Abstract Algebra to Linear Algebra

Ji, Yong-hyeon

October 27, 2025

We cover the following topics in this note.

- Symmetric Group

Symmetric group on a set

Definition. Let X be a set. The **symmetric group on** X is the group

$$S_n := \left\{\sigma \in X^X : \sigma \text{ is bijective}\right\}$$

whose elements are all bijections $\sigma : X \to X$ and whose group operation is composition of functions:

$$(\sigma \circ \tau)(x) := \sigma\big(\tau(x)\big) \quad \text{for all } x \in X.$$

The identity element is the identity map id_X, and the inverse of σ is its inverse bijection σ^{-1}.

Transpositions generate. S_n is generated by transpositions (permutations that swap two elements and fix the rest), and in fact by the adjacent transpositions $s_i = (i\ i{+}1)$ for $i = 1, \dots, n-1$.

Presentation. A standard presentation is

$$S_n \cong \left\langle s_1, \dots, s_{n-1} \;\middle|\; \begin{array}{ll} s_i^2 = 1 & \text{for } i = 1, \dots, n-1, \\ s_i s_j = s_j s_i & \text{for } |i-j| \geq 2, \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} & \text{for } i = 1, \dots, n-2 \end{array} \right\rangle.$$

Cycle notation. Elements of S_n are often written in cycle notation; composition is right-to-left by convention.

Cycle decomposition in S_n

Proposition. *Let $n \in \mathbb{N}$ and let $\sigma \in S_n$ act on the set $\{1, \ldots, n\}$. Then*

1. *There exist cycles $c_1, \ldots, c_k$ with pairwise disjoint supports such that*

$$\sigma = c_1 c_2 \cdots c_k,$$

where each c_i is a cycle of length ≥ 2; fixed points of σ may be included as 1-cycles or omitted.

2. *The cycles $c_1, \ldots, c_k$ commute (because they are disjoint), and the multiset $\{c_1, \ldots, c_k\}$ is uniquely determined by σ up to reordering of the cycles and cyclic permutation (rotation) of the entries within each cycle.*

Proof. Consider the action of the cyclic subgroup $\langle \sigma \rangle$ on $\{1, \ldots, n\}$. This partitions $\{1, \ldots, n\}$ into disjoint orbits. For each orbit $O = \{x, \sigma(x), \ldots, \sigma^{m-1}(x)\}$ (with $m \geq 1$ minimal such that $\sigma^m(x) = x$), define the cycle

$$c_O := (\, x \; \sigma(x) \; \sigma^2(x) \; \cdots \; \sigma^{m-1}(x)\,).$$

If $m = 1$ then x is a fixed point and c_O is a 1-cycle. The supports of the c_O are precisely the distinct orbits, hence pairwise disjoint, and thus the cycles commute.

For any y in an orbit O, we have $c_O(y) = \sigma(y)$ by construction, while for $y \notin O$, $c_O(y) = y$. Therefore the product over all orbits,

$$\prod_O c_O,$$

acts on each $y \in \{1, \ldots, n\}$ exactly as σ does; hence $\sigma = \prod_O c_O$. This proves existence.

For uniqueness, suppose $\sigma = d_1 \cdots d_r$ is another product of pairwise disjoint cycles (allowing 1-cycles). Each d_j permutes a subset that is a union of $\langle \sigma \rangle$-orbits, but since d_j is a single cycle, that subset must be exactly one orbit of $\langle \sigma \rangle$. Thus every d_j coincides with the corresponding c_O up to cyclic rotation of its entries. Because disjoint cycles commute, the product is independent of the order of the cycles. Hence the decomposition is unique up to reordering of cycles and rotation within cycles. □

References

[1] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 27. 추상대수학에서 선형대수학으로 : 대칭군과 행렬식의 정의 symmetric group and def of determinant" YouTube Video, 27:07. Published October 29, 2019. URL: `https://www.youtube.com/watch?v=UIlC9ikSpNc&t=1026s`.