Quadratic Reciprocity Laws:

Let p be an odd prime number. Then we have

Reciprocity of -1

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Reciprocity of 2

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$$

Reciprocity of q (an odd prime)

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \quad \text{where } p^* := (-1)^{\frac{p-1}{2}} \cdot p$$

Interchange of congruence and modulus

Goal (of next lectures): prove the third quadratic reciprocity law

There are many different approaches.

Our approach:

We will interpreate $\left(\frac{q}{p}\right)$ in terms of "sign of permutations".

And compute $\left(\frac{q}{p}\right)$ and $\left(\frac{p^*}{q}\right)$ respectively

using different characterizations of sign.

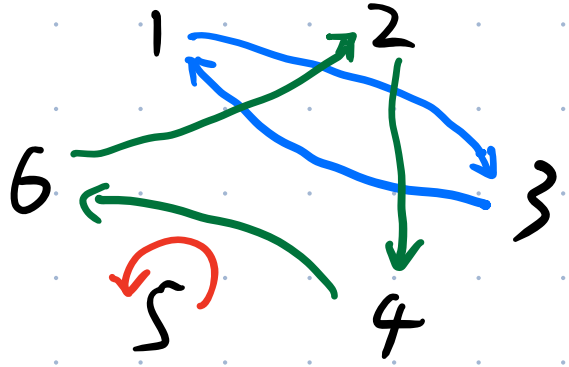
Today: • definition of permutations and sign

• Three characterizations of sign.

Defn. A **permutation** of a set S is a bijection from S to itself.

E.g. $S = \{1, 2, 3, 4, 5, 6\}$

$f: S \longrightarrow S$ as follows:



Then f consists of

a cycle of length 1: 5

a cycle of length 2: 1 ⇄ 3

a cycle of length 3: 2 → 4 → 6 → 2

Permutation consists of cycles

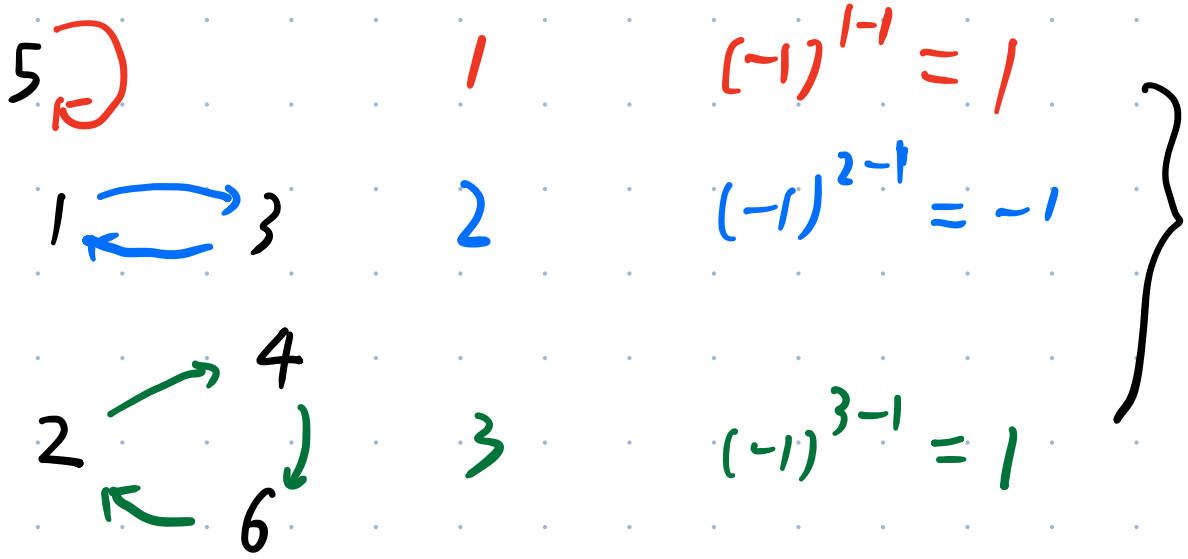
Defn. (1st def. of sign)

Let S be a finite set and f be a permutation

(1) The sign of a cycle of length ℓ is $(-1)^{\ell-1}$

(2) The sign of f is the product of the sign of cycles in f.

e.g. Let f be as in previous example.



