Mathematics for Computer Science – Isomorphism, Homomorphism and Quotient Group.

Libin Wang

School of Computer Science, South China Normal University

April 18, 2025

Table of contents

本章概览.

学习思路.

本章有一条联系紧密的知识链：从同态、同构出发，经过Kernel、正规子群、商群等，最后到达同构定理。而这整条知识链围绕着一个核心目标：考察群结构。

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 ϕ 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 ϕ is one-to-one and onto, since

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

Moreover, ϕ 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 ϕ 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 ϕ 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 ϕ 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! □

Example.

单位根群.

$\mathbb{U}_n$ 与 $\mathbb{Z}_n$ 同构！请问，令 $n = p - 1$，$\mathbb{U}_n$ 与 $\mathbb{Z}_p^*$ 同构吗?

Theorem about Isomorphisms.

Theorem

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

Proof.

Left as an exercise. □

Theorem about Isomorphisms.

Theorem

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

Proof.

Omitted. Note that, it is important. □

关于 Isomorphisms 的提醒.

提醒.

同构是研究群结构的目标!

关于 Isomorphisms 的提醒.

提醒.

同构是研究群结构的目标!

提问.

同态的目标是什么?

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 ϕ 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 ϕ 是一种群同态，因为

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

ϕ 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 ϕ 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（正规子群）.

Definition of normal subgroups.

A subgroup $\mathbb{H}$ of a group $\mathbb{G}$ is normal in $\mathbb{G}$ if $g\mathbb{H} = \mathbb{H}g$ 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 $g\mathbb{H} = \mathbb{H}g$ represents a kind of "communitive(交换性)".

Normal subgroups（正规子群）.

Definition of normal subgroups.

A subgroup $\mathbb{H}$ of a group $\mathbb{G}$ is normal in $\mathbb{G}$ if $g\mathbb{H} = \mathbb{H}g$ 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 $g\mathbb{H} = \mathbb{H}g$ represents a kind of "communitive(交换性)".

(Basic idea 2.)

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

Basic Properties of Normal Subgroup.

Proposition

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

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

Basic Properties of Normal Subgroup.

Proof.

(Proof of last proposition–1.) $(1) \Rightarrow (2)$. Since $\mathbb{H}$ is a normal subgroup of $\mathbb{G}$, $g\mathbb{H} = \mathbb{H}g$ for all $g \in \mathbb{G}$. Hence, for a given $g \in \mathbb{G}$ and $h \in \mathbb{H}$, there exists an $h' \in \mathbb{H}$ such that $gh = h'g$. Therefore, $ghg^{-1} = h' \in \mathbb{H}$ or $g\mathbb{H}g^{-1} \subset \mathbb{H}$. For $h \in \mathbb{H}$, $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in \mathbb{H}$. Hence, $g^{-1}hg = h'$ for some $h' \in \mathbb{H}$. Therefore, $h = gh'g^{-1} \in g\mathbb{H}g^{-1}$, namely, $\mathbb{H} \subset g\mathbb{H}g^{-1}$. $\square$

Basic Properties of Normal Subgroup.

Proof.

(Proof of last proposition–2.)
$(2) \Rightarrow (1)$. Suppose that for all $g \in \mathbb{G}$, $g\mathbb{H}g^{-1} = \mathbb{H}$. Then for any $h \in \mathbb{H}$ there exists an $h' \in \mathbb{H}$ such that $ghg^{-1} = h'$. Consequently, $gh = h'g$ which means $g\mathbb{H} \subset \mathbb{H}g$. Similarly, we can prove that $\mathbb{H}g \subset g\mathbb{H}$. $\square$

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 ϕ and denoted by Ker ϕ.

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 ϕ and denoted by Ker ϕ.

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 ϕ 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* ϕ *is a normal subgroup of* $\mathbb{G}$*.*

Proof.

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

关于 Homomorphisms 的提醒.

