

Algebra MATH-310

Lecture 5

Anna Lachowska

Written assignment: Published on November 17
15% of the grade due on November 24

October 13, 2025

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

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

$$\begin{array}{ccc} 1 & 2 & 3 \\ \swarrow & \downarrow & \\ 2 & 1 & 3 \end{array}$$

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

The cycle notation for the elements of S_n

Definition

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

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

is called the orbit of ρ in E . *of element x .*

$$\rho^k x = x$$

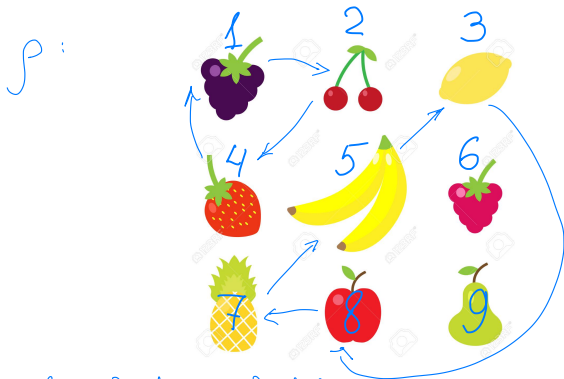
Proposition ρ is fixed

$E = \{1, 2, \dots, n\} = \bigcup_{i=1}^r \text{Orb}_\rho(x_i)$, and the union is disjoint.

Proof: $\{x_1, \rho x_1, \dots, \rho^{k-1} x_1\} \quad \{x_2, \rho x_2, \dots, \rho^{k-1} x_2\}$. If $\rho^i x_1 = \rho^j x_2 \Rightarrow$
 $\rho^{i-j} x_1 = (\rho^j)^{-1} \rho^i x_1 = x_2 \Rightarrow x_2 \in \text{Orb}_\rho(x_1) \Rightarrow \rho^i x_2 \in \text{Orb}_\rho(x_1) \Rightarrow \text{Orb}_\rho(x_2) \subset \text{Orb}_\rho(x_1)$
Symmetrically, $\text{Orb}_\rho(x_1) \subset \text{Orb}_\rho(x_2) \Rightarrow \text{Orb}_\rho(x_1) = \text{Orb}_\rho(x_2)$



Orbits of permutations on a set of elements



$$E = \{1, 2, 4\} \cup \{3, 8, 7, 5\} \cup \{6\} \cup \{9\}.$$

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:

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

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

$$\text{Orb}_\rho(1) = \text{Orb}_\rho(2) = \{1, 2\}$$

$$\text{Orb}_\rho(3) = \{3\}$$

$$E = \{1, 2, 3\} = \text{Orb}_\rho(1) \cup \text{Orb}_\rho(3)$$

ρ is a cycle, nontrivial orbit $\{1, 2\}$
of length 2.

Definition

$\pi \in S_n$ is a **cycle** if π has at most 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 :

$$\rho = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}. \quad \rho \text{ has one nontrivial orbit } \{1, 2\} \text{ it is a cycle}$$

Example: σ is **not a cycle** in S_4 :

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

σ has 2 nontrivial orbits: $\{1, 2\}$ and $\{3, 4\}$
 $\Rightarrow \sigma$ is not a cycle

Notation for the cycle

$$\pi^k = \text{id}$$

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

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

Example:

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

$$\rho = (12)$$

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

Cycle notation

Notation for the cycle

Example:

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

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

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



$$(123) = (231) = (312) = \pi$$

$$(132) \neq \pi$$

$$\parallel \\ \pi^{-1}$$

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: $\pi_1 \leftrightarrow O_1$ $\pi_2 \leftrightarrow O_2$: $O_1 \cap O_2 = \emptyset \Rightarrow$ show $\pi_1 \pi_2(x) = \pi_2 \pi_1(x) \forall x$
cycle nontr. orbit

$$(1) x \notin O_1, x \notin O_2 \Rightarrow \pi_1 \pi_2(x) = \pi_1(x) = x; \quad \pi_2 \pi_1(x) = \pi_2(x) = x$$

$$(2) x \in O_1, x \notin O_2 \Rightarrow \pi_1 \pi_2(x) = \pi_1(x) = y \in O_1; \quad \pi_2 \pi_1(x) = \pi_2(y) = y \in O_1, y \notin O_2$$

$$(3) x \notin O_1, x \in O_2 \text{ symmetric}$$

$\Rightarrow \pi_1 \pi_2 = \pi_2 \pi_1$ for disjoint cycles.



