MA1057: INTRODUCTION TO ABSTRACT ALGEBRA NORMAL SUBGROUPS AND HOMOMORPHISMS

LECTURER: ARUNDHATHI KRISHNAN

3. Normal Subgroups and Homomorphisms

3.1. Cosets.

Definition 3.1.1. Let G be a group and H be a subgroup of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH and is called the left coset of H in G containing a. Similarly, Ha denotes the set $\{ha \mid h \in H\}$ and is called the right coset of H in G containing a.

Notation 3.1.2. The set of all (left) cosets of H in G denoted by ${}^{G}\!/_{H} := \{aH \mid a \in G\}$ and is called the quotient of the group G by H.

Example 3.1.3.

(i) Let $G = S_3, H = \{(1), (1\,3)\}$. The left cosets of H in S_3 are:

$$\begin{aligned}
(1)H &= H \\
(1\,2)H &= \{(1\,2)(1), (1\,2)(1\,3)\} = \{(1\,2), (1\,3\,2)\} \\
(1\,3\,2)H &= \{(1\,3\,2)(1), (1\,3\,2)(1\,3)\} = \{(1\,3\,2), (1\,2)\} = (1\,2)H \\
(1\,3)H &= \{(1\,3), (1\,3)(1\,3)\} = \{(1\,3), (1)\} = H \\
(2\,3)H &= \{(2\,3), (2\,3)(1\,3)\} = \{(2\,3), (1\,2\,3)\} \\
(1\,2\,3)H &= \{(1\,2\,3), (1\,2\,3)(1\,3)\} = \{(1\,2\,3), (2\,3)\} = (2\,3)H.
\end{aligned}$$

Hence ${}^{G}\!/_{H} = \{H, (1\,2)H, (2\,3)H\}$. So the quotient of G by H has 3 elements (each of these elements is a set).

(ii) Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. The (left and right) cosets of H in $\mathbb{Z}$ are:

$$\begin{aligned}
0 + H &= \{3z \mid z \in \mathbb{Z}\} = [0] = H + 0 \\
1 + H &= \{3z + 1 \mid z \in \mathbb{Z}\} = [1] = H + 1 \\
2 + H &= \{3z + 2 \mid z \in \mathbb{Z}\} = [2] = H + 2,
\end{aligned}$$

where $[0], [1], [2]$ are the congruence classes in $\mathbb{Z}_3$ that we encountered in Subsection 2.8. Hence ${}^{G}\!/_{H} = \{H, 1 + H, 2 + H\} = \{[0], [1], [2]\} = \mathbb{Z}_3$.

(iii) Let $G = D_4$ be the dihedral group and $H = \{r_0, r_1, r_2, r_3\}$. The cosets of H in D_4 are:

$$\begin{aligned}
r_0H &= \{r_0, r_1, r_2, r_3\} = H = r_1H = r_2H = r_3H \\
s_0H &= \{s_0, s_1, s_2, s_3\} = s_1H = s_2H = s_3H
\end{aligned}$$

Hence ${}^{G}\!/_{H} = \{H, s_0H\}$.

Remark 3.1.4.

- Cosets are not subgroups except for the coset containing the identity.

- Cosets of a subgroup H corresponding to different elements $a, b \in G$ can be the same. That is, it may happen that $aH = bH$ even if $a \neq b$.

Lemma 3.1.5. *Let H be a subgroup of G and let $a, b \in G$. Then*

(i) Either $aH = bH$ or $aH \cap bH = \emptyset$.
(ii) $aH = bH \iff a^{-1}b \in H$.
(iii) $|aH| = |bH|$ (that is, the cardinalities of all cosets of H are the same).

Proof.

(i) Suppose $x \in aH \cap bH$. Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. This in turn implies that $ah = b(h_2h_1^{-1}h) \in bH$ for all $h \in H$. Similarly, $bh = a(h_1h_2^{-1}h) \in aH$ for all $h \in H$. This implies that if $aH \cap bH \neq \emptyset$, then $aH = bH$.
(ii) $aH = bH$ if and only if for each $h \in H$, there exists $h', h'' \in H$ such that $ah = bh'$ and $bh = ah''$. This in turn is true if and only $a^{-1}b = h(h')^{-1} \in H$, or $a^{-1}b = h''h^{-1} \in H$.
(iii) The map $ah \mapsto bh$ from aH to bH is one-to-one and onto, and hence the two sets have the same cardinality.

