MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Mon, Apr 13, 2020

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

There is a very famous theorem of Cauchy which is:

Cauchy's theorem: Let G be a finite group and let p be any prime that divides the order of the group. Then G has an element of order p

Remark: We have already established this theorem for finite cyclic groups G. The proof of Cauchy's theorem for all finite groups is difficult. We now establish Cauchy's theorem for all Abelian groups (finite) as a nice application of the idea of factor groups. That is, we now prove

Theorem 9.5 (Cauchy's Theorem for Abelian groups)

Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p. //

Remark: The proof we give below is different (somewhat) from the proof in the book. Our proof utilizes the assertions in two problems in the book which we state below as Lemmas 1 and 2 and prove these Lemmas. I suggest you also read the proof in the book on p. 182.

Lemma 1 (Problem 37, p. 189)

Let G be a finite group and H a normal subgroup of G. Then the order of an element gH in the factor group G/H divides the order of g in G.

Proof: Let $|g| = n$. This is finite since G is finite. Thus n is the minimal positive integer for which $g^n = e$. Let the order of gH in G/H be m; that is m is the minimal positive integer for which

$$(gH)^m = g^m H = H, \qquad (1)$$

which means m is the minimal positive integer for which $g^m \in H$.

Now if $|g| = n$, then $g^n = e$ and so

$$(gH)^n = g^n H = eH = H \qquad (2)$$

By the minimality of m in (1), namely the definition of the order of gH, and by (2), we see that m/n. That proves Lemma 1.

Lemma 2: (Problem 67, p. 191)

Let G be a finite group and H a normal subgroup of G. If the factor group G/H has an element of order m, then G has an element of order m.

Proof: Consider an element gH of G/H that has order m. Then by Lemma 1 we know that the order of g in G is a multiple of m. So write $|g| = mt$, with $t \in \mathbb{Z}^+$. This means

$$|\langle g \rangle| = n = mt$$

and $n = mt$ is the minimal exponent (positive) for which $g^{mt} = e$. Notice that $g^t \in \langle g \rangle$ and $|g^t| = \frac{n}{t} = m$. Thus $g^t \in G$ has order m. This proves Lemma 2.

NOTE: Lemmas 1 and 2 hold for all finite groups G, not just Abelian groups. But we will use the fact that G is Abelian in deducing Theorem 9.5 from Lemmas 1 and 2.

Proof of Thm 9.5: The theorem clearly holds if $|G| = 2$. We will prove the the theorem by the second principle of mathematical induction.

Let $|G| = N$ and assume that the theorem holds for all Abelian groups of order $M < N$. Since $N > 2$, let p be a prime which divides N. Pick any $x \in G$, $x \neq e$. Then $\langle x \rangle = H$ has an order $m | N$, $m > 1$, and H is cyclic. Now consider any prime divisor q of m, ie $q | m$. Since H is cyclic, it has a element of order q. and $q | N = |G|$ as well. Now this q need not be equal to p. If $q = p$, we are done. So we consider the case $q \neq p$, and denote by $y \in \langle x \rangle$, the element which has order q, ie $|y| = q$.

Next consider the subgroup $K = \langle y \rangle$, $|K| = q$. Since G is Abelian (we use Abelian here!), K is a normal subgroup. Thus the factor group G/K exists.

Notice that

$$|G/K| = \frac{|G|}{|K|} = \frac{N}{q} < 1 \qquad (3)$$

and the prime p satisfies

$$p \,\Big|\, |G/K| = \frac{N}{q}, \quad \text{since } p|N \text{ and } p \neq q \qquad (4).$$

By the induction hypothesis applied to the group G/K (which is Abelian and has $|G/K| = M < N$ (in view of (3)), we see from (4) that G/K has an element of order p. So by Lemma 2, G must have an element of order p. This proves Theorem 9.5

Normal subgroups and kernels of homomophisms.

We now establish a fundamental link between homomophisms and normal subgroups.

<u>Theorem</u> (Corollary to Theorem 10.2, Chapter 10, p197)

Let G, G' be groups and $\phi: G \to G'$ a homomophism. Then $H = \ker(\phi)$ is a normal subgroup of G.

<u>Proof</u>: From our earlier discussion of homomophisms, we know that $H = \ker(\phi)$ is a subgroup of G. We now show that $\ker(\phi)$ is a <u>normal</u> subgroup.

Let e and e' denote the identity elements of G and G'. Then

$$H = \ker(\phi) = \{h \in G \mid \phi(h) = e'\}, \text{ and } \phi(e) = e'. \qquad (5).$$

Now consider <u>any</u> $h \in H$ and <u>any</u> $g \in G$. From the properties of homomophisms and from (5) we see that

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)e'\phi(g^{-1}) = \phi(g)\phi(g^{-1})$$
$$= \phi(gg^{-1}) = \phi(e) = e' \qquad (6)$$

and so $ghg^{-1} \in H = \ker(\phi)$. Since $ghg^{-1} \in H$ for any $h \in H$ and any $g \in G$, we have

$$gHg^{-1} \subseteq H, \quad \forall g \in G. \qquad (7)$$

Thus $H = \ker(\phi)$ is a normal subgroup of G by the normal subgroup test.