提醒

同态是研究群结构的重要手段：通过群同态去找正规子群，即同态映射的 Kernel.

习题.

习题.

- 如果 $\mathbb{H}_1$ 和 $\mathbb{H}_2$ 是群 $\mathbb{G}$ 的正规子群，证明 $\mathbb{H}_1\mathbb{H}_2$ 也是群 $\mathbb{G}$ 的正规子群。
- 证明，$\mathbb{H}$ 是 $\mathbb{G}$ 的正规子群当且仅当对任意 $g \in \mathbb{G}$，$g\mathbb{H}g^{-1} \subset \mathbb{H}$。
- 定义映射 $\phi : \mathbb{G} \mapsto \mathbb{G}$ 为：$g \mapsto g^2$。请证明 ϕ 是一种群同态当且仅当 G 是阿贝尔群。
- 设 $\phi : \mathbb{G} \mapsto \mathbb{H}$ 是一种群同态。请证明：如果 $\mathbb{G}$ 是循环群，则 $\phi(\mathbb{G})$ 也是循环群；如果 $\mathbb{G}$ 是交换群，则 $\phi(\mathbb{G})$ 也是交换群。

Quotient Groups(商群).

Theorem

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

Quotient Groups(商群).

Theorem

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

Understand the operation.

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

Quotient Groups(商群).

Theorem

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

Understand the operation.

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

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

进一步理解商群的群操作.

Understand the operation.

To understand the operation $(a\mathbb{H})(b\mathbb{H}) = ab\mathbb{H}$, we show that since $\mathbb{H}$ is normal, then:

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

进一步理解商群的群操作.

Understand the operation.

To understand the operation $(a\mathbb{H})(b\mathbb{H}) = ab\mathbb{H}$, we show that since $\mathbb{H}$ is normal, then:

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

使用了两种属性:

- 正规子群的“交换性”
- 结合律

进一步理解商群的群操作.

Understand the operation.

To understand the operation $(a\mathbb{H})(b\mathbb{H}) = ab\mathbb{H}$, we show that since $\mathbb{H}$ is normal, then:

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

使用了两种属性:

- 正规子群的“交换性”
- 结合律

另一种理解.

有没有另一种理解方式? 借助正常的思维 (什么是正常思维?) 与底层定义（直接借助群元素的操作!)。

进一步理解商群的群操作.

正常思维!

我们需要证明 $(a\mathbb{H})(b\mathbb{H}) = ab\mathbb{H}$，即我们需要证明:

- $(a\mathbb{H})(b\mathbb{H}) \subset ab\mathbb{H}$
- $ab\mathbb{H} \subset (a\mathbb{H})(b\mathbb{H})$

进一步理解商群的群操作.

正常思维!

我们需要证明 $(a\mathbb{H})(b\mathbb{H}) = ab\mathbb{H}$，即我们需要证明:

- $(a\mathbb{H})(b\mathbb{H}) \subset ab\mathbb{H}$
- $ab\mathbb{H} \subset (a\mathbb{H})(b\mathbb{H})$

Proof.

要证明 $(a\mathbb{H})(b\mathbb{H}) \subset ab\mathbb{H}$，即任取 $ah_1bh_2 \in a\mathbb{H}b\mathbb{H}$，证 $ah_1bh_2 \in ab\mathbb{H}$。但是，这是容易的，因为:

$$
\begin{aligned}
ah_1bh_2 &= h_3abh_2 \\
&= abh_4h_2 \\
&= abh_5 \in ab\mathbb{H}
\end{aligned}
$$

另一个方向，证明 $ab\mathbb{H} \subset (a\mathbb{H})(b\mathbb{H})$ 则留给大家作为练习。 □

Theorem of Quotient Groups.

Theorem

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

Theorem of Quotient Groups.

Proof.

(Basic ideas.)

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

Theorem of Quotient Groups.

Proof.

(Basic ideas.)

