First Isomorphism & Product Groups: 2022/10/12

First Isomorphism Theorem

- **Lemma**

Lemma. $f: G \to G'$ is a homomorphism. $a, b \in G$.

Then $f(a) = f(b) \iff aN = bN$. where $N = \ker(f)$.

Pf. "$\Rightarrow$": If $f(a) = f(b)$.

Then $f(b)^{-1} f(a) = 1'$ $\Rightarrow f(b^{-1}a) = 1'$

$\Rightarrow b^{-1}a \in N$

$\Rightarrow aN = bN$

"$\Leftarrow$": If $aN = bN$.

Then $\exists\, n \in N$ such that $b = an$.

$f(b) = f(an) = f(a)f(n) = f(a) \cdot 1' = f(a)$

- Theorem

Theorem (First Isomorphism Theorem).

$f: G \to G'$ is a surjective homomorphism. Then there exists unique homomorphism $F: G/N \to G'$ ($N = \ker(f)$) such that F is an isomorphism and $f = F \circ \pi$, where $\pi: G \to G/N$, $\pi(g) = gN$ is the qustient map.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/N \arrow[ur, dashed, "\exists! F"'] & \end{tikzcd}$$

- Proof

$\pi(g)=gN$ is the

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/N \arrow[ur, dashed, "\exists! F"'] & \end{tikzcd}$$

Pf. Define $F: G/N \to G'$ by

$$F(gN) = f(g).$$

- Verify F is well-defined:

  If $aN = bN$, then by Lemma, we know $f(a) = f(b)$, i.e., $F(aN) = F(bN)$.

- F is a homomorphism:

  $$F(g_1N \cdot g_2N) = F(g_1g_2N) = f(g_1g_2) = f(g_1)f(g_2) = F(g_1N) \cdot F(g_2N).$$

- F is the unique homomorphism satisfying $f = F \circ \pi$

  Assume F and F' both satisfy $f = F \circ \pi$

  Then
  $$\left.\begin{array}{l} f(g) = F \circ \pi(g) = F(gN) \\ \quad \| \\ F' \circ \pi(g) = F'(gN) \end{array} \quad \forall g \in G \right\} \Rightarrow F = F'$$

- F is one-to-one by the <u>Lemma</u>: $F(aN) = F(bN) \Rightarrow f(a) = f(b)$
$\Rightarrow aN = bN$
- F is onto since f is onto.
$\forall g' \in G'$. $\exists g \in G$, $f(g) = g'$. Then $g' = F(gN)$.

We conclude F is the unique isomorphism satisfying $\underline{f = F \circ \pi}$.

In particular, we see $\boxed{G/N \cong G'}$ for surjective $f: G \to G'$.

- Cor

<u>Cor</u>. $f: G \to G'$ is a homomorphism. $N = \ker(f)$. Then $G/N \cong \mathrm{Im}(f)$

Pf. We can consider f as $f: G \to \mathrm{Im}(f)$. Then it becomes surjective. so we can apply the Theorem.

<u>Cor</u>. If G is a finite group. $f: G \to G'$ is a homomorphism.
Then: $|G| = |\ker(f)| \cdot |\mathrm{Im}(f)|$

<u>Pf</u>. By the previous <u>Cor</u>. $G/N \cong \mathrm{Im}(f)$.

$$\frac{|G|}{|N|} = [G:N] = |G/N| = |\mathrm{Im}(f)| \Rightarrow |G| = |\ker(f)| \cdot |\mathrm{Im}(f)|$$

<u>Remark</u>. It implies $|\mathrm{Im}(f)|$ divides $|G|$.

<u>Cor</u>. If $f: G \to G'$ is a homomorphism. $\gcd(|G|, |G'|) = 1$.
Then f is the trivial map. (i.e., $\forall g \in G$, $f(g) = 1'$).

<u>Pf</u>. We just saw $|\mathrm{Im}(f)|$ divides $|G|$.
Also, $\mathrm{Im}(f)$ is a subgroup of G', $|\mathrm{Im}(f)|$ divides $|G'|$
$\gcd(|G|, |G'|) = 1$. so $|\mathrm{Im}(f)| = 1$. $\mathrm{Im}(f) = \{1'\}$
This means $\forall g \in G$, $f(g) = 1'$.

