The language of mathematical proofs can sometimes be confusing, since some words and phrases have peculiar meanings different from their meanings in ordinary English. Here is a list of some phrases and the meanings they bear in proofs.

**Assume.** See “suppose.” This is also often used with the phrase without loss of generality.

**By definition.** This phrase is used to explain that a step in your proof is justified by the very definition of one of the words. (See “definition.”) Every time you use this phrase, you should actually be thinking about a specific definition.

**By hypothesis.** This phrase is used to indicate that something in your proof is true because it’s one of the hypotheses. (See “hypothesis.”) Every time you use this phrase, you must be referring to something actually in the statement of the problem.

**By the inductive hypothesis.** If you are doing a proof by induction, you first prove that the statement is true for a “base case” of \( n = 1 \), and then you prove that if it is true for \( n - 1 \), it is also true for \( n \). The “inductive hypothesis” is the assumption “Suppose it is true for \( n - 1 \).”

**By symmetry.** Sometimes you need to prove two statements that are exactly identical, except that two variables (say, \( x \) and \( y \)) change places. If the hypotheses about \( x \) and \( y \) are exactly the same, then once you’ve proved the first statement, you could simply rewrite exactly the same proof, just swapping \( x \) and \( y \), to prove the second statement. You can save time and ink by proving the first statement and then saying the second statement holds “by symmetry.”

Note that saying “by symmetry” is not the same as saying without loss of generality.

**Cases.** One helpful technique is a proof by cases. For example, suppose you want to prove that \( n^2 - n \) is even for all integers \( n \).

<table>
<thead>
<tr>
<th>Claim:</th>
<th>Let ( n \in \mathbb{Z} ). Then ( n^2 - n ) is even.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof:</td>
<td>We factor ( n^2 - n = n(n - 1) ).</td>
</tr>
<tr>
<td>Case I: ( n ) is even.</td>
<td>Then ( 2 \mid n ), so ( 2 \mid n(n - 1) ); thus ( n^2 - n ) is even.</td>
</tr>
<tr>
<td>Case II: ( n ) is odd.</td>
<td>Then ( n - 1 ) is even, so ( 2 \mid (n - 1) ); thus ( n^2 - n ) is again even.</td>
</tr>
</tbody>
</table>

Thus in either case, \( n^2 - n \) is even. □

In this proof, we split up into cases that cover all the alternatives: either Case I or Case II must hold. Then we complete the proof in each case, showing that no matter what, the claim holds.

Splitting a proof into cases is often a very useful technique; nevertheless, a proof without cases (if one exists) is often prettier.
Claim. The word “claim” usually means the main statement you are trying to prove, but it can also refer to some useful fact that will help you complete your proof, but which itself needs first to be justified with its own mini-proof. For example, maybe you have some subset $H$ of a group $G$, and in order to complete your proof you need to know that $H$ is a subgroup of $G$. The way to do this is simply to embed the claim and its proof within your main proof, like this:

| : Let $H = \{ x \in G : o(x) \neq 0 \}$.
| **Claim:** $H$ is a subgroup of $G$. (1)
| **Proof of Claim:** ... [proving the claim] ... Thus $H$ is a subgroup of $G$. //// (2)
| So now consider the subgroup $H$’s index $[G : H]$. (3)

Note how this sample proof (1) makes its claim, then (2) proves the claim, and finally (3) returns to the “main proof” now knowing that the claim is true. Be sure to start a new paragraph or otherwise make it clear to your reader where the proof-of-claim ends and the regular proof resumes. If the proof of a claim is especially long, it can be wise to separate it as a separate lemma.

Clearly. This is a very, very dangerous word. Writers are tempted to use this word to cover up their inability to give a real proof. If what you’re saying is so clear, why would you have to tell the reader it is clear? On the other hand, if what you’re saying is not obviously true, then inserting the word “clearly” won’t magically make it obvious. Avoid words like “clearly,” “obviously,” and “of course.”

Conclusion. The conclusion is what you are trying to prove, as opposed to the hypotheses, which are what you use to prove it.

Contradiction. One of the most powerful tools for proving statements is proof by contradiction. You suppose the claim is false, and you derive a contradiction, such as that $1 = 0$ or that the same statement is both true and false. Since that is impossible, you must have been wrong when you supposed the claim was false; hence the claim is true! When using this technique, whenever you reach your contradiction, be sure to say exactly what supposition is thereby proved false.

Do not confuse this with the contrapositive of a statement.

Contrapositive. Recall from your study of logic that every statement “If $P$, then $Q$” has a contrapositive statement “If not $Q$, then not $P$” which is logically equivalent to the original statement. Sometimes proving the contrapositive of a statement is much easier than proving the original statement. For example, consider the statement

| **Claim:** Suppose $G$ is a group and $7 \nmid |G|$. Then $G$ has no element of order 7.
The hypothesis doesn’t give you much to work with—a number not divisible by seven—and you’re asked to prove a negative, which is a hard task. Instead, let’s prove the contrapositive.

