Introduction to Topology

Collection

Haoming Wang

22 June 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.

Lecture 1. Set and Map

Content:

Proposition

If p, q are statements, We denote "if p then a" as $p \Rightarrow q$. The only case where this proposition is false is p is true while q is false, thus $p \Rightarrow q \Leftrightarrow (\neg p) \vee q$. When we use proof by contradiction to prove a proposition like $p \Rightarrow q$, what we do is that $\neg(p \Rightarrow q)$ leads to a contradiction, that is $p \wedge \neg q$ leads to a contradiction.

Quantifier

There are two quantifiers : "for all" $\forall$ and "exists" $\exists$. There are two commonly-used Propositions:

1 $\exists x, \forall y,$ s.t. proposition $P(x,y)$ holds;

2 $\forall y, \exists x,$ s.t. proposition $P(x,y)$ holds;

The difference between these proposition is former x in $P(x,y)$ could be constant, but the latter would be not.

Note 1. It is easy to check that the former is the sufficient condition of the latter. For example, suppose $P(x,y) = [\![x < y]\!]$, then the latter holds but the former does not.

Set

Inclusion

Suppose A and B are sets, we say $A \subseteq B$ if $\forall x,$ s.t. $x \in A \Rightarrow x \in B$; and $B \subseteq A$ if $\forall x,$ s.t. $x \in B \Rightarrow x \in A$. Correspondingly, $A = B$ if $\forall x,$ s.t. $x \in A \Leftrightarrow x \in B$.

Note 2. Suppose $\emptyset \nsubseteq A$, which means $\exists x \in \emptyset,$ s.t. $x \notin A$. But there is no element in $\emptyset$, thus $\emptyset \subseteq A$ logically.

Example 1. Suppose $A = \{x \in \mathbb{R} | x = x + 1\}, B = \{x \in \mathbb{Q} | x^2 = 2\}$. There's no element in either A or B, although it is a little wilder, but still fits our definition above, thus $A = B$.

Operations on set

Definition 1 (Difference)**.** Given sets A, B, the difference of sets is $A \backslash B \coloneqq \{x \in A | x \notin B\}$.

Definition 2 (Union and Intersection)**.** Given $S_j (j \in J)$, a family of sets indexed by a set J. Then, the union of sets is

$$\cup_{j \in J} S_j \coloneqq \{x | \exists j \in J, x \in S_j\};$$

the intersection of sets is

$$\cap_{j \in J} S_j \coloneqq \{x | \forall j \in J, x \in S_j\}.$$

Definition 3 (Power set)**.** Given a set S, the power set of S is $\mathcal{P}(S) \coloneqq \{A | A \subseteq S\}$, that is $\forall A, A \in \mathcal{P}(S) \Leftrightarrow A \subseteq S$.

Example 2. Suppose $S = \{0, 1\}$, then $\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. If there are n elements in a finite set S, then there are 2^n elements in its power set $\mathcal{P}(S)$. Thus sometimes we also denote the power set of S by 2^S.

Definition 4 (Cartesian porduct)**.** Given sets X and Y, then the cartesian product of them is $X \times Y \coloneqq \{(x, y) | x \in X \wedge y \in Y\}$.

Note 3. The pair (x, y) is defined as a set $\{\{x\}, \{x, y\}\}$ which indicates a truth: if $x, x' \in X, y, y' \in Y$, then $(x, y) = (x', y') \Leftrightarrow x = x' \wedge y = y'$.
The reason why we define the pair (x, y) as such form is that there is no order in set, that is $\{\{x\}, \{y\}\} = \{\{y\}, \{x\}\}$.

Relation

Definition 5 (Relation)**.** Given sets X, Y, we say a subset R of $X \times Y$ induces a binary relation among elements of X and Y.

If $x \in X, y \in Y$ fit $(x, y) \in R \subset X \times Y$, we say x, y has relation R, denote as xRy. Different subsets of $X \times Y$ induce different relation, the $\emptyset$, also a subset of $X \times Y$, means elements in X have no relationship with elements in Y.

Definition 6 (Equivalence relation)**.** $R \in X \times X$ is an equivalence relation on X if:
1. $\forall x \in X, (x, x) \in R$;
2. $\forall x, x' \in X, (x, x') \in R \Rightarrow (x', x) \in R$;
3. $\forall x, x', x'' \in X, (x, x') \in R \wedge (x', x'') \in R \Rightarrow (x, x'') \in R$.

Example 3. 1. If $R = \{(x, x) | x \in X\}$, that is R is the diagonal of $X \times X$, then R induces Equal relation.
2. If $X = \mathbb{Z}$, $R = \{(x, x') | x \equiv x' (\text{mod} 3)\}$, then R is an equivalence relation.

Definition 7 (Partial order)**.** $R \subseteq X \times X$ is a partial order on X if:
1. $\forall x \in X, (x, x) \in R$;
2. $\forall x, x' \in X, (x, x') \in R \wedge (x', x) \in R \Rightarrow x = x'$;
3. $\forall x, x', x'' \in X, (x, x') \in R \wedge (x', x'') \in R \Rightarrow (x, x'') \in R$.

Note 4. If we eliminate the second condition, then R is a Pre-order.

Example 4. Less than or equal ($\leq$), as well as greater than or equal ($\geq$), are partial order on $\mathbb{Z}$. Given a set S, inclusion ($\subseteq$) is a partial order on $\mathcal{P}(S)$.

Definition 8 (Total order)**.** A total order on X is a partial order R on X such that $\forall x, x', (x, x') \in R \vee (x', x) \in R$.

Example 5. Given a set S, inclusion ($\subseteq$) is not a total order on $\mathcal{P}(S)$, e.g. neither $(\{0\}, \{1\})$ nor $(\{0\}, \{1\})$ in relation $\subseteq$ on $\mathcal{P}(\{0, 1\})$.

Definition 9 (Well order)**.** A well order on X is a total order R on X such that: $\forall S, S \subseteq X \wedge S \neq \emptyset \Rightarrow \exists s := \min_R S \in S, \forall s' \in S,$ s.t. $(s, s') \in R$.

Example 6. $\leq$ is a well order on $\mathbb{N}_0$, but not on $\mathbb{Z}$. But we can define a new relation R, such that R is a well order on $\mathbb{Z}$. For example, define

$$n(p) = \begin{cases} 2p - 1 & p > 0, \\ -2p & p < 0, \\ 0 & p = 0 \end{cases}$$

where $p \in \mathbb{Z}$, thus $n(p) \in \mathbb{N}$, define

$$R = \{(x, x') \in X \times X | n(x) \leq n(x')\},$$

then R is a well order on $\mathbb{Z}$. For example $(3, -10) \in R$, since $n(3) = 5$ and $n(-10) = 20$. And $\min_R\{x \in \mathbb{Z} | x \leq 4\} = 0$.

Note 5. Actually, For any non-empty set, there exists a well order on it by *Axiom of Choice*.

Maps

Definition 10 (Map). Given sets X, Y, A relation $f \subseteq X \times Y$ is called a map from X to Y, if $\forall x \in X, \exists! y \in Y, (x, y) \in f$.

Note 6. $\exists! y \in Y$ represents there is one and only one $y \in Y$.

Definition 11. Given a map: $X \xrightarrow{f} Y$, for $A \subseteq X$, $B \subseteq Y$, we say:

1. The domain of f, $D_f := X$;
2. The codomain of f, $C_f := Y$;
3. The image of A under f, $f(A) := \{f(a) | a \in A\}$;
4. The pre-image of B under f, $f^{-1}(B) := \{x \in X | f(x) \in B\}$;
5. The range of f, $R_f := f(X)$.

Note 7. Notice that f^{-1} is not a map. $f^{-1}(Y) = X$.

Exercise 1. Given maps $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} Z$. Show that for $A \subseteq X$, $(g \circ f)(A) = g(f(A))$; for $C \subseteq Z$, $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$.

Proof. 1. Trivial; 2. By definition, we have $(g \circ f)^{-1}(C) = \{x \in X | g(f(x)) \in C\} =: U$, $f^{-1}(g^{-1}(C)) = \{x \in X | f(x) \in \{y \in Y | g(y) \in C\}\} =: K$. if $x \in U, x \notin K$, then $f(x) \notin \{y \in Y | g(y) \in C\}$ and $g(f(x)) \notin C$, which leads to a contradiction, thus $U \subseteq K$. Correspondingly, we can prove $K \subseteq U$ by contradiction, thus $U = K$. $\square$

Exercise 2. Given a map $X \xrightarrow{f} Y$, show that:

1. For a family of subset $T_j \subseteq Y (j \in J)$, have
$$f^{-1}(\cup_{j \in J} T_j) = \cup_{j \in J} f^{-1}(T_j) \text{ and } f^{-1}(\cap_{j \in J} T_j) = \cap_{j \in J} f^{-1}(T_j);$$
2. For $B, B' \in Y$, $f^{-1}(B \backslash B') = f^{-1}(B) \backslash f^{-1}(B')$;
3. For a family of subset $S_j \subseteq X (j \in J)$, have
$$f(\cup_{j \in J} S_j) = \cup_{j \in J} f(S_j) \text{ and } f(\cap_{j \in J} S_j) \subseteq \cap_{j \in J} f(S_j);$$
4. For $A, A' \in X$, $f(A) \backslash f(A') \subseteq f(A \backslash A')$.

Proof. 1. $\cup$: If
$$\begin{aligned} x \in f^{-1}(\cup_{j \in J} T_j) &\Rightarrow f(x) \in \cup_{j \in J} T_j \\ &\Rightarrow f(x) \in T_j (\exists j \in J) \\ &\Rightarrow x \in f^{-1}(T_j) \subseteq \cup_{j \in J} f^{-1}(T_j) \end{aligned}$$
thus $f^{-1}(\cup_{j \in J} T_j) \subseteq \cup_{j \in J} f^{-1}(T_j)$. If
$$\begin{aligned} x \in \cup_{j \in J} f^{-1}(T_j) &\Rightarrow x \in f^{-1}(T_j)(\exists j \in J) \\ &\Rightarrow f(x) \in T_j \subseteq \cup_{j \in J} T_j \\ &\Rightarrow x \in f^{-1}(\cup_{j \in J} T_j) \end{aligned}$$

thus $\cup_{j\in J} f^{-1}(T_j) \subseteq f^{-1}(\cup_{j\in J} T_j)$. Thus $f^{-1}(\cup_{j\in J} T_j) = \cup_{j\in J} f^{-1}(T_j)$.
$\cap$: If

$$\begin{aligned} x \in f^{-1}(\cap_{j\in J} T_j) &\Rightarrow f(x) \in \cap_{j\in J} T_j \\ &\Rightarrow f(x) \in T_j (\forall j \in J) \\ &\Rightarrow x \in f^{-1}(T_j)(\forall j \in J) \\ &\Rightarrow x \in \cap_{j\in J} f^{-1}(T_j), \end{aligned}$$

thus $f^{-1}(\cap_{j\in J} T_j) \subseteq \cap_{j\in J} f^{-1}(T_j)$; If

$$\begin{aligned} x \in \cap_{j\in J} f^{-1}(T_j) &\Rightarrow x \in f^{-1}(T_j)(\forall j \in J) \\ &\Rightarrow f(x) \in T_j (\forall j \in J) \\ &\Rightarrow f(x) \in \cap_{j\in J} T_j \\ &\Rightarrow x \in f^{-1}(\cap_{j\in J} T_j), \end{aligned}$$

thus $\cap_{j\in J} f^{-1}(T_j) \subseteq f^{-1}(\cap_{j\in J} T_j)$, and $f^{-1}(\cap_{j\in J} T_j) = \cap_{j\in J} f^{-1}(T_j)$.

2. If

$$\begin{aligned} f^{-1}(B\backslash B') &\Rightarrow f(x) \in B\backslash B' \\ &\Rightarrow f(x) \in B \wedge f(x) \notin B' \\ &\Rightarrow x \in f^{-1}(B) \wedge x \notin f^{-1}(B') \\ &\Rightarrow x \in f^{-1}(B)\backslash f^{-1}(B'). \end{aligned}$$

If

$$\begin{aligned} x \in f^{-1}(B)\backslash f^{-1}(B') &\Rightarrow f \in f^{-1}(B) \wedge x \notin f^{-1}(B') \\ &\Rightarrow f(x) \in B \wedge f(x) \notin B' \\ &\Rightarrow f(x) \in B\backslash B' \\ &\Rightarrow x \in f^{-1}(B\backslash B'); \end{aligned}$$

Thus $f^{-1}(B\backslash B') = f^{-1}(B)\backslash f^{-1}(B')$.

3. $\cup$: If

$$\begin{aligned} y \in f(\cup_{j\in J} S_j) &\Rightarrow y \in f(S_j)(\exists j \in J) \\ &\Rightarrow y \in \cup_{j\in J} f(S_j) \end{aligned}$$

and if

$$\begin{aligned} y \in \cup_{j\in J} f(S_j) &\Rightarrow y \in f(S_j)(\exists j \in J) \\ &\Rightarrow y \in f(\cup_{j\in J} S_j). \end{aligned}$$

Thus $f(\cup_{j\in J} S_j) = \cup_{j\in J} f(S_j)$.
$\cap$: for $\forall j \in J$, we have $f(\cap_{j\in J} S_j) \subseteq f(S_j)$, thus $f(\cap_{j\in J} S_j) \subseteq \cap_{j\in J} f(S_j)$. If $y \in \cap_{j\in J} f(S_j)$ then for $\forall j \in J$, there exists $s_j \in S_j$ such that $s_j \in f^{-1}(y)$. BUT, we can not confirm that s_j are the same number in different S_j, thus $\cap_{j\in J} S_j$ could be $\emptyset$. For example, assume that $f(x) = |x|$ with domain $X = [-2, 2]$. Set $S_1 = (-2, 0), S_2 = (0, 2), y = 1$, then $y \in f(S_1) \cap f(S_2) = (0, 2)$ but $f(S_1 \cap S_2) = f(\emptyset) = \emptyset \subseteq f(S_1) \cap f(S_2) = (0, 2)$.

Note 8. It is easy to prove that if $S_1 \subseteq S_2$ then $f(S_1) \subseteq f(S_2)$ and $f^{-1}(S_1) \subseteq f^{-1}(S_2)$.

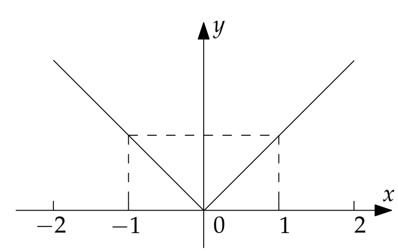


Figure 1: $f(x) = |x|$

4. If $y \in f(A)\backslash f(A')$ then $y \in f(A) \wedge y \notin f(A')$. Thus $\exists a \in A$, s.t. $a \in f^{-1}(y)$ and $\forall a' \in A'$, s.t. $a' \notin f^{-1}(y)$, which means $a \notin A'$, and $a \in A\backslash A'$, thus $y \in f(A\backslash A')$. Thus $f(A)\backslash f(A') \subseteq f(A\backslash A')$.
   Set $A = (-2,0), A' = (1,2)$, then $f(A\backslash A') = f(A) = (0,2)$. But $f(A)\backslash f(A') = (0,2)\backslash(1,2) = (0,1] \subseteq f(A\backslash A')$.

□

Note 9. Overview of basic results about images and preimages

Lecture 2. Cardinality

CONTENT:

Maps

Definition 12 (injection, surjection and bijection)**.** We say a map $X \xrightarrow{f} Y$ is an injection (1-1) if for $\forall x, x' \in X, f(x) = f(x')$ then $x = x'$; a surjection (onto) if $\forall y \in Y, \exists x \in X$, s.t. $f(x) = y$; a bijection (1-1 correspondence) if it is an injection and also a surjection.

If $X \xrightarrow{f} Y$ is a bijection, it has an inverse map $X \xleftarrow{f^{-1}} Y$. Notice that the inverse map f^{-1} is not the same as the pre-image f^{-1}.

Note 10. When we say a map $X \xrightarrow{f} Y$, we want say $\forall x \in X, \exists! y \in Y$, s.t. $y = f(x)$. When we try to think the occasion that from Y to X, the conception of *injection* preserve the "$\exists!$" of a map, and the *surjection* guarantees the "$\forall$" of a map.

For a bijection, the relationship between these is: for $y \in Y$ then

$$\{f^{-1}(y)\} = f^{-1}(\{y\}).$$

For the others cases, there does not exist an inverse map.

Exercise 3. Given maps $X \xrightarrow{f} Y, Y \xrightarrow{g} Z$, show that:
1. $g \circ f$ is an injective $\Rightarrow$ f is an injective;
2. $g \circ f$ is a surjective $\Rightarrow$ g is a surjective.

Proof. 1. Since $g \circ f$ is injection, thus for any different $x_1, x_2 \in X$, we have $g(f(x_1)) \neq g(f(x_2))$, thus $f(x_1) \neq f(x_2)$, and f is injection.
2. Since $g \circ f$ is surjection, thus for any $z \in Z$ there exists $x \in X$, s.t. $g(f(x)) = z$, which means $\exists y = f(x)$, s.t. $z = g(y)$, thus g is surjection.

□

Exercise 4. Given maps $X \xrightarrow{f_1} Y, X \xrightarrow{f_2} Y, Y \xrightarrow{g} Z$, if g is an injection, and $g \circ f_1 = g \circ f_2$ show that $f_1 = f_2$. Correspondingly, Given maps $X \xrightarrow{f} Y, Y \xrightarrow{g_1} Z, Y \xrightarrow{g_2} Z$, if f is a surjection, and $g_1 \circ f = g_2 \circ f$ show that $g_1 = g_2$.

Proof. 1. For $\forall x \in X$, we have $g(f_1(x)) = g(f_2(x))$, since g is injection, thus $f_1(x) = f_2(x)$, and $f_1 = f_2$;

2. Since f is surjection, thus $f(X) = Y$, and $g_1(f(x)) = g_2(f(x))$ for any $x \in X$, thus $g_1(y) = g_2(y)$ for any $y \in Y$, and $g_1 = g_2$.

□

Cardinality

Def.

Definition 13. Two sets X, Y have the same cardinality, if $\exists$ bijection $X \xrightarrow{f} Y$, denote as $|X| = |Y|$.

Definition 14. A set X has its cardinality smaller or equal to that of a set Y if $\exists$ an injection $X \xrightarrow{f} Y$, denote as $|X| \leq |Y|$.

Note 11. The subset of a set could have the same cardinality with it. For example, just as mentioned last lecture, $|\mathbb{N}| = |\mathbb{Z}|$.

$\mathbb{N}$ *and* $\mathbb{Q}$

We will show that the natural number set $\mathbb{N}$ could 1-1 correspond to rational number set $\mathbb{Q}$. List the rational number as a matrix, we can encode them from southwest to northeast line by line, and skip the rational number that has been encoded. We can see that specify any natural number n, there is a definite law to query the corresponding rational number in $\mathbb{Q}$ or vice versa. Thus $|\mathbb{N}| = |\mathbb{Q}|$.

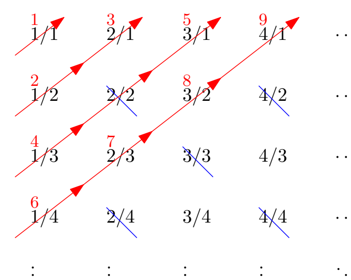


Figure 2: $\mathbb{Q} \leftrightarrow \mathbb{N}_0$

$\mathbb{N}$ *and* $\mathbb{R}$

Thus we can see that the natural number set $\mathbb{N}$ can correspond with rational number set $\mathbb{Q}$ 1 by 1, although it is density. But how about the real number set $\mathbb{R}$? Before we answer this question, we need to recall the definition of real number in Decimal notation.

