MATH 415

Modern Algebra I

Lecture 6: Permutations. Cycle decomposition.

Permutations

Let X be a nonempty set. A **permutation** of X is a bijective function $f : X \to X$.

Given two permutations π and σ of X, the composition $\pi\sigma$, defined by $\pi\sigma(x) = \pi(\sigma(x))$, is called the **product** of these permutations. In general, $\pi\sigma \neq \sigma\pi$, i.e., multiplication of permutations is not commutative. However it is associative: $\pi(\sigma\tau) = (\pi\sigma)\tau$.

All permutations of a set X form a group called the **symmetric group** on X. *Notation:* S_X, Σ_X, $\mathrm{Sym}(X)$.

All permutations of $\{1, 2, \ldots, n\}$ form a group called the **symmetric group on n symbols** and denoted S_n or $S(n)$.

Permutations of a finite set

The word "**permutation**" usually refers to transformations of finite sets.

Permutations are traditionally denoted by Greek letters (π, σ, τ, ρ,...).

Two-row notation. $\pi = \begin{pmatrix} a & b & c & \dots \\ \pi(a) & \pi(b) & \pi(c) & \dots \end{pmatrix}$,

where $a, b, c, \dots$ is a list of all elements in the domain of π. Rearrangement of columns does not change the permutation.

Example. The symmetric group S_3 consists of 6 permutations:

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

Theorem The symmetric group S_n has $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ elements.

Traditional argument: The number of elements in S_n is the number of different rearrangements $x_1, x_2, \ldots, x_n$ of the list $1, 2, \ldots, n$. There are n possibilities to choose x_1. For any choice of x_1, there are $n-1$ possibilities to choose x_2. And so on...

Alternative argument: Any rearrangement of the list $1, 2, \ldots, n$ can be obtained as follows. We take a rearrangement of $1, 2, \ldots, n-1$ and then insert n into it. By the inductive assumption, there are $(n-1)!$ ways to choose a rearrangement of $1, 2, \ldots, n-1$. For any choice, there are n ways to insert n.

Product of permutations

Given two permutations π and σ, the composition $\pi\sigma$ is called the **product** of these permutations. Do not forget that the composition is evaluated from right to left: $(\pi\sigma)(x) = \pi(\sigma(x))$.

To find $\pi\sigma$, we write π underneath σ (in two-row notation), then reorder the columns so that the second row of σ matches the first row of π, then erase the matching rows.

Example. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

$$\begin{matrix} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \\ \pi = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \end{matrix} \quad \Longrightarrow \quad \pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

To find π^{-1}, we simply exchange the upper and lower rows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Cycles

A permutation π of a set X is called a **cycle** (or **cyclic**) of length r if there exist r distinct elements $x_1, x_2, \ldots, x_r \in X$ such that

$$\pi(x_1) = x_2,\ \pi(x_2) = x_3, \ldots,\ \pi(x_{r-1}) = x_r,\ \pi(x_r) = x_1,$$

and $\pi(x) = x$ for any other $x \in X$.

Notation. $\pi = (x_1\ x_2\ \ldots\ x_r)$.

The identity function is (the only) cycle of length 1. Any cycle of length 2 is called a **transposition**.

The inverse of a cycle is also a cycle of the same length. Indeed, if $\pi = (x_1\ x_2\ \ldots\ x_r)$, then $\pi^{-1} = (x_r\ x_{r-1}\ \ldots\ x_2\ x_1)$.

Example. Any permutation of $\{1, 2, 3\}$ is a cycle.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id},\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3).$$

Cycle decomposition

Let π be a permutation of X. We say that π **moves** an element $x \in X$ if $\pi(x) \neq x$. Otherwise π **fixes** x.

Two permutations π and σ are called **disjoint** if the set of elements moved by π is disjoint from the set of elements moved by σ.

Theorem If π and σ are disjoint permutations in S_X, then they commute: $\pi\sigma = \sigma\pi$.

Idea of the proof: If π moves an element x, then it also moves $\pi(x)$. Hence σ fixes both so that $\pi\sigma(x) = \sigma\pi(x) = \pi(x)$.

Theorem Any permutation of a finite set can be expressed as a product of disjoint cycles. This **cycle decomposition** is unique up to rearrangement of the cycles involved.

Idea of the proof: Given $\pi \in S_X$, for any $x \in X$ consider a sequence $x_0 = x, x_1, x_2, \dots,$ where $x_{m+1} = \pi(x_m)$. Let r be the least index such that $x_r = x_k$ for some $k < r$. Then $k = 0$.

Examples

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

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

- $(1\ 2)(1\ 3)(1\ 4)(1\ 5) = (1\ 5\ 4\ 3\ 2).$

- $(2\ 4\ 3)(1\ 2)(2\ 3\ 4) = (1\ 4).$