**HW 4.8.:** $|G| = p^n$, pick $g \in G$, $\langle g \rangle$ is a subgroup of $G$. By Lagrange's Theorem,

$|\langle g \rangle| \mid |G| = p^n$, so $|\langle g \rangle| = p^k$ for some $k \in \mathbb{Z}^+$.

So $g^{p^k} = 1$. Can we now find an element of order $p$?

$$\left(g^{p^{k-1}}\right)^p = g^{p^{k-1} \cdot p} = g^{p^k} = 1.$$

**HW 4.5.:** By the classification of cyclic groups, $G = \mathbb{Z}$ or $G = \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}^+$.

$G = \mathbb{Z}$. $\mathrm{Aut}(\mathbb{Z}) = \{\varphi : \mathbb{Z} \to \mathbb{Z} \text{ group isomorphism}\}$

$\varphi \in \mathrm{Aut}(\mathbb{Z})$ is completely determined by $\varphi(1)$. Namely if $x \in \mathbb{Z}$, then

$$\varphi(x) = \varphi(1 + \overset{x}{\cdots} + 1) = \varphi(1) + \overset{x}{\cdots} + \varphi(1) = x \cdot \varphi(1)$$

Since $1$ is a unit in $\mathbb{Z}$, and $\varphi$ is a bijection: for every $y \in \mathbb{Z}$ we

have to find $x \in \mathbb{Z}$ with $x \cdot \varphi(1) = \varphi(x) = y$ (for $\varphi$ to be surjective).

Then we need $\varphi(1)$ to have a multiplicative inverse. So $\varphi(1)$ must be

$-1$ or $1$. Our candidate is $\{-1, 1\}$.

$$\begin{aligned}
\mathrm{Aut}(\mathbb{Z}) &\xrightarrow{\quad f \quad} \{-1,1\} \\
\varphi &\longmapsto \varphi(1) \\
\begin{pmatrix} \varphi_a : \mathbb{Z} \to \mathbb{Z} \\ 1 \mapsto a \end{pmatrix} &\xleftarrow{\quad g \quad} a
\end{aligned}$$

We want this to be a group isomorphism, so:

$f, g$ must be group homomorphisms and

$fg = \mathrm{id}_{\{-1,1\}}$, $gf = \mathrm{id}_{\mathrm{Aut}(\mathbb{Z})}$.

Note: $\{-1,1\} \cong \mathbb{Z}/2\mathbb{Z} \cong \langle b \mid b^2 = 1\rangle$

Check: $f$ is group homomorphism. If $\varphi, \phi \in \mathrm{Aut}(\mathbb{Z})$, then

$$f(\varphi\circ\phi) = \varphi\circ\phi(1) = \varphi(\phi(1)) \underset{\uparrow}{=} \phi(1)\cdot\varphi(1) = \varphi(1)\cdot\phi(1) = f(\varphi)\cdot f(\phi).$$

$\varphi(x) = x\cdot\varphi(1)$

$$g(a\cdot b) = \varphi_{ab} = \varphi_a\circ\varphi_b = g(a)\circ g(b).$$

$$\begin{aligned} \varphi_{ab} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto ab \end{aligned} \qquad \begin{aligned} \varphi_a\circ\varphi_b : \mathbb{Z} \xrightarrow{\varphi_b} &\mathbb{Z} \xrightarrow{\varphi_a} \mathbb{Z} \\ 1 \longmapsto &b \\ &1 \longmapsto a \\ 1 \longmapsto &b \longmapsto b\cdot a = ab \end{aligned}$$

$\varphi_a(b) = b\cdot\varphi_a(1) = b\cdot a$

$$fg(a) = f(\varphi_a) = \varphi_a(1) = a$$

$$gf(\varphi) = g(\varphi(1)) = \varphi_{\varphi(1)} = \varphi$$

$$\begin{aligned} \varphi_{\varphi(1)} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto \varphi(1) \end{aligned} \quad \text{is equal to} \quad \begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto \varphi(1) \end{aligned}$$

So $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

$G \cong \mathbb{Z}/m\mathbb{Z}$: Take $\varphi \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$, it is determined by $\varphi(\bar{1})$, namely

$\varphi(\bar{x}) = \varphi(\overbrace{\bar{1}+\cdots+\bar{1}}^{x}) = \bar{x}\cdot\varphi(\bar{1})$. We need $\varphi$ to be injective, surjective,

and invertible. Not all $\varphi(\bar{1}) \in \mathbb{Z}/m\mathbb{Z}$ will give $\varphi \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.

The inverse $\varphi^{-1}$ satisfies $\bar{x} = \varphi^{-1}\circ\varphi(\bar{x}) = \varphi^{-1}(\bar{x}\cdot\varphi(\bar{1})) = \bar{x}\cdot\varphi(\bar{1})\cdot\varphi^{-1}(\bar{1})$.

So $\varphi(\bar{1})\cdot\varphi^{-1}(\bar{1}) \equiv 1 \mod m$.

Recall that $x\cdot y \equiv 1 \mod m$ if and only if $x$ is coprime with $m$.

