Computation in symmetric groups

Tuesday, June 29, 2021 3:29 PM

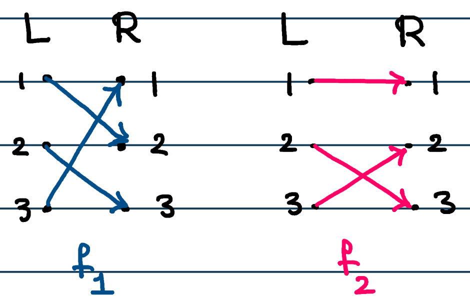
There are different ways to see elements of the symmetric group S_n and do computations in S_n.

Bipartite graphs. Every element is a bijection from $[1..n]$ to $[1..n]$. We can create a (directed) bipartite graph with two sets of vertices labelled by $1, 2, \dots, n$, and we connect i (left) to $f(i)$ (right). For instance

$f_1 : \{1,2,3\} \to \{1,2,3\}$, $f_1(1) = 2$, $f_1(2) = 3$, $f_1(3) = 1$,

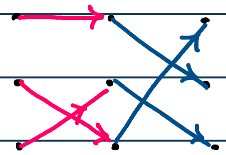
$f_2 : \{1,2,3\} \to \{1,2,3\}$, $f_2(1) = 1$, $f_2(2) = 3$, $f_2(3) = 2$

can viewed as follows



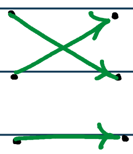
We can connect these graphs to visualize the computation in S_n.

To compute $f_1 \circ f_2$, we identify the right side vertices of f_2 with the left side vertices of f_1.

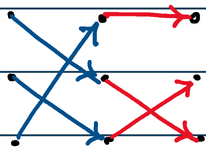


f_2 f_1

and so

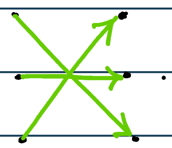


$f_1 \circ f_2$



f_1 f_2

and so



$f_2 \circ f_1$

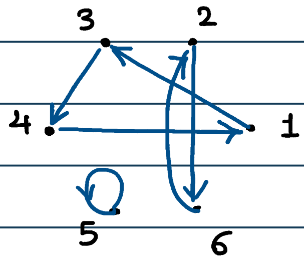
. Instead of using $2n$ vertices, we can use only n vertices.

Computation in symmetric groups

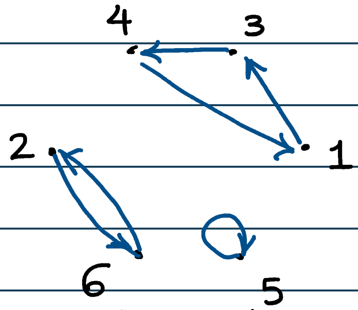
Tuesday, June 29, 2021 3:29 PM

Directed graph. We start with n vertices labelled by $1, 2, \dots, n$, and connect i to $f(i)$. For example

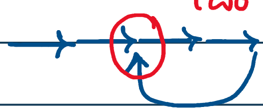
$$f: [1..6] \to [1..6],\ f(1)=3,\ f(2)=6,\ f(3)=4,$$
$$f(4)=1,\ f(5)=5,\ f(6)=2.$$



It looks better if we avoid crossing edges:



Since f is a bijection, the out degree and the in degree of every vertex is 1. We can think of it as a flow. We start with one vertex and follow the flow. At every vertex, there is only one way to go. Because there is only one way to reach to a vertex, we cannot have a path of the form



Two inward edges are not allowed.