**Proof:** We shall prove the contrapositive: if \( G \) has an element of order 7, then \( 7 \mid |G| \).

Let \( x \in G \) have order 7. Then...

Note how in this claim, the contrapositive gives us an actual element of \( G \) to start with, and our goal is to prove a positive statement (that \( 7 \mid |G| \)).

If you choose to prove the contrapositive of the original claim, *always write down the contrapositive in full* so you’re clear on what to prove.

Do not confuse the contrapositive with proof by *contradiction*.

**Definition.** In normal languages like English and German, a dictionary definition is just a guide to help you understand how real people actually use words. A mathematical definition is completely different! A mathematical definition takes a word like “eigenvector” which beforehand had no meaning, or a word like “group” that had a commonplace nonmathematical meaning, or a word like “dimension” that had a vague, intuitive meaning; it erases any existing meaning; and it gives the word a precise, exact mathematical formulation in terms of logic. Henceforth in the book, or journal article, or problem, the word means exactly what the definition said, no more and no less.

In particular, you should note that a theorem *about* a concept, or critical facts *about* a concept, or even an if-and-only-if characterization of a concept, is not the same as the definition of the concept.

**Distinct.** Synonym for “different.” If I say “Let \( p \) and \( q \) be prime numbers,” I am allowing the possibility that \( p = q \). If I say “Let \( p \) and \( q \) be distinct prime numbers,” I am explicitly stating that \( p \neq q \).

**Hypothesis.** Every statement in mathematics is ultimately of the form “If...then...” *If* certain hypotheses are true, *then* a conclusion follows. Your homework and test problems take this form too: you assume certain hypotheses and need to prove a conclusion. Be sure to differentiate the hypotheses (what you simply assume is true) from the conclusion (which you need to prove).

**iff.** Short for “if and only if,” and sometimes written symbolically as “\( \iff \)”. The statement “\( P \iff Q \)” means that both \( P \Rightarrow Q \) and \( Q \Rightarrow P \). In other words, \( P \) and \( Q \) are logically equivalent.

**In particular.** The phrase “in particular” is used when you’ve just proved a very broad statement, and now you want to focus your attention on a specific instance.

**Lemma.** A lemma is like a baby theorem that is useful in proving other theorems. Some lemmas are only used to prove one theorem, whereas others can be as famous and widely used as theorems themselves.
Let. When we say something like “Let \( x \in G \),” two things happen. First, we get to use the new symbol \( x \) in our equations and reasoning. But secondly, the new symbol is now tied down to mean one specific thing, a certain element of \( G \); we no longer have any control over which element of \( G \) it is, or any special properties we wish it had. We know absolutely nothing about \( x \) except what we said in the “Let”-statement, namely that \( x \in G \).

This limitation is also the power of the “Let”-statement: because of its very generality, anything we prove about our \( x \) will also be true of every element of \( G \).

Some sets are defined in such a way that a generic element has a particular form. For example, suppose \( \theta : S \to T \) is a function and \( A \subseteq S \). If we want to prove something about every element of \( \theta(A) \), one way would be to write

\[
\text{Let } b \in \theta(A). \text{ By definition of } \theta(A), \text{ there exists some } a \in A \text{ such that } b = \theta(a) \ldots
\]

and then go on to prove something about \( \theta(a) \). This is a little long-winded, and it would be fair to say either

\[
\text{Let } a \in A. \text{ Then } \theta(a) \ldots \quad \text{or} \quad \text{Let } \theta(a) \in \theta(A).
\]

as shorthand for all this.

Obviously. See “clearly.”

Of course. See “clearly.”

QED. You should always put a symbol at the end of your proof to let the reader know you’re done. Classic end-of-proof symbols include “QED” (short for quod erat demonstrandum, “which was to be shown”), \( \square \), \( \blacksquare \), and \( \nolimits \langle \frac{\triangledown}{\triangledown}\rangle \), but you can also invent your own.

Suppose. The word “suppose” has two subtly different uses. (a) In the theorem statement or at the beginning of your proof, it is used to state the hypotheses. (b) In course of the proof, you can use “suppose” to set up a subproof: “if such-and-such is true, then so-and-so would follow.” This is useful especially for proof by contradiction or proof by cases.

We. If you need or want to use the first person in a proof, it is traditional in mathematics to say “we” instead of “I.” The idea is that you and your reader are looking at the subject together.

Well-Defined. This term is easiest to understand through a bad example. Some mathematical objects have multiple names; for example, the names 3/7 and 6/14 and 9/21 all denote the exact same rational number.

