# A Concrete Introduction to Number Theory and Algebra– 群同构、群同态与商群

Libin Wang

School of Computer Science, South China Normal University

November 10, 2021

# Table of contents

# Isomorphisms(同构.)

**Motivation.**

Many groups may have different appearances, however they are essentially same.

# Isomorphisms(同构).

## Definition of Isomorphism.

Two group $(\mathbb{G}, \cdot)$ and $(\mathbb{H}, \circ)$ are isomorphic if there exists a one-to-one and onto map $\phi : \mathbb{G} \mapsto \mathbb{H}$ such that the group operation is preserved; that is,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

for all $a$ and $b$ in $\mathbb{G}$. If $\mathbb{G}$ is isomorphic to $\mathbb{H}$, we write $\mathbb{G} \cong \mathbb{H}$. The map $\phi$ is called an isomorphism.

# Examples of Isomorphisms.

## Example

*$\mathbb{Z}_4 \cong \langle i \rangle$, since we can define a bijective map $\phi : \mathbb{Z}_4 \mapsto \langle i \rangle$ by $\phi(n) = i^n$. The map $\phi$ is one-to-one and onto, since*

$$\begin{aligned} \phi(0) &= 1 \\ \phi(1) &= i \\ \phi(2) &= -1 \\ \phi(3) &= -i. \end{aligned}$$

*Moreover, $\phi$ preserves the group operation, since*

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n).$$

# Examples of Isomorphisms.

## Isomorphic groups.

Since $\mathbb{Z}_8^* = \{1,3,5,7\}$, $\mathbb{Z}_{12}^* = \{1,5,7,11\}$, we can find an isomorphism $\phi$ to show that:

$$\mathbb{Z}_8^* \cong \mathbb{Z}_{12}^*$$

An isomorphism $\phi : \mathbb{Z}_8^* \mapsto \mathbb{Z}_{12}^*$ is defined by :

$$\begin{array}{ccc} 1 & \mapsto & 1 \\ 3 & \mapsto & 5 \\ 5 & \mapsto & 7 \\ 7 & \mapsto & 11 \end{array}$$

Can you find another isomorphism between these two groups?

# Examples of Isomorphisms.

(Question.)

Do $\mathbb{Z}_{61}^*$ isomorphic to $\mathbb{Z}_{77}^*$? Why or why not?

# Theorem about Isomorphisms.

## Proposition

*Let $\phi : \mathbb{G} \mapsto \mathbb{H}$ be an isomorphism of two groups, then the following statements are true.*

1. $\phi^{-1} : \mathbb{H} \mapsto \mathbb{G}$ *is an isomorphism;*
2. $|\mathbb{G}| = |\mathbb{H}|$*;*
3. *If* $\mathbb{G}$ *is abelian, then* $\mathbb{H}$ *is abelian;*
4. *If* $\mathbb{G}$ *is cyclic, then* $\mathbb{H}$ *is cyclic;*
5. *if* $\mathbb{G}$ *has a subgroup of order n, then* $\mathbb{H}$ *has a subgroup of order n.*

## Proof.

Left as an exercise. □

# Theorem about Isomorphisms.

**Theorem**

*All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.*

**Proof.**

Suppose $\mathbb{G}$ is a cyclic group with infinite order, and $g \in \mathbb{G}$ is a generator. Define $\phi : \mathbb{Z} \mapsto \mathbb{G}$ by $\phi : n \mapsto g^n$. Then

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Show $\phi$ is a bijective map. Left as an exercise. $\square$

# Theorem about Isomorphisms.

**Theorem**

*If $\mathbb{G}$ is a cyclic group of order $n$, then $\mathbb{G}$ is isomorphic to $\mathbb{Z}_n$.*

**Proof.**

Let $\mathbb{G}$ be a cyclic group with order $n$, generated by $g$. Define $\phi : \mathbb{Z}_n \mapsto \mathbb{G}$ by $\phi : k \mapsto g^k$, where $0 \leq k < n$. Show $\phi$ is an isomorphism. Left as an exercise. $\square$

