In this course, you will be required to prove statements. This short note is meant to lay some basic foundation for that task. Often we have a pair of proposition P,Q and are asked to decide if the statement If P, then Q is true. We have three general approaches to verifying the proposition if P, then Q.

- *Direct.* We assume that P is true and deduce that Q is true using known results.
- *Contrapositive.* We assume not Q and deduce not P using known results.
- *Contradiction.* We assume P and not Q and deduce a contradiction of a known result.

To see how these work, it is best to select an example. The following example was given in class.

Proposition 1.1 0 is unique.

First, we must understand the statement of the proposition. What does it mean for 0 to be unique? Recall that (A2) asserted that 0 has a special property. Namely, for all $b \in F$, we have

$$b + 0 = b.$$

Technically, (A2) asserted that there exists an element 0 that has this property. It could very well be that other elements of F also have this property. To say that 0 is unique is then the following statement:

If $a \in F$ is such that for all $b \in F$, we have

$$b + a = b,$$

then $a = 0$.

Here the proposition P is the statement: for all $b \in F$, $b + a = b$. The proposition Q is the statement: $a = 0$. Now that we understand the statement of Proposition 1.1., we can now try to prove it using the above methods.

Direct Proof. In the direct proof, we assume that the proposition P is true and deduce that the proposition Q is true. Therefore, we are given that for all $b \in F$, we have $b + a = b$ and we need to show that $a = 0$. Currently, one the axioms/properties (A1)-(A4), (M1)-(M4), (EQ1)-(EQ3), (D), and (Z) are available. To begin, we know the equality

$$b + a = b \tag{1}$$

holds for all $b \in F$. In particular, if we take $b = 0$, (1) yields the equality

$$0 + a = 0.$$

By (A2) and (A4), we know that the equation

$$0 + b = b$$

holds for all $b \in F$. In particular, this equation holds for $b = a$ and so we see that

$$0 + a = a.$$

Finally, since $0 = 0 + a$ and $0 + a = a$, by (EQ3), we see that $a = 0$. Our goal was to show that $a = 0$ and so our proof of Proposition 1.1 is complete.

Contrapositive Proof. In the contrapositive proof, we assume not Q is true and deduce that not P is true. The proposition not Q is $a \neq 0$ and the proposition not P is the statement: there exists a $b \in F$ such that

$$b + a \neq b.$$

So our goal is to find a $b \in F$ for which (1) does not hold.

Remark. The negation of P is slightly subtle but you should be able to see this using common sense and your understanding of language. Recall P is the statement: for all $b \in F$, we have $b + a = b$. In order for this statement to be true, it has to hold for all $b \in F$. In particular, it is false if there exists a $b \in F$ for which $b + a \neq b$.

Returning to our proof, we seek a $b \in F$ for which $b + a \neq b$. Aside from the axioms, we are assuming $a \neq 0$. We know by (A2) that

$$a + 0 = a.$$

By (A4), this becomes

$$0 + a = a.$$

In particular, if we set $b = 0$ in (1), we see that

$$0 + a = a \neq 0.$$

Thus not P holds. As this was our goal, our proof is complete.

Contradiction Proof. In the contradiction proof, we assume that P and not Q hold and then derive a contradiction of a known result. At present, we only know the basic axioms, so we will need to contradict one of these.

Remark. Contrapositive asserts that the valid of if P, then Q is equivalent to the validity of if not Q, then not P. If we apply contradiction to this we see that we assume not Q and P as before. In particular, proof by contradiction on the statement if P, then Q and is identical to proof by contradiction on the contrapositive statement if not Q, then not P.

In the proof via contradiction, I will assume the following fact left as an exercise:

Exercise. If $a \in F$ and $b = c$, then

$$a \cdot b = a \cdot c$$

and

$$a + b = a + c.$$

Returning to our proof, we are given that

$$b + a = b$$

for all $b \in F$ and that $a \neq 0$. As $a \neq 0$, by (M3), there exists $a^{-1} \in F$ such that

$$a \cdot a^{-1} = 1.$$

Thus

$$a^{-1} \cdot (b + a) = a^{-1} \cdot b$$

by the exercise. Using (D), (M4), (M3), and (M2), this becomes

$$a^{-1} \cdot b + 1 = a^{-1} \cdot b.$$

Adding $-(a^{-1} \cdot b)$ to both side via the exercise and using (A3), we have

$$1 = -(a^{-1} \cdot b) + a^{-1} \cdot b + 1 = -(a^{-1} \cdot b) + a^{-1} \cdot b = 0.$$

Thus $1 = 0$ and we derive a contradiction of (Z). Having derived a contradiction of a known result, our proof is complete.