Def An isomorphism from a group G to itself is called an **automorphism** of G.

Example: $\phi : (\mathbb{R}, +) \longmapsto (\mathbb{R}, +)$ where $\lambda \neq 0$

$$x \longmapsto \lambda x$$

is an automorphism

Example: $\phi : (\mathbb{R}^2, +) \longmapsto (\mathbb{R}^2, +)$ is an automorphism

$$(a, b) \longmapsto (b, a)$$

Def: Let G be a group $a \in G$. The **inner automorphism** of G induced by a is defined by:

$$\phi_a : G \longrightarrow G \qquad \text{(conjugation by } a\text{)}$$
$$x \longmapsto a x a^{-1}$$

(verify that ϕ_a is an automorphism)

Example: $G = (SL_2(\mathbb{R}), \cdot)$ $\quad M \in SL_2(\mathbb{R}) = G$

$\phi_M(A) = MAM^{-1}$ conjugation by M

ϕ_M is an inner automorphism

Example: $D_4 = \{R_0\ R_{90}\ R_{180}\ R_{270}\ F_0\ F_{45}\ F_{90}\ F_{135}\}$

$\phi_{R_{90}}$:

$$R_\theta \mapsto R_{90} R_\theta R_{90}^{-1} = R_\theta$$

$$F_\theta \to R_{90}(F_\theta R_{90}^{-1}) = R_{90}(R_{90} F_\theta) = R_{180} F_\theta$$

$$= F_{\theta+90}$$

More precisely.

$\phi_{R_{90}}$ sends R_θ to R_θ

sends $F_0 \mapsto F_{90}$ $F_{90} \to F_0$

$F_{45} \to F_{135}$ $F_{135} \to F_{45}$

$\mathrm{Aut}(G)$ = set of all automorphisms of G

$\cup\!\mathsf{I}$

$\mathrm{Inn}(G)$ = set of all inner automorphisms of G

<u>Thm</u> $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are both groups under the operation of function composition and $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$

both identity map

Example $\mathrm{Inn}(D_4) = \{ \phi_{R_0}\ \phi_{R_{90}}\ \phi_{R_{180}}\ \phi_{R_{270}}\ \phi_{F_0}\ \phi_{F_{45}}\ \phi_{F_{90}}\ \phi_{F_{135}} \}$

$Z(D_4) = \{R_0, R_{180}\}$ $\quad \phi_{R_{180}}(x) = R_{180}\, x\, R_{180}^{-1} = x\, R_{180} R_{180}^{-1} = x \quad \forall x \in D_4$

$\Longrightarrow \phi_{R_{180}} = \mathrm{id}_{D_4} = \phi_{R_0}$

- $\phi_{R_{270}}(x) = R_{270}\, x\, R_{270}^{-1} = R_{90}(R_{180}\, x\, R_{180}^{-1})R_{90}^{-1} = R_{90}\, x\, R_{90}^{-1} = \phi_{R_{90}}(x)$

$\Longrightarrow \phi_{R_{270}} = \phi_{R_{90}}$

- $\phi_{F_{90}}(x) = F_{90}\, x\, F_{90}^{-1} = (F_0 R_{180})\, x\, (R_{180}^{-1} F_0^{-1}) = F_0 \underbrace{R_{180}\, x\, R_{180}^{-1}}\, F_0^{-1}$

$= F_0\, x\, F_0^{-1} = \phi_{F_0}(x)$

$\Longrightarrow \phi_{F_{90}} = \phi_{F_0}$ similarly $\phi_{F_{45}} = \phi_{F_{135}}$

Exercise: verify that $\underset{\mathrm{Id}_{D_4}}{\overset{\phi_{R_0}}{\parallel}}$ $\phi_{R_{90}}$ ϕ_{F_0} $\phi_{F_{45}}$ are all different.

Thm $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$ **note**: $\mathrm{Inn}(\mathbb{Z}_n) = \{id\}$

proof: let $\alpha: \mathbb{Z}_n \to \mathbb{Z}_n$ be an isomorphism.

Then $\alpha(0) = 0$ and $\alpha(1)$ is a generator of $\mathbb{Z}_n \Rightarrow \alpha(1) = k$ where $\gcd(k, n) = 1$

note if $\alpha(1) = k$ then $\alpha(m) = \alpha(\underbrace{1^m}_{\underbrace{1+1+\cdots+1}_{m \text{ times}}}) = \alpha(1)^m = km \mod n$

Therefore $\mathrm{Aut}(\mathbb{Z}_n) = \left\{ \phi(k) \;\middle|\; \begin{array}{l} \phi(k): \mathbb{Z}_n \to \mathbb{Z}_n \\ m \to mk \mod n \\ \gcd(k, n) = 1 \end{array} \right\}$

Define $\phi: U(n) \longmapsto \mathrm{Aut}(\mathbb{Z}_n)$

$$k \longmapsto \phi(k)$$

Verify that ϕ is an isomorphism

- ϕ is 1-1 and onto
- ϕ is operation preserving

$\phi(k_1 k_2)(m) = k_1 k_2 m \mod n$

$\| \; \forall m$ $\qquad\qquad\qquad\qquad\qquad \| \; \forall m$

$\phi(k_1)\phi(k_2)(m) = \phi(k_1)(k_2 m \mod n) = k_1 k_2 m \mod n$