Three Ways to Prove "*If A, then B*."

A statement of the form "*If A, then B*" asserts that if A is true, then B must be true also. If the statement "*If A, then B*" is true, you can regard it as a promise that whenever the A is true, then B is true also.

Most theorems can be stated in the form "*If A, then B*." Even if they are not written in this form, they can be put into this form. For example, the statements

"Every group with 4 elements is abelian." and "A group is abelian if it has 4 elements."

can both be restated as: "**If** a group G has 4 elements, **then** G is abelian."

There are three ways to prove a statement of form "*If A, then B*." They are called **direct proof**, **contrapositive proof** and **proof by contradiction.**

DIRECT PROOF. To prove that the statement "*If A, then B*" is true by means of direct proof, begin by assuming A is true and use this information to deduce that B is true. Here is a template. What comes between the first and last line of course depends on what A and B are.

Theorem: If A then B.
Proof. Suppose A is true.
$\vdots$
Therefore B is true.

CONTRAPOSITIVE PROOF. The idea is that if the statement "*If A, then B*" is really true, then it's impossible for A to be true while B is false. Thus, we can prove the statement "*If A, then B*" is true by showing that if B is false, then A is false too. Here is a template.

Theorem: If A then B.
Proof. Suppose B is false.
$\vdots$
Therefore A is false.

PROOF BY CONTRADICTION. Again, if the statement "*If A, then B*" is really true, then it's impossible for A to be true while B is false. In other words, it is a contradiction to assume A is true and B is false. Of course, since you have not proved "*If A, then B*" is a true statement, this contradiction is not at all obvious. In the technique of **proof by contradiction**, you begin by assuming A is true and B is false, and use this to deduce and *obvious* contradiction of from "C is true and C is false." Here's a template.

Theorem: If A then B.
Proof. Suppose A is true and B is false.
$\vdots$
Therefore C is true and C is false.

Examples of the Three Proof Techniques.

Here is a homework problem proved three ways — by means of direct proof, contrapositive proof, and proof by contradiction.

Section 4, Exercise 34: Let G be a group with a finite number of elements. Show that for any $a \in G$ there is an $n \in \mathbb{Z}^+$ for which $a^n = e$.

DIRECT PROOF

Theorem: If a is an element of a finite group G, then there is an $n \in \mathbb{Z}^+$ for which $a^n = e$.
Proof. Suppose a is an element of a finite group G. Say G has m elements. Consider the following list of elements of G: $a^1, a^2, a^3, a^4, \cdots a^{m+1}$. Since this list has $m+1$ items in it, and G contains only m elements, it follows that the list has at least two items that are equal. Thus $a^j = a^k$ for some integers j and k with $1 \leq j < k \leq m+1$. Then

$$\begin{aligned} a^j &= a^k \\ a^j(a^{-1})^j &= a^k(a^{-1})^j \\ a^j(a^j)^{-1} &= a^k a^{-j} \\ e &= a^{k-j} \end{aligned}$$

Setting $n = k - j$, it follows that $a^n = e$. ■

CONTRAPOSITIVE PROOF

Theorem: If a is an element of a finite group G, then there is an $n \in \mathbb{Z}^+$ for which $a^n = e$.
Proof. (Contrapositive) Suppose there is *no* $n \in \mathbb{Z}^+$ for which $a^n = e$. Consider the infinite list of group elements $a^1, a^2, a^3, a^4, a^5 \cdots$. No two elements of this list are equal, for if they were, there would be positive integers j and k with $1 \leq j < k$ and $a^j = a^k$, and multiplying both sides on the right by a^{-j} would give $e = a^{k-j}$, which we are assuming cannot happen. Thus, since no two elements on the infinite list are equal, they are all different elements of G. Thus G is infinite, so it is not finite. ■

PROOF BY CONTRADICTION

Theorem: If a is an element of a finite group G, then there is an $n \in \mathbb{Z}^+$ for which $a^n = e$.
Proof. (Contradiction) Suppose G is finite and there is *no* $n \in \mathbb{Z}^+$ for which $a^n = e$. Consider the infinite list of group elements $a^1, a^2, a^3, a^4, a^5 \cdots$. No two elements of this list are equal, for if they were, there would be positive integers j and k with $1 \leq j < k$ and $a^j = a^k$, and multiplying both sides on the right by a^{-j} would give $e = a^{k-j}$, which we are assuming cannot happen. Thus, since no two elements on the infinite list are equal, they are all different elements of G. It follows that G is infinite. But it is also finite, as stated in the first sentence of the proof. Thus G is finite and G is infinite, which is a contradiction. ■

Notice that in the proof by contradiction, to show G is infinite we ended up using much of the same reasoning used in the contrapositive proof. Thus, in this case, the contrapositive approach would be simpler. If possible you should always go with the simplest proof technique. Very often, one approach will seem impossible but another will be quite easy. If you get stuck, try a different approach.

If-And-Only-If Proofs

The theorems that can't be stated in the form of "*If A, then B*" are of the form "*A* if and only if *B*."
Such a statement is asserting two things, namely "*A if B*" **and** "*A only if B*."
Now, "*A if B*" means "*If B then A*," and "*A only if B*." means "*If A then B*."
Thus "*A* if and only if *B*." means "*If A then B*," **and** "*If B then A*."

So to prove a statement of the form "*A* if and only if *B*," you really have to do two proofs. Here is a template.

> Theorem: *A* if and only if *B*.
> Proof:
>
> Suppose *A* is true.
> ⋮
> Therefore *B* is true.
>
> Suppose *B* is true.
> ⋮
> Therefore *A* is true.

Notice that in each of the two parts, you are really proving a statement of the form "*If X then Y*," so for each part you can use direct proof, contrapositive proof, or proof by contradiction. Use whatever seems easiest.