- Isometry

<u>Definition</u>. $f: \mathbb{R}^n \to \mathbb{R}^n$ that preserves distances.

Isometries on $\mathbb{R}^n$ form a group

$$M_n = T_n \rtimes O_n$$

translations

orthogonal linear operators.

orthogonal matrices

So each isometry is of the form $t_{\vec{a}} \cdot \phi$

In particular, when $n=2$.

$[O_n(\mathbb{R}) : SO_n(\mathbb{R}^n)] = 2$.

$SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det A = 1\}$

$$SO_2(\mathbb{R}) = \left\{ \underbrace{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}}_{\rho_\theta} \middle| \theta \in \mathbb{R} \right\}$$

$$\underbrace{r = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}_{\text{reflection along } x\text{-axis}}. \qquad O_2(\mathbb{R}) = SO_2(\mathbb{R}) \sqcup SO_2(\mathbb{R})r$$

Isometries on $\mathbb{R}^2$: $t_{\vec{a}} \rho_\theta$ or $t_{\vec{a}} \rho_\theta r$

<u>Computational results</u>.

① $\phi \cdot t_{\vec{a}} = t_{\phi(\vec{a})} \cdot \phi$. $(\Longleftrightarrow \phi \cdot t_{\vec{a}} \cdot \phi^{-1} = t_{\phi(\vec{a})})$

where $\phi \in O_n$.

In particular, for the case $\mathbb{R}^2$.

$\rho_\theta t_{\vec{a}} = t_{\rho_\theta(\vec{a})} \cdot \rho_\theta$ and $r t_{\vec{a}} = t_{r(\vec{a})} \cdot r$

②. $t_{\vec{a}} \cdot t_{\vec{b}} = t_{\vec{a}+\vec{b}}$, $t_{\vec{a}}^{-1} = t_{-\vec{a}}$

$\rho_\alpha \cdot \rho_\beta = \rho_{\alpha+\beta}$. $\rho_\alpha^{-1} = \rho_{-\alpha}$.

$r^2 = id$. $r^{-1} = r$.

③ $r \rho_\theta r = \rho_{-\theta}$.

Geometric Classification of Isometries on $\mathbb{R}^2$.

Four kinds of isometries

- translation
- rotation
- reflection
- glide reflection.

$\boxed{\text{Review the proof of that theorem}}$

<u>Group Actions.</u>

Definition. Elementary Concepts: <u>orbit</u>, <u>stabilizer</u>.

$O(x) = \{g.x \in X \mid g \in G\}$

Distinct orbits form a partition of X.

$G_x = \{g \in G \mid g.x = x\}$

G_x is a subgroup of G.

transitive actions

there's only one orbit, i.e., $X = O(x)$ $\forall x \in X$

<u>Counting Formula</u>.

$|G| < \infty$. $|G| = |O(x)| \cdot |G_x|$.

$$\begin{aligned} G/G_x &\longrightarrow O(x) \\ gG_x &\longmapsto g.x \end{aligned}$$

<u>Class Equation</u>

Decompose a group G into the disjoint union of <u>conjugacy classes.</u>

orbit of G acting on itself by conjugation.

In particular, the stabilizer in this case is called a <u>normalizer</u> $N_x = \{g \in G \mid gxg^{-1} = x\}$.

Basic Examples:

- S_n acts on $X = \{1, 2, \dots, n\}$ by $\sigma.k = \sigma(k)$
- G acts on G by left multiplication
- G acts on G by conjugation.
- $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication

Properties of Group Actions:

- Fix $g \in G$, we get bijective map $\begin{aligned} X &\longrightarrow X \\ x &\longmapsto g.x \end{aligned}$

  More generally, a group action corresponding to a homomorphism $G \longrightarrow Per(X)$

<u>Quiz</u>. $K_4 = \{1, a, b, c\}$ $S = \{x, y, z\}$.

$G_x = \{1, a\}$. $G_y = \{1, b\}$.

$|O(x)| = \frac{|K_4|}{|G_x|} = 2$. $|O(y)| = \frac{|K_4|}{|G_y|} = 2$.

$O(x), O(y)$ cannot be disjoint. so $O(x) = O(y) = \{x, y\}$

$G_x = \{1, a\}$. so $b.x \in O(x)$ and $b.x \neq x \Rightarrow b.x = y$.

$b \in G_y$. so $b.y = y$ contradiction.

More Results related to Group Actions.

