Lecture 12

Let S be a set.

Let $\mathrm{Perm}(S)$ be the set of permutations of S.

We know that $\mathrm{Perm}(S)$ is a group under the binary operation of composition.

We will focus on the case in which S is a finite set.

For any positive integer n, we define S_n to be the group of permutations of $\{1, 2, \dots, n\}$.

Array notation

Let $\sigma \in S_n$. Then, we can write σ as a $2 \times n$ array as follows:

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \cdots & \sigma(n) \end{bmatrix}.$$

Example

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

Then, we write

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{bmatrix}$$

This makes it easy to calculate compositions, inverses, etc.

For example,

$$\sigma^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{bmatrix}$$

Suppose

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}.$$

We want to calculate $\sigma \circ \tau$.

$$\sigma \circ \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}$$

<u>Remember</u>: The function on the right acts first.

Order of S_n

Suppose we want to construct a permutation of the set $\{1, 2, \cdots, n\}$. Let us denote the permutation by σ.

We will construct σ by choosing the elements $\sigma(1), \sigma(2), \cdots$

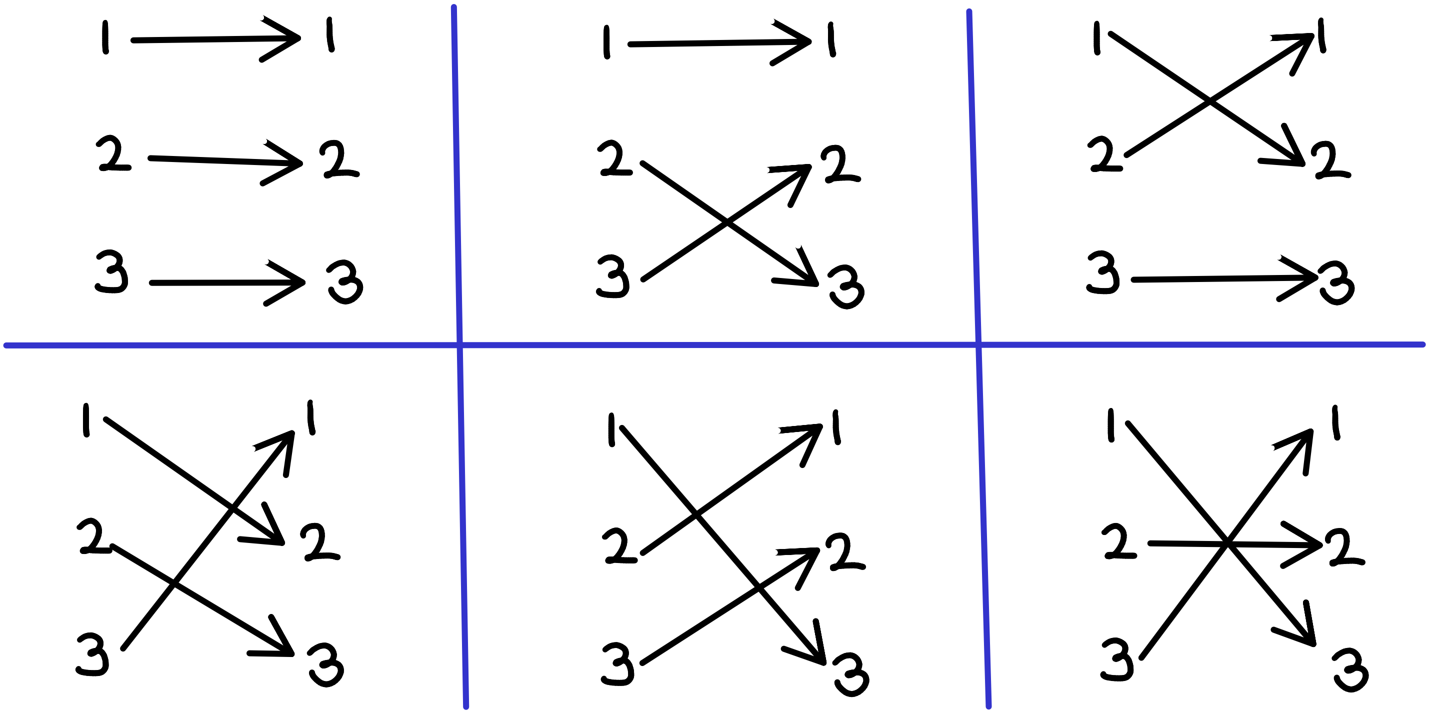
We have n choices for $\sigma(1)$.
After $\sigma(1)$ is chosen, we have $(n-1)$ choices for $\sigma(2)$ as $\sigma(2) \neq \sigma(1)$.
After $\sigma(1)$ and $\sigma(2)$ are chosen, we have $(n-2)$ choices for $\sigma(3)$.

