Discrete Mathematics, Section 001, Fall 2016

Lecture 17: Symmetry and Permutation

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

November 9, 2016

Outline

1 Permutations

2 Transpositions

3 Groups

Definitions

Permutation

Let A be a set. A **permutation** on A is a bijection from A to itself

For example,

$$f = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$$

is a permutation. In the earlier notation,

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

The set of all permutations on the set $\{1, 2, \ldots, n\}$ is denoted by S_n.

Traditional notation for permutations: $\pi, \sigma, \tau \in S_n$.

The symmetric group

The pair $(S_n, \circ)$ is called the **symmetric group on n elements.**

- The identity
$$\iota := \mathrm{id}_{\{1,2,\ldots,n\}}$$
is a permutation and therefore it's in S_n.
- $\forall \pi, \sigma \in S_n$, $\pi \circ \sigma \in S_n$.
- $\forall \pi, \sigma, \tau \in S_n$, $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$
- $\forall \pi \in S_n$, $\pi \circ \iota = \iota \circ \pi = \pi$.
- $\forall \pi \in S_n$, $\pi^{-1} \in S_n$ and $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$.

Therefore $\circ$ is an associative operation on S_n with identity ι and inverse elements being the inverses in the function sense.

Note also: $|S_n| = n!$

Cycle notation

We have seen two representations for a permutation so far, for example in S_5,

$$\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$$

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

Note that the top row is not necessary and we could just write $[2,4,1,3,5]$. However, for large n, this gets hard to decipher.

Alternatively, we can keep records of 'trajectories' or **cycles**:

$$1 \quad\to\quad 2 \quad\to\quad 4 \quad\to\quad 3 \quad\to\quad 1, \qquad\qquad 5 \quad\to\quad 5$$

and encode the information as

$$(1,2,4,3)(5)$$

Cycle notation

As another example, consider

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix}.$$

In the cycle notations,

$$\pi = (1, 2, 7)(3, 5)(4, 6, 8)(9)$$

Practice this on Problem 1 on the Worksheet.

Theorem

Every permutation of a finite set can be expressed as a collection of pairwise disjoint cycles.

Let $\pi \in S_n$ and consider the sequence

$$1, \pi(1), \pi^{(2)}(1), \pi^{(3)}(1), \dots$$

where e.g. $\pi^{(2)}(i) = (\pi \circ \pi)(i)$.

- This is a sequence in $\{1, \dots, n\}$ and must repeat itself eventually.
- Let k be the first repeat, i.e

  $$\pi^{(k)}(1) \in \{1, \pi(1), \pi^{(2)}(1), \dots \pi^{(k-1)}(1)\}$$

  and k is the smallest such number. FTSC assume that $\pi^{(k)}(1) \neq 1$, then

  $$\pi^{(k)}(1) = \pi^{(j)}(1) \qquad \text{for some } 1 < j < k.$$

[...]

Theorem

Every permutation of a finite set can be expressed as a collection of pairwise disjoint cycles.

[...]

- FTSC assume that $\pi^{(k)}(1) \neq 1$, then
$$\pi^{(k)}(1) = \pi^{(j)}(1) \qquad \text{for some } 1 < j < k.$$
- Because this is the first repeat, $\pi^{(k-1)}(1) \neq \pi^{(j-1)}(1)$, but then applying π gives
$$\pi^{(k)}(1) \neq \pi^{(j)}(1)$$
as π is one-to-one. $\Rightarrow\Leftarrow$

This proves $\pi^{(k)}(1) = 1$. If the cycle starting at element 1 does not include all the elements of $\{1, 2, \ldots n\}$, then we can restart with an element left out and build a new cycle. That all the resulting cycles are disjoint is Problem 2 on the Worksheet.

Q: Are there multiple cycle representations for the same permutations?

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix}.$$

$$\pi = (1,2,7)(3,5)(4,6,8)(9) = (5,3)(6,8,4)(9)(7,1,2)$$

However,

- $(1,2,7)$ and $(7,1,2)$ are the same cycles!
- The order in which we list the disjoint cycles does not matter!

Theorem

Every permutation of a finite set can be expressed as a collection of pairwise disjoint cycles. **This representation is unique up to rearranging the cycles and the cyclic order of the elements within cycles.**

Do Problem 3 on the Worksheet!

