Notes

These notes show examples of proofs by induction. The proofs should be written formally with each step justified by arguments.

We prove that addition is commutative. The definition of addition is

```
add(n,0) := n for all n                           (1)
add(n,next(m)) = next(add(n,m)) for all n, m.     (2)
```

This defines addition for all n, m by induction on m. Note that here we do not use induction on n. The definitions hold for all n.

We want to prove `add(n,m) = add(m,n)` for all n,m.

To do this, we prove some intermediate statements first.

Claim 1. `add(0,m) = m` for all m.

Prove this by induction on m. `add(0,0) = 0 by (1).` So Claim 1 is true for m = 0. `add(0,next(m)) = next(add(0,m)) by (2).` But `add(0,m) = m` by the induction hypothesis. Therefore `add(0,next(m)) = next(add(0,m)) = next(m)` and Claim 1 is true for next(m) if it is true for m. By induction, Claim 1 is true for all m.

Claim 2. `add(next(n),m) = next(add(n,m)).`

We prove this by induction on m. For m = 0, `add(next(n),0) = next(n)` and `next(n) = next(add(n,0))` by `(1).` Now,

```
add(next(n),next(m)) = next(add(next(n),m)) by (2)
                     = next(next(add(n,m))) by induction hypothesis
                     = next(add(n,next(m))) by (2)
```

This completes the induction step and proves Claim 2.

We can now complete the proof that addition is commutative, that is `add(n,m) = add(m,n)` for all n, m.

Again, the proof is by induction on n for any arbitrary m.

```
add(0,m) = m by Claim 1
         = add(m,0) by (1).

add(next(n),m) = next(add(n,m)) by Claim 2
               = next(add(m,n)) by induction hypothesis
               = add(m,next(n)) by (2)
```

This completes the proof. Notice that in order to prove the main result we had to prove some intermediate steps, also by induction. This occurs very frequently.

As another example, we prove the well-ordering property of numbers. If a set of numbers S is not empty then it contains a number m such that $m \leq x$ for all $x \in S$. The number m is also called a minimum element.

In this case, it is easier to prove a stronger statement than what is required, by induction.

We will show that for any number n, if a set S contains a number $x \leq n$, then S contains a minimum. We prove this by induction on n.

If $n = 0$, the only number x such that $x \leq 0$ is 0 itself, thus S must contain 0. Since $0 \leq x$ for all numbers x, 0 is the required minimum in S.

Assume the statement is true for some number n, and we will show that it holds for $next(n)$. Suppose S has an element $x \leq next(n)$. By the property of $\leq$ relation, (which should be proved separately), either $x \leq n$ or $x = next(n)$. If $x \leq n$, by induction hypothesis, S has a minimum, and we are done. Suppose $x = next(n)$. If $next(n) \leq x$ for all elements $x \in S$, then $next(n)$ is the required minimum. So suppose there is some $y \in S$ such that $next(n) \not\leq y$. Then by the property of $\leq$, we have $y \leq next(n)$. But $y \neq next(n)$ and therefore again by the properties of $\leq$, $y \leq n$. Now, by induction S must contain a minimum. This completes all cases and the proof. Notice that the proof depends on some properties of $\leq$ that need to be proved separately.

Finally, if S is a non-empty set, it contains a number n. Since $n \leq n$, the stronger statement applied to S implies it has a minimum element.

Try to prove the converse, that is assuming the well-ordering property of $\leq$, prove the induction axiom. They are equivalent ways of saying the same thing.

Exercises

1. Prove the properties of add, mult, $\leq$ stated in the slides, and any others that you know.

2. Define the quotient, remainder and square-root operations on numbers. The square-root of a number n is the largest number i such that $i^2 \leq n$.

3. Suppose you want to define the set of integers with their usual meaning. What additional operations would be required and what properties must they satisfy?

4. Let f be a function on numbers such that $f(0)$ is undefined, $f(1) = 1$, $f(i) \leq f(i+1)$ for all $i \geq 1$ and there are exactly $f(j)$ numbers i with the property $f(i) = j$. In other words, j occurs exactly $f(j)$ times in the range of f. Prove that there is exactly one such function and give a way of defining it.

5. Define a function `prime(n)` that returns true iff `n` is a prime number, using recursive definitions. You may need to define other functions for this.