot 5 \cdot 2 + 5^2 = 100k^2 + 100k + 25 = 100k(k+1) + 25$$

□

3. Logical equivalence

One other thing we can use in proofs is to switch the statement with an logically equivalent one.

3.1. **Splitting into cases.** Since $P \vee \sim P$ is a tautology, for every statemnt Q we have that $Q \equiv (P \vee \sim P) \Rightarrow Q$. In parctice, this means that if we wish to prove Q we can prove it by splliting into cases, which have have the following structure:

(1) Case 1: Assume P. We want to prove Q.
(2) Case 2: Assume $\sim P$. We want to prove Q.

Note that we can split into more cases as long as we cover all the possible cases.

Example 3.1. Claim: Let n be any integer. Then $n^2 + n$ is even.

Proof. Let n_0 be any integer. We want to prove that $n_0^2 + n_0$ is even. Let us split into cases:

(1) Case 1: Assume n_0 is even. We want to prove that $n_0^2 + n_0$ is even. Indeed, $n_0^2 + n_0 = n_0(n_0 + 1)$. A even integer times any integer is even, hence $n_0^2 + n_0$ is even.
(2) Case 2: Assume n_0 is odd. We want to prove that $n_0^2 + n_0$ is even. Since n_0 is odd, $n_0 + 1$ is even, and as in the previous case we see that $n_0^2 + n_0$ is a product of odd times even which is even.

□

3.2. **Contrapositive.** As we said earlier, we are allowed to prove logically equivalent statement. One of the most common logical equivalences which are used is the contapositive $P \Rightarrow Q \equiv (\sim Q) \Rightarrow (\sim P)$.

Example 3.2. Claim: Prove that if $n^2 - 1$ is odd then n is even.

Proof. This is an implication, let us state its contrapositive: if n is odd then $n^2 - 1$ is even.

Suppose that n is odd. We want to prove that $n^2 - 1$ is even. By our assumption, there is an integer l such that $n = 2l + 1$. It follows that,

$$n^2 - 1 = (2l + 1)^2 - 1 = (4l^2 + 4l + 1) - 1 = 4l^2 + 4l = 2(2l^2 + 2l)$$

Since $2l^2 + 2l$ is an integer, $n^2 - 1$ is even. □

3.3. **If and only if statements.** Another useful logical equivalence is $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Hence the structure of a proof of an "if and only if" statements is a *double implications*:

(1) Prove $P \Rightarrow Q$.
(2) Prove $Q \Rightarrow P$.

Example 3.3. Claim: Let n be an integer of the form $n = 10 \cdot k + d$ where k, d are integers. Then,

$$k + d \cdot 5 \text{ is divisible by } 7 \Leftrightarrow n \text{ is divisible by } 7$$

Proof. Let us prove this biconditional statement by a double implications:

(1) $\underline{k+d\cdot 5 \text{ is divisible by } 7 \Rightarrow n \text{ is divisible by } 7}$: Suppose that $k+d\cdot 5$ is divisible by 7. We want to prove that n is divisible by 7. By the assumption there is an integer l such that $k+5d=7l$ hence $k=7l-5d$. Substituting k, we see that:

$$n = 10k + d = 10(7l - 5d) + d = 70l - 49d = 7(10l - 7d)$$

Since $10l-7d$ is an integer, we conclude that n is divisible by 7.

(2) $\underline{k+d\cdot 5 \text{ is divisible by } 7 \Leftarrow n \text{ is divisible by } 7}$: Suppose that n is divisible by 6. We want to prove that $k+d\cdot 5$ is divisible by 7. By the assumption, there is an integer l such that $n=7l$. Substituting n we get $10k+d=7l$ hence $d=7l-10k$. Substituting d we get,

$$k + d5 = k + (7l - 10k)5 = 35l - 49k = 7(5l - 7k)$$

since $5l-7k$ is an integer, $k+5d$ is divisible by 7.

□

Let us apply the previous claim to a specific case: is $n=2450$ divisible by 7? for $k=245,\ d=0$ we have that $n=10k+d$. By the claim, it suffices to see if $k+5d=245$ is divisible by 7. Indeed $245=7\cdot 35$ is divisible by 7 hence 2450 is divisible by 7.

3.4. **Proof by contradiction.** Proof by contradiction is perhaps the most common proof method among the logical equivalences. The idea is to prove that the falsity of Q leads to an absurd (a contradiction). This implies the falsity of the falsity of Q which is logically equivalent to Q. Formally, if $\alpha \equiv F$ is any contradiction (for example α is $P\wedge \sim P$ is usually used) then we can use the following logical equivalence:

Problem 1. *$Q \equiv (\sim Q) \Rightarrow \alpha$.*

Hence a proof by contradiction to the statement Q has the following structure:

(1) Assume toward a contradiction that $\sim Q$.
(2) Deduce a contradiction.

There are no rules for when should one use a proof by contradiction, instead, one should always formulate the negation of the statement he wishes to prove and try to reach a contradiction. Before the examples, let us recall the lows of negation of the different logical connectives and quantifiers.

