Introduction to Topology

Group Theory, Lecture 16, 17

Haoming Wang

01 August 2019

This is the Lecture note for the *Introduction to Topology*. The course covers the following topics: Naive Set Theory, Elementary Number Theory, Group Theory, Topological Spaces and Continuous Maps, Introduction to Algebraic Topology.

Content:

Abelian Group

Definition 1 (Abelian Group)**.** Given a group $(G, \square)$, we say $(G, \square)$ is a abelian group if $\forall g, g' \in G, g\square g' = g'\square g$.

The set $\mathbb{Z} \times \mathbb{Z}$ is equivalent with $\{\{1,2\} \xrightarrow{f} \mathbb{Z} | f \text{ if a map}\}$. For any $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, it can be represented as $f : 1 \mapsto x, 2 \mapsto y$, $\{1,2\}$ is the ordinate. And for any maps $\{1,2\} \xrightarrow{f} \mathbb{Z}$, it is corresponded by $(f(1), f(2)) \in \mathbb{Z} \times \mathbb{Z}$.

Let S be a set, define

$$\mathbb{Z}^{\oplus S} := \{S \xrightarrow{f} \mathbb{Z} | f \text{ is a map s.t. } f(s) \neq 0 \text{ for finitely many } s \in S\}$$

The element of $\mathbb{Z}^{\oplus S}$ is encoding each element of S with integer, and only finite element of S will be encoded by nonzero integer.

Note 1. Sometimes, we will denote $S \xrightarrow{f} \mathbb{Z}$ by $(x_s)_{s\in S}$.

Example 1. The element of $\mathbb{Z}^{\oplus \mathbb{N}}$ is a series of integer $(x_1, x_2, \cdots)(x_i \in \mathbb{Z}, i \in \mathbb{N})$ which has only finite nonzero integers.

We can define add on $\mathbb{Z}^{\oplus S}$: $(x_s)_{s\in S} + (y_s)_{s\in S} = (x_s + y_s)_{s\in S}$. Then for any $(x_s)_{s\in S}, (y_s)_{s\in S} \in \mathbb{Z}^{\oplus S}$, the binary operation $(\mathbb{Z}^{\oplus S}, +)$ has

1. $(x_s + y_s)_{s\in S} \in \mathbb{Z}^{\oplus S}$ (for $(x_s)_{s\in S}, (y_s)_{s\in S}$ only has finite nonzero integers)
2. $e = (0)_{s\in S} \in \mathbb{Z}^{\oplus S}$
3. $((x_s)_{s\in S})^{-1} = (-x_s)_{s\in S} \in \mathbb{Z}^{\oplus S}$
4. $(x_s)_{s\in S} + (y_s)_{s\in S} = (x_s + y_s)_{s\in S} = (y_s)_{s\in S} + (x_s)_{s\in S}$

Thus $(\mathbb{Z}^{\oplus S}, +)$ is a abelian group, and we call $(\mathbb{Z}^{\oplus S}, +)$ as **Free Abelian Group**.

Definition 2 (Homomorphism)**.** Given two groups $(G, \square), (G', \square')$, a map $G \xrightarrow{T} G'$ is a homomorphism w.r.t. $\square$ and $\square'$ if $\forall g_1, g_2 \in G$, $T(g_1 \square g_2) = T(g_1)\square' T(g_2)$.

Note 2. The purpose of defining a group homomorphism is to create functions that preserve the algebraic structure. An equivalent definition of group homomorphism is: The map $G \xrightarrow{h} G'$ is a group homomorphism if whenever $a\square b = c$ we have $h(a)\square' h(b) = h(c)$.

In other words, the group G' in some sense has a similar algebraic structure as G and the homomorphism h preserves that.

Example 2. Map $\mathbb{Z} \xrightarrow{T} \mathbb{Z}/5\mathbb{Z}$ is a homomorphism, since for any $a, b \in \mathbb{Z}$, $(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) = (a + b) + 5\mathbb{Z}$.

Definition 3 (Isomorphism)**.** We say a homomorphism T is an isomorphism if T is a bijection.