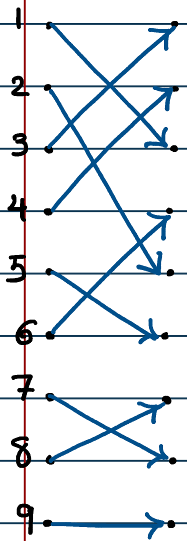
Since there are only finitely many vertices and we cannot go to the middle vertices, at some point we go back to where we have started. This means we get a cycle. Starting with a point outside

Cycle decomposition

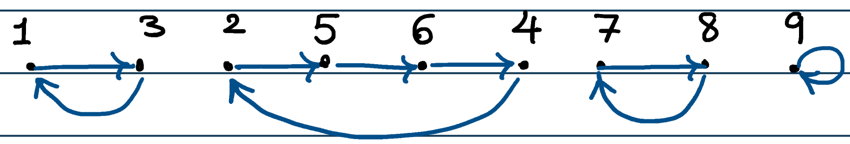
Tuesday, June 29, 2021 3:29 PM

of the 1st loop, the flow never takes us to the 1st loop. This is the case because the in-degree and out-deg. of every vertex in a directed cycle is already 1. Hence the flow gives us disjoint cycles.

Let's see another example: find the cycles of the following permutation.



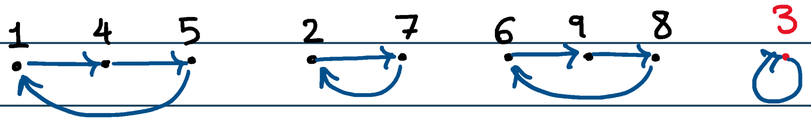
Let's follow the flow:



We use paranthesis to encode cycles. For instance the above permutation is written as $(1,3)(2,5,6,4)(7,8)(9)$. We drop cycles with one vertex. So the above permutation is written as $(1,3)(2,5,6,4)(7,8)$. For instance the directed graph of the following element of S_9 is given here:

$(1,4,5)(2,7)(6,9,8)$

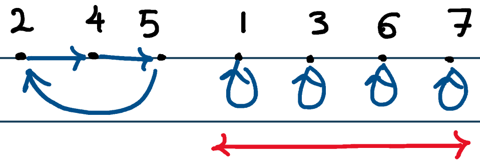
missing number



Cycle decomposition

Tuesday, June 29, 2021 3:29 PM

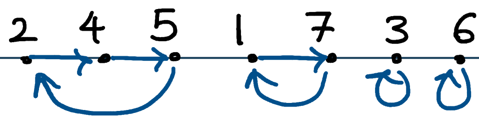
$(2,4,5)$ in S_7 has the following directed graph



numbers that not appear are

fixed under this permutation

And $(2,4,5)(1,7)$ has the following directed graph



A permutation is called a cycle if it is of the form

$$(a_1, a_2, \dots, a_m)$$

for some $a_1, \dots, a_m \in [1..n]$. This means if $f = (a_1, \dots, a_m)$, then $f(a_1) = a_2$, $f(a_2) = a_3$, $\dots$, $f(a_m) = a_1$, $f(a) = a$ if $a \in [1..n] \setminus \{a_1, \dots, a_m\}$.

A cycle of the form $(a_1, \dots, a_m)$ is called an m-cycle, and m is called length of this cycle.

There is only one cycle of length 1 and that is identity.

It is clear that the set of fixed points of a permutation

Fixed points

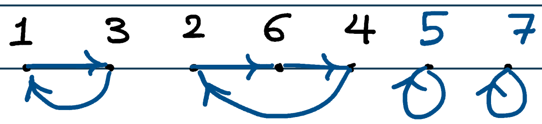
Tuesday, June 29, 2021 3:29 PM

plays an important role in understanding of that permutation.

For $\sigma \in S_n$, let $\mathrm{Fix}(\sigma) := \{ i \in [1..n] \mid \sigma(i) = i \}$.

<u>Example</u> Find $\mathrm{Fix}((1,3)(2,6,4))$ in S_7.

<u>Solution</u>.



missing numbers from $[1..7]$

Hence $\mathrm{Fix}((1,3)(2,6,4)) = \{5,7\}$.

<u>Remark</u>. If we are told that $(1,3)(2,6,4)$ is in S_8, then its set of fixed points is $\{5,7,8\}$.

