Last class:

$D_4$ symmetries of a square group with 8 elements:
4 rotations & 4 reflections.

Similarly, can define the dihedral group $D_n$:
$= \text{symmetries of a regular } n\text{-gon}$
It has $2n$ elements, $n$ rotations and $n$ reflections.

$n=3$

$n=5$

Symmetries of regular pentagon
Demain: The dihedral groups $D_n$ are not Abelian for $n \geq 3$.

e.g. for $n=4$: check: $S$ reflect in a main diagonal

\[ SR_{90} = R_{270} S + R_{90} S \]

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 multiplication mod n.
   Identity element: 1
   Problematic: inverses do not always exist!
   e.g. $0 \cdot a \mod n = 0 \neq 1$ for all integers $a$

   if $n=4$: also 2 does not have an inverse mod 4
   because $2 \cdot 1 = 2$
   $2 \cdot 2 \mod 4 = 4 \mod 4 = 0$
   $2 \cdot 3 \mod 4 = 6 \mod 4 = 2$
   $4 \cdot 4 \mod 4 = 16 \mod 4 = 0$
Lemma  \( \text{let } n > 0 \)

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

proof

Recall: \( \exists \) integers \( s \) and \( t \) such that

\[ \gcd(a, n) = sa + tn \]

\[ \implies 1 = \gcd(a, n) = sa + tn \]

\[ \implies sa = 1 - tn \]

\[ \implies sa \mod n = 1 \]

\[ \implies s \text{ is the inverse of } a \mod n \]

\[ \implies s \text{ is the inverse of } a \mod n \]

\[ \text{i.e. } sa \mod n = 1 \]

\[ \implies sa - 1 = \text{multiple of } n \]

\[ \implies sa - 1 = tn \text{ for some int. } t \implies sa - tn = 1 \]
\[ \Rightarrow \gcd(a, n) = 1. \]

**Def.** The group \( \mathcal{U}(n) \) is given by
\[ \{ r \mid 1 \leq r \leq n, \gcd(r, n) = 1 \} \]
with multiplication mod \( n \).

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

---

**General result:**

**Theorem** \( a, b \in \mathcal{U}(n) \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \)

**Proof.** By uniqueness of inverse, it suffices to check
\[(ab)(b^{-1}a^{-1}) = e \]
which holds since
\[(ab)(b^{-1}a^{-1}) = a(b b^{-1}) a^{-1} = a e a^{-1} = aa^{-1} = e \]

and \((b^{-1}a^{-1})(ab) = e\).
Ch 3:

Def. 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).

5. The order of an element $a \in G$, $\text{ord}(a)$, is the smallest positive integer $n$ such that $a^n = e$ or if no such $n$ exists, it is $\infty$. (book 10.1)
Examples:

@ \left| \text{D}_4 \right| = 8

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

\left| \mathbb{Z} \right| = \infty \quad \mathbb{Z} \text{ is an infinite group}

b) \quad R_{90} \leq \text{D}_4

\text{ord} \left( R_{90} \right) = 4

\begin{align*}
R_{90} + \text{id} &= R_0 \\
R_{90}^2 &= R_{180} + \text{id} \\
R_{90}^3 &= R_{270} + \text{id} \\
R_{90}^4 &= R_{360} = \text{id}
\end{align*}

\text{ord} \left( R_{90} \right) = 4
\[ G = \mathbb{Z}_6 \]

\[ \text{ord}(4) = ? \]

\[ 4 \mod 6 \neq 0 \]
\[ 4 + 4 = 8 \mod 6 = 2 \neq 0 \]
\[ 4 + 4 + 4 = 12 \mod 6 = 0 \]

**Result:** \[ \text{ord}(4) = 3 \text{ in } \mathbb{Z}_6 \]

**Remark:** For general statements, we usually use multiplicative notation. Sometimes we use additive notation, often for abelian groups, in particular for \( \mathbb{Z}_n \).
Warning: \( a^m = e \) does not necessarily mean \( \text{ord}(a) = m \).

E.g., if \( a^n = e \), then also \( a^{2n} = e \).

We have the following lemma:

Lemma: If \( a^m = e \), then \( \text{ord}(a) \mid m \).

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