Now if I attempt to define a function \( f : \mathbb{Q} \to \mathbb{Z} \) by letting \( f(a/b) = a + b \), then I have a real problem: one the one hand \( f(3/7) = 3 + 7 = 10 \), but \( f(3/7) = f(6/14) = 6 + 14 = 20 \). So which is it? Is \( f(3/7) \) equal to 10 or 20? My “definition” doesn’t work—\( f \) is not a real function—because the “rule” for calculating \( f(3/7) \) totally depends on whether I think of the input as 3/7 or 6/14 or 333/777. A genuine function should give me the same output, no matter which name I use for the same input.
When we define a function, we are giving a rule for turning input into output. A function is **well-defined** if whenever an input has two different names and we apply the rule to the input under the different names, we get the same output.

Just for clarity’s sake, things that are not well-defined are not functions at all! The phrase “well-defined function” is like “actually married”: if you’re not *actually* married, then you’re not married at all, and if it’s not a *well-defined* function, it’s not really a function at all.

In this course, we will often use the term “well-defined” about attempts to define operations. Stay tuned for details!

**Without loss of generality (WLOG).** Sometimes in a proof you have several variables, all playing identical roles in the proof so far, but you know that at least one of them is special in some way. Here’s an example.

<table>
<thead>
<tr>
<th>Problem: Suppose $a, b, c$ are positive integers and $abc$ is even. Prove that $a + b + c \geq 4$.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scratch Work:</strong> Since $abc$ is even, we know that at least one of $a, b,$ and $c$ is even. Shoot... is $a$ even, or $b$ even, or $c$ even? If I knew which one, I could do some more work...</td>
</tr>
</tbody>
</table>

You need to refer to the special one by name, but you don’t know which one it is. One approach would be to break your proof into cases.

<table>
<thead>
<tr>
<th><strong>Proof:</strong> Since $abc$ is even, we know that at least one of $a, b,$ and $c$ is even.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case I:</strong> $a$ is even. Then $a \geq 2$, so $a + b + c \geq 2 + 1 + 1 = 4$.</td>
</tr>
<tr>
<td><strong>Case II:</strong> $b$ is even. Then $b \geq 2$, so $a + b + c \geq 1 + 2 + 1 = 4$.</td>
</tr>
<tr>
<td><strong>Case III:</strong> $c$ is even. Then $c \geq 2$, so $a + b + c \geq 1 + 1 + 2 = 4$.</td>
</tr>
<tr>
<td>Thus in each case, $a + b + c \geq 4$. □</td>
</tr>
</tbody>
</table>

This proof is accurate but wasteful! The proofs in Cases I, II, and III are exactly the same, word for word, except for swapping around the letters $a, b,$ and $c$.

A better solution, the one mathematicians always use, is to pick one of the variables and assume that it is the special one, because if it isn’t, you could just rewrite the proof using a different letter. For this reason you haven’t “lost generality”—you’re not really stuck in just one case, because the other cases are just the same.

<table>
<thead>
<tr>
<th><strong>Proof:</strong> Since $abc$ is even, we know that at least one of $a, b,$ and $c$ is even.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without loss of generality, assume $a$ is even.</td>
</tr>
<tr>
<td>Then $a \geq 2$, so $a + b + c \geq 2 + 1 + 1 = 4$. □</td>
</tr>
</tbody>
</table>

The phrase “without loss of generality” (sometimes abbreviated WLOG) indicates that you are right now choosing which symbol you want to represent the special object. Please note that henceforth in your proof that symbol *is* special. You cannot say WLOG about the same list of variables twice. Think about why this “proof” is wrong:

<table>
<thead>
<tr>
<th><strong>Claim:</strong> Suppose $a, b, c$ are positive integers and $abc$ is even. Then $a + b + c \geq 6$.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proof:</strong> Since $abc$ is even, we know that at least one of $a, b,$ and $c$ is even.</td>
</tr>
<tr>
<td>Without loss of generality, assume $a$ is even, so $a \geq 2$.</td>
</tr>
<tr>
<td>Without loss of generality, assume $b$ is even, so $b \geq 2$.</td>
</tr>
<tr>
<td>Without loss of generality, assume $c$ is even, so $c \geq 2$.</td>
</tr>
<tr>
<td>Then $a + b + c \geq 2 + 2 + 2 = 6$. □</td>
</tr>
</tbody>
</table>
(⇐) and (⇒) These symbols are sometimes used to separate the parts of an if-and-only-if proof. If you’re trying to prove “$P$ if and only if $Q$,” for example, you could write (⇒) in front of the part of your proof which proves that $P \Rightarrow Q$ and (⇐) in front of the part which proves that $Q \Rightarrow P$.

**Useful implication words**

Because proofs consist of logical implication, you may think your proofs sound very repetitious. One way to avoid that is to use a variety of words for implication, such as the following:

- Hence
- Since
- Then
- Therefore
- Thus
- It follows that
- We see that
- Because