Queen Mary
University of London

KDLYVO – CAMPUS-M

Group Theory

Week 3, Lecture 1, 2 & 3

Dr Lubna Shaheen

Assessment 1:

Week 8 : Deadline on Friday 5:00pm
15th Nov

Week 1 – Week 5 content included.

Table of Contents

Symmetric groups

$X = \{1, 2, \cdots n\}$

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.

$f, g : X \to X$

Suppose $\varphi, \psi \in \mathrm{Sym}_X$, $\mathrm{Sym}(X)$ ✓

$\varphi \circ \psi$: composition of function

$\xi = \varphi \circ \psi : X \to X$ — Invertible - one-one & onto

G_1: ✓ $\varphi \circ \psi(x) = \varphi \circ \psi(y)$ because φ is one-one

$\varphi(\psi(x)) = \varphi(\psi(y)) \Rightarrow \psi(x) = \psi(y)$

Symmetric Groups

$\Rightarrow$ $x=y$ ψ is one-one.

Onto: $\varphi(\underline{\psi(x)})$ is surjective.

Claim

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

(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

Onto: $x \in X$, we need to check there is $z \in X$ s.t. that $(\varphi \circ \psi)(z) = x$. Since φ is surjective, $\exists\, y \in X$ $\varphi(y) = x$. Since ψ is surjective, $\exists\, z \in X$ $\psi(z) = y$

Symmetric Groups

Symmetric group: Group of all permutations on n symbols

$$(\varphi \circ \psi)(y) = \varphi(\psi(y)) = \varphi(y) = x$$

G_1: closure property.

G_2: $\varphi \circ (\psi \circ \xi) = (\varphi \circ \psi) \circ \xi$

G_3: $Id \in Sym(X)$ $\quad S_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$

G_4: $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \cdots \right\}$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3) \longrightarrow \text{Transposition}$$

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.

$$f = (13)(2)(45) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \checkmark \quad S_5$$

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

We ll apply first g and then f.

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

Disjoint cycles

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

$\sigma_X,\quad \sigma(X),\quad \sigma \in S_n \quad \mathrm{Sym}(X)$

$X = \{1, 2, \dots n\}$

$\sigma_X \in \mathrm{Sym}(X)$

$$\sigma = \left(\begin{matrix} 1 \to 4 & 2 \to 8 \\ 3 \to 7 & 4 \to 6 \\ 5 \to 5 & 6 \to 3 \\ 7 \to 1 & 8 \to 2 \end{matrix} \right\} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 7 & 6 & 5 & 3 & 1 & 2 \end{pmatrix}$$

$\sigma \in S_8$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$$

$\tau(2) = 1$

Symmetric groups

Example

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

Composition

$$f \circ g = f(\underline{g(x)})$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}}_{\text{2nd}} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}_{\text{1st}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Symmetric group

Inverses

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

Cycle Notation

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

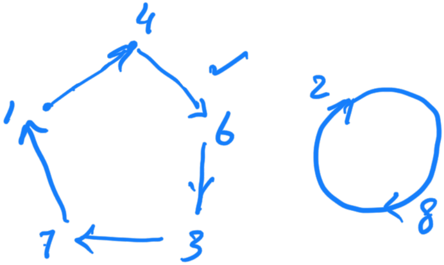
$$= (1\,4\,6\,3\,7)(5)(2\,8)$$

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

Symmetric groups

Disjoint Cycles

Remark: Disjoint cycles are not unique.



$$\sigma = (1\,4\,6\,3\,7)(2\,8)$$

$$= (7\,1\,4\,6\,3)(8\,2) = (14)(46)(63)(37)(28)$$

5 odd

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

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

As long we are following cycle, any representation is fine.

