Subgroups of cyclic groups.

Every cyclic group is isomorphic to $(\mathbb{Z},+)$ or $(\mathbb{Z}_n,+)$ for some $n\in\mathbb{N}$.

See previous lecture notes for results on subgroups of $\mathbb{Z}$.

Consider now the case of $\mathbb{Z}_n$. If $[b]\in\mathbb{Z}_n$, $\langle[b]\rangle=\{[kb] \mid k\in\mathbb{Z}\}$

<u>Proposition</u>: Let $n\in\mathbb{N}$, $b\in\mathbb{Z}\setminus\{0\}$, $d=\gcd(b,n)$. Then in $\mathbb{Z}_n$,
① $\langle[b]\rangle=\langle[d]\rangle$
② $o([b])=n/d$

In particular $[b]$ generates $\mathbb{Z}_n$ iff $o([b])=n$
iff $d=\gcd(b,n)=1$.

<u>Proof</u>: ① Can write $d=sb+tn$ for some $s,t\in\mathbb{Z}$, so

$[d]=[sb]\in\mathbb{Z}_n$. Thus $[d]\in\langle[b]\rangle$ so $\langle[d]\rangle\subseteq\langle[b]\rangle$
On the other hand, since $d|b$, $b=kd$ so $[b]=[kd]\in\langle[d]\rangle$
Hence $\langle[b]\rangle\subseteq\langle[d]\rangle$. Thus $\langle[b]\rangle=\langle[d]\rangle$

② Since $\langle[b]\rangle=\langle[d]\rangle$, $o([b])=o([d])$.
Now $o([d])$ is the smallest positive k such that $n|kd$. On the other hand $d|n$, and $n=(\frac{n}{d})d$.
So the smallest multiple that divides n is $(\frac{n}{d})d$, and $o([d])=\frac{n}{d}$.

This gives a good picture of the cyclic subgroups of $\mathbb{Z}_n$. In fact, every subgroup of $\mathbb{Z}_n$ is cyclic.

<u>Proposition</u> Let $H \leq \mathbb{Z}_n$. Either $H = \{[0]\}$ or There is d $1 \leq d \leq n-1$ such that $H = \langle [d] \rangle$

In the latter case, the smallest such d has $|H| = \frac{n}{d}$

<u>Proof</u>: Suppose $H \neq \{[0]\}$, Let $d \in \{1, \ldots, n-1\}$ be the smallest element such that $[d] \in H$.
Then $\langle [d] \rangle \leq H$.

Now take any $[b] \in H$. Write $b = kd + r$ $0 \leq r < d$ then $[r] \overset{?}{=} [b] - k[d] \in H$. Since $0 \leq r < d$, we must have $r = 0$, or else r is a smaller number than d with $[r] \in H$, contradicting minimality of d.

Thus $b = kd$ so $[b] \in \langle [d] \rangle$. Since $[b] \in H$ was arbitrary, $H \leq \langle [d] \rangle$. Thus $H = \langle [d] \rangle$.

Lastly, we must show $|H| = \frac{n}{d}$. Set $d' = \gcd(d,n)$.
By previous proposition $\langle [d'] \rangle = \langle [d] \rangle = H$, so $[d'] \in H$.
But $1 \leq d' \leq d$, and d was chosen to be smallest so that $[d] \in H$. Thus $d' = d$, so $\gcd(d,n) = d$, $d \mid n$, and $|H| = |\langle [d] \rangle| = \frac{n}{d}$. $\blacksquare$

Corollary Fix $n \geq 2$. Any subgroup of $\mathbb{Z}_n$ is cyclic with order dividing n.
For each divisor q of n, $q | n$, there is a unique subgroup of order q, namely $\langle [\frac{n}{q}] \rangle$
For subgroups $H_1, H_2 \leq \mathbb{Z}_n$

$$H_1 \leq H_2 \iff |H_1| \,\big|\, |H_2| ..$$

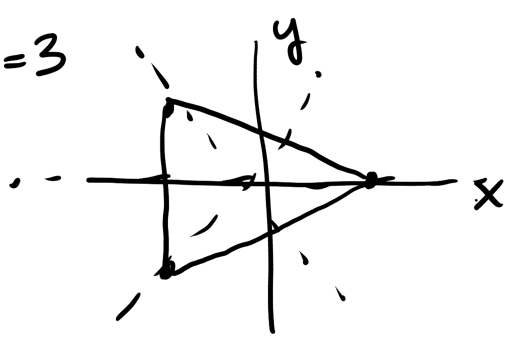
Example Subgroup lattice of $\mathbb{Z}_{12}$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & & \\
\langle[2]\rangle \arrow[d, dash] \arrow[dr, dash] & & \langle[3]\rangle \arrow[dl, dash] \\
\langle[4]\rangle \arrow[dr, dash] & \langle[6]\rangle \arrow[d, dash] & \\
 & \{[0]\} &
\end{tikzcd}
\qquad
\begin{array}{c}\text{orders}\end{array}
\begin{tikzcd}[column sep=small]
 & 12 \arrow[dl, dash] \arrow[dr, dash] & \\
6 \arrow[d, dash] \arrow[dr, dash] & & 4 \arrow[dl, dash] \\
3 \arrow[dr, dash] & 2 \arrow[d, dash] & \\
 & 1 &
\end{tikzcd}$$

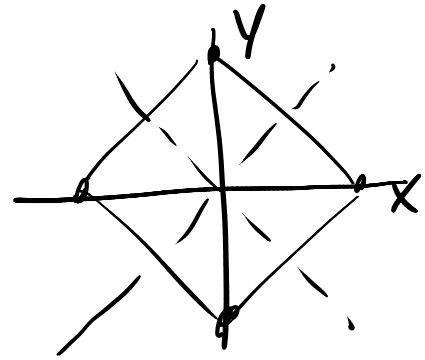
Dihedral groups Another class of groups.
They are not isomorphic to cyclic groups.
They are not commutative (ab may not $= ba$).

