Queen Mary University of London

Group Theory

Week 3, Lecture 1, 2 & 3

Dr Lubna Shaheen

Table of Contents

Symmetric groups

Symmetric group: Group of all permutations on n symbols

X-set , Sym(X)= $\{$**the collection of one-to-one and onto function** $f : X \to X\}$

The symmetric group of degree n is the symmetric group on the set $X = \{1, 2, 3, \cdots, n\}$. We ll denote this set by S_n.

Symmetric Groups

Claim

Claim: Sym(X) equipped with $\circ$ is a group.

(i) **Closed**: The operation of function composition is closed in the set of permutations of the given set X.
(ii) Function composition is always **associative**.
(iii) The trivial bijection that assigns each element of X to itself serves as an **identity**.
(iv) Every bijection has an **inverse function (permutation)** that undoes its action, and thus each element of a symmetric group have an inverse

Symmetric Groups

Symmetric group: Group of all permutations on n symbols

Symmetric Groups

Symmetric group: Group of all permutations on n symbols

Disjoint cylce notation:

The group operation in a symmetric group is function composition, denoted by the symbol $\circ$ or simply by just a composition of the permutations.

$$f = (13)(2)(45) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$g = (125)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

We ll apply first g and then f.

$$fg = f \circ g = (124)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

Symmetric group

S_2, symmetric group of degree 2

This group consists of exactly two elements: the identity and the permutation swapping the two points. It is a cyclic group and is thus abelian.

S_3, symmetric group of degree 3, $S_3 \cong D_6$

S_3 is the first non-abelian symmetric group. This group is isomorphic to the dihedral group of order 6, (D_6) the group of reflection and rotation symmetries of an equilateral triangle, since these symmetries permute the three vertices of the triangle. Cycles of length two correspond to reflections, and cycles of length three are rotations.

Symmetric groups

Notations

Symmetric groups

Example

Composition

Symmetric group

Inverses

Cycle Notation

Symmetric groups

Disjoint Cycles

Remark: Disjoint cycles are not unique.

Symmetric group

Symmetric group

Cycle of length m

Symmetric Groups

Symmetric group: Group of all permutations on n symbols

Symmetric groups

Symmetric group

Lemma

Suppose $f \in S_n$ is written in disjoint cycle notation. Then f^{-1} is obtained by reversing all the cycles.

Symmetric group

Lemma

Suppose $f \in S_n$. Then $ord(f)$ is the least common multiple of the lengths of the cycles of f.

Symmetric group

Order of a permutation

Example 1: What is the order of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 7 & 6 & 5 & 3 & 1 & 2 \end{pmatrix}$$

Example 2: What is the order of the permutation $(1357)(28)(496)$?

Alternating group

Definition

We call a permutation an m-cycle if it has one cycle of length m, and its other cycles all have length 1. A 2-cycle is also known as a transposition.

Lemma

Every element of S_n can be written as a product of transpositions.

Symmetric group

Remark: for the sake of order we need to include "the empty product which is identity". This applies that the lemma will valid even for $n = 1$.

Alternating group

Definition

Suppose $f \in S_n$. Then f is **even** if it can be written as a product of an even number of transpositions, and **odd** if it can be written as a product of an odd number of transpositions. The alternating group $\mathcal{A}_n$ is the set of even permutations in S_n.

Examples: For example, (1234) is odd, because $(1234) = (12)(23)(34)$. On the other hand, $(123)(456)$ is even, because $(123)(456) = (12)(23)(45)(56)$.

Lemma

$\mathcal{A}_n \leq S_n, \mathcal{A}_n$ is a subgroup of S_n.

Alternating group

Alternating group

Definition

Suppose $f \in S_n$. An inversion of f is a pair of numbers $a, b \in \{1, 2, \cdots, n\}$ such that $a < b$ but $f.a > f.b$. We write inv(f) for the number of inversions of f.

An inversion in a permutation is a pair (i, j) where $i < j$ but i appears after j in the permutation. In other words, in the one-line notation of a permutation, an inversion occurs if a smaller number appears to the right of a larger number.

Alternating group

Alternating group

Lemma

Suppose $g \in S_n$ and $1 \le c \le d \le n$, and let $h = (cd)g$. Then inv(g) is even if and only if inv(h) is odd.