- Examples

Example. ①. $G=\langle a\rangle$. cyclic group of order n.

$$\begin{aligned} f: \mathbb{Z} &\to G=\langle a\rangle \quad \text{is a surjective homomorphism.} \\ k &\mapsto a^k \end{aligned}$$

$$\operatorname{Ker}(f)=\{k\in\mathbb{Z} \mid a^k=1\}=\{k\in\mathbb{Z} \mid n \text{ divides } k\}=n\mathbb{Z}$$

By The First Isomorphism Theorem: $\mathbb{Z}/n\mathbb{Z} \cong G=\langle a\rangle$

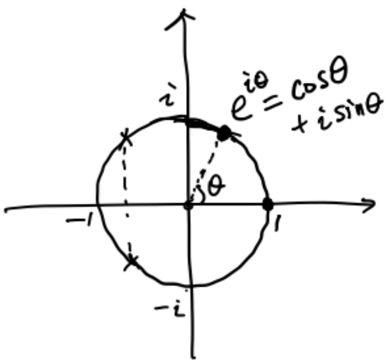
so If $G_1=\langle a\rangle$ and $G_2=\langle b\rangle$ are both cyclic groups of order n, then $G_1 \cong \mathbb{Z}/n\mathbb{Z} \cong G_2$.

We can say that, up to isomorphism, there's a unique group of order p, if p is prime.

②. $(\mathbb{R},+)$ is a group.

Let S^1 be the group of complex numbers of length 1. composition is multiplication.

$$\boxed{e^{i\theta_1}\cdot e^{i\theta_2}=e^{i(\theta_1+\theta_2)}}$$



Remark. S^1 is a subgroup of $\mathbb{C}^\times$

$\mathbb{C}^\times=\mathbb{C}-\{0\}$, with multiplication.

Let
$$\begin{aligned} f: \mathbb{R} &\to S^1 \\ r &\mapsto e^{i\cdot 2\pi r} \end{aligned}$$

S^1: "sphere of dim 1".
S^2: "sphere of dim 2"
$S^k=\{\vec{v}\in\mathbb{R}^{k+1} \mid |\vec{v}|=1\}$
"k-sphere".

f is a homomorphism:

$$\begin{aligned} f(r_1+r_2)=e^{i\cdot 2\pi(r_1+r_2)} &= e^{i(2\pi r_1+2\pi r_2)} \\ &= e^{i\cdot 2\pi r_1}\cdot e^{i\cdot 2\pi r_2} \\ &= f(r_1)f(r_2) \end{aligned}$$

f is surjective:

$$\forall\ e^{i\theta}=e^{i\cdot 2\pi\cdot\frac{\theta}{2\pi}}=f\left(\tfrac{\theta}{2\pi}\right)$$

$$\begin{aligned} \ker(f) &= \{r\in\mathbb{R} \mid e^{i\cdot 2\pi r}=1\} \\ &= \{r\in\mathbb{R} \mid 2\pi r\in 2\pi\mathbb{Z}\} \\ &= \mathbb{Z} \end{aligned}$$

By the First Isomorphism Theorem.

$$\boxed{\mathbb{R}/\mathbb{Z} \cong S^1}$$

- $\pi: G\to G/N$. the quotient map defined by $\pi(g)=gN$.

is a homomorphism.

$\pi(ab) = abN = (aN).(bN) = \pi(a).\pi(b)$. $\boxed{\ker\pi = N}$

This implies that any normal subgroup N of G is the kernel of some homomorphism defined on G.

so "kernel" $\longleftrightarrow$ "normal subgroup"

Product Groups

- Definition

<u>Def</u>. G. G' are groups. Define their product group to be $G \times G'$, the set of all ordered pairs (g, g') with $g \in G, g' \in G'$. The composition is $(g_1, g_1').(g_2, g_2') = (g_1 g_2, g_1' g_2')$

It's not hard to verify the definition is a group. with identity $(1, 1')$. and inverse $(g, g')^{-1} = (g^{-1}, g'^{-1})$.

- Properties

Elementary Properties: • $|G\times G'| = |G|\cdot|G'|$

• We can identify $\begin{cases} G \text{ with } \{(g,1')\in G\times G' \mid g\in G\} \\ G' \text{ with } \{(1,g')\in G\times G' \mid g'\in G'\} \end{cases}$

Indeed they follow from the "inclusion"

$i_1 : G \to G\times G'$. $i_1(g) = (g, 1')$

$i_2 : G' \to G\times G'$. $i_2(g') = (1, g')$.

We identify G with $Im(i_1)$.

G' with $Im(i_2)$.

Under this identification. we see G & G' are normal subgroups in $G\times G'$.

$\forall\ (g,1')\in Im(i_1)$. $\forall\ (x,y)\in G\times G'$.

$$(x,y)(g,1')(x,y)^{-1} = (xg, y)(x^{-1}, y^{-1}) = (xgx^{-1}, yy^{-1})$$
$$= (xgx^{-1}, 1') \in Im(i_1)$$

similarly we can verify $Im(i_2)$.