Definition 4. Given two groups $(G, \square), (G', \square')$, let $G \xrightarrow{T} G'$ be a homomorphism:
1. $ker(T) := T^{-1}(e') = \{g \in G | T(g) = e'\}$;
2. $im(T) := T(G) = \{T(g) | g \in G\}$.

Exercise 1. Show that $ker(T)$ is a subgroup of $(G, \square)$, $im(T)$ is a subgroup of $(G', \square')$.

Proof. 1.
(0.) Obviously $ker(T) \subseteq G$.
(1.) for $\forall g_1, g_2 \in ker(T)$:

$$\begin{aligned} T(g_1 \square g_2) &= T(g_1) \square' T(g_2) \\ &= e' \square e' = e' \end{aligned}$$

thus $g_1 \square g_2 \in ker(T)$.
(2.) for $\forall g \in ker(T)$,

$$\begin{aligned} T(g) &= T(g \square e) \\ &= T(g) \square' T(e) \\ &= e' \square' T(e) = e' \end{aligned}$$

and $T(e) \square' e' = e'$ in the same way, thus $e \in ker(T)$, and be the unit element of $ker(T)$.
(3.) for $\forall g \in ker(T)$,

$$\begin{aligned} T(e) &= T(g \square g^{-1}) \\ &= T(g) \square' T(g^{-1}) \\ &= e' \square' T(g^{-1}) \\ &= e' \end{aligned}$$

and $T(g^{-1}) \square' e' = e'$, thus $T(g^{-1}) = e'$, and $g^{-1} \in ker(T)$.
Thus $ker(T)$ is a subgroup of $(G, \square)$.

2.
0. Obviously $im(T) \subseteq G'$.
1. for $\forall g_1', g_2' \in im(T), \exists g_1, g_2,$ s.t. $T(g_1) = g_1', T(g_2) = g_2'$. Thus

$$\begin{aligned} T(g_1 \square g_2) &= T(g_1) \square' T(g_2) \\ &= g_1' \square' g_2' \end{aligned}$$

thus $g_1' \square' g_2' \in im(T)$.
(2.) Since $e \in ker(T) \Rightarrow T(e) = e' \Rightarrow e' \in im(T)$.

(3.) for $\forall g' \in im(T), \exists g \in G,$ s.t. $T(g) = g'$, and

$$\begin{aligned} T(e) &= T(g \square g^{-1}) \\ &= T(g) \square' T(g^{-1}) \\ &= g' \square' T(g^{-1}) \\ &= e' \end{aligned}$$

and $T(g^{-1}) \square' g' = e'$ in the same way, thus $T(g^{-1}) = g'^{-1}, g'^{-1} \in im(T)$.

Thus $im(T)$ is a subgroup of G'. $\square$

Exercise 2. $G \xrightarrow{T} G'$ is a homomorphism show that $T(e) = e'$ and $T(g^{-1}) = T(g)^{-1}$ for $\forall g \in G$. e' is the unit element of $(G', \square')$,

Proof. 1. $ker(T)$ is a subgroup of G, thus $e \in ker(T) \Rightarrow T(e) = e'$. 2. $T(g^{-1}) \square' T(g) = T(g^{-1} \square g) = T(e) = e'$, thus $T(g^{-1}) = T(g)^{-1}$. $\square$

Definition 5. Given two groups $(G, \square), (G', \square')$, let $G \xrightarrow{T} G'$ be a homomorphism. If $(G', \square')$ is abelian, $cok(T) := G'/im(T)$.

Normal Subgroup

Consider a group $(G, \square)$ and natural projection π. Are there is map $\square'$ such that the following commutative diagram holds? i.e. for $\forall g_1, g_2, \pi(g_1 \square g_2) = \pi(g_1) \square' \pi(g_2)$?

$$\begin{tikzcd} {}_{(a,b)}G \times G^{(a,b)} \arrow[r, "\square"] \arrow[d, "\pi\times\pi"'] & G^{a\square b} \arrow[d, "\pi"] \\ {}_{(a\square H, b\square H)}G/H \times G/H \arrow[r, "\square'"] & {}_{(a\square H)\square'(b\square H)}G/H^{a\square b\square H} \end{tikzcd}$$

Note 3. Given maps f_1, f_2 and a surjection g, we have proved if $g \circ f_1 = g \circ f_2 \Rightarrow f_1 = f_2$, thus if $\square'$ exists, there would be only one.