□

3.2. **Lagrange's Theorem.**

Theorem 3.2.1. *If G is a finite group and H is a subgroup of G, then $|\,H\,|$ divides $|\,G\,|$. The number of distinct left cosets of H in G is $\frac{|\,G\,|}{|\,H\,|}$.*

Proof. Let $a_1H, \ldots, a_rH$ denote the distinct left cosets of H in G (there are only finitely many because G is finite). Then for each $a \in G$, $aH = a_iH$ for some i, and hence $a \in aH = a_iH$. This means that each $a \in G$ belongs to a coset a_iH and so $G = a_1H \cup \ldots \cup a_rH$. This union is disjoint by part (i) of Lemma 3.1.5, hence $|\,G\,| = |\,a_1H\,| + \cdots + |\,a_rH\,| = r\,|\,H\,|$ (by part (iii) of Lemma 3.1.5). Hence $|\,H\,|$ divides $|\,G\,|$ and further, $\frac{|\,G\,|}{|\,H\,|}$ is equal to the number of left cosets of H in G.

□

Example 3.2.2. Consider (i) of Example 3.1.3. The group $G = S_3$ can be partitioned into the three cosets of $H = \{(1), (1\,3)\}$ in G thus:

$$S_3 = H \sqcup (1\,2)H \sqcup (2\,3)H.$$

The number of cosets of H in G is $\frac{|S_3|}{|H|} = \frac{6}{2} = 3$.

Another example would be to consider the subgroup $K = A_3$ and write down its cosets in $G = S_3$. We would then get (verify!)

$$S_3 = A_3 \sqcup (1\,2)A_3 = \{\text{even permutations}\} \sqcup \{\text{odd permutations}\}$$

The number of cosets of K in G is $\frac{|S_3|}{|A_3|} = \frac{6}{3} = 2$.

Definition 3.2.3. The index of a subgroup H in G is the number of distinct left cosets of H in G, denoted by $|\,G : H\,|$.

A straightforward corollary of Lagrange's Theorem 3.2.1 is the following.

Corollary 3.2.4. *If G is a finite group and H is a subgroup of G, then $|\,G : H\,| = \frac{|\,G\,|}{|\,H\,|}$.*

Definition 3.2.5. Let G be a group and $a \in G$. Then the *order* of the element a is defined as the smallest positive integer m such that $a^m = e$, the identity element of the group. If no such positive integer exists, then the element is said to be of *infinite order*.

Proposition 3.2.6. *Let G be a group and $a \in G$. Then $|\,a\,| = |\,\langle a \rangle\,|$.*

Proof. If a has finite order $m \in \mathbb{N}$, then it can be seen that $\langle a \rangle = \{e, a, \ldots, a^{m-1}\}$, which clearly has m elements. On the other hand, if a is of infinite order, then $a^j \neq a^i$ for distinct i and j in $\mathbb{Z}$. Hence the group $\langle a \rangle = \{e, a, a^2, \ldots,\}$ is of infinite order. $\square$

Corollary 3.2.7. *In a finite group, the order of each element of the group divides the order of the group.*

Proof. Let G be a finite group and $a \in G$. Then $\langle a \rangle$, the cyclic subgroup generated by a, is a subgroup of G, hence $|\,a\,| = |\,\langle a \rangle\,|$ divides the order of G. $\square$

Corollary 3.2.8. *Let G be a finite group and let $a \in G$. Then $a^{|\,G\,|} = e$.*

Proof. By Corollary 3.2.7, there exists $n \in \mathbb{N}$ such that $n\,|\,a\,| = |\,G\,|$. Hence $a^{|\,G\,|} = a^{n|\,a\,|} = e$. $\square$

Exercise 3.2.9. A group of prime order is cyclic. (Hint: Let G be a group of prime order p and let $a \in G$, $a \neq e$. Then the order of the cyclic subgroup $\langle a \rangle$ divides p.)

3.3. **Normal subgroups.** Let G be a group and H be a subgroup of G. Consider cosets aH and bH in the quotient ${}^{G}\!/_{H}$. Can we define a binary operation on them to obtain a new coset, say $(ab)H$? For this binary operation to be well-defined, we would require $(ab)H = (a'b')H$ whenever $aH = a'H$ and $bH = b'H$.

Consider for example, $G = S_3$ and $H = \{(1), (1\,3)\}$ as in (i) of 3.1.3. Then

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

and

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

But

$$((1\,2)(2\,3))\,H = (1\,2\,3)H \neq H = ((1\,3\,2)(1\,2\,3))\,H.$$

It turns out that the property of the subgroup H we require for this binary operation on (left) cosets to be satisfied is the following:

$$aH = Ha, \; \forall a \in A.$$

Definition 3.3.1. 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 $H \trianglelefteq G$.

Proposition 3.3.2. *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 $a \in G$ and $h \in H$, 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 $Hx \subseteq xH$. $\square$

Proposition 3.3.3. *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

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

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

Definition 3.3.4. Let H be a normal subgroup of a group G. Then the group ${}^{G}\!/_{H}$ is called the quotient group of G by H.

