PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 8

INSTRUCTOR: ARUNDHATHI KRISHNAN

9. Normal Subgroups

9.1. Definitions and Examples.

Definition 9.1.1. A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. This is denoted by $H \trianglelefteq G$.

Theorem 9.1.2. *A subgroup H of G is normal if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.*

Proof. If H is normal, then for each $x \in G$ and $h \in H$, $xh = h'x$ for some $h' \in H$. Hence $xhx^{-1} = h' \in H$, so that $xHx^{-1} \subseteq H$.

For the converse, suppose $xHx^{-1} \subseteq H$ for all $x \in G$. Then for each $h \in H$, there exists $h' \in H$ such that $xhx^{-1} = h'$, so that $xh = h'x$ and $xH \subseteq Hx$. On the other hand, as $x^{-1} \in G$, for each $h \in H$, there exists $h'' \in H$ such that $x^{-1}hx = h''$, so that $hx = xh''$ and $Hx \subseteq xH$. □

Remark 9.1.3.

(i) Every subgroup of an Abelian group is normal.
(ii) The center $Z(G)$ of a group is normal (verify!).
(iii) The normalizer $N(H)$ of a subgroup H of G is defined as

$$N(H) = \{x \in G \mid xHx^{-1} = H\}.$$

We have seen (in Assignment 1) that $N(H)$ is a subgroup of G. It is immediate from the definition of $N(H)$ that H is a normal subgroup of $N(H)$.
(iv) The alternating group A_n of even permutations is a normal subgroup of S_n for each n.
(v) Every subgroup of D_n consisting only of rotations is normal. To see this, note that $sr = r^{-1}s$ for every rotation r and reflection s, and that rotations commute.
(vi) If a group G has a unique subgroup H of some finite order, then H is normal in G. To see this, observe that for any $g \in G$, gHg^{-1} is a subgroup of G and $\left| gHg^{-1} \right| = |H|$.
(vii) The group $SL(2, \mathbb{R})$ is a normal subgroup of $GL(2, \mathbb{R})$.

9.2. Quotient Groups.

One of the primary reasons normal subgroups are of interest is that they can be used to create new groups. This is because the set of left (or right) cosets of a normal subgroup H in G is itself a group.

Theorem 9.2.1. *Let G be a group and let H be a normal subgroup of G. The set of all (left) cosets of H in G denoted by $G/H := \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.*

Proof. We first show that the operation is well-defined. Suppose $aH = a'H$ and $bH = b'H$. Then there exist $h_1, h_2 \in H$ such that $a' = ah_1$ and $b' = bh_2$, so that

$$\begin{aligned} a'b'H &= ah_1bh_2H = ah_1bH \\ &= ah_1Hb \ \text{ as } H \text{ is normal} \\ &= aHb = abH \ \text{ as } H \text{ is normal.} \end{aligned}$$

Clearly eH is the identity and $a^{-1}H$ is in the inverse of aH for each $a \in G$. Finally, associativity follows because for $a, b, c \in G$, $(aHbH)cH = (abH)(cH) = (ab)cH = a(bc)H = aH(bcH) = aH(bHcH)$. □

Actually, for the above group operation to be well-defined, H *must* be a normal subgroup of G. To see this note that for any $h \in H$, $hH = eH = H$. Hence for $a \in G$, $eHaH = eaH = aH$ is the same as $hHaH = haH$, so that $aH = haH$ for every $h \in H$. This gives by part (vi) of Lemma 7.1.3 that $a^{-1}ha \in H$, so we have that $a^{-1}Ha \subseteq H$ for every $a \in G$. This means that H is normal.

Theorem 9.2.1 allows us to define the following group.

Definition 9.2.2. Let H be a normal subgroup of a group G. Then the group G/H is called the quotient group of G by H.

Clearly, the order of the quotient group G/H is the number of left cosets of H in G, which is the index of H in G, given by $|\,G : H\,|$. If the order of G is finite, and H is normal, then

$$\left|\, G/H \,\right| = \frac{|\,G\,|}{|\,H\,|}. \tag{1}$$

Remark 9.2.3. Note that for a normal subgroup H of G, and $g \in G$, $|\,gH\,|$ can denote both the order of the coset gH in the quotient group G/H and the cardinality of the coset gH, and these two numbers need not be equal. It will generally be clear from the context what we mean!

Example 9.2.4.

(i) Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$. Then $\mathbb{Z}/4\mathbb{Z}$ consists of the left cosets of $4\mathbb{Z}$ in $\mathbb{Z}$, given by

$$\begin{aligned} 0 + 4\mathbb{Z} &= 4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}, \\ 1 + 4\mathbb{Z} &= \{1, 5, 9, \ldots; -3, -7, -11, \ldots\}, \\ 2 + 4\mathbb{Z} &= \{2, 6, 10, \ldots; -2, -6, -10, \ldots\}, \\ 3 + 4\mathbb{Z} &= \{3, 7, 11, \ldots; -1, -5, -9, \ldots\}. \end{aligned}$$

We next write the "multiplication table" for $\mathbb{Z}/4\mathbb{Z}$ (keep in mind that the operation in $\mathbb{Z}$ is addition!).

