Subgroups

Let $\langle G, * \rangle$ be a group. A subset $H \subseteq G$ is a subgroup of G if it is closed under $*$ and is itself a group w/ induced operation from G. We denote this by $H \leq G$ or $H < G$ if $H \leq G$ and $H \neq G$, i.e. if H is a proper subgroup.

Ex:

1.) Under $+$, $\mathbb{Z} \leq \mathbb{Q}$

2.) Consider the subset $\{e, r, r^2, r^3\} \subseteq D_8$.

This is closed under the operation, the operation is associative, e is the identity, and $r^{-1} = r^3$, $(r^2)^{-1} = r^2$. Thus, this is in fact a subgroup.

3.) Every group has $\{e\}$ as a subgroup, called the trivial subgroup.

4.) $2\mathbb{Z}$ = the set of even integers is a subgroup of $\mathbb{Z}$ under addition.

Remark: Once we know that G is a group, it is actually easier to check that a given subset is a group w/ out having to check all the axioms. e.g. if $*$ is associative, it will also be associative on any subset. Here are some simpler criteria to check:

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

1.) $H \neq \emptyset$ and

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

Proof: First assume $H \leq G$. Then $e \in H$, so $H \neq \emptyset$, and since H is a group, if $x, y \in H$, $y^{-1} \in H$, so $xy^{-1} \in H$.

Now assume 1.) and 2.) hold. We check that H is a subgroup.

If $a, b, c \in H$, then $(ab)c = a(bc)$, since the operation is associative on elements of H.

Now, by 1.), we can find some $x \in H$. Thus, by 2.), $xx^{-1} = e \in H$. So H contains an identity.

Thus, for any $y \in H$, we have $ey^{-1} = y^{-1} \in H$, so every element has an inverse.

To check H is closed under the binary operation, let $a, b \in H$. Then $b^{-1} \in H$, so $a(b^{-1})^{-1} = ab \in H$. Thus, H is indeed a subgroup. $\square$

Ex: Let X be the group of functions from $\mathbb{R} \to \mathbb{R}$ under $+$. Let $Y \subseteq X$ be the set of continuous functions from $\mathbb{R} \to \mathbb{R}$.

$f: \mathbb{R} \to \mathbb{R}$ defined $f(x) = 0$ is continuous, so $f \in Y$, so $Y \neq \emptyset$. If g, h are continuous, then $g - h$ is also continuous, so $g - h \in Y$, so Y is a subgroup

Ex: Consider the set S of odd integers together with 0 in $\mathbb{Z}$ (under $+$). This is nonempty, but $3 - 1 = 2 \notin S$, so S is not a subgroup.

Ex: If G is a group, consider $G \times G$. Let $\Delta \subseteq G \times G$ be defined $\Delta = \{(a,a) \mid a \in G\}$.

1.) $G \neq \emptyset$ so $\Delta \neq \emptyset$.

2.) If $(a,a), (b,b) \in \Delta$, then $(a,a)(b,b)^{-1}$

$= (ab^{-1}, ab^{-1}) \in \Delta$, so $\Delta \leq G \times G$.

Δ is called the <u>diagonal subgroup</u>

Cyclic subgroups

Theorem: Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and every subgroup H' s.t. $a \in H'$ also contains H. i.e. $H \subseteq H'$.

Proof: $a \in H$, so $H \neq \emptyset$. Let $a^i, a^j \in H$ for $i, j \in \mathbb{Z}$.

Then $a^i a^{-j} = a^{i-j}$. $i-j \in \mathbb{Z}$, so $a^{i-j} \in H$, so $H \leq G$.

Now suppose $H' \leq G$ s.t. $a \in H$.

Then $a^n \in H'$ for all $n \geq 1$, and $a^0 = e \in H'$, and $a^{-1} \in H'$

so $(a^{-1})^n = a^{-n} \in H'$ $\forall$ $n \geq 1$, so $H \leq H'$. $\square$

Def: The subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of G is called the cyclic subgroup of G generated by a and is denoted $\langle a \rangle$.

A group G is <u>cyclic</u> if there is some generating set consisting of a single element.

Ex: $\mathbb{Z}_n$ is cyclic $\forall$ $n \in \mathbb{Z}_+$. It is generated by 1.

Ex: $\langle \mathbb{Z}, + \rangle$ is cyclic, generated by 1. For $a \in \mathbb{Z}_+$, $a\mathbb{Z}$ = the cyclic subgroup of $\mathbb{Z}$ generated by a and consists of element of $\mathbb{Z}$ that are divisible by $\mathbb{Z}$.

Notice that $12\mathbb{Z} < 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$

More about cyclic groups later...