Symmetric group

Example:

$$(42)\circ(123)\circ(14)$$

$$\begin{array}{ccccccc}
2 & \leftarrow & 4 & \leftarrow & 4 & \leftarrow & 1 \\
3 & \leftarrow & 3 & \leftarrow & 2 & \leftarrow & 2 \\
1 & \leftarrow & 1 & \leftarrow & 3 & \leftarrow & 3 \\
4 & \leftarrow & 2 & \leftarrow & 1 & \leftarrow & 4
\end{array}$$

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

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

$$= (12)(23) \quad \text{Even.}$$

$$(14)\circ(123)\circ(42) =$$

$$\begin{array}{ccccccc}
2 & \leftarrow & 2 & \leftarrow & 1 & \leftarrow & 1 \\
1 & \leftarrow & 4 & \leftarrow & 4 & \leftarrow & 2 \\
4 & \leftarrow & 1 & \leftarrow & 3 & \leftarrow & 3 \\
3 & \leftarrow & 3 & \leftarrow & 2 & \leftarrow & 4
\end{array}$$

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

$$= (12)(34) \quad \text{Even}$$

No of Trans

Symmetric group

Cycle of length m

Any permutation which can be written as m-cycles & rest all the 1-cycle Notation is called m-permutation.

$$(14625) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 3 & 6 & 1 & 2 & 7 \end{pmatrix}$$

$$= (12)(34)$$

We can write these as

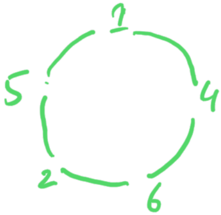
$$= (21)(43)$$

as well.

As disjoint cycles are not unique.

Symmetric Groups

Symmetric group: Group of all permutations on n symbols



$$= (1\,4\,6\,2\,5)$$
$$= (4\,6\,2\,5\,1)$$
$$= (6\,2\,5\,1\,4)$$
$$\neq (1\,5\,2\,6\,4)$$

Remember

Symmetric groups

In $S_3 = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \right\}$

Now

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

$= (13) = (31)$ Transpositions are self inverses.

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

$= (132) = (321) = (213)$

Symmetric group

Lemma

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

Proof. $(a_1, a_2 \cdots a_r)$ is a cycle of f.

$f \cdot a_1 = a_2$ $\quad$ $f^{-1}(a_2) = a_1$

$f \cdot a_2 = a_3$ $\quad$ $f^{-1}(a_3) = a_2$

Here. $\vdots$

$f \cdot a_r = a_1$ $\quad$ $f^{-1}(a_1) = a_r$

$(a_1, a_2 \cdots a_r)$ cycle for f.

$(a_r, a_{r-1}, \cdots a_1)$ cycle for f^{-1}

$f^{-1}(a_r) = a_{r-1}$ ✓

$f^{-1}(a_{r-1}) = a_{r-2}$

$f^{-1}(a_2) = a_1$, $f^{-1}(a_1) = a_r$

Symmetric group

Lemma

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

Proof: Suppose $(a_1 a_2 \ldots a_r)$ is a cycle of f.

$f \cdot a_1 = a_2$

$f(f(a_1)) = f^2(a_1) = a_3$

$f^3(a_1) = a_4$

$\vdots$

$f^m(a_1) = a_{m+1} = a_1 \equiv 1 \bmod (r)$

we need to ensure that m is divisible by all cycles length

$m+1 \equiv 1 \bmod (r)$

Symmetric group
Order of a permutation

$\operatorname{ord}(f) = \min\{m \mid f^m(x) = x,\ x \in \operatorname{Sym}(n)\}$

$= \min\{m \mid \text{every cycle divides } m\}$

$= \operatorname{l.cm}\{\text{cycle of length } m\}$

Example 1: What is the order of the permutation

$$\underbrace{(14637)}_{5}\underbrace{(28)}_{2} = f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 7 & 6 & 5 & 3 & 1 & 2 \end{pmatrix}$$

10

$f^{10} = I$

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

4 2 3

$g = (1357)(28)(496$

$\operatorname{ord}(g) = 12.$

Alternating group

$(a_1 a_2 \dots a_m)(\ \ )(\ \ )$

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.

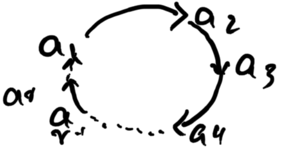
$$(23) = \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

Lemma

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

Proof: Each permutation is a product of cycles.
Any cycle $(a_1, a_2 \dots a_r)$ can be written as a product of transposition

$$(a_1 a_2 \dots a_r) = (a_1 a_2)(a_2 a_3) \dots (a_{r-1} a_r)$$



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 $n = 1$.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 1 & 2 \end{pmatrix} = (1\,4\,6\,2\,5)$$

$$= (1\,4)(4\,6)(6\,2)(2\,5)$$

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

Even

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

Alternating group

A_n – 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.

