Algebra MATH-310

Lecture 5

Anna Lachowska

October 14, 2024

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Groups: lecture 4

(a) Symmetric group S_n, definition and examples

(b) The cycle notation

(c) Disjoint cycles

(d) Product and conjugation of elements in S_n

(e) Transpositions in S_n

(f) The sign of a permutation and the alternating group A_n

next time!

Symmetric group S_n

Definition

S_n is the group of permutations of n elements with the group law given by composition of permutations, and the neutral element given by the trivial permutation.

Example: S_3 $\left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$

In general, $|S_n| = n!$.

Application of S_n in digital holography

Symmetry groups are used in digital holography to create algorithms that use symmetry properties of the object and the set of distances from the observer. Such algorithms reduce the computational complexity in the creation of digital holograms, helping to avoid redundant computations.

The cycle notation for the elements of S_n

Definition

Let $\rho \in S_n$ and $x \in E = \{1, 2, \ldots n\}$. The set

$$Orb_\rho(x) = \{\rho^k x\}_{k \in \mathbb{N}} = \{x, \rho x, \rho^2 x, \ldots \rho^{k-1} x\}.$$

is called the orbit of ρ in E.

Proposition

$E = \{1, 2, \ldots n\} = \cup_{i=1}^r Orb_\rho(x_i)$, and the union is disjoint.

Proof: $\{x_1, \rho x_1 \ldots \rho^{k-1} x_1\}$ $\{x_2, \rho x_2 \ldots \rho^{k-1} x_2\}$. If $\rho^i x_1 = \rho^j x_2 \Rightarrow$

$\rho^{i-j} x_1 = \rho^{-j} \rho^i x_1 = x_2 \Rightarrow x_2 \in Orb_\rho(x_1) \Rightarrow \rho^i x_2 \in Orb_\rho(x_1)\ \forall i \Rightarrow Orb_\rho(x_1) \subset Orb_\rho(x_2)$

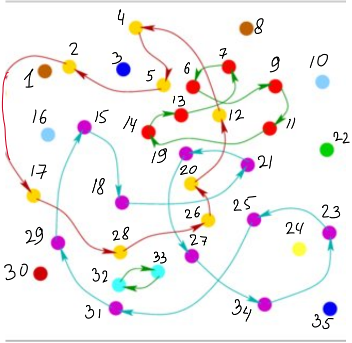
Similarly, $Orb_\rho(x_2) \subset Orb_\rho(x_1) \Rightarrow Orb_\rho(x_1) = Orb_\rho(x_2)$

Orbits of permutations on a set of elements

$E = \{1, 2 \ldots 35\}$

Group S_{35}

$\{5, 2, 17, 28, 26, 20, 12, 4\}$
$= \mathrm{Orb}_\rho(2) = \mathrm{Orb}_\rho(28)$



This permutation is $= (7,6,9,11,14,13)(19,27,34,23,25,31,29,15,18,21)(17,28,26,20,12,4,5,2)(32,33)$

The orbits are disjoint. Each orbit is a subset where the group element $\rho \in S_n$ acts by **a cyclic permutation**. Some orbits have only 1 element, that is unchanged under the action of ρ. The union of all orbits is the whole set E.

The cycle notation for the elements of S_n

Example:

$$\rho = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \in S_3.$$

$\langle \rho \rangle = \{1, \rho\}$, $\rho^2 = 1$.

$x = 1 \Rightarrow Orb_\rho(1) = \{1, 2\}$

$x = 2 \Rightarrow Orb_\rho(2) = \{1, 2\}$

$x = 3 \Rightarrow Orb_\rho(3) = \{3\}$

$E = \{1, 2, 3\} = Orb_\rho(1) \cup Orb_\rho(3)$

ρ is a cycle

Definition

$\pi \in S_n$ is a cycle if π has just one orbit with > 1 element. The length of the nontrivial orbit is the number of elements in the orbit.

