

CONTENTS

1. Recollections on Permutation Groups.....	1
2. Cycle Notation.....	2

1. RECOLLECTIONS ON PERMUTATION GROUPS

For a positive integer n , let us define

$$[n] := \{1, 2, \dots, n\}. \quad (1.1)$$

A permutation of $[n]$ is a bijection $p: [n] \rightarrow [n]$. It may be displayed in two-line notation as

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix}. \quad (1.2)$$

If p and q are permutations, we use the convention

$$qp = q \circ p; \quad (1.3)$$

thus the rightmost permutation is applied first. Let us also note that if p is a permutation, we write p^{-1} for the inverse permutation; that is, if $p(i) = k$, then $p^{-1}(k) = i$. One can check that

$$pp^{-1} = p^{-1}p = \text{id}, \quad (1.4)$$

where id is the identity permutation.

Let S_n denote the set of all permutations of $[n]$.

Proposition 1.1. *The triple $(S_n, \circ, \text{id})$ is a group.*

Proof. The composite of two bijections is again a bijection, so S_n is closed under composition. Composition of functions is associative, the identity map id is the identity element, and the inverse of a bijection is again a bijection. Hence all the group axioms hold. $\square$

2. CYCLE NOTATION

For future applications, we need to introduce the important ‘cycle notation’.

Definition 2.1. Fix a positive integer n and an integer k with $1 \leq k \leq n$. For distinct elements $a_1, \dots, a_k \in [n]$, the k -cycle $\sigma = (a_1 \cdots a_k)$ is the permutation defined by

$$\sigma(a_i) = a_{i+1} \quad (1 \leq i < k), \quad \sigma(a_k) = a_1. \quad (2.1)$$

Thus it sends $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$ and fixes every element outside $\{a_1, \dots, a_k\}$. Every one-cycle represents the identity permutation, which we denote by id or (1) . The empty product also represents the identity. A cycle of the form $(a \ b)$, with $a \neq b$, is called a *transposition*.

For example, the cycle

$$p = (1 \ 2 \ 3) \quad (2.2)$$

sends 1 to 2, 2 to 3, and 3 to 1, while fixing every other element. Thus, as a permutation of $[5]$,

$$(1 \ 2 \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}. \quad (2.3)$$

Cyclic rotations of the entries represent the same cycle. For example,

$$(1 \ 2 \ 3) = (2 \ 3 \ 1) = (3 \ 1 \ 2). \quad (2.4)$$

Composing cycles. If p, q are cycles then we would like to develop some tools for composing them, i.e. for calculating the product pq . Let’s start with a simple example:

Example 2.1 (Composing disjoint cycles). Let $q = (2 \ 3 \ 4)$ and $p = (1 \ 5)$. Then

$$qp = (2 \ 3 \ 4)(1 \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}. \quad (2.5)$$

When the entries in cycles are disjoint, the two permutations commute:

$$(2 \ 3 \ 4)(1 \ 5) = (1 \ 5)(2 \ 3 \ 4). \quad (2.6)$$

Cycles that are not disjoint *need not commute*. For example, you can verify that, as permutations of $[4]$, $(2 \ 4)(1 \ 4) \neq (1 \ 4)(2 \ 4)$. Indeed, we have

$$(2 \ 4)(1 \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad (1 \ 4)(2 \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}. \quad (2.7)$$

Here is a basic fact:

Lemma 2.1. *Every permutation is a product of disjoint cycles.*

Proof. Let p be a permutation of $[n]$. Choose $a_1 \in [n]$ and consider the sequence obtained by repeatedly applying p to a_1 , namely,

$$a_1, p(a_1), p^2(a_1), \dots \quad (2.8)$$

Since $[n]$ is finite, some term must eventually repeat. Let k be the first positive integer for which $p^k(a_1)$ is equal to an earlier term, say $p^k(a_1) = p^j(a_1)$ with $0 \leq j < k$. If $j > 0$, applying p^{-1} gives $p^{k-1}(a_1) = p^{j-1}(a_1)$, contradicting the choice of k . Hence $j = 0$.

It follows that

$$a_1, p(a_1), \dots, p^{k-1}(a_1) \quad (2.9)$$

are distinct and that p acts on them as the cycle

$$(a_1 \ p(a_1) \ \cdots \ p^{k-1}(a_1)). \quad (2.10)$$

If this cycle does not contain every element of $[n]$, choose an unused element a_2 and repeat the argument. The new cycle is disjoint from the first one: if the two cycles shared an element, say d , then for some $i, j \geq 0$ we must have

$$d = p^i(a_1) = p^j(a_2). \quad (2.11)$$

Repeatedly applying p (or p^{-1}) to this equation shows that a_2 lies in the first cycle, a contradiction.

Repeating this process gives pairwise disjoint cycles containing every element of $[n]$. Their product agrees with p on every element, and therefore equals p . (Cycles of length one may be omitted.)

□

Example 2.2 (Disjoint cycles in S_5). Consider

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}. \quad (2.12)$$

Starting with 1 and following its images gives

$$1 \mapsto 4 \mapsto 2 \mapsto 1, \quad (2.13)$$

while the remaining elements that are not yet accounted for satisfy

$$3 \mapsto 5 \mapsto 3. \quad (2.14)$$

Thus the decomposition of p into disjoint cycles is

$$p = (1 \ 4 \ 2)(3 \ 5). \quad (2.15)$$