Elements of Algebraic Structures 9th March 2024

Lecture 8: Cosets

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

Topics discussed in this lecture

In this lecture, we shall talk about the following

1. Mapping from Group G to its Automorphism Group
2. Maps and Equivalence relation on a Group
3. Cosets
4. Lagrange's Theorem

1 Mapping from Group G to its Automorphism Group

We are interested to find a mapping $f : G \to Aut(G)$ such that $Kerf = Z(G)$ .Here $Z(G)$ =Centre of the group G . Every element $a \in G$ maps to an element $f(a)$ in $Aut(G)$. We know $Aut(G)$ is a set of all possible automorphism in G (i.e isomorphism from G to itself). Hence $f(a)$ is an automorphism in G.
Now let us define the mapping $f(g) : G \to G$ as follows

$$f(g)(h) = g * h * g^{-1}$$

Now to show $f(g) \in Aut(g)$ we proof the following
(1) $f(g)(h * h') = f(g)(h) * f(g)(h')$
(2) $f(g)$ is a bijection
Proving (1)

$$\begin{aligned} f(g)(h * h') &= g * (h * h') * g^{-1} \\ &= (g * h) * (h' * g^{-1}) \\ &= (g * h) * (g^{-1} * g) * (h' * g^{-1}) \\ &= (g * h * g^{-1}) * (g * h' * g^{-1}) \\ &= f(g)(h) * f(g)(h') \end{aligned}$$

Proving (2)
For any $a, b \in G$ such that $f(g)(a) = f(g)(b)$
Which implies $g * a * g^{-1} = g * b * g^{-1} \implies a = b$
Proving $f(g)$ is injective.

Now for any $a \in G$ we have $g * h * g^{-1} = a$ for some $h \in G$.
which implies $g^{-1} * h * g = h$
Hence $f(g)$ indeed is an Automorphism.
Now

$$\begin{aligned} Kerf &= \{g \in G : f(g) \text{ is the identity map}\} \\ &= \{g \in G : f(g)(h) = h \text{ for all } h \in G\} \\ &= \{g \in G : g * h * g^{-1} = h \text{ for all } h \in G\} \\ &= \{g \in G : g * h = h * g \text{ for all } h \in G\} \\ &= Z(G) \end{aligned}$$

2 Maps and Equivalence relation on a Group

Let S and T are two non-empty sets . Let there is a mapping $f : S \to T$. Now let us define a binary relation R on S , such that for $a, b \in S$ aRb if and only if $f(a) = f(b)$. Clearly with little effort it can be shown that binary relation R is an Equivalence relation.
Now rather than just being two non-empty sets , if S and T are two groups & f being a homomorphism. Let K be the set of all equivalence classes induced by the homomorphism f. Then clearly $Kerf \in f$

Proposition 2.1 *Any member of K is of the form $aH = \{ah : h \in H\}, a \in G$*

Proof. For any $a \in G$ we need to prove the following

1. $aRb \to b \in aH$

2. $b \in aH \to aRb$

proving 1 ,
for any $a, b \in G$

$$aRb \to f(a) = f(b)$$

Pre-Multiplying $f(a)^{-1}$ both sides of the equation we get the result

$$\begin{aligned} e_G &= f(a)^{-1} * f(b) \\ &= f(a^{-1}) * f(b) \\ &= f(a^{-1} * b) \end{aligned}$$

As element $a^{-1} * b$ maps to e_G , We say that $a^{-1} * b \in H$
Hence for some $h \in H$

$$a^{-1} * b = h$$

$$b = ah$$

Hence $b \in aH$
proving 2 ,
for some $h \in H$

$$b \in aH \to b = a * h$$

implies ,

$$\begin{aligned} f(b) &= f(a * h) \\ &= f(a) * f(h) \\ &= f(a) * e_G \\ &= f(a) \end{aligned}$$

Hence aRb
This completes the proof

□

Proposition 2.2 *For any $a \in H$, there exists a bijection between set H and aH . i.e they have the same cardinality .*

Proof. Now lets define $f : H \to aH$ by $g(h) = a * h$
For any two element $m, n \in H$ if $f(m) = f(n)$ then implies,

$$a * m = a * n$$

$$m = n$$

Hence f is injective .
Now for surjectivity ,
let there be an element $q \in aH$, then q can be written in the form $q = ah$ for some $h \in H$. implies ,

$$h = a^{-1} * b$$

hence there exists a pre-image of q. This completes the proof. □

Corollary 2.3 *If G is any finite group , then $|G| = |Kerf|.|Image(f)|$*

An application of this corrollary :
Consider SG_n and AG_n
We have $|SG_n| = n!$
Consider $g : SG_n \to \{1, -1\}$(via $GL_n(R)$)
We know $Kerg = AG_n$
so , $|SG_n| = |AG_n|.2$
i.e $|AG_n| = n!/2$