(1) $\sim(\sim Q)) \equiv Q$.
(2) $\sim(P\wedge Q) \equiv (\sim P)\vee(\sim Q)$.
(3) $\sim(P\vee Q) \equiv (\sim P)\wedge(\sim Q)$.
(4) $\sim(P\Rightarrow Q) \equiv P\wedge(\sim Q)$.
(5) $\sim(\forall x(p(x))) \equiv \exists x(\sim p(x))$.
(6) $\sim(\exists x(p(x))) \equiv \forall x(\sim p(x))$.

Problem 2. *Simplify $\sim(P\Leftrightarrow Q)$.*

Example 3.4. (1) Claim: There are no integers n, m such that $12n + 15m = 2$.

Proof. Assume toward a contradiction that there are n, m such that $12n + 15m = 2$. Then $3(4n + 5m) = 2$, and since $4n + 5m$ is an integer, it follows that 3 divides 2 which is a contradiction. □

(2) Claim: If n is divisible by 3 then $n^2 - 1$ is not divisible by 3.

Proof. Suppose toward a contradiction that n is divisible by 3 and also[11] $n^2 - 1$ is divisible by 3. By the assumption, there are integers l, m such that $n = 3l$ and $n^2 - 1 = 3m$. Substituting n, we get

$$3m = n^2 - 1 = (3l)^2 - 1 = 9l^2 - 1$$

hence

$$1 = 9l^2 - 3m = 3(3l^2 - m)$$

Since $3l^2 - m$ is an integer, we conclude that 1 is divisible by 3 which is a contradiction.

□

(3) Claim: Let x, y be real numbers such that $x < 2y$. If $7xy \leq 3x^2 + 2y^2$, then $3x \leq y$.

Proof. Assume toward a contradiction that $3x > y$. By the assumptions of the claim $2y > x$ and therefore

$$3x - y > 0 \text{ and } 2y - x > 0$$

Hence

$$0 < (3x - y)(2y - x) = -2y^2 - 3x^2 + 7xy$$

. It follows that $7xy > 3x^2 + 2y^2$ This is a contradiction to the assumptions of the claim that $7xy \leq 3x^2 + 2y^2$. □

(4) Prove that the lines $y = x^2 + x + 2$ and $y = x - 2$ do not intersect.

Proof. Suppose toward a contradiction that (a, b) is a point of intersection. Then $b = a^2 + a + 2$ and $b = a - 2$. Hence $a - 2 = a^2 + a + 2$. It follows that $a^2 = -4$. However, for any real number r, $r^2 \geq 0$. This is a contradiction. □

The following theorem relies on the fact that every rational number $\frac{a}{b}$ has a reduced form. Namely $\frac{a}{b} = \frac{a'}{b'}$, where a', b' have no common divisors. This is easy to believe, since if a, b would have a common divisor we can just cancel it from the numerator and denominator. We will prove this fact formally by induction in the next chapter.

Theorem 3.5. *$\sqrt{2}$ is an irrational number.*

[11] The claim we are proving is an implication $P \Rightarrow Q$, hence if we assume toward a contradiction that $\sim (P \Rightarrow Q)$, we assume that $P \wedge \sim Q$.

Proof. Suppose toward a contradiction that $\sqrt{2}$ is rational. Then there are coprime integers n, m such that $\sqrt{2} = \frac{m}{n}$. It follows that $2 = \frac{m^2}{n^2}$ and $n^2 2 = m^2$, hence m^2 is even. It follows that m is even (why? prove it!) so there is k such that $m = 2k$ and $n^2 2 = (2k)^2 = 4k^2$. dividing the equation by 2 we have that $n^2 = 2k^2$, and by the same reasoning n should also be even. However, this is a contradiction to the choice of n, m being coprime on one hand and both even on the other hand. □

3.5. **Disproving statements.** Disproving a statement is to prove the negation of the statement.

Example 3.6. (1) To disprove a universal statement we should simply give a *counterexample*. For example, let us disprove the claim:

$$\text{For every integer } n,\ n^3 + 2n + 1 \text{ is even}$$

The witness $n = 2$ satisfy that $2^3 + 2 \cdot 2 + 1 = 13$ is a counterexample for the universal statement and therefore we have disproved it.

(2) Disproving an existential statements requires to prove a universal statement. For example, disprove the following statement:

$$\text{There is a number } x \text{ such that for every natural number } n,\ x > n.$$

4. Proving universal statements

Proving universal statements is not an easy task and requires mathematical matureness. Let us review some of the most common ways. The first, is to go over all the possibilities "one-by-one" and to prove the statement for each individual.

Example 4.1. Claim: For every integer $0 \leq n \leq 2$, $n^2 - n \leq n$.

Proof. We shall go over all possibilities one-by-one [12]:

- If $n = 0$, then $0^2 - 0 = 0 \leq 0$.
- If $n = 1$, then $1^2 - 2 = 0 \leq 1$.
- If $n = 2$, then $2^2 - 2 = 4 - 2 = 2 \leq 2$.

