Last class:

Lemma: Assume $a^m = e$ in a group $G$, $m$ pos. integer

$\Rightarrow \text{ord}(a) \mid m$

Remark: $a^m = e$ does NOT imply $\text{ord}(a) = m$

## Subgroups

Def. A subset $\emptyset \neq H \subset G$, $G$ a group is called a subgroup if it is a group by itself with the binary operation of $G$

Remark: Not every subset of $G$ is also a subgroup

# Examples / Counterexamples

Let $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition mod 4

(a) Is $H = \{2, 3\}$ a subgroup?

NO because $H$ does not have an identity element

Observation: If $u$ is an element in $H$ s.t.

$$\boxed{uh = h} \quad \text{for all } h \in H$$

$\Rightarrow u = e$ = identity element of $G$

(Proof: multiply $uh = h$ by $h^{-1}$ from the right

$$\underbrace{uhh^{-1}}_{e} = \underbrace{hh^{-1}}_{e}$$

$$u = ue = e \Rightarrow u = e \; !$$

use cancellation property!

Recall: A subgroup must always contain the identity element $e$ of $G$

(b) $H = \{0, 3\} \subset \mathbb{Z}_4 = \{0, 1, 2, 3\}$

subgroup?

$\Rightarrow$ it would have to contain the inverse of 3

inverse of 3 = 1 ($1 + 3 \bmod 4 = 4 \bmod 4 = 0$)

$1 \notin H \Rightarrow$ H not a subgroup

(c) $H = \{0, 2\}$ This is a subgroup

(I will check using subgroup test)

Recall: $U(8) = \{1, 3, 5, 7\}$ with multiple. mod 8

$= \{ 1 \le a \le 7, \gcd(a, 8) = 1 \}$

(d) Is $H = \{1, 3, 5\}$ a subgroup?

it has identity elem. 1 ✓

$3 \cdot 3 \bmod 8 = 9 \bmod 8 = 1$

$5 \cdot 5 \bmod 8 = 25 \bmod 8 = 1$

} both 3 and 5 have inverses ✓

one more thing to check:

the operation of $G$ must also define an operation on $H$

$\Rightarrow$ $h, k \in H \Rightarrow hk \in H$

check $3 \cdot 5 \bmod 8 = 15 \bmod 8 = 7 \notin H$

$\Rightarrow$ $\{1, 3, 5\}$ is NOT a subgroup of $U(8)$.

Ways to show that a subset $H \subset G$ is <u>NOT</u> a subgroup

1. $e \notin H$
2. can find an element $h \in H$ such that $h^{-1} \notin H$
3. can find elements $h, k \in H$ such that $hk \notin H$.

# Subgroup Test (in book: two step subgroup test)

Let $G$ be a group, $\emptyset \neq H \subset G$ a subset

$H$ is a subgroup if

(a) $h \in H \Rightarrow h^{-1} \in H$ for all $h \in H$

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

Proof
- by condition (b), the (binary) operation on $G$ defines a binary operation on $H$

check axioms for operation
- associativity (already true for all elements in $G \supset H$) ✓
- inverse ✓ by condition (a)
- identity pick $h \in H \overset{(a)}{\Rightarrow} h^{-1} \in H \overset{(b)}{\Rightarrow} e = hh^{-1} \in H$ ✓

## Examples:

(1) $H = \{0, 2\} \subset \mathbb{Z}_4$ is a subgroup

$0+0=0 \qquad 0+2=2=2+0 \qquad 2+2 \bmod 4 = 0 \Rightarrow$ (a)

inverse of $0 = 0$

" " $2 = 2 \bmod 4 \Rightarrow$ (b) ✓

(2) Let $G$ be a group, pick $a \in G$

Define $H = \{a^n, n \in \mathbb{Z}\}$

(if $n < 0$ we define $a^n = (a^{-1})^{|n|}$ ← inverse of $a$)

claim: $H$ is a subgroup!

$a^n, a^m \in H \Rightarrow a^n \cdot a^m = a^{\underbrace{n+m}_{\in \mathbb{Z}}} \in H$ ✓

(check that this is true also if $n<0$ or $m<0$.)

$\Rightarrow$ (a)

given $a^n \in H$ claim: $a^{-n}$ is its inverse

proof. by ind. on $n$

$a^1 \cdot a^{-1} = a a^{-1} = e$ by def. of $a^{-1}$ = inverse of $a$

$n \to n+1$ $\quad a^{n+1} \cdot a^{-(n+1)}$

$= (\underbrace{a\,a \cdots a}_{n+1 \text{ times}})(\underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n+1 \text{ times}})$

$= (\underbrace{a\,a \cdots a}_{n \text{ time}})\,\underbrace{a\,a^{-1}}_{=e}\,(\underbrace{a^{-1}\cdots a^{-1}}_{n \text{ times}})$

$= a^n \cdot a^{-n} = e$ by ind. assumption.

$\Rightarrow$ (b) ✓

$\Rightarrow H$ is a subgroup.

**Def.** (a) We denote the (sub)group $H = \{a^n,\ n \in \mathbb{Z}\}$ by $\langle a \rangle$

(b) A group $G$ is called **cyclic** if we can find an element $a$ in $G$ such that $G = \langle a \rangle$

**Examples:** (1) $G = \mathbb{Z}$ is cyclic

$G = \langle 1 \rangle$ (recall: we use additive notation for $G = \mathbb{Z}$

$a = 1, \Rightarrow a^n \sim n \cdot 1$

(2) $\mathbb{Z}_n$ is cyclic

$\mathbb{Z}_n = \langle 1 \rangle$

(3) $U(8) = \{1, 3, 5, 7\}$ with multiplication mod 8

claim: NOT cyclic. proof: check: $3^2 = 5^2 = 7^2 = 1 \bmod 8$

$\Rightarrow \langle a \rangle$ has at most 2 elements.