12-29-1993

Permutation groups.

Definition. Let A be a set. A **permutation** of (or *on*) A is a bijection $A \to A$.

Proposition. The set S_A of permutations of a set A is a group under function composition.

Proof. First, the composition of bijections is a bijection: The inverse of $\sigma \cdot \tau$ is $\tau^{-1} \cdot \sigma^{-1}$. Thus, function composition is a binary operation on the set of bijections from A to A.

Function composition is always associative. The identity map $id : A \to A$ is a permutation of A, and serves as an identity under function composition. Since bijective maps have inverses which are bijections, if $\sigma : A \to A$ is a bijection, so is σ^{-1}. Therefore, S_A is a group. □

Terminology. S_A is called the **symmetric group** on A. If S has n elements, we may as well take $S = \{1, 2, \ldots, n\}$. The corresponding symmetric group is denoted S_n, the **symmetric group on n letters**.

One way to write a permutation is to show where each element goes. For example,

$$\sigma = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{Bmatrix} \in S_6$$

means that

$$\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 6, \sigma(6) = 5.$$

Example. If

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

then $\sigma\tau$ will mean "σ first, then τ".

Here's how to compute the product:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ & & & & \sigma \\ 2 & 3 & 4 & 1 \\ & & & & \tau \\ 3 & 4 & 2 & 1 \end{array}$$

So

$$\sigma\tau = \begin{Bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{Bmatrix}. \ \square$$

Definition. A **cycle** is a permutation which maps a finite subset $\{x_1, x_2, \ldots, x_n\}$ by

$$x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1.$$

This cycle will be denoted $(x_1\ x_2\ \ldots\ x_n)$.

Examples.

1. The cycle $(x_1\ x_2\ \ldots\ x_n)$ has **length** n. A cycle of length n has order n in S_n. For example,

$$(1\ 4\ 2)^3 = \text{id}. \ \square$$

2. The permutation

$$\begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{Bmatrix}$$

can be written as a product of the cycles (1 3 5) and (2 4). Note that the cycles (1 3 5) and (2 4) are **disjoint** — no element is moved by both of them. In fact, an arbitrary permutation may be written as a product of disjoint cycles.

The cycle (2 4) simply switches the elements 2 and 4. A permutation which switches two elements is called a **transposition**. Every permutation may also be written as a product of transpositions. $\square$

Theorem. Every permutation on a finite set can be written as a product of disjoint cycles.

Proof. Induct on the number of elements in the set.

First, prove the result for a set with 1 element. This is easy — there is only one permutation (the identity), and it is the cycle (1).

Next, assume that the result is known for sets with fewer than n elements and try to prove the result for a set with n elements. Suppose, then, that a permutation on a set with less than n elements can be written as a product of disjoint cycles. I have to show that a permutation on a set with n elements — that is, an element $\sigma \in S_n$ — can be written as a product of disjoint cycles.

Since S_n is a finite group, σ has finite order. Let m be the order of σ. Look at

$$Q = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{m-1}(1)\}.$$

If $Q = S$, σ is the cycle

$$(1\ \sigma(1)\ \sigma^2(1)\ \ldots \sigma^{m-1}(1)).$$

Otherwise, $Q \neq S$, so $|S - Q| < n$.

Now σ restricted to $S - Q$ is a permutation on $S - Q$, so by the inductive assumption it can be written as a product $\tau_1 \tau_2 \cdots \tau_k$ of disjoint cycles. Then

$$\sigma = (1\ \sigma(1)\ \sigma^2(1)\ \ldots \sigma^{m-1}(1))\tau_1 \tau_2 \cdots \tau_k.$$

Thus, σ has been expressed as a product of disjoint cycles. This completes the induction step, and establishes the result for all n. $\square$

Example. The proof actually contains an algorithm for decomposing a permutation into a product of disjoint cycles. Start with an element and follow its "orbit" under the permutation until the orbit closes up. If you've exhausted all the elements, you're done. Otherwise, pick an element which wasn't in the orbit of the first element and follow the new element's orbit. Keep going.

For example,

$$\left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 4 & 5 \end{matrix}\right\} = (1\ 6\ 5\ 4)(2\ 3). \square$$

Lemma. Disjoint cycles commute.

