Class 6: CyclicGroup & Homomorphism - 2022/09/26

Review

- $x \in G$.
- Define the cyclic subgroup generated by x: $< x >= \{x^k \in G | k \in \mathbb{Z}\}$.
- The order of x, denoted by $|x|$, is defined as $| < x > |$, equivalently, $| < x > |$ is the smallest positive integer that makes $x^{|x|} = 1$
  - $< x >= \{1, x, x^2, \ldots, x^{|x|-1}\}$ when $|x| < \infty$
  - $< x >= \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$ when $|x| = \infty$
- Sometimes the group itself equals one of it's cyclic subgroups

Cyclic Group

- ## Definition

  - A group G is cyclic if $G =< x >$ for some $x \in G$
  - x is called the generator of G

- ## Example

  1. $(\mathbb{Z}, +)$ is a cyclic group.
     - $\mathbb{Z} =< 1 >=< -1 >$
  2. $G = \{\pm 1\}$. With number multiplication
     - Multiplication table:

	1	-1
1	1	-1
-1	-1	1

     - G is cyclic, $G =< -1 >$
  3. S_3 is **NOT** cyclic
     - $< id >= \{id\}$
     - $< (1\ 2) >= \{id, (1\ 2)\}$
     - $< (1\ 3) >= \{id, (1\ 3)\}$
     - $< (2\ 3) >= \{id, (2\ 3)\}$
     - $< (1\ 2\ 3) >=< (1\ 3\ 2) >= \{id, (1\ 2\ 3), (1\ 3\ 2)\}$

     Later, we'll show that S_3 is the second smallest non-cyclic group.

     > The **smallest non-cyclic group** is K_4. The **Klein Four Group**.

- ## Proposition

  - Any subgroup of a cyclic group is cyclic
  - Example: $(\mathbb{Z}, +)$
    - We've proved that its subgroups are all of the form $n\mathbb{Z}$ (cyclic subgroup generated by n).

> Later, we will show that $(\mathbb{Z}, +)$ is the **only** infinite cyclic group.

Proof

- Given a cyclic group $G =< x >$
- If H is a subgroup of G,
- Consider $S = \{k \in \mathbb{Z} | x^k \in H\}$
    - S is a subgroup of $(\mathbb{Z}, +)$ (Verify by yourself)
    - So $S = n\mathbb{Z}$ for some $n \in \mathbb{N}$
    - $S = \{k \in \mathbb{Z} | x^k \in H\} = n\mathbb{Z}$
- It follows that

$$\begin{aligned} H &= \{x^k \in G | k \in S\} \\ &= \{x^k \in G | k \in n\mathbb{Z}\} \\ &= \{x^{n \cdot l} \in G | l \in \mathbb{Z}\} \\ &=< x^n > \end{aligned}$$

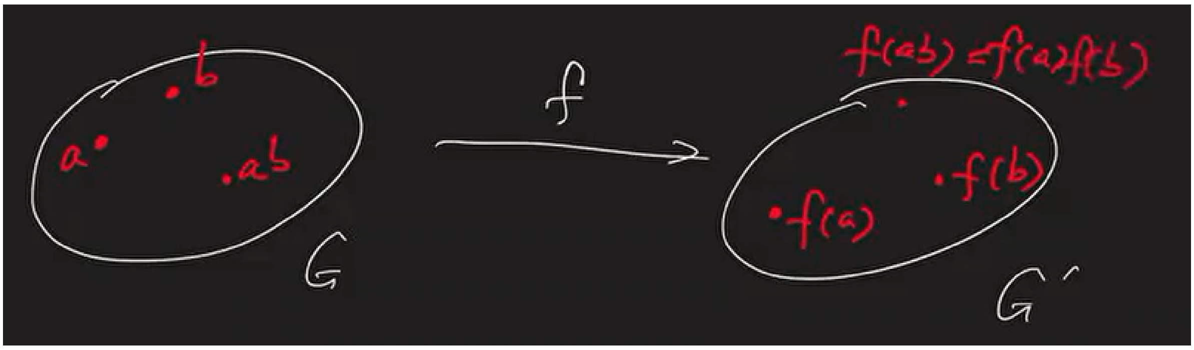
> We have been studying on the groups itself. Now we are going to study about the functions on groups

Homomorphism

Definition

A homomorphism is a map $f : G \to G'$ $(G, G'$ are goups$)$ satisfying :

$\forall a, b \in G, f(ab) = f(a)f(b)$



> -morphism: some kind of change

> This is different from homeomorphism: bijective and continous function

Example

1. $x \in G$. define

$$\begin{array}{cccc} f: & \mathbb{Z} & \to & G \\ & k & \mapsto & x^k \end{array}$$

   f is a homommorpism.

