MATH 417 Lec01-05

Wenxiao Yang[*]

[*]Department of Mathematics, University of Illinois at Urbana-Champaign

2021

目录

1 Function and Set

1.1 Function

$A \times B = \{(a,b)|a \in A, b \in B\}$.
<u>*Function*</u> is a rule σ that assigns an element B to *every* element of A.

$$\sigma : A \to B$$
$$\forall a \in A, \sigma(a) \in B.$$
$$\sigma(a) = \textit{value of } \sigma \textit{ at } a. \textit{ (the } \underline{\textit{image}} \textit{ of } a\textit{)}$$

A set $C \subset B$, we call $\sigma^{-1}(C) = \{a \in A|\sigma(a) \in C\}$ as the <u>*preimage*</u> of a.
An element $b \in B$, we call $\sigma^{-1}(b) = \{a \in A|\sigma(a) = b\}$ as the <u>*fiber*</u> of b.
A is the <u>domain</u> of σ, B is the <u>range</u> of σ.

1.1.1 Composition of functions

$\sigma : A \to B, \tau : B \to C$. The function $\tau \circ \sigma : A \to C$ is $\forall a \in A,\ (\tau \circ \sigma)(a) = \tau(\sigma(a))$

1.1.2 Proposition 1.1.3: Associativity of Functions

Proposition 1 (Proposition 1.1.3)**.** *$\sigma : A \to B, \tau : B \to C, \rho : C \to D$ functions then,*

$$\rho \circ (\tau \circ \sigma) = (\rho \circ \tau) \circ \sigma$$

1.1.3 Injective, surjective, bijective

A function $\sigma : A \to B$ is called,
1. *Injective (1 to 1)*

$$\forall a_1, a_2 \in A, \sigma(a_1) = \sigma(a_2) \Rightarrow a_1 = a_2$$

2. *Surjective (onto)*

$$\forall b \in B, \exists a \in A, s.t. \sigma(a) = b$$

3. *Bijective* (if injective and surjective)

1.1.4 Lemma 1.1.7: 两个 injective/surjective/bijective 的方程的 composition 保留性质

Lemma 1 (Lemma 1.1.7)**.** *Suppose $\sigma : A \to B, \tau : B \to C$ are functions,*
If σ, τ are injective, then $\tau \circ \sigma$ is injective.
If σ, τ are surjective, then $\tau \circ \sigma$ is surjective.
If σ, τ are bijective, then $\tau \circ \sigma$ is bijective.

1.1.5 Proposition 1.1.8: Inverse of Function

Proposition 2 (Proposition 1.1.8). *A function $\sigma : A \to B$ is a bijection if $\exists$ a function $\tau : B \to A$ such that*

$$\sigma \circ \tau = id_B = identity\ on\ B(id_B(x) = x, \forall x \in B)$$
$$\tau \circ \sigma = id_A$$

Such τ is unique, called inverse of σ, $\tau = \sigma^{-1}$.

1.2 Set

1.2.1 Well Defined Set

Definition 1. *A set S is* ***well defined*** *if an object a is either $a \in S$ or $a \notin S$.*

1.2.2 Power Set

Definition 2. *For any set A, we denote by $\mathcal{P}(A)$ the collection of all subsets of A. $\mathcal{P}(A)$ is the* ***power set*** *of A.*

1.2.3 Cardinalities of Sets, Pigeonhole Principle

Definition 3. *If A is a set, $|A| =$ cardinality of $A = \#$ of elements*

$n \in \mathbb{N}, |\{1, \dots n\}| = n$; $|\emptyset| = 0(\emptyset = \text{ empty set })$.
$|A| = |B|$ if there is a bijection $\sigma : A \to B$.
If there is an *injection* $\sigma : A \to B$, we can write $|A| \leq |B|$;
If there is a *surjection* $\sigma : A \to B$, we can write $|A| \geq |B|$.