Proof: i) $\phi \neq A_n$, ii) $f, g \in A_n$, $fg^{-1} \in A_n$

i) $\phi \neq A_n$ Since identity $Id = id \in A_n$

Alternating group

being the even permutation.

ii) Let $f, g \in A_n$

$f = f_1 f_2 \cdots f_k$

$= (\;)(\;)\cdots(\;)$

$g = g_1 \cdots g_l$

No of k – even transposition

(Transpositions are self inverse)

l - no of even transposition

$f \cdot g^{-1} = f_1 \cdots f_k \cdot (g_1 \cdots g_l)^{-1}$

$= f_1 \cdots f_k (g_l^{-1} \cdot g_{l-1}^{-1} \cdots g_1^{-1})$

$= f_1 \cdots f_k \cdot g_l \cdot g_{l-1} \cdots g_1$ Product of $k+l$ Trans

$= f_1 \cdots f_k \cdot g_1 \cdots g_l$ ($k+l$ transposition)

$(fg)^{-1} = g^{-1} f^{-1}$

$(ab) = (ba)$

$= (ab)$

Alternating group

$f \cdot g^{-1} \in A_n$: even no of Transpositions.

Definition $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ . & . & . & . & . & . \end{pmatrix}$ X

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.

Example: $f = (2\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$ $X = \{1, 2, 3, 4, 5\}$

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

No of inversions

Alternating group

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

$$\mathrm{Inv}(g) = \{(16), (17), (18), (23), (24), (25), (26), (27), (28), (34), (35), (36), (37), (38), (45), (46), (47), (48), (56), (57), (58), (67), (68)\} = 23$$

Aim: If f is even; Inversion of f is even

Alternating group

Then inv((c,d)g) & inv(g) have different parity

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.

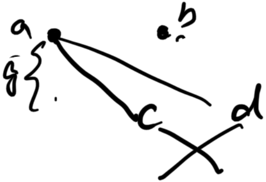
even g odd $\{a,b\} \in X$

Proof: If g(a) is not either c or d, then

$(cd)g(a) = g(a)$,

If both g(a), g(b) are not in $\{c,d\}$, then (a,b)

is an inversion for $(c,d)g \iff$ it is an inversion for g.



(a,b) change status in the following situation

• $g(a) = c$ g(b) lies between c & d

Alternating group

- $g(a) = d$ $g(b)$ lies between c & d
- $g(b) = c$, $g(a)$ " " c & d
- $g(b) = d$, $g(a)$ " " c & d
- $g(a), g(b) = c$ or d

Example

Let

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

$h = (13)g$

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

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

$2(d-c)+1$

pairs that change status

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 $\{(12), (34)\}$.

$inv((c\ d)g) \neq in(g) \mod (2)$

$(c, d) = (1, 3)$

$In(h) = \{(12), (34)\} = 2$

Alternating group

Goal: If f is even, Inversion of f is even.

odd

Even

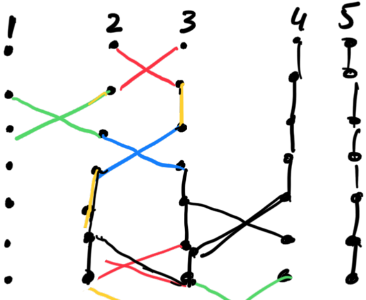
Statement: $g \in S_n$: $\mathrm{Inv}(g)$ have different parity from $\mathrm{Inv}((c,d)\,g)$

odd

Even.

Example:

$(23)\circ(34)\circ(23)\circ(34)\circ(23)\circ(12)\circ(23)$



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

$$\mathrm{Inv}(g) = \{(13), (23), (24)\} = 3$$

Alternating group

Exercise

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

Transposition.

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

$= (1\,3\,5\,7\,9)$ 5-cycle

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

$$(1,5)(13579) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}$$

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 where 1 and 5 have been swapped. We then compute inversions in this new permutation.

$$= (13)(579)$$

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 ? 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 ?
Inversion of $(24)g$ are ?

$$l = (24)g$$

Alternating group

$inv(f) =$

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.

