MATH 433

Applied Algebra

Lecture 17:
Cycle decomposition.
Order of a permutation.

Permutations

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

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.

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.

Given two permutations π and σ, 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: $\pi(\sigma\tau) = (\pi\sigma)\tau$.

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**.
In the case $S = \{1, 2, \ldots, n\}$, we define an **adjacent transposition** as a transposition of the form $(k\ k{+}1)$.

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

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 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

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

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

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

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

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

Powers of a permutation

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

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

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 and $r, s \in \mathbb{Z}$. Then
(i) $\pi^r \pi^s = \pi^{r+s}$,
(ii) $(\pi^r)^s = \pi^{rs}$,
(iii) $(\pi^r)^{-1} = \pi^{-r}$.

Remark. The theorem is proved in the same way as the analogous statement on invertible congruence classes.

Order of a permutation

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

Proof: Consider the list of powers: $\pi, \pi^2, \pi^3, \dots$. Since there are only finitely many permutations of any finite set, there must be repetitions within the list. Assume that $\pi^r = \pi^s$ for some $0 < r < s$. Then $\pi^{s-r} = \pi^s \pi^{-r} = \pi^s (\pi^r)^{-1} = \mathrm{id}$.

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 permutation of order m. Then $\pi^r = \pi^s$ if and only if $r \equiv s \bmod m$. In particular, $\pi^r = \mathrm{id}$ if and only if the order m divides r.

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

Examples. • $\pi = (1\ 2\ 3\ 4\ 5)$.

$\pi^2 = (1\ 3\ 5\ 2\ 4)$, $\pi^3 = (1\ 4\ 2\ 5\ 3)$,
$\pi^4 = (1\ 5\ 4\ 3\ 2)$, $\pi^5 = \mathrm{id}$.

$\Longrightarrow\ o(\pi) = 5$.

• $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$.

$\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$,
$\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2)$, $\sigma^6 = \mathrm{id}$.

$\Longrightarrow\ o(\sigma) = 6$.

• $\tau = (1\ 2\ 3)(4\ 5)$.

$\tau^2 = (1\ 3\ 2)$, $\tau^3 = (4\ 5)$, $\tau^4 = (1\ 2\ 3)$,
$\tau^5 = (1\ 3\ 2)(4\ 5)$, $\tau^6 = \mathrm{id}$.

$\Longrightarrow\ o(\tau) = 6$.

Lemma 1 Let π and σ be two commuting permutations: $\pi\sigma = \sigma\pi$. Then
(i) the powers π^r and σ^s commute for all $r, s \in \mathbb{Z}$,
(ii) $(\pi\sigma)^r = \pi^r\sigma^r$ for all $r \in \mathbb{Z}$,

Lemma 2 Let π and σ be disjoint permutations in $S(n)$. Then **(i)** they commute: $\pi\sigma = \sigma\pi$,
(ii) $(\pi\sigma)^r = \mathrm{id}$ if and only if $\pi^r = \sigma^r = \mathrm{id}$,
(iii) $o(\pi\sigma) = \mathrm{lcm}\big(o(\pi), o(\sigma)\big)$.

Idea of the proof: The set $\{1, 2, \ldots, n\}$ splits into 3 subsets: elements moved by π, elements moved by σ, and elements fixed by both π and σ. All three sets are invariant under π and σ. It follows that π^r and σ^r are also disjoint.

Theorem Let $\pi \in S(n)$ and suppose that $\pi = \sigma_1\sigma_2\ldots\sigma_k$ is a decomposition of π as a product of disjoint cycles. Then the order of π is the least common multiple of the lengths of cycles $\sigma_1, \ldots, \sigma_k$.