   $\forall k, l \in \mathbb{Z},\ \ f(k) \cdot f(l) = x^k \cdot x^l = x^{k+l} = f(k+l)$

2. Trivial homomorphism:

   $f : G \to G',\ \ f(g) = 1'\ \forall g \in G$

   $\forall a, b \in G, f(a)f(b) = 1' \cdot 1' = 1' = f(ab)$

Properties

If $f : G \to G'$ i s a homomophism, then

1. $f(1) = 1'$ (Identity maps to Identity)
2. $\forall g \in G, f(g)^{-1} = f(g^{-1})$

Proof

1. $f(1) = f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) = 1'$
2. $\forall g \in G,$

$$f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1'$$

$$f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1'$$

   so $f(g^{-1})$ is the inverse of $f(g)$, i.e., $f(g)^{-1} = f(g^{-1})$

Kernel and Image

Definition

If $f : G \to G'$ is a homomorphism.

- Define the Kernel of f: $\ker(f) = \{g \in G | f(g) = 1'\}$.
- Define image or range of f: $Im(f) = \{f(g) \in G' | g \in G\}$

Prop

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

- **Proof**

1. - $\forall a, b \in \ker(f), f(a) = f(b) = 1', \quad f(ab) = f(a)f(b) = 1' \cdot 1' = 1'$

     so $ab \in \ker(f)$
   - $1 \in \ker(f)$ since $f(1) = 1'$
   - $\forall a \in \ker(f), f(a) = 1', f(a^{-1}) = f(a)^{-1} = 1'^{-1} = 1'$

     so $a^{-1} \in \ker(f)$

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

2. - $\forall f(a), f(b) \in Im(f), a, b \in G$. So $ab \in G, f(ab) \in G'$.

     So $ab \in Im(f)$
   - $f(1) = 1'$. So $1' \in Im(f)$
   - $\forall f(a) \in Im(f),\ a, a' \in G.\ f(a)^{-1} = f(a^{-1}) \in G'$

- **Prop**

If $f : G \to G'$ is a homomorphism, then f is injective if and only if $\ker(f) = \{1\}$.

> Note that f must be a homomorphism, and kernel is only defined for homomorphisms

- **Proof**

- If $\ker(f) = 1$:
  - For any $a, b \in G$ with $f(a) = f(b)$

$$\begin{aligned} f(b)^{-1}f(a) &= 1' \\ f(b^{-1})f(a) &= 1' \\ f(b^{-1}a) &= 1' \end{aligned}$$

  - So $b^{-1}a \in \ker(f) = \{1\}, b^{-1}a = 1,\ a = b$
  - The function f is injective
- If f is injective:
  - The $\ker(f) = \{g \in G | f(1) = 1'\}$ consistes of at most 1 element
  - $1 \in \ker(f)$
  - So $\ker(f) = \{1\}$

- **Examples**

1. Fix $x \in G$.

   Define $\ f : \mathbb{Z} \to G.\ \ f(k) = x^k$

$$\begin{aligned} \ker(f) &= \{k \in \mathbb{Z} | f(k) = 1\} \\ &= \{k \in \mathbb{Z} | x^k = 1\} \\ &= \begin{cases} \{0\}, & |x| = \infty \\ |x|\mathbb{Z}, & |x| < \infty \end{cases} \end{aligned}$$

$$
\begin{aligned}
Im(f) &= \{f(k) \in G | k \in \mathbb{Z}\} \\
&= \{x^k \in G | k \in \mathbb{Z}\} \\
&= < x >
\end{aligned}
$$

> "
>
> Proposition:
>
> In fact, If $f : \mathbb{Z} \to G$ is a homomorphism, then $\exists x \in G,\ f(k) = x^k$
>
> Proof:
>
> Let $x = f(1)$.
>
> If $k > 0$, $f(k) = f(1 + 1 + ... + 1)$ (k copies) $= (f(1))^k = x^k$
>
> For $k \leq 0$, similar argument.
>
> Therefore we can verify that $f(k) = x^k$ and $f(1) = x$
>
> **It tells us** that **Homomorphisms from** $\mathbb{Z}$ **to** G are of this form of $f(k) = x^k$
>
> And for each homomorphism, it gives us the corresponding cyclic subgroup as a image.
>
> This is another way of interpretation of **cyclic subgroups**
>
> Each subgroup can be seen as the image of a homomorphism from $\mathbb{Z}$ to G in the form that $f(x) = x^k$
>
> (01:06:51)

2. Trivial homomorphism:

   $f : G \to G', \quad f(g) = 1' \ \forall g \in G$

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

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

> "
>
> Roughly speaking, **larger** $\ker(f)$ **leads to smaller** $Im(f)$
>
> Also, if the kernel is bigger, the function is far from injective. If the kernel is the smallest, the function is injective.
>
> We'll prove later that $|ker(f)| \cdot |Im(f)| = |G|$