An element of the quotient group ${}^{G}\!/_{H}$, that is, a coset aH is sometimes written as $[a]$. Indeed, $a \sim b$ if and only if $aH = bH$ gives an equivalence relation on the group G, and the left cosets are precisely the equivalence classes for this relation.

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, $|\, G : H \,|$. If the order of G is finite, and H is normal, then as a consequence of Lagrange's Theorem 3.2.1, the order of the quotient group ${}^{G}\!/_{H}$ is given by

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

Exercise 3.3.5. Show that for every $n \geq 2$, the subgroup of even permutations A_n is a normal subgroup of the symmetric group S_n. Also find the cardinality of the quotient group ${}^{S_n}\!/_{A_n}$.

3.4. Group Homomorphisms.

Definition 3.4.1. A homomorphism φ from a group G to a group G' is a mapping from G to G' such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

Definition 3.4.2. A group homomorphism which is also bijective is called a group isomorphism. If there exists a group isomoprhism from G onto G', we say that the groups G and G' are isomorphic. This is denoted by

$$G \cong G'.$$

Proposition 3.4.3. *Let $\varphi : G \to G'$ be a group homomorphism. Then the following are true:*

(i) $\varphi(e_G) = e_{G'}$, where e_G and $e_{G'}$ denote the identity elements of G and G' respectively.
(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$, where x^{-1} is the inverse element of x in G and $\varphi(x)^{-1}$ is the inverse element of $\varphi(x)$ in G' for each $x \in G$.

Proof.

(i) By the group homomorphism property, we have $\varphi(e_G) = \varphi(e_Ge_G) = \varphi(e_G)\varphi(e_G)$. By cancellativity in the group G', we get $\varphi(e_G) = e_{G'}$.
(ii) By the group homomorphism property and part (i), we have $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_G) = e_{G'}$. Similarly, $\varphi(x^{-1})\varphi(x) = e_{G'}$. By the uniqueness of inverse elements, we get $\varphi(x^{-1}) = \varphi(x)^{-1}$.

☐

We now define an important set associated to a group homomorphism.

Definition 3.4.4. The kernel of a homomorphism $\varphi : G \to G'$ is the set $\{x \in G \mid \varphi(x) = e_{G'}\}$. It is denoted by $\operatorname{Ker}\varphi$.

Let us now consider some examples of homomorphisms and their kernels.

Example 3.4.5.

(i) $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined as $\varphi(x) = |\, x\,|$ is a homomorphism with $\operatorname{Ker}\varphi = \{1, -1\}$.

(ii) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(m) = m \mod n$ is a group homomorphism with $\operatorname{Ker}\varphi = n\mathbb{Z} = \langle n \rangle$.

(iii) Let $\varphi : G \to G'$ be a group isomorphism. Then $\operatorname{Ker}\varphi = \{e_G\}$.

(iv) $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ given by $\varphi(x) = x^2$ is a group homomorphism with $\operatorname{Ker}\varphi = \{1, -1\}$.

(v) Consider the sign function on the symmetric group given by

$$\operatorname{sign}(\alpha) = \prod_{\substack{i<j,\\ i,j\in\{1,\dots,n\}}} \frac{\alpha(i) - \alpha(j)}{i - j}.$$

Then $\{-1, +1\}$ is a group with respect to ordinary multiplication, and for $n \geq 2$, $\operatorname{sign} : (S_n, \circ) \to (\{-1, +1\}, \cdot)$ is a surjective (but not injective, in general) group homomorphism with

$$\operatorname{Ker}(\operatorname{sign}) = A_n.$$

(vi) Let G be the group of real numbers with addition and $\overline{G}$ be the set of positive real numbers with multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\varphi(x) = 2^x$. Let us check that φ is indeed an isomorphism. First $\varphi(x + y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$ so it is indeed a group homomorphism. Suppose $2^x = 2^y$, then $\log_2 2^x = \log_2 2^y$ so that $x = y$. Hence φ is injective. Finally, that it is surjective follows by noting that for every positive real number y, $x = \log_2(y)$ is the pre-image of y under φ.

(vii) $\varphi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined as $\varphi(A) = \det A$ is a group homomorphism with $\operatorname{Ker}\varphi = SL_2(\mathbb{R})$.

(viii) Let $\mathbb{R}[x]$ be the group of real polynomials in one variable, with pointwise addition. Then $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$ defined as $\varphi(f) = f'$ (the first derivative) is a group homomorphism with $\operatorname{Ker}\varphi$ given by the set of constant polynomials.

(ix) $\varphi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined as $\varphi(x) = x^2$ is not a homomorphism as $(x+y)^2 \neq x^2+y^2$ in general.

