Introduction to Topology

Group Theory, Lecture 4

Haoming Wang

23 July 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:

Binary operation

Definition 1 (Binary operation)**.** Given a set S, a map $S \times S \xrightarrow{\square} S$ is called a binary operation on S, denote as $(S, \square)$, and for $s_1, s_2 \in S$, denote $\square(s1, s2)$ as $s_1 \square s_2$.

Example 1. $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathcal{P}(X), \backslash), (\mathcal{P}(X), \cup), (\mathcal{P}(X), \cap)$ are all binary operations.

Definition 2 (Associative)**.** Given a binary operation $(S, \square)$, we say it is associative if $\forall a, b, c \in S,$ s.t. $(a \square b) \square c = a \square (b \square c)$.

Example 2. Given a set X, $(\mathcal{P}(X), \backslash)$ is not associative. For example, let $A = \mathbb{Z}, B = C = \mathbb{N}$, then $(A \backslash B) \backslash C = -\mathbb{N}_0$, while $A \backslash (B \backslash C) = \mathbb{Z}$.

Definition 3 (Unit element)**.** Given a binary operation $(S, \square)$, we say $e \in S$ is the unit element of $(S, \square)$ if $\forall s \in S$ have $e \square s = s = s \square e$.

Example 3. $(\mathbb{N}_0, +)$ has unit element 0; $(\mathbb{N}, \cdot)$ has unit element 1; $(\mathbb{N}, +)$ has no unit element; $(\mathcal{P}(X), \cup)$ has unit element $\emptyset$; $(\mathcal{P}(X), \cap)$ has unit element X; $(\mathcal{P}(\emptyset), \backslash)$ has unit element $\emptyset$;

If unit element exists, then there would be only one, suppose e, e' are unit element of $(S, \square)$, then $e = e \square e' = e'$.

Definition 4 (Invertable)**.** Given a binary operation $(S, \square)$ that has unit element e, we say an element $s \in S$ is invertable for $\square$ if $\exists s' \in S,$ s.t. $s \square s' = e = s' \square s$, and s' is the inverse of s.

Example 4. $(\mathbb{C}, \cdot)$ has unit element $1 + 0i$, for any element $c = a + bi$ and $c \neq 0$, it has the inverse $\frac{a - bi}{a^2 + b^2}$.

Example 5. We denote the set of all maps from X to X as X^X. For example, if there are two elements in X, then there are four elements (maps) in X^X.

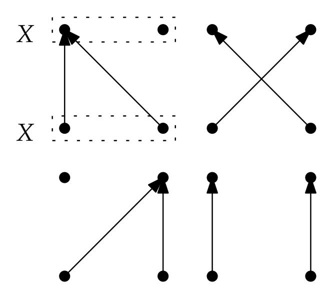


Figure 1: Four maps in X^X

So the binary operation $(X^X, \circ)$ has unit element $1_X(x) = x$ for any $x \in X$. Thus for any $x \in X, f \in X^X$, we have

$$f(1_X(x)) = f(x) = 1_X(f(x)).$$

And any map $f \in X^X$ is invertable $\Leftrightarrow$ f is bijection. $\Rightarrow$: assume g is the inverse of f, then

$$g \circ f = 1_X = f \circ g,$$

since 1_X is bijection, thus the inner map of $g \circ f$ is injection and the outer map of $f \circ g$ is surjection, thus f is bijection. $\Leftarrow$: if f is bijection, then $f^{-1}\exists$, and f^{-1} is bijection, thus $f \circ f^{-1} = 1_X = f^{-1} \circ f$.

Exercise 1. Suppose $(S, \Box)$ has unit element e and be associative, show that the invertable element s has only on inverse s'.

Proof. Suppose s', s'' are inverses of s, then

$$s'' = (s' \Box s) \Box s'' = s' \Box (s \Box s'') = s'$$

$\Box$

Note 1. Since the inverse of the element s is uniqueness, we could denote it as s^{-1}.

Exercise 2. Given an associative binary operation $(S, \Box)$ with a unit element e, show that s_1, s_2 are invertible w.r.t. $\Box$ $\Leftrightarrow$ $s_1 \Box s_2$ and $s_2 \Box s_1$ are invertible.

