Permutations

Abdennour Kitouni, Anatoliy Malyarenko, Sergei Silvestrov

November 19, 2015

Abstract

Contents of the lecture.

- ☞ Groups of permutations.
- ☞ Orbits, cycles, and the alternating groups.

Permutations

Definition 1. A **permutation** of a non-empty set A is a mapping $\sigma\colon A \mapsto A$ that is both one to one and onto.

Let $A = \{1, 2, \ldots, n\}$. A *rearrangement* is a list, with no repetitions, of all the elements of A. A rearrangement $i_1, i_2, \ldots, i_n$ of A determines a function $\sigma\colon A \mapsto A$, namely, $\sigma(1) = i_1$, $\sigma(2) = i_2$, $\ldots$, $\sigma(n) = i_n$. We use a two-rowed notation to denote the function corresponding to a rearrangement; if $\sigma(j)$ is the jth item on the list, then

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

That a list contains *all* the elements of A says that the corresponding function σ is onto; that there are no repetitions on the list says that distinct points have distinct values; that is, σ is one-to-one. Thus, each list determines a one-to-one correspondence $\sigma\colon A \mapsto A$; that is, each rearrangement determines a permutation. Conversely, every permutation σ determines a rearrangement, namely, the list $\sigma(1), \sigma(2), \ldots, \sigma(n)$ displayed as the bottom row. Therefore, rearrangement and permutation are simply different ways of describing the same thing. The advantage of viewing permutations as functions, however, is that they can now be composed and their composite is also a permutation.

Definition 2. The family of all the permutations of a set A, denoted by S_A, is called the **symmetric group** on A. When $A = \{1, 2, \ldots, n\}$, S_A is usually denoted by S_n, and it is called the **symmetric group on n letters**.

Example: S_3 and D_3

Example 1. Denote the elements of S_3 as

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The multiplication table of S_3 is as follows.

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Consider an equilateral triangle with vertices labelled as 1, 2, and 3. Let ρ_j be a rotation by $2\pi j/3$ clockwise, and let μ_j be mirror imaging in the bisector of angle j. Then our table is also the multiplication table of the group D_3 of symmetries of an equilateral triangle!

Definition 3. The **nth dihedral group** D_n is the group of symmetries of the regular n-gon. The group D_4 is called the **octic group**.

Cayley's Theorem

The next theorem shows that the symmetric groups are incredibly rich and complex.

Theorem 1. *Let G be a group. Then G is isomorphic to a subgroup of S_G.*

Sketch of proof. 1. Let $h\colon G \mapsto S_G$ be the function which sends $a \in G$ to the function $h_a\colon G \mapsto G$ defined by

$$h_a(g) = ag, \qquad g \in G.$$

For each given a, h_a is a one-to-one correspondence between G and itself.

2. h is a homomorphism, i.e., $h_{ab} = h_a h_b$.
3. h is one-to-one and thus G is isomorphic to the image $h[G] \subset S_G$.

□

Orbits

Let $\sigma \in S_A$. Define the following relation on A:

$$a \sim b \Leftrightarrow \exists n \in \mathbb{Z} \colon b = \sigma^n(a).$$

$\sim$ is an equivalence relation.

Definition 4. Let $\sigma \in S_A$. The equivalence classes in A determined by the equivalence relation $\sim$ are the **orbits** of σ.

The algorithm of finding the orbits of $\sigma \in S_n$ is as follows.

Step 1 Pick the smallest element of $\{1,2,\ldots,n\}$ which has not yet appeared — call it a (if you are just starting, $a = 1$); write $\{a$ If no such element exist, stop.

Step 2 Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the set with a right brace $\}$ (without writing b down); this completes an orbit — return to Step 1. If $b \neq a$, write b next to a in this orbit: $\{a,b$

Step 3 Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the set with a right brace $\}$ to complete the orbit — return to Step 1. If $c \neq a$, write c next to b in this orbit: $\{a,b,c$ Repeat this step using the number c as the new value for b until the orbit closes.

Example 2. Let $\sigma \in S_{13}$ be as follows.

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

The orbits are

$$\{1,12,8,10,4\}, \quad \{2,13\}, \quad \{3\}, \quad \{5,11,7\}, \quad \{6,9\}.$$

Cycles

Definition 5. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.

In *cyclic notation* the cycle is written as $\sigma = (a_1, a_2, \ldots, a_m)$, where $\sigma(a_j) = a_{j+_m 1}$, and if a_k is not among a_1,, a_2, ..., a_m, then $\sigma(a_k) = a_k$.

Example 2 shows that

$$\sigma = (1,12,8,10,4)(2,13)(3)(5,11,7)(6,9),$$

i.e., σ can be written as a product of disjoint cycles. This is a general fact.

The cycle decomposition theorem

Theorem 2. *Every $\sigma \in S_n$ is a product of disjoint cycles.*

Proof. Let O_1, O_2, ..., O_r be the orbits of σ. For $1 \leq j \leq r$, define the disjoint cycle μ_j as

$$\mu_j = \begin{cases} \sigma(x), & x \in O_j, \\ x, & x \notin O_j. \end{cases}$$

Clearly $\sigma = \mu_1 \mu_2 \ldots \mu_r$. □

Transpositions

Definition 6. A **transposition** is a cycle of length 2.

Clearly

$$(a_1, a_2, \ldots a_m) = (a_1, a_m)(a_1, a_{m-1}) \ldots (a_1, a_3)(a_1, a_2),$$

i.e., any cycle is a product of transpositions. It follows that if $2 \leq |A| < \infty$, then any $\sigma \in S_A$ is a product of transpositions.

Theorem 3. *No permutation in S_n can be expressed both as a product of an even number of transposition and as a product of an odd number of transposition.*

Proof. Let $\sigma \in S_n$ be a product of j transpositions and a product of k transpositions. We have to prove that $j - k$ is even.

Let I_n be the $n \times n$ identity matrix. Because each transposition of rows multiplies the determinant of a matrix by -1, the determinant of σI_n is equal to both $(-1)^j$ and $(-1)^k$. It follows that $(-1)^j = (-1)^k$, i.e. $j - k = 2m$. □

The alternating group

Definition 7. A permutation $\sigma \in S_n$ is **even** (**odd**) if it can be express as a product of an even (odd) number of transpositions.

Theorem 4. *If $n \geq 2$, then the set of all even permutations of the set $\{1, 2, \ldots, n\}$ form a subgroup A_n of order $n!/2$ of the symmetric group S_n.*

Definition 8. The group A_n is the **alternating group on n letters**.