Proposition 3.4.6. *If H is a normal subgroup of a group G, then the mapping $G \to {}^{G}\!/\!_{H}$ given by*

$$a \mapsto aH$$

is a group homomorphism with kernel H.

Proof. We know by Proposition 3.3.3 that ${}^{G}\!/\!_{H}$ is a group with binary operation given by

$$(aH)(bH) := abH.$$

Hence if $a \mapsto aH$ and $b \mapsto bH$, it is clear that $ab \mapsto abH = (aH)(bH)$, so the given map is a group homomorphism.

The identity element of the quotient group is H, so the kernel of the map is given by

$$\{a \in G \mid aH = H = eH\} = \{a \in G \mid ae^{-1} = a \in H\} = H.$$

$\square$

The following result is an important one in group theory, often called the first isomorphism theorem.

Theorem 3.4.7 (The fundamental theorem of group homomorphisms)**.** *Let $\varphi : G \to G'$ be a group homomorphism. Then the following holds:*

(i) $\operatorname{Ker}\varphi$ *is a normal subgroup of* G*.*

(ii) $\varphi(G) = \{\varphi(g) \mid g \in G\}$ *is a subgroup of* G'*.*

(iii) The mapping ψ *from* $G/\operatorname{Ker}\varphi \to \varphi(G)$ *given by* $\psi(g\operatorname{Ker}\varphi) = \varphi(g)$ *is an isomorphism. That is,*

$$G/\operatorname{Ker}\varphi \cong \varphi(G).$$

Proof.

(i) We first show that $\operatorname{Ker}\varphi$ is a subgroup of G. Let us denote the identities of G and G' by e_G and $e_{G'}$ respectively. Note that $e_G \in \operatorname{Ker}\varphi$, so the kernel is non-empty. Further, if $x, y \in \operatorname{Ker}\varphi$, then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_{G'}$, so the kernel is a subgroup. To show that $\operatorname{Ker}\varphi$ is a normal subgroup, let $g \in G$ and $x \in \operatorname{Ker}\varphi$. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'}$, so $gxg^{-1} \in \operatorname{Ker}\varphi$. Hence $g(\operatorname{Ker}\varphi)g^{-1} \subseteq \operatorname{Ker}\varphi$ for every $g \in G$, and so $\operatorname{Ker}\varphi$ is a normal subgroup of G.

(ii) As $e_G \in G$, $e_{G'} = \varphi(e_G) \in \varphi(G)$, so $\varphi(G)$ is a non-empty subset of G'. Next, suppose $a = \varphi(x), b = \varphi(y) \in \varphi(G)$ for $x, y \in G$. Then $ab^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in \varphi(G)$ by the properties of group homomorphisms. Hence $\varphi(G)$ is a subgroup of G'.

(iii) We first show that $g\operatorname{Ker}\varphi = h\operatorname{Ker}\varphi$ if and only if $\varphi(g) = \varphi(h)$. Indeed,

$$\begin{aligned} g\operatorname{Ker}\varphi = h\operatorname{Ker}\varphi &\iff gh^{-1} \in \operatorname{Ker}\varphi \text{ (by part (ii) of Lemma 3.1.5)} \\ &\iff \varphi(gh^{-1}) = e_{G'} \\ &\iff \varphi(g) = \varphi(h). \end{aligned}$$

Hence we have that $\psi(g\operatorname{Ker}\varphi) = \psi(h\operatorname{Ker}\varphi)$ if and only if $\varphi(g) = \varphi(h)$, implying that ψ is well-defined and injective.

The mapping ψ is clearly surjective onto $\varphi(G)$. It remains to show that ψ is multiplicative. This is true as $\psi\left((g\operatorname{Ker}\varphi)(h\operatorname{Ker}\varphi)\right) = \psi(gh\operatorname{Ker}\varphi) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(g\operatorname{Ker}\varphi)\psi(h\operatorname{Ker}\varphi)$.

Altogether we have shown that ψ is a well-defined isomorphism between the quotient group $G/\operatorname{Ker}\varphi$ and the group $\varphi(G)$.

□

Example 3.4.8. Recall the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ in part (ii) of Example 3.4.5 given by $\varphi(m) = m \bmod n$. We saw that $\operatorname{Ker}\varphi = \langle n \rangle$. The map φ is clearly onto $\mathbb{Z}_n$ (verify!). Hence by Theorem 3.4.7 $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$.

As an exercise, consider other examples of homomorphisms from part (ii) of Example 3.4.5 and apply the fundamental theorem of group homomorphisms.

Note that Proposition 3.4.6 is a converse of Theorem 3.4.7 as it shows that every normal subgroup of a group G is the kernel of some homomorphism.

References

[1] Course notes of Anca Mustata, Lecturer, University College Cork.
[2] Chapters 7, 8, 9 and 10. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.