Proof. $\Rightarrow$: since s_1, s_2 are invertible, thus $s_1^{-1}, s_2^{-1}\exists$:

$$\begin{aligned}(s_1 \Box s_2) \Box (s_2^{-1} \Box s_1^{-1}) &= s_1 \Box (s_2 \Box (s_2^{-1} \Box s_1^{-1})) \\ &= s_1 \Box ((s_2 \Box s_2^{-1}) \Box s_1^{-1}) \\ &= s_1 \Box (e \Box s_1^{-1}) = e.\end{aligned}$$

Similarly, $(s_2^{-1} \Box s_1^{-1}) \Box (s_1 \Box s_2) = e$.

$\Leftarrow$: Since $s_1 \Box s_2$ is invertible, then $\exists \alpha \in S,$ s.t. $s_1 \Box s_2 \Box \alpha = \alpha \Box s_1 \Box s_2 = e$. Thus operate s_2 on the left:

$$s_2 \Box \alpha \Box s_1 \Box s_2 = s_2 \Box e = s_2$$

and then operate s_1 on the right:

$$s_2 \Box \alpha \Box s_1 \Box s_2 \Box s_1 = s_2 \Box s_1$$

since $s_2 \Box s_1$ is invertible, thus

$$s_2 \Box \alpha \Box s_1 = e$$

thus $s_2 \Box \alpha = s_1^{-1}$. $\Box$

Group

Definition 5 (Group)**.** We say a binary operation $(G, \Box)$ is a group, if

1. $(G, \Box)$ is associative: $\forall a, b, c \in G, (a \Box b) \Box c = a \Box (b \Box c)$;
2. $(G, \Box)$ has unit element: $\exists e \in G, \forall g \in G, e \Box g = g \Box e = g$;
3. any element in G is invertible: $\forall g \in G, \exists g' \in G, g \Box g' = g' \Box g = e$.

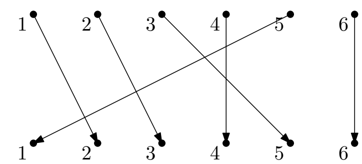
Example 6. There binary operations are groups: $(\mathbb{Z},+)$, $(\mathbb{C}^\times,\cdot)$ $(\mathbb{C}^\times = \{c \in \mathbb{C} | c \neq 0\})$.

These are not: $(\mathbb{N},+)$ (no unit element); $(\mathbb{Z},\cdot)$ (some element has no inverse); $(X^X,\circ)$ (only bijection has inverse)

For a binary operation $(X,\Box)$ that is associative and has unit element, We can select all its invertible elements and form a new binary operation $(X',\Box)$, then it is a group. For example $(X^X,\circ)$ is not a group, but $(Perm(X),\circ)$ is a group.

Note 2. If $x_1, x_2 \in X'$, thus x_1, x_2 is invertible w.r.t. $\Box$, thus $x_1 \Box x_2$ is invertible w.r.t. $\Box$, thus $x_1 \Box x_2 \in X'$. Thus $(X',\Box)$ is a binary operation.

Given a set X, we say the **permutation** of X is the set of all bijections from the set X to itself, denote by $Perm(X)$. If X is finite, we often use **cycle expression** to represent the element of $Perm(X)$. For example, if $X = \{1,2,3,4,5,6\}$, we would denote the bijection in the margin as $(1,2,3,5)(4)(6)$ or $(1,2,3,5)$, and it is an element of $Perm(X)$.



Definition 6 (subgroup)**.** Given a group $(G,\Box)$, we say a subset $H \subseteq G$ constructs a subgroup of $(G,\Box)$ is

1. for $\forall h, h' \in H, h \Box h' \in H$;
2. $(H,\Box)$ is a group.

Example 7. $C = \{e,(12)(34),(13)(24),(14)(23)\}$ constructs a subgroup of $(Perm(\{1,2,3,4\}),\circ)$. For example $(12)(34) \circ (12)(34) = e \in C$ (which implies the inverse of $c \in C$ is c); $(12)(34) \circ (13)(24) = (14)(23) \in C$.

