Lecture 14

Reference: Judson, Chapter 5

Permutation group

Cycles factorization

Recall a definition.

Definition 1: Independent cycles

We say that cycles $\sigma = (i_1, \ldots, i_k)$ and $\mu = (j_1, \ldots, j_l)$ are *independent* if

$$\{i_1, \ldots i_k\} \cap \{j_1, \ldots, j_k\} = \varnothing.$$

i.e., the sets of elements, which they cyclically permute, do not intersect.

The following proposition is obvious.

Proposition 1

If cycles σ and μ are independent, then they commute:

$$\sigma \circ \mu = \mu \circ \sigma.$$

Remark 1

If cycles are not independent, then might not commute, for example for cycles of length two $(1,2)$ and $(2,3)$ in S_3 we have (remember composing from right to left!)

$$(1,2)(2,3) = (3,1,2)$$

while

$$(2,3)(1,2) = (2,1,3)$$

are two different cycles of length 3.

Theorem 1: Factorization into independent cycles

If $\sigma \in S_n$ is any permutation, then there exist a collection of mutually independent cycles $\mu_1, \ldots, \mu_l \in S_n$ such that

$$\sigma = \mu_1 \circ \mu_2 \cdots \circ \mu_s.$$

Proof. Start with any element a in $\{1, 2, \ldots, n\}$ which is not fixed by σ. Consider iterations

$$a \mapsto \sigma(a) \mapsto \sigma^2(a) \mapsto \ldots \sigma^k(a) \mapsto \ldots.$$

At some step l_1 we again encounter a. Denote the corresponding cycle as

$$\mu_1 = (a, \sigma(a), \ldots, \sigma^{l_1 - 1}(a))$$

Then μ_1 and σ act in the same way on all the elements $\{a, \sigma(a), \ldots, \sigma^{l_1-1}(a)\}$ (equivalently $\mu_1^{-1} \circ \sigma$ fix these elements).
Pick another element $b \in \{1, \ldots, n\}$ not fixed by $\mu_1^{-1} \circ \sigma$, and repeat the procedure, identifying new cycle μ_2. This cycle will be independent with μ_1, and now $\mu_2^{-1} \circ \mu_1^{-1} \circ \sigma$ fixes even more elements then $\mu_1^{-1} \circ \sigma$.
Iterate this procedure, until we end up with the permutation $\mu_s^{-1} \circ \cdots \circ \mu_2^{-1} \circ \mu_1^{-1} \circ \sigma$ which fixes all the elements. It means that this permutation is the identity permutation, thus

$$\sigma = \mu_1 \ldots \mu_s$$

is the factorization of σ into independent cycles, as claimed. □

Example 1

Consider

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

Then following the above procedure we find a factorization

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

Remark 2

Factorization into independent cycles is unique up to a reordering of μ_i's.

Factorization into independent cycles comes in handy, when we need to find the order of a given permutation.

Theorem 2: Order of permutation

1. If μ is a cycles of length l, then order of μ is l.
2. If $\sigma = \mu_1 \dots \mu_s$ is a factorization of σ into independent cycles of length $l_1, \dots, l_s$, then the order of σ is $\mathrm{lcm}(l_1, \dots, l_s)$.

Proof. 1. If $\mu = (i_1, \dots, i_l)$ is a cyclic permutation of $\{i_1, \dots, i_l\}$, then for any $k < l$ we have

$$\mu^k(i_1) = i_{k+1} \neq i_1,$$

thus μ^k cannot be identity for $k < l$. On the other hand, after l iterations of μ each of the elements $i_1, \dots, i_l$ makes a full circle, returning back to its place, thus $\mu^l = id$.
2. Let $L := \mathrm{lcm}(l_1, \dots, l_s)$. First we check that $\sigma^L = id$. Using the fact (identity * below) that independent cycles commute with each other, we find:

$$\sigma^L = (\mu_1 \dots \mu_s)^L \overset{*}{=} \mu_1^L \dots \mu_s^L = id,$$

where in the last identity we used the fact that each $\mu_i^L = id$ as $\mathrm{length}(\mu_i) \mid L$.
Finally it remains to check that if $d < \mathrm{lcm}(l_1, \dots, l_s)$, then $\sigma^d \neq id$. Indeed, since $d < L$ we have that one of the lengths l_i of μ_i does not divide d. But then σ^d does not fix elements of cycles μ_i and cannot be identity. □

Example 2

The order of permutation

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

is $\mathrm{lcm}(3,2) = 6$.

Problem 1: Find all possible orders of elements of S_7.