<u>Example</u>. Suppose $\sigma \in S_n$. Then

$$|\mathrm{Fix}(\sigma)| \geq n-1 \iff \mathrm{Fix}(\sigma) = [1..n] \iff \sigma = \mathrm{id}.$$

<u>Example</u> Suppose m is an integer, $m \geq 2$, and

$$\sigma := (a_1, \ldots, a_m) \in S_n.$$

Then $\mathrm{Fix}(\sigma) = [1..n] \setminus \{a_1, \ldots, a_m\}$.

Let's see a few connections between the group operation in S_n and sets of fixed points. These relations will help us get a better understanding of conjugates and cycles of a permutation.

Fixed points

Tuesday, June 29, 2021 3:29 PM

Lemma. Suppose $\sigma \in S_n$ and $i \in [1..n] \setminus \mathrm{Fix}(\sigma)$. Then $\sigma(i) \in [1..n] \setminus \mathrm{Fix}(\sigma)$.

Pf. Suppose to the contrary that $\sigma(i) \in \mathrm{Fix}(\sigma)$ for some $i \in [1..n] \setminus \mathrm{Fix}(\sigma)$. Then $\sigma(\sigma(i)) = \sigma(i)$. Since σ is injective, we deduce that $\sigma(i) = i$. This means $i \in \mathrm{Fix}(\sigma)$, which is a contradiction. ∎

For $\sigma \in S_n$, $[1..n] \setminus \mathrm{Fix}(\sigma)$ is called the support of σ and it is denoted by $\mathrm{supp}(\sigma)$.

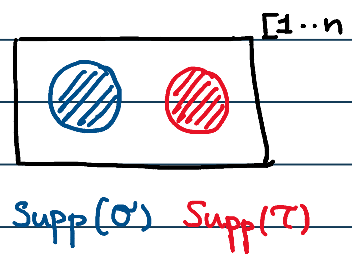
Lemma (disjoint-commute) Suppose $\sigma, \tau \in S_n$ and $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$. Then $\sigma \circ \tau = \tau \circ \sigma$.

Pf. We have to show that, for every $i \in [1..n]$,

$$\sigma(\tau(i)) = \tau(\sigma(i)).$$

Notice that since $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$, there are 3 possibilities:

1. $i \notin \mathrm{Supp}(\sigma)$ and $i \notin \mathrm{Supp}(\tau)$
2. $i \notin \mathrm{Supp}(\sigma)$ and $i \in \mathrm{Supp}(\tau)$
3. $i \in \mathrm{Supp}(\sigma)$ and $i \notin \mathrm{Supp}(\tau)$



In case 1, $i \in \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau)$ and so

Disjoint commuting

Tuesday, June 29, 2021 3:29 PM

$\sigma(\tau(i)) = \sigma(i) = i$ and $\tau(\sigma(i)) = \tau(i) = i$.

Case 2. $i \notin \mathrm{Supp}(\sigma)$ and $i \in \mathrm{Supp}(\tau)$.

Since $i \in \mathrm{Supp}(\tau)$, by the previous lemma $\tau(i) \in \mathrm{Supp}(\tau)$.

Because $\mathrm{supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$ and $\tau(i) \in \mathrm{Supp}(\tau)$, we have $\tau(i) \notin \mathrm{Supp}(\sigma)$. Therefore $\tau(i) \in \mathrm{Fix}(\sigma)$ which means $\sigma(\tau(i)) = \tau(i)$ (I). Notice that $\sigma(i) = i$ as $i \notin \mathrm{Supp}(\sigma)$.
Hence $\tau(\sigma(i)) = \tau(i)$ (II). By (I) and (II),

$$\sigma(\tau(i)) = \tau(\sigma(i)).$$

Case 3. $i \in \mathrm{Supp}(\sigma)$ and $i \notin \mathrm{Supp}(\tau)$.