Continuing in this manner, we see that σ can be constructed in $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$ ways.

We call this number the factorial of n, and write it as $n!$. Thus, $|S_n| = n!$

Example

$n = 3$, $|S_3| = 3! = 6$



Cycle decomposition

Let σ be a permutation of $\{1, 2, \cdots, n\}$.

Consider the sequence

$1, \sigma(1), \sigma^2(1), \cdots\cdots$

Since $\operatorname{ord}(\sigma)$ is finite, we know that there exists a positive integer m such that $\sigma^m(1) = 1$.

Let r be the smallest positive integer such that $\sigma^r(1) = 1$.
(Note that we do not need $\sigma^r = \mathrm{id}$, only that $\sigma^r(1) = 1$.
So r may be smaller than $\mathrm{ord}(\sigma)$.)

Thus, the sequence looks like

$$1, \sigma(1), \sigma^2(1), \ldots, \underset{\substack{\uparrow \\ r^{th} \text{ place}}}{1}, \sigma(1), \sigma^2(1), \ldots$$

We claim that the elements $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ are all distinct.

If not, there exist non-negative integers $i < j$ such that $\sigma^{i}(1) = \sigma^{j}(1)$.
Composing with σ^{-i} on both sides, we get $\sigma^{j-i}(1) = 1$.
But $j-i > 0$ and $j-i < r$.
This contradicts the minimality of r.

Thus the elements $1, \sigma(1), \cdots, \sigma^{r-1}(1)$ are all distinct.

In fact the infinite sequence

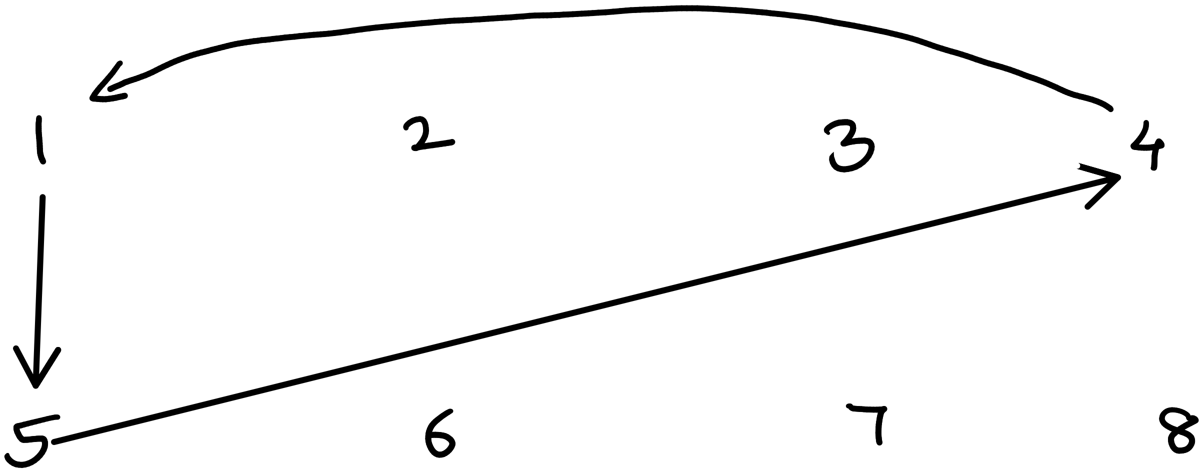
$\cdots \sigma^{-2}(1), \sigma^{-1}(1), 1, \sigma(1), \sigma^{2}(1), \cdots$

consists of the pattern

$1, \sigma(1), \cdots \sigma^{r-1}(1)$ repeating indefinitely (in both directions).