Exercise 3. Given a group $(G,\Box)$ with the unit element e, $(H,\Box)$ is the subgroup of $(G,\Box)$ with the unit element e_H, show that $e = e_H$.

Proof. For e_H is the unit element of $(H,\Box)$, $e_H \Box e_H = e_H$; For e is the unit element of $(G,\Box)$, $e_H \Box e = e_H$, thus

$$e_H \Box e_H = e_H = e_H \Box e,$$

and $\exists e_H^{-1} \in G$ such that $e_H^{-1} \Box e_H = e$:

$$\begin{aligned} & e_H^{-1} \Box (e_H \Box e_H) = e_H^{-1} \Box (e_H \Box e) \\ & \Rightarrow (e_H^{-1} \Box e_H) \Box e_H = (e_H^{-1} \Box e_H) \Box e \\ & \Rightarrow e \Box e_H = e \Box e \\ & \Rightarrow e_H = e. \end{aligned}$$

$\Box$

Note 3. It is easy to check that the inverse of $h \in H$ in G is contained by H.

Exercise 4. Given a group $(\mathbb{Z},+)$, $H \subseteq \mathbb{Z}$, let $m = \min\{h | h \in H, h > 0\}$, show that $H = m\mathbb{Z} =: \{mz | z \in \mathbb{Z}\}$.

Proof. $\supseteq$: Since $m \in H$, thus $m + m = 2m \in H, \cdots, zm \in H$ for any $z \in \mathbb{Z}$, thus $H \supseteq m\mathbb{Z}$. $\subseteq$: Suppose $x \in H$, thus $x \in \mathbb{Z}, m \in \mathbb{N}$,

$\exists q \in Z, r \in \mathbb{N}_0, 0 \leq r \leq m$, s.t. $x = qm + r$. thus $x - m = (q-1)m + r \in H, \cdots, r \in H$. If $x \notin m\mathbb{Z}$, that means $0 < r < m$ which leads to a contradiction. Thus $H \subseteq m\mathbb{Z}$ and $H = m\mathbb{Z}$. $\square$

Exercise 5 (Left Translation)**.** Given a group $(G, \square)$, $g_0 \in G$, show that the map $G \xrightarrow{l_{g_0}} G$ where $g \xrightarrow{l_{g_0}} g_0 \square g$ is a bijection. (l means *left*)

Proof. Injection: for $g_1, g_2 \in G$ if $l_{g_0}(g_1) = l_{g_0}(g_2)$, that is

$$\begin{aligned}
&g_0 \square g_1 = g_0 \square g_2 \\
&\Rightarrow g_0^{-1} \square (g_0 \square g_1) = g_0^{-1} \square (g_0 \square g_2) \\
&\Rightarrow (g_0^{-1} \square g_0) \square g_1 = (g_0^{-1} \square g_0) \square g_2 \\
&\Rightarrow e \square g_1 = e \square g_2 \\
&\Rightarrow g_1 = g_2.
\end{aligned}$$

Surjection: for $\forall g \in G, \exists g' \in G, g_0 \square g = g'$, thus

$$\begin{aligned}
&g_0^{-1} \square g_0 \square g = g_0^{-1} \square g' \\
&\Rightarrow g = g_0^{-1} \square g' \\
&\Rightarrow g = g_0 \square g_0^{-1} \square g_0^{-1} \square g' \\
&\Rightarrow g = g_0 \square g_0^{-1} \square g_0^{-1} \square g_0 \square g \\
&\Rightarrow g = g_0 \square (g_0^{-1} \square g),
\end{aligned}$$

Thus for $\forall g \in G, \exists g_0^{-1} \square g \in G$ such that $g_0 \square (g_0^{-1} \square g) = g$. $\square$

Note 4. Correspondingly, there exists a concept: *right translation*.

Definition 7 (Left Coset)**.** Given a group $(G, \square)$, $a \in G$, $(H, \square)$ is a subgroup of $(G, \square)$. way say $a \square H := \{a \square h | h \in H\}$ is the left coset of H associated to a.

