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 elem. $a \in G$

i.e. $\exists\, b$ s.t. $ab = ba = e$

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

Examples (1) $\mathbb{Z}$ integers with addition

(2) $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with "mod n"

(3) $U(n) = \{0 < j < n,\ \gcd(j,n) = 1\}$, multiple. mod n.

necessary for finding inverse

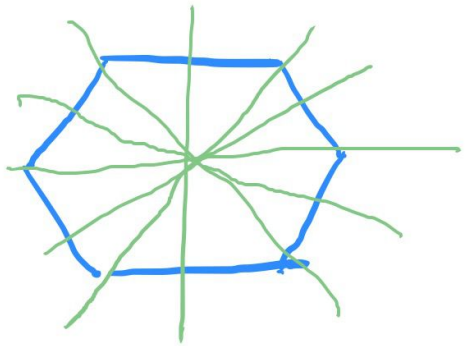
(4) $GL(2, \mathbb{R})$ = real 2×2 matrices A with $\det(A) \neq 0$

Operation: matrix multiplication.

(5) D_n dihedral group

symmetries of regular n-gon.

e.g. $n=6$. hexagon



possible axes for reflections

D_n has $2n$ elements. n rotations

n reflections

for $n=6$: • 6 rotations by angles $\frac{j2\pi}{6}$ (or $j:60°$)

$j=0$: identity element $0 \leq j < 6$

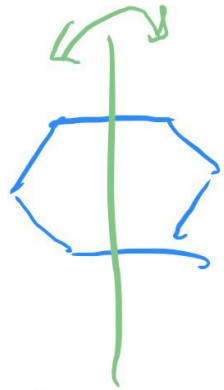
• 6 different reflections: of the form SR^j, $0 \leq j < 6$

S a fixed reflection.

Crucial observation: (check via geometry)

$$SR^jS = R^{-j}$$

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



(6) S_n = group of all permutations of $\{1, 2, \ldots, n\}$

operation: concatenation of maps

cycle notation. $(134)(26)$ stands for map

$1 \to 3$
$3 \to 4$
$4 \to 1$
$2 \to 6$
$6 \to 2$
$5 \to 5$

↖ 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

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

D_n, $GL(2, \mathbb{R})$, S_n, $n > 2$ not abelian groups

e.g. in S_3

$$(12)(23) = (123)$$

$$(23)(12) = (132)$$

Subgroups

subgroup test: $H \subset G$ is a subgroup if

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

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

cyclic subgroup: $a \in G$

$\langle a \rangle = \{a^j, j \in \mathbb{Z}\}$ is called the

cyclic subgroup generated by a

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

$\text{ord}(a) = |\langle a \rangle| = \#\text{elements in } \langle a \rangle.$

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

Can generalize notation $\langle a \rangle$ to more than one element

Def. If $a, b \in G$ then $\langle a, b \rangle$ = smallest subgroup of G which contains both a and b.

(can be generalized to more than two elements)

Example: If $n, m \in \mathbb{Z}$, $\langle n, m \rangle = \langle x \rangle$ for some number $x \in \mathbb{Z}$

(reason: $\mathbb{Z}$ is cyclic $\xrightarrow{\text{Theorem}}$ any subgroup is cyclic i.e. of the form $\langle x \rangle$)

$x = ?$ (e.g. calculate x s.t. $\langle x \rangle = \langle 4, 6 \rangle$)

Theorem $\langle n, m \rangle = \langle d \rangle$, where $d = \gcd(n, m)$

Proof. "$\subseteq$" $d \mid n \Rightarrow n = kd$ for some k

$\Rightarrow n \in \langle d \rangle \Rightarrow \langle n \rangle \subseteq \langle d \rangle$

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

"$\supseteq$" 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- $\langle 56, 84 \rangle \stackrel{?}{=} \langle 28 \rangle$

$\gcd(56, 84) = 28$

Facts about a^k, if $\text{ord}(a) = n$.

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

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

result:
- 0 elem. if $d \nmid n$
- $\phi(d)$ elements,

where $\phi(d) = \#\{0 < j < d, \ \gcd(j,d) = 1\}$

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