# Theorem about Isomorphisms.

**Corollary**

*If $\mathbb{G}$ is a cyclic group of order $p$ where $p$ is a prime, then $\mathbb{G}$ is isomorphic to $\mathbb{Z}_p$.*

**Proof.**

Easy! $\square$

# Theorem about Isomorphisms.

**Theorem**

*The isomorphism of groups determines an equivalence relation on the class of all groups.*

**Proof.**

Left as an exercise. $\square$

# Theorem about Isomorphisms.

**Theorem**

*(Cayley) Every group is isomorphic to a group of permutations.*

**Proof.**

Omitted. Note that, it is important. □

# Homomorphisms.（同态）

## Definition of Homomorphism.

Two group $(\mathbb{G}, \cdot)$ and $(\mathbb{H}, \circ)$ are homomorphic if there exists a map $\phi : \mathbb{G} \mapsto \mathbb{H}$ such that the group operation is preserved; that is,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

for all $a$ and $b$ in $\mathbb{G}$. The map $\phi$ is called a homomorphism.

## (Basic idea.)

We relax the requirement that an isomorphism of groups be bijective, we have a homomorphism.

# Examples of Homomorphisms.

## Example

$\mathbb{Z}$ 是加法群，定义映射 $\phi: \mathbb{Z} \mapsto \mathbb{Z}$ 为 $\phi(k) = 2k$，$\forall k \in \mathbb{Z}$。可以验证 $\phi$ 是一种群同态，因为

$$\phi(i + j) = 2(i + j) = 2i + 2j = \phi(i) + \phi(j)$$

$\phi$ 把整数映射为偶数。偶数在加法下成群。

# Examples of Homomorphisms.

## Example of Homomorphisms.

Let $\mathbb{G}$ be a group and $g \in \mathbb{G}$. Define a map $\phi : \mathbb{Z} \mapsto \mathbb{G}$ by $\phi(n) = g^n$. Then $\phi$ is a group homomorphism, since

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of $\mathbb{G}$ generated by $g$.

# Examples of Homomorphisms.

**Example**

设 $p$ 为素数，定义映射 $\phi : \mathbb{Z}_p^* \mapsto \mathbb{Z}_p^*$ 为 $\phi(g) = g^2$，$\forall g \in \mathbb{Z}_p^*$。可验证，$\phi$ 是一种同态映射，因为对任意的 $g_1, g_2 \in \mathbb{Z}_p^*$ 满足：$\phi(g_1 g_2) = (g_1 g_2)^2 = g_1^2 g_2^2 = \phi(g_1)\phi(g_2)$。

# Normal subgroups.

## Definition of normal subgroups.

A subgroup $\mathbb{N}$ of a group $\mathbb{G}$ is normal in $\mathbb{G}$ if $g\mathbb{N} = \mathbb{N}g$ for all $g \in \mathbb{G}$.

## (Basic idea 1.)

A normal subgroup is a subgroup that the right cosets and the left cosets are precisely the same, and $g\mathbb{N} = \mathbb{N}g$ represents a kind of "communitive(交换性)".

# Normal subgroups.

## Definition of normal subgroups.

A subgroup $\mathbb{N}$ of a group $\mathbb{G}$ is normal in $\mathbb{G}$ if $g\mathbb{N} = \mathbb{N}g$ for all $g \in \mathbb{G}$.

## (Basic idea 1.)

A normal subgroup is a subgroup that the right cosets and the left cosets are precisely the same, and $g\mathbb{N} = \mathbb{N}g$ represents a kind of "communitive(交换性)".

