Last class:

D_4 symmetries of a square

group with 8 elements

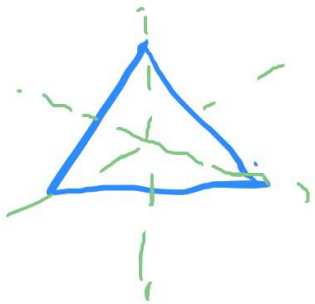
4 rotations & 4 reflections

similarly can define the dihedral group D_n

= symmetries of a regular n-gon

It has $2n$ elements, n rotations and n reflections

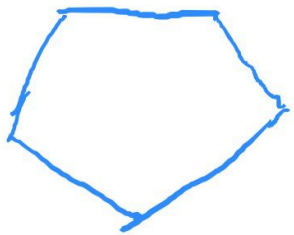
$n=3$



reflection axes

3 rotations.

$n=5$



symmetries of regular Pentagon

Remark: The dihedral groups D_n are **not** Abelian for $n \geq 3$.

e.g. for $n=4$. check: S reflection at main diagonal

$$\Rightarrow \quad S R_{90} = R_{270} S \neq R_{90} S$$

true for any dihedral group:

If R is a rotation and S is a reflection

then $$SR = R^{-1} S$$

Other examples:

① $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with addition mod n

② can also define multipl. mod n

identity element: 1

problematic: inverses do not always exist!

e.g. $0 \cdot a \bmod n = 0 \neq 1$ for all integers a

if $n=4$: also 2 does not have an inverse mod 4

because $2 \cdot 1 = 2$

$2 \cdot 2 \bmod 4 = 4 \bmod 4 = 0$

$2 \cdot 3 \bmod 4 = 6 \bmod 4 = 2$

$4 \cdot 4 \bmod 4 = 16 \bmod 4 = 0$

Lemma Let $n > 0$

The integer a has an inverse mod n $\Leftrightarrow$ $\gcd(a, n) = 1$

proof Recall: $\exists$ integers s and t such that

$$\gcd(a, n) = sa + tn$$

"$\Leftarrow$" $1 = \gcd(a, n) = sa + tn$

$$\Rightarrow \quad sa = 1 - tn$$

$$sa \bmod n = 1$$

$\Rightarrow$ s is the inverse of $a \bmod n$

"$\Rightarrow$" Let s be the inverse of $a \bmod n$

i.e. $sa \bmod n = 1$

$\Rightarrow$ $sa - 1 =$ multiple of n

$= tn$ for some int. t $\Rightarrow$ $\boxed{sa - tn = 1}$

$\Rightarrow \gcd(a,n)=1$.

Def. The group $U(n)$ is given by

$\{r,\ 0<r<n,\ \gcd(r,n)=1\}$

with multipl. mod n.

Check for yourself: This is indeed a group!
(just use the lemma!)

General result:

Theorem $a,b\in G \Rightarrow (ab)^{-1}=b^{-1}a^{-1}$

Proof. By uniqueness of inverse, it suffices to check

$(ab)(b^{-1}a^{-1}) \doteq e$ ← check here:

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ (assoc.)

$= aea^{-1}$

$= aa^{-1} = e$

and $(b^{-1}a^{-1})(ab) \doteq e$

Ch 3 :

Def. (a) The **order** of a group G, notation $|G|$

is the number of elements in the group

It is either a natural number (finite group)

or it is infinity (infinite group)

(b) The **order of an element** $a \in G$, $\text{ord}(a)$ (book $|a|$)

is the smallest positive integer n such that $a^n = e$

or if no such n exists

if is ∞.

Examples: (a) $|D_4| = 8$

$|\mathbb{Z}_n| = n = \#\{0, 1, 2, \ldots, n-1\}$

$|\mathbb{Z}| = \infty$ $\mathbb{Z}$ is an infinite group

(b) $R_{90} \in D_4$

$ord(R_{90}) = 4$

$R_{90} \neq id = R_0$

$R_{90}^2 = R_{180} \neq id$

$R_{90}^3 = R_{270} \neq id$

$R_{90}^4 = R_{360} = id$

$\Big\}$ $ord(R_{90}) = 4$

$G = \mathbb{Z}_6$

$\text{ord}(4) = ?$

$4 \bmod 6 \neq 0$

$4+4 = 8 \bmod 6 = 2 \neq 0$

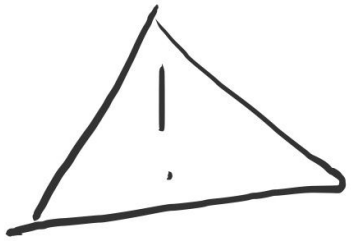
$4+4+4 = 12 \bmod 6 = 0$

recall: $\text{ord}(4) = 3$ in $\mathbb{Z}_6$

Remark: For general statements, we usually use multiplicative notation.
Sometimes we use additive notation, often for abelian groups, in particular for $\mathbb{Z}_n$

translation table

multipl.		addition
ab	$\longleftrightarrow$	$a+b$
a^n	$\longleftrightarrow$	na
a^{-1}	$\longleftrightarrow$	$-a$



Warning:

$a^n = e$ does NOT necessarily mean $\text{ord}(a) = n$

eg. if $a^n = e$ then also $a^{2n} = e$

We have the following lemma:

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

Proof. Let $\text{ord}(a) = n$

n