Calculations with permutations

- **Inverting:**

$$\pi = (1,2,7,9,8)(5,6,3)(4) \in S_9$$

Tracing it backwards:

$$\pi^{-1} = (8,9,7,2,1)(3,6,5)(4) \in S_9$$

- **Compositions:** If $\pi, \sigma \in S_9$ are

$$\pi = (1,3,5)(4,6)(2,7,8,9), \qquad \sigma = (1,4,7,9)(2,3)(5)(6,8)$$

Then we can read off e.g. $\pi(1) = 3$ and $\sigma(3) = 2$ and therefore $\sigma \circ \pi(1) = 2$. Proceding similarly,

$$\sigma \circ \pi = (1,2,9,3,5,4,8,1)(7,6)$$

Practice this in Problem 4 on WS.

Application to symmetries

Symmetry name	1	2	3	4	Cycle form
	go to positions				
I	1	2	3	4	$(1)(2)(3)(4)$
R_{90}	2	3	4	1	$(1,2,3,4)$
R_{180}	3	4	1	2	$(1,3)(2,4)$
R_{270}	4	1	2	3	$(1,4,3,2)$
F_H	2	1	4	3	$(1,2)(3,4)$
F_V	4	3	2	1	$(1,4)(2,3)$
$F_/$	3	2	1	4	$(1,3)(2)(4)$
$F_\backslash$	1	4	3	2	$(1)(2,4)(3)$

Note that in this language, we can compute

$$R_{90} \circ F_H \;{}'=' \; (1,2,3,4) \circ (1,2)(3,4) = (13)(2)(4) \;{}'=' \; F_/$$

Also note that not all elements of S_4 are used. We call the set of symmetries of the square with the composition operation as the dihedral group of index 4 and denote it by $(D_4, \circ)$.

Outline

1 Permutations

2 Transpositions

3 Groups

The simplest permutations

The simplest possible permutation is the one that doesn't do anything:

$$\iota = (1)(2)\dots(n) \in S_n$$

The next symplest are called **transpositions**, which is the exchange of exactly two elements. For example,

$$\tau = (1)(2)(3,6)(4)(5)(7)(8)(9) \in S_9$$

Transposition

A permutation $\tau \in S_n$ is called a **transposition** provided

- $\exists i, j \in \{1, 2, \dots, n\}$ with $i \neq j$ so that $\tau(i) = j$ and $\tau(j) = i$,
- $\forall k \in \{1, 2, \dots, n\}$ with $k \neq i$ and $k \neq j$, we have $\tau(k) = k$.

Since the vast majority of cycles in a transposition are singletons, we are not going to write them and just say

$$\tau = (3,6)$$

Writing permutations as compositions of transpositions

1. **Cycles:**

$$(1, 2, 3, 4, 5) = (1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2).$$

In general,

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n) \circ (a_1, a_{n-1}) \circ (a_1, a_2)$$

2. **Any permutation:**

$$(1, 2,3, 4, 5)(6, 7, 8)(9)(10, 11) =$$
$$= [(1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2)] \circ [(6, 8) \circ (6, 7)] \circ (10, 11)$$

In general, put together the decomposition of the cycles.

Do Problem 4 on the WS!

Theorem

Let π be any permutation on a finite set. Then π can be expressed as the composition of transpositions defined on that set.

However, there might be other ways to do this than what our algorithm provides:

$$\begin{aligned}(1,2,3,4) &= (1,4)\circ(1,3)\circ(1,2) = \\ &= (1,2)\circ(2,3)\circ(3,4) = \\ &= (1,2)\circ(1,4)\circ(2,3)\circ(1,4)\circ(3,4)\end{aligned}$$

But note that all three versions have an odd number of transpositions!

Theorem

Let $\pi \in S_n$. Let π be decomposed into transpositions as

$$\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a, \qquad \pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_b$$

Then a and b are either both odd or both even.

Even and odd permutations

Theorem

Let $\pi \in S_n$. Let π be decomposed into transpositions as

$$\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a, \qquad \pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_b$$

Then a and b are either both odd or both even.

We are going to use the following auxiliary result:

Lemma

If the identity permutation is written as a composition of transpositions, then that composition must use an even number of transpositions. That is, if

$$\iota = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a,$$

where the τ-s are transpositions, then a must be even.