Theorem 1 (Pigeonhole Principle). *If A and B are sets and $|A| > |B|$, then there is no injective function $\sigma : A \to B$.*

1.2.4 B^A: Sets of Function

If A, B are sets, then $B^A = \{\sigma : A \to B | \sigma \ a\ function\}$.

Example 1. *$n \in \mathbb{Z}$, we define a function $f : B^{\{1,\dots,n\}} \to B^n (= B \times B \times B \times \cdots \times B)$ by the equation $f(\sigma) = \{\sigma(1), ..., \sigma(n)\}$, where $\sigma : \{1, \dots, n\} \to B$. The f is a bijection.*

证明.
1. *Injective*:

$$f(\sigma_1) = f(\sigma_2) \Rightarrow \{\sigma_1(1), ..., \sigma_1(n)\} = \{\sigma_2(1), ..., \sigma_2(n)\}$$
$$Since\ \sigma : \{1, \dots, n\} \to B,\ it\ is\ sufficient\ to\ prove\ \sigma_1 = \sigma_2.$$

2. *Surjective*:

$$\forall \{b_1, ..., b_n\}, \text{ we have } \sigma^*(x) = b_x, x = 1, ..., n. \text{ s.t. } f(\sigma^*) = \{b_1, ..., b_n\}$$

$\square$

Example 2.

$$C(\mathbb{R}, \mathbb{R}) = \{\text{continuous functions } \sigma : \mathbb{R} \to \mathbb{R}\} \subset \mathbb{R}^{\mathbb{R}}$$

1.2.5 Binary operations on a Set, associative, commutative

A binary operation on a set A is a function $* : A \times A \to A$.
The operation is *associative* if $a * (b * c) = (a * b) * c, \forall a, b, c \in A$.
The operation is *commutative* if $a * b = b * a, \forall a, b \in A$.

Example 3. $+, \circ$ *are both associative and commutative operations on* $\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{R}$*;* $-$ *is a neither associative nor commutative operation on* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$*, but not* $\mathbb{N}$*.*

2 Equivalence relations and Partition

2.1 Equivalence relations（理性等价的定义）

理性的等价需要满足: (1)Reflexive, (2)Symmetric, (3)Transitive. Given a set X, a relation on X is a subset of $R \subset X \times X$. We write $a \sim b$.
A relation $\sim$ is said to be
1. *Reflexive* if $\forall x \in X$, we have $x \sim x$.
2. *Symmetric* if $\forall x, y \in X$, $x \sim y \Rightarrow y \sim x$.
3. *Transitive* if $\forall x, y, z \in X$, $x \sim y, y \sim z \Rightarrow x \sim z$.
The *sim* is called **equivalence relation** if it is *reflexive, Symmetric* and *Transitive.*

Example 4. *Set* $X = \{(a, b) \in \mathbb{Z}^2 | b \neq 0\}$*, satisfies* $(a, b) \sim (c, d)$ *if* $ad = bc$*.*

1. *Reflexive*: $(a, b) \sim (a, b), \forall (a, b) \in \mathbb{Z}^2$.
2. *Symmetric*: $\forall (a, b), (c, d) \in \mathbb{Z}^2, (a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$.
3. *Transitive*: $\forall (a, b), (c, d), (u, v) \in \mathbb{Z}^2, (a, b) \sim (c, d), (c, d) \sim (u, v) \Rightarrow ad = bc, cv = du \Rightarrow acv = adu = bcu \Rightarrow av = bu \Rightarrow (a, b) \sim (u, v)$.
So this is an equivalence relation.

Example 5. $f : X \to Y$ *is a function, define* $\sim_f$ *on* X *by* $a \sim_f b$ *if* $f(a) = f(b)$*.*

1. *Reflexive*: $a \sim a, \forall a \in X$.
2. *Symmetric*: $a, b \in X, a \sim b \Rightarrow b \sim a$.
3. *Transitive*: $\forall a, b, c \in X, a \sim b, b \sim c \Rightarrow f(a) = f(b) = f(c) \Rightarrow a \sim c$.
So $\sim_f$ is an equivalence relation.

