3. The Symmetric Group

Recall that given a set S, we define $A(S)$ to be the set of all permutations on S:

$$A(S) = \{f : S \to S \ : \ f \text{ is a bijection}\}.$$

This is a group under the operation of composition of functions.

When $S = \{1, \ldots, n\}$, we denote this group by S_n, and call it the <u>symmetric group</u> of degree n.

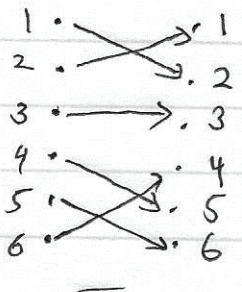
Note that $|S_n| = n!$ The elements of S_n are bijections of $\{1, \ldots, n\}$ onto itself. Thus, if $\sigma \in S_n$ then σ maps $\{1, \ldots, n\}$ 1-1 and onto itself. Hence σ simply rearranges, or permutes, the numbers $1, \ldots, n$. Therefore the elements of S_n are called <u>permutations</u>. They are typically denoted by lowercase greek letters.

3.1 Preliminaries

Notation for permutations

There are many ways to describe a permutation. Here are four ways that we will use interchangably. We illustrate these for a particular permutation $\sigma \in S_6$.

a. Picture:



σ

b. Explicit listing:

$$\sigma(1) = 2$$
$$\sigma(2) = 1$$
$$\sigma(3) = 3$$
$$\sigma(4) = 5$$
$$\sigma(5) = 6$$
$$\sigma(6) = 4$$

c. Two-line form:

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

d. Cycle notation:

$$\sigma = (12)(3)(456) = (12)(456)$$

We will explore cycle notation in more detail next.

3.2 Cycle Decomposition

Definition

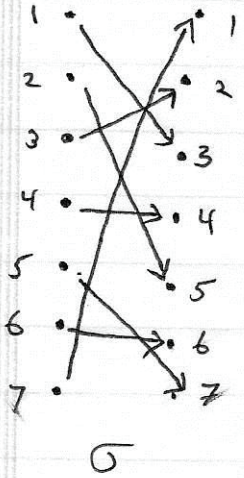
Let $i_1, i_2, \ldots, i_k$ be k distinct integers in $\{1, \ldots, n\}$.

Then $\sigma = (i_1\ i_2\ \cdots\ i_k)$ denotes the permutation of $\{1, \ldots, n\}$ defined by

$$\sigma(i_1) = i_2$$
$$\sigma(i_2) = i_3$$
$$\vdots$$
$$\sigma(i_{k-1}) = i_k$$
$$\sigma(i_k) = i_1$$

and $\sigma(i) = i$ for $i \neq i_1, \ldots, i_k$

Example $\sigma \in S_7$



σ

Two-line

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

Cycle

$(1\,3\,2\,5\,7)$

Note that the elements 4 and 6 are fixed by this permutation

Notation: We say that σ is a 5-cycle because it permutes 5 of the integers in $\{1, \ldots, 7\}$.

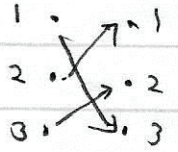
Example: $(1\,3\,2\,5\,7)(4\,6)$ is not a cycle - it is a composition of cycles

Notes

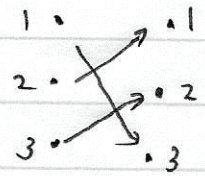
a. Cycle notation is not unique. The previous example can be written as

$$\begin{aligned}\sigma &= (1\,3\,2\,5\,7)\\ &= (3\,2\,5\,7\,1)\\ &= (2\,5\,7\,1\,3)\\ &= (5\,7\,1\,3\,2)\\ &= (7\,1\,3\,2\,5)\end{aligned}$$

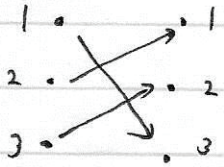
b. You can't tell from cycle notation what n is. For example, $(1\,3\,2)$ denotes a cycle in $S_3, S_4, S_5 \ldots$



$(1\,3\,2) \in S_3$



$(1\,3\,2) \in S_4$



$(1\,3\,2) \in S_5$

Definition
A 2-cycle is called a transposition.

If $\sigma = (j\ k) \in S_n$ is a transposition, then

$$\sigma(j) = k, \quad \sigma(k) = j, \quad \& \ \sigma(i) = i \text{ for } i \neq j, k$$

Thus σ just exchanges, or transposes, the two integers j & k and leaves all other numbers in $\{1, \ldots, n\}$ alone.

