Class 7: Homomorphism, Isomorphism & Automorphism - 20220928

Homomorphisms

$f : G \to G'.\quad \forall a, b \in G, f(ab) = f(a)f(b)$

$\ker(f) = \{g \in G | f(g) = 1'\}$

$Im(f) = \{f(g) \in G' | g \in G\}$

Note : $\ker(f) = \{1\} \iff f$ is injective

Conjugation

Observation

$\ker(f)$ is a subgroup of G.

$\forall g \in G,\ \forall x \in \ker(f)$, consider $gxg^{-1} \in G$

$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g) \cdot 1' \cdot f(g^{-1}) = 1'$

So $gxg^{-1} \in \ker(f)$

Definition

G is a group, $x \in G, g \in G.$ The **conjugation** of x by g is the elemnt gxg^{-1}

Conjugacy Class

We can define a relation on G by $a \sim b$ if $\exists g \in G, b = gag^{-1}$.

This can be verified to be an equivalence relation:

- $\forall a \in G,\ a = 1 \cdot a \cdot 1',\ a \sim a$
- $$\begin{aligned} & a \sim b \\ \Rightarrow\ & \exists g \in G, b = gag^{-1} \\ \Rightarrow\ & a = g^{-1}bg = g^{-1}b(g^{-1})^{-1} \\ \Rightarrow\ & b \sim a \end{aligned}$$
- $$\begin{aligned} & a \sim b, b \sim c \\ \Rightarrow\ & \exists g_1 \in G, b = g_1 a g_1^{-1}, \quad \exists g_2 \in G, c = g_2 b g_2^{-1} \\ \Rightarrow\ & c = g_2 b g_2^{-1} = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1) a (g_2 g_1)^{-1} \\ \Rightarrow\ & a \sim c \end{aligned}$$

Under this equivalence relation, if $a \sim b$, we say a, b are conjugates, each equivalence class is called a **conjugracy class**: $[a] = \{gag^{-1} \in G | g \in G\}$

Normal Subgroup

- ## Definition

A subgroup N of G is called a normal subgroup if $\forall n \in N, \forall g \in G, \quad gng^{-1} \in N$. (i.e., "closed under conjugation")

- ## Prop

The following statements are euqivalent for a subgroup N of G:

1. N is a normal subgroup of G
2. $\forall g \in G, gNg^{-1} = \{gng^{-1} \in G | g \in G, n \in N\} \subseteq N$
3. $\forall g \in G, gNg^{-1} = N$

- ### Proof

$(1) \iff (2)$ obvious by definition

$(3) \Rightarrow (2)$ obvious

$(2) \Rightarrow (3)$

$$\begin{aligned} \forall g \in G, gNg^{-1} &\subseteq N \\ g^{-1}(gNg^{-1})g &\subseteq g^{-1}Ng \\ N &\subseteq g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \\ \text{i.e.} \quad \forall g \in G,\ N &\subseteq gNg^{-1} \\ \text{so,} \quad gNg^{-1} &= N \end{aligned}$$

- ## Example

1. The motivation example:
    - for any homomorphism $f : G \to G'$
    - $\ker(f)$ is a normal subgroup of G.

    For example:

    - $\det : GL_n(\mathbb{R}) \to \mathbb{R}^x$

        > $\mathbb{R}^x$: the group of nonzero real numbers with multiplication

    - $\det$ is a homomorphism:
    - We know from Linear Algebra that $\det(AB) = \det(A) \cdot \det(B)$
    - $\ker(\det) = \{A \in GL_n(\mathbb{R}) | \det A = 1\} = SL_n(\mathbb{R})$
    - We can conclude $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$
2. G is abelian, then any subgroup H of G is a normal subgroup:
    - $\forall h \in H,\ \forall g \in G,\ ghg^{-1} = hgg^{-1} = h \in H$

> Notation Remark:

> - Sometimes people write $N \lhd G$ to mean N is a normal subgroup of G.
> - People also write $H < G$ to mean H is a subgroup of G.

