Subgroups of cyclic groups

Let $G = \langle a \rangle$. We know that every subgroup of G is cyclic (Lecture 11).

So if $H \leq G$, then $H = \langle a^k \rangle$ for some $k \in \mathbb{Z}$. We also know the order of a^k (Lecture 12).

In combination, we get a full classification.

Thm: Let $G = \langle a \rangle$ be a cyclic group.

1. If $|a| = \infty$, then $\langle a^k \rangle = \langle a^\ell \rangle$ if and only if $k = \pm \ell$.

   Hence, a complete list of subgroups of G is $\{e\} = \langle a^0 \rangle$, $G = \langle a^1 \rangle$, $\langle a^2 \rangle$, $\langle a^3 \rangle$, ...

2. If $|a| = n \in \mathbb{N}$, then for each positive divisor $d \mid n$, there is a unique subgroup of G of order d, namely $\langle a^{n/d} \rangle$.

Moreover, these are all subgroups of G, since $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$ for all $k \in \mathbb{Z}$.

<u>Proof</u>: ① Suppose $|a| = \infty$ and $\langle a^k \rangle = \langle a^l \rangle$ for some $k, l \in \mathbb{Z}$.

Then $a^k \in \langle a^l \rangle$, so

$$a^k = (a^l)^m = a^{lm}$$

for some $m \in \mathbb{Z}$. Since $|a| = \infty$, this implies $k = lm$, so $l \mid k$.

By identical reasoning, $k \mid l$ also. Thus, $k = \pm l$.

✓

② Now, suppose $|a| = n$ and $d \mid n$. Since $\gcd(\frac{n}{d}, n) = \frac{n}{d}$, we have

$$|\langle a^{n/d} \rangle| = |a^{n/d}| = \frac{n}{(n/d)} = d,$$

proving existence.

For uniqueness, suppose $H \leq G$ and $|H| = d$. Since H is cyclic, $H = \langle a^k \rangle$ for some integer k.

Now,

$$d = |H| = |a^k| = \frac{n}{\gcd(n,k)},$$

so $\gcd(n,k) = \frac{n}{d}$. In particular, $\frac{n}{d}$ divides k, so $x^k \in \langle x^{n/d} \rangle$.

Hence,

$$\langle x^k \rangle \leq \langle x^{n/d} \rangle.$$

Since these subgroups have the same (finite) order, we have $\langle x^k \rangle = \langle x^{n/d} \rangle$.

Finally, for any $k \in \mathbb{Z}$, the equation

$$|a^k| = \frac{n}{\gcd(k,n)}$$

shows that $|a^k|$ is a divisor of n.

