Recall: $a \in G$

$$\text{ord}(a) = \begin{cases} \text{smallest positive integer } n \text{ such that } a^n = e \\ \infty \quad \text{if } a^n \neq e \text{ for all } n > 0 \end{cases}$$

$\langle a \rangle$ = subgroup generated by a

$= \{ a^k , k \in \mathbb{Z} \}$

Lemma (a) $\text{ord}(a) = |\langle a^4 \rangle|$

(b) $b \in \langle a \rangle \Rightarrow \langle b \rangle \subset \langle a \rangle$

proof (a) assume $\text{ord}(a) = n < \infty$

$\Rightarrow |\langle a \rangle| = |\{ e, a, \ldots, a^{n-1} \}| = n$ ✓

Theorem $\quad \operatorname{ord}(a) = n$, fix $k \in \mathbb{Z}$

(a) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$

(b) $\operatorname{ord}(a^k) = \dfrac{n}{\gcd(k,n)}$

Proof. Let $d = \gcd(n,k)$

(a). "$\subset$" $\quad d = \gcd(n,k) \mid k$

$\Rightarrow k = md$

$\Rightarrow a^k = (a^d)^m \in \langle a^d \rangle$ ✓

"$\supset$" $\quad d = sn + tk$ for some integers s and t

$a^d = a^{sn+tk} = (a^n)^s (a^k)^t$

$= e^t = (a^k)^t \in \langle a^k \rangle \Rightarrow$ claim. (use Lemma b)

(b) $\operatorname{ord}(a^k) = |\langle a^k \rangle| = |\langle a^d \rangle| = \operatorname{ord}(a^d)$

($\operatorname{ord}(a^k) =$ Lemma a; $|\langle a^k \rangle| =$ part (a))

$d = \gcd(n,k) \mid n \Rightarrow \boxed{n = md}$

$\Rightarrow (a^d)^j = a^{jd} \neq e$ if $0 < j < m$

(because then $0 < jd < md = n$, hence $a^{jd} \neq e$; $\uparrow$ $\operatorname{ord}(a)$!)

and $(a^d)^m = a^{md} = a^n = e$

$\Rightarrow \operatorname{ord}(a^d) = m = \frac{n}{d}$ ✓

$\rightarrow$ $\operatorname{ord}(a^k)$

Example: What is the order of 20 in $\mathbb{Z}_{50}$?

recall: $\mathbb{Z}_{50}$ is cyclic with generator $1 \sim a$

(if $a=1$: $a^k \sim k$ (translating to additive notation.

$$n = 50 = \text{ord}(1)$$

$$\text{ord}(20) = \gcd(20, 50) = \boxed{10}$$

This was a special case of

Corollary 1 The order of m in $\mathbb{Z}_n$ is equal to $\gcd(m, n)$.

Corollary 2 Let G be a cyclic group $|G| = n$

$b \in G \Rightarrow \text{ord}(b) \mid n$

proof. Let a be a generator of G, i.e. $G = \langle a \rangle$

$\Rightarrow b = a^k$ for some k. $\Rightarrow \text{ord}(b) = \gcd(k, n) \mid n$. ✓

Corollary 3 — which elements in $\langle a \rangle$ generate $\langle a \rangle$?

$$\langle a^k \rangle = \langle a \rangle \iff \gcd(k, n) = 1$$

Example: Assume $\text{ord}(a) = 12$, $G = \langle a \rangle$

Find all elem. b in G s.t. $G = \langle b \rangle$?

Solution: by Coroll. 3 $b = a^k$ s.t. $\gcd(k, 12) = 1$

Solution: $k \in \{1, 5, 7, 11\}$

i.e. $\langle a \rangle = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle$

Question: What are the possible subgroups of a cyclic group?

Theorem Let $G = \langle a \rangle$ cyclic

Any subgroup $H \subset G$ is also cyclic,
i.e. $H = \langle a^k \rangle$ for some k

Proof: Let $H \subset G$ be a subgroup

Let t be smallest positive integer such that $a^t \in H$
(assume $H \neq \{e\}$!)

Claim: any elem. in H is of the form $a^{tm} = (a^t)^m$
for some integer m.

proof Let $a^k \in H$

Let $k = tq + r$, $0 \leq r < t$

$$a^k = (a^t)^q a^r$$

$a^k \in H$, $(a^t)^q \in H$

can solve for a^r, as $\left[(a^t)^q\right]^{-1} \in H$

$$\Rightarrow \quad a^r = (a^{tq})^{-1} a^k \in H$$

$(a^{tq})^{-1} \in H$, $a^k \in H$

If $r > 0$ ↯ contradicts t smallest pos. integer s.t. $a^t \in H$ (as $r < t$!)

$\Rightarrow r = 0$

i.e. $k = tq$

$\Rightarrow b = a^k = (a^t)^q \in \langle a^t \rangle \Rightarrow H$ cyclic.

Theorem G finite cyclic group $|G| = n$

$\Rightarrow$ there exists exactly one subgroup H for each divisor $d \mid n$, and these are all subgroups of G

proof follow from previous theorem and its proof.

have seen $H \leq G$ subgroup $\Rightarrow H = \langle a^t \rangle = \langle a^{\gcd(t,n)} \rangle$ ($\gcd(t,n) = d$)

↑ first theorem today

Example: Write down all subgroups of $\mathbb{Z}_{12}$

answer: given by divisors of 12:

subgroups are

$\langle 1 \rangle = \mathbb{Z}_{12}$, $\langle 2 \rangle = \{0,2,4,6,8,10\}$, $\langle 3 \rangle$, $\langle 4 \rangle = \{0,4,8\}$, $\langle 6 \rangle = \{0,6\}$