A pictorial representation

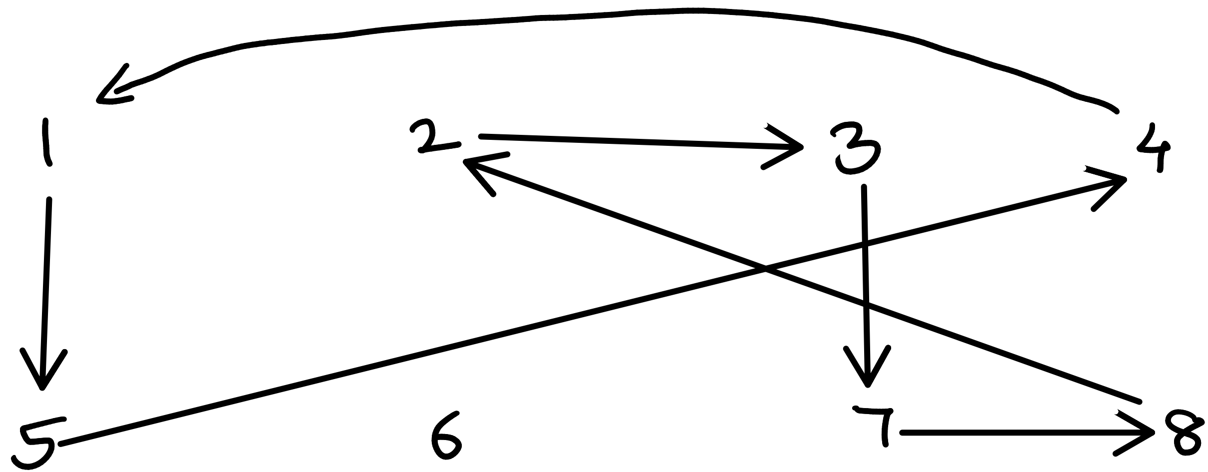
$n = 8$. $\sigma(1) = 5$, $\sigma(2) = 3$, $\sigma(3) = 7$, $\sigma(4) = 1$
$\sigma(5) = 4$, $\sigma(6) = 6$, $\sigma(7) = 8$, $\sigma(8) = 2$



Let $A_1 = \{1, \sigma(1), \cdots \sigma^{r-1}(1)\}$.
If $A_1 \neq \{1, 2, \cdots n\}$, choose some $x \notin A_1$ and repeat the process to obtain a "cycle" $x, \sigma(x), \cdots \sigma^{s-1}(x)$ (for some integer s).
Let $A_2 = \{x, \sigma(x), \cdots \sigma^{s-1}(x)\}$.

In our example, we take $x=2$.

$\sigma(1)=5$, $\sigma(2)=3$, $\sigma(3)=7$, $\sigma(4)=1$
$\sigma(5)=4$, $\sigma(6)=6$, $\sigma(7)=8$, $\sigma(8)=2$



Observe that A_1 and A_2 are disjoint.

If $A_1 \cup A_2 = \{1, 2, \cdots n\}$, we stop. Otherwise, we choose some $y \notin A_1 \cup A_2$ and repeat the process.

This process must end in at most n steps.

Suppose, after p steps, we have disjoint sets $A_1, A_2, \cdots, A_p$ such that σ acts on the elements of each A_i "cyclically".

__Definition__ A permutation σ of a set S is called a cycle if there exists a finite set $A = \{a_1, \cdots, a_r\}$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\cdots$, $\sigma(a_r) = a_1$.

The integer r is called the <u>length of the cycle</u>.

The cycle σ is then written as $(a_1, a_2, \cdots, a_r)$.

Two cycles $(a_1, \cdots, a_r)$ and $(b_1, \cdots, b_s)$ are said to be disjoint if $a_k \neq b_l$ for any k, l.

Recall that we have partitioned the set $\{1, 2, \cdots n\}$ into p disjoint subsets $A_1, \cdots A_p$ such that for each i, $1 \le i \le p$, $A_i := \{a_{i1}, a_{i2}, \cdots a_{ir_i}\}$ and $\sigma(a_{i1}) = a_{i2}$, $\sigma(a_{i2}) = a_{i3}, \cdots$; $\sigma(a_{ir_i}) = a_{i1}$.

Then, we observe that if $\sigma_i = (a_{i1}, a_{i2}, \cdots a_{ir_i})$, then $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p$.

Indeed for any $x \in \{1, 2, \cdots n\}$, there is some i such that $x \in A_i$.

Let us compute $\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p(x)$.

If $j > i$, $\sigma_j(x) = x$.

So $\sigma_{i+1} \circ \cdots \sigma_p(x) = x$.

$\sigma_i(x) = \sigma(x)$

So $\sigma_i \circ \sigma_{i+1} \circ \cdots \circ \sigma_p(x) = \sigma(x)$.

$\sigma(x) \in A_i \Longrightarrow \sigma(x) \notin A_j$ for $j < i$.