Given a real number in decimal notation, like $r = 0.112123123412345\cdots$, what does it mean? Define a family of close intervals $I_{i,j}(i \in \mathbb{N}, j \in \{0, 1, \cdots, 9\})$, where $I_{0,0} = [0, 1]$ and $I_{i,j}$ is the $j+1$-th part of tenth division of $I_{i-1,*}$. For example, $I_{1,3}$ is the 4-th of ten division of $I_{0,0}$, thus $I_{1,3} = [0.3, 0.4]$. On this base, $I_{2,2} = [0.32, 0.33]$, and $I_{3,9} = [0.329, 0.330]$ and so on. Thus we have that

$$I_{0,0} \supseteq I_{1,*} \supseteq I_{2,*} \supseteq I_{3,*} \supseteq \cdots$$

Thus the definition of real number in decimal notation is the intersection of thus a family of interval, for example,

$$r = I_{0,0} \cap I_{1,1} \cap I_{2,1} \cap I_{3,2} \cap I_{4,1} \cap I_{5,2} \cap \cdots;$$

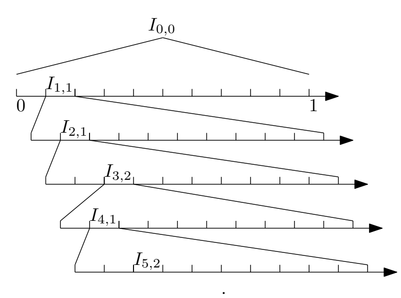


Figure 3: real number in decimal notation

Since the length of $I_{i,*}$ is the one tenth of the $I_{i-1,*}$, the length of interval will trend to 0 as i approaches to ∞. Thus any given decimal notation only represents one real number. If there is a decimal notation $\{I_{i,j}\}$ that denotes two different real number r, r', where $d(r, r') > 0$. then there exist N for any $i > N$, the length of $I_{i,*}$ is small than $d(r, r')$, thus $I_{i,*}$ can not cover r, r' at the same time, which leads to a contradiction.

But please note that, although a given decimal notation only represents one real number, some real number could be represented in two kind of decimal notations. This kind of real number is so called *finite decimal*, that is it locates on the bounds of some intervals. Like $r' = 0.113$ falls on the right boundary of $I_{3,2} = [0.112, 0.113]$ and the left boundary of $I_{3,3} = [0.113, 0.114]$, thus

$$r' = I_{0,0} \cap I_{1,1} \cap I_{2,1} \cap I_{3,3} \cap I_{4,0} \cap I_{5,0} \cdots$$

and could be written as $r' = 0.113000\cdots$; but as we said, r' can also be covered by another family of intervals:

$$r' = I_{0,0} \cap I_{1,1} \cap I_{2,1} \cap I_{3,2} \cap I_{4,9} \cap I_{5,9} \cdots$$

thus it could be also written as $r' = 0.112999\cdots$, and these two forms are equivalent. We call the latter form of expression as *infinite expression*.

Proposition 1 (Cantor). *$\nexists$ a surjection such that $\mathbb{N} \xrightarrow{f} \mathbb{R}$.*

Proof. Assume that f is a surjection from $\mathbb{N}$ to $\mathbb{R}$. Write down the maps relationship in infinite expression:

$$\begin{aligned}
f(1) &= a_1 + 0.a_{11}a_{12}a_{13}\cdots \\
f(2) &= a_2 + 0.a_{21}a_{22}a_{23}\cdots \\
f(3) &= a_3 + 0.a_{31}a_{32}a_{33}\cdots \\
f(4) &= a_4 + 0.a_{41}a_{42}a_{43}\cdots \\
&\vdots
\end{aligned}$$

Where $a_i \in \mathbb{Z}, a_{ij} \in \mathbb{N}(i, j \in \mathbb{N})$. Define a real number $r = b + 0.b_1b_2b_3\cdots$, such that $b \in \mathbb{Z}$ and b_i is the smallest number among $\{1, 2, \cdots, 9\}$ which is not a_{ii}. Thus r is not equal to any of the numbers on the right-hand side of the above equations, which represent $\mathbb{R}$ since f is surjection. Thus it leads to a contradiction. $\square$

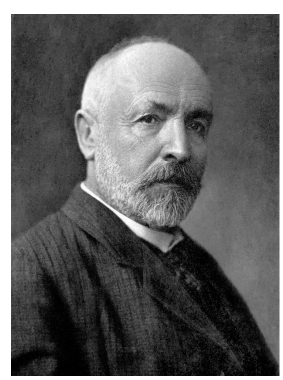


Figure 4: Georg Cantor (1845-1918)

This proof method is called *Cantor's diagonal argument*, it is a powerful weapon.

S and $\mathcal{P}(S)$

If S is a finite set, then the number of elements in S and $\mathcal{P}(S)$ are n and 2^n respectively. It is easy to check that there is no 1 to 1 correspondence between S and $\mathcal{P}(S)$ since $n < 2^n$ for any $n \in \mathbb{N}$. But what if S is infinite? We will elaborate it beginning with the case $S = \mathbb{N}$

Proposition 2. *$\nexists$ a surjection such that $\mathbb{N} \xrightarrow{f} \mathcal{P}(\mathbb{N})$.*

Proof. Suppose there exists a surjection such that $\mathbb{N} \xrightarrow{f} \mathcal{P}(\mathbb{N})$, then for any natural number n, $f(n) \subseteq \mathbb{N}$. Denote $f(n)$ as $a_{n1}a_{n2}a_{n3}\cdots$ where if $i \in f(n)$ then set $a_{ni} = 1$, otherwise set $a_{ni} = 0$. Thus we have:

$$
\begin{aligned}
f(1) &= a_{11}a_{12}a_{13}a_{14}\cdots \\
f(2) &= a_{21}a_{22}a_{23}a_{24}\cdots \\
f(3) &= a_{31}a_{32}a_{33}a_{34}\cdots \\
f(4) &= a_{41}a_{42}a_{43}a_{44}\cdots \\
&\vdots
\end{aligned}
$$

Define a series $b = b_1b_2b_3b_4\cdots$ where $b_i \in \{0,1\}$ and $b_i \neq a_{ii}$, thus the subset of $\mathbb{N}$, which is in $\mathcal{P}(N)$, represented by b is not in the $f(\mathbb{N})$, thus f is not a surjection. □

Note 12. That is, for example, if $6 \notin f(6)$ then select 6 in b otherwise the opposite. Clarify this will help to understand the proof in the general case.

Proposition 3. *$\nexists$ a surjection such that $S \xrightarrow{f} \mathcal{P}(S)$ for any set S.*

Proof. Suppose f is a surjection such that $S \xrightarrow{f} \mathcal{P}(S)$. Then for any $x \in S$, we have $f(x) \in \mathcal{P}(S)$ is a subset of S. Define a subset of S: $A := \{x \in S | x \notin f(x)\}$ (which is just the series $b_1b_2b_3b_4\cdots$ in the last case), we will show that $A \notin f(S)$.

If $A \in f(S)$, then $\exists s \in S$, such that $A = f(s)$. If $s \in A = f(s)$, then $s \notin A$; If $s \notin A = f(s)$ then $s \in A$, which all lead to contradiction, thus $A \notin f(S)$, and f is not a surjection. □

$\mathbb{R}$ and $\mathbb{C}$

Proposition 4. *Given sets S, T. If exist two injections f, g such that $S \xrightarrow{f} T$ and $T \xrightarrow{g} S$, then exist a bijection h such that $S \xrightarrow{h} T$. Briefly, $|S| \leq |T| \wedge |T| \leq |S| \Rightarrow |T| = |S|$.*

Proof. For any point $s \in S$, We do two operations: Inferring and tracing, that is what is the point $t \in T$ such that $t = f(s)$; and whether there exists a point $t' \in T$ such that $s = g(t')$. And repeat the operations above in S and T alternatively.

Since f, g are injection, thus we can always infer next step infinitely, that is for $\forall s \in S$, there exist a t such that $t = f(s)$, and then $\exists s',$ s.t. $s' = g(t)$, and then $\exists t',$ s.t. $t' = f(s')$, and so on.

But when tracing the point s (or t), there would be two occasions, (1) there is no t' (or s'), such that $t' = f(s)$ (or $s' = f(t)$). (2) There is one and only one to correspond. Thus when we infer and trace for all elements in S and T, there would be only 4 kinds of occasions:

1. Infer infinity and trace end at T:

$$T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} \cdots$$

2. Infer infinity and trace end at S:

$$S \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} \cdots$$

3. Infer and trace construct a loop:

$$\begin{tikzcd} S \arrow[r, "f"] & T \arrow[r, "g"] & S \arrow[r, "f"] & \cdots \arrow[r, "g"] & S \arrow[r, "f"] & T \arrow[lllll, bend left, "g"] \end{tikzcd}$$

4. Infer and trace infinity without repeat:

$$\cdots \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} S \xrightarrow{f} T \xrightarrow{g} \cdots$$

These 4 occasion consist of all element of S and T, and there is nothing in common between any two occasions. Thus we can define a bijection h from S to T: for any $s \in S$, if s belongs to the last 3 occasions, then $h(s) = f(s)$; if s belongs to the first occasion, then $h(s) = \arg_t\{s = g(t)\}$. Thus for any $t \in T$ there exists a $s \in S$, such that $t = h(s)$, and for any s_1, s_2 ($s_1 \neq s_2$), we have $h(s_1) \neq h(s_2)$, since f, g are injections. Thus $S \xrightarrow{h} T$ is a bijection, and $|S| = |T|$.

$\square$

Proposition 5. *$\exists$ a bijection f such that $\mathbb{R} \xrightarrow{f} \mathbb{C}$.*

Proof. Only thing we need to do is construct two injection between $\mathbb{R}$ and $\mathbb{C}$. Define for any $r \in \mathbb{R}$, $f(r) = (r, r)$, then $\mathbb{R} \xrightarrow{f} \mathbb{C}$ is an injection. For any $(a, b) \in \mathbb{C}$, we could write them as infinite expression decimal notation:

$$a = a_0 + 0.a_1 a_2 a_3 \cdots$$
$$b = b_0 + 0.b_1 b_2 b_3 \cdots$$

where $a_i, b_i (i \in \mathbb{N}_0) \in \mathbb{N}_0$. Define $g(a, b) = 0.a_0 b_0 a_1 b_1 a_2 b_2 a_3 b_3 \cdots \in \mathbb{R}$, thus $\mathbb{C} \xrightarrow{g} \mathbb{R}$ is a injection. $\square$

Lecture 3. Elementary Number Theory

CONTENT:

Fundamental Theorem of Arithmetic

Proposition 6 (Division). $\forall a \in \mathbb{Z}, b \in \mathbb{N}, \exists! q \in \mathbb{Z}, r \in \mathbb{N}_0,$ s.t. $a = bq + r \wedge 0 \leq r < b$.

Note 13. Dividend a, quotient $q \in \mathbb{Z}$, divisor $b \in \mathbb{N}$, factor $r \in \mathbb{N}_0$.

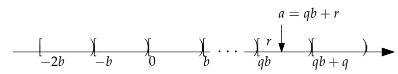


Figure 5: $a = qb + r$.

You can divide the number axis as a family of intervals with open left and closed right $[kb, (k+1)b)$, just like right figure.

So any integer a would fall into a specific interval of the axis, denote as $[qb, qb+b)$, and it can only be represented as $a = qb + r$ with $0 \leq r < b$, which implies the existence and uniqueness of the q and r.

Exercise 5. Show that if $a \in \mathbb{Z}, b \in \mathbb{N}$, then $b|a \Leftrightarrow \exists q \in \mathbb{Z}, r \in \mathbb{N}_0$ s.t. $a = qb + r \wedge r = 0$.

Note 14. For $b, a \in \mathbb{Z}$, $b|a$ means $\exists m \in \mathbb{Z}$, s.t. $a = bm$. Notice that we do not restrict b in $\mathbb{N}$. Thus $\cdot|\cdot$ is a distinct concept with Division whose $r = 0$. For example, we could say $-2|-4$, but -2 can not be a divisor.

Proof. $\Rightarrow$: Trivial, $\Leftarrow$: if $b|a$ then $\exists \mu \in \mathbb{Z}$, s.t. $a = \mu b = \mu b + 0$. Since the existence and uniqueness of q, r, we have that $q = \mu, r = 0$. □

Proposition 7 (Greatest common factor). *Assume that $a, b \in \mathbb{Z}$ and one of a, b is not 0, $\exists x_0, y_0 \in \mathbb{Z}, n = ax_0 + by_0$, such that*
1. *$\forall x, y \in \mathbb{Z}, n|ax + by$;*
2. *$\forall m \in \mathbb{N}, m|a \wedge m|b \Rightarrow m|n$.*

That is n is the greatest common factor of a, b.

Proof. Define a set $S := \{ax + by | x, y \in \mathbb{Z}, ax + by > 0\}$, and $\min S =: n = ax_0 + by_0$, thus $n \in \mathbb{N}$. For any $x, y \in \mathbb{Z}$, $\exists! q \in \mathbb{Z}, 0 \leq r < n,$ s.t. $ax + by = qn + r$.

$$ax + by = qn + r = q(ax_0 + by_0) + r$$

thus $r = a(x - qx_0) + b(y - qy_0) \in S$. If $r \neq 0 (r > 0)$, then $r \geq n$, which leads to a contradiction, thus $r = 0$ and $n|ax + by$ for any $x, y \in \mathbb{Z}$.

On the other hand, if $m \in \mathbb{N}, m|a \wedge m|b$, then $\exists \mu, \nu \in \mathbb{Z}$, such that $a = \mu m, b = \nu m$, and $n = ax_0 + by_0 = \mu m a x_0 + \nu m b y_0 = (\mu a x_0 + \nu b y_0)m$, thus $m|n$.

Thus n is the greatest common factor of a, b, denoted as $n = (a, b)$. □

Note 15. Generally, we can prove that $n = \min\{\sum_{i=1}^N a_i x_i \,\Big|\, x_i \in \mathbb{Z}, \sum_{i=1}^N a_i x_i > 0\}$ is the greatest common factor of any integer $a_1, \cdots, a_N$.

Proposition 8. *Given $\forall a, b, c \in \mathbb{Z}$, $(a, b) = 1 \wedge a|bc \Rightarrow a|c$.*

Proof. As we know, $\exists \mu, \nu \in \mathbb{Z}$, s.t. $n = \mu a + \nu b = (a, b) = 1$, then

$$\mu ac + \nu bc = c \Rightarrow \mu + \nu \frac{bc}{a} = \frac{c}{a},$$

since $\mu + \nu \frac{bc}{a} =: m \in \mathbb{Z}$, $c = ma$, thus $a|c$. □

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ can be represented in exactly one way as a product of prime powers:*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the n_i are positive integers.

Proof. The existence is trivial, we will show the uniqueness. Suppose there exists another distinct primes series $q_1, \cdots, q_l$ with $m_1, \cdots, m_l$ are positive integers, such that

$$\prod_{i=1}^{k} p_i^{n_i} = \prod_{i=1}^{l} q_j^{m_j},$$

suppose that $q_s (s \in \{1, 2, \cdots, l\}) \notin \{p_1, \cdots, p_k\}$; denote $\frac{1}{q_s} \prod_{i=1}^{l} q_j^{m_j}$ as w, then $w \in \mathbb{Z}$, and $\prod_{i=1}^{k} p_i^{n_i} = q_s w$, thus $q_s | \prod_{i=1}^{k} p_i^{n_i}$. Since

$$(q_s, \underbrace{p_1, \cdots, p_1}_{n_1}, \cdots, \underbrace{p_k, \cdots, p_k}_{n_k}) = (q_s, p_1, \cdots, p_k) = 1$$

we have that $q_s | \prod_{i=1}^{k} p_i^{n_i} \frac{1}{p_1}$. Repeat this process leads to $q_s | p_k$, which is a contradiction. So $q_s \nexists$, and $p_1, \cdots, p_k, n_1, \cdots, n_k$ are unique. □

Note 16. If we prime factorize two numbers a, b, the greatest common factor of the two numbers, denote as (a, b), is the production of the intersection of their prime factors. The least common multiple, denote as $[a, b]$, is the production of the union.

Thus for $a, b, c \in \mathbb{Z}$, we have that $([a, b], c) = [(a, c), (b, c)]$, and $[(a, b), c] = ([a, c], [b, c])$.

Integer equation

Exercise 6. Given $a, b, c \in \mathbb{Z}$ show that $(a, b) | c \Leftrightarrow$ equation $ax + by = c$ has integer solution.

Proof. $\Rightarrow$: $(a, b)|c$, thus $\exists x_0, y_0, m \in \mathbb{Z}$ such that $m(a, b) = m(x_0 a + y_0 b) = c$, thus $x = m x_0, y = m y_0$. $\Leftarrow$: $\exists m, n \in \mathbb{Z}$, such that $a = m(a, b), b = n(a, b)$, thus $c = ax + by = xm(a, b) + yn(a, b) = (a, b)(xm + yn)$, thus $(a, b)|c$. □

Note 17. Generally, for integers $a_i (i = 0, \cdots, N)$, $\sum_{i=1}^{N} a_i x_i = a_0$ has integer solution $\Leftrightarrow (a_1, \cdots, a_N)|a_0$.

Now we want to explore how to find all possible $x, y \in \mathbb{Z}$ such that $ax + by = c$? Assume that $a, b, c, x_0, y_0 \in \mathbb{Z}$ and $ax_0 + by_0 = c$. If $x, y \in \mathbb{Z}$, s.t. $ax + by = c \Leftrightarrow a(x_0 - x) = b(y - y_0) \Leftrightarrow \frac{a}{(a,b)}(x_0 - x) = \frac{b}{(a,b)}(y - y_0)$, thus $\frac{a}{(a,b)} \Big| \frac{b}{(a,b)}(y - y_0)$. Since $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$, we have that $\frac{a}{(a,b)} \Big| (y - y_0)$, that is $\exists t \in \mathbb{Z}$, s.t. $(y - y_0) = t\frac{a}{(a,b)}$ and $(x_0 - x) = t\frac{b}{(a,b)}$. Thus the sufficient and necessary condition of $x, y \in \mathbb{Z}$ is the solution of $ax + by = c$ is

$$y = y_0 + t\frac{a}{(a, b)}, \quad x = x_0 - t\frac{b}{(a, b)}$$

for $\forall t \in \mathbb{Z}$.

Congruence

Definition 15 (Congruence)**.** For $a, b, m \in \mathbb{Z}$, we say that $a \equiv b(\text{mod } m)$ if $m|(a-b)$.

Exercise 7. When $m \in \mathbb{N}$, show that $a \equiv b(\text{mod } m) \Leftrightarrow r_{a,m} = r_{b,m}$. ($r_{a,m}$ is the factor of a is divided by m)

Proof. $\Leftarrow$: Trivial. $\Rightarrow$: $a \equiv b(\text{mod } m)$ then $\exists \mu \in \mathbb{Z}$ such that $m\mu = (a-b)$. Since $m \in \mathbb{N}$, thus $\exists q_{a,b}, q_{b,m} \in \mathbb{Z}$ and $r_{a,m}, r_{b,m} \in \mathbb{N}_0$ where $0 \leq r_{a,m}, r_{b,m} < m$, such that $a = q_{a,m} \cdot m + r_{a,m}$, $b = q_{b,m} \cdot m + r_{b,m}$ and $(a-b) = m(q_{a,m} - q_{b,m}) + (r_{a,m} - r_{b,m})$. Since the conclusion of Exercise 5, we have $q_{a,m} - q_{b,m} = \mu$ and $r_{a,m} - r_{b,m} = 0$. □

Thus the intuition of mod is just like the right figure. It is easily to check that congruence is an equivalence relation on $\mathbb{Z}$.

