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

A homomorphism $G \to H$ 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.

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

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

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

$g^n = e_G \Rightarrow \underset{\substack{\| \\ \phi(g)^n}}{\phi(g^n)} = \phi(e_G) = e_H$

$\phi(g^{-1}) = \phi(g)^{-1}$ since $gg^{-1} = e_G \Rightarrow \underset{\substack{\| \\ \phi(g)\phi(g^{-1})}}{\phi(gg^{-1})} = \phi(e_G) = e_H$

The kernel 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)

Theorem: $\ker\phi$ is a subgroup of G.

Proof 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 $g^{-1} \in \ker\phi$. So $\ker\phi \leq G$.

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

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 $\phi(\sigma) \in \operatorname{Sym} X = \operatorname{Sym}\{\pi_1, \pi_2, \pi_3\}$).

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

Eg. $\phi((13))$:
$$\begin{aligned}
\pi_1 &\mapsto (13)\pi_1(13)^{-1} = (13)(12)(34)(13)^{-1} = (32)(14) = (14)(23) = \pi_3 \\
\pi_2 &\mapsto (13)\pi_2(13)^{-1} = (13)(13)(24)(13)^{-1} = (3\ 1)(24) = (13)(24) = \pi_2 \\
\pi_3 &\mapsto (13)\pi_2(13)^{-1} = (13)(14)(23)(13)^{-1} = (34)(2\ 1) = (12)(34) = \pi_1
\end{aligned}$$
$\phi((13)) = (13)$

$\phi((142))$:
$$\begin{aligned}
\pi_1 &\mapsto (142)\pi_1(142)^{-1} = (142)(12)(34)(142)^{-1} = (4\ 1)(3\ 2) = (14)(23) = \pi_3 \\
\pi_2 &\mapsto (142)\pi_2(142)^{-1} = (142)(13)(24)(142)^{-1} = (4\ 3)(1\ 2) = (12)(34) = \pi_1 \\
\pi_3 &\mapsto (142)\pi_3(142)^{-1} = (142)(14)(23)(142)^{-1} = (4\ 2)(13) = (13)(24) = \pi_2
\end{aligned}$$
$\phi((142)) = (132)$

ϕ 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.
$(\pi_3 = \pi_1\pi_2)$

ϕ is a homomorphism; it is 4-to-1.

The image of a homomorphism $\phi: G \to H$ i.e. the subgroup $\phi(G) = \{\phi(g) : g \in G\} \le H$ is a <u>homomorphic image</u> of G.

Fractional Linear Transformations (or Linear Fractional Transformations)

A map $\mathbb{R}\cup\{\infty\} \to \mathbb{R}\cup\{\infty\}$ (actually a permutation) of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix} : x \longmapsto \dfrac{ax+b}{cx+d}$ where $ad-bc \neq 0$.

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad-bc \neq 0 \right\}$ for actual invertible 2×2 real matrices.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right) = \frac{a\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right)+b}{c\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right)+d} = \frac{a(\alpha x+\beta)+b(\gamma x+\delta)}{c(\alpha x+\beta)+d(\gamma x+\delta)} = \frac{(a\alpha+b\gamma)x+(a\beta+b\delta)}{(c\alpha+d\gamma)x+(c\beta+d\delta)}$$

$$= \begin{bmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{bmatrix}(x)$$

Compare with multiplication of actual 2×2 invertible matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}$$

We denote by $PGL_2(\mathbb{R})$ the group of all fractional linear transformations $\mathbb{R}\cup\{\infty\} \to \mathbb{R}\cup\{\infty\}$ i.e.

$$PGL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\quad ad-bc \neq 0 \right\}.$$

This is a homomorphic image of $GL_2(\mathbb{R})$ under the homomorphism $\phi : GL_2(\mathbb{R}) \to PGL_2(\mathbb{R})$,
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. This map is a homomorphism: $\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}\right)$

$$= \begin{bmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\phi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right).$$

This homomorphism is onto $PGL_2(\mathbb{R})$ by definition but it's not onto because $\phi\left(\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}\right) = \begin{bmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

since $\begin{bmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{bmatrix}(x) = \dfrac{\lambda a x+\lambda b}{\lambda c x+\lambda d} = \dfrac{ax+b}{cx+d} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}(x)$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(5) = \frac{3\times5+4}{1\times5+7} = \frac{19}{12}.$$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(\infty) = \frac{3\times\infty+4}{1\times\infty+7} = 3$$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(-7) = \frac{3\times(-7)+4}{1\times(-7)+7} = \frac{-17}{0} = \infty$$

$$\begin{bmatrix}3&4\\0&7\end{bmatrix}(\infty) = \frac{3\times\infty+4}{\cancel{0\times\infty}+7} = \infty.$$

In $GL_2(\mathbb{R})$, $\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$. $(ad-bc\neq0)$

$\mathbb{F}_q$ = field of order q

$|GL_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$ divide by $q-1$.

