Lecture Notes for Abstract Algebra: Lecture 9

1 Symmetric groups

1.1 Permutation groups: symmetric and alternate groups

We write S_n for the for the set of permutations (bijective maps $X \longrightarrow X$, where $X = \{1, 2, \dots, n\}$. This group is called the symmetric group on n letters.

Proposition 1. *The symmetric group on n letters, S_n, is a group with $n!$ elements, where the binary operation is the composition of maps.*

Proof. The identity element is the function $\mathrm{id}\colon X \longrightarrow X$ sending $i \mapsto i$ for all elements $1 \leq i \leq n$. The maps $f\colon X \longrightarrow X$ are bijective and therefore admit inverse $f^{-1}\colon X \longrightarrow X$. On the other hand, the image of an element $i \in X = \{1, 2, \dots, n\}$ must be an element in that set (not assigned as image of any $j \neq i$, hence the number of elements). □

Definition 2. A cycle of length k is an element of S_n of order k. A cycle of length k is therefore an element $\sigma \in S_n$ such that, for some $a_1, a_2, \dots, a_k \in S_n$, we have:

$$\sigma(a_1) = a_2, \qquad \sigma(a_2) = a_3, \quad \dots, \quad \sigma(a_k) = a_1.$$

A cycle of order 2 is called a transposition.

Example 3. In S_7, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1\,6\,2\,3\,5\,4\,1),$$

is a cycle of length 6. On the other hand, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\,2\,4\,3)(5\,6),$$

is a product of two disjoint cycles.

Proposition 4. *Two disjoint cycles commute in S_n*

Proof. Let $\sigma = (a_1\,a_2 \dots a_k)$ and $\sigma' = (b_1\,b_2 \dots b_l)$. If $a_i \in \{a_1, a_2, \dots, a_k\}$, then $a_i \notin \{b_1, b_2, \dots, b_l\}$ and $\sigma \circ \sigma'(a_i) = \sigma(a_i) = \sigma' \circ \sigma(a_i)$. We proceed similarly for $b_j \in \{b_1, b_2, \dots, b_l\}$. □

Theorem 5. *Every permutation $\sigma \in S_n$ can be written as product of disjoint cycles.*

Proof. Take the set $X_1 = \{1, \sigma(1), \dots \sigma^k(1) \dots\}$. The set X_1 is a finite set and we can find the first element i such that $i \notin X_1$. Now, consider the set $X_2 = \{i, \sigma(i), \sigma^k(i), \dots\}$, also a finite set. Since the set X is finite, this process will end with the selection of disjoint sets $X_1, \dots, X_r$ and we can build cycles:

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i \end{cases},$$

in such a way that $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$ is the product of r disjoint cycles. $\square$

Example 6. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

Then $\sigma = (1\,12\,8\,10\,4)(2\,13)(3)(5\,11\,7)(6\,9)$ and we do not include the cycle (3) in the notation. Hence $\sigma = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$

Remark 7. For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} can be obtained by writing the numbers on the cycles in the reverse order. In the previous example, we will have:

$$\sigma = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9) \quad \text{and} \quad \sigma^{-1} = (4\,10\,8\,12\,1)(13\,2)(7\,11\,5)(9\,6).$$

Remark 8. For a cycle $\sigma = (a_1\ \dots a_m)$ we have $\sigma^n(a_i) = a_{i+n \bmod m}$.

Remark 9. Any permutation can be expressed as product of transposition. A cycle of length k, for example, can be written as product of $k-1$ transpositions:

$$(a_1\,a_2 \dots a_k) = (a_1\,a_2)(a_2\,a_3)\dots(a_{k-1}\,a_k).$$

This is representations is however not unique for instance, the identity (1) in S_4 is also $(1) = (1\,3)(3\,1)(2\,4)(4\,2)$.

Remark 10. The order of a permutation is the lcm of the lengths of the cycles in the cycle decomposition.

Lemma 11. *If the identity is expressed as the product $id = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r$ of transpositions τ_i, then r is an even number.*

Proof. The proof is done by induction on the number r of transpositions. Clearly $r > 1$. If $r = 2$, we are done. Otherwise, we have the following cases for the product of the last two transpositions $\tau_{r-1} \circ \tau_r$:

$$\begin{aligned} (a\,b)(a\,b) &= \text{id} \\ (b\,c)(a\,b) &= (a\,c)(b\,c) \\ (c\,d)(a\,b) &= (a\,b)(c\,d) \\ (a\,c)(a\,b) &= (a\,b)(b\,c) \end{aligned}$$

where a, b, c, d are distinct numbers. We are going to pay attention to the movement of a in this product of transpositions. By doing one of the above transformations, we can either reduce the length by two and we are done by induction or move a to the $r-1$ transposition, but not in the last one. Continuing in this way, either we finish by induction or manage to move a to only the first transposition τ_1 which will contradict the fact that the identity fixes a. □

Proposition/Definition 12. *A permutation σ_n is even when it can be expressed as $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_n$, for transpositions τ_i and n is even. Otherwise is said to be odd. The group A_n is the subgroup of S_n of even permutations of n elements.*

Proof. We need to check the following properties:

1. The product of two even permutations is again an even permutation.

2. The inverse of an even permutation is again even:

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_r \Rightarrow \sigma^{-1} = \sigma_r \circ \cdots \circ \sigma_1.$$

3. The identity id is an even permutation.

□

1.2 Cycle types and conjugacy classes

Definition 13. The cycle type of a permutation $\sigma \in S_n$ is the unordered sequence of $i_1, i_2, \ldots$ specifying the number of cycles i_j of size j.

Example 14. For $\sigma = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$, the cycle type will be $(1, 2, 1, 0, 1)$ or $i_1 = 1, i_2 = 2, i_3 = 1, i_4 = 0$ and $i_5 = 1$. Observe that

$$\sum_j j \cdot i_j = 1 + 4 + 3 + 5 = 13.$$

Proposition 15. *Two permutations in S_n are conjugate if and only if they have the same cycle type.*

Proof. The idea here is that if a permutation α sends x to y, then conjugating α by σ gives a permutation that sends $\sigma(x)$ to $\sigma(y)$. The reason for this is because:

$$(\sigma\alpha\sigma^{-1})(\sigma(x)) = \sigma(\alpha(x)) = \sigma(y)$$

Suppose that we have a permutation α and the cycle $(a_1\, a_2 \ldots\, a_n)$ as part of the cycle decomposition. Conjugation by σ sends this cycle of the permutation to an equivalent cycle, where all the elements of the cycle are replaced by their images under σ. In other words:

$$\sigma(a_1\, a_2\, \ldots\, a_n)\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\, \ldots\, \sigma(a_n))$$

Thus, the lengths of the cycles in the cycle decomposition remain unaffected, so the number of cycles of each length remains unaffected.

Suppose that the cycle type is the same. Construct a bijection between cycles in the first permutation and cycles in the second, such that the bijection matches cycles of the same size. Note that such a bijection is not necessarily unique. For a pair of cycles $(a_1\, a_2\, \ldots\, a_n)$ and $(b_1\, b_2\, \ldots\, b_n)$, define $\sigma(a_i) = b_i$. Note that since we can write a cycle to begin with any element, the choice of σ is not necessarily unique. In any case, a σ chosen in this way conjugates the first permutation to the second permutation.

□

Practice Questions:

1. Find all possible cycle decompositions for elements in S_3. Determine the size of the conjugacy classes.