Previously.

- Arithmetic Modulo n
- Some further results

This Section.

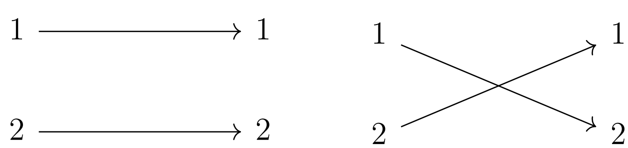
- Permutations
- Notation for Permutations
- Composition of Permutations
- Cycles
- Disjoint Cycles
- Transpositions
- Even vs Odd Permutations

Definition. A permutation of $T_n = \{1, 2, \ldots, n\}$ is a mapping $\sigma\colon T_n \to T_n$ that is both one-to-one and onto (a bijection).

We call the collection of all permutations of T_n the symmetric group of order n, and we write

$$S_n := \{\sigma\colon T_n \to T_n \mid \sigma \text{ is a permutation}\}.$$

Example. $n = 2$: $T_2 = \{1, 2\}$ and $S_n = \{\text{id}, \sigma\}$ where id is the identity map and σ is the map that swaps 1 and 2



id σ

Exercise 1. What are a couple of elements of S_3?

Note. We can define a permutation on any set X to be a bijection $\sigma\colon X \to X$. And the set of all permutation on X is the set of symmetries of X:

$$S_X := \{\sigma\colon X \to X \mid \sigma \text{ is a bijection}\}.$$

Notation 1 - Two-Line Notation

Definition (`Two-Line Notation`)**.** For $\sigma : T_n \to T_n$, we can write

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Think of the top row as the input and the bottom row as the output.

Exercise 2. In the case of $\sigma : T_4 \to T_4$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ means

(a) $\sigma(1) = 3$ (b) $\sigma(2) =$ (c) $\sigma(3) =$ (d) $\sigma(4) =$

Notation 2 - One-Line Notation

Definition (`One-Line Notation`)**.** For $\sigma : T_n \to T_n$, we can write

$$\sigma = \sigma(1)\ \sigma(2)\ \dots\ \sigma(n).$$

Think of the one line notation as only the bottom row of two-line notation.

Example. For the previous example, the permutation in two-line notation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

can instead be written as

$$\sigma = 3\ 2\ 4\ 1.$$

Exercise 3. There are 6 permutations in S_3. Write them in both one-line and two line notation.

Notation 3 - Cycle Notation

Definition. The r-cycle $(x_1\ x_2\ \dots\ x_r)$ in S_n is the permutation that sends

$$\begin{array}{ccc} x_1 & \mapsto & x_2 \\ x_2 & \mapsto & x_3 \\ x_3 & \mapsto & x_4 \\ & \vdots & \\ x_{r-1} & \mapsto & x_r \\ x_r & \mapsto & x_1. \end{array}$$

Example. $(2\ 4\ 1) \in S_5$ does the following

$$\begin{array}{ccc} 2 & \mapsto & 4 \\ 4 & \mapsto & 1 \\ 1 & \mapsto & 2 \end{array}$$

Question 4. What does this permutation do to 3 and 5?

Note. There are several equivalent ways to write $(2\ 4\ 1)$:

Exercise 5. Convert the permutation from two-line notation to cycle notation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 1 & 4 & 2 & 7 & 6 & 5 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 7 & 3 & 2 & 4 \end{pmatrix}$$

Exercise 6. Convert the permutation from cycle notation to two-line notation: Assume that $\alpha, \beta \in S_8$.

$\alpha = (1\ 4\ 5\ 7)(2\ 3)(6\ 8)$

$\beta = (3\ 8\ 7)$

Conventions. We establish the following conventions for cycle notation.

- The smallest number in a cycle will be written first.
- When there are multiple cycles, sort them according to their smallest element. (Do not do any sorting if any cycles have the same number!)