Exercise
If $\sigma = (i_1\ i_2 \cdots i_k)$ is a k-cycle, then

$o(\sigma) = k$, i.e., $\sigma, \sigma^2, \ldots, \sigma^{k-1} \neq e$ (the identity map on $\{1, \ldots, n\}$) and $\sigma^k = e$. That is, k is the smallest positive integer such that $\sigma^k = e$

Exercise
If $\sigma = (i_1\ i_2 \cdots i_k)$ then

$$i_2 = \sigma(i_1), \quad i_3 = \sigma^2(i_1), \quad \ldots, \quad i_k = \sigma^{k-1}(i_1),$$

so $\sigma = (i_1\ \sigma(i_1)\ \sigma^2(i_1) \cdots \sigma^{k-1}(i_1))$.

Recall that if $f \in A(S)$, which means that $f: S \to S$ is a bijection, then the orbit of $s \in S$ is

$$[s] = \{ f^n(s) : n \in \mathbb{Z} \}.$$

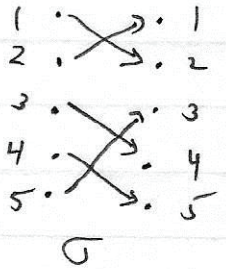
Exercise

Show that if $\sigma = (i_1\ i_2\ \cdots\ i_k)$ is a k-cycle then

$$[i_1] = \{ i_1, i_2, \ldots, i_k \}$$

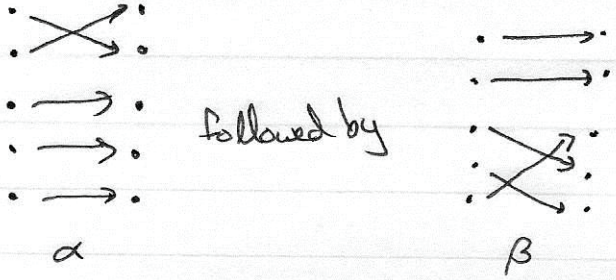
Notes

Not every permutation is a k-cycle. For example



σ is not a cycle.

However, σ is a composition of two cycles:



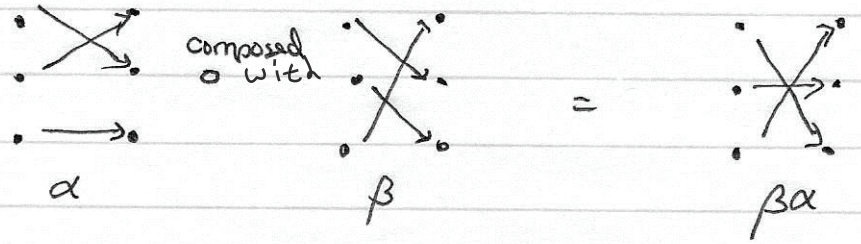
$\sigma = \beta\alpha = (1\,2)(3\,4\,5)$

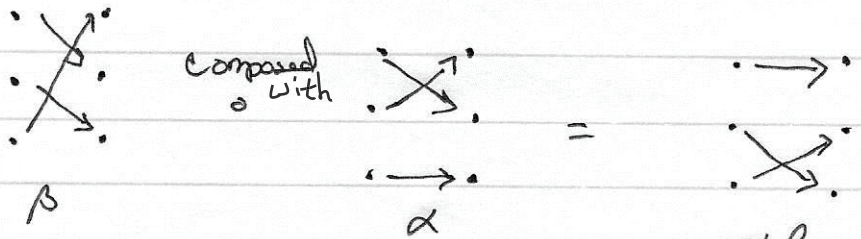
Be careful with order: α followed by β is the composition $\beta\alpha$! Thus we are saying that

$$\sigma = \beta\alpha.$$

For this example we also have $\sigma = \alpha\beta$, but in general cycles need not commute.