- Cauchy's Theorem.
- Fix Point Theorem
- $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$
- groups of order p^2 are abelian (p prime).

<u>Classification of Groups.</u>

Tools: <u>Sylow Theorems</u> & <u>Semidirect Products</u>

there's <u>unique</u> Sylow p-subgroup iff this Sylow p-subgroup is a normal subgroup of G.

- General Construction.

  $G \rtimes_\phi G'$, $\phi: G' \to Aut(G)$

  composition:

  $(g_1, g_1')(g_2, g_2') = (g_1 \phi_{g_1'}(g_2), g_1' g_2')$

- $G = H \rtimes K$.

  It means $f: H \rtimes_\phi K \to G$ is an isomorphism, where $\phi: K \to Aut(H)$, $\phi_k(h) = khk^{-1}$. $f(h, k) = hk$

  - $H \lhd G$
  - $H \cap K = \{1\}$
  - $G = HK$.

<u>Results for Classification</u>:

- $|G| = p$, prime.

  $G \cong C_p \cong \mathbb{Z}/p\mathbb{Z}$.

- $|G| = 2p$. p prime

  $G \cong \mathbb{Z}/2p\mathbb{Z}$ or $G \cong D_p$.

- $|G| = p^2$. p prime.

  $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

- $|G| = 12$: 5 cases
- $|G| = 8$: 5 cases.
- $|G| = 15$: $G \cong \mathbb{Z}/15\mathbb{Z}$.

<u>Rings</u>

- Definition $(R, +, \times)$

- Important concepts:
  - unit & <u>group of units</u>. $R^\times$
  - associates: x & ux are associates if $u \in R^\times$.

Examples of Rings:

- $(\mathbb{Z}, +, \times)$
- M_n, ring of $n \times n$ matrices (non-commutative ring when $n > 1$)
- $\mathbb{Z}/n\mathbb{Z}$.
- Fields. $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$.
- <u>Polynomial Rings.</u> <u>$R[x]$</u>
  - degree of a polynomial.
  - division algorithm for $f(x)$ divided by a <u>monic</u> polynomial $g(x)$.

    $f(x) = q(x)g(x) + r(x)$. <u>$\deg r(x) < \deg g(x)$</u>

- Integral Domains. $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime.

  $n = a \cdot b$, $a > 1$, $b > 1$.

  $\bar{a} \cdot \bar{b} = \bar{0} \in \mathbb{Z}/n\mathbb{Z}$.

- Ring homomorphisms.

  $f: R \to R'$. <u>definition</u>

  $\ker(f) = \{r \in R \mid f(r) = 0'\}$.

- <u>Ideals</u>

  $I \subseteq R$. <u>definition</u>

  Principal ideals: $(a) = \{ar \in R \mid r \in R\}$.

  - $I \neq R$. $\Longleftrightarrow I \cap R^\times = \emptyset$. $(I = R \Longleftrightarrow I \cap R^\times \neq \emptyset)$
  - $(I, +)$ is a subgroup of $(R, +)$.

- Quotient Ring.

  $R/I = \{r + I\}_{r \in R}$. <u>$r_1 + I = r_2 + I \Longleftrightarrow r_2 - r_1 \in I$.</u>

  $$\begin{cases} (a+I) + (b+I) = (a+b) + I. \\ (a+I)(b+I) = ab + I. \end{cases}$$

  - maximal ideal.

    R/I is a field $\Longleftrightarrow I$ is maximal.

  Applied to polynomials.

  $\mathbb{F}$ is a field. $\mathbb{F}[x]$ is P.I.D. <u>$p(x) \neq 0$</u>.

  $(p(x))$ is maximal $\Leftrightarrow p(x)$ is irreducible.

  so $\mathbb{F}[x]/(p(x))$ is a field $\Longleftrightarrow p(x)$ is irreducible

  Example. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

  - Algebraic numbers. $\mathbb{F} \subseteq \mathbb{E}$. $\gamma \in \mathbb{E}$ is algebraic over $\mathbb{F}$

    Then the minimal polynomial $m(x)$ of γ is irreducible.

    $\mathrm{Im}(\Phi) \cong \mathbb{F}[x]/(m(x))$ is a field.

    $$\begin{aligned} \mathbb{F}[x] &\xrightarrow{\Phi} \mathbb{E} \\ p(x) &\longmapsto p(\gamma). \end{aligned}$$

First Isomorphism Theorem for Rings

$f: R \to R'$.

$R/\ker(f) \cong \mathrm{Im}(f)$