So $\sigma_j(\sigma(x)) = \sigma(x)$ for any $j < i$.

So,

$$\sigma_1 \circ \sigma_2 \cdots \sigma_{i-1}(\sigma_i \circ \cdots \sigma_p(x))$$

$$= \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1}(\sigma(x))$$

$$= \sigma(x).$$

Thus $\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p(x) = \sigma(x)$ for any $x \in \{1, 2, \cdots n\}$

So $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p$.

This is called the cycle decomposition of σ.

For example:

$n=8$. $\sigma(1)=5$, $\sigma(2)=3$, $\sigma(3)=7$, $\sigma(4)=1$
$\sigma(5)=4$, $\sigma(6)=6$, $\sigma(7)=8$, $\sigma(8)=2$

Then, $\sigma=(1,5,4)(2,3,7,8)(6)$.

The cycle decomposition of a permutation is unique.

However, a single cycle may be written in multiple ways. For example, $(a,b,c) = (b,c,a)$.

Secondly, <u>disjoint</u> cycles commute. So, they may be composed in any order. (See Gallian, Thm 5.2)

For example,

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

Except for this, it is easy to see that cycle decomposition is unique.

Also, note that a cycle of length 1 is just the identity element.

So, we often choose not to write 1-cycles in a cycle decomposition.

Examples

Elements of S_3:

id, $(1,2)$, $(2,3)$, $(1,3)$, $(1,2,3)$, $(1,3,2)$.

Elements of S_4:

Identity element: id

2-cycles: $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$.

3-cycles: $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$

Products of 2-cycles:

$(1,2)(3,4)$, $(1,4)(2,3)$, $(1,3)(2,4)$.

4-cycles: $(1,2,3,4)$, $(1,2,4,3)$, $(1,3,2,4)$, $(1,3,4,2)$, $(1,4,2,3)$, $(1,4,3,2)$

"Types" of cycle decomposition $\longleftrightarrow$ ways to partition 4.

$4 = 1+1+1+1 = 2+1+1 = 2+2$
$= 3+1$

(More on this later.)

Order of a permutation

Let S be a set.

Let $\sigma = (a_1, \cdots a_m)$ and $\tau = (b_1, \cdots, b_n)$ be disjoint cycles in $\mathrm{Perm}(S)$. Then, we will prove that $\mathrm{ord}(\sigma\tau) = \mathrm{lcm}(m, n)$.

Let $A = \{a_1, \dots a_m\}$,

$B = \{b_1, \dots, b_n\}$ and $C = S \setminus (A \cup B)$.

So, S is the <u>disjoint</u> union

of A, B and C.

Let r be an integer.

Then, $(\sigma\tau)^r = id \Leftrightarrow (\sigma\tau)^r(x) = x$

for all $x \in S$.

$*$ Observe that if $x \in A$,
$(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x)$.

Also, note that in this case $\sigma(x) \in A$.

So $(\sigma\tau)^2(x) = (\sigma\tau)(\sigma\tau(x))$
$= (\sigma\tau)(\sigma(x))$
$= \sigma(\sigma(x))$ (Apply $(*)$ to $\sigma(x)$.)

Continuing in this manner, we see that $(\sigma\tau)^k(x) = \sigma^k(x)$ for any positive integer.

So, $(\sigma\tau)^r(x) = x \iff \sigma^r(x) = x$

$$\iff m \mid r.$$

Similarly, if $x \in B$, we see that $(\sigma\tau)^r(x) = x \iff n \mid r$.

If $x \in C$, $\sigma(x) = x$ and $\tau(x) = x$.

So, in that case $(\sigma\tau)^r(x) = x$

for any r.

Thus $(\sigma\tau)^r(x) = x$ for <u>all</u> x

$\iff$ $m \mid r$ and $n \mid r$.

The smallest positive r with this property is $\operatorname{lcm}(m, n)$.

More generally, with this argument we can prove:

<u>Theorem</u> Let S be a finite set and let $\sigma \in \mathrm{Perm}(S)$. If $\sigma = \sigma_1 \circ \cdots \circ \sigma_p$ is the cycle decomposition of σ, where σ_i is a cycle of

length n_i, then

$ord(\sigma) = lcm(n_1, n_2, \ldots, n_p)$.

Example

$n = 10$.

$\sigma = (1, 4, 7, 2, 9, 3)(5, 8, 6, 10)$.

Then, $ord(\sigma) = lcm(6, 4) = 12$.