5 : 1 : $(-1)^{1-1} = 1$

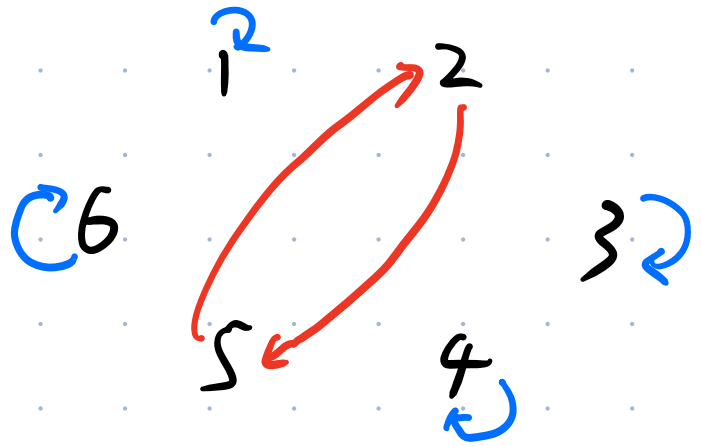
$1 \rightleftarrows 3$: 2 : $(-1)^{2-1} = -1$

$2 \to 4 \to 6 \to 2$: 3 : $(-1)^{3-1} = 1$

$\Big\}$ $\operatorname{sign}(f) = -1$.

Defn. A transposition of S is a permutation of S that exchanges 2 element $a \neq b \in S$ and fixes the rest.

e.g. $S = \{1, 2, 3, 4, 5, 6\}$



Notations:

If τ is the transposition exchanging a and b. Then τ is denoted by

- $(a\ b)$
- $\tau_{a,b}$ \tau_{a,b}

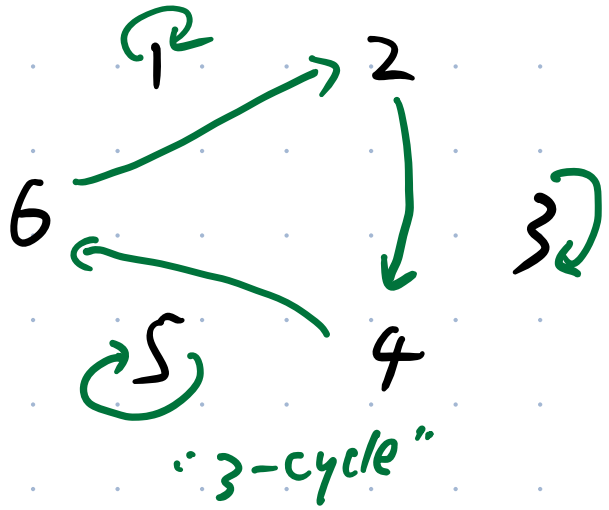
$(-1)^{2-1} = -1$

sign

Rmk: Any transposition has sign -1.

More generally, a cyclic permutation of length ℓ of S is a permutation that consists of a cycle of length ℓ and fixes the rest. Also called "ℓ-cycle"

e.g. $S = \{1, 2, 3, 4, 5, 6\}$



∵ 3-cycle"

Notations:

If the cyde is $a_1 \to a_2 \to a_3 \to \cdots \to a_\ell \to a_1$

then we denote the cyclic permutation by

- $(a_1\ a_2\ a_3 \cdots a_\ell)$

Rmk: transposition = 2-cycle

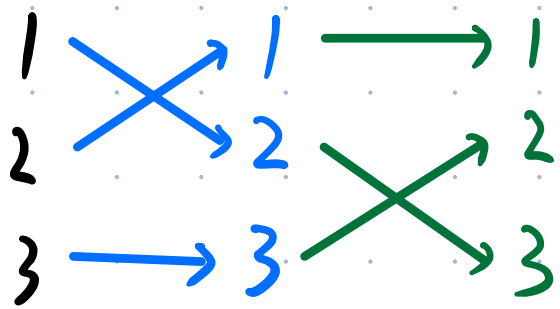
Prop. If f, g are two permutations of S, then

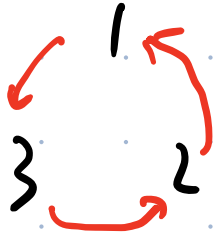
$g \circ f$ is also a permutation. bijection ∘ bijection = bijection.

WARN: $g \circ f \neq f \circ g$ in general!

