Cyclic Groups:

<u>Def'n</u>: G is cyclic iff $G = \{a^n \mid a \in G, n \in \mathbb{Z}\} = \langle a \rangle$

<u>Ex</u> $\mathbb{Z}$ is cyclic under addition: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$1^3 = 1 + 1 + 1$

<u>Non-Ex</u> D_4 is not cyclic

<u>Ex</u> $\mathbb{Z}_n$ is cyclic

<u>Ex</u>: $U(12) = \{1, 5, 7, 11\}$ — not cyclic

Powers of
5: $5, 5^2 = 1$ ($25 \bmod 12 = 1$) $\{1, 5\}$
7: $7, 49 \bmod 12 = 1$, $\{1, 7\}$
11: $\{1, 11\}$ b/c

$(n-1)^2 = n^2 - 2n + 1 \bmod n$
$= 1$

$U(10) = \{1, 3, 7, 9\}$

Powers of $3 = U(10)$ ($\Rightarrow$ it's cyclic)

$\{3, 9, 7, 1\}$

powers of $7 = \{7, 9, 3, 1\}$

Question: When does $a^i = a^j$?

Thm: 1 If $|a|$ is infinite $a^i = a^j \Rightarrow i = j$. (4.1)

2 If $|a|$ is finite then $a^i = a^j \Rightarrow n \mid i-j$

($|a| = n$)

order of the element

(Ex. $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$1^{17} = 17 \bmod 6 = 5 = 1^5$ & 6 divides $17-5$

order $\qquad$ 12

$i-j$.

3 & $\underbrace{\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}}_{\text{order of the group generated } a:}$.

Two concepts of order are the same for cyclic groups

order of element a $=$ # of elements generated by a

Ex

$n = 13$

$\mathbb{Z}_{13}$ is cyclic, generated by 1 (mod 13)

$\left\{ \begin{array}{l} \text{In } \mathbb{Z}_{13} \text{ the order of } 1 \text{ is } 13. \\ \text{the order of } \mathbb{Z}_{13} \text{ is ALSO } 13. \end{array} \right\}$

$1^2 = 2$

$1^7 = 7$

$1^{15} = 15 \bmod 13 = 2$

$1^{13} = 13 \bmod 13 = 0$

id elt.

proof.

① If $|a|$ is infinite, then $a^i = a^j$ implies $i-j=0$

Assume $a^i = a^j$.

$$a^i \cdot a^{-j} = a^j \cdot a^{-j}$$

$$a^{i-j} = e.$$ (Now, we have some power of a equaling the identity yet $|a| = \infty$.)

So $i-j=0$

or $i=j$

---

② Assume $|a| = n$. Show If $a^i = a^j$ then $n \mid i-j$.

Div. Alg $\Rightarrow$ $i-j = nk + r$ & $0 \leq r < n$

So $a^{i-j} = a^{nk+r} = a^{nk} \cdot a^r = (a^n)^k \cdot a^r = e^k \cdot a^r = a^r$.

$a^{i-j} = e$

b/c $|a|=n$ $\Downarrow$ $a^n = e$

& n is the smallest such power

So... $r = 0$.

thus $i-j = nk$

$\Rightarrow$ n divides $i-j$.

---

③ If $|a| = n$, show any power of a, say a^k, lives in $\langle a \rangle$.

Recall, $a^n = e$. here, n = 3

$$a^k = \underbrace{\overbrace{a \cdot a \cdot a}^{e} \cdot \overbrace{a \cdot a \cdot a}^{e} \cdot \overbrace{a \cdot a \cdot a}^{e} \cdot \overbrace{a \cdot a \cdot a}^{e} \cdot \overbrace{a \cdot a \cdot a}^{e} \cdot \overbrace{a \cdot a \cdot a}^{e} \cdot a \cdot a}_{k} = a^2$$

div alg.

i.e., $k = nq + r$ & $0 \leq r < n$

So $a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r$ $0 \leq r < n$

So $a^r \in \{e, a, a^2, \dots, a^{n-1}\}$

Point: $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

<u>Corollary</u>: $|a| = |\langle a \rangle|$

order of elt a — order of group generated by a.

<u>Corollary</u>: $a^k = e$ implies k is a multiple of $|a|$

(i.e., $|a|$ divides k)

<u>Thm 4.2</u> On Friday