This is similar to the previous case:

$i \in \mathrm{Supp}(\sigma) \Rightarrow \sigma(i) \in \mathrm{Supp}(\sigma)$ (previous lemma)

$\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset \Rightarrow \sigma(i) \notin \mathrm{Supp}(\tau)$

$\Rightarrow \sigma(i) \in \mathrm{Fix}(\tau)$

$\Rightarrow \tau(\sigma(i)) = \sigma(i)$. (I)

$i \notin \mathrm{Supp}(\tau) \Rightarrow i \in \mathrm{Fix}(\tau) \Rightarrow \tau(i) = i$

$\Rightarrow \sigma(\tau(i)) = \sigma(i)$ (II)

By (I) and (II), $\tau(\sigma(i)) = \sigma(\tau(i))$.

Altogether we have $\sigma(\tau(i)) = \tau(\sigma(i))$ for every i. ∎

Cycle decomposition

Tuesday, June 29, 2021 3:29 PM

Two permutations $\sigma, \tau \in S_n$ are called disjoint if

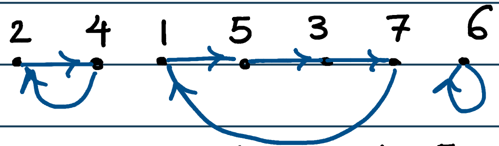
$$\mathrm{supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset.$$

So the previous lemma states that

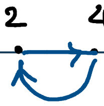
two disjoint permutations commute.

- Let's go back to cycle decomposition of a permutation.

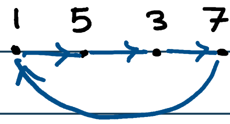
We showed that for a given $\sigma \in S_n$, there is a unique directed graph with vertices labelled by $1, 2, \ldots, n$, which consists of disjoint cycles. To each one of these directed cycles that have at least two vertices we can associate a cycle for instance in



this to



we associate $(2,4)$ and to



we associate $(1,5,3,7)$.

<u>Theorem</u> Every non-identity element of S_n can be written as a product of pairwise disjoint cycles and this decomposition is unique up to reordering the terms.

(This is called a cycle decomposition.)

Cycle decomposition

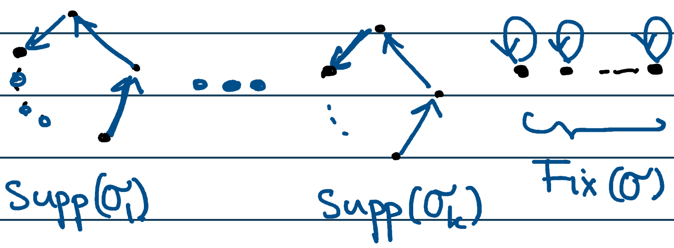
Tuesday, June 29, 2021 3:29 PM

Outline of proof. Suppose the directed graph attached to σ has k disjoint cycles with at least 2 vertices. Let $\sigma_1, \dots, \sigma_k$ be the cycles associated to these disjoint cycles. Notice that $\mathrm{supp}(\sigma_i)$ consists of labels of the i-th cycle of the graph attached to σ. Hence σ_i's are pairwise disjoint.

Claim. $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$.

Pf of Claim. For every $i \in [1..n]$, i can be in at most one of $\mathrm{supp}(\sigma_1), \dots, \mathrm{supp}(\sigma_k)$.

We notice two things



① For every $m \in \mathrm{Supp}(\sigma_j)$,

$\sigma(m) = \sigma_j(m)$,

$\sigma_l(m) = m$ if $l \neq j$, and $\sigma_j(m) \in \mathrm{Supp}(\sigma_j)$

② $m \notin \mathrm{Supp}(\sigma_1) \cup \cdots \cup \mathrm{Supp}(\sigma_k) \iff m \in \mathrm{Fix}(\sigma)$.

Using the above remarks we are going to show that

$\sigma(m) = \sigma_1(\sigma_2(\cdots(\sigma_k(m))\cdots))$ for every $m \in [1..n]$.