E.g. $S = \{1, 2, 3\}$ $f = (12)$ $g = (23)$

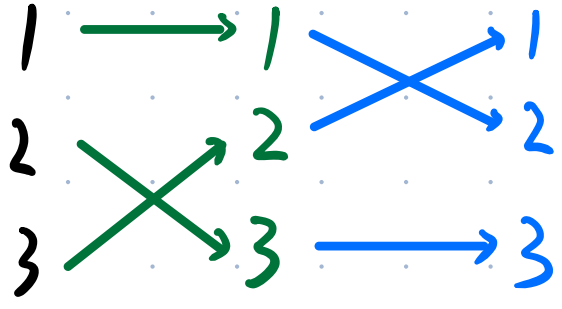
Then $g \circ f$ is

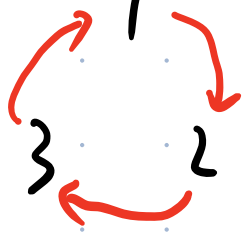




(132)

$f \circ g$ is





(123)

Some terminology & notations

- The set of ALL permutations of a finite set S has a group structure: the binary operation is "composition" and the identity is the identity map.

WARN: this group is NOT commutative!

(Indeed, this is where the notion of "group" arise.)

This group $(\{\text{perms of } S\}, \circ, \mathrm{id})$ is called the **permutation group** / **symmetric group** of S

Notation: $\mathrm{Perm}(S)$, $\mathrm{Sym}(S)$, $\mathfrak{S}_S$ \mathfrak{S}_{S}

Now, suppose f is a permutation on S.

1. It consists of cycles:

   For any $a \in S$, $a, f(a), fff(a), \cdots, f^n(a), \cdots$ must repeat.

   Since f is invertible, the sequence falls into a cycle.

2. Suppose $C_1, C_2, \cdots, C_t$ are the cycles in f, then

   we have $$f = C_1 \circ C_2 \circ \cdots \circ C_t$$

   and the composition can be rearranged in any order.

   Since C_i only acts on its members as f and fixes the rest.

Prop. (Generators of $Sym(S)$)

Any permutation of S is an iterated composition of transpositions.

Proof. Only need to show that:

any cycle is an iterated composition of transpositions.

$$f = (a_1\ a_2\ \cdots\ a_n)$$

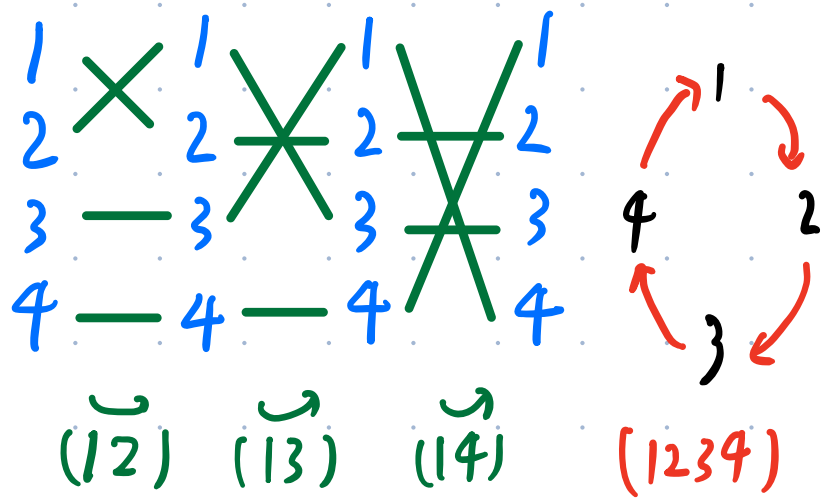
1) $f = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_2)$