□

This method is quit simple but not very useful as this only applies for universal statement regarding a *small enough* number of individuals to consider. What does it mean small enough? well, this depends. If we were at home with a few hours to waste, then perhaps 100 cases to check would be considered small enough. During the final exams, this would be too much. On the other hand, if we can run a computer program to check all the possibilities then a billion cases is probably doable for modern computers.

[12] Here we declare which is the method we are using to prove the universal statement.

Remark 4.2. The *Four Color Theorem* in is simplest form states that no more then 4 colors are required to color a regional map such that any two adjacent regions have different colors. This was a long standing open problem in graph theory which was resolve in 1976 by Kenneth Appel and Wolfgang Haken from the University of Illinois.

The four color theorem is a theorem of the form "for every regional map...", hence it is a universal statement with potentially infinitely many individual maps to consider. The proof of Appel and Haken, reduced the problem to checking 1,834 maps, then they used a computer to check all the possibilities which took 1200 hours for the computer to check. Eventually, the computer announced that each one of the 1,834 many possibilities can be colored with 4 colors. A sceptical person can argue against this kind of proofs by computers claiming that we can never be sure that the computer did not miss a case.

What should we do then if we have too many cases to go over one-by-one or even infinitely many cases to consider? The most common method is a proof for a "general object". The structure of the proof is to work with a variable x_0 which represent a general/random object, but is considered used as if it was a fixed object. But as a wise uncle once said:

"With great power comes great responsibility"

The status of this variable x_0 is tricky and one should be extra careful with this kind of variable. On one hand, we cannot assume any property of x_0, as it is supposed to range over all the cases, and if we were to make any assumption/restriction on x_0 it might fail to represent all the possibilities. On the other hand, we treat x_0 as if it was a specific object and therefore it can be used in formulas, and in the definition of other objects. Here the choice of words is crucial, to emphasize that x_0 has this special status in the proof we use the dramatic opening line "Let x_0 be...", whenever a mathematician encounter such an opening line, the status of x_0 is as described above. In general, the structure of a proof for a universal statement which uses a general object is:

(1) Declare you general object "Let $x_0/n_0/a_0$... be a (object type)", where the object type is either explicit in the claim or understood from the context of the claim.
(2) Formulate a simplified statement which is what we need to prove about the general variable.
(3) Prove the simplified statement about the general variable according to the logical structure of it.

Example 4.3. Prove the following universal statements:

(1) Claim: $\forall x(x + 1 > 0 \vee x^2 \geq 1)$

Proof. Let x_0 be any number[13]. Our goal is to prove that[14]: $x_0+1 > 0 \vee x_0^2 \geq 1$.

Let us split into cases[15]:

- If $x_0 > -1$, then $x_0+1 > 0$ and in particular $x_0+1 > 0 \vee x_0^2 \geq 1$.
- If $x_0 \leq -1$, then $x_0^2 \geq 1$ and in particular $x_0+1 > 0 \vee x_0^2 \geq 1$.

At any rate, we conclude that $x_0+1 > 0 \vee x_0^2 \geq 1$. □

(2) Claim: $\forall x((\forall y(x \cdot y = 0)) \Rightarrow x = 0)$

Proof. Let x_0 be any number. We want to prove that: $(\forall y(x_0 \cdot y = 0)) \rightarrow x_0 = 0$, Suppose that[16] $\forall y(x_0 \cdot y = 0)$, we want to prove that $x_0 = 0$. In particular, for $y = 1$ we conclude that[17] $x_0 \cdot 1 = 0$ and therefore $x_0 = 0$. □

(3) Claim: $\forall x((\exists y(y + x = y)) \Rightarrow x = 0)$.

Proof. Let x_0 be any number. We want to prove that $(\exists y(y + x_0 = y)) \Rightarrow x_0 = 0$. Suppose that $\exists y(y + x_0 = y)$, we want to show that $x_0 = 0$. Let y_0 be a witness[18], namely $y_0 + x_0 = y_0$. Reduce from both side of the equation y_0, to conclude that $x_0 = 0$. □

[13] This is the declaration of the general variable, it is clear from the context that the claim is about numbers.

[14] This is the second step, where we formulate what there is to prove about the general number x_0.

[15] In the third step we prove the simplified claim according to the its logical structure, it this case it is a $\vee$-statement. It is common to split into cases when we prove $\vee$-statements, this is allowed even when we dill with a general object as long as we cover all the possible cases.

[16] Recall that when we prove an implication we assume that the antecedent holds and we want to prove the consequent.

[17] Note here that we **assume** a universal statement and therefore we have in hand a very powerful assumption, that *for every* y we choose, we know for a fact that $x_0 \cdot y = 0$, so we might as well pick our favorite y, and apply the assumption to it.

[18] Here the antecedent if an *existential statement*, namely we are given that there some y, $x + y = y$. This is a very weak assumption, since this y can be any y and we cannot assume that y is any specific number. But still, this y exists. Therefore y has a similar status to that of a general variable and we use "Let y_0..." to fix an object y_0 which witness the statement without restricting y_0 to be specific.