MATH 433

Applied Algebra

Lecture 18:
Cycle decomposition (continued).
Order of a permutation.

Cycles

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

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

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

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

The identity function is (the only) cycle of length 1.
Any cycle of length 2 is called a **transposition**.
In the case $S = \{1, 2, \dots, n\}$, 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 $\pi = (x_1\ x_2\ \dots\ x_r)$, then $\pi^{-1} = (x_r\ x_{r-1}\ \dots\ x_2\ x_1)$.

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.

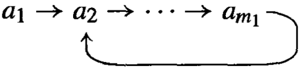
Theorem If π and σ are disjoint permutations in S_X, then they commute: $\pi\sigma = \sigma\pi$.

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

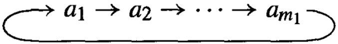
Theorem Any permutation of a finite set can be expressed as a product of disjoint cycles. This **cycle decomposition** is unique up to rearrangement of the cycles involved.

Idea of the proof: Given $\pi \in S_X$, for any $x \in X$ consider a sequence $a_1 = x, a_2, a_3, \dots,$ where $a_{m+1} = \pi(a_m)$. Let r be the least index such that $a_r = a_k$ for some $k < r$. Then $k = 1$.

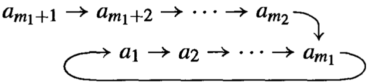
Cycle decomposition



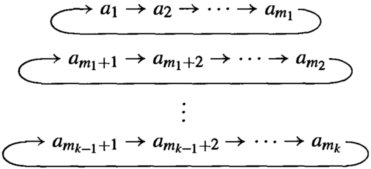
wrong picture



right picture



wrong picture



right picture

Remark. Any cycle of length m can be denoted in m different ways depending on a choice of the initial point. For example, $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$.

Examples

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

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

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

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

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

Examples

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

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

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

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

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

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

Hence $(1\ 2)(2\ 3)(3\ 4)(4\ 5)(5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$

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

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. Hence we have $\pi^r = \pi^s$, where $0 < r < s$. 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 If a permutation π is a cycle, then the order $o(\pi)$ equals the length of the cycle.

Examples. • $\pi = (1\ 2\ 3\ 4\ 5)$.

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

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

• $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$.

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

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

• $\tau = (1\ 2\ 3)(4\ 5)$.

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

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

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_X. Then
(i) the powers π^r and σ^s are also disjoint,
(ii) $\pi^r\sigma^s = \mathrm{id}$ implies $\pi^r = \sigma^s = \mathrm{id}$.

Lemma 3 Let π and σ be disjoint permutations in S_X. 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) $o(\pi\sigma) = \mathrm{lcm}\big(o(\pi), o(\sigma)\big)$.

Theorem Let $\pi \in S_X$ and suppose that $\pi = \sigma_1\sigma_2\dots\sigma_k$ is a decomposition of π as a product of disjoint cycles. Then the order of π equals the least common multiple of the lengths of the cycles $\sigma_1, \dots, \sigma_k$.

Examples

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

The cycle decomposition is $\pi = (1\ 2\ 4\ 9\ 3\ 7\ 5)(6\ 12\ 8\ 11)$ or $\pi = (1\ 2\ 4\ 9\ 3\ 7\ 5)(6\ 12\ 8\ 11)(10)$. It follows that $o(\pi) = \mathrm{lcm}(7, 4) = \mathrm{lcm}(7, 4, 1) = 28$.

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

This permutation is a product of three disjoint transpositions. Therefore the order of σ equals $\mathrm{lcm}(2, 2, 2) = 2$.

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

The permutation is given as a product of transpositions. However, the transpositions are not disjoint and so this representation does not help to find the order of τ. The cycle decomposition is $\tau = (5\ 4\ 3\ 2\ 1)$. Hence τ is a cycle of length 5 so that $o(\tau) = 5$.