Subgroup theorems

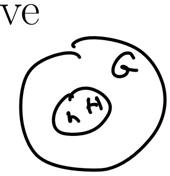
The following theorems simplify the work of verifying that a subset of a group is in fact a subgroup.

Proposition: (First subgroup theorem) Let G be a group and H a subset of G. Then H is a subgroup if and only if:

1. If h_1 and h_2 are in H, then so is $h_1 h_2$. (*this property is called closure*)
2. The identity e of G belongs to H.
3. if $h \in H$, then $h^{-1} \in H$ where h^{-1} is the inverse of h in G.

Proof: Suppose first that H is a subgroup of G. Then the first condition holds by the definition of a subgroup.

For the second point, since H is a group, it must have an identity element; call that element u. Since $u \in H \subset G$, we have $eu = u$. On the other hand, we also have $uu = u$. since $eu = uu$, we have $e\cancel{(uu)}^{-1} = u\cancel{(uu)}^{-1}$ so $e = u$. Therefore $e \in H$.



For the third point, let $h \in H$. Then there is an element $x \in H$ so that $hx = e$ since H is a group. But the equation $hx = e$ also holds in G and by uniqueness of inverses has only one solution: $x = h^{-1}$. Therefore $h^{-1} \in H$.

$x = h^{-1}e = h^{-1}$ since e is the identity in G.

Proof: (continued) Now suppose all three properties hold for H. We know that the binary operation is associative, since it is the same as the operation for G. Points 2 and 3 tell us that H has an identity (e) and every element of H has an inverse h^{-1}. Therefore H is a group, and hence a subgroup of G.

Second subgroup theorem

This theorem simplifies the identification of subgroups even further.

Proposition: Let G be a group, and let H be a subset of G. Then H is a subgroup of G if and only if it is non-empty and, for all $g, h \in H$, we have $gh^{-1} \in H$.

h^{-1} is the inverse of h in G.

Proof: If H is a subgroup, then it must have these properties.

follows from the first subgp theorem.

$g, h \in H$, $h^{-1} \in H$, $gh^{-1} \in H$

So let's assume that H is a subset with these properties and prove that H is a subgroup.

First, H is non-empty, so choose an element $h \in H$.

Then $hh^{-1} = e \in H$.

$e \in H$

Then if h is any element of H we have $eh^{-1} = h^{-1} \in H$.

given $e, h \rightarrow eh^{-1} \in H$ ~~so~~ $eh^{-1} = h^{-1}$ so $h^{-1} \in H$.

This gives us properties 2 and 3 of the first subgroup theorem.

Finally, if g and h are in H, then $h^{-1} \in H$, so $g(h^-)^{-1} = gh \in H$ so the first property also holds for H and it is therefore a subgroup.

$g \in H, h \in H \Downarrow h^{-1} \in H \Rightarrow g(h^{-1})^{-1} \in H \Rightarrow gh \in H$

property 1 of 1st subgp theorem.

H is a subgroup!