Exercise 6. Suppose $(H, \square)$ is a subgroup of $(G, \square)$, $\forall a, b \in G$, show that either $a \square H = b \square H$ or $a \square H \cap b \square H = \emptyset$.

Proof. Suppose that $a \square H \cap b \square H \neq \emptyset$, thus $\exists x \in G, h_1, h_2 \in H$ such that $a \square h_1 = x = b \square h_2$. Then for any $h \in H$, we have

$$\begin{aligned}
&a \square h_1 = b \square h_2 \\
&\Rightarrow a \square h_1 \square h_1^{-1} = b \square h_2 \square h_1^{-1} \\
&\Rightarrow a \square h = b \square h_2 \square h_1^{-1} \square h,
\end{aligned}$$

where $h' := h_2 \square h_1^{-1} \square h \in H$. So for $\forall h \in H, \exists h' \in H$, s.t. $a \square h = b \square h' \in b \square H$, that is for any element $a \square h \in a \square H$, it is contained by $b \square H$, thus $a \square H \subseteq b \square H$. Similarly we can prove $b \square H \subseteq a \square H$. Thus if $a \square H \cap b \square H \neq \emptyset$ then $a \square H = b \square H$. $\square$

Specially, since $\forall h \in H, e \square h = h$, we have $H = e \square H$. And then for $\forall h \in H$:

$$H = e \square H = h \square H$$

because $e\Box H$ and $h\Box H$ has common element h ($e \in H$ implies $h \in h\Box H$). Furthermore, for $\forall g \in G, g = g\Box e$, thus $g \in g\Box H$. This means that any element $g \in G$ is covered by some coset of H, and any two cosets of H are either equal or disjoin. Thus G is the disjoin union of the left cosets of H.

Note 5. Given a subgroup $(H, \Box)$ of $(G, \Box)$, the cosets of H divide G into disjoin blocks. But note that only H (or $h\Box H (h \in H)$) construct the subgroup of $(G, \Box)$. The others cosets **does not**, because they are disjoin with $h\Box H$, thus the unit element e is not covered by them.

Exercise 7. Suppose $(H, \Box)$ is a subgroup of $(G, \Box)$, $\forall a, b \in G$, show that $a\Box H = b\Box H \Leftrightarrow a^{-1}\Box b \in H$.

Proof. $\Rightarrow$: Since the unit element $e \in H$, thus $b \in b\Box H = a\Box H$. Thus $\exists h \in H$, such that $a\Box h = b \Rightarrow h = e\Box h = a^{-1}\Box b \in H$.

$\Leftarrow$: if $a^{-1}\Box b \in H$, $\exists h \in H$, s.t. $a^{-1}\Box b = h \Rightarrow b = a\Box h \in a\Box H$. While $b \in b\Box H$, thus $b \in a\Box H \cap b\Box H$, thus $a\Box H = b\Box H$. $\Box$

Note 6. Since $\forall h_1, h_2 \in H$, have $h_1^{-1}, h_2^{-1} \in H$ and $h_1^{-1}\Box h_2 \in H$. So $h_1\Box H = h_2\Box H = H$.

Since left translation $H \xrightarrow{l_a} a\Box H (a \in G)$ is a bijection, thus H has the same cardinality as $a\Box H$, that is $|H| = |a\Box H|$. Furthermore, any two cosets of H have the same cardinality.

Since G is the disjoin union of the cosets of H, and any cosets of H have the same cardinality, if $(G, \Box)$ is a finite group, then $|H| \,|\, |G|$. (that is $\exists q \in \mathbb{Z}$, s.t. $q|H| = |G|$, i.e. $|H|$ must be a factor of $|G|$). For example if G has 24 elements, then the subset that has such as 5,7,9,10,11,13,... elements could never construct the subgroup of $(G, \Box)$.

Definition 8 (Quotient set)**.** Given a group $(G, \Box)$ with a subgroup $(H, \Box)$, we call $G/H := \{g\Box H | g \in G\}$ the quotient set of G associated to H.

Note 7. Thus G/H is the set of all cosets of H, and $G/H \subseteq \mathcal{P}(G)$.