Proof. If σ and τ are disjoint cycles, say

$$\sigma = (a_1\ a_2\ \ldots a_m) \quad \text{and} \quad \tau = (b_1\ b_2\ \ldots b_n),$$

where $\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots b_n\} = \emptyset$.

Then

$$\sigma\tau(i) = \tau\sigma(i) = \begin{cases} \sigma(i) & \text{if } i \in \{a_1, a_2, \ldots, a_m\} \\ \tau(i) & \text{if } i \in \{b_1, b_2, \ldots b_n\} \\ i & \text{otherwise} \end{cases} \quad \square$$

Definition. Let G be a group, $S \subset G$. If $a \in G$, aSa^{-1} is called the **conjugate** of S by a. The operation $x \mapsto axa^{-1}$ is called **conjugation**.

Conjugation is an important operation in group theory. For example, a normal subgroup is a subgroup which is equal to all of its conjugates. Here is how to compute the conjugate of a permutation. First, if $\sigma \in S_n$ and $\tau \in S_n$, write σ as a product of disjoint cycles:

$$\sigma = \phi_1 \phi_2 \cdots \phi_m.$$

Then

$$\tau\sigma\tau^{-1} = \tau\phi_1\phi_2\cdots\phi_m\tau^{-1} = (\tau\phi_1\tau^{-1})(\tau\phi_2\tau^{-1})\cdots(\tau\phi_m\tau^{-1}).$$

It follows that to conjugate a permutation, you only need to know how to conjugate a cycle.

Lemma. Let τ be a permutation and let $(a_1\ a_2\ \ldots a_n)$ be a cycle. Then

$$\tau^{-1}(a_1\ a_2\ \ldots a_n)\tau = (\tau(a_1)\ \tau(a_2)\ \ldots \tau(a_n)).$$

Proof. Remember that products of permutations are read from left to right. What does the product on the left do to $\tau(a_i)$? Well, $\tau^{-1}\tau(a_i) = a_i$. Feed a_i to the cycle; it is sent to a_{i+1} (with $a_n \mapsto a_1$). Finally, apply τ to send a_{i+1} to $\tau(a_{i+1})$. Thus, the product on the left certainly maps

$$\tau(a_1) \mapsto \tau(a_2) \mapsto \cdots \tau(a_n) \mapsto \tau(a_1).$$

Next, I must show that the product on the left does not move anything else. Suppose k is not one of the elements $\tau(a_1)$, $\tau(a_2)$, ..., $\tau(a_n)$. What is $\tau^{-1}(k)$? Well, $\tau^{-1}(k) \neq a_i$ for any i, or else $k = \tau(a_i)$. $\times$

Since $\tau^{-1}(k)$ is not one of the a_i's, it is not moved by the cycle. So it "passes through" to get hit by τ, and $\tau\tau^{-1}(k) = k$. Thus, the product on the left does not move anything outside of the set $\{\tau(a_1), \tau(a_2), \ldots, \tau(a_n)\}$.

Its effect on the elements of $\{\tau(a_1), \tau(a_2), \ldots, \tau(a_n)\}$ is that of the cycle $(\tau(a_1)\ \tau(a_2)\ \ldots \tau(a_n))$, so it *is* the cycle $(\tau(a_1)\ \tau(a_2)\ \ldots \tau(a_n))$. $\square$

Example.

$$\sigma = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 4 & 5 \end{Bmatrix} = (1\ 6\ 5\ 4)(2\ 3).$$

Let $\tau = (4\ 6\ 3)$. Then

$$\tau^{-1}\sigma\tau = (1\ 3\ 5\ 6)(2\ 4).\ \square$$

Definition. A **transposition** is a permutation which interchanges two elements and leaves everything else fixed. (That is, a transposition is a cycle of length 2.)

Proposition. Every permutation is a product of transpositions.