($x, m$ are coprime if and only if $1 = xy + mn$ for some $y, n \in \mathbb{Z}$)

$$\begin{array}{ccc} \mathrm{Aut}(\mathbb{Z}_m) & \xrightarrow{\quad f \quad} & (\mathbb{Z}/m\mathbb{Z})^\times \\ \varphi & \longmapsto & \varphi(\bar{1}) \\ \left(\begin{array}{l}\varphi_a : \mathbb{Z}_m \to \mathbb{Z}_m \\ \quad \bar{1} \mapsto \bar{a}\end{array}\right) & \xleftarrow{\quad g \quad} & \bar{a} \end{array}$$

We want this to be a group isomorphism, so:

$f, g$ must be group homomorphisms and

$a$ coprime with $m$.

$fg = \mathrm{id}_{(\mathbb{Z}/m\mathbb{Z})^\times}$, $gf = \mathrm{id}_{\mathrm{Aut}(\mathbb{Z}_m)}$.

Note: the coprime elements to $m$ are exactly $(\mathbb{Z}/m\mathbb{Z})^\times$.

Check: $f$ is group homomorphism. If $\varphi, \phi \in \mathrm{Aut}(\mathbb{Z}_m)$, then

$$f(\varphi\circ\phi) = \varphi\circ\phi(1) = \varphi(\phi(\bar{1})) \underset{\varphi(\bar{x}) = \bar{x}\cdot\varphi(\bar{1})}{=} \phi(\bar{1})\cdot\varphi(\bar{1}) = \varphi(\bar{1})\cdot\phi(\bar{1}) = f(\varphi)\cdot f(\phi).$$

$$g(\bar{a}\cdot\bar{b}) = g(\overline{a\cdot b}) = \varphi_{ab} = \varphi_a\circ\varphi_b = g(\bar{a})\circ g(\bar{b}).$$

$$\begin{array}{l} \varphi_{ab} : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m \\ \qquad \bar{1} \longmapsto \overline{ab} \end{array}$$

$$\begin{array}{l} \varphi_a\circ\varphi_b : \mathbb{Z}_m \xrightarrow{\varphi_b} \mathbb{Z}_m \xrightarrow{\varphi_a} \mathbb{Z}_m \\ \qquad \bar{1} \longmapsto \bar{b} \\ \qquad\qquad\quad 1 \longmapsto \bar{a} \\ \qquad \bar{1} \longmapsto \bar{b} \longmapsto \bar{b}\cdot\bar{a} = \overline{ab} \end{array}$$

$$\varphi_a(\bar{b}) = \bar{b}\cdot\varphi_a(\bar{1}) = \bar{b}\cdot\bar{a}$$

$$fg(\bar{a}) = f(\varphi_a) = \varphi_a(\bar{1}) = \bar{a}$$

$$gf(\varphi) = g(\varphi(\bar{1})) = \varphi_{\varphi(\bar{1})} = \varphi$$

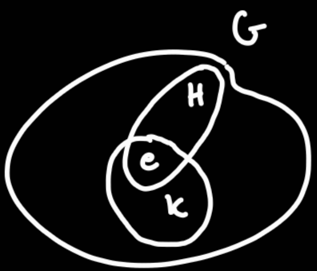
$$\varphi_{\varphi(\bar{1})}: \mathbb{Z}_m \longrightarrow \mathbb{Z}_m \quad \text{is equal to} \quad \varphi: \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$$
$$1 \longmapsto \varphi(\bar{1}) \qquad\qquad\qquad 1 \longmapsto \varphi(\bar{1})$$

So $\mathrm{Aut}(\mathbb{Z}_m) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$.

(*) $\varphi_a : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$, $\bar{1} \longmapsto \bar{a}$ has to be invertible. It has inverse $\varphi_b : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$

with $\bar{a} \cdot \bar{b} \equiv \bar{1}$ mod $m$. (of course, it has to be a group homomorphism)

**HW 4.9.:**




$H = \mathbb{Z}/5\mathbb{Z}$, $K = \mathbb{Z}/5\mathbb{Z}$

$e \in H \cap K$, do we have $x \in H \cap K$, $x \neq e$?

If $x \in H \cap K$, then $x \in H$ and $x \in K$.

$H = \langle a \mid a^5 = e \rangle$ so $x = a^i$ for some fixed $i \in \mathbb{Z}^+$ so $a^i = b^j$.
$K = \langle b \mid b^5 = e \rangle$ $\quad x = b^j \quad j \in \mathbb{Z}^+$

Suppose $|G| = p$ prime. Then by Lagrange's Theorem, any subgroup has order $p$ or 1. Now pick $x \in G$, $\langle x \rangle$ is a subgroup of $G$, $|\langle x \rangle| > 1$ so $|\langle x \rangle| = p$ so $x$ has order $p$.

Now: $a = a^6 = a^i \cdot a^{6-i} = b^j \cdot b^{6-j} = b^6 = b$, contradiction with $H \neq K$, so $H \cap K = \{e\}$.

If $H_1, \dots, H_8$ are different subgroups of order 5, how many different elements do we have? 4 for each, so $8 \cdot 4 = 32$, which is more than $|G| = 30$, contradiction.

So $G$ has at most 7 subgroups of order 5.