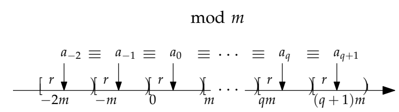


Figure 6: Intuition

Exercise 8. Show that $a \equiv b(\text{mod } m), a' \equiv b'(\text{mod } m) \Rightarrow a \pm a' \equiv b \pm b'(\text{mod } m)$ and $aa' \equiv bb'(\text{mod } m)$.

Proof. $\exists \mu, \nu \in \mathbb{Z}$, s.t. $a - b = \mu m$ and $a' - b' = \nu m$, thus $(\mu \pm \nu)m = (a \pm a') - (b \pm b')$, thus $a \pm a' \equiv b \pm b'(\text{mod } m)$. Since $aa' - bb' = aa' - ba' + ba' - bb' = a'(a-b) + b(a'-b') = a'\mu m + b\nu m = m(a'\mu + b\nu)$, where $a'\mu + b\nu \in \mathbb{Z}$, thus $aa' \equiv bb'(\text{mod } m)$. □

Note 18. If $a \equiv b(\text{mod } m)$, for $n \in \mathbb{Z}$ have $an \equiv bn(\text{mod } mn)$.

Before we talk about the "division" in mod relation, we need talk about the "Modular Multiplicative Inverse" in mod.

Proposition 9. *Given $a, b, m \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $ax \equiv b(\text{mod } m) \Leftrightarrow (a, m)|b$.*

Proof. $ax \equiv b(\text{mod } m) \Leftrightarrow \exists y \in \mathbb{Z}$ s.t. $ym = ax - b$ that is the equation $ax - my = b$ has integer solutions $\Leftrightarrow (a, -m)|b \Leftrightarrow (a, m)|b$. □

Specially, when $(a, m) = 1$, $\exists x \in \mathbb{Z}$ such that $ax \equiv 1(\text{mod } m)$ and x is the Modular Multiplicative Inverse of a.

Theorem 2 (The Chinese remained theorem)**.** *For $a_1, \cdots, a_n, m_1, \cdots, m_n \in \mathbb{Z}$, if $(m_i, m_i') = 1 (i = 1, \cdots, n)$ where $m_j' = [m_1, \cdots, m_{j-1}, m_{j+1}, \cdots, m_n]$, then $\exists x \in \mathbb{Z}$, such that $x \equiv a_i(\text{mod } m_i)(i = 1, \cdots, n)$ at the same time.*

Proof. Consider the equations system:

$$
\begin{aligned}
x &\equiv 1(\text{mod } m_1) \\
x &\equiv 0(\text{mod } m_2) \\
&\cdots \\
x &\equiv 0(\text{mod } m_n)
\end{aligned}
$$

Thus any x that satisfies the last $n-1$ equations is the multiples of the $[m_2, \cdots, m_n] = m2 \cdots m_n$. Thus $x = tm2 \cdots m_n, t \in \mathbb{Z}$. Substitute into the first equation, the issue is transformed to whether or not $\exists t, s \in \mathbb{Z},$ s.t. the following equation holds:

$$tm2 \cdots m_n - sm_1 = 1$$

The answer is positive since $(m_1, m2 \cdots m_n) = 1$. Thus there exist $x_1 \in \mathbb{Z}$ that satisfies the equation system above. And the same thing for $x_2, \cdots, x_n$. Thus we create a group of orthogonal basis for the equation, and the integer $x = \sum_{i=1}^{n} a_i x_i$ is the solution of $x \equiv a_i (\text{mod } m_i)(i = 1, \cdots, n)$. □

Note 19. The condition, $(m_i, m_i') = 1(i = 1, \cdots, n)$, is equivalent with $m_i(i = 1, \cdots, n)$ pairwise co-prime.

Suppose $\exists x_0, x \in \mathbb{Z}$, s.t. $x_0 \equiv a_i(\text{mod } m_i)(i = 1, \cdots, n)$ and $x \equiv a_i(\text{mod } m_i)(i = 1, \cdots, n)$. Then $(x - x_0) \equiv 0(\text{mod } m_i)(i = 1, \cdots, n)$. Thus $x - x_0$ is the multiples of the least common multiple of $m_1, \cdots, m_n$, that is $x = x_0 + t \prod_{i=1}^{n} m_i, t \in \mathbb{Z}$, which leads to the all integer solutions of the equation $x \equiv a_i(\text{mod } m_i)(i = 1, \cdots, n)$.

But what if we release the restriction that $m_i(i = 1, \cdots, n)$ pairwise co-prime.

Proposition 10. $\exists x \in \mathbb{Z}$, s.t. $x \equiv a(mod\ m) \wedge x \equiv b(mod\ n) \Leftrightarrow (m, n)|(b - a)$.

Proof. $\Rightarrow$: $\exists \mu, \nu \in \mathbb{Z},$ s.t. $x - a = \mu m, x - b = \nu n \Rightarrow b - a = \mu m - \nu n$, which forms a integer equation, thus $(m, n)|(b - a)$.

$\Leftarrow$: All $x \in \mathbb{Z}$ that satisfies $x \equiv a(\text{mod } m)$ has $x - a = \mu m$, for some $\mu \in \mathbb{Z}$. Substitute this formula into the second equation: $a + \mu m \equiv b(\text{mod } n)$, that is

$$a + \mu m - b = \nu n$$

for some $\mu, \nu \in \mathbb{Z}$. That is $\mu m - \nu n = b - a$ has integer solutions whose sufficient condition is $(m, n)|(b - a)$. □

So suppose $x_0, x \in \mathbb{Z}$ satisfies the equations system, then $x - x_0 \equiv 0(\text{mod } m)$ and $x - x_0 \equiv 0(\text{mod } n)$, thus $x = x_0 + t \cdot [m, n], t \in \mathbb{Z}$, this is the all solutions for the equations system.

Lecture 4. Binary operation, Group and Subgroup

CONTENT:

Binary operation

Definition 16 (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 7. $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathcal{P}(X), \backslash), (\mathcal{P}(X), \cup), (\mathcal{P}(X), \cap)$ are all binary operations.

Definition 17 (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 8. 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 18 (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 9. $(\mathbb{N}_0, +)$ 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 19 (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.

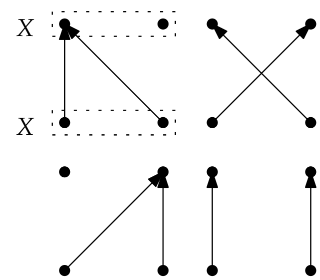


Figure 7: Four maps in X^X

Example 10. $(\mathbb{C}, \cdot)$ 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 11. 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.

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 9. Suppose $(S, \square)$ 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

$$s'' = (s'\square s)\square s'' = s'\square(s\square s'') = s'$$

$\square$

Note 20. Since the inverse of the element s is uniqueness, we could denote it as s^{-1}.

Exercise 10. Given an associative binary operation $(S, \square)$ with a unit element e, show that s_1, s_2 are invertible w.r.t. $\square \Leftrightarrow s_1 \square s_2$ and $s_2 \square s_1$ are invertible.

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

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

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

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

$$s_2 \square \alpha \square s_1 \square s_2 = s_2 \square e = s_2$$

and then operate s_1 on the right:

$$s_2 \square \alpha \square s_1 \square s_2 \square s_1 = s_2 \square s_1$$

since $s_2 \square s_1$ is invertible, thus

$$s_2 \square \alpha \square s_1 = e$$

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

Group

Definition 20 (Group)**.** We say a binary operation $(G, \square)$ is a group, if

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

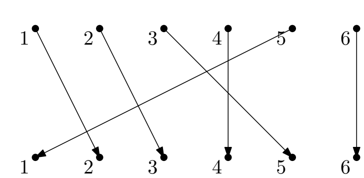
Example 12. There binary operations are groups: $(\mathbb{Z}, +)$, $(\mathbb{C}^\times, \cdot)$ $(\mathbb{C}^\times = \{c \in \mathbb{C} | c \neq 0\})$.

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

Note 21. If $x_1, x_2 \in X'$, thus x_1, x_2 is invertible w.r.t. $\square$, thus $x_1 \square x_2$ is invertible w.r.t. $\square$, thus $x_1 \square x_2 \in X'$. Thus $(X', \square)$ 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 21 (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 13. $C = \{e, (12)(34), (13)(24), (14)(23)\}$ 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 11. 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 $e_H^{-1} \Box e_H = e$:

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

Note 22. It is easy to check that the inverse of $h \in H$ in G is contained by H.

$\Box$

Exercise 12. 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 $H = m\mathbb{Z}$. $\Box$

Exercise 13 (Left Translation)**.** Given a group $(G, \Box)$, $g_0 \in G$, show that the map $G \xrightarrow{l_{g_0}} G$ where $g \xrightarrow{l_{g_0}} g_0 \Box g$ 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

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

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

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

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

Note 23. Correspondingly, there exists a concept: *right translation*.

Definition 22 (Left Coset)**.** Given a group $(G, \Box)$, $a \in G$, $(H, \Box)$ is a subgroup of $(G, \Box)$. way say $a \Box H := \{a \Box h | h \in H\}$ is the left coset of H associated to a.

Exercise 14. Suppose $(H, \Box)$ is a subgroup of $(G, \Box)$, $\forall a, b \in G$, show that either $a \Box H = b \Box H$ or $a \Box H \cap b \Box H = \emptyset$.

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

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

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

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

$$H = e \Box H = h \Box H$$

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 24. 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 15. 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 $a \Box H = b \Box H$.

□

Note 25. 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 23 (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 26. Thus G/H is the set of all cosets of H, and $G/H \subseteq \mathcal{P}(G)$.

Lecture 5. Group Actions

CONTENT:

Subgroup

Definition 24 (Cyclic Subgroup)**.** Given a group $(G, \Box)$, for any $g \in G$, and $k \in \mathbb{Z}$, we define

$$g^k := \begin{cases} \underbrace{g\Box \cdots \Box g}_{k}, & k > 0 \\ e, & k = 0 \\ \underbrace{g^{-1}\Box \cdots \Box g^{-1}}_{k}, & k < 0. \end{cases}$$

$\{g^k | k \in \mathbb{Z}\}$ constructs a subgroup of $(G, \Box)$. We call $\{g^k | k \in \mathbb{Z}\}$ is a cyclic subgroup generated by g, denote as $\langle g \rangle$.

Given $g \in G$, for any $g^{k_1}, g^{k_2} \in \langle g \rangle$, $g^{k_1}\Box g^{k_2} = g^{k_1+k_2} \in \langle g \rangle$, $e \in \langle g \rangle$ and for any $g^k \in \langle g \rangle$, $(g^k)^{-1} = g^{-k} \in \langle g \rangle$, thus $\langle g \rangle$ constructs a subgroup of $(G, \Box)$.

Note 27. The concept of cyclic subgroup provide a method to construct a subgroup of $(G, \Box)$.

Example 14. Given $g \in G$, suppose $g^k \neq e(k = \{1, 2, 3, 4, 5, 6\})$, and $g^7 = e$. Then $g^7 = g^6\Box g = g\Box g^6 = e$, thus $g^6 = g^{-1}$.

It is easy to check that $\langle g \rangle = \{g, g^2, g^3, g^4, g^5, g^6, e\}$. For any other element such as $g^9 = g^7\Box g^2 = g^2$, thus $\langle g \rangle$ has at most 7 elements. If $g^3 = g^5$, then $g^3 = g^3\Box g^2 = g^2\Box g^3 \Rightarrow g^2 = e$, it is a contradiction, thus $\langle g \rangle$ has at least 7 elements.

So if $\exists k \in \mathbb{Z}$, such that $g^k = e$, then $\langle g \rangle$ is finite and $\langle g \rangle = \{g, g^2, \cdots, g^k\}$, otherwise $\langle g \rangle$ is infinite.

There would be two occasions of $\langle g \rangle$:

1. $\exists a, b \in \mathbb{Z}, a < b,$ s.t. $g^a = g^b$.
   In this case, $g^a = g^b = g^a \Box g^{b-a} = g^{b-a} \Box g^a$, thus $g^{b-a} = e$, we say $\min\{b-a\}$ is the degree of g, denote as $|\langle g \rangle|$.
2. $\forall a, b \in \mathbb{Z}, a < b, g^a \neq g^b$
   In this case, we say $|\langle g \rangle| = \infty$.

Given a finite group $(G, \Box)$, $g \in G$, $\langle g \rangle$ is a subgroup of G. Thus $\langle g \rangle$ is a finite group, which means $\exists a < b$, s.t. $g^a = g^b \Rightarrow g^{b-a} = e$. Thus $\langle g \rangle$ has total $|\langle g \rangle| = \min\{b-a\}$ elements, and $g^{|\langle g \rangle|} = e$. Notice that $\langle g \rangle$ is the subgroup of $(G, \Box)$, thus $|\langle g \rangle| \mid |G|$ ($\exists q \in \mathbb{Z}$, s.t. $|G| = q|\langle g \rangle|$). Thus for a finite group $(G, \Box)$, $\forall g \in G, g^{|G|} = e$.

Definition 25 (Equivalence Class)**.** Given a set X, an equivalence relation R on X and $\forall x \in X$, we say $\{x' \in X | x' R x\}$ the equivalence class of x under R, denote as $R(x)$.

Definition 26 (Quotient Set)**.** We say the set whose elements are all equivalence class of the elements in X, that is $\{R(x) | \forall x \in X\}$, the quotient set of X under R, denote as X/R.

Example 15. Define an equivalence relation $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x \equiv y (\text{mod } 5)\}$. The equivalence class of 1 under R is $R(1) = \{1 + q \cdot 5 | q \in \mathbb{Z}\}$, and the Quotient set of $\mathbb{Z}$ under R is $\mathbb{Z}/R = \{R(1), R(2), R(3), R(4), R(5)\}$.

Given a set X and an equivalence relation R, for $\forall x \in X, x \in R(x)$; for $\forall x_1, x_2 \in X$, either $R(x_1) = R(x_2)$ or $R(x_1) \cap R(x_2) = \emptyset$ (this can be proved by transitivity). Collectively,

1. X is the union of all equivalence classes;
2. different equivalence classes are disjoined.

Conversely, if we can divide a set X into many blocks, then the disjoined blocks(subsets) define an equivalence relation.

Group actions

Given a set X, a group $(G, \Box)$ and a map $G \times X \xrightarrow{\alpha} X$, for any $g \in G, x \in X$, we denote $\alpha(g, x)$ as $g * x$ for simplifying the notations. You can view g and x as a driver and an item respectively. So the map $G \times X \xrightarrow{\alpha} X$ means the process where a driver drives an old item into a new item.

Definition 27 (Left group actions)**.** We call the map α is a (left) group action on $(G, \Box)$ if

1. for $\forall g, g' \in G, x \in X, g * (g' * x) = (g \Box g') * x$;
2. for $\forall x \in X, e * x = x$.

Example 16. Given a set X, for $g \in Perm(X)$ and $x \in X$, $g * x = g(x)$ is a group action on X.

Definition 28 (Orbit)**.** Given a group $(G, \Box)$ which actions on a set X, for $x \in X$, we call the set $G(x) = \{g * x | g \in G\}$ is the orbit of x.

Example 17. Group $(\mathbb{Z}, +)$ actions on $\mathbb{R}$ as for $\forall t \in \mathbb{Z}, (x, y) \in \mathbb{R}^2$, let $t * (x, y) = (x + 2t, y - t)$, then the orbits of $x_1, x_2, x_3, x_4 \in \mathbb{R}^2$ are like the margin figure.

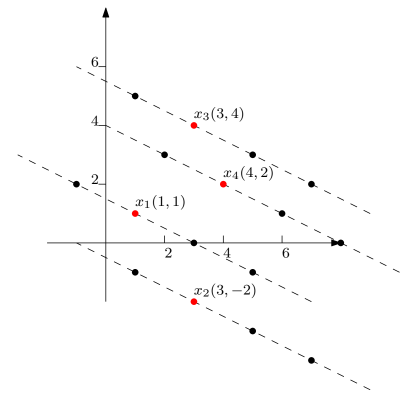


Figure 8: Orbits of x_1, x_2, x_3, x_4

Exercise 16. Suppose a group $(G, \Box)$ actions on a set X, define a relation $R := \{(x, x') \in X \times X | \exists g \in G, \text{ s.t. } x' = g * x\}$, that is $R := \{(x, x') \in X \times X | x' \in G(x)\}$. Show that R is an equivalence relation.

Proof. All we need to prove is:

1. $x \in G(x)$;
2. $x' \in G(x) \Rightarrow x \in G(x')$;
3. $x' \in G(x), x'' \in G(x') \Rightarrow x'' \in G(x)$.

1. Since $e \in G$, and $x = e * x$, thus $x \in G(x)$; 2. $x' \in G(x)$, thus $\exists g \in G$, s.t.

$$\begin{aligned}
&x' = g * x \\
&\Rightarrow g^{-1} * x' = g^{-1} * (g * x) \\
&\Rightarrow g^{-1} * x' = (g^{-1} \Box g) * x \\
&\Rightarrow g^{-1} * x' = e * x = x
\end{aligned}$$

since $g^{-1} \in G$, $x \in G(x')$; 3. $x' \in G(x), x'' \in G(x')$, thus $\exists g_1, g_2 \in G$, s.t.

$$\begin{aligned}
x'' &= g_2 * x' \\
&= g_2 * (g_1 * x) \\
&= (g_2 \Box g_1) * x
\end{aligned}$$

$g_1, g_2 \in G$, thus $g_2 \Box g_1 \in G$, and $x'' \in G(x)$. $\Box$

This exercise shows the orbit of x is an equivalence class of x, thus the difference orbits are disjoin, and the union of all orbits is X.

Definition 29 (Stablizer)**.** Suppose a group $(G, \Box)$ actions on a finite set X, for any $x \in X$, we call $G_x = \{g \in G | g * x = x\}$ the stablizer of x.

Exercise 17. Show that G_x constructs a subgroup of $(G, \Box)$.

Proof. All we need to prove is 1) G_x is enclosed; 2) $(G_x, \Box)$ is a group.

1. for $\forall x \in X, \forall g_1, g_2 \in G_x$:

$$\begin{aligned}
(g_1 \Box g_2) * x &= g_1 * (g_2 * x) \\
&= g_1 * x \\
&= x,
\end{aligned}$$

thus $g_1 \Box g_2 \in G_x$, similarly, $g_2 \Box g_1 \in G_x$.

2. since $\forall g_1, g_2, g_3 \in G_x \subseteq G$, the associative follows; 3. since $e * x = x$, $e \in G_x$; 4. for $\forall x \in X, \forall g \in G_x$:

$$\begin{aligned} g^{-1} * x &= g^{-1} * (g * x) \\ &= (g^{-1} \Box g) * x \\ &= e * x \\ &= x, \end{aligned}$$

thus $g^{-1} \in G_x$. The first proof shows G_x is enclosed, the last 3 proofs show $(G_x, \Box)$ is a group, thus $(G_x, \Box)$ is a subgroup of $(G, \Box)$. □

Definition 30 (Orbit Map)**.** Suppose a group $(G, \Box)$ actions on a finite set X, given $x \in X$, we say the map $G \xrightarrow{o_x} G(x)$ with $g \mapsto g * x$ is the orbit map of x.

Note 28. o_x is a surjection.

Exercise 18. For $\forall g, g' \in G$, show that $o_x(g) = o_x(g') \Leftrightarrow g \Box G_x = g' \Box G_x$.