2.2 Partition（满足不重叠，无剩余的 set 拆分结果）

X a set, a partition of X is a collection ω of subsets of X s.t.

1) $\forall A, B \in \omega$ either $A = B$ or $A \cap B = \emptyset$.

2) $\cup_{A\in\omega} A = X$.

The subsets are the **cell**s of partition.

2.3 Equivalence class

2.3.1 $[x]$: equivalence class

Define the **equivalence class** of x to be the subset $[x] \subset X$:

$$[x] = \{y \in X | y \sim x\}$$

Where $\sim$ is an equivalence relation.
$\sim$ is reflexive $\Rightarrow x \in [x]$. We say that any $y \in [x]$ as a **representative** of the equivalence class.

2.3.2 $X/\sim$: set of equivalence classes

Set of equivalence classes 是一个 **set** 被某种 *equivalence relation* 分类的结果
We write the set of equivalence classes

$$X/\sim = \{[x] | x \in X\}$$

2.4 Relationship of ***Equivalence relation***, ***Set of equivalence classes*** and ***Partitions***

给定 X，*Equivalence relation* $\sim$ 与*Set of equivalence classes* $X/\sim$ 具有相同的信息量；包含所有*Partitions* 的集合与包含所有*Set of equivalence classes* 的集合相同。

2.4.1 Theorem 1.2.7: Equivalence relation $\sim \Leftrightarrow$ Set of equivalence classes $X/\sim$; {all Sets of equivalence classes} = {all Partitions}

Theorem 2 (Theorem 1.2.7)**.** *$X/\sim$ is a partition of X. Conversely, given a partition ω of X, there exists a unique equivalence relation $\sim_\omega$ s.t. $X/\sim_\omega = \omega$.*

(1) *Equivalence relation* $\sim$ 生成一个对应的*Set of equivalence classes* $X/\sim$，该 $X/\sim$ 就是一个 Partition。(可以看作 1. 所有 Set of equivalence classes 都是 Partitions; 2.$\sim\Rightarrow X/\sim$ 由方式推结果)
(2) 反之，我们也可以根据已有的 Partition ω, 将其作为一种分类方式 $\sim_\omega$ 的 _(i.e. $X/\sim_\omega = \omega$) 这个对应的 $\sim_\omega$ 存在且是唯一的。(可以看作 1. 所有 Partitions 都是 Set of equivalence classes; 2.$X/\sim\Rightarrow\sim$ 由结果推方式)

证明.
(1)$X/\sim$ is a partition of X:

$$\forall x, y \in X \ s.t.\ [x] \cap [y] \neq \emptyset$$
$$Let\ z \in [x] \cap [y] \Rightarrow z \sim x, z \sim y$$
$$\forall w \in [x] \Rightarrow w \sim x \Rightarrow x \sim w \Rightarrow z \sim w \Rightarrow w \sim z \Rightarrow w \sim y \Rightarrow [x] \subset [y]$$
$$Similarly\ we\ can\ prove\ [y] \subset [x] \Rightarrow [x] = [y]$$

(2)Given a partition ω of X, there exists a unique equivalence relation $\sim_\omega$ s.t. $X/\sim_\omega = \omega$:
(2.1) Prove there exists an equivalence relation s.t. $X/\sim_\omega = \omega$:
We define a relation: $x \sim_\omega y$ if there exists $A \in \omega$ s.t. $x, y \in A \Rightarrow \sim_\omega$ is symmetric and transitive. Since $\cup_{A\in\omega} A = X$, we know $\forall x \in X, \exists A \in \omega\ s.t.\ x \in A \Rightarrow \sim_\omega$ is reflexive. So $\sim_\omega$ is an equivalence relation.
We know $A = [x], \forall A \in \omega, \forall x \in A$ (by $\sim_\omega$), then $X/\sim_\omega = \{[x] | x \in \cup_{A\in\omega} A\} = \{\{A^* | x \in A^*\} | A^* \in \omega\} = \omega$.
(2.2) Prove the equivalence relation is unique:
Set $\sim$ be any equivalence relation that make $X/\sim = \omega$, then we know $\forall A \in \omega, \exists x \in X$ s.t. $[x] = A$. According to the definition of $[x]$, if $x \in A$, $y \sim x$ if and only if $y \in [x] = A$. Which is exactly the $\sim_\omega$. □

