Lecture 3: More on Permutations, Division Algorithm

Summary:
We continue our exploration of permutations and introduce the division algorithm. We prove that every permutation can be written as a product of disjoint cycles, with a unique representation up to reordering. We define the order of a permutation and show that it equals the least common multiple of the lengths of its disjoint cycles. We present the division algorithm for integers and prove its existence and uniqueness. We use this algorithm to establish properties about the order of permutations and their powers. We prove that powers of a permutation are equal if and only if their exponents are congruent modulo the permutation's order.

Topics Covered: division algorithm for integers, identity permutation, order of a permutation, representation of a permutation as disjoint cycles

Theorem: Every permutation in S_n can be written as a product of disjoint cycles. Moreover, the presentation is unique up to reordering of cycles.

Example:

Consider the following permutation:

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

We can write it as a product of disjoint cycles as follows:

$$\sigma = (1,2)(3)(4)(5,6,7)$$

Proof:

Consider

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots.$$

Assume that j is the smallest positive number such that

$$\sigma^j(1) \in \{1, \sigma(1), \dots., \sigma^{j-1}(1)\}$$

We want to understand which $i < j$ is such that

$$\sigma^j(1) = \sigma^i(1)$$

We want to show that $i = 0$.

Suppose, for contradiction that $i > 0$, but, j is still the smallest positive number such that

$$\sigma^j(1) = \in \{1, \sigma(1), \dots., \sigma^{j-1}\}$$

So, we have that

$$\sigma^i(1) = \sigma^j(1)$$

Apply σ^{-1} to each side, which exists since σ is a bijection.

$$\implies \sigma^{i-1}(1) = \sigma^{j-1}(1)$$

Which contradicts the minimality of j.

So, we now know that $i = 0$.

$$\implies$$

If

$$\{1, \sigma(1), \dots., \sigma^{j-1}(1)\} = [n]$$

then

$$\sigma = (1, \sigma(1), \ldots, \sigma^{j-1}(1)\}$$

Otherwise, pick the smallest element

$$a \in [n] - [\{1, \sigma(1), \ldots, \sigma^{j-1}(1)\}$$

and consider the sequence

$$a, \sigma(a), \sigma^2(a), \ldots.$$

Getting your next cycle $(a, \sigma(a), \ldots, \sigma^{k-1}(a))$ and continue this fashion until your cycles contain all elements in $[n]$.

We can represent the permutation as a graph of disjoint cycles.

> Exercise: show that the product of disjoint cycles is unique up to reordering of the cycles

Consider the following cycle

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

Note that

$$\sigma^2(1) = 1$$
$$\sigma^2(2) = 2$$
$$\sigma^3(3) = 3$$
$$\sigma^3(4) = 4$$
$$\sigma^3(5) = 5$$

Therefore,

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

Definition: The smallest positive integer m such that $\sigma^m = \mathrm{id}$ is called the **order** of σ.

Question: What is the order of $\sigma = (a_1, \ldots, a_k)$?

It's k, because $\sigma^k = \mathrm{id}$ and for any $i \in \{1, \ldots k-1\}$, $\sigma^i(a_j) \neq a_j$

$$\sigma^k = \mathrm{id}$$
$$\sigma^{k+1} = \sigma$$

Consider

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

The order of π is 4.

Proposition: The order of σ is the least common multiple of the lengths of the disjoint cycles in the cycle representation of σ.

Proof:

If we have one cycle longer than 1, then we know the proposition.

If we have 2 cycles longer than 1

$$(a_1, \ldots a_k)(b_1, \ldots, b_m), \;\; (a_1, \ldots, a_k) \cap (b_1, \ldots, b_m) \neq \emptyset$$
$$(a_1, \ldots, a_k)^k = \mathrm{id} \;\; \text{on} \;\; a_1, \ldots, a_k$$
$$(b_1, \ldots, b_m)^m = \mathrm{id} \;\; \text{on} \;\; b_1, \ldots, b_m$$
$$\sigma^j = (a_1, \ldots, a_k)^j \, (b_1, \ldots, b_m)^j$$

Note that the LCM of m, k satisfies

$$\sigma^{\text{LCM}(m,k)} = \text{id}$$

Proposition: Let $\sigma \in S_n$ have order m. Then, $\forall i, j \in \mathbb{Z}$, we have

$$\sigma^i = \sigma^j \iff m \mid i - j$$

We can also write the right side as

$$i \equiv j \ (\bmod m)$$

To prove this theorem, we will need the division algorithm

Theorem: (Existence of quotient and remainder):

Let $a, b \in \mathbb{Z}$ and $a \geq 0$ and $b > 0$. Here, a is the number we are dividing, and b is the divisor.

Then, $\exists q, r \in \mathbb{Z}$ such that

$$a = qr + r$$

and

$$0 \leq r < b$$

q is the quotient and r is the remainder.

Proof:

$0 \cdot b = 0, 1 \cdot b, 2 \cdot b, 3 \cdot b, ...$

$\exists q \in \mathbb{Z}$ such that

$$q \cdot b \leq a < (q+1)b$$
$$r = a - qb$$

Theorem: uniqueness of quotient and remainder:

Let $a, b \in \mathbb{Z}$ with $a \geq 0$ and $b > 0$ and let $q, r, q', r' \in \mathbb{Z}$ such that

$$a = qb + r$$
$$0 \leq r < b$$
$$a = q'b + r'$$
$$0 \leq r' < b$$

Then, it holds that $q = q', r = r'$.

Proof:

We know that $a = qb + r$ and $a = q'b + r'$, Subtract them to get

$$(q - q')b = r' - r$$

Since $0 \leq r, r' < b$, we know that $-b < r' - r < b$

$$\implies -b < (q - q')b < b$$
$$-1 < q - q' < 1 \implies q - q' = 0 \implies q = q', r = r'$$
$$QED$$

Going back to the other theorem

$$i - j = (qm + r) - (q'm + r') = m(q - q') + (r - r')$$

Note that $i \equiv j \ (\bmod m)$ means the remainders of i and j upon division by m are equal.

Proof: The smallest positive integer for which $\sigma^j = \mathrm{id}$ is $m : \sigma^m = \mathrm{id}$

Assuming $\sigma^i = \sigma^j, i, j \in \mathbb{Z}$

Multiply by σ^{-i}, we get

$$\sigma^{i-i} = \sigma^0 = \mathrm{id} = \sigma^{j-i}$$

So,

$$\mathrm{id} = \sigma^{j-i} = \sigma^{qm+r} = \sigma^{qm}\sigma^r = (\sigma^m)^q\sigma^r = (\mathrm{id})^q\sigma^r = \sigma^r$$
$$0 \leq r < m$$
$$\implies r = 0$$
$$\implies m | j - i$$

Which means $i \equiv j \pmod m$

$$QED$$

The proof in the other direction is not difficult.