Proof. $\Rightarrow$:

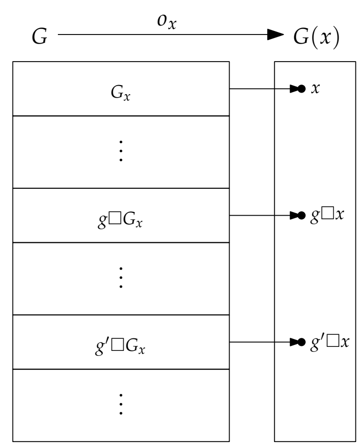
$$\begin{aligned} (g^{-1} \Box g') * x &= g^{-1} * (g' * x) \\ &= g^{-1} * (g * x) \\ &= (g^{-1} \Box g) * x \\ &= e * x \\ &= x, \end{aligned}$$

thus $g^{-1} \Box g' \in G_x \Rightarrow g \Box G_x = g' \Box G_x$.

$\Leftarrow$: $g \Box G_x = g' \Box G_x \Rightarrow \forall h \in G_x$ s.t. $g \Box h = g' \Box h$. Thus

$$\begin{aligned} g * x &= g * (h * x) \\ &= (g \Box h) * x \\ &= (g' \Box h) * x \\ &= g' * (h * x) \\ &= g' * x. \end{aligned}$$

□



So if $\exists g, g' \in G$, s.t. $g' \Box x = g \Box x$ then g, g' come from the same coset of G_x; conversely, if g, g' are from the same coset of G_x, then $g' \Box x = g \Box x$. That means o_x is a **bijection** from the quotient set G/G_x to the orbit $G(x)$. Thus for finite group $(G, \Box)$ actioning on X, and $x \in X$, have

$$|G/G_x| = |G|/|G_x| = |G(x)|.$$

Note 29. Remember that the cosets of G_x have the same cardinality.

Theorem 3 (Burnside). *Suppose a finite group $(G, \square)$ actions on a finite set X, then X has*

$$\frac{1}{|G|} \cdot \sum_{g \in G} |\{x \in X | g * x = x\}|$$

orbits.

Proof. Denote the number of orbits as τ. We now compute $\delta = |\{(g, x) \in G \times X | g * x = x\}|$ in two orders. The meaning of these operations is like the right margin figure.

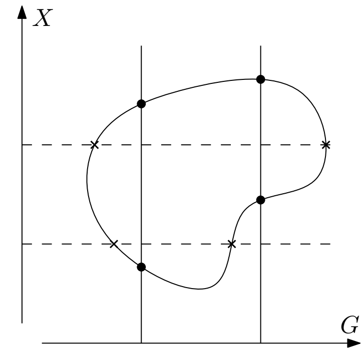


Figure 9: $|\{(g, x) \in G \times X | g * x = x\}|$

1. Fix x: so

$$\begin{aligned}
\delta &= \sum_{x \in X} |\{g \in G | g * x = x\}| \\
&= \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G(x)|} \\
&= |G| \cdot \sum_{x \in X} \frac{1}{|G(x)|} \\
&= |G| \cdot \tau.
\end{aligned}$$

Notice the last equation, remember that X is the disjoin union of the all orbits. So the sum of $\frac{1}{|G(x)|}$ where xs are in the same orbit is 1. And the sum of $\frac{1}{|G(x)|}$ of all $x \in X$ is the number of orbits τ.

2. Fix g: so

$$\delta = \sum_{g \in G} |\{x \in X | g * x = x\}|.$$

Simultaneous equations, we have

$$|G| \cdot \tau = \sum_{g \in G} |\{x \in X | g * x = x\}|,$$

thus $\tau = \frac{1}{|G|} \cdot \sum_{g \in G} |\{x \in X | g * x = x\}|$. $\square$

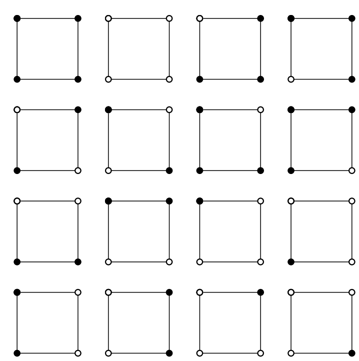
Example 18. Color four vertices of a square in black or white, allowing rotation, How many different coloring methods are there?

Solution. Let X be the all coloring method without rotation, so $|X| = 2^4 = 16$. Let G be the set that are all rotations of X, let r represents rotate 90 degrees in clockwise, then $G = \{e, r, r^2, r^3\} = \langle r \rangle$. Now the question is how many orbits of X under G are there?

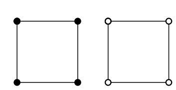
Fix $g = e$, then $|\{x \in X | e * x = x\}| = 16$, these are the all element if X; Fix $g = r$, then $|\{x \in X | r * x = x\}| = 2$; Fix $g = r^2$, then $|\{x \in X | r * x = x\}| = 4$; Fix $g = r^3$, then $|\{x \in X | r * x = x\}| = 2$.

Thus the number of the orbits is

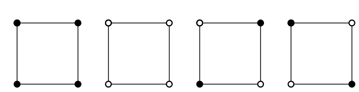
$$\begin{aligned}
\tau &= \frac{1}{|G|} \cdot \sum_{g \in G} |\{x \in X | g * x = x\}| \\
&= \frac{1}{4} \cdot (16 + 2 + 4 + 2) \\
&= \frac{24}{4} = 6.
\end{aligned}$$



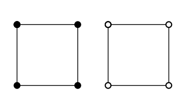
$\{x \in X | e * x = x\}$



$\{x \in X | r * x = x\}$



$\{x \in X | r^2 * x = x\}$



$\{x \in X | r^3 * x = x\}$

So there are totally 6 coloring methods. $\square$

Lecture 6. Open Sets on Metric Space (i)

CONTENT:

Metric space

Definition 31 (Metric Space)**.** Let $X \times X \xrightarrow{d} \mathbb{R}$ be a function, we cay that d is a metric on X or (X, d) is a metric space if for $\forall x, x', x'' \in X$ have

1. Positivity: $d(x, x') \geq 0$ and $d(x, x'') = 0$ iff $x = x'$;
2. Symmetry: $d(x, x') = d(x', x)$;
3. Triangle inequality: $d(x, x') \leq d(x, x'') + d(x'', x')$.

Exercise 19. Show that the triangle inequality is equivalent with for $\forall x, x', x'' \in X$

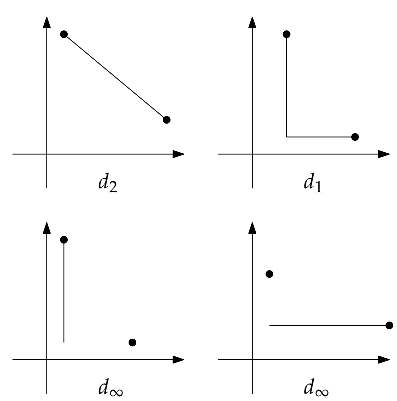
$$d(x, x') \geq |d(x, x'') - d(x', x'')|.$$

Proof. $\geq \Rightarrow \leq$: since $d(x, x') \geq |d(x, x'') - d(x', x'')| \geq d(x, x'') - d(x', x'')$, we have that $d(x, x'') \leq d(x, x') + d(x', x'')$.

$\leq \Rightarrow \geq$: if $\exists x, x', x''$ such that $d(x, x') < |d(x, x'') - d(x', x'')|$, then

$$\begin{aligned} d(x, x') &< |d(x, x'') - d(x', x'')| \\ &\leq |d(x, x') + d(x', x'') - d(x', x'')| \\ &\leq d(x, x') \end{aligned}$$

thus $d(x, x') < d(x, x')$, which leads to a contradiction. $\square$



Example 19. Here are some metric examples:

1. define $d_2(x, y) := \left(\sum_i^m |x_i - y_m|^2\right)^{1/2}$, $x, y \in \mathbb{R}^m$. Then d_2 is a metric on $\mathbb{R}^m$ by cauchy inequality.
2. define $d_1(x, y) := \sum_{i=1}^m |x_i - y_i|$, $x, y \in \mathbb{R}^m$. Then d_1 is a metric on $\mathbb{R}^m$.
3. define $d_\infty(x, y) := \max\{|x_i - y_i|\}$, $i \in \{1, 2, \cdots, m\}$, $x, y \in \mathbb{R}^m$. Then d_∞ is a metric on $\mathbb{R}^m$.

d_2 can be proved to be a metric by Cauchy inequality:

Exercise 20 (Cauchy inequality)**.** For any $(x_1, \cdots, x_n), (y_1, \cdots, y_n) \in \mathbb{R}^n$, show that

$$(x_1 y_1 + \cdots, x_n y_n)^2 \leq (x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2)$$

and "=" holds iff $\exists a, b \in \mathbb{R}$ which are not all 0.

Proof. Consider the polynomial $p(t) = \sum_{i=1}^{n}(x_i t + y)^2 = t^2 \sum_{i=1}^{n} x_i^2 + 2\sum_{i=1}^{n} x_i y_i + \sum_{i=1}^{n} y_i^2 \geq 0$, thus $\Delta = 4\left(\sum_{i=1}^{n} x_i y_i\right)^2 - 4\sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i^2 \leq 0 \Rightarrow \left(\sum_{i=1}^{n} x_i y_i\right)^2 \leq \sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i^2$. $\square$

Example 20 (p-adic)**.** If p is a prime number, $x \in \mathbb{Q}$, define

$$|x|_{p-adic} := \begin{cases} p^{-m}, & x = \dfrac{a}{b} \cdot p^m, x \neq 0, \\ 0, & x = 0, \end{cases}$$

where $a, b, m \in \mathbb{Z}$, $(a, p) = (b, p) = 1$. For $\forall x, y \in \mathbb{Q}$, define $d_{p-adic}(x, y) = |x - y|_{p-adic}$, then d_{p-adic} is a metric on $\mathbb{Q}$.

Assume $x = (a/b)p^m, y = (s/t)p^n \in \mathbb{Q}$ where $a, b, s, t, m, n \in \mathbb{Z}, (a, p) = (b, p) = (s, p) = (t, p) = 1, m > n$, then $|x|_{p-adic} = p^{-m} < |y|_{p-adic} = p^{-n}$, and

$$\begin{aligned} |x - y|_{p-adic} &= |(a/b)p^m - (s/t)p^n|_{p-adic} \\ &= \left| \frac{adp^{m-n} - bc}{bd} p^n \right|_{p-adic}. \end{aligned}$$

it is easy to check $adp^{m-n} - bc, bd \in \mathbb{Z}$ and $(adp^{m-n} - bc, p) = (bd, p) = 1$, thus

$$|x - y|_{p-adic} = p^{-n} = |y|_{p-adic} = \max\{|x|_{p-adic}, |y|_{p-adic}\}.$$

Thus for any $x, y, z \in \mathbb{Q}$, we have that

$$\begin{aligned} d_{p-adic}(x, y) &= \max\{|x|_{p-adic}, |y|_{p-adic}\} \\ &\leq \max\{|x|_{p-adic}, |z|_{p-adic}\} + \max\{|z|_{p-adic}, |y|_{p-adic}\} \\ &= d_{p-adic}(x, z) + d_{p-adic}(y, z), \end{aligned}$$

which follows the triangle inequality, the other two conditions is trivial.

Open set on metric space

Definition 32 (Open Ball)**.** Let (X, d) be a metric space, for $\forall r > 0$ and $x_0 \in X$, we let

$$B_r(x_0) := \{x \in X | d(x, x_0) < r\},$$

and call it the open ball with center x_0 and radius r; let

$$\overline{B_r(x_0)} := \{x \in X | d(x, x_0) \leq r\},$$

and call it the close ball with center x_0 and radius r.

Example 21 (discrete metric)**.** For $\forall x, x' \in \mathbb{R}^2$, define metric $d(x, x') = 0$ if $x = x'$, and $d(x, x') = 1$ if $x \neq x'$, then $B_1(x) = \{x\}$, $\overline{B_1(x)} = \mathbb{R}^2$, $B_{1.1}(x) = \mathbb{R}^2$.

Definition 33 (Open Set). $S(\subseteq X)$ is called an Open Set of X with respect to d, if $\forall x_0 \in S$, $\exists r > 0$ such that $B_r(x_0) \subseteq S$; $F(\subseteq X)$ is Close Set of X w.r.t. d if $X \backslash F$ is open set of X w.r.t. d.

Exercise 21. Prove that $B_r(x)$ is open set and $\overline{B_r(x)}$ is close.

Proof. For $\forall x' \in B_r(x)$, we have $d(x, x') < r$, donate $r - d(x, x')$ by s, then for $\forall x'' \in B_{s/2}(x')$ satisfy

$$\begin{aligned} d(x, x'') &\leq d(x, x') + d(x', x'') \\ &\leq d(x, x') + \frac{s}{2} \\ &< r, \end{aligned}$$

thus $x'' \in B_r(x)$ and $B_{s/2}(x') \subseteq B_r(x)$ and $B_r(x)$ is a open set. For $\forall x' \in X \backslash \overline{B_r(x)}$ has $d(x, x') > r$. Denote $d(x, x') - r$ by t, then for $\forall x'' \in B_{t/2}(x')$ satisfy

$$\begin{aligned} d(x, x'') &\geq |d(x, x') - d(x', x'')| \\ &\geq d(x, x') - d(x', x'') \\ &\geq d(x, x;) - \frac{t}{2} \\ &> r. \end{aligned}$$

Thus $B_{t/2}(x') \subseteq X \backslash \overline{B_r}$ and $X \backslash \overline{B_r}$ is an open set, thus $\overline{B_r}$ is a close set. □

Exercise 22. Let (X, d) be a metric space. show that

1. $X, \varnothing \subseteq_{open} X$;
2. $O_1, O_2 \subseteq_{open} X \Rightarrow O_1 \cap O_2 \subseteq_{open} X$;
3. $O_\alpha \subseteq_{open} X, (\alpha \in A) \Rightarrow \cup_{\alpha \in A} O_\alpha \subseteq_{open} X$ (α not necessarily be integral or countable);
4. All above corresponding statements for close set are true.

Note 30. First 3 statements are the essential intuition for the definition of *Topology*.

Proof. 1. Obviously X is an Open set thus $\varnothing$ is a close set. If $\varnothing$ is not an open set, then $\exists x \in \varnothing$, $\forall r > 0$ such that $B_r(x) \not\subseteq \varnothing$, which is impossible. Thus $\varnothing$ is an open set (logically) and X is a close set;
2. $\forall x \in O_1 \cap O_2$, $\exists r_1, r_2 > 0$, s.t. $B_{r_1}(x) \subseteq O_1$ and $B_{r_2}(x) \subseteq O_2$. Thus $\forall x' \in B_{\min\{r_1, r_2\}}(x) = B_{r_1}(x) \cap B_{r_2}(x) \Rightarrow x' \in O_1 \cap O_2 \Rightarrow B_{\min\{r_1, r_2\}}(x) \subseteq O_1 \cap O_2$, thus $O_1 \cap O_2$ is open. Collectively, the intersection of any finite open sets is an open set;
3. For $\forall x \in \cup_{\alpha \in A} O_\alpha$, $\exists$ at least one $\alpha' \in A$, s.t. $x \in O_{\alpha'}$, then $\exists r > 0$, s.t. $B_r(x) \subseteq O_{\alpha'} \subseteq \cup_{\alpha \in A} O_\alpha$, thus $\cup_{\alpha \in A} O_\alpha$ is an open set;
4. Take complementary set: The union of finite close sets is close; the intersection of any close sets is close.

□

Exercise 23. Show that an open set is the union of open balls.

Proof. Given an open set O, for any $o \in O, \exists r_o > 0,$ s.t. $B_{r_o}(o) \subseteq O$, define $O' = \cup_{o\in O} B_{r_o}(o)$. Thus for $\forall x \in O', \exists o',$ s.t. $x \in B_{r'_o}(o') \subseteq O \Rightarrow O' \subseteq O$;

On the other hand, for any $y \in O, \exists r_y > 0,$ s.t. $B_{r_y}(y) \subseteq O \Rightarrow y \in B_{r_y}(y) \subseteq O' \Rightarrow O \subseteq O'$. Thus $O = O' = \cup_{o\in O} B_{r_o}(o)$. $\square$

Definition 34 (Convergence)**.** Let (X, d) be a metric space, $a_n \in X, (n \in \mathbb{N}), L \in X$, define $\lim_{n\to\infty} a_n = L$ w.r.t. d, if $\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N$ s.t. $d(a_n, L) < \epsilon$, that is $a_n \in B_\epsilon(L)$.

Exercise 24. Show that

1. $\lim_{n\to\infty} a_n = L \Leftrightarrow \lim_{n\to\infty} d(a_n, L) = 0$;
2. $\lim_{n\to\infty} a_n = L \Leftrightarrow \forall L \in U \subseteq_{open} X, \exists N \in \mathbb{N}, \forall n \geq N$ s.t. $a_n \in U$.

Proof. (1) Trivial; (2) $\Rightarrow$: Suppose that $\lim_{n\to\infty} a_n = L$, for $\forall U$ that $L \in U, \exists r > 0,$ s.t. $B_r(L) \subseteq U$, and $\exists N \in \mathbb{N}$ such that $\forall n \geq N,$ s.t. $a_n \in B_r(L) \subseteq U$; $\Leftarrow$: Suppose $L \in U \subseteq_{open} X$, then $\exists r > 0$ such that $B_r(L) \subseteq U$. Since $B_r(L)$ is also an open set, then $\exists N \in \mathbb{N}$, for $\forall n \geq N,$ s.t. $a_n \in B_r(L) \subseteq U$. $\square$

We say $S \subseteq X$ is bounded w.r.t. d, if $\exists r > 0$ and $x_0 \in X,$ s.t. $S \subseteq B_r(x_0)$.

Theorem 4 (Bolzano-Weierstrass theorem)**.** *If $a_n \in \mathbb{R}^m (n \in \mathbb{N})$ is bounded w.r.t. d_2, then $\exists$ a subsequence $a_{n_m} (m \in \mathbb{N})$ which converges.*

Proof. We only prove $\mathbb{R}^2$ case. If we want to prove that the vector $a = (a_1, \cdots, a_m) \in \mathbb{R}^m \to L = (l_1, \cdots, l_m) \in \mathbb{R}^m$, all we need to prove is $\lim_{n\to\infty} a_i = l_i, (i = 1, \cdots, m)$.

Choose $M > 0,$ s.t. $a_n \in Q = [-M, M] \times [-M, M]$ for all $n \in \mathbb{N}$. Divide Q into 4 squares with equal size and choose one, say Q_1, such that $|\{n | a_n \in Q\}| = \infty$. Select $n_1 \in \mathbb{N}$, such that $a_{n_1} \in Q_1$. Repeat this and we have $\cap_{k=1}^{\infty} Q_k = \{a\}$. By theorem of nested interval we have that $\lim_{k\to\infty} a_{n_k} = a$. $\square$

Exercise 25. Let (X, d) be a metric space, $F \subseteq X$ show that $F \subseteq_{close} X \Leftrightarrow \forall a_n \in F(n \in \mathbb{N})$ and $\lim_{n\to\infty} a_n = a \in X$ then $a \in F$.

Proof. $\Rightarrow$: Assume that F is close and $a_n \in F$. If $a_n \to a \in X \backslash F$, then $\exists r > 0,$ s.t. $B_r(a) \in X \backslash F$. Since $\lim_{n\to\infty} a_n = a$, for r, there exists $N \in \mathbb{N}, \forall n \geq N,$ s.t. $d(a_n, a) < r$, i.e. $a_n \in B_r(a) \subseteq X \backslash F$, which leads to a contradiction. $\Leftarrow$: Suppose that $\forall a_n \in F(n \in \mathbb{N})$ and $\lim_{n\to\infty} a_n = a \in X$ then $a \in F$, and F is not close, which means $X \backslash F$ is not open, and $\exists x \in X \backslash F, \forall r > 0, B_r(x) \cap F \neq \emptyset$. Select $n \in \mathbb{N}$ such that $a_n = B_{\frac{1}{n}}(x) \cap F$. Thus $\lim_{n\to\infty} a_n = x \notin F$, which leads to a contradiction. $\square$

Note 31. Set family of sets as $\{B_{1/n}(x)\}_{n\in\mathbb{N}}$ is a very useful skill.