Disjoint cycles

$$= \sigma_{\pi_1} \\ \{2, 5, 1\}$$

$$= \sigma_{\pi_2} \\ \{3, 4, 6\}$$

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

$$\Rightarrow (251)(346) = (346)(251) \\ \pi_1 \pi_2 = \pi_2 \pi_1 \\ \{2, 5, 1\} \cap \{3, 4, 6\} = \emptyset$$

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

$$\{2, 5, 1\}$$

$$\{2, 3\}$$

$(251)(23)$ not disjoint!

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

Product of cycles in S_n

Examples:

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

$$(1426)(235) = (235614)$$

$$(1453)(321) = (3245)(1) = (3245)$$

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:

$$E = \{1, \dots, n\} = \bigcup_{i=1}^r \text{Orb}_{\sigma}(x_i), \quad \text{Set } \pi_i = \sigma \Big|_{\text{Orb}_{\sigma}(x_i)} \text{ and trivial on } E \setminus \text{Orb}_{\sigma}(x_i)$$

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

$\searrow \downarrow \swarrow$
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)*
 $= (236)(14)$

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 by $\pi(k)$. The elements ρ and $\pi\rho\pi^{-1}$ have the same cycle type.

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

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

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

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

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

$\Rightarrow \rho = (a_1, a_2, \dots, a_m)$ cycle notation

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

It works the same on a product of disjoint cycles.



Conjugation in the cycle notation

$$\begin{aligned} \text{Examples: } & \overline{\pi} \quad \overline{\pi}^{-1} \\ & (45)(134)(45)^{-1} = (\overline{\pi}(1) \ \overline{\pi}(3) \ \overline{\pi}(4)) = (1 \ 3 \ 5) \\ & \overleftarrow{(45)(134)(45)} = \underline{\underline{(351)}} \end{aligned}$$

$$\begin{aligned} & \overline{\pi} \quad \overline{\pi}^{-1} \\ & (234)(25461)(234)^{-1} = (\overline{\pi}(2) \ \overline{\pi}(5) \ \overline{\pi}(4) \ \overline{\pi}(6) \ \overline{\pi}(1)) = (35261) \\ & \quad \quad \quad \underline{\underline{(432)}} \end{aligned}$$

Exercise: check it by a direct computation.

$$(234)(25461)(432) = (35261)$$

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 $\beta_1, \beta_2, \dots, \beta_r$. Then $t \beta_1 \beta_2 \dots \beta_r t^{-1} = \beta_1 \dots \beta_r$
where t sends each number in each of the disjoint cycles
 β_1, \dots, β_r to the corresponding elt of the disjoint cycles
 β_1, \dots, β_r



Conjugation in the cycle notation

Example:

Find an element $t \in S_7$ such that

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

$$\begin{array}{cccc} (12)(367) & 4 & 5 & \\ \downarrow\downarrow & \downarrow\downarrow\downarrow & \downarrow\downarrow & \\ (43)(156) & 2 & 7 & \end{array}$$

$$\begin{array}{cccc} (12)(367) & 4 & 5 & \\ \downarrow\downarrow & \downarrow\downarrow\downarrow & \downarrow\downarrow & \\ (34)(156) & 2 & 7 & \end{array}$$

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

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

$$t' = (13)(24)(657) \text{ also works}$$

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

Exercise: check by a direct computation.

$$t(12)(367)t^{-1} = t'(12)(367)(t')^{-1} = (34)(156)$$

Poll: Product of cycles in S_n

Poll: Let $\sigma = (134)(425)(135)(23)(143) \in S_5$.

Then

A: $\sigma = (12345)$

B: $\sigma = (123)(45)$

C: $\sigma = (1435)$

D: $\sigma = (12)(345)$

E: $\sigma = (15)(243)$

$$\sigma = (125)(345)(24) = (12)(345)$$

Conclusions

- A **cycle** (i_1, i_2, \dots, i_n) is a permutation that sends $i_1 \rightarrow i_2, i_2 \rightarrow i_3, \dots, i_n \rightarrow i_1$ and stabilizes the remaining elements.
- Two cycles $(i_1, i_2, \dots, i_k) \in S_n$ and $(j_1, j_2, \dots, j_m) \in S_n$ 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 $(i_1, i_2, \dots, i_k)(j_1, j_2, \dots, j_m) = (j_1, j_2, \dots, j_m)(i_1, i_2, \dots, i_k)$.
- Any $\sigma \in S_n$ can be written as a **product of disjoint cycles** $\sigma = ()()(\dots) \dots ()$ 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 $\pi(i_1, i_2, \dots, i_k)\pi^{-1} = (\pi(i_1), \pi(i_2), \dots, \pi(i_k))$.
The cycle type is preserved by conjugation.