Alternating group

Example

Let

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Find the inversion of $h = (13)g$

Inversion of g are 3, which are $\{(14), (24), (34)\}$.
Inversion of (1 3)g are 2, which are $\{(12), (34)\}$.

Alternating group

Alternating group

Exercise

Find the inversions of the permutation $(c, d)g$ where

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 5 & 1 & 7 & 6 & 9 & 8 & 1 \end{pmatrix}$$

in $\mathcal{S}_9$.

(i) The effect of (c, d) is to swap the positions of elements c and d in the permutation.
(ii) The final permutation $(c, d)g$ is the result of applying the 5-cycle g first and then applying the transposition (c,d).

Case I: (c, d) involves elements of the cycle g

If c and d are elements of the 5-cycle $g = (13579)$ swapping them will change the relative order of these elements in the cycle, potentially creating or removing inversions between them and other elements of the cycle.

Alternating group

For example $c = 1$ and $d = 5$ so the transposition $(1, 5)$ swaps these two elements.The permutation $g = (13579)$ becomes after applying (15), the new permutation becomes (53179) where 1 and 5 have been swapped. We then compute inversions in this new permutation.

Case II: (c,d) involves elements outside the cycle g. If c and d are not part of the cycle g, then applying (c, d) will simply swap two elements outside the cycle, and the relative order of elements within the cycle will remain the same.
In this case, the number of inversions would only be affected by the transposition involving c and d.

Example Inversion: Inversion of g are 8. Lets $(c, d) = (1, 5)$ and $g = (13579)$.
Then $h = (1, 5)g$ swaps 1 and 5, so the new permutation is (13)(579).
Total inversions of h are 13.
Inversion of $(24)g$ are 9.

Alternating group

Lemma

Suppose $f \in S_n$. If f is even, then $inv(f)$ is even. If f is odd, then $inv(f)$ is odd. So f cannot be both even and odd.

Alternating group

Definition

Suppose $f \in S_n$. Write ev(f) for the number of cylces of f of even length.

Alternating group

Proposition

Suppose $n \geq 2$. Then $|\mathcal{A}_n| = \dfrac{n!}{2}$.

Quotient group

A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves some of the group structure (the rest of the structure is "factored out").

Definition

For a group G and a subgroup $H \leq G$, the quotient group of H in G, written G/H and read "G modulo H", is the set of cosets of H in G. Quotient groups are also called factor groups.
Let $g \in G$, the **right coset of H containing** g is the set

$$Hg = \{hg|\ h \in H\}$$

The **left coset of H containing g** is the set

$$gH = \{gh|\ h \in H\}$$

Quotient group

Properties of Quotinet group

1. The identity element of a quotient group is the subgroup itself.
2. The quotient group G/G has correspondence to the trivial group, that is, a group with one element.
3. The quotient group $G/\{e\}$ has correspondence to the group itself.

Quotient group

Example: Let G be the additive group of integers and N be the subgroup of G containing all the multiples of 3. The quotient group of G is given by $G/N = \{N + a|$ a is in $G\}$. Find the order of G/N.

Solution:

Quotient group

Example: Let $G = \{1, -1, i, -i\}$ be a multiplicative group and $N = \{1, -1\}$ be a subgroup of G. Find the number of elements in the quotient group of G.

Quotient group

Example

Take $G = \mathcal{S}_3$, $H = \langle(12)\rangle = \{\mathrm{id}, (12)\}$ and $g = (23)$. Then

$$Hg = \{(23), (123)\}, \qquad gH = \{(23), (132)\}.$$

Example

1. H is always a right coset of itself, since

$$H1 = \{h1 | h \in H\} = \{h | h \in H\} = H.$$

2. We can have $Hf = Hg$ even when $f \neq g$. For example, let $G = \mathcal{C}_6 = \{1, z, z^2, z^3, z^4, z^5\}$. Then $H = \{1, z^3\}$ is a subgroup. We have $Hz = \{z, z^4\}$, and also $Hz^4 = \{z, z^4\}$. Later on, we'll see exactly when $Hf = Hg$.

Cosets and Conjugacy

Proposition

Suppose G is a group, $H \leq G$ and $f, g \in G$.

1. $|Hg| = |H|$.
2. If $f \in Hg$, then $Hf = Hg$.
3. Each element of G is contained in exactly one right coset of H.

