__Recall__: $H, K \leq G$, $H \cap K = \{e_G\}$. $H, K \trianglelefteq G \Rightarrow HK \cong H \times K$.
Note if only $H \trianglelefteq G$, we still have $HK \leq G$. Observe that

$$\begin{aligned} h_1 k_1 h_2 k_2 &= h_1 k_1 h_2 k_1^{-1} k_1 k_2 \\ &= \underbrace{h_1 (k_1 \cdot h_2)}_{\in H \text{ b/c } H \trianglelefteq G} k_1 k_2 \end{aligned}$$

Define $\psi: K \to \mathrm{Aut}(H)$ by $k \mapsto (\varphi(k): h \mapsto khk^{-1})$. Hence
$\mapsto k.h$
$h_1 k_1 h_2 k_2 = h_1 \varphi(k_1)(h_2) k_1 k_2$.

Our goal is to build a group G from groups H and K if we have a map $\psi: K \to \mathrm{Aut}(H)$.

__Theorem__: Let H and K be groups, $\psi: K \to \mathrm{Aut}(H)$ a homomorphism. Define $G = \{(h,k) : h \in H, k \in K\}$. Define a binary operation on G by:

$$(h_1, k_1) * (h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2).$$

We have the following:

1) This makes G into a group of order $|H| \cdot |K|$ w/ $|G| = \infty$ if $|H| = \infty$ or $|K| = \infty$.
2) Define $\tilde{H} = \{(h, e_K) : h \in H\}$ and $\tilde{K} = \{(e_H, k) : k \in K\}$. These are subgroups of G and $\tilde{H} \cong H$, $\tilde{K} \cong K$.
3) We have $\tilde{H} \trianglelefteq G$, $\tilde{H} \cap \tilde{K} = \{e_G\}$, and for every $\tilde{h} \in \tilde{H}$ and $\tilde{k} \in K$, then $\tilde{k} * \tilde{h} * \tilde{k}^{-1} = (\varphi(k)(h), e_K)$, where $\tilde{h} = (h, e_K)$ and $\tilde{k} = (e_H, k)$.

__Proof__. 1) Clearly $G \neq \emptyset$ b/c $(e_H, e_K) \in G$.
Let $(h,k) \in G$. We have

Recall $\varphi: H \xrightarrow{\cong} H$ and $\psi: K \to \mathrm{Aut}(H)$ defined by $k \mapsto (\varphi(k): H \to H)$, $h \mapsto khk^{-1}$.

$$\begin{aligned} (h,k) * (e_H, e_K) &= (h \varphi(k)(e_H), k e_K) \\ &= (h e_H, k e_K) \\ &= (h, k) \\ &= (e_{\mathrm{Aut}(H)} \cdot h, e_K \cdot k) \\ &= (e_H \varphi(e_K)(h), e_K \cdot k) \\ &= (e_H, e_K) * (h, k). \end{aligned}$$

φ is an iso., by def, identities will get mapped to identities.

$\psi: K \to \mathrm{Aut}(H)$ also an iso I think, so $e_K \mapsto e_{\mathrm{Aut}(H)}$.

Thus $e_G = (e_H, e_K)$.

For $(h,k) \in G$, we have:

$$
\begin{aligned}
(h,k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) &= (h\varphi(k)(\varphi(k^{-1})(h^{-1})), kk^{-1}) \\
&= (h(\varphi(k) \circ \varphi(k^{-1}))(h^{-1}), kk^{-1}) \\
&= (h\varphi(kk^{-1})(h^{-1}), kk^{-1}) \\
&= (h\varphi(e_K)(h^{-1}), kk^{-1}) \\
&= (hh^{-1}, e_K) \\
&= (e_H, e_K)
\end{aligned}
$$

$$
\begin{aligned}
(\varphi(k^{-1})(h^{-1}), k^{-1}) * (h,k) &= (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), k^{-1}k) \\
&= (\varphi(k^{-1})(h^{-1}h), k^{-1}k) \\
&= (\varphi(k^{-1})(e_H), k^{-1}k) \\
&= (e_H, e_K)
\end{aligned}
$$

Thus $(h,k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1})$.

Let $(h_1,k_1), (h_2,k_2), (h_3,k_3) \in G$. We have:

$$
\begin{aligned}
(h_1,k_1) * [(h_2,k_2) * (h_3,k_3)] &= (h_1,k_1) * (h_2\varphi(k_2)(h_3), k_2k_3) \\
&= (h_1\varphi(k_1)(h_2\varphi(k_2)(h_3)), k_1k_2k_3) \\
&\qquad f(a \cdot g(x)) = f(a) \cdot f(g(x)) \\
&= (h_1\varphi(k_1)(h_2)\varphi(k_1)(\varphi(k_2)(h_3)), k_1k_2k_3)
\end{aligned}
$$

$$
\begin{aligned}
[(h_1,k_1) * (h_2,k_2)] * (h_3,k_3) &= (h_1\varphi(k_1)(h_2), k_1k_2) * (h_3,k_3) \\
&= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), k_1k_2k_3) \\
&= (h_1\varphi(k_1)(h_2)\varphi(k_1)(\varphi(k_2)(h_3)), k_1k_2k_3)
\end{aligned}
$$

Thus G is a group.

