Groups of Permutations on a Finite Set

Cycles

Philippe B. Laval

KSU

Current Semester
In these slides, we focus on permutations $\alpha : A \to A$ where $A$ is finite.

In the process, we will develop a new notation for permutations.

We will also learn about cycles and even and odd permutations.

Let us recall the various objects we are dealing with.

- The finite set $A$ which we denote $\{1, 2, 3..., n\}$. $A$ is a set of mathematical objects.
- The symmetric group of $A$ denoted $S_n$. It is the set of all permutations of $A$.
- Permutations which are bijections from $A$ into $A$. We often denote them with a lower case Greek letter such as $\alpha$.
- Recall that $\alpha \in S_n$ but $\alpha : A \to A$ that is $\alpha$ acts on elements of $A$. 
Cycle Notation

There is a more compact way to write permutations. This notation is due to Augustin Cauchy (1789 - 1857). We now present this new notation.

**Definition**

Let $x_1, x_2, \ldots, x_r$ with $1 \leq r \leq n$ be $r$ distinct elements of $\{1, 2, 3, \ldots, n\}$. The r-cycle $(x_1, x_2, \ldots, x_{r-1}, x_r)$ is the element of $S_n$ that maps

\[ x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow \ldots \rightarrow x_r \rightarrow x_1 \]

In particular, the 1-cycle $(x_i)$ maps $x_i \rightarrow x_i$. 1-cycles are usually omitted.

**Definition**

In an r-cycle $(x_1, x_2, \ldots, x_r)$, $r$ is called the length of the cycle.

Note: Unless it is necessary to know how many elements are in a cycle, we will call an r-cycle a cycle.
Note: certain texts (such as ours) do not use commas to separate the elements of a cycle. In these slides, we will use commas. So, while our book would write \((153)\), I will write \((1, 5, 3)\).

Example

Find \(\alpha(1)\), \(\alpha(2)\) and \(\alpha(4)\) if \(\alpha = (1, 4, 3, 2)\).

The operation on cycles is also composition. They are composed from right to left.

Example

What will 3 be mapped to by \((1, 2)(3)(4, 5)(1, 5, 3)(2, 4)\)?
Cycle Notation

For the examples on the previous slide, we should have found:

Example

Find $\alpha(1)$, $\alpha(2)$ and $\alpha(4)$ if $\alpha = (1, 4, 3, 2)$.

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

The operation on cycles is also composition. They are composed from right to left.

Example

What will 3 be mapped to by $(1, 2)(3)(4, 5)(1, 5, 3)(2, 4)$?

We proceed from right to left. $(2, 4)$ has no action on 3. $(1, 5, 3)$ maps 3 to 1. So, now we have 1. $(4, 5)$ has no action on 1. $(3)$ has no action on 1. $(1, 2)$ maps 1 to 2. So, the result is $3 \rightarrow 2$. 
Disjoint Cycles

Definition
When two cycles have no elements in common, they are said to be **disjoint**.

We now illustrate how permutations can be represented by cycles with examples.

Example
The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ can be represented $(1) (2, 4) (3)$ or $(2, 4)$ if we omit the 1-cycles with the understanding that the elements missing are mapped to themselves.

Note: The cycle notation is not unique. For example $(2, 4)$ is the same as $(4, 2)$. 
Example
Write the permutation \( (1, 3)(2, 7)(4, 5, 6)(8) \) in array form in \( S_{10} \).
Disjoint Cycles: Examples

In the examples above, we should have found:

**Example**

The permutation \( (1 \ 2 \ 3 \ 4 \ 5 \ 6) \) can be represented by \( (1, 2) \ (3, 4, 6) \ (5) \) or \( (1, 2) \ (3, 4, 6) \) if we omit the 1-cycle.

You will note that \( (1, 2) \ (3, 4, 6) \) is the same as \( (3, 4, 6) \ (1, 2) \). This is a specific case of a more general result we will see and prove below, which states that disjoint cycles commute.