2) $f = (a_1\ a_2)(a_2\ a_3)\cdots(a_{n-1}\ a_n)$

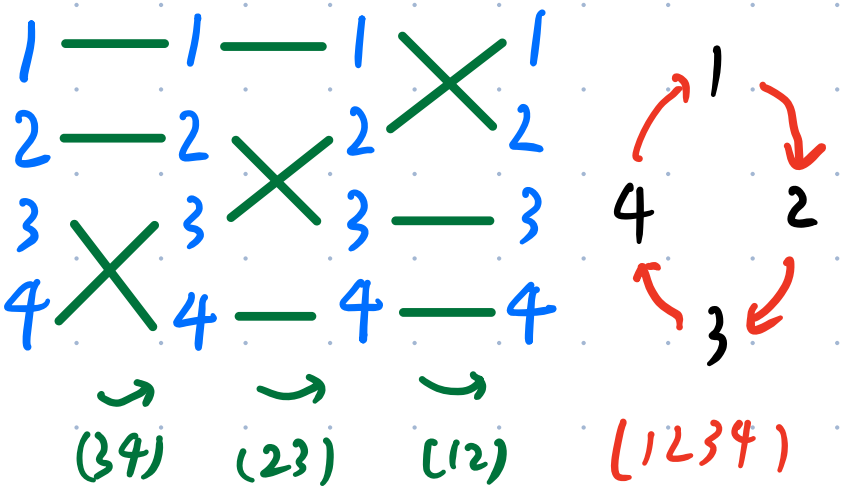
any of them works.

e.g. $f = (1234)$

1) $(1234) = (14)(13)(12)$



2) $(1234) = (12)(23)(34)$



In general: trace a_i

How does it be mapped ?

1) When $j < i$, $(a_1\ a_j)$ fixes a_i

$$(a_1\ a_{i-1}) \cdots (a_1\ a_2) \cdot a_i = a_i \quad (\text{acts on } a_i)$$

Then $(a_1\ a_i)$ exchanges a_1 & a_i:

$$(a_1\ a_i) \cdot a_i = a_1$$

Then $(a_1\ a_{i+1})$ exchanges a_1 & a_{i+1}:

$$(a_1\ a_{i+1}) \cdot a_1 = a_{i+1}$$

Combine them, we get

$$(a_1\ a_{i+1})(a_1\ a_i)(a_1\ a_{i-1}) \cdots (a_1\ a_2) \cdot a_i = a_{i+1}$$

The rest $(a_1\ a_k)$ $(k > i+1)$ fixes a_{i+1}:

Hence: $(a_1\ a_n) \cdots (a_1\ a_2) \cdot a_i = a_{i+1}$

convention: $a_{n+1} = a_1$.

2) When $j > i$, $(a_j\ a_{j+1})$ fixes a_i:

$$(a_{i+1}\ a_{i+2}) \cdots (a_{n-1}\ a_n) \overset{\text{acts on}}{\cdot}\ a_i = a_i$$

Then $(a_i\ a_{i+1})$ exchange a_i & a_{i+1}:

$$(a_i\ a_{i+1}) \cdots (a_{n-1}\ a_n) \cdot a_i = a_{i+1}$$

Then for $k < i$, $(a_k\ a_{k+1})$ fixes a_{i+1}:

$$(a_1\ a_2) \cdots (a_{i-1}\ a_i) \cdot a_{i+1} = a_{j+1}$$

Hence,

$$(a_1\ a_2) \cdots (a_{n-1}\ a_n) \cdot a_i = a_{i+1},$$

$$(a_1\ a_2)(a_1\ a_3) \cdots (a_{n-1}\ a_n) = (a_1\ a_2 \cdots a_n)$$

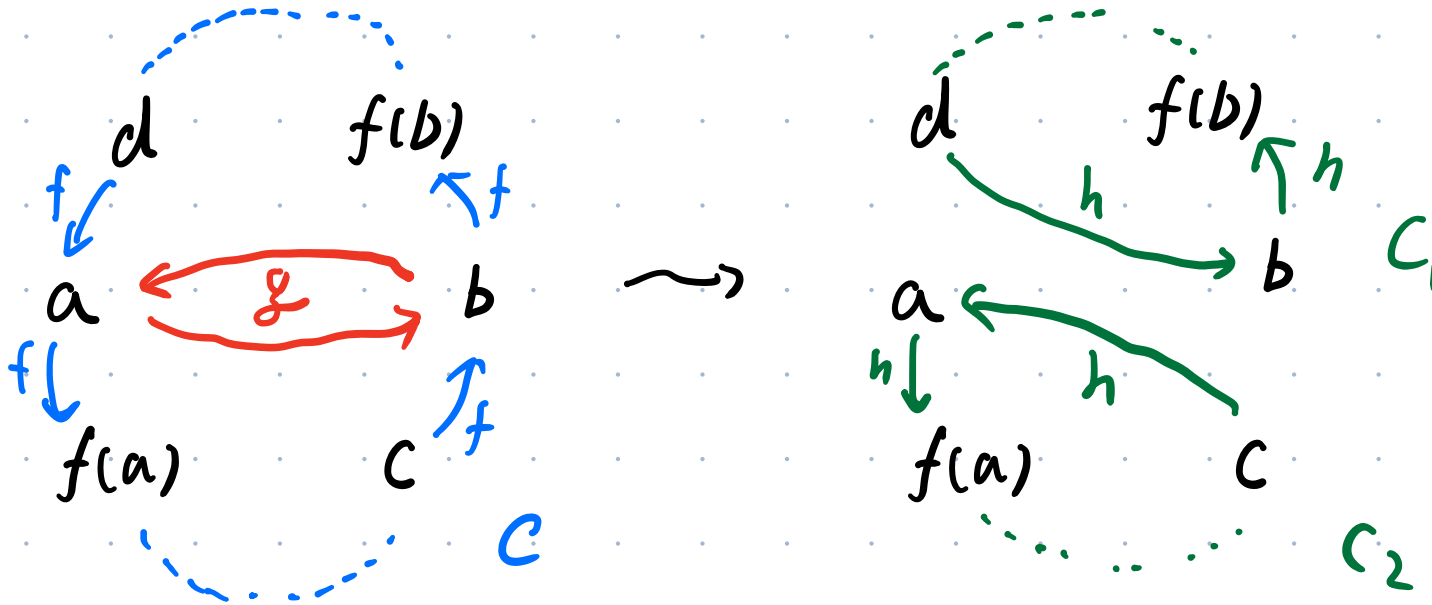
Q: What is the composition of a permutation & a transposition.

$h = g \circ f$ $\quad f$ $\quad g = (a\ b)$

There are two cases: 1) a, b belong to the same cycle of f.

2) a, b belong to different cycles of f.

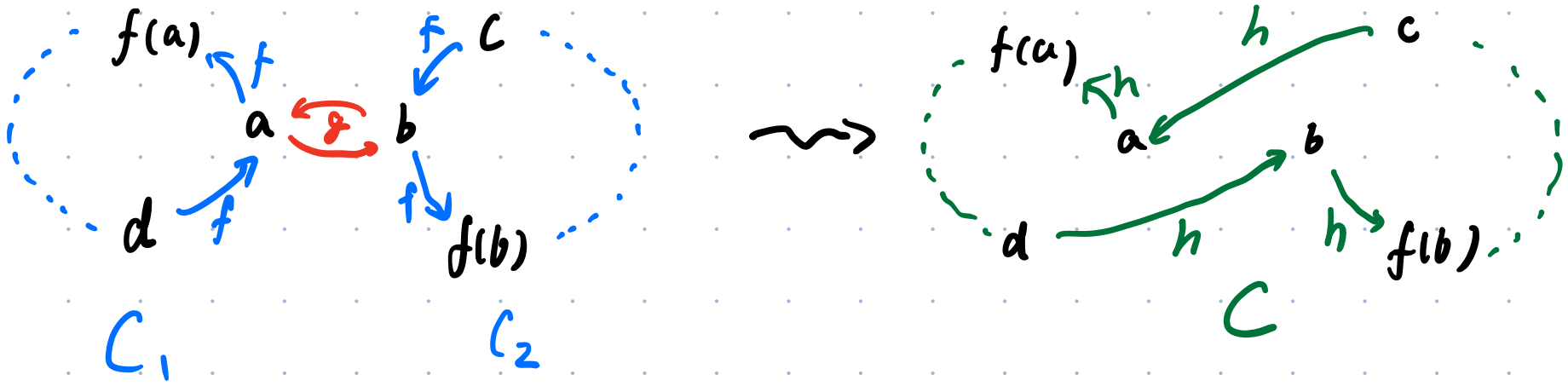
1)



In case 1), composing with g breaks the cycle containing a, b into two cycles.

And Length of C = Length of C_1 + Length of C_2

2)



In case 2), composing with g **merges** the cycles containing a & b resp. into a single one. And Length of C = Length of C_1 + Length of C_2

So what is $\text{sign}(g \circ f) / \text{sign}(f)$?

Case 1: $(-1)^{l-1}$ in $\text{sign}(f)$ becomes $(-1)^{l_1-1}(-1)^{l_2-1}$ in $\text{sign}(g \circ f)$.