Example





In cycle notation:

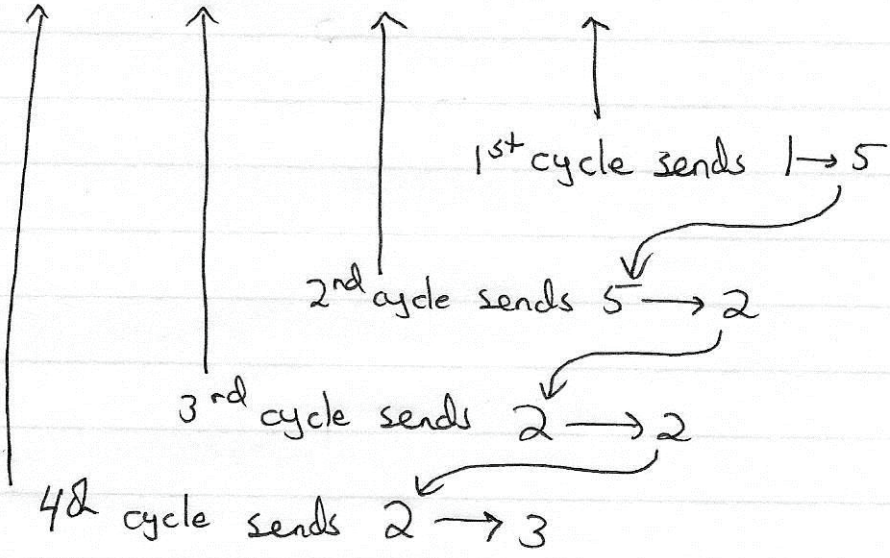
$$\beta\alpha = (1\ 2\ 3)(1\ 2) = (1\ 3)$$

$$\alpha\beta = (1\ 2)(1\ 2\ 3) = (2\ 3)$$

Exercise

Practice computing cycles! What is

$$\sigma = (2\,3\,5\,4)(1\,3)(2\,4\,3\,5)(1\,5) \quad ?$$



All told, σ mapped $1 \longrightarrow 3$, so $\sigma(1) = 3$.

Now determine all the other values $\sigma(i)$. It's easiest to follow through the orbits. Check $i = 3$ next:

$$3 \longrightarrow 3 \longrightarrow 5 \longrightarrow 5 \longrightarrow 4 \quad \text{so } \sigma(3) = 4$$

Then check $i = 4$:

$$4 \longrightarrow 4 \longrightarrow 3 \longrightarrow 1 \longrightarrow 1 \quad \text{so } \sigma(4) = 1.$$

We're back to where we started, so $\{1, 3, 4\}$ is one orbit. Now find the others. For $i = 2$, σ maps

$$2 \longrightarrow 2 \longrightarrow 4 \longrightarrow 4 \longrightarrow 2 \quad \text{so } \sigma(2) = 2$$

Finally, for $i = 5$:

$$5 \to 1 \to 1 \to 3 \to 5 \qquad \text{so } \sigma(5) = 5.$$

Thus σ is the 3-cycle

$$\sigma = (1\ 3\ 4)$$

Note
You don't have to end with a single cycle. Check that

$$(3\ 4)(1\ 3)(3\ 2)(1\ 3) = (1\ 2)(3\ 4)$$

Note

For two cycles we can easily tell if they are disjoint: just check whether they share any common numbers. For example,

$$(1\ 3\ 5) \quad \text{and} \quad (2\ 6\ 4)$$

are disjoint.

However, it becomes more complicated to tell if the permutations are not written in "simple" form. For example, are

$$(1\ 2\ 3)(2\ 3) \quad \text{and} \quad (3\ 4)$$

disjoint? Yes, because

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

This is a cycle that is "disjoint" from $(3\ 4)$

It is much easier to deal with permutations when they are written as compositions of disjoint cycles.

Question

Can an arbitrary permutation be written as a product of disjoint cycles?

Answer: Yes!

The difficult part of computing compositions of permutations is when both permutations move the same numbers. For example,

$$(1\ 3) \quad \text{and} \quad (1\ 3\ 2)$$

both move 3. Their composition is

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

as we can check by seeing where each $i = 1, 2, 3$ gets moved to by the composition.

In contrast, compositions are easy when the two cycles move completely different elements. For example,

$$(1\ 3)(2\ 4)$$

simply interchanges $1 \leftrightarrow 3$ & $2 \leftrightarrow 4$. We say that $(1\ 3)$ & $(2\ 4)$ are disjoint because they move completely different elements. An especially nice fact is that

disjoint cycles commute!

We have $(1\ 3)(2\ 4) = (2\ 4)(1\ 3)$.

Definition

A permutation $\sigma \in S_n$ *moves* $i \in \{1, \ldots, n\}$ if $\sigma(i) \neq i$.

A permutation $\sigma \in S_n$ *fixes* $i \in \{1, \ldots, n\}$ if $\sigma(i) = i$.

