Lecture 13

Reference: Judson, Chapter 5

Permutation group

Let X be a finite set. For concreteness rename its elements so that

$$X = \{1, 2, \dots, n\}.$$

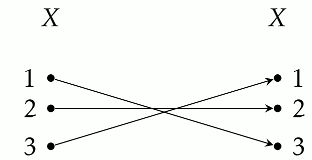
Recall that $\mathcal{B}(X)$ denotes the set of all bijections (or *shuffles* of X)

$$f : X \to X.$$

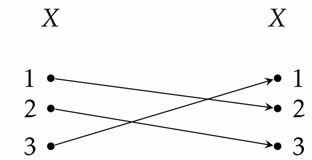
Example 1: $n = 3$

Below are diagrams of two bijections $f_1 : X \to X$ and $f_2 : X \to X$ for $X = \{1, 2, 3\}$.

f_1 :

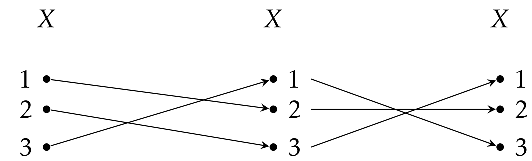


f_2 :

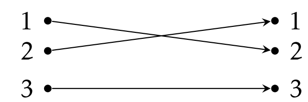


Given two maps $f_1 : X \to X$ and $f_2 : X \to X$ we can compose them in any order we like. In terms of mapping diagrams as above this amounts to *stacking* the together. For instance $f_1 \circ f_2$ (first f_2, then f_1 — right to left, as usual with compositions) has the mapping diagram as follows

$f_1 \circ f_2$:



$f_1 \circ f_2$:



Problem 1: Find the mapping diagram of $f_2 \circ f_1$ and verify that $f_2 \circ f_1 \neq f_1 \circ f_2$.

The set of bijections $\mathcal{B}(X)$ together with the composition operation form a group. Traditionally it is denoted by S_n, where $n = |X|$ is the cardinality of X, and its elements (bijections of X) are denoted by Greek letters $(\sigma, \tau, \mu, \dots)$.

Definition 1: Permutation group

Permutation group S_n of the set $X = \{1, 2, \dots, n\}$ is the set of all bijections

$$\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots n\}$$

endowed with the composition operation.

Specifying elements of S_n.

The most straightforward way to specify an element σ of S_n is to encode all the images $\sigma(i)$ of individual elements $1 \leqslant i \leqslant n$. It is convenient to store this data in a table of size $2 \times n$:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

For example map f_2 from above would be

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Problem 2: Consider a permutation σ given by a table

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Prove that the table of σ^{-1} is obtained from

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

by reordering its columns according to the top values in the first row.

The neutral element of S_n is given by the "trivial" table

$$id = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Proposition 1

$|S_n| = n!$, where $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$.

Proof. To specify the number of bijections $\sigma\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ we need to

1. set $\sigma(1)$ — we have n choices for it (any element of $\{1, 2, \dots, n\}$)
2. set $\sigma(2)$ — we have $(n-1)$ choices left (any element of $\{1, 2, \dots, n\}$ except for $\sigma(1)$, since σ is bijective)
3. …

n. set $\sigma(n)$ — we have exactly one choice left (the unique element other that $\sigma(1), \sigma(2), \dots, \sigma(n-1)$).

Overall this gives $n \cdot (n-1) \cdot \dots \cdot 1 = n!$ options. □

Cycles

Definition 2: Cycle

Permutation $\sigma \in S_n$ is called as cycle of length $k \geqslant 2$, if there exist k distinct elements $i_1, \dots, i_k \in \{1, 2, \dots n\}$ such that σ *cyclically rotates* $i_1, \dots, i_k$:

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \xrightarrow{\sigma} \dots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1,$$

and all the remaining elements are kept in place.

For σ as above, we will use a shorthand

$$\sigma = (i_1, i_2, \dots i_k).$$

This presentation is clearly not uniques, as we can also write the same σ as

$$\sigma = (i_2, i_3, \dots i_k, i_1).$$

Example 2

Element $\sigma \in S_3$

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

is a cycle of length 2, as it cyclically permutes 1 and 3.
On the contrary element $\tau \in S_4$

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

is not a cycle, since it *simultaneously* swaps 1 with 3 and 2 with 4.

Definition 3: Independent cycles

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

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

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

The following proposition is obvious.

Proposition 2

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

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

Theorem 1: Factorization into independent cycles

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

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

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

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

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

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

Then μ_1 and σ act in the same way on all the elements $\{a, \sigma(a), \dots, \sigma^{l_1-1}(a)\}$ (equivalently $\mu_1^{-1} \circ \sigma$ fix these elements).
Pick another element $b \in \{1, \dots, n\}$ 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 the permutation σ is decomposed into a product of independent cycles. □

Example 3

Consider

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

The following the above procedure we find a factorization

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

Remark 1

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