MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Fri, Apr 10, 2020.

Chapter 9: Normal subgroups and factor groups cont'd.

In the course of proving Lagrange's theorem, we considered the set $[G:H]_\ell$ of left cosets of a subgroup H of a group G. We noted that any two left cosets have the same cardinality (size). A natural question to ask is:

Q: Under what conditions can $[G:H]_\ell$ be endowed with a group structure? (When $[G:H]_\ell$ is given a group structure we ~~write~~ denote this group by G/H and call this the factor group (as in the book), or the quotient group, as in some other books.) The answer to the question Q is given by:

Theorem 9.2: Let G be a group and H a normal subgroup of G. Then the set $G/H = \{aH \mid a \in G\}$ is a group under the operation

$$aH \cdot bH = abH. \qquad (1)$$

Proof: We need to first show that this multiplication operation is well defined. This is because aH could be replaced by $a'H = aH$ and bH could be replaced by $b'H = bH$ and this would give $a'Hb'H = a'b'H$. But then would $abH = a'b'H$? We will show this to be the case, and hence the operation in (1) would be well defined.

Note that

$$\left.\begin{array}{l} aH = a'H \iff \exists\, h_1 \in H, \text{ such that } a' = ah_1 \\ bH = b'H \iff \exists\, h_2 \in H, \text{ such that } b' = bh_2 \end{array}\right\} \qquad (2).$$

Thus

$$a'b'H = ah_1 bh_2 H = ah_1 b(h_2 H) = ah_1 bH \qquad (3)$$

Now we use the fact that $H \triangleleft G$ to infer that $bH = Hb$. So (3) can be recast as

$$a'b'H = ah_1 Hb = a(h_1 H)b = aHb = a(Hb) = a(bH) = abH,$$

and this establishes ~~we~~ that the operation is well defined.

Clearly by (1) we have G/H is closed under the operation. The associative law holds because H is a normal subgroup.

To see this note that

$$(aH\, bH)cH = (abH)cH = abc\,H = a(bcH) = aH(bcH) = aH(bH \cdot cH)$$

Next observe that $eH = H$ is the identity in G/H, because by (1),

$$eH \cdot aH = e \cdot aH = aH = a \cdot eH = aH \cdot eH \quad , \forall a \in G.$$

Consequently $(aH)^{-1} = a^{-1}H$ in G/H because

$$aH \cdot a^{-1}H = a \cdot a^{-1}H = eH \quad \& \quad a^{-1}H \cdot aH = a^{-1}aH = eH.$$

This proves that G/H is a group under the operation in (1).

<u>Remark on Notation</u>: When H is any subgroup of G, we used the notation $[G:H]_\ell$ and $[G:H]_r$ to denote the set of left cosets and the set of right cosets to distinguish between them. When H is <u>normal</u>, every left coset is equal to the corresponding right coset. So we <u>drop the subscript</u> ℓ and use the G/H notation to denote the <u>group</u> of left ~~left~~ (= right) cosets. This leads to

<u>Q2</u>: If the set of left cosets is a group under the operation in (1), should H be a normal subgroup?

The answer to this question is YES and this is the converse to Thm 9.2:

<u>Problem 39; p189</u> (Converse of Thm 9.2).

Let G be a group and H a subgroup of G such that the operation in (1) is well defined. Then H is a normal subgroup.

Remark: In proving Thm 9.2, the main point was to show that the operation in (1) is well defined. From that, the group properties followed automatically. Hence in the converse stated above, we focus on (1) being well defined.

<u>Proof of the converse to Thm 9.2</u>: Pick <u>any</u> $x \in G$ and any $h \in H$. Then consider

$$\begin{aligned} xhx^{-1}H &= (xh) \cdot x^{-1}H = (xh)H \cdot x^{-1}H \quad \text{(using (1))} \\ &= x(hH)x^{-1}H = xH \cdot x^{-1}H = x \cdot x^{-1}H \quad \text{(using (1) again)} \\ &= eH = H \end{aligned} \tag{4}$$

Since $xhx^{-1}H = H$, it follows that $xhx^{-1} \in H$, $\forall h \in H$. This means $xHx^{-1} \subseteq H$, and $x \in G$ is arbitrary. Hence H is a normal subgroup (by the normal subgroup test).

An important example: We already noted that if $G = (\mathbb{Z}, +)$ and $H = (n\mathbb{Z}, +)$, where n is a positive integer, then the set of cosets is given by $\mathbb{Z}_n$; the set of residue classes mod n. Since $G = \mathbb{Z}$ is Abelian, we have $H = n\mathbb{Z}$ is a normal subgroup. Thus $\mathbb{Z}_n$ is a group, which it is under the operation $+_n$ (addition modulo n).

Given any group G, its center $Z(G)$ is a normal subgroup. So a natural question to ask is: what is $G/Z(G)$? The answer is:

Theorem 9.4: For any group G, the group $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$, the group of inner automorphisms of G.