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

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

Theorem of Quotient Groups.

Proof.

(Basic ideas.)

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

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

3. Why we need "well-defined"?

Theorem of Quotient Groups.

Proof.

(Basic ideas.)

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

Example

(非良定义操作与商群) 设有限循环群 $\mathbb{G} = \langle g \rangle$，$\mathbb{H}$ 是群 $\mathbb{G}$ 的子群，自然也是正规子群，于是形成商群 $\mathbb{G}/\mathbb{H}$。定义映射 $\phi_g : \mathbb{G}/\mathbb{H} \mapsto \mathbb{Z}$，对任意的 $a\mathbb{H}$，如果 $a = g^k$，则 $\phi_g(a\mathbb{H}) = k$。可以验证这是一种非良定义映射。

Theorem of Quotient Groups.

Example

(非良定义操作与商群) 比如，设 $p = 7$，则 $\mathbb{Z}_p^* = \{1, 2, 3, 4, 5, 6\}$，取生成元 $g = 3$。记 $\mathbb{S} = \{1, 6\}$，可验证 $\mathbb{S}$ 是 $\mathbb{Z}_p^*$ 的子群。所以形成商群，$\mathbb{Z}_p^*/\mathbb{S} = \{\mathbb{S}, 2\mathbb{S}, 3\mathbb{S}\}$。此时 $3\mathbb{S} = 4\mathbb{S}$，$\phi_3(3\mathbb{S}) = 1$，但是 $\phi_3(4\mathbb{S}) = 4$。也就是说，对同一个陪集，因为选取了不同的代表元，得到的映射值不同，该操作不能独立于代表元的选取。

Theorem of Quotient Groups.

Remark

(群操作的良定义性.) Let $a\mathbb{H} = b\mathbb{H}$, $c\mathbb{H} = d\mathbb{H}$. *We must prove that*

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

Theorem of Quotient Groups.

Remark

(群操作的良定义性.) Let $a\mathbb{H} = b\mathbb{H}$, $c\mathbb{H} = d\mathbb{H}$. *We must prove that*

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

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

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

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.

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

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 $(7\mathbb{S})(7\mathbb{S}) = 4\mathbb{S} = \mathbb{S}$.

Isomorphism Theorem.

同构定理.

上述知识点可以形成这样一条知识链：从一个群同态 $\phi : \mathbb{G}_1 \mapsto \mathbb{G}_2$ 出发。首先可以找到 ϕ 的 Kernel，于是得到一个 $\mathbb{G}_1$ 的正规子群；接着，构造 $\mathbb{G}_1$ 上的商群 $\mathbb{G}_1/\text{Ker}\ \phi$。从而完成我们一直以来的主要任务：研究群（商群）的结构！

Canonical Homomorphism.

正规同态（自然同态）.

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.

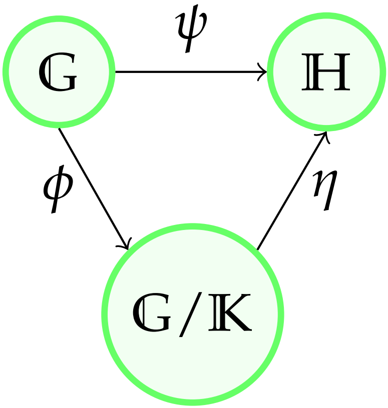

Figure: A diagrammatic interpretation of First Isomorphism Theorem.

First Isomorphism Theorem.

(证明思路.)

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

First Isomorphism Theorem.

(证明第一步.)

- 定义映射 $\eta : \mathbb{G}/\mathbb{K} \mapsto \psi(\mathbb{G})$ 为 $\eta(g\mathbb{K}) = \psi(g)$。

First Isomorphism Theorem.

(证明第二步.)