**Example**

Write the permutation \( (1, 3) \ (2, 7) \ (4, 5, 6) \ (8) \) in array form.

\[
(1, 3) \ (2, 7) \ (4, 5, 6) \ (8) = 
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
3 & 7 & 1 & 5 & 6 & 4 & 2 & 8 \\
\end{pmatrix}
\]
Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$. Write $\alpha$ and $\beta$ in cycle notation. Then, write $\alpha \beta$ in cycle notation. Finally, write $\alpha \beta$ so that the cycles which appear are disjoint.

Do it on your own, then check your answer on the next slide.
Example

Let \( \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \) and \( \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \). Write \( \alpha \) and \( \beta \) in cycle notation. Then, write \( \alpha \beta \) in cycle notation. Finally, write \( \alpha \beta \) so that the cycles which appear are disjoint.

\[
\alpha = (1, 2) (3) (4, 5) \\
= (1, 2) (4, 5)
\]

\[
\beta = (1, 5, 3) (2, 4)
\]

Thus

\[
\alpha \beta = (1, 2) (3) (4, 5) (1, 5, 3) (2, 4)
\]

We can see that \( \alpha \beta \) is written as a product of cycles which are not disjoint. We see that \( \alpha \beta (1) = 4, \alpha \beta (2) = 5, \alpha \beta (3) = 2, \alpha \beta (4) = 1 \) and \( \alpha \beta (5) = 3 \). Hence, \( \alpha \beta = (1, 4) (2, 5, 3) \).
Disjoint Cycles: Examples

Example
As noticed above, 1-cycles are usually omitted in a product of cycles with the understanding that they map the omitted element to itself. However, if the permutation is the identity as in \( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \) then we have to write something. We can represented by \((1)\) or \((2)\) or \((i)\) for \(i = 1, 2, \ldots, 5\).

Example
What is the inverse of \((1, 2, 3)\)?
From the previous example, we should have found:

**Example**

What is the inverse of $(1, 2, 3)$?

Since the composition of a cycle and its inverse must give the identity, if a cycle maps $i$ into $j$, then its inverse must map $j$ back to $i$. So, $(1, 2, 3)^{-1} = (3, 2, 1)$. We can verify that $(1, 2, 3)(3, 2, 1) = e$.

In general, the inverse of the $r$-cycle $(x_1, x_2, \ldots, x_{r-1}, x_r)$ is $(x_r, x_{r-1}, \ldots, x_2, x_1)$ in other words

$$(x_1, x_2, \ldots, x_{r-1}, x_r)^{-1} = (x_r, x_{r-1}, \ldots, x_2, x_1)$$
Examples of Permutations

Example

Our last example will be the elements of $S_3$ we derived in the previous set of slides. Rewrite them in cycle notation.

Recall we found that $S_3 = \{\varepsilon, \alpha, \beta, \gamma, \delta, \kappa\}$ where:

- $\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
- $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
- $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
- $\delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
- $\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
Examples of Permutations

Example

Our last example will be the elements of $S_3$ we derived in the previous set of slides. Rewrite them in cycle notation.

It is easy to see that:

- $\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = (2) = (3)$
- $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3)$
- $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$
- $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)$
- $\delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2)$
- $\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)$

Note that with the exception of the identity, we did not write the 1-cycles.
Theorem
Every permutation of a finite set is either the identity, a 1-cycle, or can be written as a product of disjoint cycles.

Before doing a general proof, try to write
\[ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 2 & 8 & 1 & 6 \end{pmatrix} \]
as a product of disjoint cycles.

Being able to write a permutation as a product of disjoint cycles has several advantages:

- When finding the image of an element, we just need to find the cycle which contains it. If the cycles are disjoint, that element will only appear once.
- Disjoint cycles commute. We prove this next.
Properties of Permutations

Sketch of a proof.