In the other word, for $(a, b) \in G \times G$, we can define map $\square'$ as

$$(a \square H) \square' (b \square H) := a \square b \square H$$

But there is not well-defined, because there would exists $a', b' \in G$ such that $a' \square H = a \square H, b' \square H = b \square H$, thus $(a \square H) \square' (b \square H) = (a' \square H) \square' (b' \square H)$, but $a' \square b' \square H \neq a \square b \square H$.

Note 4. The definition of normal subgroup is equivalent with

1. $\forall g \in G, \forall h \in H, g \square h \square g^{-1} \in H$.
2. $g^{-1} \square H \square g \subseteq H$
3. $g \square H \square g^{-1} \subseteq H$
4. $g^{-1} \square H \square g = H$
5. $g \square H \square g^{-1} = H$

Definition 6 (Normal Subgroup)**.** Given a group $(G, \square)$, $(H, \square)$ is a subgroup of $(G, \square)$ (denote by $H \leq G$). We call H is a normal subgroup, denote by $H \trianglelefteq G$, if $\forall g \in G, \forall h \in H, g^{-1} \square h \square g \in H$.

Exercise 3. Show that the definition of normal subgroup is equivalent with $g^{-1} \square H \square g = H$.

Proof. $\forall g \in G, \forall h \in H$, $g^{-1}\Box h\Box g \in H \Leftrightarrow g^{-1}\Box H\Box g \subseteq H$ by the definition of coset. And then for $\forall g \in G, H\Box g \subseteq g\Box H$ and $g^{-1}\Box H \subseteq H\Box g^{-1} \Rightarrow g\Box H \subseteq H\Box g$ Because $g = (g^{-1})^{-1}$. So $g\Box H = H\Box g$ and $g^{-1}\Box H\Box g = H$. □

Exercise 4. If $H \trianglelefteq G$, show that $a^{-1}\Box a' \in H, b^{-1}\Box b' \in H \Rightarrow (a\Box b)^{-1}\Box(a'\Box b') \in H$, that is $H \trianglelefteq G$ is the **sufficient condition**.

Proof. Denote $a^{-1}\Box a' = h \in H$, $\exists h' \in H$, s.t. $b^{-1}\Box b' = h' \Rightarrow b' = b\Box h'$, thus

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

$H \trianglelefteq G \Rightarrow b^{-1}\Box h\Box b \in H \Rightarrow (a\Box b)^{-1}\Box(a'\Box b') \in H$. □

Note 5. a, a' belong to the same coset of $H \Leftrightarrow a\Box H = a'\Box H \Leftrightarrow a^{-1}a' \in H \Leftrightarrow a' = a\Box h$.

We have seen that if $H \trianglelefteq G$ then there is a binary operation $G/H \times G/H \xrightarrow{\Box'} G/H((a\Box H, b\Box H) \mapsto a\Box b\Box H)$, such that the commutative diagram

$$\begin{array}{ccc} G\times G & \xrightarrow{\Box} & G \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/H\times G/H & \xrightarrow{\Box'} & G/H \end{array}$$

holds.

Exercise 5 (Quotient Group)**.** $H \trianglelefteq G$, show that $(G/H, \Box')$ is a group.

Proof. 0. $H \trianglelefteq G \Rightarrow \Box'$ is well-defined by $(g_1\Box H)\Box'(g_2\Box H) := (g_1\Box g_2)\Box H$ for any $g_1, g_2 \in G$.

1. $\forall g_1, g_2 \in G, g_1\Box H, g_2\Box H \in G/H$, then $(g_1\Box H)\Box'(g_2\Box H) = (g_1\Box g_2)\Box H$. $g_1\Box g_2 \in G$ thus $(g_1\Box g_2)\Box H \in G/H$.

2. $\forall g \in G, g\Box H \in G/H$, then $(g\Box H)\Box H = (g\Box e)\Box H = g\Box H$, thus $e_{G/H} = H \in G/H$.