The cycle notation for the elements of S_n

Example: ρ is a 2-cycle in S_3:

$$\rho = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

ρ has one nontrivial orbit $\{1, 2\}$
it is a cycle

Example: σ is not a cycle in S_4:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

$Orb_\sigma(1) = \{1, 2\}$
$Orb_\sigma(2) = \{1, 2\}$
$Orb_\sigma(3) = \{3, 4\}$
$Orb_\sigma(4) = \{3, 4\}$

2 nontrivial orbits:
$\{12\}$ and $\{34\}$
$\Rightarrow \sigma$ is not a cycle.

Notation for the cycle

Let $\pi \in S_n$ be a k-cycle. Then $\pi = (x, \pi(x), \pi^2(x) \dots \pi^{k-1}(x))$ for any $x \in Orb_\pi(x)$.

A cycle $(i_1, i_2, \dots i_k)$ is the permutation that sends $i_1 \to i_2$, $i_2 \to i_3$, ... $i_{k-1} \to i_k$, $i_k \to i_1$, and leaves the remaining elements of $E = \{1, 2, \dots n\}$ stable.

Example:

$$\rho = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

$\boxed{\rho = (1, 2)}$

Cycle notation

is written as $\rho = (12)$ in the cycle notation.

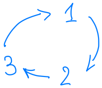
Notation for the cycle

Example:

$$\pi = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

$\pi = (1, 2, 3)$

Attention: $\pi = (2, 3, 1) = (3, 1, 2)$ denote the same element of S_3 that is π



$(123) = (231) = (312)$

$(132) \neq (123)$

$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \neq \pi = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$

π is a 3-cycle.

Conclusion: the cycle notation is defined up to a cyclic permutation

The length of the cycle = the number of elements in the nontrivial orbit of the cycle.

Disjoint cycles

Definition

Two cycles ρ and π in S_n are disjoint if their **nontrivial** orbits do not intersect.

Proposition

Disjoint cycles commute.

Proof: $\underset{\text{cycle}}{\pi_1} \longleftrightarrow \underset{\text{nontri}}{\mathcal{O}_1}$ $\quad \pi_2 \longleftrightarrow \mathcal{O}_2$ $\quad \mathcal{O}_1 \cap \mathcal{O}_2 = \emptyset \Rightarrow$ show $\pi_1\pi_2(x) = \pi_2\pi_1(x)$.

(1) $x \notin \mathcal{O}_1 \cup \mathcal{O}_2 \Rightarrow \pi_1 \underbrace{\pi_2(x)}_{=x} = \underbrace{\pi_1(x)}_{=x} = x$; $\pi_2 \underbrace{\pi_1(x)}_{=x} = \pi_2(x) = x$

(2) $x \in \mathcal{O}_1, x \notin \mathcal{O}_2 \Rightarrow \pi_1 \underbrace{\pi_2(x)}_{=x,\ x\notin\mathcal{O}_2} = \pi_1(x) = \underset{\in\mathcal{O}_1}{y}$ $\quad \pi_2\pi_1(x) = \pi_2(\underset{\in\mathcal{O}_1 \Rightarrow y\notin\mathcal{O}_2}{y}) = y$

(3) $x \in \mathcal{O}_2, x \notin \mathcal{O}_1$ is symmetric.

$\Rightarrow \pi_1\pi_2 = \pi_2\pi_1$ for disjoint cycles $\quad \blacksquare$

Disjoint cycles

Example 1: $\pi_1 = (251) \in S_6$, $\pi_2 = (346) \in S_6$ are disjoint cycles.

$(251)(346) = (346)(251)$

$\{2,5,1\} \cap \{3,4,6\} = \emptyset$

we proved that in this case

$\pi_1 \pi_2 = \pi_2 \pi_1$

Example 2: $\rho_1 = (251) \in S_6$, $\rho_2 = (23) \in S_6$ are not disjoint.

$(251)(23)$ not disjoint!

