Notes on Proofs

Mathematical symbols used in proofs: In the following p and q represent statements that must be either true or false.

1. $p \implies q$ means 'p implies q' or 'if p, then q.'
2. $p \impliedby q$ means 'p is implied by q' or 'p only if q' or 'if q then p.'
3. $p \iff q$ means 'p if and only if q,' i.e. 'if p then q' and 'if q then p.'
4. $\exists$ means 'there exists' or 'there is a.'
5. $\forall$ means 'for all' or 'for every.'
6. $\in$ means 'is a member of'
7. $\subset$ means 'is a subset of' *(See Definition 1.3)*
8. $\supset$ means 'is a superset of.' (A is a superset of $B \iff B$ is a subset of A.)

Remark 1. *These symbols are appropriate for use on the board but should be used sparingly and very carefully in formal write ups. More explanation of this follows in the discussion below.*

Key Points

1. You will rarely be able to write down a completely correct proof, with good mathematical style, on your first attempt. Usually you need to work out how the proof will go and then work out the best way to write it down. Proofs by induction (Sheet 0) are unusual in that there is a basic format that you follow.
2. Proofs must be **written entirely in complete sentences** and should not just consist of calculations (see Example 3). Sentences should not start with symbols.
3. Another student should be able to read your proof and understand it easily. This should be kept in mind especially when writing your journal. You should think of your journal as a textbook that you are writing.
4. You have to be very careful about your use of logical connectives.

   For example, if you want to prove

   $$x^2 + 2xy + y^2 \geq 0, \tag{1}$$

   it is not correct to write

$$\begin{aligned} x^2 + 2xy + y^2 &\geq 0 \\ (x+y)^2 &\geq 0 \\ \text{True} &\quad . \end{aligned}$$

It is clear from this kind of work that you know what you are doing, however it is not a *proof*. You can easily turn it into a proof however. One temptation is to add $\iff$ symbols where appropriate. ($\iff$ means 'if and only if,' so can be used to join two equivalent statements.) For example,

$$\begin{aligned} x^2 + 2xy + y^2 &\geq 0 \\ \iff (x+y)^2 &\geq 0, \end{aligned}$$

which is true.

However, although this is correct, it is not good mathematical style. It is much preferable to write something like:

Since the square of any real number is non-negative, $(x+y)^2 \geq 0$, and so $x^2+2xy+y^2 = (x+y)^2 \geq 0$.

In general, it is much better to use 'so' or 'therefore' than the implication symbol $\implies$, which can be ambiguous. Does "so $a = 0 \implies b = 0$" mean "so $a = 0$ and therefore $b = 0$," or "so if $a = 0$ then $b = 0$"? It is much better to avoid the ambiguity by using the words rather than the symbol.

5. "If p then q" is not the same is "if q then p," so you must be sure that you are writing your proof in the correct direction.

   For example

$$\begin{aligned} x^2 + 2xy + y^2 &\geq 0 \\ \implies (x+y)^2 &\geq 0 \end{aligned}$$

   is true but will not help for the proof of (1) as the implication is in the wrong direction. The fact that (1) implies something true does not mean that (1) must itself be true. It is easy to come up with examples of false statements that imply true ones. For example:

$$\begin{aligned} 0 &= 1 \\ \implies 0 \cdot 1 &= 1 \cdot 0 \\ \implies 0 &= 0. \end{aligned}$$

6. The equals sign, =, should only be used when 2 quantities are equal and not as a logical connective. For example you should not write

$$\begin{aligned} x^2 + 2xy + y^2 &\geq 0 \\ = (x+y)^2 &\geq 0; \end{aligned}$$

this makes no sense grammatically. (Try reading it aloud.)

7. Make sure that every variable you use has been introduced with a quantifier such as "for every", "there exists", or 'for some". You should generally state what set the variables lie in, unless this is completely obvious from the context. It is usually better to write out quantifiers in words although on the board you may use the symbols above (4 and 5) for brevity.

8. Placement of quantifiers is crucial. Consider the following examples:

   There is a student in this class who is sick every day.

   or

   Every day there is a student in this class who is sick.

   A more mathematical example:

   For every natural number n there is natural number m such that $n < m$.

   or

   There is a natural number m such that $n < m$ for every natural number n.

Do you see the difference?

A couple of examples of proofs

For the sake of the following discussion we will assume that we know the following definition.

Definition 2. a) A positive integer n is even if it can be written as $n = 2k$ for some positive integer k.

b) A positive integer n is odd if it can be written as $n = 2k + 1$ for some positive integer k.

Example 3. If $n \in \mathbb{N}$ and n is odd then n^2 is also odd.

Proof. (first 'proof')
$n = 2k + 1, n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$ □

Proof. (second proof) Since n is odd, we can write n as $n = 2k + 1$ for some $k \in \mathbb{N}$. Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $n^2 = 2m + 1$ for some $m \in \mathbb{N}$, n^2 is odd. □

The first 'proof' is not really a proof. It is simply the calculation that is needed for the proof. In your journals, you need to be writing your proofs more like the second proof. You needn't write as much when presenting at the board, but you do need to write enough that your audience is able to follow your argument. **It usually will not be sufficient to copy down what is written on the board.**

Types of Proof

To *disprove* a statement we need only come up with a *counterexample*, i.e. an example that shows that the statement cannot hold. To *prove* a statement, there are three possible strategies, besides mathematical induction. We suppose that we want to prove a statement of the form **'if** p **then** q**'** (i.e. p is the assumption, q is the conclusion):

1. Direct Proof - we start by assuming that p is true and argue directly, using the assumption, p, and any other statement that has been previously established, until we arrive at statement q.