3 Cosets

Definition

Let G be a group and H be a subgroup of G. The left coset of H in G is defined as:

$$aH = \{ah : h \in H\},$$

where $a \in G$.
Similarly, the right coset of H in G is defined as:

$$Ha = \{ha : h \in H\},$$

where $a \in G$.

Examples

1. Let $G = \mathbb{Z}$, the group of integers under addition, and $H = 2\mathbb{Z}$, the subgroup of even integers. Then:

$$1 + 2\mathbb{Z} = \{1 + 2k : k \in \mathbb{Z}\} = \{..., -3, -1, 1, 3, ...\}$$

the set of all odd integers.

2. Consider the group $G = \mathbb{R}^*$, the set of nonzero real numbers, under multiplication, and let $H = \{x \in \mathbb{R}^* : |x| = 1\}$ be the subgroup of complex numbers with magnitude 1. Then:

$$\{-1, 1\}H = \{-1, 1\},$$

and

$$iH = \{i, -i\},$$

where i is the imaginary unit.

3. Let $G = S_3$, the symmetric group on three letters, and $H = \{e, (1\,2)\}$ be the subgroup generated by the transposition $(1\,2)$. Then:

$$(1\,3)H = \{(1\,3), (1\,2\,3)\},$$

and

$$H(1\,2) = \{(1\,2), (1\,3\,2)\}.$$

We will denote "Left Coset" as "Coset" , Unless otherwise specified .
In previous propositions we have found that , We can form a partition in G considering the subgroup $Ker f$ corresponding to a homomorphism f with domain G.
Is the above observation also true for any subgroup H of G ?

Proposition 3.1 *Let $\mathcal{K}$ denote the set of all cosets of H in G. Then, G can be partitioned by members of $\mathcal{K}$, that is*

1. $G = \bigcup_{a \in G} aH$
2. *for any $aH, bH \in \mathcal{K}$, either, $aH = bH$ or $aH \cap bH = \varnothing$*

Proof.

1. *Take any $g \in G$. To show that $g \in aH$ for some $a \in G$, note that $g \in gH$ and we are done.*
2. *Take any $aH, bH \in \mathcal{K}$.*
   - *If $aH = bH$, we are done.*
   - *Suppose not, i.e., $aH \neq bH$. We have to show that $aH \cap bH = \varnothing$. Suppose not.*
   - *Let $c \in aH \cap bH$. Then $c \in aH$ and $c \in bH$. So, $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$.*
   - *Then, $a = bh_2h_1^{-1} \in bH$, so $aH \subseteq bH$.*
   - *Similarly, we can show that $bH \subseteq aH$.*
   - *So, $aH = bH$, a contradiction. Hence, the proof is complete.*

□

Thus, G can be partitioned by the cosets of H in G, where H is a subgroup of G. Also, the cardinality of each such coset of H is the same as that of H.
Let us denote the number of such cosets of H in G to be the index of H in G, written as $[G : H]$.

Corollary 3.2 *If G is a finite group, then $|G| = |H| \cdot [G : H]$.*

This immediately tells us that for a finite group G, and a subgroup H of G:

4 Lagrange's Theorem

Theorem 4.1 ***Lagrange's Theorem:*** *The order of a subgroup of a finite group G divides the order of G.*

4.1 Application of Lagrange's theorem

1. Let G be a finite group and let $g \in G$. Then, $\mathcal{O}_G(g) \big| |G|$.

Proof. Take $g \in G$.
Consider $\langle g \rangle$, the cyclic subgroup of G generated by g.

Now, by Lagrange's theorem, $|\langle g\rangle| \big| |G|$. But $|\langle g\rangle| = \mathcal{O}_G(g)$.
Hence, the result. □

Lagrange Theorem

Claim 4.2 *Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.*

Proof. The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G : H]|H|$. □

Homework: Let H and K be subgroups of a finite group G such that $G \supseteq H \supseteq K$. Then show that $[G : K] = [G : H][H : K]$.

Homework: Is the converse of Lagrange's Theorem true? Prove or disprove