**Theorem:** Let $G$ be a group and let $x \in G$

Define

$$H = \{x^n \mid n \in \mathbb{Z}\} = \{\ldots, \underset{(x^{-1})^3}{x^{-3}}, \underset{(x^{-1})^2}{x^{-2}}, x^{-1}, \underset{x^0 = e}{x^0}, x^1, x^2, x^3, \ldots\}$$

Then $H \leq G$ ($H$ is a subgroup of $G$)

Moreover $H$ is the smallest subgroup of $G$ that contains $x$.

We denote this $H$ by $\langle x \rangle$

**Example:**

$G = \mathbb{Z}_{12}$ $\qquad e = \bar{0}$

$x = \bar{4}$, inverse of $\bar{4}$ is $\bar{8}$ since $\bar{4} + \bar{8} = \overline{12} = \bar{0}$

$H = \langle \bar{4} \rangle = \{\ldots, \bar{8}+\bar{8}+\bar{8}, \bar{8}+\bar{8}, \bar{8}, \bar{0}, \bar{4}, \bar{4}+\bar{4}, \bar{4}+\bar{4}+\bar{4}, \ldots\}$

$= \{\ldots, \bar{0}, \bar{4}, \bar{8}, \underset{e}{\bar{0}}, \underset{x}{\bar{4}}, \underset{x+x}{\bar{8}}, \bar{0}, \bar{4}, \bar{8}, \bar{0}, \ldots\}$

$= \{\bar{0}, \bar{4}, \bar{8}\}$ this repetition usually happens when a group is finite $(\mathbb{Z}_{12})$

By the theorem $\{\bar{0}, \bar{4}, \bar{8}\}$ is a subgroup of $\mathbb{Z}_{12}$ and it is also the smallest subgroup that contains $x = \bar{4}$.

**Proof of theorem**

we first show that $H \leq G$

(1) closure; Let $a, b \in H$ then $a = x^{n_1}$ and $b = x^{n_2}$ where $n_1, n_2 \in \mathbb{Z}$, so $ab = x^{n_1} x^{n_2} = x^{n_1 + n_2} \in H$

(2) identity $e = x^0 \in H$

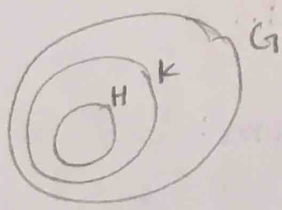
(3) inverses Let $c \in H$ then $c = x^n$ where $n \in \mathbb{Z}$

Then $c^{-1} = (x^n)^{-1} \underset{x^n x^{-n} = x^0 = e}{=} x^{-n} \in H$

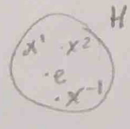
so $H \leq G$

Now lets show that $H$ is the smallest subgroup of $G$ that contains $x$

Suppose $K$ is another subgroup of $G$ that contains $x$, we now show that $H \leq K$




since $x \in K$ we know that if $n > 0$ then $x^n = x\, x\, x \cdots x \in K$ b/c $K$ is closed.




$x^0 = e \in K$ since $K \leq G$

since $x \in K$ and $K \leq G$ we know $x^{-1} \in K$

Therefore, for $n > 0$ $(x^{-1})^n = x^{-1} x^{-1} x^{-1} \cdots x^{-1} \in K$ since $K$ is closed.

So $H \leq K$ $\boxtimes$

Example:

$G = \mathbb{Z}$, $* = +$

$\langle 3 \rangle = \{\ldots, (-3)+(-3), (-3), 0, 3, 3+3, 3+3+3, \ldots\}$

$= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{3n \mid n \in \mathbb{Z}\}$

Def: Let $G$ be a group

Let $x \in G$, Then $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ is called the cyclic subgroup generated by $x$.

If $G = \langle b \rangle$ for some $b \in G$ then we say that $G$ is a cyclic group and call $b$ a generator of $G$.

Example: $\mathbb{Z}$

$\langle 3 \rangle \leftarrow$ The cyclic subgroup generator by 3.

$\langle 1 \rangle = \{\ldots, (-1)+(-1), \underset{}{\overset{\text{inverse of 1 under +}}{(-1)}}, 0, 1, 1+1, 1+1+1, \ldots\}$

$= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z}$

So $\mathbb{Z}$ is a cyclic group and $1$ is a generator for $\mathbb{Z}$

$\langle 0 \rangle = \{\ldots 0+0, 0, 0, 0, 0+0, \ldots\} = \{0\}$

$\langle -1 \rangle = \{\ldots, 3, 2, 1, 0, -1, -2, -3, \ldots\} = \mathbb{Z}$

1 and $-1$ are the only generators of $\mathbb{Z}$

9/19 P.2

Example: $\mathbb{Z}_n$ is cyclic

$\bar{1}$ is a generator

inverse of $\bar{1}$ is $\bar{3}$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\langle \bar{1} \rangle = \{\ldots, \bar{3}+\bar{3}, \bar{3}, \bar{0}, \bar{1}, \bar{1}+\bar{1}, \ldots\}$

$= \{\ldots \bar{1}, \bar{2}, \bar{3}, \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{0}, \ldots\}$

**Def:** Let $G$ be a group and $x \in G$

If $\exists$ a positive integer $m \geq 1$ where $x^m = e$, then the **order of $x$** is defined to be the smallest positive integer $n \geq 1$ where $x^n = e$

If no such $m$ exists then we say that the order of $x$ is infinite.

