Definition for reference:

```
  let rec plus a b =
    match b with
    | Zero -> a
    | S c -> plus (S a) c
```

Here is a useful lemma that is used throughout:

```
plus (S a) b = S (plus a b)
```

proof by induction on b. Case b = Zero:

```
  plus (S a) b
= {case}
  plus (S a) Zero
= {def}
  match Zero with
    | Zero -> S a
    | S c -> plus (S (S a)) c
= {match}
  S a
= {match}
  S ()
= {match}
  S (match Zero with
    | Zero -> a
    | S c -> plus (S a) c)
= {def}
  S (plus a Zero)
= {case}
  S (plus a b)
```

Case b = S c, IH: plus (S a) c = S (plus a c)

```
  plus (S a) b
= {case}
  plus (S a) (S c)
= {def}
  match S c with
    | Zero -> S a
    | S c -> plus (S (S a)) c
= {match}
  plus (S (S a)) c
= {IH}
  S (plus (S a) c)
= {match}
= {def}
  S (plus a b)
```

Thus we have proved that 'plus (S a) b = S (plus a b)'.
I'll call this lemma 'S and plus commute in their first argument'.

P1) Prove plus Zero b = b

This proof would be trivial if we used P2, but we cannot prove P2 without P1.
Here's a proof by induction on b: Case b = Zero:

```
  plus Zero b
= {case}
  plus Zero Zero
= {def}
  match Zero with
    | Zero -> Zero
    | S c -> plus (S Zero) c
= {match}
  Zero
= {case}
  b
```

Case b = S d, with IH: plus Zero d = d

```
  plus Zero b
= {case}
  plus Zero (S d)
= {def}
  match S d with
    | Zero -> Zero
    | S c -> plus (S Zero) c
= {match}
  plus (S Zero) d
= {lemma 'S and plus commute in their first argument'}
  S (plus Zero d)
= {IH}
  S d
= {case}
  b
```

Thus we have proved that 'plus Zero b = b'.
I'll call this lemma 'P1'.

P2) Prove plus a b = plus b a

We'll prove this by induction on b

Base case: b = Zero

```
  plus a b
= {case}
  plus a Zero
```

```
= {def}
  match Zero with
    | Zero -> a
    | S c -> plus (S a) c
= {match}
  a
= {lemma 'P1'}
  plus Zero a
= {case}
  plus b a
```

Inductive case: b = S c, with IH: plus a c = plus c a

```
  plus a b
= {case}
  plus a (S c)
= {def}
  match S c with
   | Zero -> a
   | S c -> plus (S a) c
= {match}
  plus (S a) c
= {lemma 'S and plus commute in their first argument'}
  S (plus a c)
= {IH}
  S (plus c a)
= {lemma 'S and plus commute in their first argument'}
  plus (S c) a
= {case}
  plus b a
```

Thus we have proved that 'plus a b = plus b a'.
I'll call this lemma 'P2'.

P3) Prove plus a (plus b c) = plus (plus a b) c

With P2 under our belt, we can move arguments to plus around all we like, so it really doesn't matter on what argument we do induction. However, I can use lemma 'S and plus commute in their first argument', since that avoids me having to use definitions (which is two steps rather than one).
For that reason I give a proof by induction on a here.

Here's a proof by induction on a: case a = Zero

```
  plus a (plus b c)
= {case}
  plus Zero (plus b c)
= {lemma 'P2'}
  plus (plus b c) Zero
= {lemma 'P1'}
  plus b c
```

```
= {lemma 'P1'}
  plus (plus b Zero) c
= {lemma 'P2'}
  plus (plus Zero b) c
= {case}
  plus (plus a b) c

case a = S d, IH: plus d (plus b c) = plus (plus d b) c
  plus a (plus b c)
= {case}
  plus (S d) (plus b c)
= {lemma 'S and plus commute in their first argument'}
  S (plus d (plus b c))
= {IH}
  S (plus (plus d b) c)
= {lemma 'S and plus commute in their first argument'}
  plus (S (plus d b)) c
= {lemma 'S and plus commute in their first argument'}
  plus (plus (S d) b) c
= {case}
  plus (plus a b) c
```

Thus we have proved that 'plus a (plus b c) = plus (plus a b) c' by induction.