Proof. It suffices to show that every cycle is a product of transpositions, since every permutation is a product of cycles. Just observe that

$$(1\ 2\ \ldots n) = (1\ 2)(1\ 3)\ldots(1\ n).\ \square$$

Remark. While the decomposition of a permutation into disjoint cycles is unique up to order and representation of the cycles (i.e. $(1\ 2\ 3) = (2\ 3\ 1)$), a permutation may be written as a product of transpositions in infinitely many ways. You can always tack on trivial terms of the form $(a\ b)(a\ b) = 1$. $\square$

Example. $(2\ 7\ 4\ 5) = (2\ 7)(2\ 4)(2\ 5)$ $\square$

Definition. A permutation is **even** if it can be written as a product of an even number of transpositions; a permutation is **odd** if it can be written as a product of an odd number of transpositions.

Lemma. A permutation cannot be written as a product of both an odd and an even number of transpositions.

Proof. Suppose to the contrary that

$$\sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n,$$

where m is even and n is odd, and all the σ's and τ's are transpositions.

Since $\tau_i^{-1} = \tau_i$,

$$\tau_n \cdots \tau_2 \tau_1 \sigma_1 \sigma_2 \cdots \sigma_m = 1.$$

Note that the identity permutation 1 has been written as a product of an odd $(m + n)$ number of transpositions. If this is impossible, I have a contradiction.

It therefore suffices to show that the identity permutation 1 *cannot* be written as a product of an odd number of transpositions.

Suppose

$$1 = \sigma_1 \sigma_2 \cdots \sigma_m,$$

where m is odd.

Here is a clever idea. Consider a polynomial $f(x_1, \ldots, x_n)$ in n variables. A permutation $\sigma \in S_n$ transforms f into another polynomial by "permuting the variables":

$$\sigma(f) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

For example, suppose $f(x_1, x_2, x_3) = x_1^3 + 3x_1x_3 - 5x_2^7x_3^4 + 1$. Suppose $\sigma = (2\ 1\ 3)$. Then

$$\sigma(f) = x_3^3 + 3x_3x_2 - 5x_1^7x_2^4 + 1.$$

Now consider the polynomial

$$f(x_1, \ldots, x_n) = \prod_{i>j} (x_i - x_j).$$

For example, if $n = 3$,

$$f(x_1, x_2, x_3) = (x_3 - x_1)(x_3 - x_2)(x_2 - x_1).$$

Obviously, the identity permutation takes f to itself.

On the other hand, a transposition $(i\ j)$ for $i > j$ takes the factor $x_i - x_j$ to $x_j - x_i = -(x_i - x_j)$. In other words, a factor of -1 is introduced for each transposition. Since $\sigma_1\sigma_2 \cdots \sigma_m$ contains an odd number of transpositions, it will send f to $(-1)^m f = -f$.

This is a contradiction: If 1 and $\sigma_1\sigma_2 \cdots \sigma_m$ are the same permutation, they should have the same effect on f. Therefore, the identity cannot be written as a product of an odd number of transpositions. Hence, a permutation cannot be written as a product of both an even and an odd number of transpositions. □

Remark. The decomposition

$$(1\ 2\ \ldots n) = (1\ 2)(1\ 3)\ldots(1\ n)$$

shows that a cycle of length n is even if n is even, and odd if n is odd. □

Definition. The **alternating group** A_n on n letters is the subgroup of S_n consisting of the even permutations.

I should check that A_n really is a subgroup. First, 1 is even, so $1 \in A_n$. Next, if σ and τ are even, then τ^{-1} is even (decompose τ into transpositions, and write the product backwards). Therefore, $\sigma\tau^{-1}$ is even (by concatenating decompositions of σ and τ^{-1} into products of transpositions). Hence, $\sigma\tau^{-1} \in A_n$.

If $n \geq 3$, there are an equal number of even and odd permutations. Therefore, $(S_n : A_n) = 2$. In fact, A_n is a **normal** subgroup of S_n.

Example. Here is the multiplication table for S_3:

	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)	(1 2)
id	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3 2)	id	(1 3)	(1 2)	(2 3)
(1 3 2)	(1 3 2)	id	(1 2 3)	(1 2)	(2 3)	(1 3)
(2 3)	(2 3)	(1 2)	(1 3)	id	(1 3 2)	(1 2 3)
(1 3)	(1 3)	(2 3)	(1 2)	(1 2 3)	id	(1 3 2)
(1 2)	(1 2)	(1 3)	(2 3)	(1 3 2)	(1 2 3)	id

The alternating group on 3 letters is the "rotation subgroup":

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}. \ \square$$