Group homomorphism.

Define: $n \in \mathbb{Z}_{>0}$ $\quad a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ copies}}$ $\qquad a^0 = e$

$$a^{-n} = (a^{-1})^n.$$

check $a^{m+n} = a^m \cdot a^n$ for all $m, n \in \mathbb{Z}$.

Ex: $\rho: \mathbb{Z} \to G$ group homo
$n \mapsto a^n$,

so $\mathrm{Im}\,\rho \cong \mathbb{Z}/\ker\rho$.

$\ker\rho$ subgroup of $\mathbb{Z}$. $\cong n\mathbb{Z}$.

$n \geq 1$, call $\mathrm{ord}(a) = n$.
$n = 0$, call $\mathrm{ord}(a) = \infty$

minimal $k > 0$, s.t. $a^k = e$

$\mathrm{Im}\,\rho$ = subgroup generated by a or $\langle a \rangle$

Cor (Lagrange) : $\# G < +\infty \Rightarrow \operatorname{ord}(a) \mid \# G$.

Define (cyclic group) $G = \langle a \rangle$ or

$G \cong \mathbb{Z}/n\mathbb{Z}$, $n \geq 1$

or $\mathbb{Z}$

Correspondence :

$\rho : G_1 \longrightarrow G_2$, ρ surjective

$$\{\text{subgroups containing } \ker\rho\} \xleftrightarrow{1:1} \{\text{subgroups in } G_2\}$$

$$H \longmapsto \operatorname{Im}\rho$$

$$\rho^{-1}(\bar{H}) \longleftarrow\!\shortmid \bar{H}$$

$$\{\text{subgroups of } \mathbb{Z} \text{ containing } n\mathbb{Z}\}$$

$$\longleftrightarrow \{\text{subgroups of } \mathbb{Z}/n\mathbb{Z}\}$$

Group actions (operations) (Symmetry)

Defn: X set, G group, G operates on X

if $G \times X \to X$

$(g, x) \mapsto g \cdot x$ or gx

s.t. ① $g_1(g_2 x) = (g_1 g_2) x$

② $e \cdot x = x$

Denote by $G \curvearrowright X$

Ex: ① $S_n \times [n] \to [n]$

$(\sigma, m) \mapsto \sigma \cdot m = \sigma(m)$

② $$\boxed{\begin{aligned} GL(n, \mathbb{R}) \times \mathbb{R}^n &\to \mathbb{R}^n \\ (A, x) &\mapsto A \cdot x \end{aligned}}$$

$\Downarrow$

Further properties $A \cdot (x+y) = Ax + Ay$

preserving linear structure $A(\lambda x) = \lambda (Ax)$

③ left product $G \times G \to G$

$(g, h) \mapsto g \cdot h$

④ right product $G \times G \to G$

$(g, h) \mapsto h g^{-1}$

⑤ conjugation

$$\boxed{\begin{array}{l} G \times G \to G \\ (g, h) \mapsto g h g^{-1} \end{array}} \equiv g * h$$

$\Downarrow$

Further property preserving group structure

$g * (h_1 h_2) = (g * h_1)(g * h_2)$

Another point of view.

$S_X = \{ f : X \to X \mid f \text{ bijection} \}$

$G \curvearrowright X$, fix $g \in G$. define

$$m_g : X \to X$$
$$g \mapsto g \cdot x$$

① $m_g \cdot m_h = m_{gh}$.

② $m_e = Id_X$

$\Rightarrow$ $m_g \cdot m_{g^{-1}} = m_e = Id_X$

$m_{g^{-1}} \cdot m_g = m_e = Id_X$

$\Rightarrow$ m_g is bijection : $X \to X$

i.e. $m_g \in S_X$

Prop: $\rho : G \to S_X$ is a group homomorphism.
$g \mapsto m_g$

Conversly: Given $\rho: G \to S_X$

Define $G \curvearrowright S_X$ by

$$g \cdot x = \rho(g)(x)$$

$$\{G \curvearrowright X\} \xleftrightarrow{1:1} \{\rho : G \to S_X\}$$

bijection

Why this is helpful?

Defn: When $\ker \rho = \{e\}$, the operation is called faithful.

$\Leftrightarrow$ If $g \cdot x = x$ for all $x \in X$ then $g = id$.