Example 6 (the same as example 5). *$f : X \to Y$ is a function, define $\sim_f$ on X by $a \sim_f b$ if $f(a) = f(b)$. In this example the **equivalence classes** are precisely the fibers $[x] = f^{-1}(f(x))$. $y \sim_f x \Rightarrow y \in f^{-1}(f(x))$*

Example 7 (the same as example 4). *Set $X = \{(a, b) \in \mathbb{Z}^2 | b \neq 0\}$, satisfies $(a, b) \sim (c, d)$ if $ad = bc$. i.e. we write the equivalence of (a, b) as $\frac{a}{b} = [(a, b)]$. Then $X/\sim = \mathbb{Q}$.*

2.4.2 Proposition 1.2.12: 根据结果 $X/\sim = \{[x] | x \in X\}$ 推断的 $\sim_\pi$ equals to $\sim$.

Proposition 3 (Proposition 1.2.12). *If $\sim$ is an equivalence relation on X, define a surjective function $\pi : X \to X/\sim$ by $\pi(x) = [x]$. Then $\sim_\pi = \sim$(the definition of $\sim_f$ in example 6.)*

证明.
(1)Surjective:
$X/\sim = \{[x] | x \in X\} = \{\pi(x) | x \in X\}$, so $\forall y \in X/\sim$, $y \in \{\pi(x) | x \in X\}$, there exists $x \in X$ s.t. $\pi(x) = y$.
(2)$\sim_\pi = \sim$
$a \sim_\pi b$ if $\pi(a) = \pi(b) \Leftrightarrow [a] = [b]$, which is exactly the definition of $\sim$. □

逻辑:
1. Given $\sim$;
2. Get the corresponding $X/\sim = \{[x] | x \in X\}$;

3. $\pi(x) = [x]$;
4. $\sim_\pi$: $a \sim_\pi b$ iff $\pi(a) = \pi(b)$
5. $\sim_\pi = \sim$
根据结果 $X/\sim = \{[x] | x \in X\}$ 推断的 $\sim_\pi$ equals to $\sim$.

2.4.3 Proposition 1.2.13: 给 X 标记 Y: f, 给 $X/\sim$ 标记 Y : $\tilde{f}$, ; 两函数之间一一对应

Proposition 4 (Proposition 1.2.13). *Given any function $f : X \to Y$ there exists a unique function $\tilde{f} : X/\sim \to Y$ such that $\tilde{f} \circ \pi = f$, where $\pi : X \to X/\sim$ in proposition 3. Furthermore, $\tilde{f}$ is a bijection onto the image $f(X)$.*

证明.
(1) Existence:
We define $x_1 \sim_f x_2$ if $f(x_1) = f(x_2)$. Set $\tilde{f} : X/\sim_f \to Y$, $\tilde{f}([x]) = f(x)$. Then $\tilde{f}[\pi(x)] = \tilde{f}([x]) = f(x)$. Exactly what we require.
(2) Uniqueness:
Set any $\tilde{f}'$ s.t. $\tilde{f}' \circ \pi = f$, then $\tilde{f}'[\pi(x)] = \tilde{f}'([x]) = f(x)$, i.e. the $\tilde{f}$ is unique.
(3) Bijection:
Surjective, which we proved before $\forall f, \exists \tilde{f}$ s.t. $\tilde{f} \circ \pi = f$;
Injective, we also have proved the uniqueness $f = \tilde{f} \circ \pi = \tilde{f}' \circ \pi \Rightarrow \tilde{f}' = \tilde{f}$. $\square$

3 Permutations 改变位置

Definition 4. *Let X be a finite set, a permutation is bijection $\sigma : X \to X$.*

Definition 5. *Let S_X ($Sym(X)$) be the set of all bijection $\sigma : X \to X$.*

If $|X| = n$, $|S_X| = n!$.