Definition 35 (Open cover, Compact set)**.** Let (X, d) be a metric space, $S \subseteq X$, $O_\alpha \in X(\alpha \in A)$, we say that $O_\alpha(\alpha \in A)$ form an open cover of S, if $S \subseteq \cup_{\alpha \in A} O_\alpha$. S is called a compact set if $\forall$ open cover $O_\alpha(\alpha \in A)$ of S, $\exists \alpha_1, \cdots, \alpha_m \in A$, s.t. $S \subseteq \cup_{i=1}^m O_{\alpha_i}$, where $\cup_{i=1}^m O_{\alpha_i}$ is called a finite subcover.

If there exists an open cover of F whose any finite subcover can not cover it, then F is not a compact set. for instance, let $F = (0, 1), O_n = (1/n, 2), n \in \mathbb{N}$, then O_n is an open cover of F, however any finite subcover of O_n can not cover F.

Theorem 5 (Heine-Borel theorem)**.** *Let $S \subseteq \mathbb{R}^n$, then S is compact $\Leftrightarrow$ S is bounded and closed.*

Proof. $\Rightarrow$: Suppose that S is compact, select a point $s \in S$ arbitrarily, define $O_i = B_i(s)$, it is easy to check that $S \subseteq \cup_{i \in \mathbb{N}} O_i$, since for any $s' \in S$, we have that $s' \in B_{2d(s,s')}(s) \subseteq O_{\lceil 2d(s,s') \rceil}$. Since S is compact, there exists a finite subcover, thus S is bounded.

Suppose S is compact, but S is not closed, which means $X \backslash S$ is not open and $\exists x \in X \backslash S$, s.t. $\forall r > 0, B_r(x) \cap S \neq 0$. Since S is bounded, define $\iota = \sup_{s \in S} d(s, x)$, define open cover

$$O_n = B_{\frac{\iota}{n}}(x) - B_{\frac{\iota}{n+1}}(x),$$

thus $O_i \cap O_j = \emptyset (i \neq j)$ and $O_i \cap S \neq \emptyset (\forall i)$. Thus O_n has no finite subcover, which leads to a contradiction and S is closed.

$\Leftarrow$: Suppose that S is bounded and closed, and $\exists$ an open cover $O_\alpha(\alpha \in A)$ of S which admits no finite subcover. Choose a cube Q containing S (S is bounded), divide Q into 4 equal-sized cubes and select one of them denoted by Q_1, s.t. $Q_1 \cap S$ can not be covered by finitely many Q_α, select a point such that $s_1 \in Q_1 \cap S$. Repeat.

Obviously, $\lim_{n \to \infty} s_n = a$, notice that $s_n \in Q_n \cap S \subseteq S$, thus $\lim_{n \to \infty} s_n = a \in S$ for S is closed. Thus there exist O_i such that $a \in O_i$. Since O_i is open, $\exists r > 0$, s.t. $B_r(a) \subseteq O_i$. Then $\exists N \in \mathbb{N}, \forall n \geq N$, s.t. $Q_n \subseteq B_r(a) \subseteq O_i$. Since $Q_n \cap S$ can not be covered by finitely many O_α, but could be covered by O_i, which leads to a contradiction. $\square$

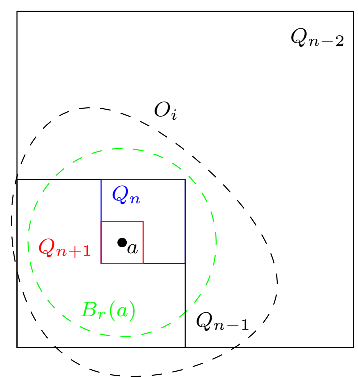


Figure 10: Heine-Borel theorem

Lecture 7. Open Sets on Metric Space (ii)

CONTENT:

Open set on metric space

Theorem 6 (The Lebesgue number of an open cover)**.** *Let (X, d) be a metric space and $K (\subseteq X)$ a compact set. For any given open cover*

$O_\alpha(\alpha \in A)$ *of* K*, there exists* $\delta > 0$*,* s.t. *for every* $x \in K$ *we have* $B_\delta(x) \subseteq O'_\alpha$ *for some* $\alpha' \in A$ *(*α' *depending on* x*).*

Proof. Since K is compact, for any open cover of K, there exists an finite subcover of K, that is $\exists O_{\alpha_i}, i = 1, \cdots, N$ such that

$$K \subseteq \bigcup_{i=1}^{N} O_{\alpha_i}.$$

For any point $x \in K$ there exist $O_{\alpha_j} \in \{O_{\alpha_i}\}_{i=1}^N$, s.t. $x \in O_{\alpha_j}$ and exists $\delta_x > 0$, s.t. $B_{\delta_x/2}(x) \subseteq B_{\delta_x}(x) \subseteq O_{\alpha_j}$ for O_{α_j} is open. Obviously we have that $B_{\delta_x/2}(x)$ is an open cover of K, i.e.

$$K \subseteq \bigcup_{x \in K} B_{\delta_x/2}(x),$$

and $B_{\delta_x/2}(x)$ has an finite subcover of K, donate as $\{B_{\delta_{x_i}/2}(x_i)\}_{i=1}^M$. Let $\delta = \min\{\delta_{x_i}\}_{i=1}^M$. Then for any $y \in K$, there exists $B_{\delta_{x_j}/2}(x_j) \in \{B_{\delta_{x_i}/2}(x_i)\}_{i=1}^M$ such that $y \in B_{\delta_{x_j}/2}(x_j)$ and $d(y, x_j) < \delta_{x_j}/2$. and for any y' where $d(y', y) < \delta/2 < \delta_{x_j}/2$, we have $d(x_j, y') \le d(x_j, y) + d(y, y') < \delta_{x_j}$, thus $y, y' \in B_{\delta_{x_j}}(x_j) \subseteq O_{\alpha'}$, or say $y, y' \in B_{\delta/2}(y) \subseteq B_{\delta_{x_j}}(x_j) \subseteq O_{\alpha'}$. □

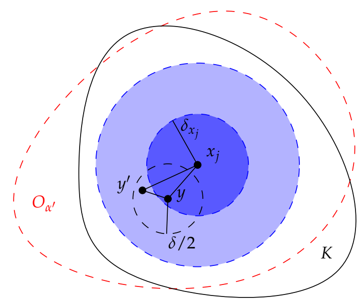
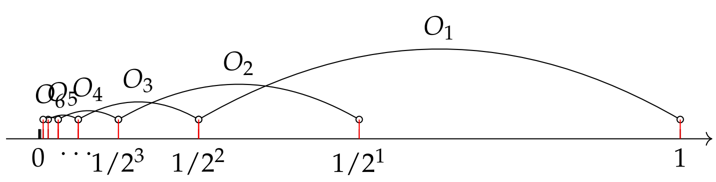


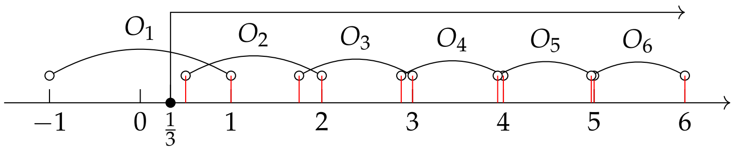
Figure 11: The Lebesgue number of an open cover

The theorem indicates for any open cover O_α of K, $\exists \delta > 0$, s.t. for $\forall x \in K, x' \in X$, is $d(x, x') < \delta$, then $\exists \alpha \in A$ we have $x, x' \in O_\alpha$. Such a $\delta > 0$ is called a **Lebesgue number** of the given open cover $O_\alpha(\alpha \in A)$. Notice that the statement could be false if the compactness assumption is dropped.

Exercise 26 (Open set)**.** Let $(X, d) = (\mathbb{R}, d_2), K = (0, 1), O_\alpha = (1/2^{\alpha+1}, 1/2^{\alpha-1})(\alpha \in \mathbb{N})$. Thus $1/2^\alpha \in O_\alpha$ and $\notin O_{\alpha'}$ if $\alpha' \neq \alpha(\alpha, \alpha' \in \mathbb{N})$. It is easy to check O_α is an open cover of K, but $|1/2^\alpha - 1/2^{\alpha+1}| = 1/2^{\alpha+1}$ can be arbitrarily small if $\alpha \uparrow$. Thus there exists $x \in K, x' \in X$ can not be covered one O_α, no matter how close they are.



Exercise 27 (Unbounded set)**.** Let $(X, d) = (\mathbb{R}, d_2), K = [1/3, \infty), O_\alpha = (\alpha - 1 - 1/2^{\alpha-1}, \alpha)(\alpha \in \mathbb{N})$. Thus $x = \alpha - 1/2^\alpha \in O_\alpha$ and $x' = \alpha \in O_{\alpha+1}$ and $d(x, x')$ could be arbitrarily small as $\alpha \uparrow$. Thus there exists $x \in K, x' \in X$ can not be covered one O_α, no matter how close they are.

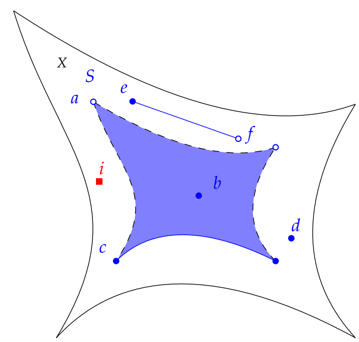


Definition 36 (Isolated point, limit point and accumulation point)**.**
Let (X, d) be a metric space and $S \subseteq X$. A point $x \in X$ is called:

- an **isolated point** of S, if $\exists \epsilon > 0$, s.t. $B_\epsilon(x) \cap S = \{x\}$ ($\Rightarrow x \in S$);
- a **limit point** of S, if $\forall \epsilon > 0$, s.t. $B_\epsilon(x) \cap S \backslash \{x\} \neq \emptyset$;
- an **accumulation point** of S, if $\exists$ seq. $a_n \in S (n \in \mathbb{N})$, s.t. $x = \lim_{n\to\infty} a_n$.

Example 22. $S \subseteq X$ is as the margin figure, point $i \notin S$:

point	iso. pts. of S	limit pts. of S	acc. pts. of S	$\in S$
i	$\times$	$\times$	$\times$	$\times$
a	$\times$	$\surd$	$\surd$	$\times$
b	$\times$	$\surd$	$\surd$	$\surd$
c	$\times$	$\surd$	$\surd$	$\surd$
d	$\surd$	$\times$	$\surd$	$\surd$
e	$\times$	$\surd$	$\surd$	$\surd$
h	$\times$	$\surd$	$\surd$	$\times$



Notice that x is a isolated point of $S \Rightarrow x \in S$; but x is a limit/accumulate point of $S \not\Rightarrow x \in S$.

Exercise 28. Let (X, d) be a metric space, $S \subseteq X$,

1. Show that x is an isolated/limit point of $S \Rightarrow x$ is a accumulate point of S;
2. Donate $\{\text{iso. pts. of} S\}, \{\text{limit pts. of} S\}$ and $\{\text{acc. pts. of} S\}$ by I_S, L_S, A_S respectively. Show that $I_S \cup L_S = A_S$;
3. Suppose $S \subseteq K \subseteq X$, where S is infinite and K is compact, show that $\{\text{limit pts. of} S\} \neq \emptyset$; (Prove by contradiction)

Proof. 1. If x is an isolated point of S, thus $x \in S$. Let $a_n \equiv x$, then $\lim_{n\to\infty} a_n = x$, thus x is an accumulate point of S; If x is a limit point of S, then for any $\epsilon > 0, B_\epsilon(x) \cap S \backslash \{x\} \neq \emptyset$. Let $a_n \in B_{1/n}(x) (n \in \mathbb{N})$, then $d(a_n, x) < 1/n$ for $\forall n \in N$, thus $\lim_{n\to\infty} a_n = x$, and x is an accumulate point of S.

2. We have obtained that $I_S, L_S \subseteq A_S$. Suppose $x \in A_S \backslash (I_S \cup L_S) \neq \emptyset$. Which means : (1) there exists seq. $a_n \in S$ such that $\lim_{n\to\infty} a_n = x$; (2) $\forall \epsilon > 0$, s.t. $B_\epsilon(x) \cap S \neq \{x\}$ ($\neg I_S$);(3) $\exists \epsilon' > 0$, s.t. $B_{\epsilon'}(x) \cap S \backslash \{x\} = \emptyset$ ($\neg L_S$). Let $B_\epsilon(x) \cap S = Q_\epsilon \neq \{x\}$, if $x \in Q_\epsilon$, then it leads to a contradiction with (3); If $x \notin Q_\epsilon$, then $Q_{\epsilon'} = \emptyset$, that is $B_{\epsilon'}(x) \cap S = \emptyset$ and for $\forall s \in S \Rightarrow d(s, x) \geq \epsilon'$, which leads to a contradiction with (1). Thus $A_S \backslash (I_S \cup L_S) = \emptyset$. Because $I_S, L_S \subseteq A_S$, we have $I_S \cup L_S = A_S$.

3. Since S is infinite, there exists an infinite seq. $a_n \in S$. By Bolzano-Weierstrass theorem, there exists a subseq. $a_{n_i} \in S$ such that $\lim_{i\to\infty} a_{n_i} = a$. Suppose $L_S = \emptyset$, which means for $\forall x, \exists \epsilon' > 0$, s.t. $B_{\epsilon'}(x) \cap S \backslash \{x\} = \emptyset$, thus there exists ϵ_a, s.t. $B_{\epsilon_a}(a) \cap S\backslash\{a\} = \emptyset$, which means $\forall s \in S, d(s,a) \geq \epsilon_a$ and leads to a contradiction.

□

Exercise 29. Let $(X,d) = (\mathbb{R}, d_2), S \subseteq \mathbb{R}$, show that if $\sup S$ ($\inf S$) exists, then it is an accumulate point.

Proof. If $\sup S \exists$, then for $\forall x \in S$, s.t. $x \leq \sup S$ and for $\forall \epsilon > 0$, $\exists x' \in S$, s.t. $\sup S - \epsilon < x'$. For any $n \in \mathbb{N}$, there exists $x_n \in S$ s.t. $\sup S - 1/n < x' \leq \sup S$, and $d(x_n, \sup S) < 1/n$, thus $x_n \to \sup S$ as $n \to \infty$. □

Exercise 30. Show that, if (X,d) be a metric space, then

$$S \subseteq_{close} X \Leftrightarrow A_S = S \Leftrightarrow L_S \subseteq S.$$

Proof. For any $x \in S$, let $a_n = x$, then $\lim_{n\to\infty} a_n = x$, thus $S \subseteq A_S$. Since example (**??**), we have $S \subseteq_{close} X \Leftrightarrow A_S = S$. $\Rightarrow$ Since $I_S \cup L_S = A_S$, we have $L_S \subseteq A_S = S$; $\Leftarrow$, for $L_S \subseteq A_S \subseteq S$, we have $S \subseteq A_S \Rightarrow S = A_S$. □

Limits of maps

Let (X, d_X) and (Y, d_Y) be metric spaces and $S \subseteq X$. We consider a map $f : S \mapsto Y$. e.g. $X = \mathbb{R}^2, Y = \mathbb{R}, S = \mathbb{R}^2 \backslash \{(0,0)\}, f : (x,y) \mapsto 1/x^2 + y^2$. (the reason why shrink X)

Definition 37. Limit Let $a \in X$ (not necessarily $\in S$) and $b \in Y$. We say that $\lim_{x\to a} f(x) = b$ if $\forall \epsilon > 0, \exists \delta > 0, \forall x \in S$, s.t. $0 < d_X(x,a) < \delta \Rightarrow d_Y(f(x), b) < \epsilon$.

Exercise 31. Show that

1. If a is a limit point of S and $\lim_{x\to a} f(x) = b$ and $\lim_{x\to a} f(x) = b'$ then $b = b'$;
2. Let $(Y, d_Y) = (\mathbb{R}^m, d_2)$ and $f : S \mapsto Y, g : S \mapsto Y$, where $S \subseteq X, a \in X$. If $\lim_{x\to a} f(x) = b$ and $\lim_{x\to a} g(x) = c$, then $\lim_{x\to a}(f(x) \pm g(x)) = b \pm c$. If furthermore $(Y, d_2) = (\mathbb{R}, d_2)$, then $\lim_{x\to a} f(x)g(x) = bc$; if $c \neq 0$, then $\exists \delta > 0$, s.t. $g(x) \neq 0$ for all $x \in B_\delta(a)\backslash\{a\}$ and $\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{b}{c}$.

Proof. 1. Since $\lim_{x\to a} f(x) = b$ and $\lim_{x\to a} f(x) = b'$, for $\forall \epsilon > 0$, $\exists \delta_1, \delta_2 > 0$, s.t. $\forall x \in B_{\delta_1}(a) \cap S\backslash\{a\} \Rightarrow d(f(x), b) < \epsilon$, and the same thing for δ_2. Let $\delta = \min\{\delta_1, \delta_2\}$, then for $\forall x \in B_\delta(a) \cap S\backslash\{a\}$,

Note 32. There are 3 points deserved mention.

1. 3 conditions of x: 1. $x \in B_\delta(a)$; 2. $x \neq a$; 3. $x \in S$. Collectively, $x \in B_\delta(a) \cap S\backslash\{a\}$.
2. We require $d_X(x,a) > 0$, since $f(a)$ could be totally unconnective with $f(B_\delta(a) \cap S\backslash\{a\})$.
3. If $\exists r > 0$, s.t. $B_r(a) \cap S = \emptyset$, then $\lim_{x\to a} f(x) = b$ (logically) holds for every $b \in Y$. Otherwise $\exists \epsilon > 0, \forall \delta > 0, \exists x \in S, 0 < d_X(x,a) < \delta, \cdots$, but if let $\delta < r$, then any $x \in S$ commits $d(x,a) > r > \delta$, which leads to a contradiction.

we have $d(f(x), b) < \epsilon$ and $d(f(x), b') < \epsilon$ simultaneously , thus $d(b, b') < \epsilon$ for $\forall \epsilon > 0$, thus $b = b'$.

2. for $\forall \epsilon > 0, \exists \delta > 0, \forall x \in B_\delta(a) \cap S \backslash \{a\} \Rightarrow d_2(f(x), b) < \epsilon$ and $d_2(g(x), c) < \epsilon$. Thus

$$\begin{aligned} d_2(f(x) + g(x), b + c) &= [(f(x) + g(x) - b - c)^T (f(x) + g(x) - b - c)]^{1/2} \\ &= [(f(x) - b)^T (f(x) - b) + (g(x) - c)^T (g(x) - c) + 2(f(x) - b)^T (g(x) - c)]^{1/2} \\ &< [2\epsilon^2 + 2(f(x) - b)^T (g(x) - c)]^{1/2}. \end{aligned}$$

Notice that $(f(x) - b)^T (g(x) - c) = (g(x) - c)^T (f(x) - b)$, thus $(f(x) - b)^T (g(x) - c) = [(g(x) - c)^T (f(x) - b)(f(x) - b)^T (g(x) - c)]^{1/2} = \epsilon^2$. and $d_2(f(x) + g(x), b + c) < (4\epsilon^2)^{1/2} = 2\epsilon$, thus $\lim_{x \to a}(f(x) + g(x)) = b + c$. Others are trivial.