Definition. Two cycles $(x_1\ x_2\ \ldots\ x_r)$ and $(y_1\ y_2\ \ldots\ y_s)$ are `disjoint` if

$$\{x_1, x_2, \ldots, x_r\} \cap \{y_1, y_2, \ldots, y_s\} = \emptyset.$$

Theorem. Disjoint cycles commute. That is if σ and τ are disjoint cycles then $\sigma\tau = \tau\sigma$.

Theorem 1.4.5 (Cycle Decomposition Theorem). Every $\sigma \in S_n$ with $\sigma \neq \varepsilon$ can be written as a product of disjoint cycles.

Exercise 7. Let's complete this table of various notation for elements of S_3.

Verbal	Two-Line	One-Line	Cycle
Identity			
Swap $1 \leftrightarrow 2$			
Swap $1 \leftrightarrow 3$			
Swap $2 \leftrightarrow 3$			
$1 \to 2 \to 3 \to 1$			
$1 \to 3 \to 2 \to 1$			

Notation 4 - Permutation Matrices

Recall: Standard basis for $\mathbb{R}^n$, $\{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$
We can view permutations as "permuting" the indices of the $\vec{e}_i$.

Example. The permutation $\sigma = 3\,2\,4\,1$ corresponds to the linear transformation $T\colon \mathbb{R}^4 \to \mathbb{R}^4$ defined by

$$T(\vec{e}_1) = \vec{e}_3, \quad T(\vec{e}_2) = \vec{e}_2, \quad T(\vec{e}_3) = \vec{e}_4, \quad T(\vec{e}_4) = \vec{e}_1$$

Which corresponds to the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Read from the columns - 1 goes to 3 because the first column has a 1 in the 3rd row. That being said, as long as you're consistent with whether you read the row or the column, all will work out in the end.

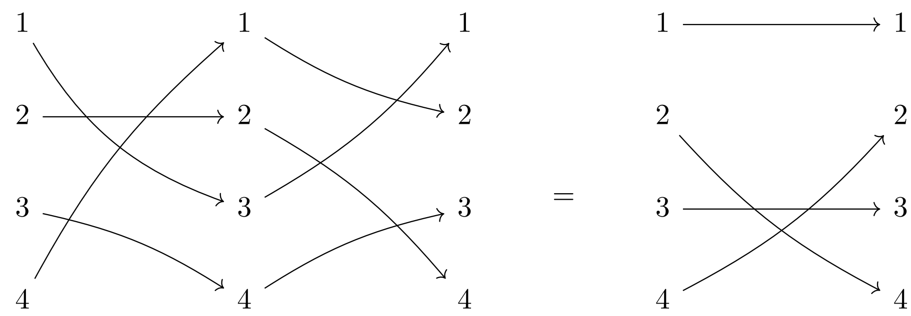
Definition. A `permutation matrix` is an $n \times n$ matrix that has exactly one 1 in each row and column and every other entry is 0.

Exercise 8. Write down all of the 3×3 permutation matrices.

Note. Every permutation matrix has determinant ± 1, and can be constructed by swapping columns (or rows) of the identity matrix.

Composition - The operation of permutations

Example. Suppose that, in cycle notation, $\sigma = (1\ 3\ 4)$ and $\tau = (1\ 2\ 4\ 3)$ and we want to compute $\tau \circ \sigma = \tau\sigma$. We could first translate to arrow diagrams.
Note that the composition notation means that $\tau\sigma(1) = \tau(\sigma(1))$, so we apply σ first. Thus we draw σ on the left, then we write τ.



σ τ $\tau\sigma$

Exercise 9. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 1 & 3 & 6 \end{pmatrix}$.

Write $\tau\sigma = \tau \circ \sigma$ in two-line notation.

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$$

Write $\sigma\tau = \sigma \circ \tau$ in two-line notation.

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$$

Multiplication in Cycle Notation

Note. When multiplying cycles, work from right to left one cycle at a time.

Exercise 10. Let $\alpha = (1\ 3\ 2)$, and $\beta = (1\ 5\ 3)$. Write $\alpha\beta$ and $\beta\alpha$ in cycle notation.