Sol $f \in S_n$ $\quad$ f is even $\Longleftrightarrow$ $inv(f)$ is even

We start with identity, no inversion.
We multiply with one Transposition.
The No of inversion changes from
even $\to$ odd } if we have even number of
or odd $\to$ Even } Transposition, we end up
with even inversion. Similarly, if we had odd no of Transposit-

Alternating group

we end up with odd .
Inversions.

Definition

$ev(f)$ = even no of Transpositions.

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

f is even $\iff$ $ev(f)$ is even.

Sol Any cycle of length m can be written as a product of $m-1$ Transposition $(123) = (12)(23)$

$(a_1 a_2 \ldots a_m) = (a_1 a_2)(a_2 a_3) \ldots (a_{m-1} a_m)$

Each cycle of even length would have odd no Transpositions

" " " odd length " " even no

Each cycle of even length $\to 1$
" " " odd " $\to 0$

$\Big\}$ Transpositio mod (2).

Alternating group

$A_n \le S_n = \mathrm{Sym}(X)$

Proposition

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

$X = \{1, 2, \ldots n\}$

$|S_n| = n!$

$\varphi : S_n \longrightarrow S_n$

$\varphi : f \longrightarrow fg$ $\quad g = (1\ 2)$

What is the inverse of φ.

φ is a bijection,

if f is even $\Rightarrow$ fg is odd, so φ is a bijection between the set of even permutations & the set of odd permutations.

$|A_n| = |S_n \setminus \{A_n\}| = \frac{n!}{2}$

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

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

Cosets

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

Hg

$\circ$ operation here is the multiplication

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

gH

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

$G/H = \{Hg_1, Hg_2, \ldots\}$

cosets of H by g_1

Quotient group

$|G| = |H| \cdot Ind(H)$

Properties of Quotinet group

1. The identity element of a quotient group is the subgroup itself.
2. If N is a normal subgroup of G, the Order of G/N is equal to the order of G divided by the order of N.That is, $|G/H| = |G|/|N|$.
3. Quotient group of an abelian group is abelian, but the converse is not true.
4. Every quotient group of a cyclic group is cyclic, but the opposite is not true.
5. The quotient group G/G has correspondence to the trivial group, that is, a group with one element.
6. The quotient group $G/\{e\}$ has correspondence to the group itself.
7. If G is nilpotent then so is the quotient group G/N.
8. If G is solvable then the quotient group G/N is as well

Quotient group

$\mathbb{Z}$, $3\mathbb{Z}$

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: Given $G = \{\ldots -2, -1, 0, 1, 2, 3, \ldots\}$ $= \mathbb{Z}$
And $N = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ $= 3\mathbb{Z}$
$G/N = \{N + a|$ a is in $G\}$
then $N + 1 = \{\ldots, -5, -2, -1, 2, 5, \ldots\}$
$N + 2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
Now$a = 3b + c$ where b is in G and $c = 0, 1, 2$.
Therefore, $N + a = N + (3b + c) = (N + 3b) + c = N + c$ many
As 3b belong to N.
Thus, $G/N = \{N, N + 1, N + 2\}$
Now, Order of G/N = Index of N in G = Number of cosets of N in G = 3.

$G/H = Hg$

$Hg = N+a$

$N+1, N+2, N+0$

Coset

$N+3 = \{\ldots, -3, 0, 3, 6, \ldots\} = N$

$G/N = \{N, N+1, N+2\}$ Order $(N) = 3$

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.

Solution: Clearly, G is abelian being a multiplicative group, then N is a normal subgroup.

The quotient group $G/N = \{Na|$ a is in $G\}$

$G/H = \{Hg \mid h \in H,\ g \in G\}$

$N1 = \{1, -1\} = N$ ✓

$N(-1) = \{-1, 1\} = N$ ✓

$Ni = \{i, -i\}$ ✓

$N(-i) = \{-i, i\} = Ni$

$G/N = \{N, Ni\}$

$$\boxed{|G| = |H| \cdot \mathrm{Ind}(H)}$$

$$= 2 \cdot 2 = 4$$

Quotient group

$(12)(12) = id \qquad (23) = g \in S_3$

$(12)(23) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Example

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

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

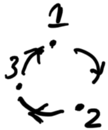
$Hg = \{(23), (12)(23)\} = \{(23), (123)\} = \{(23), (312)\} = \{(32), (231)\}$

Example

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

   What about $(23)(12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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



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 $Hf = Hg$.