Transpositions

Definition

A **transposition** is a 2-cycle in S_n . Example: (13)

Proposition $k \geq 2$

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

Proof: Induction on k : $k = 2 \Rightarrow (ij) = (ij)$ is a transposition
 $k = 3 \Rightarrow (abc) = (ac)(ab)$

Hypothesis: $(12 \dots k) = (1k)(1k-1) \dots (13)(12)$

Induction step: Suppose \uparrow holds. $(12 \dots k k+1) = (1k+1)(123 \dots k) =$
 $= (1k+1)(1k)(1k-1) \dots (13)(12)$.

\Rightarrow By induction, $(123 \dots k) = (1k)(1k-1) \dots (13)(12)$



Products of transpositions

Corollary

The group S_n is generated by transpositions $\{(ij)\}_{1 \leq i < j \leq n}$.

Proof:

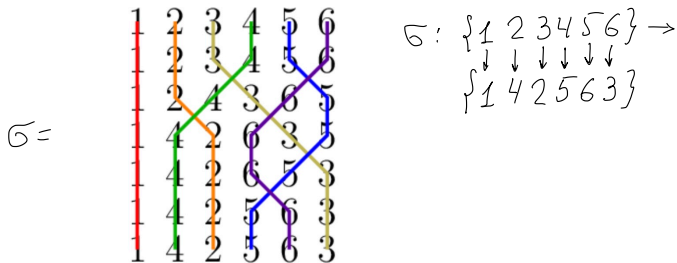
Any elt is a product of transpositions.
 $(ij) = (ji)$

Remark: This presentation is **not unique**.

$$\begin{aligned}(abc) &= (ac)(ab) \\ &= (ba)(cb)\end{aligned}$$

Any element of S_n is a product of transpositions

A transposition (ij) can be visualized as a crossing of two lines that correspond to elements i and j . Then any element $\sigma \in S_n$ can be represented as a tangle of threads. Each intersection corresponds to a transposition.



$\sigma =$

$$(56)(35)(24)(36)(34)(56) = (24563)$$

The sign of a permutation

Definition

An **inversion** in the ordered set $\{a_1, a_2, \dots, a_n\}$ is a couple $a_i > a_j$, where $i < j$.

Theorem

Let $\sigma \in S_n$ be given as a product of transpositions. Then the number of transpositions in σ has the same parity as the number of inversions in $\sigma(1, 2, \dots, n)$.

Proof: $\sigma(1 \ 2 \ \dots \ n) = (a_1 \ a_2 \ \dots \ i \ b_1 \ b_2 \ \dots \ j \ c_1 \ c_2 \ \dots)$

Act by (ij) . $(ij)\sigma(1 \ 2 \ \dots \ n)$ vs. $\sigma(1 \ 2 \ \dots \ n)$ how the # of inversions is changed?
 a_k, c_k do not contribute to the change of # of inversions.

If $b_k > i$ and $b_k > j$ or $b_k < i$ and $b_k < j \Rightarrow$ no change in # of inversions

If $i < b_k < j$ or $j < b_k < i \Rightarrow$ # of inversions changes by ± 2

Finally, the swap $i \leftrightarrow j$ adds or subtracts one more inversion.

\Rightarrow Totally, action by a transposition (ij) changes the # of inversions in a string by an **odd number**.

$\sigma = 1 \Rightarrow (1\ 2 \dots n)$ no inversions

$\sigma = (ij) \Rightarrow$ odd # of inversions in the result

$\sigma = (kl)(ij) \Rightarrow$ odd + odd = even # of inversions in the result

Therefore the number of transposition in σ has the same parity as the number of inversion in the resulting string $\sigma(1\ 2 \dots n)$.

Theorem

A product of an odd number of transpositions cannot be equal to a product of an even number of transpositions in S_n .

$\sigma(1\ 2 \dots n)$ has a fixed number of inversions.

The parity of the number of inversions equals the parity of the number of transpositions in σ .