Let $G, H$ be groups (assumed to be multiplicative with identity elements $e_G \in G$, $e_H \in H$).

A <u>homomorphism</u> $G \to H$ is a map satisfying $\phi(gg') = \phi(g)\phi(g')$ for all $g, g' \in G$.

Note: An isomorphism is the same thing as a bijective homomorphism.

<u>Eg.</u> $\underbrace{\phi : GL_n(F)}_{\text{invertible } n\times n \text{ matrices over a field } F} \to \underbrace{F^\times}_{\text{multiplicative group of nonzero elements of } F}$, $\phi = \det$.

Properties: $\phi(e_G) = e_H$. $\quad (\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G) \Rightarrow \phi(e_G) = e_H)$.

If $g \in G$ has order $n$ then $|\phi(g)|$ divides $n = |g|$. $\quad$ eg. if $|g| = 6$ then $|\phi(g)|$ has order 1,2,3 or 6.

$g^n = e_G \Rightarrow \underbrace{\phi(g^n)}_{=\phi(g)^n} = \phi(e_G) = e_H$

$\phi(g^{-1}) = \phi(g)^{-1}$ since $gg^{-1} = e_G \Rightarrow \underbrace{\phi(gg^{-1})}_{=\phi(g)\phi(g^{-1})} = \phi(e_G) = e_H$

The <u>kernel</u> of a homomorphism $\phi : G \to H$ is $\ker\phi = \{g \in G : \phi(g) = e_H\}$. (Compare: the null space of a linear transformation)

<u>Theorem</u>: $\ker\phi$ is a subgroup of $G$.

<u>Proof</u> If $g, g' \in \ker\phi$ then $\phi(g) = \phi(g') = e_G$ then $\phi(gg') = \phi(g)\phi(g') = e_G e_G = e_G$ so $gg' \in \ker\phi$.

Since $\phi(e_G) = e_H$, $e_G \in \ker\phi$.

If $g \in \ker\phi$ then $\phi(g) = e_H$ so $\phi(g^{-1}) = \phi(g)^{-1} = e_H^{-1} = e_H$ so $g^{-1} \in \ker\phi$. $\quad$ So $\ker\phi \leq G$.

Note: If $\phi$ is one-to-one then $\ker\phi = \{e_G\}$. Conversely, if $\ker\phi = \{e_G\}$ then we show $\phi$ is one-to-one:

If $\phi(g) = \phi(g')$ then $\phi(g^{-1}g') = \phi(g^{-1})\phi(g') = \phi(g)^{-1}\phi(g') = e_H$ i.e. $g^{-1}g' \in \ker\phi = \{e_G\}$ so $g^{-1}g' = e_G$ so $g' = g$. $\quad\square$

The image of a homomorphism $\phi: G \to H$ then the image $\phi(G) = \{\phi(g) : g \in G\}$ is a subgroup of $H$.

Proof Given two elements in $\phi(G)$, say $\phi(g), \phi(g')$ for some $g, g' \in G$, then $\phi(g)\phi(g') = \phi(gg') \in \phi(G)$. Also $e_H = \phi(e_G) \in \phi(G)$. If we take any element in $\phi(G)$, say $\phi(g)$ where $g \in G$, then $\phi(g)^{-1} = \phi(g^{-1}) \in \phi(G)$. So $\phi(G) \le H$. $\square$

Note: $\phi: G \to H$ is onto iff $\phi(G) = H$.

Eg. Define $\phi: S_4 \to S_3$ as follows: Take $\pi_1 = (12)(34)$, $\pi_2 = (13)(24)$, $\pi_3 = (14)(23)$ in $S_4$. These form a conjugacy class in $S_4$ $\{\pi_1, \pi_2, \pi_3\} = X$. (Really $\phi(\sigma) \in \mathrm{Sym}\, X = \mathrm{Sym}\{\pi_1, \pi_2, \pi_3\}$).

Given $\sigma \in S_4$, we have a map $X \to X$, $\pi_i \xmapsto{\phi(\sigma)} \sigma \pi_i \sigma^{-1}$.

Eg. $\phi((13))$:

$$\begin{aligned}
\pi_1 &\mapsto (13)\pi_1(13)^{-1} = (13)(12)(34)(13)^{-1} = (32)(14) = (14)(23) = \pi_3 \\
\pi_2 &\mapsto (13)\pi_2(13)^{-1} = (13)(13)(24)(13)^{-1} = (31)(24) = (13)(24) = \pi_2 \\
\pi_3 &\mapsto (13)\pi_3(13)^{-1} = (13)(14)(23)(13)^{-1} = (34)(21) = (12)(34) = \pi_1
\end{aligned}$$

$\phi((13)) = (13)$

$\phi((142))$:

$$\begin{aligned}
\pi_1 &\mapsto (142)\pi_1(142)^{-1} = (142)(12)(34)(142)^{-1} = (41)(32) = (14)(23) = \pi_3 \\
\pi_2 &\mapsto (142)\pi_2(142)^{-1} = (142)(13)(24)(142)^{-1} = (43)(12) = (12)(34) = \pi_1 \\
\pi_3 &\mapsto (142)\pi_3(142)^{-1} = (142)(14)(23)(142)^{-1} = (42)(13) = (13)(24) = \pi_2
\end{aligned}$$

$\phi((142)) = (132)$

$\phi$ is onto $S_3$. (why? $\phi(S_4)$ is a subgroup of $S_3$. By Lagrange's Theorem, $|\phi(S_4)|$ is divisible by $|\phi((13))| = |(13)| = 2$ and $|\phi((142))| = |(132)| = 3$ so $\phi(S_4) = S_3$.)

$\ker\phi = C_{S_4}(X) = \langle \pi_1, \pi_2 \rangle = \{(), \pi_1, \pi_2, \pi_3\}$ is a Klein four subgroup of order 4 in $S_4$.
$(\pi_3 = \pi_1\pi_2)$

$\phi$ is a homomorphism; it is 4-to-1.