$|SL_2(\mathbb{F}_q)| = (q^2-1)q$

Every fractional linear transformation is a permutation of $\mathbb{R}\cup\{\infty\}$

$PGL_2(\mathbb{R})$ is a group. $\begin{bmatrix}a&b\\c&d\end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix} = \begin{bmatrix}d&-b\\-c&a\end{bmatrix}$.

The identity $\begin{bmatrix}1&0\\0&1\end{bmatrix}(x) = \frac{1\times x+\cancel{0}}{\cancel{0\times x}+1} = x$.

You can think of $PGL_2(\mathbb{R})$ as the same as 2×2 invertible matrices but where we identify nonzero scalar multiples i.e. $\lambda\begin{bmatrix}a&b\\c&d\end{bmatrix} = \begin{bmatrix}\lambda a&\lambda b\\\lambda c&\lambda d\end{bmatrix} = \begin{bmatrix}a&b\\c&d\end{bmatrix}$.

$$GL_2(\mathbb{F}_2) = \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\} = SL_2(\mathbb{F}_2).$$

$|GL_2(\mathbb{F}_2)| = (2^2-1)(2^2-2) = 3\times2 = 6.$

$\mathbb{F}_2 = \{0,1\}$ is the field of order 2:

$$PGL_2(\mathbb{F}_2) = \left\{\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}, \begin{bmatrix}1&1\\1&0\end{bmatrix}, \begin{bmatrix}0&1\\1&1\end{bmatrix}, \begin{bmatrix}1&0\\1&1\end{bmatrix}\right\} \cong GL_2(\mathbb{F}_q) \cong SL_2(\mathbb{F}_2) \cong S_3$$

why? $PGL_2(\mathbb{F}_2)$ is a group of permutations of $\{\underbrace{0,1}_{\mathbb{F}_2},\infty\}$

$\mathrm{Sym}\{0,1,\infty\} = \{$all permutations of $0,1,\infty\}$

so $PGL_2(\mathbb{F}_2)$ is isomorphic to a subgroup of S_3.

$|GL_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 8\times6 = 48$

$\mathbb{F}_3 = \{0,1,2\}$ $\quad \frac{1}{2} = 2 = -1$ $\quad |PGL_2(\mathbb{F}_3)| = \frac{48}{2} = 24$ $\quad PGL_2(\mathbb{F}_3) \cong S_4$.

The map $GL_2(\mathbb{F}_3) \to PGL_2(\mathbb{F}_3)$ is 2-to-1.

$PGL_2(\mathbb{F}_3)$ is a group of permutations of $\mathbb{F}_3\cup\{\infty\} = \{0,1,2,\infty\}$.

$\begin{pmatrix}a&b\\c&d\end{pmatrix} \mapsto \begin{bmatrix}a&b\\c&d\end{bmatrix}$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ field of order 4

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$|GL_2(\mathbb{F}_4)| = (4^2-1)(4^2-4) = 15 \times 12 = 180$

$|SL_2(\mathbb{F}_4)| = \frac{180}{3} = 60$

$|A_5| = \frac{5!}{2} = 60$

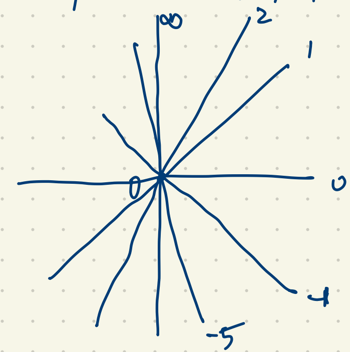
$SL_2(\mathbb{F}_4) \cong A_5$.

$PSL_2(\mathbb{F}_4) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad-bc = 1, \quad a,b,c,d \in \mathbb{F}_4 \right\} \cong SL_2(\mathbb{F}_4)$

The map $SL_2(\mathbb{F}_4) \longrightarrow PSL_2(\mathbb{F}_4)$ acting as all even permutations of $\mathbb{F}_4 \cup \{\infty\} = \{0, 1, \alpha, \beta, \infty\}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(x) = \frac{1 \times x + 1}{0 \times x + 1} = x + 1 \quad : \quad (0, 1)(\alpha, \beta)(\infty)$



$\mathbb{R} \cup \{\infty\} = \{$all possible slopes of lines through the origin in $\mathbb{R}^2\}$