

Frequently Used Proof Patterns

Sometimes the word "proof" can be frightening, making one think that one must use a mysterious style that only mathematicians can fathom. Actually "proof" just means giving a logical argument, based on the definitions of the terms involved, as to why a given assertion holds. To make your argument clear and unambiguous, you must be careful to use proper quantifications such as "for all", "for some" or "there exists". You must adhere to the definitions of the terms involved and use sound logical reasoning. You must also choose good notation for your named variables. Here are a few examples of proof patterns that we will be using throughout this course:

Proving a given subset H of a group G is a subgroup of G

The proof pattern for this should start with: "Let x and y be in H ". Of course, whether you call your elements x and y or a and b has little relevance. Once you have made your choice, however, be consistent. You then use the definition of the given set H to establish that $xy \in H$ and $x^{-1} \in H$, where xy and x^{-1} are obtained from the binary operation and existence of inverses in G .

Example: Let G be an abelian group and let $H = \{x \in G : x^2 = e\}$. Prove that H is a subgroup of G .

Proof: Let x and y be in H . The $x^2 = e$ and $y^2 = e$. We must show that $xy \in H$ and $x^{-1} \in H$. By the definition of H we must show that $(xy)^2 = e$ and $x^{-1} = e$. But $(xy)^2 = (xy)(xy) = (xx)(yy) = x^2y^2 = ee = e$. Therefore $xy \in H$. (Note that we used the hypothesis, G is abelian, as well as associativity in the middle step.) Also, since $x^2 = e$, we have that $x = x^{-1}$ in G . Therefore $x = x^{-1} \in H$. Therefore $H \leq G$.

In general, proving that a given subset $H \subseteq G$ is a subgroup of G can also be accomplished by proving the following single assertion:

Let x and y be in H . Then $xy^{-1} \in H$.

Can you see why this is sufficient to establish that $H \leq G$?

Proving a given function $\phi : G \rightarrow G'$ is an isomorphism

In this case, you must show that:

1. ϕ is one-to-one. This means establishing that $\phi(x) = \phi(y)$ implies $x = y$. Alternately, you may also prove the contrapositive: $x \neq y$ implies $\phi(x) \neq \phi(y)$.
2. ϕ is onto. This means establishing that for every $x' \in G'$, there exists an $x \in G$ such that $\phi(x) = x'$.
3. ϕ is "operation preserving", i.e. $\phi(xy) = \phi(x)\phi(y)$. To show this step, you must be careful to note that the binary operations of G and G' may be different, so that xy refers to the operation of G , whereas $\phi(x)\phi(y)$ refers to that of G' .

Example: Let \mathbf{C}^* denote the set of nonzero complex numbers under complex multiplication, and \mathbf{M} the set of all nonzero matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Prove that the function $\phi : \mathbf{C}^* \rightarrow \mathbf{M}$, given by

$\phi(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism.

Proof: The fact that ϕ is one-to-one and onto is left as an easy exercise (don't say that in your homework or tests!!). We will show that ϕ is operation preserving. Let $x = a + ib$ and $y = c + id$ be in \mathbf{C}^* . Then

$$\begin{aligned} \phi(xy) &= \phi((a + ib)(c + id)) \\ &= \phi((ac - bd) + i(ad + bc)) = \begin{pmatrix} a + ib & c + id \\ -(c + id) & a + ib \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \phi(a + ib)\phi(c + id) \\ &= \phi(x)\phi(y). \end{aligned}$$

Exercise: Show that the set \mathbf{M} given above is a subgroup of the group, $GL(2)$ (sometimes called the *general linear group*) of all invertible two by two matrices.