Chapter 5

Defn: Let A be a nonempty set.
A permutation of A is a bijection $\alpha: A \to A$.
The permutation group of A is the set of all permutations of A with the binary operation of composition of functions.

We will focus on the case where $A = \{1, 2, 3, \dots, n\}$ for some $n \in \mathbb{Z}$, $n \geq 1$.

Defn: The symmetric group of degree n, denoted S_n, is the permutation group of $\{1, 2, \dots, n\}$.
We will denote the identity of S_n by ε

Ex/Defn: Consider $\alpha \in S_5$ where
$\alpha(1) = 4 \quad \alpha(2) = 3 \quad \alpha(3) = 5 \quad \alpha(4) = 1 \quad \alpha(5) = 2$

We express α in array form by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix}$$

← input values written in order

← associated output values

In general, for $\beta \in S_n$ we write

$$\beta = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ \beta(1) & \beta(2) & \beta(3) & \cdots & \beta(n) \end{bmatrix}$$

Suppose $\alpha \in S_5$ is as above and

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix}$$

Then

$$\alpha\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{bmatrix}$$

Also

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}$$

Note: When building $\alpha \in S_n$ you have

- n choices for $\alpha(1)$
- $n-1$ remaining choices for $\alpha(2)$

  ⋮

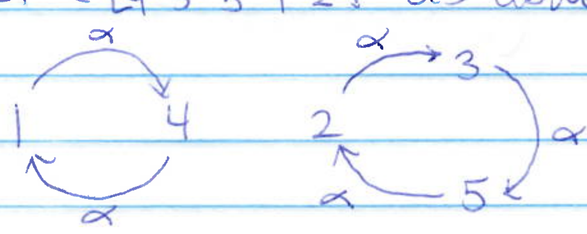
- 2 choices for $\alpha(n-1)$
- only 1 choice for $\alpha(n)$

Therefore S_n has order $|S_n| = n!$

Cycle Notation

Every $\alpha \in S_n$ divides (partitions) S_n into cycles

Ex: $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix}$ as above



We therefore write α in <u>cycle notation</u> as

$$\alpha = (14)(235)$$

<u>Note</u>: The cycle notation is not unique.
We could also write

$$\alpha = (235)(14) \text{ or}$$
$$\alpha = (41)(352) \text{ or}$$
$$\alpha = (523)(14) \text{ etc.}$$

Here's another example

if $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 3 & 7 & 2 & 5 \end{bmatrix}$

Then in cycle notation

$$\beta = (143)(26)(57)$$

And another

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 3 & 2 & 7 & 4 & 5 \end{bmatrix}$$

$$\gamma = (1642)(3)(57)$$

When there are cycles having only one element, it is customary to not write them

$$\gamma = (1642)(57)$$

Similarly if

$$\delta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{bmatrix}$$

Then we can write

$$\delta = (1\,5)(2)(3)(4\,7)(6)$$

or

$$\delta = (1\,5)(4\,7)$$

with the bottom notation being most preferred.

For the identity

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix}$$

we can write

$$\varepsilon = (1) \text{ or } \varepsilon = (2) \text{ or } \cdots \text{ or } \varepsilon = (7)$$

<u>Defn</u> A permutation of the form $(a_1, a_2, \cdots, a_m)$ is called a <u>cycle of length m</u> or an <u>m-cycle</u>

~~Ex: Write $\alpha\beta$ in cycle notation~~

<u>Note</u>: When we express permutations using cycle notation, we typically wish to express them as a product of <u>disjoint</u> cycles (meaning no two distinct cycles have a number in common)

<u>Ex</u>: Express $\alpha\beta \in S_8$ as a product of disjoint cycles if

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

$\alpha\beta = (1\ 6\ 5\ 2\ 4)(3\ 7)(2\ 8\ 4)(1\ 5)(6\ 7)$ ← but these cycles are not disjoint

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

$$\boxed{\alpha\beta = (1\ 2\ 8)(3\ 7\ 5\ 6)}$$

<u>Thm 5.1</u>: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Should be intuitively self-evident. See the book for detailed proof.