Definition

Permutations $\sigma, \tau \in S_n$ are *disjoint* if for each $i = 1, \ldots, n$,

$$\sigma \text{ moves } i \implies \tau \text{ fixes } i$$

and

$$\tau \text{ moves } i \implies \sigma \text{ fixes } i$$

Example

$\sigma = (1\ 6)(2\ 7\ 8)$ and $\tau = (3\ 5\ 4)$

are disjoint.

Exercise

Show that disjoint permutations commute.

Hint: Suppose $\sigma, \tau \in S_n$ are disjoint. Show that $(\sigma\tau)(i) = (\tau\sigma)(i)$ for $i = 1, \ldots, n$.

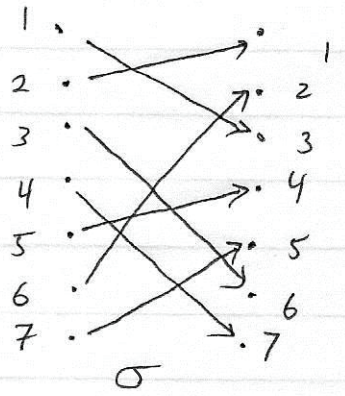
Recall that $(\sigma\tau)(i) = \sigma(\tau(i))$.

Theorem

Every permutation σ can be written as a product of disjoint cycles.

Examples

The cycles correspond to the distinct orbits in $\{1,\dots,n\}$, which we know partition $\{1,\dots,n\}$. Consider the permutation σ defined by



The orbit of $i=1$ is determined by computing first

$$\sigma^0(1)=1,\quad \sigma^1(1)=3,\quad \sigma^2(1)=6,\quad \sigma^3(1)=2,\quad \sigma^4(1)=1$$

So one of the disjoint cycles is $(1\ 3\ 6\ 2)$.

Now pick a number not in this orbit, & compute its orbit:

$$\sigma^0(4)=4,\quad \sigma^1(4)=7,\quad \sigma^2(4)=5,\quad \sigma^3(4)=4$$

So another disjoint cycle is $(4\ 7\ 5)$.

As a product of disjoint cycles,

$$\sigma = (1\ 3\ 6\ 2)(4\ 7\ 5) = (4\ 7\ 5)(1\ 3\ 6\ 2).$$

This is the basic idea. A rigorous proof can be given, based on induction on the number of points moved by σ.

Order of a permutation

If σ is a k-cycle, then an earlier exercise shows that $o(\sigma) = k$. What if σ is a product of disjoint cycles?

Example: $\sigma = (1\ 2)(3\ 4\ 5)$

$$\sigma^2 = (3\ 5\ 4)$$
$$\sigma^3 = (1\ 2)$$
$$\sigma^4 = (3\ 4\ 5)$$
$$\sigma^5 = (1\ 2)(3\ 5\ 4)$$
$$\sigma^6 = e$$

Exercise

Suppose $\sigma = \alpha_1 \alpha_2 \cdots \alpha_k$ where $\alpha_1, \ldots, \alpha_k$ are disjoint cycles. Let m_i = length of α_i.

Show that

$$o(\sigma) = \text{lcm}\,(m_1, \ldots, m_k).$$

[lcm = least common multiple]

Decomposition into transpositions

We've seen that every permutation can be written as a product of disjoint cycles. This is a very useful decomposition, but there are others that are also useful in different ways.

We begin by observing that every cycle can be written as a product of (not disjoint) transpositions.

Example/Exercise

Verify that $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$.

Exercise

Show that $(i_1\ i_2 \cdots i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)$.

By repeating this for each disjoint cycle, we obtain the next theorem.

Theorem

If $\sigma \in S_n$, then $\exists$ transpositions $\alpha_1, \ldots, \alpha_k$ s.t. $\sigma = \alpha_1 \alpha_2 \cdots \alpha_k$.

Note, however, that a decomposition into products of transpositions is <u>not</u> unique.

A trivial example:

$$(1\ 2) = (1\ 2)(3\ 4)(3\ 4) = (3\ 4)(1\ 2)(3\ 4)$$

If α is a transposition, then $\alpha^2 = e$, so we can always insert as many $\alpha\alpha$ terms as we like: $\sigma = \sigma\alpha\alpha = \alpha\alpha\sigma\alpha\alpha$, etc. Still, this suggests that we have to insert or delete transpositions two at a time, and this suggestion is correct. - we will prove this in the next section.