D_n = the group of symmetries of the regular n-gon.

$n=3$



$n=4$



To be specific, we assume the vertices of the n-gon are

$$\left(\cos\frac{2\pi k}{n},\ \sin\frac{2\pi k}{n},\ 0\right) \quad (k=0,\dots,n-1)$$

Let r_θ be the rotation through angle θ about z-axis.
Let j_θ be rotation by π about the line in the xy-plane that makes angle θ with x-axis.
We call r_θ a rotation, and j_θ a flip.

The symmetries of the n-gon are

r_θ for $\theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \dots, \frac{2\pi(n-1)}{n}$

and j_θ for $\theta = 0, \frac{\pi}{n}, \frac{2\pi}{n}, \dots, \frac{(n-1)\pi}{n}$.

I.e. $D_n = \{ r_{\frac{2\pi k}{n}}, j_{\frac{\pi k}{n}} \mid k = 0, 1, \dots, n-1 \}$.

On homework you are asked to verify $j_\phi r_\theta = r_{-\theta} j_\phi$

we also have $r_\theta r_\phi = r_{\theta+\phi}$ and $j_\theta^2 = e = r_0$

$r_{2\pi} = r_0 = e$

These facts let us deduce other equations in D_n
such as $r_\theta^{-1} = r_{-\theta}$, $j_\theta^{-1} = j_\theta$, $r_\theta j_\phi r_{-\theta} = j_{\phi+\theta}, \dots$

<u>Note</u> Even though there is no "2-gon", the pattern can be extended to $n=2$:

$D_2 = \{ e, r_\pi, j_0, j_{\pi/2} \} \cong$ symmetries of rectangle.

Now fix $n \geq 2$. Set $j = j_0$ and $r = r_{2\pi/n}$
Then we can write

$$D_n = \{e, r, \ldots, r^{n-1}, j, rj, r^2 j, \ldots, r^{n-1} j\}$$

Thus $|D_n| = 2n$.

Observe $C_n = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\} \leq D_n$ is cyclic $C_n \cong \mathbb{Z}_n$.

<u>Proposition</u> Let $n \geq 2$ and $H \leq D_n$. Then either
(i) $H \cong \mathbb{Z}_k$ where $k | n$ or
(ii) $H \cong D_k$ where $k | n$.
Moreover, all of these types of subgroups exist.

<u>Proof</u> Let $H_0 = H \cap C_n$. This is subgroup of cyclic group $\langle r \rangle$ so by classification of subgroups of cyclic groups,

$H_0 = \langle r^d \rangle$ for some $d | n$. Write $n = kd$:

$$H_0 = \{e, r^d, \ldots, (r^d)^{k-1}\} \qquad |H_0| = k$$

$H_0 \cong \mathbb{Z}_k$.

If $H = H_0$, we are done. If not, $H \setminus H_0$ consists of flips

$$H \setminus H_0 = \{ j_{\theta_0}, j_{\theta_1}, \ldots, j_{\theta_{\ell-1}} \} \qquad 0 \leq \theta_0 < \theta_1 < \cdots < \theta_{\ell-1} < \pi$$

Now $j_{\theta_i} j_{\theta_0} = r_{2(\theta_i - \theta_0)} \in H \cap C_n = H_0$

Thus the function $R_{j_{\theta_0}} : H \setminus H_0 \to H_0$ maps $H \setminus H_0$ into H_0

Since $R_{j_{\theta_0}}$ is injective, $|H \setminus H_0| \leq |H_0|$.

On the other hand $R_{j\theta_0}: H_0 \to H \setminus H_0$ ($j\theta_0 r^s$ is a flip)

so $|H_0| \leq |H \setminus H_0|$, and $|H_0| = |H \setminus H_0|$,
and $R_{j\theta_0}$ is a bijective function $H_0 \to H \setminus H_0$

Thus $H = \{e, r^d, \ldots, (r^d)^{k-1}, j\theta_0, r^d j\theta_0, \ldots, (r^d)^{k-1} j\theta_0\}$

or $H = \{ r_{\frac{2\pi i}{k}}, r_{\frac{2\pi i}{k}} j\theta_0 \mid i = 0, 1, \ldots, k-1 \}$

Now $D_k = \{ r_{\frac{2\pi i}{k}}, r_{\frac{2\pi i}{k}} j_0 \mid i = 0, 1, \ldots, k-1 \}$

Define $\varphi: H_0 \to D_k$ by

$$\varphi(a) = r_{-\theta_0} a r_{\theta_0}$$

Then $\left.\begin{cases} \varphi(r_{\frac{2\pi i}{k}}) = r_{\frac{2\pi i}{k}} \\ \varphi(r_{\frac{2\pi i}{k}} j\theta_0) = r_{\frac{2\pi i}{k}} j_0 \end{cases}\right\}$ so φ is bijective.

Also $\varphi(ab) = r_{-\theta_0} ab\, r_{\theta_0} = r_{-\theta_0} a\, r_{\theta_0} r_{-\theta_0} b\, r_{\theta_0} = \varphi(a)\varphi(b)$

so φ is an isomorphism.

Existence is an exercise.