3. $(g\Box H)^{-1} = g^{-1}\Box H \in G/H$. □

Exercise 6. $G \xrightarrow{T} G'$ is a homomorphism, show that $ker(T) \trianglelefteq G$ and $im(T) \leq G'$.

Proof. 1. For $\forall g \in G, k \in ker(T)$,

$$\begin{aligned}T(g^{-1}\Box k\Box g) &= T(g^{-1})\Box' e'\Box' T(g)\\&= T(g)^{-1}\Box' T(g)\\&= e'\end{aligned}$$

Thus $g^{-1}\Box k\Box g \in ker(T) \Rightarrow ker(T) \trianglelefteq G$.

2. (1.) $T(g_1)\Box' T(g_2) = T(g_1\Box g_2) \in im(T)$; (2.) $e' = T(e) \in im(T)$; (3) $T(g)^{-1} = T(g^{-1}) \in im(T)$. □

Thus if subgroup $(H, \square)$ is normal then $(G/H, \square')$ is a group. Conversely, if $(G, \square)$ is abelian, then any subgroup $(H, \square)$ is normal, for $ghg^{-1} = gg^{-1}h = h \in H$; and $(G/H, \square')$ is abelian, for

$$\begin{aligned}
&(a\square H)\square'(b\square H)\\
&= a\square b\square H = b\square a\square H\\
&= (b\square H)\square'(a\square H).
\end{aligned}$$

Exercise 7. $G \xrightarrow{T} G'$ is a homomorphism, show that T is injection $\Leftrightarrow ker(T) = \{e\}$.

Proof. $\Rightarrow$: $\forall g \in G, k \in ker(T)$, $T(g\square k) = T(g)\square' T(k) = T(g)\square' e' = T(g) \Rightarrow g = g\square k$. Similarly, $g = k\square g$, thus $k = e(\forall k \in ker(T))$ and $ker(T) = \{e\}$.

$\Leftarrow$: For any $g_1, g_2 \in G$, if $T(g_1) = T(g_2)$, then

$$\begin{aligned}
T(g_2)\square T(g_2)^{-1} &= T(g_1)\square' T(g_2)^{-1}\\
&= T(g_1)\square' T(g_2^{-1})\\
&= T(g_1\square g_2^{-1})\\
&= e'
\end{aligned}$$

Thus $g_1\square g_2^{-1} \in ker(T) = \{e\} \Rightarrow g_1\square g_2^{-1} = e \Rightarrow g_1 = g_2$. $\square$

Theorem of Isomorphism

Theorem 1 (Theorem of homomorphism)**.** *Given groups $(G, \square)$ and $(G', \square')$, suppose $G \xrightarrow{T} G'$ is a homomorphism, $H \leq G$. Then*

1. *$T(H) = \{e'\}$, i.e. $H \subseteq ker(T) \Leftrightarrow \exists!$ map $G/H \xrightarrow{\tilde{T}} G'$ s.t.*

$$\begin{tikzcd}
G \arrow[rr, "T"] \arrow[dr, "\pi"'] & & G' \\
& G/H \arrow[ur, "\tilde{T}"'] &
\end{tikzcd}$$

2. *If $H \subseteq ker(T)$ and $H \trianglelefteq G$ then $G/H \xrightarrow{\tilde{T}} G'$ is a homomorphism.*
3. *$H = ker(T) \Leftrightarrow \tilde{T}$ is injection.*
4. *T is surjection $\Leftrightarrow \tilde{T}$ is surjection.*

Proof. 1. $\Leftarrow$: for $\forall h \in H$, $\pi(h) = \pi(e) = H$, thus

$$T(h) = \tilde{T} \circ \pi(h) = \tilde{T} \circ \pi(e) = T(e) = e',$$

thus $T(h) = e'(\forall h \in H)$, that is $H \subseteq ker(T)$.

$\Rightarrow$: Define $\tilde{T}(g\square H) := T(g)$. For any $g, g_1 \in G$, s.t. $\pi(g) = \pi(g_1)$, that is $g\square H = g_1\square H \Leftrightarrow \exists h \in H$ s.t. $g = g_1\square h$. Thus $T(g) = T(g_1\square h) = T(g_1)\square' T(h) = T(g_1)$. Thus the definition of $\tilde{T}$ is **well defined**. π is surjection $\Rightarrow \tilde{T}$ has uniqueness.