- If $m \notin \mathrm{Supp}(\sigma_1) \cup \cdots \cup \mathrm{Supp}(\sigma_k)$, then

Cycle decomposition

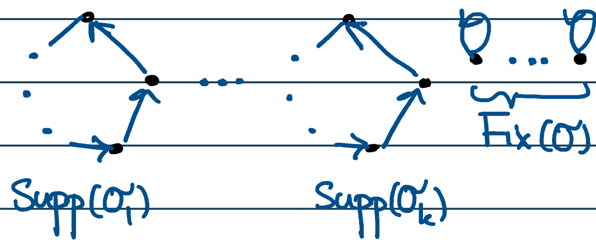
Tuesday, June 29, 2021 3:29 PM

$\sigma_1(m) = m$

$\vdots$

$\sigma_k(m) = m$, and

$\sigma(m) = m$.



Hence $\sigma_1(\cdots(\sigma_k(m))\cdots) = m = \sigma(m)$.

. Suppose $m \in \mathrm{Supp}(\sigma_j)$. Then $\sigma_j(m) \in \mathrm{Supp}(\sigma_j)$. Hence for every $l \neq j$, $m, \sigma_j(m) \in \mathrm{Fix}(\sigma_l)$. Therefore

$$\sigma_1(\cdots(\sigma_j(\cdots(\sigma_k(m))\cdots))\cdots) = \sigma_1(\cdots(\sigma_j(m))\cdots)$$
$$= \sigma_j(m)$$

We have also observed that for $m \in \mathrm{Supp}(\sigma_j)$, $\sigma(m) = \sigma_j(m)$.

Thus $\sigma(m) = (\sigma_1 \circ \cdots \circ \sigma_k)(m)$. The claim follows.

This claim shows that σ can be written as a product of disjoint cycles.

Uniqueness. To show the uniqueness, we discuss that if $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$ where σ_i's are pairwise disjoint cycles, then the directed graph of σ is given by the cycles of σ_i. (Exercise). $\square$

Cycle decomposition

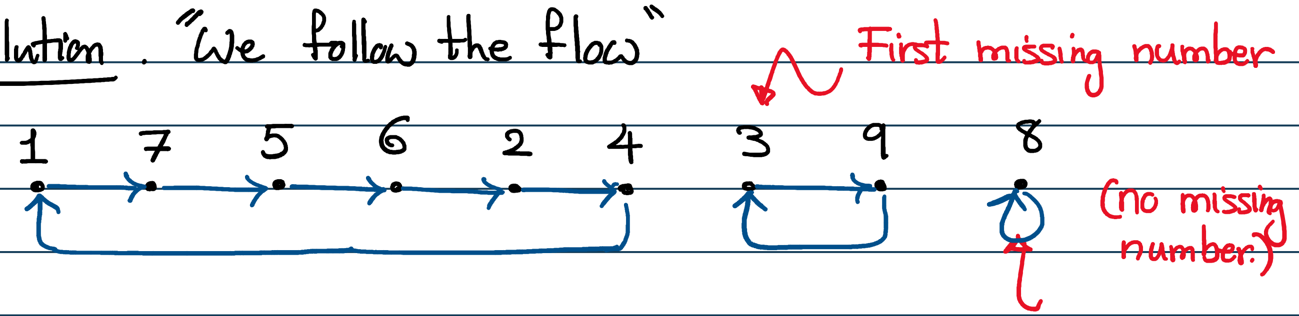
Tuesday, June 29, 2021 3:29 PM

Example. Find a cycle decomposition of $\sigma \in S_9$ where

$\sigma(1) = 7$, $\sigma(2) = 4$, $\sigma(3) = 9$, $\sigma(4) = 1$, $\sigma(5) = 6$,

$\sigma(6) = 2$, $\sigma(7) = 5$, $\sigma(8) = 8$, $\sigma(9) = 3$

Solution. "We follow the flow"



So a cycle decomposition of σ is

First missing number

$$(1,7,5,6,2,4) \circ (3,9).$$

- We drop the $\circ$ symbol when we use the cycle notation.
- We have to be extra careful when we are doing computation in a symmetric group using the cycle notation.