2. Proof by Contradiction - we start by assuming that the implication is false and argue until we arrive at a false statement, at which point we have a contradiction to the assumption that our implication was false, which proves that the implication is in fact true. For 'if p then q' to be false it must be that p holds but q does not, so a proof by contradiction always starts by assuming that p holds and q does not.

3. Proof by Contraposition - 'if p then q ' is logically equivalent to 'if not q then not p.' A proof by contraposition is a direct proof of the implication 'if not q then not p.'

Some results can be proved by any one of these methods while others may only readily be proven by one of them. Figuring out which proof technique is the best for the problem at hand takes practice. As an example we consider the following lemma.

Lemma 4. *Let x, y be positive integers. Then xy is odd if, and only if, x and y are both odd.*

Proof. Note that since this is an 'if and only if' statement we must prove two implications, namely

(i) If xy is odd, then x and y are both odd, and

(ii) If x and y are both odd, then xy is odd.

(For (i) it is hard to see how to proceed with a direct proof since we need to somehow separate out the x and y, so it is more natural to try one of the other approaches. In this case, the argument is similar whether we use proof by contradiction or contrapositve. We will give one here - you should try the other.)

We will prove (i) by contradiction. So we suppose that xy is odd but (at least) one of x or y is not odd. It follows that (at least) one of x and y must be even. If x is even then

$x = 2k$ for some positive integer k and then $xy = 2(ky)$ which is even also. Similarly, if y is even then xy is even. This contradicts our assumption that xy is odd. Hence x and y must both be odd.

(For (ii) a direct proof is straightforward.)

To prove (ii) we suppose that x and y are both odd. So, by the definition above, there are positive integers k and l with $x = 2k + 1$ and $y = 2l + 1$. Then $xy = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$, which is of the form $2m + 1$ for $m = 2kl + k + l$, hence is odd.

□

Corollary 5. *Let x, y be positive integers. Then xy is even if, and only if, at least one of x and y is even.*

Exercise 6. Prove Corollary 5.

Theorem 7. *There are no positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 2n^2$.*

Proof. We first want to rephrase the theorem as an 'if p then q ' implication. So we want to prove that 'if $m, n \in \mathbb{N}$ have no common factors (other than 1), then $m^2 \neq 2n^2$. *(It seems very hard to know how to approach this either directly or by the contrapositive but proof by contradiction looks more approachable).*

We assume, for the sake of contradiction, that $m, n \in \mathbb{N}$ have no common factors (other than 1) and $m^2 = 2n^2$. Since m^2 is even, we know from Corollary 5 that m must be even. Then $m = 2k$, for some $k \in \mathbb{N}$ and $m^2 = 4k^2 = 2n^2$, so $n^2 = 2k^2$. But then n^2 is even, and from Corollary 5 it follows that n is even. But if m and n are both even then we have a contradiction since we assumed that they have no common factors (other than 1).

□

Exercise 8. a) Are there positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 3n^2$? Either give an example or prove that no example is possible.

b) Are then positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 6n^2$? Either give an example or prove that no example is possible.

c) Are then positive integers m, n such that m and n have no common factors (other than 1) and $m^2 = 4n^2$? Either give an example or prove that no example is possible.

Remark 9. *Note that Theorem 7 tells us that there is no rational whose square is equal to 2, i.e. that $\sqrt{2}$ is irrational. However at this point in the course we have yet to meet rationals and irrationals.*

We finish with some examples of proofs that involve sets. This section should be read *after you have seen Script 1, Theorem 1.7.*

Example 10. Let A and B be two sets. If $A \cup B = A \cap B$ then $A = B$.

Proof. When giving a direct proof that 2 sets are equal Theorem 1.7a) is usually invoked. We suppose that $A \cup B = A \cap B$. We first note that A and B can be interchanged in Theorem 1.7. Suppose that $x \in A$. Then, by Theorem 1.7b) , $x \in A \cup B$ and so, since $A \cup B = A \cap B$, by Theorem 1.7c), $x \in B$. Hence every element in A is also in B and so $A \subset B$. A similar argument shows that $B \subset A$ and so $A = B$ (by Theorem 1.7a)). □

This result could also be proved by the contrapositive or by contradiction. We give an alternative proof by contrapositive.

Proof. We want to show that if $A \neq B$, then $A \cup B \neq A \cap B$. Well, if $A \neq B$, then by Definition 1.2, either there is some $a \in A$ such that $a \notin B$, or there is some $b \in B$ such that $b \notin A$. We suppose that $a \in A, a \notin B$. (The other case is similar.) Then $a \in A \cup B$, by Theorem 1.7b) but $a \notin A \cap B$, by definition of intersection. So $A \cup B \neq A \cap B$.

□

Exercise 11. Use Theorem 1.7 to prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Exercise 12. (See Definition 1.11) Let A, B be subsets of a set X. Show that

a) if $A \subset B$ then $X \setminus B \subset X \setminus A$.

b) $X \setminus (X \setminus A) = A$.