<u>Thm 5.2</u>: If $\alpha = (a_1, a_2, \cdots, a_m)$ and $\beta = (b_1, b_2, \cdots, b_n)$ are disjoint cycles then $\alpha\beta = \beta\alpha$

<u>Pf</u>: Say α, β are permutations of a set S. To show the functions $\alpha\beta$ and $\beta\alpha$ are equal, we must check that $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all $x \in S$. Consider any $x \in S$.

Case 1: $x = a_i$ for some $1 \le i \le m$.

Then $\alpha(x) = a_j$ where

$$j = \begin{cases} i+1 & \text{if } i < m \\ 1 & \text{if } i = m \end{cases}$$

Since α and β are disjoint we have $\beta(x) = \beta(a_i) = a_i = x$ and $\beta(a_j) = a_j$.

So

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = a_j = \beta(a_j) = \beta(\alpha(x)) = (\beta\alpha)(x)$$

Case 2: $x = b_i$ for some $1 \le i \le n$

As in Case 1, $\beta(x) = b_j$ for some j and $\alpha(x) = x$, $\alpha(b_j) = b_j$ (since α, β disjoint).

So

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(b_j) = b_j = \beta(x) = \beta(\alpha(x)) = (\beta\alpha)(x)$$

Case 3: $x \notin \{a_1, \dots, a_m, b_1, \dots, b_n\}$

Then $\alpha(x) = x$ and $\beta(x) = x$ so

$$(\alpha\beta)(x) = \alpha(\beta(x)) = x = \beta(\alpha(x)) = (\beta\alpha)(x) \quad \boxtimes$$

Thm 5.3: The order of a product of disjoint cycles is equal to the least common multiple of the lengths of the cycles

Pf: We'll prove this for the product of 2 disjoint cycles. The proof of the general case is similar.

Say α and β are disjoint cycles of lengths m and n. Note that

$$m = \text{order of } \alpha, \quad n = \text{order of } \beta.$$

Setting $k = \text{lcm}(m,n)$, we have $\alpha^k = \varepsilon = \beta^k$.

Since α, β disjoint, they commute, so

$$(\alpha\beta)^k = \alpha^k \beta^k = \varepsilon\varepsilon = \varepsilon$$

Therefore (order of $\alpha\beta$) $\leq k$.

On the other hand, for every $0 < t < k$ we have that α^t and β^{-t} are disjoint since α, β are disjoint, so we must have

$$\alpha^t \neq \beta^{-t}$$ (since they are disjoint and at least one is not ε since $0<t<\text{lcm}(m,n)$)

thus $\alpha^t \beta^t \neq \varepsilon$ and so $(\alpha\beta)^t = \alpha^t\beta^t \neq \varepsilon$. $\square$

<u>Ex</u>: Order of $(169)(25)(78)$ is $\text{lcm}(3,2,2) = 6$

Order of $(5732)(146)(89)$ is $\text{lcm}(4,3,2) = 12$

<u>Ex</u>: List all possible orders for elements of S_6.

The identity has order 1. All other elements can be written as a product of disjoint cycles each having length at least 2, and the sum of their lengths at most 6 (since the cycles must partition the 6 element set $\{1,2,3,4,5,6\}$). We list all possibilities:

- the identity — order 1
- a 6-cycle — order 6
- a 5-cycle — order 5
- a 4-cycle — order 4
- a 4-cycle & a 2-cycle — order 4
- a 3-cycle — order 3
- a 3-cycle & a 2-cycle — order 6
- a 3-cycle & a 3-cycle — order 3
- a 2-cycle — order 2
- a 2-cycle & a 2-cycle — order 2
- a 2 cycle & a 2-cycle & a 2-cycle — order 2

So $\{\text{order of } \alpha : \alpha \in S_6\} = \{1, 2, 3, 4, 5, 6\}$

(See Example 5 in the book for something more interesting)

Ex: How many elements in S_6 have order 6?