3. G is a group.

   Define the <u>**center**</u> of G: $Z(G) = \{g \in G | \forall x \in G, gx = xg\}$

   (In particular, if G is abelian, $Z(G) = G$)

   We'll verify $Z(G)$ is a subgroup of G:

   - $\forall a, b \in Z(G),\ \forall x \in G.$

     $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

     So $ab \in Z(G)$
   - $1 \in Z(G) : \forall x \in G, 1x = x1 = x$
   - $\forall a \in Z(G), \forall x \in G, ax = xa.$

     $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$

     $xa^{-1} = a^{-1}x$

     So $a^{-1} \in Z(G)$

   Next we'll verify $Z(G)$ is normal

   - $\forall a \in Z(G),\ \forall g \in G, gag^{-1} = agg^{-1} = a \in Z(G)$

Isomorphism

Definition

A map $f : F \to G'$ is an <u>isomorphism</u> if it's a **bijective homomorphism**

Example

$G =< a >$ is an infinite cyclic group

$f : \mathbb{Z} \to G,\quad f(k) = a^k$

We've proved f is a homomorphism

f is also <u>bijective</u>

- $\ker(f) = \{k \in \mathbb{Z} | f(k) = 1\} = \{0\} \quad \Rightarrow \quad f$ is injective
- Surjectivity of f follows directly from the definition of $G =< a >$ (each element of G is a power of a)

Inverse

- **Prop**

The inverse of an isomophism is also an isomorphism

- **Proof**

- Suppose $f : G \to G'$, an isomorphism, it has inverse $f^{-1} : G' \to G$

  We need to show f^{-1} is a homomorphism

  $\forall x, y \in G$. We need to show $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$
- Let $a = f^{-1}(x), b = f^{-1}(y)$. We have $f(a) = x$, $f(b) = y$.

  f is a homomorphism.

  $\Rightarrow f(ab) = f(a)f(b) = xy$

  $\Rightarrow ab = f^{-1}(xy)$

  $\Rightarrow f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$

Isomorphic

Definition

G, G' are groups. We say G is **isomorphic** to G' if there exists an **isomorphism** $f : G \to G'$ and we write $G \cong G'$

Remark

- The proposition above indicates $G \cong G' \Rightarrow G' \cong G$

  So we can say **G and G' are isomorphic** if $G \cong G'$
- If two groups are isomoprphic, then they're "essentially" the same group. i.e., they'll have the same algebraic properties

  So in the study of group theory, we often identify isomorphic groups to be a same groups

Exercise

Show $G \cong G', G' \cong G'' \Rightarrow G \cong G''$

Automorphism

Definition

An isomorphism $G \to G$ is called an <u>automorphism</u>

Examples

1. $id_G : G \to G$ is an automorphism

   $g \mapsto g$

2. Fix $g \in G$. Define ϕ_g: $G \to G$ by $\phi_g(x) = gxg^{-1}$

   ϕ_g is an automorphism:

   - $\phi_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$
   - $\phi_g^{-1} \circ \phi_g(x) = g^{-1}(gxg^{-1})(g^{-1})^{-1} = (g^{-1}g)x(g^{-1}(g^{-1})^{-1}) = x,$

     So $\phi_{g^{-1}} \circ \phi_g = id_G$

     Similarly, you can verify $\phi_g \circ \phi_{g^{-1}} = id_G$

     $\Rightarrow \phi_g^{-1} = \phi_{g^{-1}},\ \phi_g$ invertible

     $\Rightarrow$ bijective

3. $G = (\mathbb{Z}, +)$

   $f : \mathbb{Z} \to \mathbb{Z}, \quad f(k) = -k$

   Exercise: Verify it's an automorphism

Group of Automorphism

The <u>group of automorphism</u> of G, $Aut(G)$, is the group consisting of all the automorphisms $G \to G$, withe function composition

- The identity of $Aut(G)$ is id_G.
- The inverse of $f \in Aut(G)$ is its inverse function f^{-1}

Inner automorphism

An <u>inner automorphism</u> is an automorphism of the form ϕ_g in example (2).

We'll show the set of inner automrphisms form a normal subgroup of $Aut(G)$.