Summary on Lecture 20, May 26th, 2015

The Symmetric Group.

Recall that a set G is a group if there is a binary operation $(g_1, g_2) \mapsto g_1 \circ g_2$ called a *product* satisfying the folllowing properties:

(1) For all elements $g_1, g_2 \in G$, $g_1 \circ g_2 \in G$ (Closure of G under the operation).
(2) For all elements $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ (The Associative property).
(3) There exists $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$ (Existence of the identity).
(4) For each $g \in G$ there exists $\bar{g} \in G$ such that $g \circ \bar{g} = \bar{g} \circ g = e$ (Existence of Inverses).

We already know few examples of groups:

- $(G, \circ) = (\mathbf{Z}, +)$, where $e = 0 \in \mathbf{Z}$, and the inverse of n is $-n$.
- $(G, \circ) = (\mathbf{Z}_n, +)$, where again $e = 0 \in \mathbf{Z}_n$.
- Let p be a prime, and $\mathbf{Z}_p^* = \{1, 2, \ldots, p-1\}$. Then $(G, \circ) = (\mathbf{Z}_p^*, *)$, the multiplicative group of $\mathbf{Z}_p$ (where we exclude 0). Here $e = 1 \in \mathbf{Z}_p^*$, and $a * b \equiv ab \bmod p$. Clearly there the inverses exist since p is a prime.

The above examples are such that $g_1 \circ g_2 = g_2 \circ g_1$ for any elements $g_1, g_2 \in G$. Such groups are called *abelian*.

Theorem 1. Let $(G, \circ)$ be a group. Then

(a) The identity $e \in G$ is unique.
(b) The inverse of each element is unique.
(c) If $g_1, g_2, h \in G$ and $g_1 \circ h = g_2 \circ h$, then $g_1 = g_2$.
(d) If $g_1, g_2, h \in G$ and $h \circ g_1 = h \circ g_2$, then $g_1 = g_2$.

Exercise. Prove Theorem 1.

Symmetric group. Let $S = \{1, \ldots, n\}$ be the set of first n natural numbers. A bijection map $\sigma : S \to S$ is called a *permutation*. We denote $\sigma(i)$ the image of the integer i. It is convenient to describe a permutation as follows:

$$\sigma = \begin{pmatrix} 1 & \cdots & i & \cdots & n \\ \sigma(1) & \cdots & \sigma(i) & \cdots & \sigma(n) \end{pmatrix}$$

We define the symmetric group S_n as the set of all bijections $\{\sigma : S \to S\}$, where the operation $\sigma \circ \tau$ is given by the composition

$$\tau \circ \sigma : S \xrightarrow{\sigma} S \xrightarrow{\tau} S$$

Consider the case $n = 4$. Let

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

We see that

$$\tau : 2 \mapsto 3, \quad \tau : 3 \mapsto 4, \quad \tau : 4 \mapsto 2, \quad \tau : 1 \mapsto 1.$$

We obtain:

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

We can easily write the inverse of σ:

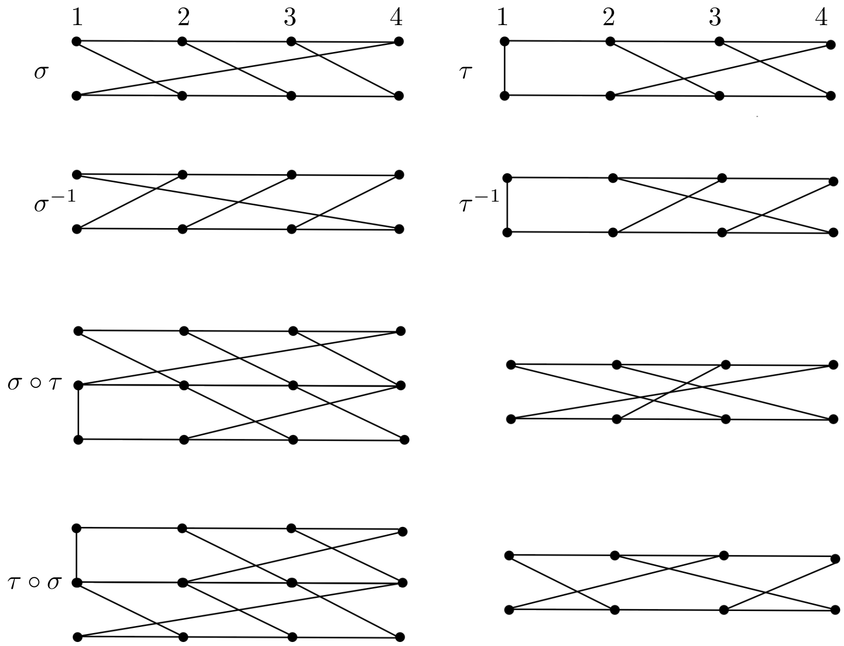
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \text{or} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

It is easy to compute the product $\sigma \circ \tau$:

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

Clearly, $\sigma \circ \tau \neq \tau \circ \sigma$. Thus the groups S_n are non-commutative for $n \geq 3$. We also note that there are $n!$ elements in the group S_n.

The groups S_n are rather complicated; futhermore, every finite group G could be realized as a subgroup of S_n for an appropriate n. We will analyze only basic structural properties of the symmetric groups. Firts, we would like to introduce a *geometric way* to present elements of S_n. Here we display the above elements $\sigma, \tau, \sigma^{-1}, \tau^{-1} \in S_4$ and the products $\sigma \circ \tau$ and $\tau \circ \sigma$:



Definition. Let $\{n_1, \dots, n_s\} \subset \{1, \dots n\}$ be a subset. A map

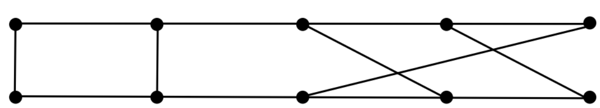
$$\sigma : \{1, \dots n\} \to \{1, \dots n\}$$

is a *cycle* (denoted by $(n_1, \dots, n_s)$) if

$$\sigma : n_1 \mapsto n_2 \mapsto \cdots n_s \mapsto n_1, \quad \text{and} \quad \sigma(i) = i, \quad \text{if} \quad i \notin \{n_1, \dots, n_s\}.$$

Here are the examples of the cycles $(3,4,5) \in S_5$, $(1,4,2,6,3) \in S_6$:

$(3,4,5) \in S_5$



$(1,4,2,6,3) \in S_6$