Exponents.. We write exponents to mean the repeated composition of :

$$\sigma^k := \underbrace{\sigma\sigma\cdots\sigma}_{k}.$$

Exercise 11. Let $\sigma = (1\ 4\ 2\ 6) \in S_6$. Compute σ^k for $k = 2, 3, 4, 5, \ldots$.

Order of a Permutation

Definition. The order of a permutation, $\sigma \in S_n$ is the smallest positive integer k such that $\sigma^k = \varepsilon$.

Exercise 12. (a) What is the order of $(1\ 2)(3\ 4)$?

(b) What is the order of $(1\ 2)(3\ 4\ 5)$?

Note. In the homework: Prove that the order of an r-cycle is r.

Inverse Permutations

Exercise 13. Recall that permutations are bijective maps, so they ALL have inverses! (Woo!)

(a) Find the inverse of the cycle $(1\ 2)$.

(b) Find the inverse of the cycle $(1\ 4\ 2\ 5\ 3\ 6)$.

Theorem. The inverse of the cycle $(x_1\ x_2\ \ldots\ x_r)$ is the cycle $(x_r\ x_{r-1}\ \ldots\ x_2\ x_1)$.

Exercise 14. If $\sigma = (1\ 2\ 3)$ and $\tau = (3\ 2\ 1)$, verify that $\sigma\tau = \varepsilon$ and $\tau\sigma = \varepsilon$.

Theorem 0.3.5(3) - Specialized. Let $\sigma, \tau \in S_n$, then

$$(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}.$$

Exercise 15. Let $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (5\ 6)$.
Use Theorem 0.3.5 to compute $(\sigma\tau)^{-1}$.

Transpositions

Definition. A `transposition` is a cycle of length 2.

Theorem 1.4.6. If $n \geq 2$, then every cycle in S_n can be written as a product of transpositions.

"Proof."

$$(x_1\ x_2\ \ldots\ x_r) = (x_1\ x_r)(x_1\ x_{r-1}) \cdots (x_1\ x_3)(x_1\ x_2) \tag{1}$$

□

Exercise 16. Verify that $(1\ 2\ 5\ 3) = (1\ 3)(1\ 5)(1\ 2)$.

Exercise 17. Write $(1\ 5\ 4)(2\ 6\ 7\ 8\ 3)$ as a product of transpositions.

Even Permutations and the Alternating Group

Definition. A permutation $\sigma \in S_n$ is called even if it can be written as a product of an even number of transpositions.
Similarly, permutations can be called odd.

The Parity Theorem (Theorem 1.4.7). If a permutation has two factorizations

$$\sigma = \gamma_n \cdots \gamma_2 \gamma_1 = \mu_m \cdots \mu_s \mu_1,$$

where each of γ_i and μ_j are transpositions, then $m \equiv n \pmod 2$ (m and n have the same parity).

Definition. The alternating group of degree n is the set of even permutations in S_n. We call it A_n.

Exercise 18. Determine A_3.

Question 19. How do you think $|A_n|$ compares with $|S_n|$?

Exercise 20. Determine whether each of the following permutations is even or odd.

(a) (2 3 6 8 5 7)

(b) (2 8 5)(3 7)

(c) (1 4)(2 9 8)(3 7)

(d) (1 4 6)(2 5)(3 8 7)

More Practice

Exercise 21. Let $f = (1\ 3)(2\ 5\ 6\ 8\ 4)$ and $g = (1\ 5\ 2\ 4)(3\ 7)(6\ 8)$.

(a) Compute

i. fg

ii. g^{-1}

iii. f^{-1}

iv. fgf^{-1}

Note. The set S_n has an operation, composition. With this operation on S_n, we have

(a) an identity, id, the identity map, usually denoted ε

(b) associativity, $\sigma \circ (\tau \circ \gamma) = (\sigma \circ \tau) \circ \gamma$, and

(c) inverses, if $\sigma \in S_n$, then $\sigma^{-1} \in S_n$.

A look ahead to the future: This is why we can call S_n a *group*.