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

It follows then that $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$, and of course, the order of the quotient group is 4.

It is not hard to show that for any $n \in \mathbb{N}$, taking $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(ii) Consider the subgroup $K = \{r_0, r_2\}$ of the dihedral group D_4. We have already seen in part (iii) of Example 7.1.2 that $r_0K = r_2K, r_1K = r_3K, s_0K = s_2K$ and $s_1K = s_3K$. K is a normal subgroup of D_4 and the quotient group ${}^{D_4}\!/_K = \{K, r_1K, s_0K, s_1K\}$ with multiplication table:

	K	r_1K	s_0K	s_1K
K	K	r_1K	s_0K	s_1K
r_1K	r_1K	K	s_1K	s_0K
s_0K	s_0K	s_1K	K	r_1K
s_1K	s_1K	s_0K	r_1K	K

This table can be written as follows:

	r_0	r_2	r_1	r_3	s_0	s_2	s_1	s_3
r_0	r_0	r_2	r_1	r_3	s_0	s_2	s_1	s_3
r_2	r_2	r_0	r_3	r_1	s_2	s_0	s_3	s_1
r_1	r_1	r_3	r_2	r_0	s_1	s_3	s_2	s_0
r_3	r_3	r_1	r_0	r_3	s_3	s_1	s_0	s_2
s_0	s_0	s_2	s_3	s_1	r_0	r_2	r_3	r_1
s_2	s_2	s_0	s_1	s_3	r_2	r_0	r_1	r_3
s_1	s_1	s_3	s_0	s_2	r_1	r_3	r_0	r_2
s_3	s_3	s_1	s_2	s_0	r_3	r_1	r_2	r_0

The above table is simply the multiplication table of D_4 but arranged in a way that corresponds to the multiplication table of ${}^{D_4}\!/_K$. In Gallian's words, we see that the formation of a quotient group causes a systematic collapse of the elements of G. That is, all the elements in the coset of H containing a reduce to a single element aH in ${}^{G}\!/_H$.

9.3. **Applications of Quotient Groups.** Quotient groups are useful as they often give useful information about the group itself. Moreover, if the group is finite, then the order of a quotient group is smaller than that of the group itself, and this can be handy in induction arguments as will be illustrated in Cauchy's Theorem 9.3.4 below.

We first consider an example.

Example 9.3.1. We have already seen that the alternating group A_4 has no subgroups of order 6 in Remark 7.2.8. We will give another proof using quotient groups.

Suppose H is a subgroup of A_4 of order 6. Our first claim is that H is a normal subgroup. In fact, we show that for any group G, a subgroup H with index 2 must be normal.

To see this, let $a \in G$. If $a \in H$, then of course $aH = H = Ha$. On the other hand, if $a \notin H$, then aH and Ha are both the sets of elements of G that do not belong to H, hence they are equal to each other. Hence H is normal.

We can thus consider the quotient group ${}^{A_4}\!/_H$ which must have order 2. Hence, for every $\alpha \in A_4$, $\alpha^2 H = (\alpha H)^2 = H$ so that $\alpha^2 \in H$ for each $\alpha \in A_4$. But its can be verified that A_4 has 9 distinct elements of the form α^2, whereas H was assumed to have order 6. Hence, we arrive at a contradiction, and there can be no subgroups of A_4 of order 6.

Theorem 9.3.2. *Let G be a group and $Z(G)$ be the center of G. If ${}^{G}\!/_{Z(G)}$ is cyclic, then G is Abelian.*

Proof. G is Abelian if and only if $G = Z(G)$. We will show that $G/Z(G) = \{Z(G)\}$ and this implies that $G = Z(G)$.

By the hypothesis of cyclicity, $G/Z(G) = \langle gZ(G)\rangle$ for some $g \in G$. Let $a \in G$. Then $aZ(G) = (gZ(G))^i = g^iZ(G)$ for some $i \in \mathbb{Z}$. Hence $a = g^iz$ for some $z \in Z(G)$. As $z, g \in C(g)$ (where $C(g)$ is the centralizer of g which is a subgroup), we also have $a \in C(g)$. Hence $ag = ga$. But the element a was chosen arbitrarily, hence g commutes with a for all $a \in G$, that is, $g \in Z(G)$, so that $gZ(G) = Z(G)$ and $G/Z(G) = \{Z(G)\}$.

□

Actually, the above proof shows that if G/H is cyclic for any subgroup H of $Z(G)$, then G is Abelian.

A consequence of Theorem 9.3.2 is that if G is not Abelian, then $G/Z(G)$ is not cyclic. In particular, suppose G has order pq, where p and q are primes. Suppose $e \neq a \in Z(G)$, then $|\,Z(G)\,|$ is either p or q by Lagrange's theorem. By another application of Lagrange's theorem, this means that $\left|G/Z(G)\right|$ is q or p, so that $G/Z(G)$ is cyclic (see Corollary 7.2.5). Hence G must be Abelian or $Z(G) = \{e\}$.