Ex. Find a cycle decomposition of

$$\sigma := (1,3)(2,3,5,1)(4,1,7)$$

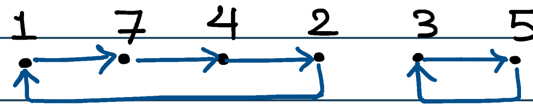
Solution. Again we try to "follow the flow". We have to find $\sigma(1)$. Notice we have to apply cycles from right to left:

$$1 \xmapsto{(4,1,7)} 7 \xmapsto{(2,3,5,1)} 7 \xmapsto{(1,3)} 7.$$

Examples of cycle decomposition

Tuesday, June 29, 2021 3:29 PM

(Recall $\sigma = (1,3)(2,3,5,1)(4,1,7)$.)



$$7 \xmapsto{(4,1,7)} 4 \xmapsto{(2,3,5,1)} 4 \xmapsto{(1,3)} 4.$$

$$4 \xmapsto{(4,1,7)} 1 \xmapsto{(2,3,5,1)} 2 \xmapsto{(1,3)} 2.$$

$$2 \xmapsto{(4,1,7)} 2 \xmapsto{(2,3,5,1)} 3 \xmapsto{(1,3)} 1.$$

first missing

$$3 \xmapsto{(4,1,7)} 3 \xmapsto{(2,3,5,1)} 5 \xmapsto{(1,3)} 5.$$

$$5 \xmapsto{(4,1,7)} 5 \xmapsto{(2,3,5,1)} 1 \xmapsto{(1,3)} 3.$$

Now we have covered all the numbers in the union

$$\{1,3\} \cup \{2,3,5,1\} \cup \{4,1,7\}$$

of the support of cycles. Notice if i is not in these supports it is fixed by σ. Hence

$$\sigma = (1,7,4,2)(3,5). \qquad \blacksquare$$

The next two general examples are extremely useful from both computational and theoretical points of view.

Lemma (Linking) Suppose a_i's are pairwise distinct integers. Then $(a_1, \ldots, a_m)(a_m, a_{m+1}, \ldots, a_n) = (a_1, \ldots, a_n)$

Linking

Tuesday, June 29, 2021 3:29 PM

(If supports of two cycles have exactly one element in common, we can "link" the cycles and get a larger cycle!)

Pf. We only need to focus on the elements in the union of the supports of these cycles; all the other points are fixed. We start with a_1 and "follow the flow".