Let \( \alpha \) be a permutation on \( A = \{1, 2, \ldots, n\} \) which is not the identity. Let \( a_1 \) be the first element of \( A \) such that \( \alpha(a_1) \neq a_1 \). Explain why such an element exists.

Compute \( a_2 = \alpha(a_1), a_3 = \alpha(a_2) = \alpha^2(a_1) \) and so on. Explain why the sequence \( a_1, a_2, a_3, \ldots \) must be finite.

Hence, there exist \( i < j \) for which we have
\[
a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \ldots \rightarrow a_i \rightarrow \ldots \rightarrow a_j \text{ with } \alpha(a_j) = a_i.
\]
Explain why \( \alpha(a_j) = a_1 \).

So, we have our first cycle: \( (a_1, a_2, \ldots, a_j) \). If we did not use all the elements of \( A \), then we pick \( b_1 \) among the elements of \( A \) which do not appear in \( (a_1, a_2, \ldots, a_m) \) and repeat the same process to get a cycle \( (b_1, b_2, \ldots, b_k) \). Explain why \( (b_1, b_2, \ldots, b_k) \) and \( (a_1, a_2, \ldots, a_j) \) are disjoint and finish the proof.
Theorem

Disjoint cycles commute in other words, if $\alpha = (a_1, a_2, ..., a_m)$ and $\beta = (b_1, b_2, ..., b_n)$ have no element in common, then $\alpha\beta = \beta\alpha$. 
Properties of Permutations

Sketch of a proof.

- We show $\alpha \beta = \beta \alpha$ by showing that $\alpha \beta (x) = \beta \alpha (x)$ for every $x$ in $A$, the set on which our permutations are defined. We can write $A$ as $A = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\}$ where the $c'$s are the elements of $A$ left untouched by $\alpha$ and $\beta$.
- Compute $\alpha \beta (a_i)$ and $\beta \alpha (a_i)$.
- Compute $\alpha \beta (b_i)$ and $\beta \alpha (b_i)$.
- Compute $\alpha \beta (c_i)$ and $\beta \alpha (c_i)$.
- Conclude.
Definition
A 2-cycle is called a transposition.

Example
(1, 2), (1, 5), (2, 4) are examples of transpositions.

Example
What is the inverse of a transposition?
Transpositions

For the last example, we should have found:
A transposition on $S_n$ is of the form $(a_i, a_j)$.
It is easy to see that $(a_i, a_j)(a_i, a_j) = e$, so every transposition is its own inverse. This is important to remember, we’ll state it as a theorem.

**Theorem**

_Every transposition is its own inverse that is $(a_i, a_j)^{-1} = (a_i, a_j)$._

Another important result about transpositions is:

**Theorem**

_Any cycle in $S_n$ with $n > 1$ can be written as the product of transpositions._

**Example**

_Write $(1, 3, 7)$ as a product of transpositions. Same question for $(1, 2, 3, 4, 5)$. _
Transpositions

Sketch of a proof.

- Write a 1-cycle as a product of transpositions.
- Do the same for a 2-cycle, a 3-cycle.
- Once you understand the construct for 2-cycles and 3-cycles, generalize the technique for r-cycles.
- Can you think of several ways to do this.
Transpositions

In the example above, we should have found

\[(1, 3, 7) = (1, 7) (1, 3) = (7, 3) (7, 1) = (1, 3) (3, 7)\]

and

\[(1, 2, 3, 4, 5) = (1, 5) (1, 4) (1, 3) (1, 2) = (5, 4) (5, 3) (5, 2) (5, 1) = (1, 2) (2, 3) (3, 4) (4, 5)\]

Combining the previous theorems, we have:

**Theorem**

*Every permutation in $S_n$ with $n > 1$ can be written as a product of transpositions.*
Example

Write the permutations below as a product of transpositions:

