Announcements

1/26/11

1) Career paths in Math Sciences event
Monday 1/3, CB 1030

2) Substitute teacher Friday.

Recall from last time
$\langle G, \cdot \rangle$ is a group. $S \subseteq G$. We denoted by $\langle S \rangle$ the smallest subgroup of G containing S.
We call $\langle S \rangle$ the subgroup generated by S.

Def: $\langle G, \cdot \rangle$ is called cyclic if $G = \langle g \rangle$ for some $g \in G$.

Remark: for any $g \in G$, $\langle g \rangle = \{ g^n : n \in \mathbb{Z} \}$ with the convention that $g^n = e_g$, the identity element of $\langle G, \cdot \rangle$.
check: $g^n g^m = g^{n+m} \in \langle g \rangle$
and $(g^n)^{-1} = g^{-n} \in \langle g \rangle$

If $\langle G, \cdot \rangle$ is cyclic, then $\forall x \in G$, $x = g^n$ for some $n \in \mathbb{Z}$

Examples (of cyclic groups)

1) $\mathbb{Z}_n$ is a cyclic group
$\langle 1 \rangle = \mathbb{Z}_n$
$= \{ k \cdot 1 : k \in \mathbb{Z}_n \}$

2) $\langle \mathbb{Z}, + \rangle$ is a cyclic group
$\langle 1 \rangle = \mathbb{Z}$
$= \{ k \cdot 1 : k \in \mathbb{Z} \}$

3) Up to isomorphism, $\mathbb{Z}_n$ and $\langle \mathbb{Z}, + \rangle$ are the only cyclic groups.

4) $\langle \mathbb{Q}, + \rangle$ is not cyclic
let $x \in \mathbb{Q}$, write $x = \frac{a}{b}$ with a, b in lowest terms ($a, b \in \mathbb{Z}$, $b \neq 0$)
$\langle x \rangle = \{ \frac{ka}{b} : k \in \mathbb{Z} \}$
If $b = 1$, then $\frac{1}{2} \notin \langle x \rangle$
if $b \neq 1$ $\frac{a}{b+1}$ is not expressible as $\frac{ka}{b}$ $(a \neq 0)$
If this were true then $\frac{ka}{b} = \frac{a}{b+1} \Rightarrow k(b+1) = b$
then $k = \frac{b}{b+1}$ but $\gcd(b, b+1) = 1$ so $k \notin \mathbb{Z}$
Therefore, $\langle \mathbb{Q}, + \rangle$ is not cyclic

<u>Thm:</u> Suppose $\langle G, \cdot \rangle$ is cyclic. Then $\langle G, \cdot \rangle$ is either isomorphic to $\mathbb{Z}_n$ or $\langle \mathbb{Z}, + \rangle$.
<u>Pf:</u> We know since $\langle G, \cdot \rangle$ is cyclic that there is a $g \in G$, $\langle g \rangle = G$.
<u>Case 1:</u> There is no natural number n with $g^n = e_G$. Define $\varphi : \langle G, \cdot \rangle \to \langle \mathbb{Z}, + \rangle$ $\varphi(g^n) = n$. We claim φ is an isomorphism. Prove φ is bijective. It is clear that φ is surjective.
Suppose $\varphi(g^n) = \varphi(g^m)$. Then $n = m$, so $g^n = g^m$ hence φ is injective.
$\varphi(g^n \cdot g^m) = \varphi(g^{n+m}) = n + m = \varphi(g^n) + \varphi(g^m)$
so, φ is an isomorphism.
<u>Case 2:</u> There is an $n \in \mathbb{N}$ with $g^n = e_G$. Choose the smallest natural number k with $g^k = e_G$. Define $\varphi : \langle G, \cdot \rangle \to \mathbb{Z}_k$ $\varphi(g^m) = m$, can check that this is an isomorphism.

a group of one element is also cyclic

Corollary: Every subgroup of a cyclic group is cyclic.

Pf: By previous theorem, we only need to consider $\langle \mathbb{Z}, + \rangle$ and $\mathbb{Z}_n$.
Suppose $H \leq \mathbb{Z}$. If $H = \{0\}$, H is isomorphic to $\mathbb{Z}_1$. If $H \neq \{0\}$, if $m \in H$ then $-m \in H$. Choose the minimal $m \in H \cap \mathbb{N}$. Suppose $mk \leq n < m(k+1)$ for some $k \in \mathbb{Z}$. then $mk \leq n < mk + m$
subtract mk to get $0 \leq n - mk < m$
If $n - mk \in H$, then since m is the minimal natual number in H we must have, $n - mk = 0$
Hence $n = mk$. This implies $H = \langle m \rangle$
$\mathbb{Z}_n$ case is identical ∎