Subgroups

Let G be a group. Recall that before, we defined a subgroup H in G to be a subset of G s.t. H is a group under the binary operation of G.

However, if we know G is a group, we don't actually need to check all the group axioms for H:

Prop (The subgroup criterion): A subset H of a group G is a subgroup of G if and only if

(1) $H \neq \emptyset$, and

(2) If $x, y \in H$, $xy^{-1} \in H$.

Pf: If $H \leq G$, then (1) holds since $1 \in H$ and (2) holds since $y^{-1} \in H$ and H is closed under multiplication.

For the converse, assume H is a subset of G that satisfies (1) and (2).

Let $a \in H$ (by (1)). Then $1 = aa^{-1} \in H$ and $a^{-1} = 1a^{-1} \in H$ by (2), so H has an identity and inverses.

If $a, b \in H$, then $b^{-1} \in H$, so $ab = a(b^{-1})^{-1} \in H$, so H is closed under the operation.

The operation is associative on G, so it must be on H as well. $\square$

Ex:

1.) Every group G has $\{1\} \leq G$ and $G \leq G$. $\{1\}$ is called the trivial subgroup, and is denoted just 1.

2.) $\{1, r, r^2, \dots, r^n\} \leq D_{2n}$ and $\{1, s\} \leq D_{2n}$.

3.) $S_k \leq S_n$ for $k \leq n$.

4.) If $K \leq H$ and $H \leq G$, then $K \leq G$.