## (Basic idea 2.)

A subgroup $\mathbb{N}$ of a group $\mathbb{G}$ is normal in $\mathbb{G}$ iff $\forall g \in \mathbb{G}$, $g\mathbb{N}g^{-1} \subset \mathbb{N}$. Moreover, for all $\forall g \in \mathbb{G}$, $g\mathbb{N}g^{-1} = \mathbb{N}$

# Basic Properties of Normal Subgroup.

## Proposition

*Let $\mathbb{G}$ be a group and $\mathbb{N}$ be a subgroup of $\mathbb{G}$. Then the following statements are equivalent.*

1. *The subgroup $\mathbb{N}$ is a normal subgroup of $\mathbb{G}$, namely, $g\mathbb{N} = \mathbb{N}g$ for all $g \in \mathbb{G}$.*
2. *For all $g \in \mathbb{G}$, $g\mathbb{N}g^{-1} = \mathbb{N}$.*

# Basic Properties of Normal Subgroup.

**Proof.**

(Proof of last proposition.) $(1) \implies (2)$. Since $\mathbb{N}$ is a normal subgroup of $\mathbb{G}$, $g\mathbb{N} = \mathbb{N}g$ for all $g \in \mathbb{G}$. Hence, for a given $g \in \mathbb{G}$ and $n \in \mathbb{N}$, there exists an $n' \in \mathbb{N}$ such that $gn = n'g$. Therefore, $gng^{-1} = n' \in \mathbb{N}$ or $g\mathbb{N}g^{-1} \subset \mathbb{N}$. For $n \in \mathbb{N}$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in \mathbb{N}$. Hence, $g^{-1}ng = n'$ for some $n' \in \mathbb{N}$. Therefore, $n = gn'g^{-1} \in g\mathbb{N}g^{-1}$, namely, $\mathbb{N} \subset g\mathbb{N}g^{-1}$.
$(2) \implies (1)$. Suppose that for all $g \in \mathbb{G}$, $g\mathbb{N}g^{-1} = \mathbb{N}$. Then for any $n \in \mathbb{N}$ there exists an $n' \in \mathbb{N}$ such that $gng^{-1} = n'$. Consequently, $gn = n'g$ which means $g\mathbb{N} \subset \mathbb{N}g$. Similarly, we can prove that $\mathbb{N}g \subset g\mathbb{N}$. □

# Basic Properties of Homomorphisms.

## Proposition

*Proposition 1. Let $\phi : \mathbb{G}_1 \mapsto \mathbb{G}_2$ be a homomorphism of groups. Then*

1. *If e is the identity of $\mathbb{G}_1$, then $\phi(e)$ is the identity fo $\mathbb{G}_2$;*
2. *For any element $g \in \mathbb{G}_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *If $\mathbb{H}_1$ is a subgroup of $\mathbb{G}_1$, then $\phi(\mathbb{H}_1)$ is a subgroup of $\mathbb{G}_2$;*
4. *If $\mathbb{H}_2$ is a subgroup of $\mathbb{G}_2$, then $\phi^{-1}(\mathbb{H}_2)$ is a subgroup of $\mathbb{G}_1$. Furtheremore, if $\mathbb{H}_2$ is normal in $\mathbb{G}_2$, then $\phi^{-1}(\mathbb{H}_2)$ is normal in $\mathbb{G}_1$.*

# Basic Properties of Homomorphisms.

## Proposition

*Proposition 1. Let* $\phi : \mathbb{G}_1 \mapsto \mathbb{G}_2$ *be a homomorphism of groups. Then*

1. *If e is the identity of* $\mathbb{G}_1$, *then* $\phi(e)$ *is the identity fo* $\mathbb{G}_2$;
2. *For any element* $g \in \mathbb{G}_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;
3. *If* $\mathbb{H}_1$ *is a subgroup of* $\mathbb{G}_1$, *then* $\phi(\mathbb{H}_1)$ *is a subgroup of* $\mathbb{G}_2$;
4. *If* $\mathbb{H}_2$ *is a subgroup of* $\mathbb{G}_2$, *then* $\phi^{-1}(\mathbb{H}_2)$ *is a subgroup of* $\mathbb{G}_1$. *Furtheremore, if* $\mathbb{H}_2$ *is normal in* $\mathbb{G}_2$, *then* $\phi^{-1}(\mathbb{H}_2)$ *is normal in* $\mathbb{G}_1$.