A question that arises now is whether all normal subgroups can be realized as kernels of homomorphism. The answer to this is YES :

Theorem 10.4 : Let G be a group and N a normal subgroup of G. Then N is the kernel of the homomorphism

$$\phi : G \longrightarrow G/N \tag{8}$$

given by

$$\phi(g) = gN, \quad \forall g \in G. \tag{9}$$

Proof: Since N is a normal subgroup, we know that the set of cosets of N, namely G/N, is a group under the operation

$$g_1 N g_2 N = g_1 g_2 N. \tag{10}$$

Note that the map ϕ in (8) and (9) is a homomorphism because of (10) that is, $\forall\, g_1, g_2 \in G$, we have

$$\phi(g_1 g_2) = g_1 g_2 N = g_1 N g_2 N = \phi(g_1)\phi(g_2). \tag{11}$$

The identity element in G/N is the coset $eN = N$. Thus the kernel of ϕ is

$$\ker(\phi) = \{ g \in G \,|\, \phi(g) = gN = eN = N \} \tag{12}$$

But

$$gN = N \iff g \in N \tag{13}$$

So by (12) and (13) we see that $\ker(\phi) = N$. Thus every $N \lhd G$ arises as the kernel of a homomorphism. This proves Theorem 10,4.

Terminology: Given a normal subgroup N of a group G, the homomorphism given in (8) and (9) is called the natural homomorphism induced by N.

Examples

I) Let $G = S_n$ and ϕ the homomorphism given by

$$\phi : S_n \to \{1, -1\} = G'$$

even permutations $\to 1$

odd permutations $\to -1$.

Here $e' = 1$. Thus $\mathrm{kerl}(\phi) = A_n \lhd S_n$.

II) Very important Example

Let $G = GL(n, \mathbb{R})$ = group of $n \times n$ invertible Matrices with real entries
= group of $n \times n$ matrices with real entries and with non-zero determinatnt.

Given $A, B \in G$, define A to be Similar to B, if $\exists\, C \in G$ such that

$$A = CBC^{-1} ; \qquad (14).$$

Note that similarity of matrices is an equivalence relation. Clearly A is similar to A with $C = I_n$ the identity (unit) matrix of dimension n.
Also A similar to B implies B similar to A. This is because

$$A = CBC^{-1} \Leftrightarrow B = C^{-1}AC = C^{-1}A(C^{-1})^{-1}.$$

Finally, if

$$A = CBC^{-1} \text{ and } B = EDE^{-1}, \text{ then } A = C(EDE^{-1})C^{-1} = (CE)D(CE)^{-1}$$

with $\det(CE) \neq 0$. Thus similarity of matrices is an equivalence relation.
Now consider the map

$$\phi : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^{\times} = \mathbb{R} - \{0\} = \text{multiplicative group of non-zero reals}$$

given by

$$A \longrightarrow \det(A) \quad , \quad \phi(A) = \det(A) \qquad (15)$$

Then ϕ is a homomorphism, ~~Hence~~ because

$$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B). \qquad (16).$$

~~Th~~ Since $1 = e'$ is the ~~the~~ identity of $\mathbb{R}^{\times} = G'$, the kernel of this homomorphism is

$$\ker(\phi) = \{ A \in GL(n, \mathbb{R}) \mid \det(A) = 1 \} = SL(n, \mathbb{R}). \qquad (17)$$

Since $SL(n, \mathbb{R})$ is $\ker(\phi)$, we deduce that $SL(n, \mathbb{R})$ is a normal subgroup of $GL(n, \mathbb{R})$.

Another way to realize this is to note that similar matrices A and B have the same determinant. That is if $A = CBC^{-1}$, then

$$\det(CBC^{-1}) = \det C \cdot \det B \cdot \det C^{-1} = \det C \cdot \det B \cdot \frac{1}{\det(C)} = \det B \quad (1$$

From (18) it follows that if $B \in SL(n, \mathbb{R})$ and $C \in GL(n, \mathbb{R})$, then

$$\det(CBC^{-1}) = \det(B) = 1 \Leftrightarrow CBC^{-1} \in SL(n, \mathbb{R}) \qquad (19)$$

Since (19) holds $\forall\, B \in SL(n, \mathbb{R})$ and $\forall\, C \in GL(n, \mathbb{R})$, we conclude that $SL(n, \mathbb{R}) \lhd GL(n, \mathbb{R})$.