2. $H \trianglelefteq G$, thus $(G/H, \square^*)$ is a group, where $(g_1 \square G)\square^*(g_2 \square H) = g_1 \square g_2 \square H$ for any $g_1, g_2 \in G$. Thus

$$\begin{aligned}\tilde{T}((g_1 \square H)\square^*(g_2 \square H)) &= \tilde{T}(g_1 \square g_2 \square H)\\ &= T(g_1 \square g_2) = T(g_1)\square' T(g_2)\\ &= \tilde{T}(g_1 \square H)\square' \tilde{T}(g_2 \square H).\end{aligned}$$

So $\tilde{T}$ is a homomorphism.

3. We now explore the structure of $ker(\tilde{T})$. Given $a \in G$, then

$$\begin{aligned}a \square H \in ker(\tilde{T}) &\Leftrightarrow \tilde{T}(a \square H) = T(a) = e'\\ &\Leftrightarrow a \in ker(T)\\ &\Rightarrow a \square H \in ker(T)/H\end{aligned}$$

Note 6. Easy to check: $H \leq G, ker(T) \leq G, H \subseteq ker(T) \Rightarrow H \leq ker(T)$.
If $H \leq ker(T)$, then $ker(T)/H := \{k \square H | k \in ker(T)\}$.

If $a \square H \in ker(T)/H$, then $\exists k \in ker(T)$, s.t. $a \square H = k \square H$, then $\exists h \in H \subseteq ker(T)$, s.t. $a = k \square h \in ker(T)$ (for $k, h \in ker(T)$, $ker(T) \leq G$ and enclosed with $\square$) Thus $a \square H \in ker(\tilde{T}) \Leftrightarrow a \square H \in ker(T)/H$, thus $ker(\tilde{T}) = ker(T)/H$.

Thus $\tilde{T}$ is injection $\Leftrightarrow$ $ker(\tilde{T}) = \{H\}$ (for H is unit element of G/H) $\Leftrightarrow ker(T) = H$.

4.$\Rightarrow$: $\tilde{T} \circ \pi$ is surj. $\Rightarrow$ $\tilde{T}$ is surj. $\Leftarrow$: Composite of surj. is surj. $\square$

Collectively, $\tilde{T}$ is inj. $\Leftrightarrow$ $H = ker(T)$; $\tilde{T}$ is surj. $\Leftrightarrow$ T is surj. Thus $\tilde{T}$ is isomorphism (bij. + homomorphism) $\Leftrightarrow$ T is surj and $H = ker(T)$.

So $G \xrightarrow{T} G'$ is a homomorphism then exists an isomorphism $G/ker(T) \xrightarrow{\tilde{T}} im(T)$, denote by $G/ker(T) \simeq im(T)$. This conclusion is called **1st theorem of isomorphism**.

Example 3. Define $S_3 := \{\{1,2,3\} \xrightarrow{\sigma} \{1,2,3\} | \sigma \text{ is bij.}\}$, then $(S_3, \circ)$ is a group. And the element of $(S_3, \circ)$ is $e' = (1)(2)(3)$.

Given a group $(\mathbb{Z}, +)$, define a homomorphism $\mathbb{Z} \xrightarrow{T} S_3$. So if $1 \mapsto (12)$, then $T(2) = T(1+1) = T(1) \circ T(1) = e'$, $T(-1) = T(1)^{-1} = T(1) = (12)$. Furthermore $T(2\mathbb{Z}) = e'$, $T(2\mathbb{Z}+1) = (12)$. And $ker(T) = 2\mathbb{Z}, im(T) = \{(12), e'\}$. So $\mathbb{Z}/2\mathbb{Z} \simeq \{(12), e'\}$. Similarly, $\mathbb{Z}/3\mathbb{Z} \simeq \{e', (123), (132)\}$ (Define $T(1) = (123)$).

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, "T"] \arrow[dr, "\pi"'] & & S_3 \\ & \mathbb{Z}/2\mathbb{Z} \arrow[ur, "\tilde{T}"'] & \end{tikzcd}$$