Hence, by uniqueness, $\langle a^k \rangle = \langle a^{n/|a^k|} \rangle$

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

∎

Ex: $\mathbb{Z}$ is an infinite cyclic group, so its subgroups are

$$\{0\} = \langle 0 \rangle$$

$$\mathbb{Z} = \langle 1 \rangle$$

$$2\mathbb{Z} = \langle 2 \rangle$$

$$3\mathbb{Z} = \langle 3 \rangle$$

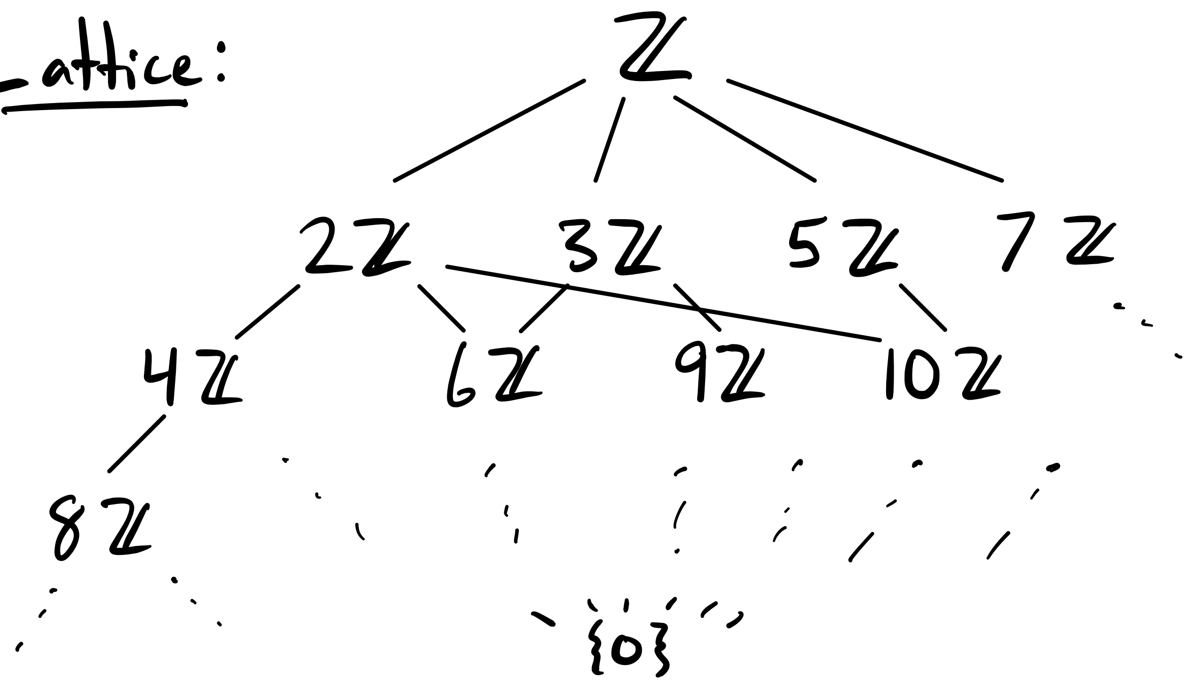
$$\vdots$$

$$k\mathbb{Z} = \langle k \rangle$$

$$\vdots$$

$$\boxed{k\mathbb{Z} \le l\mathbb{Z} \iff l \mid k}$$

Lattice:



$\underline{\text{Ex}}$: $\mathbb{Z}_{20}$. Divisors of 20 are 1, 2, 4, 5, 10, 20, so the subgroups are

- $\langle \frac{20}{1} \rangle = \langle 20 \rangle = \langle 0 \rangle = \{0\}$
- $\langle \frac{20}{2} \rangle = \langle 10 \rangle$
- $\langle \frac{20}{4} \rangle = \langle 5 \rangle = \langle 15 \rangle$
- $\langle \frac{20}{5} \rangle = \langle 4 \rangle = \langle 8 \rangle = \langle 12 \rangle = \langle 16 \rangle$
- $\langle \frac{20}{10} \rangle = \langle 2 \rangle = \langle 6 \rangle = \langle 14 \rangle = \langle 18 \rangle$
- $\langle \frac{20}{20} \rangle = \langle 1 \rangle = \mathbb{Z}_{20} = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$
  $= \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$

$$\boxed{\begin{aligned} \langle \tfrac{20}{d_1} \rangle \leq \langle \tfrac{20}{d_2} \rangle \quad &\Leftrightarrow \quad d_1 \mid d_2 \\ &\Leftrightarrow \quad \tfrac{20}{d_2} \,\Big|\, \tfrac{20}{d_1} \end{aligned}}$$

__Lattice__:

$$\begin{tikzcd}
 & & \mathbb{Z}_{20} = \langle 1 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle 2 \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 5 \rangle \arrow[dl, dash] \\
\langle 4 \rangle \arrow[dr, dash] & & \langle 10 \rangle \arrow[dl, dash] & \\
 & \langle 20 \rangle = \{0\} & &
\end{tikzcd}$$

Corresponds to the divisor lattice

$$\begin{tikzcd}
 & & 20 \arrow[dl, dash] \arrow[dr, dash] & \\
 & 10 \arrow[dl, dash] \arrow[dr, dash] & & 4 \arrow[dl, dash] \\
5 \arrow[dr, dash] & & 2 \arrow[dl, dash] & \\
 & 1 & &
\end{tikzcd}$$