Prop: G finite and $\# G = n$, then G is isomorphic to a subgroup of S_n

Pf: $G \curvearrowright G$ by $g \cdot h = gh$

Then $\rho : G \to S_G = S_n$

If $g \cdot h = h$ for all h, then $g = e$

$\Rightarrow$ $G \cong \operatorname{Im}\rho$ a subgroup of S_n $\square$

Classification of G-operations.

Defn (orbits) $G \curvearrowright X$,

define equivalence relation by

$x \sim y$ iff $\exists\, g \in G$, s.t. $g \cdot x = y$

Check $x \sim y, \Rightarrow y \sim x$

$x \sim x, \quad \forall x \in X$

$x \sim y, y \sim z \Rightarrow x \sim z$

Each equivalence class is called an orbit.

$O_x = \{ g \cdot x \mid g \in G \}$.

Then X is disjoint union of equivalence classes or orbits of G operation

---

Ex: $H \subset G$ subgroup.

$$H \times G \to G$$
$$(h, g) \mapsto gh^{-1}$$

Then any H-orbit has the form gH or right H-coset.

Ex: $$G \times G/H \to G/H$$
$$(g, g'H) \mapsto g \cdot g'H$$

Ex: $G \times G \to G$
$(g, h) \mapsto ghg^{-1}$

(Defn) each orbit is called a conjugation class.

---

reduce the classification to each orbit.

Defn (Transitive) If $G \curvearrowright X$ has only one orbit, then we call it transitive.

Ex: $G \curvearrowright G/H$, transitive.

Defn (Stabilizer) $\forall x \in X$, $\mathrm{Stab}_x = \{g \in G \mid g \cdot x = x\}$

Prop: Stab_x is a subgroup of G.

Pf: check □

Prop: Assume $G \curvearrowright X$ transitively.

There is a bijection between

$$F : G/\mathrm{Stab}_x \to X, \quad \text{s.t.}$$
$$g\mathrm{Stab}_x \mapsto g \cdot x.$$

$$\begin{tikzcd} G \times G/\mathrm{Stab}_x \arrow[r] \arrow[d, "\mathrm{id}_G \times F"'] \arrow[dr, phantom, "\circlearrowleft"] & G/\mathrm{Stab}_x \arrow[d, "F"] \\ G \times X \arrow[r] & X \end{tikzcd}$$

Pf: Check F "well-defined" bijective, and preserves the G-operation $\square$

Cor: $G \curvearrowright X$ transitive $\Rightarrow$

$$\# X = \#G / \#\mathrm{Stab}_x$$

Notice: $\mathrm{Stab}_{gx} = g\,\mathrm{Stab}_x\, g^{-1}$

Counting: $G \curvearrowright X$ have orbits

$O_1, \dots, O_n$, $x_i \in O_i$.

Then ① $\# X = \sum \# O_i$

② $\# O_x = \dfrac{\# G}{\# \mathrm{Stab}_{x_i}}$

Application: classification of groups of order p^2, p prime number.

Prop: $\# G = p \Rightarrow G$ cyclic of order p

Prop: $\# G = p^2 \Rightarrow G$ abelian.

pf: Let $O_1 \cdots O_n$ by conjugaly classes of G. then

$\# O_i \mid p^2$, $\# O_i = 1, p$, or p^2

If $O_1 = \{e\}$, then $\# O_1 = 1$.

$\Rightarrow \# O_i = 1$ or p.

$$\sum_{i=1}^{n} \# O_i = p^2 \equiv 0 \pmod p$$

$$\Rightarrow \sum_{i=2}^{n} \# O_i \equiv -1 \pmod p$$

$\Rightarrow \exists\ O_i,\ i \geq 2$, s.t.

$\# O_i = 1$. such $O_i = \{x_i\}$ satisfying $g x_i g^{-1} = x_i$.

Defin $C(G) = \{ h \in G \mid hg = gh \ \forall g \in G \}$

$C(G)$ is a normal subgroup of G.

So $C(G) \neq \{e\}$.

$\Rightarrow$ $\underbrace{C(G) = G}_{\checkmark}$ or $\underline{\# C(G) = p}$

$\Downarrow$

$G/C(G) \cong \mathbb{Z}/p\mathbb{Z}$

Lemma: If G/H cyclic, and $H \subset C(G)$, then G abelian

pf: $G/H = \bigcup a^i H$.

$\Rightarrow (a^i h_i)\cdot(a^j h_j) = a^{i+j}(h_i h_j)$

$= (a^j h_j)(a^i h_i)$

$\square$

More work $\Rightarrow$ $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

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

Application to group theory. Sylow Thm.