$$a_1 \xmapsto{(a_m,\dots,a_n)} a_1 \xmapsto{(a_1,\dots,a_m)} a_2$$

$$a_2 \xmapsto{(a_m,\dots,a_n)} a_2 \xmapsto{(a_1,\dots,a_m)} a_3$$

$$\vdots \qquad\qquad \vdots$$

$$a_{m-1} \xmapsto{(a_m,\dots,a_n)} a_{m-1} \xmapsto{(a_1,\dots,a_m)} a_m$$

$$a_m \xmapsto{(a_m,\dots,a_n)} a_{m+1} \xmapsto{(a_1,\dots,a_m)} a_{m+1}$$

$$a_{m+1} \xmapsto{(a_m,\dots,a_n)} a_{m+2} \xmapsto{(a_1,\dots,a_m)} a_{m+2}$$

$$\vdots \qquad\qquad \vdots$$

$$a_{n-1} \xmapsto{(a_m,\dots,a_n)} a_n \xmapsto{(a_1,\dots,a_m)} a_n$$

$$a_n \xmapsto{(a_m,\dots,a_n)} a_m \xmapsto{(a_1,\dots,a_m)} a_1$$

$$a_1 \to a_2 \to \cdots \to a_m \to a_{m+1} \to \cdots \to a_n.$$

This completes the proof. ∎

Using linking relation

Tuesday, June 29, 2021 3:29 PM

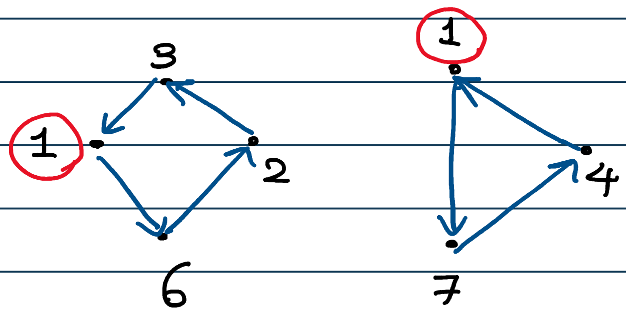
Ex. Find a cycle decomposition of

$$\sigma = (2,3,1,6)\,(4,1,7)$$

Solution. The support of cycles $(2,3,1,6)$ and $(4,1,7)$ have exactly one point in common which is 1. To use the linking relation, we need to have this common element at the end of the first cycle and at the start of the second cycle. Notice that

$(2,3,1,6) = (6,2,9,1)$ and

$(4,1,7) = (1,7,4)$.



Hence $(2,3,1,6)(4,1,7) = (6,2,9,1)(1,7,4)$

(the linking relation) $\overset{\downarrow}{=} (6,2,9,1,7,4)$.

Lemma. (1) $\mathrm{Fix}(\sigma\circ\tau\circ\sigma^{-1}) = \sigma(\mathrm{Fix}(\tau))$, and

$$\mathrm{Supp}(\sigma\circ\tau\circ\sigma^{-1}) = \sigma(\mathrm{Supp}(\tau)).$$

(2) $\sigma\,(a_1, a_2, \dots, a_m)\,\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_m))$.

Pf. (1) $i \in \mathrm{Fix}(\sigma\circ\tau\circ\sigma^{-1}) \iff \sigma\circ\tau\circ\sigma^{-1}(i) = i$

$$\iff \tau(\sigma^{-1}(i)) = \sigma^{-1}(i)$$

Conjugation of cycles

Tuesday, June 29, 2021 3:29 PM

Hence $i \in \mathrm{Fix}(\sigma \circ \tau \circ \sigma^{-1}) \iff \sigma^{-1}(i) \in \mathrm{Fix}(\tau)$

$\overset{\sigma:\text{ bijection}}{\iff} i \in \sigma(\mathrm{Fix}(\tau))$

Therefore $\mathrm{Fix}(\sigma \circ \tau \circ \sigma^{-1}) = \sigma(\mathrm{Fix}(\tau))$.

. Notice that $\mathrm{supp}(\sigma \circ \tau \circ \sigma^{-1}) = [1..n] \setminus \mathrm{Fix}(\sigma \circ \tau \circ \sigma^{-1})$

$= [1..n] \setminus \sigma(\mathrm{Fix}(\tau))$

$\overset{\sigma:\text{ bijection}}{=} \sigma([1..n] \setminus \mathrm{Fix}(\tau))$

$= \sigma(\mathrm{Supp}(\tau))$.

(2) By the first part we know that

$$\mathrm{Supp}(\sigma\,(a_1, \ldots, a_m)\,\sigma^{-1}) = \sigma(\{a_1, \ldots, a_m\})$$

$$= \{\sigma(a_1), \ldots, \sigma(a_m)\},$$

which is the same as the support of $(\sigma(a_1), \ldots, \sigma(a_m))$.

So in order to prove $\sigma\,(a_1, \ldots, a_m)\,\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_m))$ it is enough to show that these permutations send $\sigma(a_j)$ to the same element (for every $1 \le j \le m$). Notice that the cycle $(\sigma(a_1), \ldots, \sigma(a_m))$ sends $\sigma(a_j)$ to $\sigma(a_{j+1})$ (with the understanding that $a_{m+1} = a_1$).

Conjugation

Tuesday, June 29, 2021 3:29 PM

Next we want to see what $\sigma(a_1,\dots,a_m)\sigma^{-1}$ does to $\sigma(a_j)$.

$$\sigma(a_j) \xmapsto{\sigma^{-1}} a_j \xmapsto{(a_1,\dots,a_m)} a_{j+1} \xmapsto{\sigma} \sigma(a_{j+1})$$

(Again $a_{m+1}=a_1$.) So we get the desired equality. ∎

<u>Ex.</u> Suppose $\sigma=(1,2,4)(3,5)$ and

$$\tau=(1,5,6)(2,3,4).$$

Find a cycle decomposition of $\sigma\circ\tau\circ\sigma^{-1}$.