3.1 $Sym(X) = \{\sigma : X \to X | \sigma$ *is a bijection*$\}$: permutation group of X; elements in $Sym(X)$: permutations of X

We set $Sym(X) = \{\sigma : X \to X | \sigma \text{ is a bijection}\} \subset X^X$. We call it **symmetric group of X** or **permutation group of X**. We call the elements in $Sym(X)$ the **permutations of X** or the **symmetries of X**.

3.1.1 Properties of $\circ$ on $Sym(X)$

Proposition 5 (Proposition 1.3.1.). *For any nonempty set X, $\circ$ is an operation on $Sym(X)$ with the following properties:*
(i) $\circ$ is associative.
(ii) $id_X \in Sym(X)$, and for all $\sigma \in Sym(X)$, $id_X \circ \sigma = \sigma \circ id_X = \sigma$, and
(iii) For all $\sigma \in Sym(X)$, $\sigma^{-1} \in Sym(X)$.

Permutations 类似于 rearrangement，交换 X 中元素的排序。

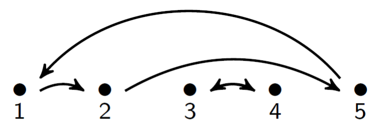
3.1.2 S_n: Permutation group on n elements, σ^i

Note 1. *When $X = \{1, ..., n\}, n \in \mathbb{Z}$, write $S_n = Sym(X)$* ***symmetric/permutation group on n elements****.*

Note 2. *$\sigma \in Sym(X)$, write $\sigma^n = \sigma \circ \sigma \circ ... \circ \sigma$, $\sigma^0 = id_X$, $\sigma^{-1} = inverse$, $r > 0, \sigma^{-r} = (\sigma^{-1})^r$. So, $r, s \in \mathbb{Z}, \sigma^{r+s} = \sigma^r \circ \sigma^s = \sigma^s \circ \sigma^r$.*

3.1.3 k-cycle, cyclically permute/fix

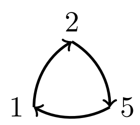
Example 8.



$$1 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 1, \quad \tau_1$$

$$3 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 3, \quad \tau_2$$

图 1: Example of Cycle

In the example of *Figure 1*, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$, $\sigma = \tau_1 \circ \tau_2$, where $\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$. τ_1 is 3-cycle, τ_2 is 2-cycle. We could represent $\tau_1 = (1\ 2\ 5) = (2\ 5\ 1) = (5\ 1\ 2)$, i.e. 

Similarly, we can represent $\tau_2 = (3, 4) = (4, 3)$, i.e. $3 \longleftrightarrow 4$

We can find that $\forall x \in \{1, 2, 3, 4, 5\}$, $\tau_1^3(x) = x, \tau_2^2(x) = x$, so we write τ_1 as a **3-cycle** in S_5, τ_2 as a **2-cycle** in S_5.

Given $k \geq 2$, a **k-cycle** in S_n is a permutation σ with the property that $\{1, ..., n\}$ is the union of two disjoint subsets, $\{1, ..., n\} = Y \cup Z$ and $Y \cap Z = \emptyset$, such that

1. $\sigma(x) = x$ for every $x \in Z$, and
2. $|Y| = k$, and for any$x \in Y$,$Y = \{\sigma(x), \sigma^2(x), \sigma^3(x) ... \sigma^k(x) = x\}$.

We say that σ **cyclically permutes** the elements of Y and **fixes** the elements of Z.
$\tau_1 = (1\ 2\ 5)$ **cyclically permutes** the elements of $Y = \{1, 2, 5\}$ and **fixes** the elements of $Z = \{3, 4\}$.
$\tau_2 = (3\ 4)$ **cyclically permutes** the elements of $Y = \{3, 4\}$ and **fixes** the elements of $Z = \{1, 2, 5\}$.