$\rho_1 \rho_2 \neq \rho_2 \rho_1$

Product of cycles in S_n

Examples:

$(12)(23) = (231)$

$(1426)(235) = (142356)$

$(1453)(321) = (1)(2453)$

Theorem

Any element $\sigma \in S_n$ can be written as a product of disjoint cycles. This presentation is unique up to the order of factors.

Proof:

$$E = \{1 \dots n\} = \bigcup_{i=1}^{r} Orb_\sigma(x_i) \quad ; \quad \text{Set } \pi_i = \sigma\big|_{Orb_\sigma(x_i)} \text{ trivial on } E \setminus Orb_\sigma(x_i)$$

$$\Rightarrow \sigma = \pi_1 \pi_2 \dots \pi_r$$

disjoint cycles

The cycle type in S_n

Definition

An element $\sigma \in S_n$ written as a product of disjoint cycles is called the cycle notation for σ. The set of lengths of the disjoint cycles in σ is called the cycle type of σ.

Example: $\sigma = (14)(236)$ cycle type $(2,3)$

$= (236)(14)$

conjugation of ρ by π

In the cycle notation it is easier to compute $\pi\rho\pi^{-1}$ than $\pi\rho$.

Conjugation in the cycle notation

Proposition

Let $\pi, \rho \in S_n$. The cycle notation for the element $\pi\rho\pi^{-1}$ is obtained from the cycle notation of ρ by replacing each number k in the cycle notation of ρ by $\pi(k)$. The elements ρ and $\pi\rho\pi^{-1}$ have the same cycle type.

Proof: Consider $\pi\rho\pi^{-1}(\pi(k)) = \pi\rho\underbrace{\pi^{-1}\pi}_{1}(k) = \pi\rho(k)$

Let ρ be a cycle $\rho : k \to \rho(k)$: $\rho = (k, \rho(k), \rho^2(k) \dots)$ cycle notation for ρ.

$\pi\rho\pi^{-1} : \pi(k) \to \pi\rho(k)$

$\pi\rho(k) \to \pi\rho(\rho(k)) = \pi\rho^2(k)$

$\pi\rho\pi^{-1} = (\pi(k), \pi\rho(k), \pi\rho^2(k) \dots\dots)$

$\Rightarrow \rho = (a_1 \ a_2 \dots \ a_m)$

$\pi\rho\pi^{-1} = (\pi(a_1) \ \pi(a_2) \ \dots \dots \pi(a_m))$

It works the same on a product of disjoint cycles.

Conjugation in the cycle notation

Examples: $\overset{\pi}{\downarrow}(45)(134)\overset{\pi^{-1}}{\downarrow}(45)^{-1}$ $= (\pi(1)\ \pi(3)\ \pi(4)) = (1\ 3\ 5)$

$(45)(134)(45) = (3\,5\,1)$

$\overset{\pi}{\downarrow}(234)(25461)\underset{(432)}{(234)^{-1}}$ $= (\pi(2)\ \pi(5)\ \pi(4)\ \pi(6)\ \pi(1)) = (3\ 5\ 2\ 6\ 1)$

Check by a direct computation: Exercice

Conjugation in the cycle notation

Proposition

Let $g, h \in S_n$. If $h = \rho_{l_1}\rho_{l_2}\dots\rho_{l_r}$ as a product of disjoint cycles of lengths $l_1, l_2, \dots l_r$, then $ghg^{-1} = \gamma_{l_1}\gamma_{l_2}\dots\gamma_{l_r}$ is a product of disjoint cycles of the same lengths. Any element that is a product of disjoint cycles of lengths $l_1, l_2, \dots l_r$ can be obtained from h by conjugation by an element of S_n.