- 证明 η 是良定义映射，即证明如果对于两个不同的 $g_1, g_2 \in \mathbb{G}$，有 $g_1\mathbb{K} = g_2\mathbb{K}$，则 $\eta(g_1\mathbb{K}) = \eta(g_2\mathbb{K})$。因为 $g_1\mathbb{K} = g_2\mathbb{K}$，则存在 $k \in \mathbb{K}$ 使得 $g_1 = g_2 k$，这仅仅利用了陪集相等的定义。因此：

$$\eta(g_1\mathbb{K}) = \psi(g_1) = \psi(g_2 k) = \psi(g_2)\psi(k) = \psi(g_2) = \eta(g_2\mathbb{K})$$

  请注意，上式中第四个等号之所以成立是因为 $k \in \mathbb{K}$，而 $\mathbb{K}$ 是 ψ 的 Kernel，k 必然映射到 $\mathbb{H}$ 的单位元。这就证明了 η 映射独立于陪集代表元的选择。之所以 η 是唯一定义的，因为给定了 ψ 和 ϕ，而 $\psi = \eta\phi$，且 ϕ 是满射。

First Isomorphism Theorem.

(一个问题.)

确保 η 的唯一性，为什么需要 ϕ 是满射?（课后练习!）

First Isomorphism Theorem.

(证明第三步.)

- 可证明 η 是同态且是双射。η 是同态，因为：

$$\begin{aligned}\eta(g_1\mathbb{K}g_2\mathbb{K}) &= \eta(g_1g_2\mathbb{K})\\ &= \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2)\\ &= \eta(g_1\mathbb{K})\eta(g_2\mathbb{K})\end{aligned}$$

η 显然是满射，最后，只需证明 η 是单射。

First Isomorphism Theorem.

(证明第三步.)

- 可证明 η 是同态且是双射。η 是同态，因为：

$$\begin{aligned}\eta(g_1\mathbb{K}g_2\mathbb{K}) &= \eta(g_1g_2\mathbb{K})\\ &= \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2)\\ &= \eta(g_1\mathbb{K})\eta(g_2\mathbb{K})\end{aligned}$$

η 显然是满射，最后，只需证明 η 是单射。

(一点点提醒.)

为什么 η 显然是满射?

First Isomorphism Theorem.

(证明第三步.)

- 证明 η 是单射。任取 $g_1\mathbb{K}, g_2\mathbb{K}$，假设 $\eta(g_1\mathbb{K}) = \eta(g_2\mathbb{K})$，则 $\psi(g_1) = \psi(g_2)$。g_1 和 g_2 是 $\mathbb{G}$ 中两个不同的元素，所以

$$\psi(g_1) = \psi(g_2 g_2^{-1} g_1) = \psi(g_2)\psi(g_2^{-1} g_1)$$

即 $\psi(g_2^{-1} g_1)$ 是 $\psi(\mathbb{G})$ 的单位元，也即 $g_2^{-1} g_1 \in \mathbb{K}$。所以 $g_2^{-1} g_1\mathbb{K} = \mathbb{K}$，最后得到 $g_1\mathbb{K} = g_2\mathbb{K}$。

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 $n \mapsto g^n$，$\forall n \in \mathbb{Z}$。ϕ 是同态映射，因为：

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

ϕ 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 ϕ 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 ϕ is not onto, and Ker $\phi = \{1, p-1\}$ is a normal subgroup of $\mathbb{Z}_p^*$. We know Ker ϕ 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 ϕ is a group homomorphism. $\mathbb{S} = \{\phi(g) : \text{for all } g \in \mathbb{Z}_n^*\}$, if we know the order of Ker ϕ, 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 $\mathbb{H}$ be a normal subgroup of a group $\mathbb{G}$. Then $\mathbb{H} \mapsto \mathbb{H}/\mathbb{H}$ is a one-to-one correspondence between the set of subgroups $\mathbb{H}$ containing $\mathbb{H}$ and the set of subgroups of $\mathbb{G}/\mathbb{H}$. Furthermore, the normal subgroups of $\mathbb{G}$ containing $\mathbb{H}$ correspond to normal subgroups of $\mathbb{G}/\mathbb{H}$.

