main topic of course: groups

set $G$ with binary operation $(g,h) \in G \times G \to gh \in G$ satisfying

- associativity
- existence of identity element, $e$
- existence of inverse for each element $a \in G$

i.e. $\exists b \text{ s.t. } ab = ba = e$

have seen: identity elem. and inverse elem. are unique.

Examples

1. $\mathbb{Z}$ integers with addition
2. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with $\text{“}$ mod $n$
3. $\mathbb{U}(n) = \{0 < j < n, \gcd(j, n) = 1\}$, multiplicative mod $n$.
4. $\mathbb{GL}(2, \mathbb{R}) = \text{real 2x2 matrices } A \text{ with } \det(A) \neq 0$

necessary for finding inverse.
On dihedral group
symmetries of regular \( n \)-gon.
e.g. \( n = 6 \), hexagon

\[
6 \quad \text{rotations by angles } \frac{j \cdot 2\pi}{6} \quad (\text{or } j:60^\circ)
\]

\( j = 0 \): identity element  \( 0 \leq j < 6 \)

6 different reflections: of the form \( SR_j \),  \( 0 \leq j < 6 \)

S a fixed reflection.
Crucial observation: (check via geometry)

\[ SR^j S = R^{-j} \]

(for e.g. \( S \) = reflection at vertical axis)

\[ S_m = \text{group of all permutations of } \{1, 2, ..., n\} \]

operation: concatenation of maps

cycle notation: \((134)(26)\) stands for map

1 \(\rightarrow\) 3
3 \(\rightarrow\) 4
4 \(\rightarrow\) 1
2 \(\rightarrow\) 6
6 \(\rightarrow\) 2
5 \(\rightarrow\) 5

A number which does not appear is mapped to itself. (e.g. here: 5)
Remark: If $ab = ba$ for all $a, b$ in $G$, $G$ is called an abelian group.

We have seen: $\mathbb{Z}, \mathbb{Z}_n, \mathbb{U}(n)$ abelian groups.

On, $C_2(2, \mathbb{R})$, $S_n$, $n > 2$ not abelian groups.

E.g. in $S_3$:

\[(12)(23) = (123)\]
\[(23)(12) = (132)\]
Subgroups

Subgroup test:

1. $HCG$ is a subgroup if $h, k \in H \implies hk \in H$ for all $h, k \in H$.
2. $h \in H \implies h^{-1} \in H$ for all $h \in H$.

Cyclic subgroup:

If $a \in G$, $\langle a \rangle = \{a^j, j \in \mathbb{Z} \}$ is called the cyclic subgroup generated by $a$.

$\text{ord}(a) = \begin{cases} \text{smallest positive integer } n \text{ s.t. } a^n = e & \text{if } a^n \neq e \text{ for all } n > 0 \\ \infty & \text{if } a^n = e \text{ for all } n > 0 \end{cases}$

$\text{ord}(a) = 1 \langle a \rangle = \# \text{elements in } \langle a \rangle$. 
Lemma: \[ a^m = e \Rightarrow \text{ord}(a) \mid m \]

Can generalize notation \(<a>\) to more than one element.

Def. if \(a, b \in G\) then \(<a, b>\) = smallest subgroup of \(G\) which contains both \(a\) and \(b\).

(can be generalized to more than two elements)

Example: If \(m, n \in \mathbb{Z}\), \(<mn> = <x>\)

for some number \(x \in \mathbb{Z}\).

(reason: \(\mathbb{Z}\) is cyclic \(\Rightarrow\) any subgroup is cyclic)

Theorem i.e. of the form \(<x>\)

\(x = 2\)

(e.g. calculate \(x\) s.t. \(<x> = <4, 6>\)
Theorem \( \langle n, m \rangle = \langle d \rangle \), where \( d = \gcd(n, m) \)

Proof. "c" \( d|n \Rightarrow n = kd \) for some \( k \)
\[ \Rightarrow n \in \langle d \rangle \Rightarrow \langle n \rangle \subseteq \langle d \rangle \]

same way show that \( m \in \langle d \rangle \Rightarrow \langle m \rangle \subseteq \langle d \rangle \)

"c" need to show that \( d \in \langle n, m \rangle \)

Crucial Fact: There exist \( s \) and \( t \) s.t.
\[ d = sn + tm \in \langle n, m \rangle \]
\[ \Rightarrow \langle d \rangle \subseteq \langle n, m \rangle \]

Example. \( \langle 56, 84 \rangle \subseteq \langle 28 \rangle \)
\[ \gcd(56, 84) = 28 \]
Facts about $a^n$, if $\text{ord}(a) = n$.

**Theorem.** $\langle a^n \rangle = \langle a^{\text{gcd}(k,n)} \rangle$

- $\text{ord}(a^n) = \frac{n}{\text{gcd}(n,k)}$

Can calculate $\# \{ b \in \langle a \rangle, \text{ord}(b) = d \}$

**Result:**
- 0 elements if $d \nmid n$
- $\phi(d)$ elements, where $\phi(d) = \# \{ 1 \leq j < d, \text{gcd}(j,d) = 1 \}$

Properties of $\phi$:
- $\phi(p^k) = (p-1)p^{k-1}$ if $p$ a prime number
- $\phi(nm) = \phi(n)\phi(m)$ if $\text{gcd}(n,m) = 1$