□

Exercise 32 (Composite maps)**.** Let X, Y, Z be metric space and $f : S \mapsto T, g : T \mapsto Z$, where $S \subseteq X, T \subseteq Y$. Show that if $\lim_{x \to a} f(x) = b, \lim_{y \to b} g(y) = c$ and $b \notin f(S)$, then $\lim_{x \to a}(g \circ f)(x) = c$. If condition $b \notin f(S)$ is dropped, find an example s.t. $\lim_{x \to a}(g \circ f)(x) \neq c$.

Proof. 1. Since $\lim_{y \to b} g(y) = c$, then for $\forall \epsilon > 0, \exists \delta_y > 0, \forall y \in B_{\delta_y}(b) \cap T \backslash \{b\} \Rightarrow d(c, g(y)) < \epsilon$. And because $\lim_{x \to a} f(x) = b$, then $\exists \delta_x > 0$, for $\forall x \in B_{\delta_x}(a) \cap S \backslash \{a\}$, s.t. $d(b, f(x)) < \delta_y \Rightarrow f(x) \in B_{\delta_y}(b) \cap T$ (Since $f : S \mapsto T$). If $\forall x \in S$ has $f(x) \neq b$, that is $b \notin f(S)$, then $f(x) \in B_{\delta_y}(b) \cap T \backslash \{b\}$, and then $d(g(f(x)), c) < \epsilon$, i.e. $\lim_{x \to a}(g \circ f)(x) \neq c$.

2. Intuitively, If $g(y)$ is un-continuous as $y = b$, and $f(x)$ touches b with an extremely frequence as $x \to a$ then $g \circ f$ would be oscillating as $x \to a$. For example, let $f(x) = \sin(1/x), g(y) = y$ for $y \neq 0$ and 1 for $y = 0$, then $g \circ f(x)$ has no limit as $x \to 0$.

□

Exercise 33 (Example of nonexistence of limit)**.** Let $f : \mathbb{R}^2 \backslash \{(0,0)\} \mapsto \mathbb{R}$ where $f(x, y) = \frac{xy}{x^2 + y^2}$. Show that $\lim_{(x,y) \to (0,0)} f(x, y) \nexists$, using property of composite maps.

Proof. Consider map $g : \mathbb{R} \backslash \{0\} \mapsto \mathbb{R}^2 \backslash \{(0,0)\}$ thus $(0,0) \notin g(\mathbb{R} \backslash \{0\})$. Let $g(t) = (at, bt)$ then $\lim_{(x,y) \to (0,0)} f(x, y) = \lim_{t \to 0} f(g(t)) = \frac{ab}{a^2 + b^2}$ depending on g. Thus if you set different g, that is different parameters a, b then you get different limit of composite maps $f \circ g$ which is equal to the limit of f, thus $\lim f \nexists$. □

Lecture 8. Topology Space, Subspace Topology

CONTENT:

Continuous maps and topology space

Definition 38 (Continuous)**.** Let $(X, d_X), (Y, d_Y)$ be metric spaces. $a \in S \subseteq X, f : S \mapsto Y$, we say map f is continuous at a if for $\forall \epsilon > 0, \exists \delta > 0$, for $\forall x \in B_\delta(a) \cap S$, s.t. $f(x) \in B_\epsilon(f(a))$, that is $f(B_\delta(a)) \subseteq B_\epsilon(f(a))$.

We say f is a continuous map if f is continuous at every $a \in S$.

Exercise 34. Given a map $X \xrightarrow{f} Y, a \in X$, Show that

1. f is continuous at $a \Leftrightarrow$ for $\forall V \subseteq_{open} Y$, where $f(a) \in V$, $\exists U \subseteq_{open} X$, where $a \in U$, such that $f(U) \subseteq V$.
2. f is a continuous map $\Leftrightarrow$ for $\forall V \subseteq_{open} Y, f^{-1}(V) \subseteq_{open} X$.

Proof. 1. $\Rightarrow$: for $\forall V \subseteq_{open} Y$, where $f(a) \in V$, $\exists \epsilon > 0$, s.t. $B_\epsilon(f(a)) \subseteq V$, thus $\exists U = B_\delta(a)$. $\Leftarrow$: trivial.

2. $\Rightarrow$: Given an open set $V \subseteq_{open} Y$, for $\forall x \in f^{-1}(V)$, have $f(x) \in V$. Since V is open, $\exists r > 0$ s.t. $B_r(f(x)) \subseteq V$. Since $f(x)$ is continuous map, $\exists \epsilon > 0$, s.t. $f(B_\epsilon(x)) \subseteq B_r(f(x)) \subseteq V \Rightarrow B_\epsilon(x) \in f^{-1}(V)$, thus $f^{-1}(V)$ is open.

$\Leftarrow$: Given $x \in X, f(x) \in Y$, given $r > 0$, s.t. $B_r(f(x)) \subseteq Y$, then $f^{-1}(B_r(f(x))) \subseteq_{open} X$, and $x \in f^{-1}(B_r(f(x)))$. Thus $\exists \epsilon > 0$, s.t. $B_\epsilon(x) \subseteq f^{-1}(B_r(f(x)))$ and $f(B_\epsilon(x)) \subseteq B_r(f(x))$. □

Note 33. It can also be proved that f is cont. $\Leftrightarrow$ for $\forall V \subseteq_{close} Y, f^{-1}(V) \subseteq_{close} X$.

Suppose $V \subseteq_{close} Y$, then $X \backslash f^{-1}(V) = f^{-1}(X \backslash V) \subseteq_{open} X$, thus $f^{-1}(V) \subseteq_{close} X$.

Exercise 35. Given maps $X \xrightarrow{f} Y, Y \xrightarrow{g} Z$, show that

1. If f is continuous at x_0, g is continuous at $f(x_0)$, then $g \circ f$ is continuous at x_0.
2. If f, g are continuous maps, then $g \circ f$ is a continuous map.

Proof. 1. For any V, s.t. $g(f(x_0)) \in V \subseteq_{open} Z$, $\exists U$, s.t. $f(x_0) \in U \subseteq_{open} Y$, $\exists W$, s.t. $x_0 \in W \subseteq X$, thus $g \circ f$ is continuous at x_0.

2. For any $V \subseteq_{open} Z, \exists U \subseteq_{open} Y, \exists W \subseteq_{open} X$, thus $g \circ f$ is continuous. □

Note 34. Prove this exercise using sets instead of metrics.

We replaced open ball with open set in Exercise 1, this is a meaningful operation, which means we could **substitute the metric with set** (here is open set), which drives the concept of topology. Generally, topology is a family of sets which have the basic properties of open set, but not necessarily be open sets. Using these sets, we can no longer rely on metric d.

Definition 39 (Topology)**.** Given a set X, we say a family of subsets $\mathscr{T} (\subseteq \mathcal{P}(X))$ is a topology on X if

1. $X, \emptyset \in \mathscr{T}$;
2. $U, V \in \mathscr{T} \Rightarrow U \cap V \in \mathscr{T}$;

3. $U_\alpha \in \mathscr{T}(\alpha \in A) \Rightarrow \cup_{\alpha \in A} U_\alpha \in \mathscr{T}$. ($A$ is an arbitrary index set)

Note 35. From here on, we define the **open sets** as elements in a topology, instead of the previous metric-based definition.

Example 23. Given a set X,

1. $\mathscr{T} = \{\emptyset, X\}$ is called trivial topology. In this case, we define only X and $\emptyset$ are open sets.
2. Given a metric space (X, d), the previous definition of open sets is $\mathscr{T}_d = \{U \subseteq \mathcal{P}(X) | \forall x \in U, \exists r > 0, \text{ s.t. } B_r(x) \subseteq U\}$.

Given different metric d, we will obtain different topology. For example, if we use discrete metric, then for $\forall x \in X, \exists r > 0$, such as $r = 0.5$, s.t. $B_r(x) = \{x\} \subseteq \{x\}$, thus $\{x\}$ is an open set. For $\forall U \subseteq X, U = \cup\{x | x \in U\}$, thus any subset of X is an open set. In this case, $\mathscr{T} = \mathcal{P}(X)$, and we call it the discrete topology.

Definition 40 (Topology Space)**.** A topological space $(X, \mathscr{T})$ consists of a set X and a topology $\mathscr{T}$ on X.

Definition 41 (Open set)**.** Let $(X, \mathscr{T})$ be a topological space, any $A \in \mathscr{T}$ is called an open set in X w.r.t. $\mathscr{T}$; and $X \backslash A$ is called a closed set in X w.r.t. $\mathscr{T}$.

Definition 42. Let $(X, \mathscr{T})$ be a top. space and $A \subseteq X, x \in X$.

1. x is an interior point of A in X w.r.t. $\mathscr{T}$, if $\exists U \in \mathscr{T}$, s.t. $x \in U \subseteq A$ (that is $U \cap X \backslash A = U \backslash A = \emptyset$). U is called an open neighborhood of x w.r.t. $\mathscr{T}$.
2. x is an exterior point of A in X w.r.t. $\mathscr{T}$, if $\exists U \in \mathscr{T}$, s.t. $x \in U \subseteq X \backslash A$. (i.e. x is an interior of $X \backslash A$).
3. x is a boundary point of A in X w.r.t. $\mathscr{T}$, if $\forall U \in \mathscr{T}$, if $x \in U$, then $U \cap A \neq \emptyset \wedge U \backslash A \neq \emptyset$.

Note 36. The definition of boundary point is the complementary of interior points union with exterior points.

Definition 43. Let $(X, \mathscr{T})$ be a top. space and $A \subseteq X$. The set consists of all interior points of A in X w.r.t. $\mathscr{T}$ is called interior (of A in X w.r.t. $\mathscr{T}$), denote as $int_X A (= A^\circ)$; the set of all exterior points is called exterior, denoted as $ext_X A (= A^e)$; and the set of all boundary points is called boundary, denoted as $bdy_X A (= \partial A)$.

Note 37. Let $(X, \mathscr{T})$ be a top. space $\forall A \subseteq X$, $X = A^\circ \cup A^e \cup \partial A$, and $A^\circ, A^e, \partial A$ are disjoin.

A° is the exterior of $X \backslash A$, A^e is the interior of $X \backslash A$, and ∂A is the boundary of $X \backslash A$, which means

$$A^\circ = (X \backslash A)^e$$
$$A^e = (X \backslash A)^\circ$$
$$\partial A = \partial (X \backslash A).$$

Example 24. Given a top. space $(\mathbb{R}, \mathscr{T}_d)$, where $d = |x - y|, \forall x, y \in \mathbb{R}$. Let $A = [0, 1)$. Then $A^\circ = (0, 1), A^e = (-\infty, 0) \cup (1, \infty), \partial A = \{0, 1\}$.

Exercise 36. Show that A°, A^e are open sets (on X w.r.t $\mathscr{T}$, that is $A^\circ, A^e \in \mathscr{T}$); ∂A is close set.

Proof. 1. $\forall x \in A^\circ, \exists U_x \in \mathscr{T}$, s.t. $x \in U_x$, thus $A^\circ = \cup_{x \in A^\circ} U_x \in \mathscr{T}$, thus A° is open on X w.r.t. $\mathscr{T}$.

2. A^e is the interior of $X \backslash A$ by definition, thus A^e is open.
3. $A^\circ, A^e \in \mathscr{T} \Rightarrow A^\circ \cup A^e \in \mathscr{T}$, thus $\partial A = X \backslash (A^\circ \cup A^e) \in \mathscr{T}$. □

Exercise 37. Given a topology space $(X, \mathscr{T}), A \subseteq X$, show that

$$A^\circ = \cup\{U|U \subseteq_{open} A\}.$$

Proof. $\subseteq$: for $\forall x \in A^\circ, \exists U \in \mathscr{T}$, s.t. $x \in U \subseteq A \Rightarrow x \in \cup\{U|U \subseteq_{open} A\}$; $\supseteq$: for $\forall x \in \cup\{U|U \subseteq_{open} A\}, \exists U_x \subseteq_{open} A$, s.t. $x \in U_x$, thus x is an interior point, and $x \in A^\circ$. □

Note 38. A° is the largest open set in X contained in A. Thus,

$$A = A^\circ \Leftrightarrow A \subseteq_{open} X \Leftrightarrow \partial A \cap A = \emptyset$$

for $\partial A \cap A = \partial A \cap A^\circ = \emptyset$. And furthermore $(A^\circ)^\circ = A^\circ$.

Definition 44 (Closure)**.** Given a topology space $(X, \mathscr{T}), A \subseteq X$, the set

$$\overline{A} = cls_X A := \cap\{C|A \subseteq C \subseteq_{close} X\}$$

is called the closure of A in X w.r.t. $\mathscr{T}$.

Note 39. $\overline{A}$ is the smallest close set in X containing in A. Thus,

$$A = \overline{A} \Leftrightarrow A \subseteq_{close} X \Leftrightarrow \partial A \subseteq A$$

for $\partial A \subseteq A^\circ \cup \partial A = \overline{A} = A$. And furthermore $\overline{\overline{A}} = \overline{A}$.

Exercise 38. Given a topology space $(X, \mathscr{T}), A \subseteq X$, show that $\overline{A} = A^\circ \cup \partial A$.

Proof.

$$\begin{aligned} A^\circ \cup \partial A &= X \backslash A^e \\ &= X \backslash (X \backslash A)^\circ \\ &= X \backslash \cup \{U|U \subseteq_{open} X \backslash A\} \\ &= \cap\{X \backslash U|U \subseteq_{open} X \backslash A\} \\ &= \cap\{C|A \subseteq C \subseteq_{close} X\} \\ &= \overline{A}. \end{aligned}$$

□

Note 40.

$$\begin{aligned} &U \subseteq X \backslash A \\ &\Rightarrow \forall x \in U \Rightarrow x \in X \backslash A \\ &\Rightarrow \forall x \notin X \backslash A \Rightarrow x \notin U \\ &\Rightarrow \forall x \in A \Rightarrow x \in X \backslash U \\ &\Rightarrow A \subseteq X \backslash U, \end{aligned}$$

U is open $\Rightarrow$ $X \backslash U$ is close, hence $C = X \backslash U \subseteq_{close} A$.

Exercise 39. Show that $X \backslash \overline{A} = (X \backslash A)^\circ$ and $X \backslash A^\circ = \overline{(X \backslash A)}$.

Proof. 1.

$$\begin{aligned} \overline{A} &= A^\circ \cup \partial A \\ &= X \backslash A^e \\ &= X \backslash (X \backslash A)^\circ \\ X \backslash \overline{A} &= (X \backslash A)^\circ. \end{aligned}$$

2.

$$\begin{aligned} X \backslash A^\circ &= A^e \cup \partial A \\ &= (X \backslash A)^c \cup \partial (X \backslash A) \\ &= \overline{(X \backslash A)}. \end{aligned}$$

□

Note 41. We denote $X \backslash A$ as A^c if X is clearly given. Thus

$$\begin{aligned} (\overline{A})^c &= (A^c)^\circ \\ (A^\circ)^c &= \overline{A^c} \end{aligned}$$

Exercise 40. If $A \subseteq B$, show that $A^\circ \subseteq B^\circ$, $\overline{A} \subseteq \overline{B}$.

Proof. 1. Given $x \in A^\circ = \cup\{U|U \subseteq_{open} A\}, \exists U_x \subseteq_{open} A$, s.t. $x \in U_x \subseteq_{open} A \subseteq B$, thus $x \in \cup\{V|V \subseteq_{open} B\}$, and $x \in B^\circ$. 2. the same way with 1. □

Exercise 41. Given a set U, (denote $\overline{U}$ as U^-,) show that $U \subseteq_{open} X \Rightarrow U^- = U^{-c-c-}$.

Proof.

$$\begin{aligned} U^{-c-c-} &= (U^-)^{c-c-} \\ &= (U^-)^{\circ cc-} \\ &= U^{-\circ-} \end{aligned}$$

$U \subseteq U^- \Rightarrow U = U^\circ \subseteq U^{-\circ} \Rightarrow U^- \subseteq U^{-\circ-}$. Let $C = U^- \subseteq_{close} X$, thus $C^\circ \subseteq C \Rightarrow C^{\circ-} \subseteq C^- = C \Rightarrow U^{-\circ-} \subseteq U^-$, thus $U^- = U^{-\circ-} = U^{-c-c-}$. □

Exercise 42 (Kuratowski's 14 sets)**.** Given a top. sp. X, $A \subseteq X$, Show that among

$$\begin{aligned} &A, A^-, A^{-c}, A^{-c-}, A^{-c-c} \cdots \\ &A^c, A^{c-}, A^{c-c}, A^{c-c-} \cdots \end{aligned}$$

there are at most 14 different subsets of A.

Proof. On the one hand,

$$A, A^-, \underbrace{A^{-c}}_{open}, A^{-c-}, A^{-c-c}, A^{-c-c-}, A^{-c-c-c}, \underbrace{A^{-c-c-c-}}_{=(A^{-c})^{-c-c-}}, \cdots$$

On the other hand,

$$A^c, A^{c-}, \underbrace{A^{c-c}}_{open}, A^{c-c-}, A^{c-c-c}, A^{c-c-c-}, \underbrace{A^{c-c-c-c-}}_{=(A^{c-c})^{-c-c-}}, \cdots$$

thus there are at most 14 different subsets of A. □

Definition 45 (Continuous Map)**.** Let X, Y be top. spaces. A map $X \xrightarrow{f} Y$ is continuous at a point $x_0 \in X$ if $\forall$ open neighborhood (nbd.) V of $f(x_0)$, $\exists$ open nbd. U of x_0, s.t. $f(U) \subseteq V$. f is a continuous map, if f is continuous at every $x_0 \in X$.

Note 42. We have discussed that f is conti. $\Leftrightarrow$ for $\forall V \subseteq_{open} Y, f^{-1}(V) \subseteq_{open} X \Leftrightarrow$ for $\forall V \subseteq_{close} Y, f^{-1}(V) \subseteq_{close} X$.

Exercise 43. Let X, Y be top. spaces, $X \xrightarrow{f} Y$ is a conti. map, show that $\overline{f^{-1}(B)} \subseteq f^{-1}(\overline{B})$, and $f(\overline{A}) \subseteq \overline{f(A)}$.

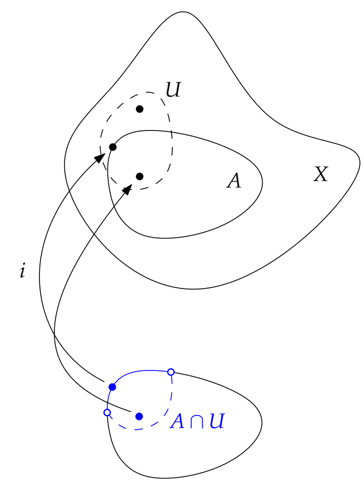
Proof. 1. $B \subseteq \overline{B} \Rightarrow f^{-1}(B) \subseteq f^{-1}(\overline{B})$ where $f^{-1}(\overline{B})$ is close, thus $\overline{f^{-1}(B)} \subseteq \overline{f^{-1}(\overline{B})} = f^{-1}(\overline{B})$.

2. $f(A) \subseteq \overline{f(A)} \Rightarrow A \subseteq f^{-1}(\overline{f(A)})$ where $f^{-1}(\overline{f(A)})$ is close, thus $\overline{A} \subseteq \overline{f^{-1}(\overline{f(A)})} = f^{-1}(\overline{f(A)}) \Rightarrow f(\overline{A}) \subseteq \overline{f(A)}$. □

Note 43. $f(A) \subseteq B \Rightarrow A \subseteq f^{-1}(B)$ by the definition of pre-image.