Theorem 9.3.3. *For any group G, $G/Z(G) \cong \mathrm{Inn}(G)$*

Proof. For $g \in G$, define $T(gZ(G)) := \varphi_g$, where φ_g is the inner automorphism given by $\varphi_g(x) = gxg^{-1}$, $\forall x \in G$. We will show that T is a well-defined isomorphism.

We have $gZ(G) = hZ(G)$ if and only if $h^{-1}g \in Z(G)$. Now, for each $x \in G$, $\varphi_g(x) = \varphi_h(x)$ if and only if $gxg^{-1} = hxh^{-1}$ if and only if $h^{-1}gx = xh^{-1}g$ for each $x \in G$ which is true if and only if $h^{-1}g \in Z(G)$, that is, if and only if $gZ(G) = hZ(G)$. Hence φ is well-defined and one-to-one. T is clearly onto $\mathrm{Inn}(G)$ as every inner automorphism is of the form φ_g for some $g \in G$.

Finally, we observe that $\varphi_g\varphi_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}(x)$ for each $x \in G$. Hence $T(gZ(G)hZ(G)) = T(ghZ(G)) = \varphi_{gh} = \varphi_g\varphi_h = T(gZ(G))T(hZ(G))$, so that T is a group homomorphism, and indeed, an isomorphism. □

Theorem 9.3.4 (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.*

Proof. The proof is by induction on $|\,G\,|$. Suppose $|\,G\,| = 2$. Then $G = \{e, a\}$ and a must have order 2.

Suppose the result is true for all Abelian groups with order less than $|\,G\,|$. Suppose x is some element of G with order $m > 1$. Then $m = qn$ for some prime q, so that $|\,x^n\,| = q$. This implies that G must have elements of prime order. Now, if $q = p$ we are done. Suppose $q \neq p$ and let $\overline{G} = G/\langle x^n\rangle$. Then $\overline{G}$ is Abelian as it is a quotient of an Abelian group. Further, as $|\,\overline{G}\,| = \frac{|G|}{q}$ and $q \neq p$, the prime p divides $|\,\overline{G}\,|$. As $|\,\overline{G}\,| < |\,G\,|$, by the induction hypothesis, there exists $y \in G$ such that the order of the coset $y\langle x^n\rangle$ is p.

Now $y^p\langle x^n\rangle = (y\langle x^n\rangle)^p = \langle x^n\rangle$. Hence $y^p \in \langle x^n\rangle$. If $y^p = e$, we are done. Otherwise as $\langle x^n\rangle$ has order q, $(y^p)^q = e = (y^q)^p$, so the element y^q has order p. □

9.4. **Connection to Direct Products.** Last week we showed that the internal direct product of subgroups of a group is isomorphic to their external direct product. We will consider some consequences of this. One strength of the external direct product is that its order is simply the product of the orders of the constituent groups.

Theorem 9.4.1. *Every group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Proof. Let $|\,G\,| = p^2$. If G has an element of order p^2, then G is cyclic and hence isomorphic to $\mathbb{Z}_{p^2}$. If not, then every non-identity element of G must have order p. We claim that for each $a \in G \setminus \{e\}$, the subgroup $\langle a \rangle$ is normal. Suppose it is not normal, then there exists $b \in G$ with $bab^{-1} \notin \langle a \rangle$. Then $\langle a \rangle$ and $\langle bab^{-1} \rangle$ are distinct subgroups of order p. Since $\langle a \rangle \cap \langle bab^{-1} \rangle$ is a subgroup of both groups, it must be the trivial subgroup $\{e\}$. This gives us that the distinct left cosets of $\langle bab^{-1} \rangle$ in G are $\langle bab^{-1} \rangle, a\langle bab^{-1} \rangle, a^2\langle bab^{-1} \rangle, \ldots, a^{p-1}\langle bab^{-1} \rangle$. The element b^{-1} must belong to one of these cosets, that is, $b^{-1} = a^i(bab^{-1})^j = a^iba^jb^{-1}$ for some integers i and j. But this implies that $a^iba^j = e$ which gives that $b = a^{-i-j} \in \langle a \rangle$, a contradiction as $bab^{-1} \notin \langle a \rangle$. Hence $\langle a \rangle$ is normal.

This means that for $x \neq y \in G$, both of order p, $\langle x \rangle \times \langle y \rangle$ is isomorphic to $\langle x \rangle \oplus \langle y \rangle$, and hence is a subgroup of G of order p^2. This means that $G = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, as promised. □

An immediate consequence of Theorem 9.4.1 is the following.

Corollary 9.4.2. *If $|\,G\,| = p^2$ where p is a prime, then G is Abelian.*

References

[1] Chapters 8, 9. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.