$x^m = e$

$\underbrace{x * x * x * \cdots * x}_{m \text{ times}} = e$

**Example:** $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$

$* = +$

order of $\bar{6}$

$\underset{1}{\bar{6}} + \underset{2}{\bar{6}} = \overline{12} = \bar{0}$, so $\bar{6}$ has order $\underline{2}$.

order of $\bar{4}$

$\underset{1}{\bar{4}} + \underset{2}{\bar{4}} + \underset{3}{\bar{4}} = \overline{12} = \bar{0}$, so $\bar{4}$ has order $\underline{3}$

order of $\bar{8}$

$\bar{8} + \bar{8} + \bar{8} + \bar{8} + \bar{8} + \bar{8} = \overline{48} = \overline{12 \cdot 4}$

$= \overline{0 \cdot 4} = \bar{0}$

this doesn't say that $\bar{8}$ has order 6 since 6 is not the smallest positive integer

$\bar{8} \neq \bar{0}$

$\bar{8} + \bar{8} = \overline{16} = \bar{4} \neq \bar{0}$

$\bar{8} + \bar{8} + \bar{8} = \overline{24} = \bar{0}$ & 8 has order 3

| element | order |
|---|---|
| $\bar{0}$ | 1 |
| $\bar{5}, \bar{1}, \overline{11}, \bar{7}$ | 12 |
| $\bar{2}, \overline{10}$ | 6 |
| $\bar{3}, \bar{9}$ | 4 |
| $\bar{4}, \bar{8}$ | 3 |
| $\bar{6}$ | 2 |

Fact
$x$ has the same order as $x^{-1}$
HW #4

- $\mathbb{Z}_{12}$ is cyclic generators are $\bar{1}, \bar{5}, \bar{7}$, and $\overline{11}$.

$D_6 = \{1, r, r^2, s, sr, sr^2\}$

| element | order |
|---|---|
| 1 | 1 |
| $r, r^2$ | 3 |
| $s, sr, sr^2$ | 2 |

Later in class we'll prove that the order of a group is a divisor of the group

ex order : 1, 3, 2 group $D_6$

$D_6$ is not cyclic, no elements of order 6

**Example:** $G = \mathbb{Z}$, $e = 0$

order of 1

$1$

$1+1=2$

$1+1+1=3$

$1+1+1+1=4$

$\vdots \quad \vdots$

never goes to 0, 1 has a infinite order

**Division Algorithm**

Let $m$ be a positive integer and $n$ be any integer. then $\exists$ unique integers $q$ and $r$ where $n = mq + r$ and $0 \le r < m$

**Example** $n = 711$

$m = 13$

54 ← q

13 | 711 ← n

m

−65

61

−52

9 ← r < 13

$711 = 13(54) + 9$

$n = m(q) + r$

9/21 P. 2

Example: $n=6$ $\quad 6=2(3)+0$

$m=2$ $\quad n=m(q)+r$

Example: $n=-5$ $\quad -5=2(-3)+1$

$m=2$ $\quad n=m(q)+r$

since $0\le r<m$

$0\le 1<2$

Claim: Let $G$ be a group and $x\in G$

① If $x$ has a finite order $n$, then

$$\langle x\rangle=\{e,x,x^2,\dots,x^{n-1}\}$$

Furthermore, $x^k\neq x^h$ if $0\le k<h<n$

hence $n=|\langle x\rangle|$

② If $x$ has infinite order, then

$$\langle x\rangle=\{\dots,x^{-3},x^{-2},x^{-1},e,x,x^2,x^3,\dots\}$$

Furthermore $x^k\neq x^h$ if $k\neq h$

proof continued...

Suppose $x^k=x^h$ where $0\le k<h<n$

Then $x^k x^{-k}=x^h x^{-h}$

so $e=x^{h-k}$

but $0<h-k<n$

so you can't have $e=x^{h-k}$ b/c $n$ is the order of $x$.

Thus $|\langle x\rangle|=n$

Proof

① Suppose $x$ has a finite order $n \leftarrow x^n = e$

Let $S = \{e, x, x^2, \dots, x^{n-1}\}$

we want to show that

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$$

is equal to $S$.

Certainly, $S \subseteq \langle x \rangle$

now lets show $\langle x \rangle \subseteq S$

Pick some $x^k \in \langle x \rangle$ where $k \in \mathbb{Z}$

By the division algorithm $\exists\, q, r$ where

$k = nq + r$ and $\underbrace{0 \le r < n}_{0 \le r \le n-1}$

Then $x^k = x^{nq+r} = (x^n)^q x^r \underset{\uparrow \atop x^n = e}{=} e^q x^r \underset{\uparrow \atop e^q = e}{=} x^r$

so $x^k = x^r \in S$ Therefore, $\langle x \rangle \subseteq S$, so $S = \langle x \rangle$

Example $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$\langle r \rangle = \{\dots, r^{-3}, r^{-2}, r^{-1}, e, r, r^2, r^3, \dots\}$

$= \{1, r, r^2\}$ order of $r$ is 3 since $r^3 = 1$