Subspace Topology

Let X be a top. space and $A \subseteq X$. A top. space is a set which has been specified some subsets are open but the others are not. Not consider how to transform a subset A into a top. space in a reasonable way. And the issue is that what kind of subsets of A should be defined as open.



Consider the inclusion map $A \xrightarrow{i} X$ where $a \mapsto a$. Thus an intuitive motivation is we need select open sets in the top. space of A such that keep i is continuous. Because, for any point a in the codomain of i, if $\exists$ an open set $U \in X$, such that covers a, then it covers the pre-image of a (in the top. space of X), since $i^{-1}(a) = a \in U$. So if any point $a \in X$ has an open nbd. U then it's pre-image should have an open nbd. U_A, otherwise the subspace top. would be too simple or wried to show the inheritance of the "sub".

Thus we wish create a corresponding open set U_A of U in the top. space of A, thus for any point in the codomain, if it has open nbd. in the top. space of X, then it's pre-image has open nbd. in the top. space of A, and i is continuous. Specially, if we define $\mathscr{T}_A = \mathcal{P}(A)$, that is discrete topology, then any point forms an open set, thus i is continuous. But we want to find the concisest situation that fits the demand. The concisest way to construct topology of A is selecting the pre-image of the open sets in X, that is for any $U \in \mathscr{T}_X$, $i^{-1}(U) = U \cap A \in \mathscr{T}_A$.

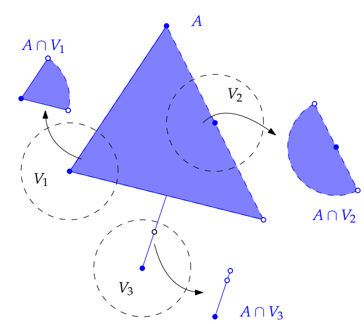
1. $\emptyset \in \mathscr{T}_X \Rightarrow \emptyset \cap A = \emptyset \in \mathscr{T}_A$, $X \in \mathscr{T}_X, \Rightarrow X \cap A = A \in \mathscr{T}_A$.

2. $\forall U_1, U_2 \in X, U_1 \cap U_2 \in X$, thus $(U_1 \cap A) \cap (U_2 \cap A) = (U_1 \cap U_2) \cap A \in \mathscr{T}_A$.

3. $\forall U_\alpha \in X(\alpha \in I), \cup_{\alpha \in I} \in X$, thus $\cup_{\alpha \in I}(U\alpha \cap A) = A \cap (\cup_{\alpha \in I} U_\alpha) \in A$.

thus $\{U \cap A | \forall U \subseteq_{open} X\}$ is a topology which is the smallest topology that satisfies our demand.

Definition 46. The subspace topology on A inherited from X is $\mathscr{T}_A = \{U \cap A | U \subseteq_{open} X\}$.



Example 25. Given a top. space $(\mathbb{R}^2, \mathscr{T}_d)$ where $d = d_2$, a subset A of X like the margin figure. we can see that the elements of $\mathscr{T}_A$: $A \cap V_1$, $A \cap V_2$ and $A \cap V_3$ are all open sets on $(A, \mathscr{T}_A)$, even thought they are not open sets on $(\mathbb{R}^2, \mathscr{T}_d)$.

Exercise 44. Given a map $X \xrightarrow{f} Y$, X, Y are top. spaces. Suppose $\exists B \subseteq Y$ is a subspace top. inherited from Y. If $f(X) \subseteq B$, we denote the map $X \xrightarrow{f} B$ by $f|^B$. Show that f is continuous $\Leftrightarrow f|^B$ is continuous.

Proof. $\Rightarrow$: f is conti. then $\forall V \subseteq_{open} Y$ has $f^{-1}(V) \subseteq_{open} X$, and $V \cap B \subseteq_{open} B$. Since:

$$\begin{aligned} f^{-1}(V \cap B) &= f^{-1}(V) \cap f^{-1}(B) \\ &= f^{-1}(V) \cap X \\ &= f^{-1}(V) \subseteq_{open} X \end{aligned}$$

thus $f|^B$ is conti.

$\Leftarrow$: $\forall V \subseteq_{open} Y, f^{-1}(V \cap B) = f^{-1}(V) \cap f^{-1}(B) = f^{-1}(V) \cap X = f^{-1}(V) \subseteq_{open} X$. Thus f is conti. $\square$

Lecture 9. Product Topology, Quotient Topology

CONTENT:

Product Topology

Definition 47 (Homeomorphism)**.** A map $X \xrightarrow{f} Y$ between top. sp. is a homeomorphism if f is a bijection, and f and f^{-1} (inverse of f) are continuous.

We say two top. sp. X and Y are homeorphic if $\exists$ homeomorphism from X onto Y.

Given sets, we can create new sets from them, thus given topologies we also want to create new topologies from them. We just defined the subspace topology, now we want to create new topology on the cartesian product of the sets.

Let X, Y be top. sp., maps $X \times Y \xrightarrow{p_1} X((x,y) \mapsto x)$ and $X \times Y \xrightarrow{p_2} Y((x,y) \mapsto y)$ are called the natural projections. A natural intuition is these two natural projections need be continuous.

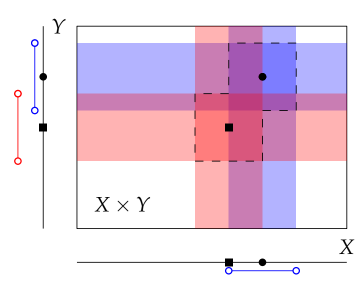
If $\mathscr{T}$ is a topology on $X \times Y$ such that $X \times Y \xrightarrow{p_1} X((x,y) \mapsto x)$ and $X \times Y \xrightarrow{p_2} Y((x,y) \mapsto y)$ both are continuous, then for $\forall U \subseteq_{open} X, V \subseteq_{open} Y$,

$$p_1^{-1}(U) = U \times Y = \subseteq_{open} X \times Y$$

and

$$p_2^{-1}(V) = X \times V = \subseteq_{open} X \times Y$$

thus $(U \times Y) \cap (X \times V) = U \times V \subseteq_{open} X \times Y$. Unfortunately, $\{U \times VU \subseteq_{open} X, V \subseteq_{open} Y\}$ is not a topology, because the union of $U_\alpha \times V_\beta$ are not necessarily covered by $\{U \times V | U \subseteq_{open} X, V \subseteq_{open} Y\}$. (like the margin figure)



Thus for $U_\alpha \subseteq_{open} X(\alpha \in A), V_\beta \subseteq_{open} Y(\beta \in B)$, then it need be true that $U_\alpha \times V_\beta \subseteq_{open} X \times Y((\alpha \times \beta) \in A \times B)$ and $\cup_{(\alpha,\beta) \in A \times B}(U_\alpha \times V_\beta) \subseteq_{open} X \times Y$.

Proposition 11. *A, B are index sets,*

$$\mathscr{T}_{X\times Y} := \left\{ \bigcup_{(\alpha,\beta)\in A\times B} (U_\alpha \times V_\beta) | U_\alpha \subseteq_{open} X, V_\beta \subseteq_{open} Y \right\}$$

is a topology on $X \times Y$.

Proof. The union of two elements of $\mathscr{T}_{X\times Y}$ is in $\mathscr{T}_{X\times Y}$ is trivial, the only thing we need confirm is the intersection of two elements of $\mathscr{T}_{X\times Y}$ is in $\mathscr{T}_{X\times Y}$. Suppose C, D are index sets, and $U_\alpha, S_\delta \subseteq_{open} X$, $V_\beta, T_\gamma \subseteq_{open} Y$, then

$$\begin{aligned} &\left(\bigcup_{(\alpha,\beta)\in A\times B} (U_\alpha \times V_\beta) \right) \bigcap \left(\bigcup_{(\delta,\gamma)\in C\times D} (S_\delta \times T_\gamma) \right) \\ &= \bigcup_{(\delta,\gamma)} \left[(S_\delta \times T_\gamma) \bigcap \left(\bigcup_{(\alpha,\beta)} (U_\alpha \times V_\beta) \right) \right] \\ &= \bigcup_{(\delta,\gamma)} \left[\bigcup_{(\alpha,\beta)} (U_\alpha \times V_\beta) \bigcap (S_\delta \times T_\delta) \right] \\ &= \bigcup_{(\delta,\gamma)} \left[\bigcup_{(\alpha,\beta)} (U_\alpha \cap S_\delta) \times (V_\beta \cap T_\gamma) \right] \end{aligned}$$

$U_\alpha, S_\delta \subseteq_{open} X \Rightarrow U_\alpha \cap S_\delta \subseteq_{open} X$, and $V_\beta \cap T_\gamma \subseteq_{open} Y$ in the same way $\Rightarrow \cup_{(\alpha,\beta)}(U_\alpha \cap S_\delta) \times (V_\beta \cap T_\gamma) \in \mathscr{T}_{X\times Y} \Rightarrow$ $\cup_{(\delta,\gamma)} \left[\cup_{(\alpha,\beta)} (U_\alpha \cap S_\delta) \times (V_\beta \cap T_\gamma) \right] \in \mathscr{T}_{X\times Y}$. □

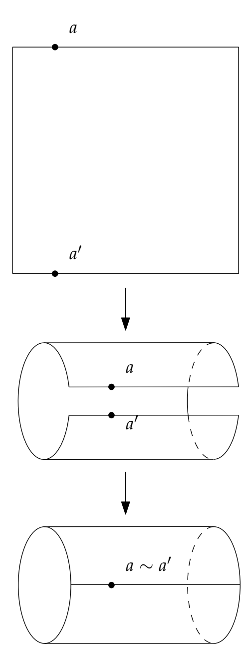
Note 44. Thus $\mathscr{T}_{X\times Y}$ is the smallest topology on $X \times Y$ that holds projections p_1, p_2 continuous.

Definition 48 (Product Topology)**.** *X, Y are top. sp. the topology $\mathscr{T}_{X\times Y}$ is called the Product Topology on $X \times Y$.*

Quotient Topology

We now introduce a new method to create top. which is on the set where some points are viewed as same. For example, when we fold a piece of paper into a column, the corresponding points on the top and bottom edges of the paper are regarded as the same point. If we have already defined a topology on the paper, now we want to define a topology on the column.

If X is a top. sp., and R is a equivalent relation on X. Recall that X is the disjoin union of the element in quotient set X/R (whose elements are distinct equivalent class $R(x)$), we can regard the points in the identical equivalent class as the same. And we want to define topology on the quotient set X/R which is associated with the top. on X.



Thus a fairly intuitive association between X and X/R is the natural projection $X \xrightarrow{\pi} X/R(x \mapsto R(x))$, so we need define a topology $\mathscr{T}$ on X/R such that π is continuous. This is different with the subspace top. and product top. where the undetermined top. is the domain, whereas in this case (quotient top.) the undetermined top. is the codomain. Thus in the previous cases, we need to find the smallest top. which satisfies conditions, in this case, we need to find the largest one.

Clearly, if the top. $\mathscr{T}$ on X/R makes π be continuous, then $\mathscr{T} \subseteq \{S \subseteq X | \pi^{-1}(S) \subseteq_{open} X\}$. Thus if $\{S \subseteq X | \pi^{-1}(S) \subseteq_{open} X\}$ is a top. then it is the largest one what we are looking for.

Note 45. Define a bijection $X \xrightarrow{id_X} X(x \mapsto x)$, If we want to define topology on X such that id_X is not continuous, we can define a large top. for codomain X, like discrete top.; and define a small top. for domain X, like trivial top. Then, if $X \neq \emptyset$, f is not continuous.

Exercise 45. Suppose X is a top. sp. Y is a set, $X \xrightarrow{f} Y$ is a map. Show that $\mathscr{S} := \{S \subseteq Y | f^{-1}(S) \subseteq_{open} X\}$ is a topology on Y.

Proof. 1. $f^{-1}(\emptyset) = \emptyset \subseteq_{open} X$ thus $\emptyset \in \mathscr{S}$; $f^{-1}(Y) = X \subseteq_{open} X$, thus $Y \in \mathscr{S}$.

2. For any $S_1, S_2 \in \mathscr{S}$, $f^{-1}(S_1 \cap S_2) = f^{-1}(S_1) \cap f^{-1}(S_2) \subseteq_{open} X$, thus $S_1 \cap S_2 \in \mathscr{S}$.

3. For any $S_\alpha(\alpha \in A) \in \mathscr{S}$, $f^{-1}(\cup_{\alpha \in A} S_\alpha) = \cup_{\alpha \in A} f^{-1}(S_\alpha) \subseteq_{open} X$, thus $\cup_{\alpha \in A} S_\alpha \in \mathscr{S}$. □

Note 46. Actually, $\mathscr{S}$ is the largest top. on Y such that f is continuous.

Thus $\{S \subseteq X | \pi^{-1}(S) \subseteq_{open} X\}$ is the largest topology on X/R.

Definition 49 (Quotient Topology)**.** Suppose X is a top. sp., and R is a equivalent relation on X. $\{S \subseteq X | \pi^{-1}(S) \subseteq_{open} X\}$ is called the quotient topology on X/R.

Example 26. Let $X = [0,1] \times [0,1]$ is a subspace topology inherited from $\mathbb{R}^2$. We now fold X up and down to form a column, this operation can be view as defining an equivalent class R on X:

$$R(x,y) = \begin{cases} \{(x,y)\}, & 0 \leq x \leq 1, 0 < y < 1, \\ \{(x,0),(x,1)\}, & 0 \leq x \leq 1. \end{cases}$$

And the topology on the column is $\{S \subseteq X | \pi^{-1}(X) \subseteq_{open} X\}$.

Lecture 10. Compactness on Topology Space

CONTENT:

Compactness

Definition 50 (Compact)**.** Let X be a top. sp. we say that X is compact if $\forall U_\alpha \subseteq_{open} X(\alpha \in A), X = \cup_{\alpha \in A} U_\alpha \Rightarrow \exists \alpha_1, \cdots, \alpha_k \in A,$ s.t. $X = U_{\alpha_1} \cup \cdots \cup U_{\alpha_k}$.

Definition 51 (Compact Subset)**.** Let X be a top. sp. $K \subseteq X$, we say K is a compact subset in X, if $\forall U_\alpha \subseteq_{open} X(\alpha \in A), K \subseteq \cup_{\alpha \in A} U_\alpha \Rightarrow \exists \alpha_1, \cdots, \alpha_k \in A,$ s.t. $K \subseteq U_{\alpha_1} \cup \cdots \cup U_{\alpha_k}$.

Exercise 46. Show that K is a compact subset in $X \Leftrightarrow K$ (equipped with the subspace topology) is a compact space.

Proof. $\Rightarrow$: For any $V_\alpha \subseteq_{open} K, \exists U_\alpha \subseteq_{open} X,$ s.t. $V_\alpha = U_\alpha \cap K$. For any

$$\begin{aligned} K &= \cup_{\alpha \in A} V_\alpha \\ &= \cup_{\alpha \in A} U_\alpha \cap K \\ &= K \cap \cup_{\alpha \in A} U_\alpha \\ &= K \cap (U_{\alpha_1} \cup \cdots U_{\alpha_k}) \\ &= V_{\alpha_1} \cup \cdots V_{\alpha_k} \end{aligned}$$

Thus K is compact. $\Leftarrow$: for any $K \subseteq \cup_{\alpha \in A} U_\alpha$, we have $\cup_{\alpha \in A}(U_\alpha \cap K) \subseteq K$ and

$$\begin{aligned} K &= K \cap K \\ &\subseteq K \cap \cup_{\alpha \in A} U_\alpha \\ &= \cup_{\alpha \in A}(K \cap U_\alpha) \end{aligned}$$

Thus $K = \cup_{\alpha \in A}(K \cap U_\alpha) = \cup_{\alpha \in A} V_\alpha$, where $V_\alpha \subseteq_{open} K$. And $\exists V_{\alpha_1}, \cdots, V_{\alpha_k} \subseteq_{open} K,$ s.t.

$$\begin{aligned} K &= V_{\alpha_1} \cup \cdots V_{\alpha_k} \\ &= K \cap (U_{\alpha_1} \cup \cdots U_{\alpha_k}) \\ &\subseteq U_{\alpha_1} \cup \cdots U_{\alpha_k} \end{aligned}$$

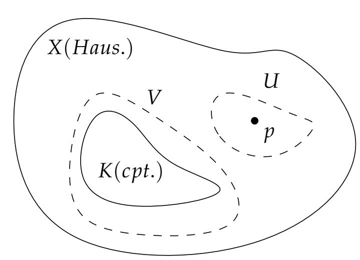
Thus K is a compact subset in X. □

Definition 52 (Hausdorff Topology Space)**.** A top. sp. X is Hausdorff if $\forall p, q \in X, p \neq q \Rightarrow \exists$ open nbds U of p and V of q in X such that $U \cap V = \emptyset$.

Example 27. Let $X = \{1, 2\}$, $\mathscr{T}$ is trivial topology, then $(X, \mathscr{T})$ is not a Hausdorff topology space.

Note 47. Thus the larger top. is, the more likely it is to be Hausdorff.

Proposition 12. *Suppose X is Hausdorff, $K(\subseteq X)$ is compact, $p \in X \backslash K \Rightarrow \exists U, V \subseteq_{open} X,$ s.t. $K \subseteq V, p \in U$, and $U \cap V = \emptyset$.*



Proof. X is Hausdorff $\Rightarrow \forall q \in K, \exists U_q, V_q \subseteq_{open} X$ s.t. $q \in V_q, p \in U_q, U_q \cap V_q = \emptyset$. Thus $K \subseteq \cup_{q \in K} V_q = \cup_{i=1}^k V_{q_i}$, Let $V = \cup_{i=1}^k V_{q_i}, U = \cap_{i=1}^k U_{q_i}$, then

$$\begin{aligned} U \cap V &= \left(\cap_{j=1}^k U_{q_j}\right) \cap \left(\cup_{i=1}^k V_{q_i}\right) \\ &= \cup_{i=1}^k \left[\cap_{j=1}^k \left(U_{q_j} \cap V_{q_i}\right)\right] \\ &= \cup_{i=1}^k \emptyset = \emptyset. \end{aligned}$$

□

Corollary 1. *Suppose X is Hausdorff, $K \subseteq_{cpt.} X$ is compact $\Rightarrow K$ is closed.*

Proof. For $\forall p \in X \backslash K, \exists W_p \subseteq_{open} X,$ s.t. $x \in W_p$ and $W_p \cap K = \emptyset$, that is $W_p \subseteq X \backslash K$. And because

$$X \backslash K = \cup_{p \in X \backslash K} \{p\} \subseteq \cup_{p \in X \backslash K} W_p \subseteq X \backslash K$$

we have that $X \backslash K = \cup_{p \in X \backslash K} W_p \subseteq_{open} X$, and then $K \subseteq_{close} X$. □

Exercise 47. Suppose X is locally compact Hausdorff, $K \subseteq_{cpt.} X$, $C \subseteq_{close} X$, show that if $C \cap K = \emptyset \Rightarrow \exists U, V \subseteq_{open} X,$ s.t. $K \subseteq V, C \subseteq U$ and $U \cap V = \emptyset$.

Proposition 13. *Suppose X is a compact space, $K \subseteq_{close} X \Rightarrow K \subseteq_{cpt.} X$.*

Note 48. If X is Haus. $K \subseteq_{cpt.} X$ is close; If X is cpt. $K \subseteq_{close} X$ is cpt.