## Proof.

Omitted. □

# Basic Properties of Homomorphisms.

## Definition

(Definition of Kernel.) Let $\phi : \mathbb{G} \mapsto \mathbb{H}$ be a group homomorphism and $e$ is the identity of $\mathbb{H}$. By previous proposition, $\phi^{-1}(\{e\})$ is subgroup of $\mathbb{G}$. This subgroup is called the kernel of $\phi$ and denoted by $\ker \phi$.

# Basic Properties of Homomorphisms.

**Definition**

(Definition of Kernel.) Let $\phi : \mathbb{G} \mapsto \mathbb{H}$ be a group homomorphism and $e$ is the identity of $\mathbb{H}$. By previous proposition, $\phi^{-1}(\{e\})$ is subgroup of $\mathbb{G}$. This subgroup is called the kernel of $\phi$ and denoted by ker $\phi$.

**Example**

设 $p$ 为素数，同态映射 $\phi : \mathbb{Z}_p^* \mapsto \mathbb{Z}_p^*$ 定义为 $\phi(g) = g^2$，$\forall g \in \mathbb{Z}_p^*$。可验证，$\phi$ 把 $\{1, p-1\}$ 映射为群 $\phi(\mathbb{Z}_p^*)$ 的单位元 1，所以 Ker $\phi = \{1, p-1\}$。

# Basic Properties of Homomorphisms.

**Proposition**

*(Kernel.) Let $\phi : \mathbb{G} \mapsto \mathbb{H}$ be a group homomorphism. Then the kernel of $\phi$ is a normal subgroup of $\mathbb{G}$.*

# Basic Properties of Homomorphisms.

**Proposition**

*(Kernel.) Let $\phi : \mathbb{G} \mapsto \mathbb{H}$ be a group homomorphism. Then the kernel of $\phi$ is a normal subgroup of $\mathbb{G}$.*

**Proof.**

Trivial. Since the trivial subgroup of $\mathbb{H}$ is normal. $\square$

# Quotient Groups.(商群)

**Definition**

If $\mathbb{N}$ is a normal subgroup of a group $\mathbb{G}$, then the cosets of $\mathbb{N}$ in $\mathbb{G}$ form a group $\mathbb{G}/\mathbb{N}$ under the operation $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$. This group is call the *quotient group* or *factor group* of $\mathbb{G}$ and $\mathbb{N}$.

# Quotient Groups.(商群)

## Definition

If $\mathbb{N}$ is a normal subgroup of a group $\mathbb{G}$, then the cosets of $\mathbb{N}$ in $\mathbb{G}$ form a group $\mathbb{G}/\mathbb{N}$ under the operation $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$. This group is call the *quotient group* or *factor group* of $\mathbb{G}$ and $\mathbb{N}$.

## Understand the operation.

How to understand the operation $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$?

# Quotient Groups.(商群)

## Definition

If $\mathbb{N}$ is a normal subgroup of a group $\mathbb{G}$, then the cosets of $\mathbb{N}$ in $\mathbb{G}$ form a group $\mathbb{G}/\mathbb{N}$ under the operation $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$. This group is call the *quotient group* or *factor group* of $\mathbb{G}$ and $\mathbb{N}$.