Since $l = l_1 + l_2$, we have $\text{sign}(g \circ f) / \text{sign}(f) = -1$.

Case 2: $(-1)^{l_1-1}(-1)^{l_2-1}$ in $\operatorname{sign}(f)$ becomes $(-1)^{l-1}$ in $\operatorname{sign}(g \circ f)$.

Since $l = l_1 + l_2$, we have $\operatorname{sign}(g \circ f) / \operatorname{sign}(f) = -1$.

Lem: Let f be a permutation and g be a transposition of a set S.

Then $$\operatorname{sign}(g \circ f) = -\operatorname{sign}(f).$$

Thm (2nd defn. of sign)

Let S be a finite set and f be a permutation of S.

If f can be written as the composition of n transpositions,

then $\operatorname{sign}(f) = (-1)^n$.

Proof. Let's say $f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_n$ $\quad \tau_i$ are transpositions

Then by the lemma,

$$\begin{aligned} \operatorname{Sign}(f) &= -\operatorname{Sign}(\tau_2 \circ \tau_3 \circ \cdots \circ \tau_n) \\ &= \quad \cdots \quad \cdots \\ &= (-1)^{n-1} \operatorname{sign}(\tau_n) \\ &= (-1)^n. \end{aligned}$$

□

Coro. If f, g are two permutations of S, then

$$\operatorname{Sign}(g \circ f) = \operatorname{Sign}(g)\operatorname{Sign}(f)$$

If $f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_n$, $g = \tau_1' \circ \tau_2' \circ \cdots \circ \tau_m'$, then $g \circ f = \tau_1' \circ \tau_2' \circ \cdots \circ \tau_m' \circ \tau_1 \circ \cdots \circ \tau_n$ (m+n transpositions).

$\operatorname{sign}(g \circ f) = (-1)^{m+n} = (-1)^m (-1)^n = \operatorname{sign}(g) \cdot \operatorname{sign}(f)$.

A finite set S can be identified with a subset of positive numbers by numbering its elements. "linear order" = a bijection from S to $\{1, 2, \cdots, n\}$

$$S = \{a_1, a_2, \cdots, a_n\} \xrightarrow{\sim} \{1, 2, \cdots, n\}$$

e.g. : $a_i \mapsto i$

Defn. Let f be a permutation of S (identified with $\{1, 2, \cdots, n\}$)

An **inversion** of f is a pair (a, b) in S s.t.

$$a < b \quad \text{and} \quad f(a) > f(b).$$

Then $\text{inv}(f) :=$ # inversions of f.

e.g. $S = \{\pi, \mathbb{C}, \text{today}\}$

$\downarrow \quad \downarrow \quad \downarrow$

$\{1, 2, 3\}$

f: $\pi \to \text{today} \to \mathbb{C}$

$(\pi, \mathbb{C})$ is an inversion!

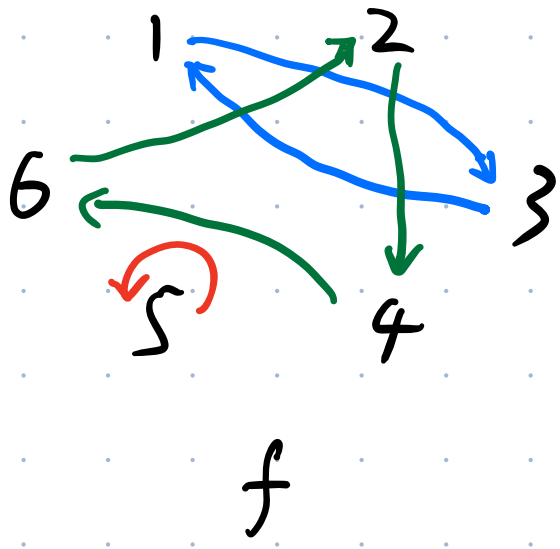
$(\pi, \mathbb{C})$ $\quad \pi < \mathbb{C}$

$1 \quad 2 \qquad 1 < 2$

$(\text{today}, \mathbb{C})$ $\quad \text{today} > \mathbb{C}$

$3 \quad 2 \qquad 3 > 2$

E.g. $S = \{1, 2, 3, 4, 5, 6\}$



f

Fill in $(f(a), f(b))$ for $1 \le a < b \le 6$

a \ b	2	3	4	5	6
1					
2					
3					
4					
5					