3.2 Disjoint cycles

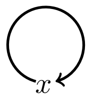
Since the sets are cyclically permuted by τ_1, τ_2 (i.e.Y) are disjoint. We call the **disjoint cycle notation** $\sigma = \tau_1 \circ \tau_2 = (1\ 2\ 5)(3\ 4)$. (Commute the order is irrelevant)

3.2.1 Theorem: Every permutation is a union of disjoint cycles, uniquely.

Given $\sigma \in S_n$, there exists a unique (possibly empty) set of pairwise disjoint cycles.

Theorem 3. *Let X be a finite set, the graph of permutation $\sigma \in S_X$ is a union of disjoint cycle.*

证明. Prove by induction:

If $|X| = 1$, the graph is circle: 

For $|X| > 1$, let $i_1 \in X$ and let $\mathcal{O}(i_1) = \{\sigma^r(i_1), r \geq 0\} = \{i_1, \sigma(i_1), \sigma^2(i_1), ...\}$. $\mathcal{O}(i_1)$ is finite, and there is a smallest r s.t. $\sigma^r(i_1) \in \{i_1, \sigma(i_1), \sigma^2(i_1), ..., \sigma^{r-1}(i_1)\}$. Then $\sigma^r(i_1) = i_1$ because other elements already have a pre-change under σ.
Then $i_1 \to \sigma(i_1) \to \sigma^2(i_1) \to \cdots \to \sigma^{r-1}(i_1) \to i_1$ is a cycle of length r.
For $j \notin \mathcal{O}(i_1), \sigma(j) \notin \mathcal{O}(i_1), \sigma^{-1}(j) \notin \mathcal{O}(i_1)$. Let $Y = X/\mathcal{O}(i_1)$ then $\sigma : Y \to Y$ is a bijection. Then prove by induction.

□

Example 9. $\sigma_1 = (1\ 2\ 6\ 5)(3)(4)$, *can be written by* $\sigma_1 = (1\ 2\ 6\ 5)$, $\sigma_2 = (2\ 3\ 5\ 4)$

$\sigma_1 \circ \sigma_2 = (1\ 2\ 6\ 5) \circ (2\ 3\ 5\ 4)$

$$1 \xrightarrow{(2\ 3\ 5\ 4)} 1 \xrightarrow{(1\ 2\ 6\ 5)} 2$$
$$2 \xrightarrow{(2\ 3\ 5\ 4)} 3 \xrightarrow{(1\ 2\ 6\ 5)} 3$$
$$3 \xrightarrow{(2\ 3\ 5\ 4)} 5 \xrightarrow{(1\ 2\ 6\ 5)} 1$$
$$4 \xrightarrow{(2\ 3\ 5\ 4)} 2 \xrightarrow{(1\ 2\ 6\ 5)} 6$$
$$5 \xrightarrow{(2\ 3\ 5\ 4)} 4 \xrightarrow{(1\ 2\ 6\ 5)} 4$$
$$6 \xrightarrow{(2\ 3\ 5\ 4)} 6 \xrightarrow{(1\ 2\ 6\ 5)} 5$$

Then $\sigma_1 \circ \sigma_2 = (1\ 2\ 3) \circ (4\ 6\ 5)$

$\sigma_2 \circ \sigma_1 = (2\ 3\ 5\ 4) \circ (1\ 2\ 6\ 5)$

$$1 \xrightarrow{(1\ 2\ 6\ 5)} 2 \xrightarrow{(2\ 3\ 5\ 4)} 3$$
$$2 \xrightarrow{(1\ 2\ 6\ 5)} 6 \xrightarrow{(2\ 3\ 5\ 4)} 6$$
$$3 \xrightarrow{(1\ 2\ 6\ 5)} 3 \xrightarrow{(2\ 3\ 5\ 4)} 5$$
$$4 \xrightarrow{(1\ 2\ 6\ 5)} 4 \xrightarrow{(2\ 3\ 5\ 4)} 2$$
$$5 \xrightarrow{(1\ 2\ 6\ 5)} 1 \xrightarrow{(2\ 3\ 5\ 4)} 1$$
$$6 \xrightarrow{(1\ 2\ 6\ 5)} 5 \xrightarrow{(2\ 3\ 5\ 4)} 4$$