By previous example, ~~~~ the elements in S_6 of order 6 are 6-cycles and products of a 3-cycle and a disjoint 2-cycle

There are $6!$ ways to order the numbers 1 through 6, and each such ordering describes a 6-cycle. However each 6-cycle $(a_1 a_2 \cdots a_6)$ can be written in 6 ways:

$$(a_1 a_2 \cdots a_6) = (a_2 a_3 \cdots a_6 a_1) = \cdots = (a_6 a_1 a_2 \cdots a_5)$$

So # of 6-cycles $= 6!/6 = 5! = 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120$

Similarly,

$$\underbrace{\begin{matrix}\text{\# permutations that} \\ \text{can be written as a} \\ \text{product of a 3-cycle} \\ \text{and a disjoint 2-cycle}\end{matrix}}{} = \frac{\overbrace{6\cdot5\cdot4}^{\substack{\text{\# of ways of choosing an ordered} \\ \text{sequence of 3 elements} \\ \text{from 1 through 6}}}}{\underset{\substack{\text{every 3-cycle} \\ \text{can be written} \\ \text{in 3 ways}}}{3}} \cdot \frac{\overbrace{3\cdot2}^{\substack{\text{\# of ways of choosing} \\ \text{an ordered pair} \\ \text{from a set of 3 elements}}}}{\underset{\substack{\text{every 2-cycle} \\ \text{can be written} \\ \text{in 2 ways}}}{2}} = 120$$

Therefore S_6 has $120+120=\boxed{240}$ elements having order 6

<u>Thm 5.4</u>: Every $\alpha \in S_n$ (with $n>1$) can be written as a product of 2-cycles

<u>Pf</u>: α can be written as a product of disjoint cycles (Thm 5.2). So it suffices to check every cycle can be written as a product of 2-cycles. Indeed, one can directly verify that

$$(a_1 a_2 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \cdots (a_1 a_2). \quad \square$$

<u>Ex</u>: $(5\,1\,3\,2\,4) = (5\,4)(5\,2)(5\,3)(5\,1)$

Any given permutation can be written as a product of 2-cycles in many ways. However:

<u>Lemma</u>: If $\underset{\text{the identity}}{\varepsilon} = \beta_1\beta_2\cdots\beta_r$ where each β_i is a 2-cycle, then r is even.

Pf: See the book.

Thm 5.5: Every permutation of a finite set can be written as a product of an even number of 2-cycles or a product of an odd number of 2-cycles, but not both

Pf: Towards a contradiction, suppose there is a permutation α and 2-cycles $\beta_1, \ldots, \beta_r, \gamma_1, \ldots, \gamma_s$ with $\beta_1 \beta_2 \cdots \beta_r = \alpha = \gamma_1 \gamma_2 \cdots \gamma_s$, r even, and s odd. Then

$$\varepsilon = \beta_r^{-1} \beta_{r-1}^{-1} \cdots \beta_1^{-1} \gamma_1 \gamma_2 \cdots \gamma_s$$

and $r+s$ is odd, contradicting the above lemma □

Defn A permutation is

- even if it can be written as a product of an even number of 2-cycles
- odd if it can be written as a product of an odd number of 2-cycles.

Thm 5.6 The set of even permutations in S_n form a subgroup of S_n.

Pf: We'll use One-Step Subgroup Test.
e is even by Lemma, so set of even permutations is nonempty.

Next suppose α, β are even permutations.
This means there are 2-cycles $\gamma_1, \dots, \gamma_r$, $\delta_1, \dots, \delta_s$ with r, s even and

$$\alpha = \gamma_1 \cdots \gamma_r, \quad \beta = \delta_1 \cdots \delta_s.$$

Then

$$\alpha\beta^{-1} = \gamma_1\gamma_2 \cdots \gamma_r (\delta_1\delta_2 \cdots \delta_s)^{-1}$$
$$= \gamma_1\gamma_2 \cdots \gamma_r \delta_s \delta_{s-1} \cdots \delta_1 \quad \text{(2-cycles are their own inverse)}$$

Since $r+s$ is even, $\alpha\beta^{-1}$ is an even permutation $\square$

Defn The group of even permutations of $\{1, 2, \dots, n\}$ is denoted A_n and called the alternating group of degree n

Thm 5.7 A_n has order $\frac{n!}{2}$.

Pf: Define $f: S_n \to S_n$ by $f(\alpha) = (12)\alpha$.
Then f is a bijection, and it takes even permutations to odd permutations and odd permutations to even permutations. So

$$\#\text{ even permutations} = \#\text{ odd permutations}$$

and therefore $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}(n!)$ $\square$