1. \((1, 6, 3, 2)(4, 5, 7)\)
2. \(
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
3 & 5 & 7 & 4 & 2 & 8 & 1 & 6
\end{pmatrix}
\)
Examples of Permutations

In the example above, we should have found:

\[(1, 6, 3, 2) (4, 5, 7) = (1, 2) (1, 3) (1, 6) (4, 7) (4, 5)\]

and

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
3 & 5 & 7 & 4 & 2 & 8 & 1 & 6
\end{pmatrix}
= (1, 3, 7) (2, 5) (4) (6, 8)
= (1, 7) (1, 3) (2, 5) (4, 5) (5, 4) (6, 8)
\]

What if we had omitted the 1-cycle?

Every permutation can be written as a product of transpositions. As we know, this product is not unique. Whether the number of transpositions in this product is odd or even is important. We investigate this next.
Even and Odd Permutations

Definition
A permutation is said to be **even** if it can be written as an even number of transpositions. It is said to be odd if it can be written as an **odd** number of transpositions.

**Note:** Do you see any problem with this definition?

Example
Is \((1, 3, 7)\) even or odd?

Example
Is \(\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 7 & 5 \end{pmatrix}\) even or odd?
Even and Odd Permutations

In the examples above, we should have found that:

- \((1, 3, 7) = (1, 7)(1, 3)\) hence it is even.
- \[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 4 & 6 & 1 & 3 & 7 & 5
\end{pmatrix}
\]
  \(= (1, 2, 4)(3, 6, 7, 5) = (1, 4)(1, 2)(3, 5)(3, 7)(3, 6)\) hence it is odd.

Of course, in view of the fact that there are many ways to write a permutation, the reader may wonder if a permutation can be both even and odd. That would not be good. It turns out it cannot happen. Before we prove it, we state a lemma without proof.
Lemma

The identity permutation on $S_n$ is even.

and now the theorem.

Theorem

No permutation is both even and odd.

Sketch of a proof:

- Let $\alpha$ be a permutation and suppose that $\alpha$ is both even and odd that is $\alpha = \beta_1 \beta_2 \ldots \beta_l = \gamma_1 \gamma_2 \ldots \gamma_k$ where the $\beta'$s and $\gamma'$s are transpositions, $k$ is even and $l$ odd.
- Using the fact that every transposition is its own inverse, write the identity $\varepsilon$ in terms of the $\beta'$s and $\gamma'$s.
- Explain why it would contradict the lemma.
**Definition**

The set of even permutations is an important set. It is denoted $A_n$.

**Theorem**

$A_n$ is a subgroup of $S_n$. It is called the alternating group of degree $n$.

**Proof.**

*See homework.*

**Theorem**

For $n \geq 2$, $A_n$ has order $\frac{n!}{2}$ that is $|A_n| = \frac{n!}{2}$. 
Exercises

1. Prove that $A_n$ is a subgroup of $S_n$. What about the set of odd permutations, is it also a subgroup of $S_n$?

2. Prove that $A_n$ has order $\frac{n!}{2}$ by proving that the number of even permutations is the same as the number of odd permutations. Since $|S_n| = n!$, the result will follow. To do this, follow the sketch below:

   1. Explain why for each odd permutation $\alpha$ in $S_n$, $(1,2)\alpha$ is even.
   2. Explain why if $\alpha \neq \beta$ then $(1,2)\alpha \neq (1,2)\beta$.
   3. Let $m_e$ be the number of even permutations and $m_o$ be the number of odd permutations, using parts a and b, explain why we can say that $m_e \geq m_o$.
   4. Using a similar argument, prove that $m_e \leq m_o$.
   5. Conclude.

3. Do the following problems from your book: A1a, A1c, A1e, A2a, A3a, A3d, A4a, A4b, A5, A6a, B1a, B1b, B2, B3, B4, C1a, C1b, C2, C3, D1, D2, E1, E2, F1, F2, F3.