Elements of Algebraic Structures DATE

Lecture 7: Normal Subgroup

Lecture: Sujata Ghosh *Scribe: Rajdeep Das and Soumik Guha Roy*

Contents

1 Cycle and Transposition

1.1 Definition

- A permutation which can be represented in a cyclic form is called a **cycle**.
- A permutation which replaces n objects cyclically is called a **cyclic** or **circular permutation of degree n**
- In a permutation, the cycle of length 2 is called **transposition**.

1.1.1 Example

Examples of Cycles and Degree of cycles

- Consider the permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$.This permutation can also be written in the cyclic form $(1\ 2\ 4\ 3)$ with a degree 4.

- Consider the permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.This permutation can also be written in the cyclic form $(1) \circ (2) \circ (3) \circ (4)$.Each of the 4 cycle has degree 1 and the permutation has no transpositions or cycles of length 2.

- Consider the permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.This permutation can also be written in the cyclic form $(1\ 2) \circ (3\ 4)$.Both the cycle has degree 2 and the permutation has 2 transpositions.

- Consider the group SG_3 and $\tau \in SG_3.\tau$ can also be written in the cyclic form as $(1) \circ (2\ 3)$.Here the 1^{st} cycle has degree 1 and the 2^{nd} cycle has degree 2.The permutation has only one transposition.

1.2 Even permutation

- If a permutation is a product of even number of transposition, then the permutation is called **even permutation**.

- An even permutation $\sigma \in SG_n$ is such that $A_\sigma \in GL_n(\mathbb{R})$ is obtained from $I_n \in M_n(\mathbb{R})$ by even number of column exchanges

Examples of even permutation

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

- $(1\ \ \ 5\ \ 3\ \ 4\ \ 2) = (1\ \ 2) \circ (1\ \ 4) \circ (1\ \ 3) \circ (1\ \ 5)$

- Cosider the following permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 & 9 & 10 & 8 \end{pmatrix}$.The cyclic form is $(1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (8\ 9\ 10) = (1\ 7) \circ (1\ 6) \circ (1\ 5) \circ (1\ 4) \circ (1\ 3)) \circ (1\ 2) \circ (8\ 10) \circ (8\ 9)$.The given permutation has 8 transpositions. Hence, the permutation is even permutation.

1.3 Odd permutation

- If a permutation is a product of odd number of transposition, then the permutation is called **odd permutation**.
- An even permutation $\sigma \in SG_n$ is such that $A_\sigma \in GL_n(\mathbb{R})$ is obtained from $I_n \in M_n(\mathbb{R})$ by odd number of column exchanges

Examples of odd permutation

- $(1\ \ 2\ \ 3\ \ 4) = (1\ \ 4) \circ (1\ \ 3) \circ (1\ \ 2)$
- $(1\ \ 6\ \ 5\ \ 3\ \ 4\ \ 2) = (1\ \ 2) \circ (1\ \ 4) \circ (1\ \ 3) \circ (1\ \ 5) \circ (1\ \ 6)$
- Cosider the following permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 & 10 & 9 \end{pmatrix}$.The cyclic form is $(1\ 2\ 3\ 4) \circ (5\ 6\ 7\ 8) \circ (9\ 10) = (1\ 4) \circ (1\ 3) \circ (1\ 2) \circ (5\ 8) \circ (5\ 7)) \circ (5\ 6) \circ (9\ 10)$.The given permutation has 7 transpositions. Hence, the permutation is odd permutation.

2 Relation between SG_n and GL_n

2.1 Permutation Matrix A_σ w.r.t a permutation $\sigma \in SG_n$

Consider the symmetric group of order 3 donoted by SG_3 and the identity matrix of order 3 which is $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

- Now $\tau'' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.Then $A_{\tau''} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ which is obtained by interchanging the 1st and 2nd column of I_3
- Now $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.In the same way,$A_\sigma = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ which is obtained by shifting 2nd column to the 1st column and 3rd column to the 2nd column and 1st column to the 3rd column of I_3,i.e the j^{th} column of I_3 is replaced by the $\sigma(j)^{th}$ column.