Proof. Suppose that $U_\alpha \subseteq_{open} X(\alpha \in A)$ cover K, i.e. $K \subseteq \cup_{\alpha \in A} U_\alpha$. Then

$$\begin{aligned} X = K \cup (X \backslash K) \subseteq \\ (\cup_{\alpha \in A} U_\alpha) \cup (X \backslash K) \\ = \left[\cup_{i=1}^k U_{\alpha_i}\right] \cup (X \backslash K) \\ = \cup_{i=1}^k \left[U_{\alpha_i} \cup (X \backslash K)\right] \end{aligned}$$

Note 49. So the standard routines for proving a set K is cpt. is suppose $U_\alpha(\alpha \in A)$ cover it at first, and then try to argue $K \subseteq \cup_{i=1}^k U_{\alpha_i}$.

and

$$\begin{aligned} K = K \cap X = K \cap \left[\cup_{i=1}^k U_{\alpha_i} \cup (X \backslash K)\right] \\ = \cup_{i=1}^k \left[K \cap ((X \backslash K) \cup U_{\alpha_i})\right] \\ = \cup_{i=1}^k \left[(K \cap (X \backslash K)) \cup (K \cap U_{\alpha_i})\right] \\ = \cup_{i=1}^k (K \cap U_{\alpha_i}) \\ \subseteq \cup_{i=1}^k U_{\alpha_i}. \end{aligned}$$

Thus K is compact.

□

Exercise 48. X is locally compact Hausdorff (LCH) space, $C \subseteq_{close} X$, show that $\forall c \in C, \exists T_c \subseteq_{cpt.} C,$ s.t. $c \in T_c$.

Proof. For $\forall c \in C, \exists S_c \subseteq_{cpt.} X,$ s.t. $c \in S_c$ and $c \in S_c \cap C$. Since $S_c \subseteq_{cpt.} X \Rightarrow S_c \subseteq_{close} X \Rightarrow S_c \cap C \subseteq_{close} X$

$$\begin{aligned} X \backslash (S_c \cap C) \subseteq_{open} X \\ \Rightarrow S_c \cap (X \backslash (S_c \cap C)) \subseteq_{open} S_c \\ \Rightarrow S_c \backslash [S_c \cap (X \backslash (S_c \cap C))] \subseteq_{close} S_c \\ \Rightarrow (S_c \backslash S_c) \cup [S_c \backslash X \backslash (S_c \cap C)] \subseteq_{close} S_c \\ \Rightarrow S_c \backslash X \backslash (S_c \cap C) \\ = S_c \cap C \subseteq_{close} S_c. \end{aligned}$$

Note 50. $A \subseteq_{close} X$, $A \subseteq B \subseteq X$, then $A \subseteq_{close} B$.

Since $S_c \cap C \subseteq_{close} S_c, S_c$ is cpt. $\Rightarrow S_c \cap C \subseteq_{cpt.} S_c \Rightarrow S_c \cap C$ is cpt. $\Rightarrow S_c \cap C \subseteq_{cpt.} C$. □

Proposition 14. *X, Y are cpt. space $\Rightarrow$ $X \times Y$ (equipped with the product topology) is compact.*

Note 51. Remember that $A \subseteq_{cpt.} B$ means A is a cpt. subset of B, which is equivalent with A is a cpt. set.

Proof. Trivial. Fix x, consider $\{x\} \times Y$. then utilize the definition of product topology, and then use the compactness of Y.Thus $\{x\} \times Y$ could be covered by finite open set. For detailed argument, see here(0:52:00). □

Proposition 15 (continuous maps preserve compactness)**.** *Suppose X, Y are top. sp. $X \xrightarrow{f} Y$ is continuous. $K \subseteq_{cpt.} X \Rightarrow f(K) \subseteq_{cpt.} Y$.*

Proof. Suppose $V_\alpha(\alpha \in A)$ cover $f(K)$, that is $f(K) \subseteq \cup_{\alpha \in A} U_\alpha$, thus

$$
\begin{aligned}
K &\subseteq f^{-1}(\cup_{\alpha \in A} U_\alpha) \\
&= \cup_{\alpha \in A} f^{-1}(U_\alpha) \\
&= \cup_{i=1}^{k} f^{-1}(U_{\alpha_i}) \\
&= f^{-1}(\cup_{i=1}^{k} U_{\alpha_i}).
\end{aligned}
$$

Note 52. Since f is continuous, $f^{-1}(U_\alpha)(\alpha \in A)$ are open.

Thus $f(K) \subseteq \cup_{i=1}^{k} U_{\alpha_i}$ and it is compact. □

Corollary 2. *Suppose map $X \xrightarrow{f} Y$ is conti. X is compact, Y is Hausdorff, then f is a closed map, i.e. $C \subseteq_{close} X \Rightarrow f(C) \subseteq_{close} Y$.*

Proof. $C \subseteq_{close} X$, X is compact $\Rightarrow$ $C \subseteq_{cpt.} X \Rightarrow f(C) \subseteq_{cpt.} Y$, Y is Hausdorff $\Rightarrow f(C)$ is close. □

Corollary 3. *Suppose map $X \xrightarrow{f} Y$ is conti. bijection, X is compact, Y is Hausdorff $\Rightarrow$ f is a homeomorphism.*

Proof. f is closed map, and f is a bijection, thus f^{-1} is continuous. f is bijection, f and f^{-1} are continuous, thus f is a homeomorphism. □

Bound

Definition 53 (Upper Bound)**.** Given $A \subseteq \mathbb{R}$, we call $u \in \mathbb{R}$ is a upper bound of A if $a \leq u$ for $\forall a \in A$; $l \in \mathbb{R}$ is a lower bound of A if $l \leq a$ for $\forall a \in A$.

Definition 54 (Greatest Element)**.** $x \in \mathbb{R}$ is the greatest (smallest) element of A if $x \in A$ and x is a upper (lower) bound of A.

Definition 55 (Least Upper Bound)**.** $u \in \mathbb{R}$ is the least upper bound (or supremum) of A, if u is the smallest element of the set of all upper bounds of A, denote as $u = \sup A$.

$l \in \mathbb{R}$ is the greatest lower bound (or infimum) of A, if l is the greatest element of the set of all lower bounds of A, denote as $l = \inf A$.

Example 28. Let $A = [0,1)$, the set of upper bound of A is $[1,\infty)$, the set of lower bound of A is $(-\infty, 0]$. Thus $\sup A = 1, \inf A = 0$.

Suppose we admit that the gapless property of real number: if $\emptyset \neq S \subseteq \mathbb{R}$ has upper bound (lower bound), then $\sup S (\inf S) \exists$.

Theorem 7. $[0,1]$ *(as a subspace of* $\mathbb{R}$*) is compact.*

Proof. Suppose that $V_\alpha \subseteq_{open} \mathbb{R} (\alpha \in A)$ cover $[0,1]$. Consider

$$S := \{s \in [0,1] | [0,s] \text{ can be covered by finitely many } V_\alpha\}$$

Thus $0 \in S$, $S \neq \emptyset$. $S \subseteq [0,1]$, thus S has an upper bound $\Rightarrow \sup S \exists$. Let $s_0 := \sup S$. Since 1 is an upper bound of S, $s_0 \leq 1$. For $\forall t \leq s_0$, t is not an upper bound of S, $\exists s' \in S$, s.t. $t < s'$, thus $[0,t]$ could be covered by finitely many V_α.

Since $s_0 \leq 1$, $\exists \alpha_0$, s.t. $s_0 \subseteq V_{\alpha_0}$, $\exists r > 0$, s.t. $B_r(s_0) \subseteq V_{\alpha_0}$. Thus $[0, s_0 - r]$ can be covered by finitely many of V_α, and $(s_0 - r, s_0 + r)$ can be covered by V_{α_0}. Thus $[0, s_0 + r)$ can be covered by finitely many V_α. Thus $s_0 = 1$ and $s_0 \in S \Rightarrow S = [0,1]$. □

Thus $[0,1] \times [0,1]$, as a subspace of $\mathbb{R}^2$, which coincides with the product space of $[0,1]$ and $[0,1]$, is compact.

More generally, we can reprove the **Heine–Borel theorem**: for $K \subseteq \mathbb{R}^n$, then $K \subseteq_{cpt.} \mathbb{R}^n \Leftrightarrow K \subseteq_{close} \mathbb{R}^n$ and K is bdd.

Proof. $\Rightarrow$: $\mathbb{R}^n$ is metric space $\Rightarrow$ $\mathbb{R}^n$ is Hausdorff $\Rightarrow$ $K \subseteq_{close} \mathbb{R}^n$. Since $K \subseteq \cup_{n \in \mathbb{N}} B_n(0) \Rightarrow \exists r_1, \cdots, r_k$, s.t. $K \subseteq \cup_{i=1}^k B_{n_{r_i}}(0) \Rightarrow K$ is bdd.

$\Leftarrow$: K is bdd. $\Rightarrow, \exists r > 0$, s.t. $K \subseteq B_r(0), \Rightarrow \exists [a_1, b_1], \cdots, [a_n, b_n] \in \mathbb{R}$, s.t. $K \subseteq B_r(0) \subseteq \times_{i=1}^n [a_i, b_i]$. Since $K \subseteq_{close} \mathbb{R}^n \Rightarrow K \subseteq_{close} \times_{i=1}^n [a_i, b_i] \subseteq_{cpt.} \mathbb{R}^n \Rightarrow K \subseteq_{cpt.} \times_{i=1}^n [a_i, b_i] \Rightarrow K$ is cpt. □

Note 53. Actually, In any metric space X, $K \subseteq_{cpt.} X \Rightarrow K \subseteq_{close} X$ and be bdd.

Exercise 49. Suppose $S \subseteq_{close} \mathbb{R}$ and $S \neq \emptyset$, S has an upper bound, show that $\sup S \in S$.

Proof. Let $s_0 := \sup S$. If $s_0 \notin S \Rightarrow s_0 \in \mathbb{R} \backslash S \subseteq_{open} \mathbb{R}$. Thus $\exists r > 0$, s.t. $B_r(s_0) \in \mathbb{R} \backslash S$, that is $s_0 - r \in \mathbb{R} \backslash S \Rightarrow s_0 - r \geq s (\forall s \in S)$. But s_0 is the smallest upper bound, then $\forall s' < s_0, \exists s \in S$, s.t. $s > s'$, which leads to a contradiction. □

Corollary 4. *Given a conti. map* $K \xrightarrow{f} \mathbb{R}$, *K is cpt.* $\Rightarrow$ *f has a max. and min.*

Proof. K is cpt., f is conti. $\Rightarrow f(K) \subseteq_{cpt.} \mathbb{R} \Rightarrow f(K) \subseteq_{close} \mathbb{R}$ and be bdd. Thus $f(K)$ has a upper bound and lower bound, thus $\max f(K) = \sup f(K) \in f(K)$ and $\min f(K) = \inf f(K) \in f(K)$. □

Lecture 11. Homomorphism, Isomorphism and Homotopy.

CONTENT:

Abelian Group

Definition 56 (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 54. Sometimes, we will denote $S \xrightarrow{f} \mathbb{Z}$ by $(x_s)_{s \in S}$.

Example 29. 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 57 (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 55. 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 30. 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 58 (Isomorphism)**.** We say a homomorphism T is an isomorphism if T is a bijection.

Definition 59. 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 50. Show that $ker(T)$ is a subgroup of $(G, \Box)$, $im(T)$ is a subgroup of $(G', \Box')$.

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

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

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

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

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

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

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

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

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

thus $g_1' \Box' g_2' \in im(T)$.
(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

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

and $T(g^{-1}) \Box' g' = e'$ 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 51. $G \xrightarrow{T} G'$ 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 60. 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 56. 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 $a'\square b'\square H \neq a\square b\square H$.

Definition 61 (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 $\forall g \in G, \forall h \in H$, $g^{-1}\square h\square g \in H$.

Note 57. 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. $g\square H\square g^{-1} = H$

Exercise 52. Show that the definition of normal subgroup is equivalent with $g^{-1}\square H\square g = H$.

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

Exercise 53. If $H \trianglelefteq G$, show that $a^{-1}\square a' \in H, b^{-1}\square b' \in H \Rightarrow (a\square b)^{-1}\square(a'\square b') \in H$, 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 58. 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

$$\begin{tikzcd} G \times G \arrow[r, "\Box"] \arrow[d, "\pi\times\pi"'] & G \arrow[d, "\pi"] \\ G/H \times G/H \arrow[r, "\Box'"] & G/H \end{tikzcd}$$

holds.

Exercise 54 (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 55. $G \xrightarrow{T} G'$ 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 $(H, \Box)$ is normal then $(G/H, \Box')$ is a group. Conversely, if $(G, \Box)$ is abelian, then any subgroup $(H, \Box)$ is normal, for $ghg^{-1} = gg^{-1}h = h \in H$; and $(G/H, \Box')$ is abelian, for

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

Exercise 56. $G \xrightarrow{T} G'$ 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 8 (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 59. 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 31. 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 $T(1) = (123)$).

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

Homotopy

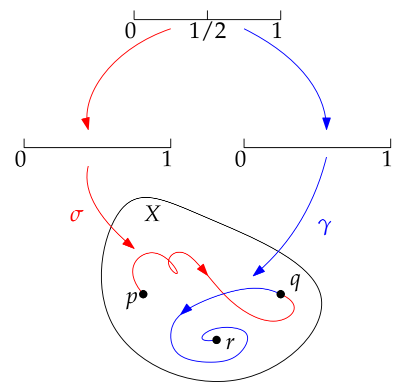
Definition 62 (Path)**.** Assume X is a top. sp. $p, q \in X$.

1. A path from p to q in X is a continuous map $[0,1] \xrightarrow{\gamma} X$, s.t. $\gamma(0) = p, \gamma(1) = q$.
2. Define $\Omega(X, p, q) := \{[0,1] \xrightarrow{\gamma} | \gamma \text{ is conti.}, \gamma(0) = p, \gamma(1) = q\}$.
3. $\forall \gamma \in \Omega(X, p, q)$, define inverse path $[0,1] \xrightarrow{\gamma^-} X(t \mapsto \gamma(1-t))$.

Thus we attain a map $\Omega(X, p, q) \to \Omega(X, q, p)(\gamma \mapsto \gamma^-)$, which is a bijection.

Definition 63. Assume X is a top. sp. $p, q, r, s \in X$. For $\sigma \in \Omega(X, p, q), \gamma \in \Omega(X, q, r)$, define $[0,1] \xrightarrow{\sigma\cdot\gamma} X$ by

$$(\sigma \cdot \gamma)(t) := \begin{cases} \sigma(2t), & t \in [0, 1/2], \\ \gamma(2t-1), & t \in [1/2, 1]. \end{cases}$$



Exercise 57. Given a top. sp. X and subspace A, B of X, s.t. $X = A \cup B$ and either $A, B \subseteq_{open} X$ or $A, B \subseteq_{close} X$. Show that a map $X \xrightarrow{f} Y$ to a top. sp. Y is conti. $\Leftrightarrow A \xrightarrow{f|_A} Y$ and $B \xrightarrow{f|_B} Y$ are conti.

Proof. $\Rightarrow$: f is conti, thus $\forall U \subseteq_{open} Y, f^{-1}(U) \subseteq_{open} X$. And $f|_A^{-1}(U) = f^{-1}(U) \cap A \subseteq_{open} A$, since A is equipped by subspace top. So $f|_A$ is conti. and the same thing to $f|_B$.

Note 60. Notice that the open set in subspace topology is not necessarily open set in (parent) topology.

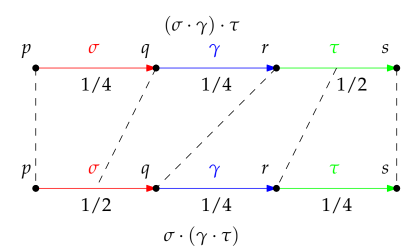
$\Leftarrow$: Suppose $A, B \subseteq_{open} X$, for any $U \subseteq_{open} Y$, since $f|_A$ conti., $f|_A^{-1}(U) \subseteq_{open} A$, thus $\exists V \subseteq_{open} X$, s.t. $f|_A^{-1}(U) = V \cap A \subseteq_{open} X$, and similarly $f|_B^{-1}(U) \subseteq_{open} X$. Thus

$$\begin{aligned} f^{-1}(U) &= \{x \in X | f(x) \in U\} \\ &= \{x \in A | f(x) \in U\} \cup \{x \in B | f(x) \in U\} \\ &= f|_A^{-1}(U) \cup f|_B^{-1}(U) \\ &\subseteq_{open} X. \end{aligned}$$

Thus f is conti. If $A, B \subseteq_{close} X$, the argument is similar, because $X \xrightarrow{f} Y$ is conti. $\Leftrightarrow \forall U \subseteq_{open} Y, f^{-1} \subseteq_{open} X \Leftrightarrow \forall U \subseteq_{close} Y, f^{-1} \subseteq_{close} X$. $\square$

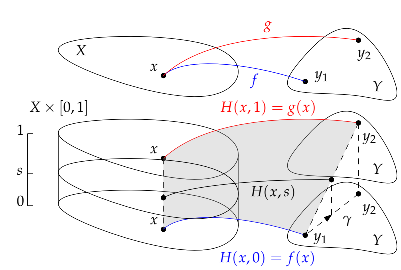
Thus map $[0,1] \xrightarrow{\sigma\cdot\gamma} X$ is also conti. and $\sigma \cdot \gamma \in \Omega(X, p, r)$. And we can define another map: $\Omega(X, p, q) \times \Omega(X, q, r) \to \Omega(X, p, r)((\sigma, \gamma) \mapsto \sigma \cdot \gamma)$.

Notice that the "composite" path does not have "associative" property, that is for any 3 paths $\sigma \in \Omega(X, p, q), \gamma \in \Omega(X, q, r), \tau \in \Omega(X, r, s)$, $(\sigma \cdot \gamma) \cdot \tau$ is not necessarily equal to $\sigma \cdot (\gamma \cdot \tau)$. Because the time (or say speed) distribution on these two composite paths is different, the former is $\sigma(0 - 1/4) \to \gamma(1/4 - 1/2) \to \tau(1/2 - 1)$, whereas the later is $\sigma(0 - 1/2) \to \gamma(1/2 - 3/4) \to \tau(3/4 - 1)$.



Definition 64 (Homotopy)**.** Given two conti. maps $X \xrightarrow{f} Y, X \xrightarrow{g} Y$ between top. sp. X and Y. A map $X \times [0,1] \xrightarrow{H} Y$ is a homotopy from f to g if H is conti. and $\forall x \in X, H(x, 0) = f(x), H(x, 1) = g(x)$.

The intuition of homotopy is creating a map H that starts from f and generally approximates to g as time goes on. On the other hand, we can also view H as creating a path from y_1 to y_2. If H exists, we say f and g are homotopy, denote by $f \underset{H}{\sim} g$.



Definition 65. Suppose X is a top. sp. $p, q \in X, \sigma, \gamma \in \Omega(X, p, q)$, we say σ and γ are homotopic with fixed initial and end point if $\exists$ homotopy $[0,1] \times [0,1] \xrightarrow{H} X$ from σ to γ, s.t. $\forall s \in [0,1], H(0,s) = p, H(1,s) = q$, and denote by $p \underset{\cdot\cdot}{\sim} q$.

Notice that homotopy is only required to be two maps at beginning and end, that is $H(x,0) = \sigma(x)$ and $H(x,1) = \gamma(x)$. But when we say two paths are homotopic, we need for any $s \in [0,1]$, path $H(x,s)$ is from p to q. $\underset{\cdot\cdot}{\sim}$ is an equivalence relation on $\Omega(X, p, q)$, and define $\pi_1(X, p, q) := \Omega(X, p, q) / \underset{\cdot\cdot}{\sim}$, and denote the equivalence class of $\gamma \in \Omega(X, p, q)$ as $[\gamma]$. So if $\gamma \underset{\cdot\cdot}{\sim} \sigma$, then $[\gamma] = [\sigma] \in \pi_1(X, p, q)$.