Then $\sigma_2 \circ \sigma_1 = (1\ 3\ 5) \circ (2\ 6\ 4)$

Note: $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$

Example 10 (Exercise 1.3.2.)**.** *Consider $\sigma = (3\ 4\ 8)(5\ 7\ 6\ 9)$ and $\tau = (1\ 9\ 3\ 5)(2\ 7\ 4)$ in S_9 expressed in disjoint cycle notation. Compute $\sigma \circ \tau$ and $\tau \circ \sigma$ expressing both in disjoint cycle notation.*

$$\begin{aligned}
&1 \to \sigma(\tau(1)) = \sigma(9) = 5;\ 2 \to \sigma(\tau(2)) = \sigma(7) = 6;\\
&3 \to \sigma(\tau(3)) = \sigma(5) = 7;\ 4 \to \sigma(\tau(4)) = \sigma(2) = 2;\\
&5 \to \sigma(\tau(5)) = \sigma(1) = 1;\ 6 \to \sigma(\tau(6)) = \sigma(6) = 9;\\
&7 \to \sigma(\tau(7)) = \sigma(4) = 8;\ 8 \to \sigma(\tau(8)) = \sigma(8) = 3;\\
&9 \to \sigma(\tau(9)) = \sigma(3) = 4;\\
\Rightarrow &\sigma \circ \tau = (1\ 5)(2\ 6\ 9\ 4)(3\ 7\ 8)
\end{aligned}$$

$$\begin{aligned}
&1 \to \tau(\sigma(1)) = \tau(1) = 9;\ 2 \to \tau(\sigma(2)) = \tau(2) = 7;\\
&3 \to \tau(\sigma(3)) = \tau(4) = 2;\ 4 \to \tau(\sigma(4)) = \tau(8) = 8;\\
&5 \to \tau(\sigma(5)) = \tau(7) = 4;\ 6 \to \tau(\sigma(6)) = \tau(9) = 3;\\
&7 \to \tau(\sigma(7)) = \tau(6) = 6;\ 8 \to \tau(\sigma(8)) = \tau(3) = 5;\\
&9 \to \tau(\sigma(9)) = \tau(5) = 1;\\
\Rightarrow &\tau \circ \sigma = (1\ 9)(2\ 7\ 6\ 3)(4\ 8\ 5)
\end{aligned}$$

Example 11. *Let $\sigma, \tau \in S_7$, given in disjoint cycle, notation by $\sigma = (1\ 5\ 4)(3\ 7), \tau = (1\ 3\ 2\ 6\ 4)$, Compute $\sigma^2, \sigma^{-1}, \tau \circ \sigma$*

$$\begin{aligned}
&\sigma^2 = (1\ 4\ 5), && \sigma^{-1} = (4,5,1)(3,7),\\
&1 \to \tau(\sigma(1)) = \tau(5) = 5, && 2 \to \tau(\sigma(2)) = \tau(2) = 6,\\
&3 \to \tau(\sigma(3)) = \tau(7) = 7, && 4 \to \tau(\sigma(4)) = \tau(1) = 3,\\
&5 \to \tau(\sigma(5)) = \tau(4) = 1, && 6 \to \tau(\sigma(6)) = \tau(6) = 4,\\
&7 \to \tau(\sigma(7)) = \tau(3) = 2,\\
\Rightarrow &\tau \circ \sigma = (1,5)(2,6,4,3,7)
\end{aligned}$$

3.3 Transposition

Definition 6. *A **transposition** is a cycle of length 2:* $\sigma = (i\ j)$*.*

3.3.1 Theorem: 每个 permutation 可以由若干个（可能不 disjoint 的）transposition 表示

Theorem 4. *Every permutation* σ *of* X *is a product of transposition. (the product is not unique)*
Equivalent: *Given* $n \geq 2$*, any* $\sigma \in S_n$ *can be expressed as a composition of 2-cycles.(not require disjoint)*

证明.