3 Kernel of a Homomorphism

Consider a homomorphism f $f : G \mapsto G^{'}$. Let $g \in G$ and $h \in ker f$. Now as $g, h \in G \implies ghg^{-1} \in G$.
Hence $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e_{g^{'}}f(g)^{-1} = f(g)f(g)^{-1} = e_{g^{'}}$
Hence, we can say that $ghg^{-1} \in ker f$.This is true for all $h \in G$.
Therefore, $gKerfg^{-1} \subseteq G$

Exercise

Prove that $kerf \subseteq g\ Kerf\ g^{-1}, \forall g \in G$.

4 Monomorphism and $kerf$

Theorem 4.1 *Let $\phi : (G, \circ) \mapsto (G^{'}, *)$ be a homomorphism. Then ϕ is Monomorphism $\iff$ $ker\ \phi = \{e_G\}$. That is $ker\ \phi$ has only one element e_G.*

Proof.
($\implies$ **)**We have ϕ is one to one function.Then $\phi(e_G) = e_{G'} \implies e_G$ is a pre-image of $e_{G'}$.
Now as ϕ is one to one function , $e_{G'}$ will have only one pre-image $e_G \implies kerf = \{e_G\}$
($\impliedby$ **)**We have $kerf = \{e_G\}$ and let us assume that $a, b \in G$ and $\phi(a) = \phi(b)$. Then
$\phi(a^{-1} \circ b) = \phi(a^{-1}) * \phi(b)$
$\phi(a^{-1} \circ b) = \phi(a)^{-1} * \phi(b)$ [As $\phi : G \mapsto G^{'}$is homomorphism $\implies \forall a \in G$,$\phi(a^{-1}) = \phi(a)^{-1}$]
$\phi(a^{-1} \circ b) = \phi(b)^{-1} * \phi(b)$ [As $\phi(a) = \phi(b)$]
$\phi(a^{-1} \circ b) = e_{G'}$
As $ker\phi = \{e_G\} \implies ker\phi$ has only one element $\implies a = b$
Hence, we have shown that $\phi(a) = \phi(b) \implies a = b \implies \phi$ is one-to-one function.

□

Examples related to theorem 1

- Consider $f : (\mathbb{Z}, +) \mapsto (SG_2, \circ)$. The function f defined as :

$$f(z) = \begin{cases} e & \text{if z is even} \\ \tau & \text{if z is odd} \end{cases} \tag{1}$$

  We can see that $kerf = 2\mathbb{Z} \neq \{0\} \implies$ f is not one-to-one i.e f is not monomorphism.

- Consider $f : (GL_n(\mathbb{R}), *) \mapsto (GL_1(\mathbb{R}), *)$. the function f defined as:

$$f(A) = det(A) \tag{2}$$

  We know the identity element of $(GL_1(\mathbb{R}), *)$ is $e^{'}_{G} = 1$. Hence $kerf = \{A \in GL_1(\mathbb{R})$ where $det(A) = 1\}$. We can say that $I_n \in kerf$ and $RrI_n \in ker$-f where RrI_n is all row reversed identity matrix of order n.Hence $kerf \neq \{I_n\} \implies f$ is not monomorphism

5 Normal Subgroup

5.1 Definition

Let, G be a group and H is a sub group of G. H is called normal subgroup of G iff $\forall g \in G$ $gHg^{-1} = H$.
Here,$\forall g \in G$ the set $gHg^{-1} = \{ghg^{-1} | \forall h \in H\}$.
Notation: H, a subgroup of G is denoted as $H \lhd G$.

Exercise

Prove that $gHg^{-1}$is a subgroup of G, where H is a subgroup of G and $g \in G$.

