Recall:

Lemma: $a^m = e \Rightarrow \text{ord}(a) \mid m$

crucial observation in proof was:

If $\text{ord}(a) = n$ and m any integer

$\Rightarrow$ $a^m = a^r$, where $m = qn + r$, $0 \leq r < n$

Theorem: Let $a \in G$

(a) If $\text{ord}(a) = \infty \Rightarrow a^i = a^j \Leftrightarrow i = j$

(b) If $\text{ord}(a) = n \Rightarrow a^i = a^j \Leftrightarrow n \mid (j-i)$

$\Leftrightarrow i \bmod n = j \bmod n$

Proof (a) $\text{ord}(a) = \infty$ means $a^i \neq e$ for any $i \neq 0$

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

$\Rightarrow e = a^0 = a^{i-i} = a^{j-i}$

$\Rightarrow j - i = 0$ i.e. $j = i$

(4) $U(8) = \{1,3,5,7\}$ cyclic?

$a=3$: $3^2 \bmod 8 = 9 \bmod 8 = 1$

$3^3 = 3^2 \cdot 3 = 1 \cdot 3 = 3 \bmod 8$

$\Rightarrow \{3^k, k \in \mathbb{Z}\} = \{1,3\} \neq U(8)$

$a=5$ $5^2 = 25 \bmod 8 = 1$

$\Rightarrow$ $5^{\text{even}} = 1$, $5^{\text{odd}} = 5$ $\Rightarrow \langle 5 \rangle = \{1,5\} \neq U(8)$

$a=7$ check for yourself: $\langle 7 \rangle = \{1,7\}$

Result: None of the elements $a \in U(8)$ satisfies $\langle a \rangle = U(8)$ $\Rightarrow$ $U(8)$ NOT cyclic!

Recall: If $a \in G$, $H = \{a^k, k \in \mathbb{Z}\} = \langle a \rangle$ ← notation

is a subgroup of G

H is called a cyclic subgroup

Def. A group G is called cyclic if there is an $a \in G$ such that $G = \langle a \rangle$

Have seen: ① $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}_n = \langle 1 \rangle$ are cyclic groups

② Is $U(10)$ cyclic? $U(10) = \{1, 3, 7, 9\}$

Try $a = 3$.

$3^2 \bmod 10 = 9$

$3^3 \bmod 10 = 27 \bmod 10 = 7$

$3^4 \bmod 10 = 81 \bmod 10 = 1$

$\{3, 3^2, 3^3, 3^4\}$

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

$= U(10)$

$\Rightarrow U(10)$ is cyclic

(3) G abelian group

$H = \{ x \in G,\ x^2 = e \}$

claim: H is a subgroup!

$x \in H \Rightarrow x \cdot x = e$ by def. ✓

$\Rightarrow$ inverse of x is x itself

$x, y \in H$ to show $xy \in H$

i.e. to show: $(xy)^2 = e$ by def. of H

$(xy)^2 = x(yx)y = xxyy = x^2y^2 = e$

($yx = xy$ ← H abelian!)

$\Rightarrow xy \in H$ ✓

Subgroup $H \subset G$

is a subset of G which is a group with the binary operation of G.

Subgroup Test: $H \subset G$ a subgroup if

(a) $h \in H \Rightarrow$ its inverse $h^{-1} \in H$

(b) $h, k \in H \Rightarrow hk \in H$

Examples: (1) $\{\pm 1, \pm i\}$ is a subgroup of $(\mathbb{C}\setminus\{0\}, \cdot)$

apply subgroup test

(2) more generally: Fix $n \in \mathbb{N}$

$$H = \{ e^{2\pi i k/n}, k \in \mathbb{Z} \} = \{ (e^{2\pi i/n})^k, k \in \mathbb{Z} \}$$

claim: this is a subgroup of $(\mathbb{C}\setminus\{0\}, \cdot)$

sketch for subgroup test

- inverse of $e^{2\pi i k/n} = e^{2\pi i(-k)/n} \in H$ ($-k \in \mathbb{Z}$)
- $e^{2\pi i k/n} \cdot e^{2\pi i l/n} = e^{2\pi i (k+l)/n} \in H$ ($k+l \in \mathbb{Z}$)

H has n elements because

if $k = qn + r$

then $e^{2\pi i k/n} = e^{2\pi i (nq+r)/n}$

$= e^{2\pi i q} \cdot e^{2\pi i r/n}$

$= \underbrace{e^{2\pi i q}}_{=1}$

$= e^{2\pi i r/n}$

$\Rightarrow H = \{ e^{2\pi i r/n}, \ 0 \le r < n \}$

$\Rightarrow |H| = n$.

We can say more if $ab = ba$!

Lemma: Assume $\boxed{ab = ba}$

$\Rightarrow$ (a) $ab^k = b^k a$ for all $k \in \mathbb{Z}$

(b) $(ab)^k = a^k b^k$ " " " " "

Proof. prove by ind. on k. (exercise!)

Theorem: Assume $ab = ba$, $\operatorname{ord}(a) = n$, $\operatorname{ord}(b) = m$

$\Rightarrow$ $\operatorname{ord}(ab) \mid nm$

proof. $(ab)^{nm} \underset{\uparrow \text{Lemma(b)}}{=} a^{nm} b^{nm} = (a^n)^m (b^m)^n$

$= e^m e^n = e$

By lemma of previous lecture $\Rightarrow$ $\operatorname{ord}(ab) \mid nm$. ✓

Question: Say $\operatorname{ord}(a) = 6$

what about $\operatorname{ord}(a^4)$?

Try brute force: $a^4 \neq e$ (otherwise $\operatorname{ord}(a) \leq 4$!)

$$(a^4)^2 = a^8 = a^2 \neq e$$

green formula

$$8 = 1 \cdot 6 + 2$$

$$(a^4)^3 = a^{12} = a^0 = e$$

$$12 = 2 \cdot 6 + 0$$

Recall: $\operatorname{ord}(a^4) = 3$

(b) $\text{ord}(a) = n$

$a^i = a^j \Rightarrow e = a^{i-i} = a^{j-i}$

$\Rightarrow n = \text{ord}(a) \mid j-i \Rightarrow$ claim

Lemma

Question: If $\text{ord}(a) = n$ and $\text{ord}(b) = m$

what can we say about the order of ab?

Answer: nothing in general if $ab \neq ba$

check in homework problem:

let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$

then both A and B have finite orders (just calculate $A^2, A^3, A^4 \ldots$ until you get I; same $B, B^2 \ldots$)

but AB has infinite order! (check $(AB)^n \neq I$ for all $n > 0$)

General Situation:

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

(a) $\langle a^k \rangle = \{a^{mk}, m \in \mathbb{Z}\} = \langle a^{\gcd(k,n)} \rangle$

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

check for our example: $n = 6$, $k = 4$

we showed: $\langle a^4 \rangle = \{a^4, a^2, e\} = \langle a^2 \rangle$

$2 = \gcd(4,6)$.

$3 = \operatorname{ord}(a^4) = \dfrac{6}{\gcd(4,6)} = \dfrac{6}{2}$ ✓

↑ checked on previous page