Cosets and Conjugacy

Cosets and Conjugacy

Coset Lemma

Suppose G is a group, $H \leq G$ and $f, g \in G$. Then:

- $Hf = Hg$ if and only if $fg^{-1} \in H$;
- $fH = gH$ if and only if $f^{-1}g \in H$.

Cosets and Conjugacy

Proposition

If G is a group and $H \leq G$, then the number of right cosets of H is equal to the number of cosets of H.

Exams Style Questions

Exam Year, 2023

Question 1:

1. Let G be a group and let $f, g \in G$. Suppose that f and g have finite order and that $fg = gf$. Show that the order of fg is *less than or equal to* the least common multiple of the orders of f and g.
2. Give an example of two permutations $f, g \in S_3$ such that the order of fg is *not equal to* the least common multiple of the orders of f and g.
3. Consider the permutations $f, g \in S_8$ given by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 4 & 3 & 1 & 8 & 7 & 2 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 8 & 1 & 4 & 7 & 5 & 2 & 6 \end{pmatrix}$$

Write f, g and fg in disjoint cycle notation and state the order of each of f, g and fg.

Exams Style Questions

Exam Year, 2023

Question 2:

Let $n \geq 3$ and consider the group S_n.

1. Show that every element of S_n can be written as a product of transpositions.
2. Let $(1k), (1\ell) \in S_n$ be transpositions, where $2 \leq k, \ell \leq n$ and $k \neq \ell$. Write down the permutation $(1k)(1\ell)(1k)$ in disjoint cycle notation.
3. Suppose that H is a subgroup of S_n which contains every transposition of the form $(1k)$, where $2 \leq k \leq n$. Explain why H must be equal to S_n.
4. Suppose that H is a subgroup of S_n which contains the permutation (12) and also contains the permutation $(2345 \cdots n)$. Show that H contains every permutation of the form $(1k)$ where $2 \leq k \leq n$.
5. What is the group $\langle (12), (2345 \cdots n) \rangle$?

Exams Style Questions

Question 3: Find the following subgroups of $\mathcal{D}_{12}$ generated by the given elements.

1. $\langle rs, r^4 s \rangle$
2. $\langle r^4 \rangle$
3. $\langle r^5 \rangle$
4. $\langle r^2 s \rangle$

Exams Style Questions

Question 4: Let $H = \langle r^3, r^2 s\rangle \leq \mathcal{D}_{12}$. Give a list of the left cosets of H in $\mathcal{D}_{12}$, and also give a list of all the right cosets of H in G. Are they same.

Exams Style Questions

Question 5: Let $H = \langle r^3, r^2 s \rangle \leq G$. Give a list of the left cosets of H in G, and also give a list of all the right cosets of H in G. Are they same.

Exams Style Questions

Exams Style Questions

QMplus Quiz 3

Attempt Quiz 3 at QMplus page

Some Useful Notations

Throughout this course, we use the following notation.

- $\mathcal{C}_n$ denotes the cyclic group of order n.
- Klein group often symbolized by the letter $\mathcal{V}_4$ or as $K_4 = \mathbb{Z}_4 \times \mathbb{Z}_4$ denotes the group $\{1, a, b, c\}$, with group operation given by

$$a^2 = b^2 = c^2 = 1, \qquad ab = ba = c,\ ac = ca = b,\ bc = cb = a.$$

- $\mathcal{U}_n$ is the set of integers between 0 and n which are prime to n, with the group operation being multiplication modulo n.

Some Useful Notations

- $\mathcal{D}_{2n}$ is the group with $2n$ elements

  $$1,\ r,\ r^2,\ \ldots,\ r^{n-1},\ s,\ rs,\ r^2s,\ \ldots,\ r^{n-1}s.$$

  The group operation is determined by the relations $r^n = s^2 = 1$ and $sr = r^{n-1}s$.
- $\mathcal{S}_n$ denotes the group of all permutations of $\{1, \ldots, n\}$, with the group operation being composition.
- $GL_n(\mathbb{R})$ is the group of $n \times n$ invertible matrices with entries in $\mathbb{R}$, with the group operation being matrix multiplication.
- $\mathcal{Q}_8$ is the group $\{1, -1, i, -i, j, -j, k, -k\}$, in which

  $$i^2 = j^2 = k^2 = -1, \qquad ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$