## Understand the operation.

How to understand the operation $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$?
Since $\mathbb{N}$ is normal, then:

$$(a\mathbb{N})(b\mathbb{N}) = (\mathbb{N}a)(b\mathbb{N}) = (ab\mathbb{N})\mathbb{N} = ab\mathbb{N}$$

# Example for Quotient Groups.

## (Example of Quotient Groups).

Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$. The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are

$$0 + 3\mathbb{Z} = \{\cdots, -3, 0, 3, 6, \cdots\}$$

$$1 + 3\mathbb{Z} = \{\cdots, -2, 1, 4, 7, \cdots\}$$

$$2 + 3\mathbb{Z} = \{\cdots, -1, 2, 5, 8, \cdots\}.$$

The group $\mathbb{Z}/3\mathbb{Z}$ is given by the multiplicative table below.

| $+$ | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ |
|---|---|---|---|
| $0 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ |
| $1 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ |
| $2 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ |

# Theorem of Quotient Groups.

**Theorem**

*(Quotient Groups). If $\mathbb{N}$ is a normal subgroup of a group $\mathbb{G}$, then the cosets of $\mathbb{N}$ in $\mathbb{G}$ form a group $\mathbb{G}/\mathbb{N}$ of order $[\mathbb{G} : \mathbb{N}]$.*

# Theorem of Quotient Groups.

## Proof.

(Basic ideas.)

1. What is the group operation? $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$

# Theorem of Quotient Groups.

**Proof.**

(Basic ideas.)

1. What is the group operation? $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$
2. Prove this operation is well-defined; that is group operation must be independent of the choice of coset representative. Let $a\mathbb{N} = b\mathbb{N}$, $c\mathbb{N} = d\mathbb{N}$. We must prove that

$$(a\mathbb{N})(c\mathbb{N}) = ac\mathbb{N} = bd\mathbb{N} = (b\mathbb{N})(d\mathbb{N})$$

# Theorem of Quotient Groups.

**Proof.**

(Basic ideas.)

1. What is the group operation? $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$
2. Prove this operation is well-defined; that is group operation must be independent of the choice of coset representative. Let $a\mathbb{N} = b\mathbb{N}$, $c\mathbb{N} = d\mathbb{N}$. We must prove that

$$(a\mathbb{N})(c\mathbb{N}) = ac\mathbb{N} = bd\mathbb{N} = (b\mathbb{N})(d\mathbb{N})$$

3. Why we need "well-defined"?

# Theorem of Quotient Groups.

## Proof.

(Basic ideas.)

1. What is the group operation? $(a\mathbb{N})(b\mathbb{N}) = ab\mathbb{N}$
2. Prove this operation is well-defined; that is group operation must be independent of the choice of coset representative. Let $a\mathbb{N} = b\mathbb{N}$, $c\mathbb{N} = d\mathbb{N}$. We must prove that

$$(a\mathbb{N})(c\mathbb{N}) = ac\mathbb{N} = bd\mathbb{N} = (b\mathbb{N})(d\mathbb{N})$$

3. Why we need "well-defined"?
4. Check the axioms of group. Easy!

□

# Theorem of Quotient Groups.

## Remark

*(良定义操作.) 所谓良定义的操作，就是要求操作独立于所参与操作的代表元。比如，对任意群 $\mathbb{G}$ 和其上的某种操作 $\psi : \mathbb{G} \mapsto \mathbb{G}$，要求 $\psi$ 良定义就是要求对任意的群元 $a, b \in \mathbb{G}$，如果 $a = b$，则 $\psi(a) = \psi(b)$。一眼看上去，这个要求很无理，毫无意义，但是对于商群来说就必不可少。请注意，商群中操作的是陪集，$a\mathbb{H} = b\mathbb{H}$ 并不意味 $a = b$。*

# Theorem of Quotient Groups.

## Remark

*(Some details.) Let* $a\mathbb{N} = b\mathbb{N}$, $c\mathbb{N} = d\mathbb{N}$. *We must prove that*

$$(a\mathbb{N})(c\mathbb{N}) = ac\mathbb{N} = bd\mathbb{N} = (b\mathbb{N})(d\mathbb{N})$$