Theorem

Let $\pi \in S_n$. Let π be decomposed into transpositions as

$$\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a, \qquad \pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_b$$

Then a and b are either both odd or both even.

Proof.

Note that we can write (HW) π^{-1} as

$$\pi^{-1} = \sigma_b \circ \sigma_{b-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$$

and thus

$$\iota = \pi \circ \pi^{-1} = \tau_1 \circ \cdots \circ \tau_a \circ \sigma_b \circ \cdots \circ \sigma_1 .$$

By the lemma, $a + b$ is even and so a and b are either both odd or both even. $\square$

Definition

Let π be a permutation on a finite set. We call π **even** provided it can be written as the composition of an even number of transpositions. Otherwise, we call it an **odd** permutation.

For example,

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

is an odd permutation while

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

is even.

Definition

Let A_n be the set of all even permutations in S_n. Then $(A_n, \circ)$ is called the alternating group.

Outline

1 Permutations

2 Transpositions

3 Groups

Inverses

Definition

Let $*$ be an operation on a set A and suppose that it has an identity element $e \in A$. Let $a \in A$. An element b is an **inverse** of a provided $a * b = b * a = e$.

For example,

- In $(S_n, \circ)$, $(1,2,3)^{-1} = (1,3,2)$.
- In $(\mathbb{Z}, +)$, the identity element is $e = 0$ and for any $a \in \mathbb{Z}$ then $(-a) + a = a + (-a) = 0$ and so the inverse of a is $-a$.

Q: Must inverses be unique?

Inverses

Q: Must inverses be unique?

*	e	a	b	c
e	e	a	b	c
a	a	a	e	e
b	b	e	b	e
c	c	e	e	c

- e is an identity element.
- $a * b = b * a = e$
- $a * c = c * a = e$
- Therefore b and c are both inverses of a.

- $(a * b) * c = e * c = c \neq a = a * e = a * (b * c)$
- So $*$ is not associative.

In most of our examples, the inverses were unique, but those were also associative, e.g.

- $(\mathbb{Z}, +)$
- $(\mathbb{Q} - \{0\}, \cdot)$
- $(S_n, \circ)$, $(A_n, \circ)$, $(D_{2n}, \circ)$.

Groups

Definition

Let $*$ be an operation defined on a set G. We call a pair $(G, *)$ a **group**, provided

1. The set G is closed under $*$; that is, $\forall g, h \in G$, $g * h \in G$.
2. $*$ is associative.
3. There is an identity $e \in G$.
4. For every element g, there is an inverse element $h \in G$.

Q: We have seen that the identity element must be unique. Is this structure enough now for the inverse to be unique?

Uniqueness of inverses in groups

Proposition

Let $(G, *)$ be a group. Every element $g \in G$ has a unique inverse.

Proof.

We already know that every element has an inverse. For the sake of contradiction, assume that $g \in G$ has two (or more) distinct inverses $h, k \in G$. Then

$$h = h * e = h * (g * k) = (h * g) * k = e * k = k,$$

and therefore $h = k$ giving a contradiction. $\Rightarrow\Leftarrow$ □

Therefore we can talk about THE inverse of $g \in G$. Notation:

- The inverse of g is mostly denoted by g^{-1}.
- Sometimes for additive groups, $(-g)$ is more appropriate.

Number groups

- $(\mathbb{Z}, +)$: Integers with addition is a group.
- $(\mathbb{Q}, +)$: Rationals with addition is a group.
- $(\mathbb{Q}, \cdot)$: This is not a group, no 0^{-1}.
- $(\mathbb{Q} - \{0\}, \cdot)$: This is a group.
- $(\mathbb{Q}^{+}, \cdot)$: Positive rationals with multiplication is a group.

The operation in these groups is all commutative. We have a special names for groups like this.

Definition

We call a group $(G, *)$ **Abelian** provided $*$ is a commutative operation on G, i.e.

$$g * h = h * g, \qquad \forall g, h \in G$$

More exotic examples

Permutation groups:

- $(S_n, \circ)$: permutations with composition is the *symmetric group*. It is not Abelian.
- $(A_n, \circ)$: set of all even permutations in S_n is the *alternating group*. (Problem 2 on WS)

Symmetry groups:

- $(D_{2n}, \circ)$: the symmetries of an n-gon is the *dihedral group*.

An odd example:

- If A is a set $(2^A, \Delta)$ is a group (Homework).