2) We have $\tilde{H} \neq \emptyset$ b/c $(e_H, e_K) \in \tilde{H}$. Let $(h_1, e_K), (h_2, e_K) \in \tilde{H}$.
Observe that:

$$
\begin{aligned}
(h_1, e_K) * (h_2, e_K)^{-1} &= (h_1, e_K) * (\varphi(e_K^{-1})(h_2^{-1}), e_K^{-1}) \\
&= (h_1\varphi(e_K)(\varphi(e_K^{-1})(h_2^{-1})), e_Ke_K^{-1}) \\
&= (h_1\varphi(e_Ke_K^{-1})(h_2^{-1}), e_Ke_K^{-1}) \\
&= (h_1h_2^{-1}, e_K) \in \tilde{H}
\end{aligned}
$$

Thus $\tilde{H} \leq G$.

Define $\varphi: H \to \tilde{H}$ by (h, e_K). Let $(h, e_K) \in \tilde{H}$. Then $\varphi(h) = (h, e_K)$, hence φ is surj.
Let $\varphi(h_1) = \varphi(h_2)$. Then $(h_1, e_K) = (h_2, e_K)$; i.e., $h_1 = h_2$. Thus φ is inj.
Observe that $\varphi(h_1h_2) = (h_1h_2, e_K) = (h_1\varphi(e_K)(h_2), e_Ke_K) = (h_1, e_K) * (h_2, e_K)$
$= \varphi(h_1)\varphi(h_2)$.

Thus $H \cong \tilde{H}$.

The proof for $\tilde{K} \leq G$ and $K \cong \tilde{K}$ is identical.

3) Let $(h, e_K) \in \tilde{H}$ and $(h_1, k_1) \in G$. We have that:

$$(h_1, k_1) * (h, e_K) * (h_1, k_1)^{-1} = \dots$$
$$= (h_1 \varphi(k_1)(h) h_1^{-1}, e_K) \in H$$

showed $\tilde{h} g \tilde{h}^{-1} \in H$; i.e., normal

Thus $\tilde{H} \trianglelefteq G$.
The proof for $\tilde{K} \trianglelefteq G$ is identical.

Let $\tilde{k} = (e_H, k)$ and $\tilde{h} = (h, e_K)$. Then:

$$\tilde{k} * \tilde{h} * \tilde{k}^{-1} = (e_H, k) * (h, e_K) * (e_H, k)^{-1}$$
$$= \dots$$
$$= (\varphi(k)(h), e_K).$$

■

<u>Definition</u>: The group G is called the <u>semi-direct product</u> of H and K (with respect to φ) and denoted $H \rtimes_\varphi K$.

<u>Example</u>: Define $\varphi: K \to \mathrm{Aut}(H)$ by $k \mapsto e_{\mathrm{Aut}(H)}$. We have that $G = H \rtimes_\varphi K$ and $H \rtimes_\varphi K = H \times K$ because:

$$(h_1, k_1) * (h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2)$$
$$= (h_1 \cdot e_{\mathrm{Aut}(H)} \cdot h_2, k_1 k_2)$$
$$= (h_1 h_2, k_1 k_2).$$

<u>Proposition</u>: Let G be a cyclic group of order n. Then $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
Proof. Let $G = \langle x \rangle$ and $\varphi \in \mathrm{Aut}(G)$.
We have that $\varphi(x) = x^a$ for some $a \in \mathbb{Z}_{\geq 0}$. (Since $\varphi: G \to G$ and $G = \langle x \rangle$).
Since φ is an isomorphism, $|\varphi(x)| = |x| = |G|$.
If $|G| = n$ and $G = \langle x \rangle$, then $\langle x^a \rangle = G$ iff <u>$\gcd(a, n) = 1$</u>. Assuming this.
Hence, from $\varphi(x) = x^a$, $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.
If $\varphi(x) = x^a$, then a <u>completely</u> determines φ, and φ determines a.
So $\varphi_a \in \mathrm{Aut}(G)$, where φ_a defined by $x \mapsto x^a$.
Define $\Psi: \mathrm{Aut}(G) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ by $\varphi_a \longmapsto [a]_n$.
This is well-defined b/c $\gcd(a, n) = 1$.
Let $\varphi_a, \varphi_b \in \mathrm{Aut}(G)$. Observe that:

$$(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x))$$
$$= \varphi_a(x^b)$$

$$
\begin{aligned}
&= (x^b)^a \\
&= x^{ab} \\
&= \varphi_{ab}(x).
\end{aligned}
$$

Hence:

$$
\begin{aligned}
\Psi(\varphi_a \circ \varphi_b) &= \Psi(\varphi_{ab}) \\
&= [ab]_n \\
&= [a]_n [b]_n \\
&= \Psi(\varphi_a)\Psi(\varphi_b).
\end{aligned}
$$

Thus Ψ is a homomorphism.

Let $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\Psi(\varphi_a) = [a]_n$