MATH 433

Applied Algebra

Lecture 10:
Permutations.

Permutations

Let X be a finite set. A **permutation** of X is a bijection from X to itself.

Let $f : X \to X$ be a function. Given $x \in X$, the element $y = f(x)$ is called the **image** of x under the function f. Also, x is called **preimage** of y under f.

The function $f : X \to X$ is **injective** (or **one-to-one**) if any $y \in X$ has at most one preimage. The function f is **surjective** (or **onto**) if any $y \in X$ has at least one preimage. The function f is **bijective** if any $y \in X$ has exactly one preimage.

The inverse function f^{-1} is defined by the rule

$$x = f^{-1}(y) \iff y = f(x).$$

The inverse f^{-1} exists if and only if f is a bijection. If f^{-1} exists then it is also a bijection.

Theorem If X is a finite set, then the following conditions on a function $f : X \to X$ are equivalent:

- f is injective,
- f is surjective,
- f is bijective.

Examples. • The identity function $\mathrm{id}_X : X \to X$, $\mathrm{id}_X(x) = x$ for every $x \in X$.

• Let G_n be the set of invertible congruence classes modulo n, $[a] \in G_n$, and define a function $f : G_n \to G_n$ by $f([x]) = [a][x]$. Then f is a permutation on G_n (which is the key fact in the proof of Euler's theorem).

Symmetric group

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 a permutation.

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

The set of all permutations of $\{1, 2, \dots, n\}$ is called the **symmetric group** on n symbols and denoted $S(n)$ or S_n.

Theorem (i) For any two permutations $\pi, \sigma \in S_X$, the composition $\pi\sigma$ is also in S_X.
(ii) The identity function id_X is a permutation on X.
(iii) For any permutation $\pi \in S_X$, the inverse π^{-1} is in S_X.

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 $n! = 1 \cdot 2 \cdot 3 \cdots n$ 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: if $\tau = \pi\sigma$, then $\tau(x) = \pi(\sigma(x))$. In general, $\pi\sigma \neq \sigma\pi$.

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

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

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. $\pi = (x_1\ x_2\ \ldots\ x_n)$.

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 $\pi = (x_1\ x_2\ \ldots\ x_n)$, then $\pi^{-1} = (x_n\ x_{n-1}\ \ldots\ x_2\ x_1)$.

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 $S(n)$, then they commute: $\pi\sigma = \sigma\pi$.

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

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

Order of a permutation

Let π be a permutation. The positive **powers** of π are defined inductively:

$$\pi^1 = \pi \quad \text{and} \quad \pi^{k+1} = \pi \cdot \pi^k \quad \text{for every integer} \quad k \geq 1.$$

The negative powers of π are defined as the positive powers of its inverse: $\pi^{-k} = (\pi^{-1})^k$ for every positive integer k. Finally, we set $\pi^0 = \mathrm{id}$.

Theorem Let π be a permutation. Then there is a positive integer m such that $\pi^m = \mathrm{id}$.

The **order** of a permutation π, denoted $o(\pi)$, is defined as the smallest positive integer m such that $\pi^m = \mathrm{id}$.

Theorem Let π be a cyclic permutation. Then the order $o(\pi)$ is the length of the cycle π.