QUICK NOTES ON PERMUTATION GROUPS

1. Definitions

By a *permutation* of the set S, we mean a bijective function $\sigma : S \to S$. This definition will only be used when S is a finite set. Let $n \in \mathbb{N}$. The *symmetric group on n letters* is the group of all permutations of the set $\{1, 2, \ldots, n\}$. (The terminology is classical; the "letters" are in fact numbers, although they could be any objects whatsoever.)

It is well known that there are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (3) \cdot (2) \cdot (1)$ permutations of a collection $X = \{x_0, \ldots, x_{n-1}\}$ of n elements. Here is the argument: let σ be a permutation of X. There are n choices for $\sigma(x_0)$. Then $\sigma(x_1) \in X \setminus \{\sigma(x_0)\}$, which has $n-1$ elements. Similarly, at the ith stage, there are $n-i$ choices for $\sigma(x_i)$. Thus the total number of choices is precisely $n!$.

We see that the symmetric group has $n!$ elements. However, it is denoted S_n – or $\mathfrak{S}_n$, if we want to be old-fashioned – and this is the only exception to our rule that a group denoted H_m has m elements. An element $\sigma \in S_n$ is traditionally denoted by a matrix with n columns and 2 rows, where the top row is always $\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \end{pmatrix}$, and the second row shows the effect of the permutation, like this:

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

Thus if $n = 4$, the permutation

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

takes 1 to 2, 2 to 4, 3 to 1, and 4 to 3.

Another way to represent this permutation is

$$1 \to 2 \to 4 \to 3 \to 1,$$

but this notation only works if all the numbers are in a single cycle. This leads to the introduction of *cycle* notation.

2. Cycle decomposition of a permutation

Suppose X is the set $\{1, 2, \ldots, n\}$. Let $X^1 \subset X$, with $|X^1| = n_1$. Suppose $\sigma \in S_n$ is a permutation with the following property: we can label the elements of X^1 $a_1, \ldots, a_{n_1}$ in such a way that

$$\sigma(a_1) = a_2; \sigma(a_2) = a_3; \ldots \sigma(a_i) = a_{i+1} \ldots \sigma(a_{n_1}) = a_1;$$

and $\sigma(a) = a$ if $a \in X \setminus X^1$. Then σ is said to be a *cycle*, or an n_1-cycle, and can be written

$$\sigma = (a_1, a_2, \ldots, a_{n_1}).$$

Theorem 2.1. *Any permutation $\sigma \in S_n$ has a cycle decomposition. Precisely, there is a unique partition*

$$X = X^1 \coprod X^2 \coprod \cdots \coprod X^r$$

of X into r disjoint subsets, with $n_j = |X^j|$ and

$$n = n_1 + n_2 + \cdots + n_r,$$

and for each j, an n_j-cycle

$$\sigma_j = (a^j_1, a^j_2, \ldots, a^j_{n_j})$$

where $X^j = \{a^j_1, a^j_2, \ldots, a^j_{n_j}\}$, such that

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r.$$

For example, if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ as above, then $\sigma = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ is itself a 4-cycle. On the other hand, if

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

then

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

is a product of two 2-cycles.

To simplify notation we omit 1-cycles; thus when $n = 4$, we write

$$\begin{pmatrix} 1 & 4 & 2 \end{pmatrix}$$

instead of

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

Important fact: disjoint cycles *commute*. For example if

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

we can also write

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

it doesn't matter how the cycles are ordered. In the above example,

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

Above we wrote

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r$$

but we could write

$$\sigma = \sigma_{i_1} \cdot \sigma_{i_2} \cdot \cdots \cdot \sigma_{i_r}$$

for any ordering (permutation!) of the indices $1, 2, \ldots, r$.

Proof of the theorem. This is best understood using the notion of *orbit*. The orbits of σ are the subsets $X^j \in X$ such that, for any $x \neq y \in X^j$, there is an integer $m > 0$ such that $\sigma^m(x) = y$, and if $x \in X^j$ then $\sigma(x) \in X^j$. In other words, setting $n_j = |X_j|$, for for any $x \in X^j$, $\sigma^{n_j}(x) = x$ and X^j is a set of the form

$$\{x, \sigma(x), \sigma^2(x), \dots \sigma^{n_j - 1}(x)\}$$

for any $x \in X_j$. We define a relation on X: we say $xR_\sigma y$ if there exists some $m > 0$ such that $\sigma^m(x) = y$. This is an equivalence relation:

(reflexive) Since S_n is a finite group, $\sigma^M = e$ for some $m > 0$; then $\sigma^M(x) = x$ for all x.

(symmetric) If $\sigma^m(x) = y$ then $\sigma^{-m}(y) = x$, but $\sigma^{-m} = \sigma^{M-m} = \sigma^{dM-m}$ for any d, and for d sufficiently large $dM - m > 0$.

(transitive) If $\sigma^m(x) = y$ and $\sigma^{m'}(y) = z$ then $\sigma^{m+m'}(x) = z$.

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X. For each j σ induces a permutation σ_j of X^j that fixes all the $X^i, i \neq j$. Then $\sigma = \prod_j \sigma_j$ (in any order).

□

3. Multiplying permutations

This is potentially the most confusing aspect of the theory of the symmetric group. Suppose $\sigma, \tau \in S_n$. Then $\sigma \cdot \tau$ is a permutation in S_n, with the property that, for any $i \in \{1, 2, \dots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. Since every $\sigma \in S_n$ is bijective, it has an inverse function which also belongs to S_n. Of course the identity permutation, that takes each i to itself, is in S_n. Finally, composition of functions is associative:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

for any triple of functions f, g, h. Thus multiplication in S_n is associative, and S_n is indeed a group.