Correspondence Theorem.(对应定理)

Understanding Correspondence Theorem.

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

Correspondence Theorem.(对应定理)

Understanding Correspondence Theorem.

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

Correspondence Theorem.(对应定理)

Understanding Correspondence Theorem.

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

Correspondence Theorem.

Proof ideas of the Correspondence Theorem.

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

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:*

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

习题.

习题.

- 证明：如果 $\mathbb{H}$ 是群 $\mathbb{G}$ 上指标为 2 的子群，则 $\mathbb{H}$ 是 $\mathbb{G}$ 的正规子群。
- 给定任意群 $\mathbb{G}$，$\mathbb{H}$ 是群 $\mathbb{G}$ 的正规子群。请证明，如果群 $\mathbb{G}$ 是阿贝尔群，则商群 $\mathbb{G}/\mathbb{H}$ 也是阿贝尔群。
- 给定任意群 $\mathbb{G}$，$\mathbb{H}$ 是群 $\mathbb{G}$ 的正规子群。请证明，如果群 $\mathbb{G}$ 是循环群，则商群 $\mathbb{G}/\mathbb{H}$ 也是循环群。
- 设 p 和 q 是两个不同的素数，$\mathbb{G}$ 是阶为 pq 的阿贝尔群，请证明 $\mathbb{G}$ 是循环群。

习题讲解.

习题.

设 p 和 q 是两个不同的素数，$\mathbb{G}$ 是阶为 pq 的阿贝尔群，请证明 $\mathbb{G}$ 是循环群。

思路：找阶为 p 的群元 g_1 和阶为 q 的群元 g_2，则可知 g_1g_2 的阶是 pq，则 $\mathbb{G}$ 是循环群。

习题讲解.

习题.

设 p 和 q 是两个不同的素数，$\mathbb{G}$ 是阶为 pq 的阿贝尔群，请证明 $\mathbb{G}$ 是循环群。

思路：找阶为 p 的群元 g_1 和阶为 q 的群元 g_2，则可知 g_1g_2 的阶是 pq，则 $\mathbb{G}$ 是循环群。

Proof.

不妨假设存在阶为 p 的群元 g_1，$\mathbb{H} = \langle g_1 \rangle$ 为循环群。可得阶为 q 的商群 $\mathbb{G}/\mathbb{H}$，它也必然为循环群。记 $\mathbb{G}/\mathbb{H}$ 的生成元是 $g_2\mathbb{H}$。此时，g_2 的阶不能是 1。同时，g_2 的阶不能是 p，否则 $(g_2\mathbb{H})^p = \mathbb{H}$。如果 $p < q$，则 $g_2\mathbb{H}$ 不能是生成元。如果 $p > q$，则 q 整除 p，这是不可能的！所以，g_2 的阶只能是 q 或者 pq，无论是什么情况，$\mathbb{G}$ 都是循环群。 □

关于第一同构定理运用的习题.

习题.

- 证明：$\mathbb{GL}_n(R)/\mathbb{SL}_n(R)$ 与乘法群 $\mathbb{R}^*$ 同构。
- 证明商群 $\mathbb{R}/\mathbb{Z}$ 同构于圆圈群 $\mathbb{O}$。
- 设 $\phi : \mathbb{G} \mapsto \mathbb{H}$ 是一种群同态。请证明 ϕ 是单射当且仅当 $\text{Ker}\ \phi = \{e\}$。
- 给定有限阿贝尔群 $\mathbb{G}$ 和正整数 n，定义映射 $\phi : \mathbb{G} \mapsto \mathbb{G}$ 为，$\forall g \in \mathbb{G}$，$\phi(g) = g^n$。请分析并证明，在什么条件下 ϕ 会是一种单射?