5.2 Examples of Normal subgroups

- For any homomorphism $f : G \mapsto G^{‘}$, $kerf \lhd G$.

- If G is commutative group, then any subgroup of G is a normal sub group of G

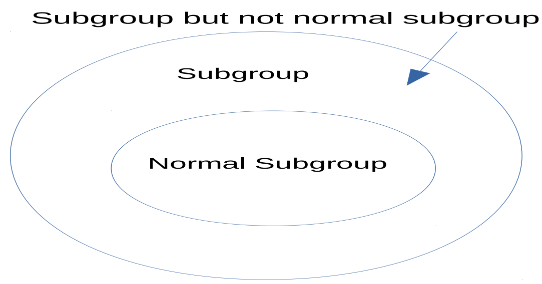

Figure 1: Subgroup and Normal subgroup.

5.3 Subgroup vs Normal subgroup

Example of subgroup which is not normal subgroup

Consider the SG_3 group and subgroup H=$\{e, \tau\}$.Here $\forall a \in SG_3$ $a \circ H \neq H \circ a$. Hence, H=$\{e, \tau\}$ is subgroup of SG_3 but not normal subgroup of SG_3.

Exercise

- Is there any non-trivial Normal subgroup of the group SG_3?
- Show that $\{e, \sigma\, \sigma^{'}\}$ is a normal subgroup of the group SG_3.

5.4 Special Linear Group

We are given with $f : (GL_n(\mathbb{R}), *) \mapsto (GL_1(\mathbb{R}), *)$. the function f defined as:

$$f(A) = det(A) \tag{3}$$

then $kerf = \{A \in GL_1(\mathbb{R})$ where $det(A) = 1\}$. Now $kerf$ is a special linear group of order n ,denoted by $SL_n(\mathbb{R})$.

- $SL_n(\mathbb{R})$ is also normal subgroup of $GL_n(\mathbb{R})$ under matrix multiplication.

5.5 Alternating group

Consider the groups $SG_n, GL_n(\mathbb{R}), GL_1(\mathbb{R})$.From the section 2.1,we have

$$f : (SG_n, \circ) \mapsto (GL_n(\mathbb{R}), *) \tag{4}$$

From 5.4, we have

$$g : (GL_n(\mathbb{R}), *) \mapsto (GL_1(\mathbb{R}), *) \tag{5}$$

From 4 and 5,we have

$$h = g \circ f : (SG_n, \circ) \mapsto (GL_1(\mathbb{R}), *) \tag{6}$$

Now $ker\ h = ker\ g \circ f = \{\sigma\ \ : \text{where } det(A_\sigma) = 1\}$ also called the **Alternating group** denoted by AG_n.

- Alternating group AG_n is also Normal subgroup.

5.6 Center of a Group

Let us assume that $(G, \circ)$ is a group.H be a subset of G defined as $H = \{x \in G : x \circ g = g \circ x\ \forall g \in G\}$.The set H, called **center of the group G** is subgroup of G.

- Center of a group G is denoted by Z(G).
- Elements of the group Z(G) are called **central element of G**.
- Z(G) is commutative subgroup of group.
- G is commutative group $\implies$ Z(G)=G.

Example: Elements of $Z(\mathbb{Z})$ that is center of the group $(\mathbb{Z}, +)$

$Z(\mathbb{Z}) = \{...., -3, -2, -1, 0, 1, 2, 3...\} = \mathbb{Z}$

Example: Elements of $Z(\mathbb{R}^*)$ that is center of the group $(\mathbb{R}^*, *)$

$Z(\mathbb{R}^*) = \mathbb{R}^*$

Exercise

- Prove that $Z(G) \lhd G$

5.7 Aut G

Given a homomorphism f where $f : G \mapsto G$. Aut G defined as set of homomorphism from G to G.
Aut G=$\{f\ |f : G \mapsto G\}$

Exercise

- Prove that $(Aut(G), \circ)$ is a group.

- Aut G is non-abelian group.