$(23)(12) = (321) \neq (123)$ Not commutative S_3

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.

Tutorial

Exams Style Questions

MEWMYZ – Code

Exam Year, 2023

$g = (1\,3)(2\,8\,6\,5\,7)(4)$ ord$(g) = \text{lcm}(2,5) = 10$

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.

$f = \underbrace{(1\,5)}_{2}\underbrace{(2\,6\,8)}_{3}\underbrace{(3\,4)}_{2}$ ord$(f) = \text{lcm}(2,3,2) = 6$

Exams Style Questions

Exam Year, 2023

Question 2:

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

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

$$= (143576)(8)(2)$$

$\text{ord}(fg) = 6$

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 $\langle (12), (2345 \cdots n) \rangle$?

Which of these $f, g, fg \in A_n$.

$f = (15)(26)(68)(34) \in A_n$

4 Transpositions.

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. $\langle r^2 s\rangle$

Q2 (above slide): Write down permutation $(1k)(1\ell)(1k)$ in disjoint cycle notations.

$$\begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix}\begin{pmatrix} 1 & \ell \\ \ell & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix} = \begin{pmatrix} 1 & k & \ell \\ 1 & \ell & k \end{pmatrix} = (k, \ell)$$

Now $(1k)(1\ell)(1k) = (\ell k) = (k\ell) \in H$

$$S_n \subseteq H$$

as all transpositions are in H.

Exams Style Questions $\langle r^3, r^2 s\rangle = \{e, r^3, r^2 s, r^5 s\}$

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.

Sol $\langle rs, r^4 s\rangle$. we are interested to find out the elements of D_{12}.

$D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, rs, r^2 s, r^3 s, r^4 s, r^5 s\}$

$\langle rs, r^4 s\rangle$

$(rs)^2 = rs \cdot rs = r\,\underline{s \cdot r}\,s = r r^{-1} s \cdot s$
$= e \cdot e = e$

$(r^4 s)^2 = (r^4 s)\cdot(r^4 s) = r^4 s \cdot r^4\, s = r^4 (\underline{s \cdot r}) r^3 s$
$= r^4 \cdot r^{-1} s r^3 \cdot s = r^3 s r^3 \cdot s = r^3 \cdot r^{-1} \cdot s r^2 s$
$= r^2 s r^2 s = r \cdot rs\, r \cdot r \cdot s$

Exams Style Questions

$= r(r^{-1}s)\,r\,(r^{-1}s) = s^2 = e$

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.

$$(rs)\cdot(r^4 s) = r\cdot \underline{s\,r}\cdot r^3 s$$
$$= r\,r^{-1} s\, r^3 s$$
$$= s\, r^3 s = \underline{s\cdot r}\, r^2 s = s r^3 s$$
$$= r^{-1} s\, r^2 s = r^{-1}(s r)\, r s$$
$$= r^{-1}\,\underline{(r^{-1} s)}\, r s$$
$$= r^{-2}\, r^{-1} s\cdot s$$
$$= r^{-3}\cdot s^2 = r^{-3}$$
$$= r^3$$

Exams Style Questions

$$\left\{1, rs, r^4 s, r^3, \underline{\underline{r^{-2}}}, \underline{\underline{r^7}}\right\} = \langle rs, r^4 s\rangle$$

verify about these elements

Next you need to find the cosets of this subgroup

Exams Style Questions

$$\langle r^3, r^2 s\rangle = \{r^3, r^2 s, r^5 s, e\}$$

completed Subgroup

r^3, $(r^3)^2 = r^6 = 1$

$$(r^2 s)^2 = (r^2 s)(r^2 s)$$
$$= r^2\ s . r . rs$$
$$= r^2 . r^{-1} s . rs$$
$$= r\, \underline{s . r}\, s = r r^{-1} s . s = e$$

$$(r^3)(r^2 s) = r^5 s$$

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

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

  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

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