Proof: Recall that given $g \in G$, the inner automorphism i_g generated by g is given by

$$\left.\begin{array}{l} i_g : G \longrightarrow G \\ \quad x \rightarrow gxg^{-1} \end{array}\right\} \; i_g(x) = gxg^{-1}, \; \forall x \in G. \qquad (5)$$

We have already established in Problem 47, Chapter 6, p135 (see page 5 of my Lecture Notes dated ~~Wed~~ Mon, Mar 16) that

$$i_g = i_h \iff h^{-1}g \in Z(G) \iff g^{-1}h \in Z(G). \qquad (6)$$

What (6) is saying is that

$$i_g = i_h \iff gZ(G) = hZ(G) \qquad (7)$$

because $h^{-1}g \in Z(G) \iff gZ(G) = hZ(G)$ as cosets. Thus the equality of i_g and i_h is the equality of cosets $gZ(G)$ and $hZ(G)$. This means the map

$$\left.\begin{array}{l} \phi : G/Z(G) \longrightarrow \mathrm{Inn}(G) \\ \quad gZ(G) \rightarrow i_g \end{array}\right\} \qquad (8)$$

is a well defined map from the set of cosets of $Z(G)$ to $\mathrm{Inn}(G)$. From (6) and (7) it follows that ϕ is a bijection. The operation preserving property of ϕ follows because we know that $i_{gh} = i_g \circ i_h$. That is

$$\phi(ghZ(G)) = i_{gh} = i_g \circ i_h = \phi(gZ(G)) \circ \phi(hZ(G))$$

Hence ϕ is an isomorphism.

Some properties of factor groups

Problem 11, p. 188: Let G be a cyclic group and H a subgroup. Prove that G/H is cyclic.

Remark: We know that every subgroup of a cyclic group is cyclic. Thus H is cyclic. What is asserted here is that G/H is also cyclic.

Proof: Since G cyclic $\Rightarrow$ G is Abelian, we have $H \lhd G$. Since G is cyclic, $G = \langle a \rangle$, and since H is cyclic, $H = \langle a^k \rangle$, for some $k \in \mathbb{Z}^+$. We distinguish two cases.

Case 1: $|G| < \infty$.

Let $|G| = n$. Then $H = \langle a^d \rangle$, for some $d \mid n$, and $|H| = \frac{n}{d}$.
Then

$$G/H = \{H, aH, a^2H, \dots, a^{d-1}H\} = \langle aH \rangle$$

since $a^d \in H$ and d is the minimal positive integer such that $a^d \in H$. Thus G/H is cyclic.

Case 2: $|G| = \infty$. In this case, with $H = \langle a^k \rangle$, $k \in \mathbb{Z}^+$, we have

$$G/H = \{H, aH, a^2H, \dots, a^{k-1}H\}$$

since $a^k \in H$ and k is the minimal positive integer satisfying $a^k \in H$.
Thus G/H is cyclic.

Remark: Note from the above proof, that regardless of whether G is finite or infinite, if G is cyclic, then G/H is a finite cyclic group and hence is isomorphic to $\mathbb{Z}_m$, for some $m \in \mathbb{Z}^+$.

Problem 12, p. 188: Let G be an Abelian group and H a subgroup. Prove that G/H is Abelian.

Remark: We know that H is Abelian, and G Abelian implies $H \lhd G$. What is asserted here is that G/H is Abelian.

Proof: Start with $G/H = \{aH \mid a \in G\}$. Since G and H are Abelian, and H is a normal subgroup, we have $\forall\, a, b \in G$,

$$aH \cdot bH = abH = baH = bH \cdot aH.$$

Hence G/H is Abelian.

We already noticed that A_n is a normal subgroup of S_n and that $R^{(n)}$, the subgroup of all rotations in D_{2n} is a normal subgroup of D_{2n}. In both these examples we have

$$|S_n : A_n| = |S_n/A_n| = 2 = |D_{2n} : R^{(n)}| = |D_{2n}/R^{(n)}| = 2.$$

The following assertion is a generalization of this observation:

Problem 9, p. 188: If G is a group and H a subgroup of G such that H has index 2, that is $|G:H| = 2$, then H is a normal subgroup.

Proof: Since H has index 2, there are just two cosets of H, namely H and $G-H$. As left cosets we have

$$aH = H, \ \forall a \in H, \ \& \ aH = G-H, \ \forall a \notin H. \tag{9}$$

Similarly

$$Ha = H, \ \forall a \in H, \ \& \ Ha = G-H, \ \forall a \notin H. \tag{10}$$

So by (9) and (10) we see that

$$aH = Ha, \quad \forall a \in G$$

Thus H is a normal subgroup of G.

What about subgroups of order 2? Here we have:

Problem 70, p192: Let G be a group and H a normal subgroup of order 2. Then H is contained in $Z(G)$, the center of G.

Proof: We are given that $H \lhd G$ and $|H| = 2$, that is $H = \{1, a\}$, with $a \neq e$, but $a^2 = e$. To show that $H \subseteq Z(G)$, we have to show that every element of H commutes with every element of G. Clearly e commutes with every element of G. So we need to show that

$$ax = xa, \quad \forall x \in G. \tag{11}$$

Now (11) is equivalent to

$$xax^{-1} = a, \quad \forall x \in G. \tag{12}$$

Since H is normal, we have $xax^{-1} \in H$. Thus $xax^{-1} = e$ or $xax^{-1} = a$.
If $xax^{-1} = e$, then $xa = ex = x \Rightarrow a = e$, which is a contradiction.
Thus $xax^{-1} = a$, $\forall x \in G$ which proves (12) which is equivalent to (11). Hence $H \subseteq Z(G)$ as asserted.