# Theorem of Quotient Groups.

## Remark

*(Some details.) Let* $a\mathbb{N} = b\mathbb{N}$, $c\mathbb{N} = d\mathbb{N}$. *We must prove that*

$$(a\mathbb{N})(c\mathbb{N}) = ac\mathbb{N} = bd\mathbb{N} = (b\mathbb{N})(d\mathbb{N})$$

*For* $a = bn_1$ *and* $c = dn_2$ *for some* $n_1$ *and* $n_2$ *in* $\mathbb{N}$. *Hence,*

$$\begin{aligned} ac\mathbb{N} &= bn_1dn_2\mathbb{N} \\ &= bn_1d\mathbb{N} \\ &= bn_1\mathbb{N}d \\ &= b\mathbb{N}d \\ &= bd\mathbb{N} \end{aligned}$$

# Example for Quotient Groups.

**(Quotient Groups of $\mathbb{Z}_n^*$).**

Let $n = 15$, then $\mathbb{Z}_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Let $g = 2$, we set $\mathbb{S} = \langle g \rangle = \{1, 2, 4, 8\}$ which is a subgroup of $\mathbb{Z}_n^*$. Then $\mathbb{Z}_n^*/7\mathbb{S} = \{\mathbb{S}, 7\mathbb{S}\}$, please check that $\mathbb{S}$ is the identity, $7\mathbb{S}$'s inverse is itself, namely $(7\mathbb{S})(7\mathbb{S}) = 4\mathbb{S} = \mathbb{S}$.

# Canonical Homomorphism.

**(Canonical Homomorphism.)**

Let $\mathbb{H}$ be a normal subgroup of $\mathbb{G}$, define a map

$$\phi : \mathbb{G} \mapsto \mathbb{G}/\mathbb{H}$$

by

$$\phi(g) = g\mathbb{H}.$$

This map is indeed a homomorphism, check it! We call this map a natural or canonical homomorphism, and $\ker \phi = \mathbb{H}$.

# First Isomorphism Theorem.

## Theorem

*(First Isomorphism Theorem.) If* $\psi : \mathbb{G} \mapsto \mathbb{H}$ *is a group homomorphism with* $\mathbb{K} = \ker \psi$*, then* $\mathbb{K}$ *is normal in* $\mathbb{G}$*. Let* $\phi : \mathbb{G} \mapsto \mathbb{G}/\mathbb{K}$ *be the canonical homomorphism. Then there exists a unique isomorphism* $\eta : \mathbb{G}/\mathbb{K} \mapsto \psi(\mathbb{G})$ *such that* $\psi = \eta\phi$*.*

# First Isomorphism Theorem.

**(Proof ideas.)**

1. Define $\eta : \mathbb{G}/\mathbb{K} \mapsto \psi(\mathbb{G})$ by $\eta(g\mathbb{K}) = \psi(g)$;
2. Prove $\eta$ is well-defined;
3. Prove that $\eta$ is a homomorphism and is a bijective map.

# First Isomorphism Theorem.

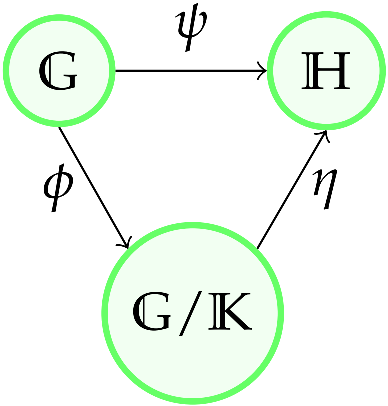


Figure: A diagrammatic interpretation of First Isomorphism Theorem.