Proof:

Suppose $\beta_{l_1}\beta_{l_2}\dots\beta_{l_r}$. Then $t\rho_{l_1}\rho_{l_2}\dots\rho_{l_r}t^{-1} = \beta_{l_1}\beta_{l_2}\dots\beta_{l_r}$
where t sends each number in each of the disjoint cycles
$\rho_{l_1}\dots\rho_{l_r}$ to the corresponding elt of the disjoint cycles
$\beta_{l_1}\dots\beta_{l_r}$

Conjugation in the cycle notation

Example:
Find an element $t \in S_7$ such that

$$t(12)(367)t^{-1} = (43)(156)$$

Write t in the cycle notation.

$$t: \begin{array}{ccccccc} (1 & 2) & (3 & 6 & 7) & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ (4 & 3) & (1 & 5 & 6) & 2 & 7 \end{array}$$

$$t = (1423)(657)$$

$$t': \begin{array}{ccccccc} (1 & 2) & (3 & 6 & 7) & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ (4 & 3) & (1 & 5 & 6) & 7 & 2 \end{array}$$

$t' = (1476523)$ also works:

$$t'(12)(367)(t')^{-1} = (43)(156)$$

Exercise: check by a direct computation:

$$t(12)(367)t^{-1} = t'(12)(367)(t')^{-1}$$

Poll: Product of cycles in S_n

$= \cancel{(1)}\cancel{(2)}(3564)$ (directly)

Poll: Let $\sigma = \overset{\pi}{\underbrace{(165)}}\underbrace{(32)(36)(4261)}\overset{\pi^{-1}}{\underbrace{(156)}} \in S_6$.

Then

$(6143)(2)$

$(32)(36)(4261) = (1436)(2) = (1436)$

$\underset{\pi}{\underset{\shortparallel}{(165)}}(1436)(165)^{-1} = (6435) \Rightarrow C$

$= (\pi(1)\ \pi(4)\ \pi(3)\ \pi(6)) =$

$= (6435)$

A: $\sigma = (16542)$

B: $\sigma = (165)(432)$

C: $\sigma = (6435)$

D: $\sigma = (64352)$

E: $\sigma = (15)(643)$

Conclusions

- A cycle $(i_1, i_2, \ldots i_n)$ is a permutation that sends $i_1 \to i_2$, $i_2 \to i_3$, ... $i_k \to i_1$ and stabilizes the remaining elements.
- Two cycles $(i_1, i_2, \ldots i_k) \in S_n$ and $(j_1, j_2, \ldots j_m) \in S_n$ are disjoint if and only if $i_t \neq j_p$ for all t and p.
- Disjoint cycles commute in S_n: if $i_t \neq j_p$ for all t and p, then $(i_1, i_2, \ldots i_k)(j_1, j_2, \ldots j_m) = (j_1, j_2, \ldots j_m)(i_1, i_2, \ldots i_k)$.
- Any $\sigma \in S_n$ can be written as a product of disjoint cycles $\sigma = (\ )(\quad)(\quad)\ldots(\ )$ uniquely up to the order of the cycles. The cycle type of σ is the set of lengths of the disjoint cycles in its decomposition.
- In S_n we have $\pi(i_1, i_2, \ldots i_k)\pi^{-1} = (\pi(i_1), \pi(i_2), \ldots \pi(i_k))$. The cycle type is preserved by conjugation.

Transpositions

Definition

A transposition is a 2-cycle in S_n. *Example:* $(1\,3)$ $(5\,2)$

Proposition

Every k-cycle in S_n is product of $(k-1)$ transpositions.

Proof: Induction on k: $k=2 \Rightarrow (i\,j)=(i\,j)$ is a transposition

$k=3 \Rightarrow (a\,b\,c)=(a\,c)(a\,b)$ direct computation

Induction step: Suppose $(1\,2\,3\,\ldots\,k)=(1\,k)(1\,k-1)\ldots(1\,3)(1\,2)$ induction hypothesis

Consider $(1\,2\,3\quad k\;k+1)=(1\quad k+1)(1\,2\,3\,\ldots\,k)=(1\;k+1)(1\,k)(1\;k-1)\ldots(1\,3)(1\,2)$

$\Rightarrow$ By induction, $(1\,2\,3\ldots\,k)=(1\,k)(1\;k-1)\ldots(1\,3)(1\,2)$

$\blacksquare$