So far, so good. The confusion sets in when it comes time to multiply

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

by

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \tau(1) & \tau(2) & \dots & \tau(n-1) & \tau(n) \end{pmatrix}.$$

The matrix notation does not help; how would you multiply two $2 \times n$ matrices with the same top row? There are some shortcuts – for example, see the top of p. 28 of Howie's notes – but the simplest way to answer the question is to illustrate it with an example. Suppose $n = 4$,

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

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

We compute: $\sigma \cdot \tau(1) = \sigma(\tau(1)) = \sigma(4) = 3$. Similarly, $\sigma \cdot \tau(2) = \sigma(1) = 2$; $\sigma \cdot \tau(3) = \sigma(3) = 1$; and $\sigma \cdot \tau(4) = \sigma(2) = 4$. Thus

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

Multiplication is not more obvious in cycle notation. We have

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

and

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 3 \end{pmatrix} (= \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix}).$$

Howie's notes also suggests a shortcut for computing σ^{-1} on p. 28. Here the cycle notation can be more helpful.

4. Conjugacy classes

We can define an equivalence relation $\sim$ on S_n: two permutations $\sigma, \sigma' \in S_n$ satisfy $\sigma \sim \sigma'$ if and only if their cycle

Theorem 4.1. *Suppose $\sigma, \sigma' \in S_n$ both have cycle decompositions with partition $n = n_1 + n_2 + \cdots + n_r$. Then there exists $\lambda \in S_n$ such that*

$$\sigma' = \lambda \sigma \lambda^{-1}.$$

Thus S_n has a partition according to the shape of the cycle decomposition.

Proof. Say $X = \{1, \ldots, n\}$ as before. We write $X = \coprod_i X^i = \coprod_i Y^i$ where the X^i are the orbits of σ and the Y^i are the orbits of σ'. We can order the partitions so that $|X^i| = |Y^i| = n_i$ for each i. We define λ_1 to be any element of S_n such that $\lambda_1(X^i) = Y^i$ for every i. (For example, if $n = 5$ and we have

$$X^1 = \{1, 3, 4\}, X^2 = \{2, 5\}; \ Y^1 = \{1, 2, 5\}, Y^2 = \{3, 4\},$$

then we can let

$$\lambda_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.)$$

Then for all i,

$$\lambda_0 \sigma \lambda_0^{-1}(Y^i) = \lambda_0 \circ \sigma(X^i) = \lambda_0(X^i) = Y^i.$$

Replacing σ by $\lambda_0 \sigma \lambda_0^{-1}$, it follows that we can assume $X^i = Y^i$ for all i.

We write $\sigma = \prod_i \sigma_i$, $\sigma' = \prod_i \sigma_i'$, where each σ_i, σ_i' is a cycle whose orbit is X^i. Now for each i, it suffices to find λ_i such that

$$\lambda_i \sigma_i \lambda_i^{-1} = \sigma_i'.$$

In other words, we may replace X by each X^i separately, or (by induction) we may assume $X = X^i$ and σ and σ' are n-cycles. We carry out the first in order to show the computation in detail.

So suppose

$$\sigma_i = (a_1(i), a_2(i), \dots, a_{n_i}(i));\ \sigma' = (a_1'(i), a_2'(i), \dots, a_{n_i}'(i)).$$

In other words, $\sigma(a_j(i)) = a_{j+1}(i)$, $\sigma'(a_j'(i)) = a_{j+1}'(i)$, and $\sigma(a_{n_i}(i)) = a_1(i)$. Define λ_i to be the permutation

$$\lambda_i(a_j(i)) = a_j'(i), j = 1, \dots, n_i.$$

Then

$$\lambda_i \sigma_i \lambda_i^{-1}(a_j'(i)) = \lambda \circ \sigma(a_j(i)) = \lambda(a_{j+1}(i)) = a_{j+1}'(i).$$

It follows that $\lambda_i \sigma_i \lambda_i^{-1} = \sigma_i'$ for each i.

Now setting

$$\lambda = \prod_i \lambda_i \cdot \lambda_0,$$

we verify easily that

$$\lambda \sigma \lambda^{-1} = \sigma'.$$

□

5. Transpositions

A *transposition* in S_n is a cycle of the form $\tau_{ij} = \begin{pmatrix} i & j \end{pmatrix}$ where $1 \leq i \neq j \leq n$. In other words, τ_{ij} exchanges i and j and leaves the other numbers unchanged. Then obviously $\tau_{ij} \cdot \tau_{ij}$ is the identity element e.

We will see later in the course that every $\sigma \in S_n$ can be written as a product of transpositions. This product expression is not unique – for example, the identity element e can be written $\tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij}$ and in infinitely many other ways – it suffices to keep adding pairs of τ_{ij}. What is unique, however, is the *sign* of σ.

Theorem 5.1. *If σ can be written in one way as a product of an even number of transpositions, then every such expression for σ has an even number of transpositions.*

It follows that if σ can be written in one way as an odd number of transpositions then *every* such expression for σ has an odd number of transpositions. We define the sign of σ, denoted $sgn(\sigma)$ to be 1 if it can be written as a product of an even number of transpositions, and -1 if it can be written as a product of an odd number of transpositions. In particular $sgn(\tau_{ij}) = -1$ for any $i \neq j$.

We say τ_{ij} is an adjacent transposition if $j = i + 1$. It can be shown that every $\sigma \in S_n$ can be written as a product of adjacent transpositions.

The *length* of σ is then the shortest expression of σ as a product of adjacent transpositions. We will not be discussing length in this course.

6. Parting suggestion

The site `https://www.wolframalpha.com/examples/mathematics/discrete-mathematics/combinatorics/permutations/` has many examples.