# Example for First Isomorphism Theorem.

## (Homomorphism from Cyclic Group.)

设 $\mathbb{G}$ 是由生成元 $g$ 生成的循环群。定义映射 $\phi : \mathbb{Z} \mapsto \mathbb{G}$ 为 $n \mapsto \ g^n$，$\forall n \in \mathbb{Z}$。$\phi$ 是同态映射，因为：

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)。$$

$\phi$ 显然是满射。如果 $\mathbb{G}$ 的阶为 $m$，因为 $g$ 是生成元，则 $ord(g) = m$。于是，$g^m = e$，且有 $\text{Ker } \phi = m\mathbb{Z}$。根据第一同构定理，则有：

$$\mathbb{Z}/\text{Ker } \phi = \mathbb{Z}/m\mathbb{Z} \cong \mathbb{G}。$$

如果 $\mathbb{G}$ 是无限阶，则 $g$ 也是无限阶，则 $\text{Ker } \phi = \{0\}$，则 $\mathbb{Z}$ 与 $\mathbb{G}$ 同构。因此，两个循环群同构当且仅当它们有相同的阶。在同构的意义上，只有两种循环群：$\mathbb{Z}$ 和 $\mathbb{Z}_n$。

# Example for First Isomorphism Theorem.

## (Homomorphism from $\mathbb{Z}_p^*$ to $\mathbb{Z}_p^*$.)

Let $p$ be a prime, $\mathbb{Z}_p^*$ is a cyclic group. Define a map $\phi : \mathbb{Z}_p^* \mapsto \mathbb{Z}_p^*$ by $\phi(g) = g^2$ for all $g \in \mathbb{Z}_p^*$. Then $\phi$ is a group homomorphism, since

$$\phi(g_1 g_2) = (g_1 g_2)^2 = g_1^2 g_2^2 = \phi(g_1)\phi(g_2).$$

Clearly $\phi$ is not onto, and Ker $\phi = \{1, p-1\}$ is a normal subgroup of $\mathbb{Z}_p^*$. We know Ker $\phi$ because we believe that the following equation

$$x^2 \equiv 1 \pmod{p}$$

has only two solutions, namely $1$ and $p-1$. Check that $\mathbb{S} = \{\phi(g) : \text{for all } g \in \mathbb{Z}_p^*\}$ is a group. What is the order of $\mathbb{S}$? By the First Isomorphism Theorem, $|\mathbb{S}| = |\mathbb{Z}_p^*/\text{Ker } \phi| = |\mathbb{Z}_p^*|/|\text{Ker } \phi|$.

# Example for First Isomorphism Theorem.

**(Homomorphism from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$.)**

Let $n = pq$ be a composite integer, $p$ and $q$ are two primes, and $\mathbb{Z}_n^*$ is a group. Define a map $\phi : \mathbb{Z}_n^* \mapsto \mathbb{Z}_n^*$ by $\phi(g) = g^2$ for all $g \in \mathbb{Z}_n^*$. Then $\phi$ is a group homomorphism. $\mathbb{S} = \{\phi(g) : \text{for all } g \in \mathbb{Z}_n^*\}$, if we know the order of Ker $\phi$, then we know the order of $\mathbb{S} = |\mathbb{Z}_n^*|/|\text{Ker } \phi|$ by the First Isomorphism Theorem. How many solutions does the following equation have?

$$x^2 \equiv 1 \pmod{n}$$

Unfortunately, we donot solve it until we learn CRT.

# Example for First Isomorphism Theorem.

## Homomorphism for Signed Group

Let $n$ be a positive integer. For $x \in \mathbb{Z}_n$, we define $|x|$ as the absolute value of $x$, where $x$ is represented as a signed integer in the set $\{-(n-1)/2, \cdots, (n-1)/2\}$. From $\mathbb{Z}_n^*$, we define the set $\mathbb{G}^+$ as

$$\mathbb{G}^+ = \{|x| : x \in \mathbb{Z}_n^*\}$$

with the following operations

$$g \circ h = |g \cdot h \bmod n|,$$

where $g, h \in \mathbb{G}^+$. We know that $(\mathbb{G}^+, \circ)$ is indeed a group. What is the order of the group, and why?