Version 1:

$$\begin{aligned}(x_1\ x_k)(x_1\ x_2, \ldots\ x_{k-1}\ x_k) &= (x_1\ x_2\ \ldots\ x_{k-1}) \\ (x_1\ x_2\ \ldots\ x_{k-1}\ x_k) &= (x_1\ x_k)(x_1, x_2\ \ldots\ x_{k-1}) \\ &= (\mathbf{x_1}\ \mathbf{x_k})(\mathbf{x_1}\ \mathbf{x_{k-1}})(\mathbf{x_1}\ \mathbf{x_2}\ \ldots\ \mathbf{x_{k-2}}) \\ &\ldots \\ &= (\mathbf{x_1}\ \mathbf{x_k})(\mathbf{x_1}\ \mathbf{x_{k-1}})(\mathbf{x_1}\ \mathbf{x_{k-2}}) \ldots (\mathbf{x_1}\ \mathbf{x_2})\end{aligned}$$

Version 2:

$$\begin{aligned}(x_1\ x_2, \ldots\ x_{k-1}\ x_k)(x_1\ x_k) &= (x_2\ x_3\ \ldots\ x_k) \\ (x_1\ x_2\ \ldots\ x_{k-1}\ x_k) &= (x_2\ x_3\ \ldots\ x_k)(x_1\ x_k) \\ &\ldots \\ &= (\mathbf{x_{k-1}}\ \mathbf{x_k})(\mathbf{x_{k-2}}\ \mathbf{x_k}) \ldots (\mathbf{x_2}\ \mathbf{x_k})(\mathbf{x_1}\ \mathbf{x_k})\end{aligned}$$

□

3.3.2 Sign of Permutation

Theorem 5. *Although the product of transposition of a permutation is not unique, the parity (odd or even) of the r in a product is unique. We call it the **sign** of permutation.*

$$\begin{aligned}sign(\sigma) &= (-1)^{(\#\ \text{even-length cycles in}\ \sigma)} \\ &= (-1)^{(\#\ \text{transpositions in}\ \sigma)}\end{aligned}$$

What happens to a permutation σ's cycles if $\sigma \to (i\ j) \circ \sigma$?
1. i and j are not contained in σ.
2. i and j appear in the same cycle of σ.
3. i and j appear in disjoint cycles.

$$\begin{aligned}(i\ j) \circ (i - -j \sim\sim) &= (i - -) \circ (j \sim\sim) \\ (i\ j) \circ (i - -) \circ (j \sim\sim) &= (i - -j \sim\sim)\end{aligned}$$

Proposition 6. $sign((i\ j) \circ \sigma) = -1 \cdot sign(\sigma)$

证明.

Suppose $\sigma = (a_1\ a_2\ \cdots a_k\ \sigma_1\ \sigma_2\ \cdots \sigma_l)$
Then $(a_1\ b_1) \circ \sigma = (a_1\ a_2\ \cdots a_k)(\sigma_1\ \sigma_2\ \cdots \sigma_l)$

$$sign(\sigma) = \begin{cases} +1 & \text{if } k+l \text{ is odd} \\ -1 & \text{if } k+l \text{ is even} \end{cases}$$

$$sign((a_1\ b_1) \circ \sigma) = \begin{cases} -1 & \text{if } k+l \text{ is odd} \\ +1 & \text{if } k+l \text{ is even} \end{cases}$$

□

参考文献

[1] Christopher J Leininger Introduction to Abstract Algebra (Draft) 2017.