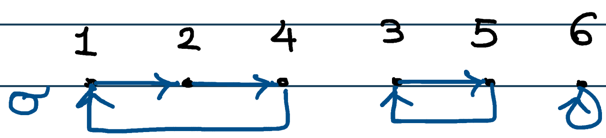
<u>Solution.</u> We know that conjugation by σ is a group homomorphism. So

$$\sigma\circ\tau\circ\sigma^{-1}=(\sigma(1,5,6)\sigma^{-1})(\sigma(2,3,4)\sigma^{-1})$$

previous lemma

$$\begin{aligned}&=(\sigma(1),\sigma(5),\sigma(6))\,(\sigma(2),\sigma(3),\sigma(4))\\ &=(2,3,6)(4,5,1)\end{aligned}$$

And these are disjoint cycles. So we are done. ∎



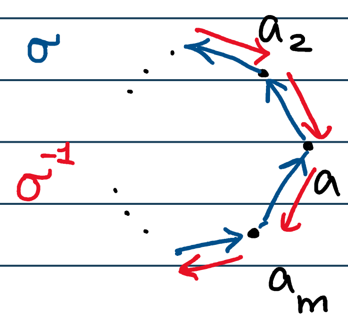
- Can we quickly compute a cycle decomposition of σ if a cycle decomposition of σ is given?

Ex. Suppose $(a_1, \ldots, a_m)$ is an m-cycle. Find a cycle decomposition of $(a_1, \ldots, a_m)^{-1}$.

Solution. Let $\sigma := (a_1, \ldots, a_m)$. Then $\sigma(i) = i$ if i is not in $\{a_1, \ldots, a_m\}$, and so $\sigma^{-1}(i) = i$ if $i \notin \{a_1, \ldots, a_m\}$. For every $1 \le j \le m$, $\sigma(a_j) = a_{j+1}$ (where $a_{m+1} = a_1$). Hence $\sigma^{-1}(a_{j+1}) = a_j$ for every $1 \le j \le m$. Therefore we have

$$a_m \xmapsto{\sigma^{-1}} a_{m-1} \xmapsto{\sigma^{-1}} \cdots \xmapsto{\sigma^{-1}} a_1 \xmapsto{\sigma^{-1}} a_m$$

Hence $\sigma^{-1} = (a_m, a_{m-1}, \ldots, a_1)$.



To find the inverse of a cycle we simply write it "backward".

Ex. Find a cycle decomposition of

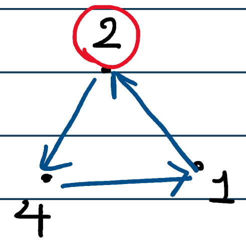
$$(1,2,4)(5,2,7,3)^{-1}.$$

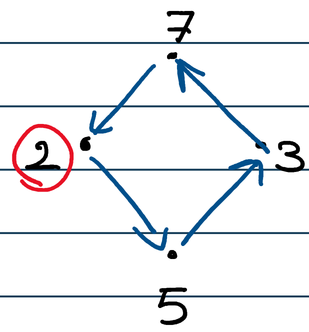
Solution. By the above example $(5,2,7,3)^{-1} = (3,7,2,5)$. Notice that the support of cycles $(1,2,4)$ and $(3,7,2,5)$ have exactly one common point which is 2. So we

Final example

Tuesday, June 29, 2021 3:29 PM

Can use the linking relation. To that end we have to rewrite the first cycle to have 2 at the end and we have to rewrite the second cycle to have 2 at the start.





$(1,2,4) = (4,1,2)$

and $(3,7,2,5) = (2,5,3,7)$. Hence

$$(1,2,4)(3,7,2,5) = (4,1,2)(2,5,3,7)$$

the linking relation $= (4,1,2,5,3,7)$.