# Example for First Isomorphism Theorem.

## Find the order of $\mathbb{G}^+$.

$$\mathbb{G}^+ = \{|x| : x \in \mathbb{Z}_n^*\}$$

## Answer.

We observe that taking absolute value is a homomorphism, since

$$\phi(x \cdot y) = |x \cdot y| = |x| \circ |y| = \phi(x) \circ \phi(y)$$

Since $-1 \in \mathbb{Z}_n^*$, Ker$\phi = \{1, -1\}$. Then the oder of $\mathbb{G}^+$ is $|\mathbb{Z}_n^*|/2$.

# Second Isomorphism Theorem.

## Theorem

*(第二同构定理.)* $\mathbb{H}$ *是群* $\mathbb{G}$ *的子群（不必然是正规子群），*$\mathbb{K}$ *是群* $\mathbb{G}$ *的正规子群。则* $\mathbb{HK}$ *是群* $\mathbb{G}$ *的子群，*$\mathbb{H} \cap \mathbb{K}$ *是* $\mathbb{H}$ *的正规子群，且*

$$\mathbb{H}/(\mathbb{H} \cap \mathbb{K}) \cong \mathbb{HK}/\mathbb{K}\text{。}$$

# Correspondence Theorem.

**Correspondence Theorem. (对应定理)**

Let $\mathbb{N}$ be a normal subgroup of a group $\mathbb{G}$. Then $\mathbb{H} \mapsto \mathbb{H}/\mathbb{N}$ is a one-to-one correspondence between the set of subgroups $\mathbb{H}$ containing $\mathbb{N}$ and the set of subgroups of $\mathbb{G}/\mathbb{N}$. Furthermore, the normal subgroups of $\mathbb{G}$ containing $\mathbb{N}$ correspond to normal subgroups of $\mathbb{G}/\mathbb{N}$.

# Correspondence Theorem.(对应定理)

**Understanding Correspondence Theorem.**

1. What is the map $\mathbb{H} \mapsto \mathbb{H}/\mathbb{N}$?

## Correspondence Theorem.(对应定理)

### Understanding Correspondence Theorem.

1. What is the map $\mathbb{H} \mapsto \mathbb{H}/\mathbb{N}$?
2. A map: $\{$the set of subgroups $\mathbb{H}$ containing $\mathbb{N}\} \mapsto \{$the set of subgroups of $\mathbb{G}/\mathbb{N}\}$

# Correspondence Theorem.(对应定理)

**Understanding Correspondence Theorem.**

1. What is the map $\mathbb{H} \mapsto \mathbb{H}/\mathbb{N}$?
2. A map: $\{$the set of subgroups $\mathbb{H}$ containing $\mathbb{N}\} \mapsto$ $\{$the set of subgroups of $\mathbb{G}/\mathbb{N}\}$
3. To understand what is a subgroup of $\mathbb{G}/\mathbb{N}$?

# Correspondence Theorem.

## Proof ideas of the Correspondence Theorem.

1. $\mathbb{H}/\mathbb{N}$ is a subgroup of $\mathbb{G}/\mathbb{N}$;
2. The map $\mathbb{H} \mapsto \mathbb{H}/\mathbb{N}$ is one-to-one and onto;
3. $\mathbb{H}$ is normal in $\mathbb{G}$, if and only if $\mathbb{H}/\mathbb{N}$ is normal in $\mathbb{G}/\mathbb{N}$.

# Third Isomorphism Theorem.

**Theorem**

*(第三同构定理)* $\mathbb{H}$ *和* $\mathbb{K}$ *是群* $\mathbb{G}$ *的正规子群，且* $\mathbb{K} \subset \mathbb{H}$*。则:*

$$\mathbb{G}/\mathbb{H} \cong \frac{\mathbb{G}/\mathbb{K}}{\mathbb{H}/\mathbb{K}}。$$