PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 9

INSTRUCTOR: ARUNDHATHI KRISHNAN

10. Group Homomorphisms

10.1. **Definitions and examples.** We have already studied isomorphisms in some detail. We now consider group homomorphisms and find that they also encode important information about groups. We build up to the first isomorphism theorem, a fundamental result in the study of any algebraic structures.

Definition 10.1.1. A homomorphism φ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

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

Definition 10.1.2. The kernel of a homomorphism $\varphi : G \to \overline{G}$ is the set $\{x \in G \mid \varphi(x) = e_{\overline{G}}\}$. It is denoted by $\operatorname{Ker}\varphi$.

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

Example 10.1.3.

(i) $\varphi : GL(2,\mathbb{R}) \to \mathbb{R}^*$ defined as $\varphi(A) = \det A$ is a group homomorphism with $\operatorname{Ker}\varphi = SL(2,\mathbb{R})$.
(ii) $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined as $\varphi(x) = |\,x\,|$ is a homomorphism with $\operatorname{Ker}\varphi = \{1, -1\}$.
(iii) 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.
(iv) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(m) = m \mod n$ is a group homomorphism with $\operatorname{Ker}\varphi = n\mathbb{Z} = \langle n \rangle$.
(v) $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ given by $\varphi(x) = x^2$ is a group homomorphism with $\operatorname{Ker}\varphi = \{1, -1\}$.
(vi) $\varphi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined as $\varphi(x) = x^2$ is not a homomorphism as $(x+y)^2 \neq x^2 + y^2$ in general.

We notice that the kernels of the homomorphisms given above are subgroups. This is not a coincidence as we will see in the following theorem.

10.2. **Properties of homomorphisms.**

Theorem 10.2.1. *Let $\varphi : G \to \overline{G}$ be a homomorphism, $g \in G$ and $e_G, e_{\overline{G}}$ be the identity elements of G and $\overline{G}$ respectively.*

(i) $\varphi(e_G) = e_{\overline{G}}$.
(ii) $\varphi(g^n) = [\varphi(g)]^n \ \forall n \in \mathbb{Z}$.
(iii) If $|\,g\,|$ is finite, then $|\,\varphi(g)\,|$ divides $|\,g\,|$.
(iv) $\operatorname{Ker}\varphi$ *is a subgroup of* G.
(v) $\varphi(a) = \varphi(b)$ *if and only if* $a \operatorname{Ker}\varphi = b \operatorname{Ker}\varphi$.

(vi) If $\varphi(g) = g'$, then $\varphi^{-1}(g') = \{x \in G \mid \varphi(x) = g'\} = g \operatorname{Ker} \varphi$.

Proof. The proofs of (i) and (ii) are just as in the corresponding results (Theorem 6.3.1) for isomorphisms- you can check that bijectivity was not used in the proof!

For (iii), note that if $g^n = e_G$, then $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_{\overline{G}}$ by parts (i) and (ii). For part (iv), note that $e_G \in \operatorname{Ker} \varphi$, so the kernel is non-empty. Further, if $x, y \in \operatorname{Ker} \varphi$, then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_{\overline{G}}$, so the kernel is a subgroup.

For part (v), note that $\varphi(a) = \varphi(b) \iff \varphi(a^{-1}b) = e_{\overline{G}} \iff a^{-1}b \in \operatorname{Ker} \varphi \iff a \operatorname{Ker} \varphi = b \operatorname{Ker} \varphi$.

Finally, for part (vi), note that if $h \in g \operatorname{Ker} \varphi$, then $h = gk$ for some $k \in \operatorname{Ker} \varphi$, so that $\varphi(h) = \varphi(gk) = \varphi(g)\varphi(k) = g'$, so $g \operatorname{Ker} \varphi \subseteq \varphi^{-1}(g')$. Suppose $x \in \varphi^{-1}(g')$ so that $\varphi(x) = g' = \varphi(g)$. By part (v), this implies that $x \operatorname{Ker} \varphi = g \operatorname{Ker} \varphi$, so that $x \in g \operatorname{Ker} \varphi$, and we have $\varphi^{-1}(g') \subseteq g \operatorname{Ker} \varphi$. □

Group homomorphisms preserve the binary operation structure of groups, hence it is natural that they preserve certain properties of groups as seen in the following theorem.

Theorem 10.2.2. *Let φ be a homomorphism from G to $\overline{G}$ and H be a subgroup of G. Then*

(i) $\varphi(H) = \{\varphi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
(ii) If H is cyclic, then $\varphi(H)$ is cyclic.
(iii) If H is Abelian, then $\varphi(H)$ is Abelian.
(iv) If H is a normal subgroup of G, then $\varphi(H)$ is a normal subgroup of $\varphi(G)$.
(v) If $|\operatorname{Ker} \varphi| = n$, then φ is an n-to-1 mapping from G onto $\varphi(G)$.
(vi) $|\varphi(H)|$ divides $|H|$.
(vii) If $\overline{K}$ is a subgroup of $\overline{G}$, then $\varphi^{-1}(\overline{K}) = \{k \in G \mid \varphi(k) \in \overline{K}\}$ is a subgroup of G.
(viii) If $\overline{K}$ is normal, then $\varphi^{-1}(\overline{K})$ is normal.
(ix) If φ is onto and $\operatorname{Ker} \varphi = \{e_G\}$, then φ is an isomorphism from G to $\overline{G}$.

Proof. The proofs of (i), (ii) and (iii) are just as in Theorem 6.3.2. For part (iv), let $\varphi(h) \in \varphi(H)$ and $\varphi(g) \in \varphi(G)$. Then $\varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1}) \in \varphi(H)$ as H is normal.

For part (v), note that for $g' = \varphi(g) \in \varphi(G)$, $\varphi^{-1}(g') = g \operatorname{Ker} \varphi$, so $\left|\varphi^{-1}(g')\right| = |g \operatorname{Ker} \varphi| = |\operatorname{Ker} \varphi| = n$.

For part (vi), set $\varphi_H = \varphi_{|H}$, the restriction of φ to the subgroup H. Then $\varphi_H : H \to \varphi(H)$ is an onto homomorphism. Suppose $|\operatorname{Ker} \varphi_H| = t$, then by part (v), φ_H is a t-to-1 mapping. Hence $t\,|\varphi(H)| = |H|$, so $|\varphi(H)|$ divides $|H|$.

For part (vii) first note that $e_G \in \varphi^{-1}(\overline{K})$, so it is non-empty. Suppose $x, y \in \varphi^{-1}(\overline{K})$. then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} \in \overline{K}$ as $\overline{K}$ is a subgroup. Hence $\varphi^{-1}(\overline{K})$ is a subgroup.

For part (viii), let $k \in \varphi^{-1}(\overline{K})$ and $x \in G$. Then $\varphi(xkx^{-1}) = \varphi(x)\varphi(k)\varphi(x)^{-1} \in \overline{K}$ as $\overline{K}$ is normal and $\varphi(k) \in \overline{K}$. Hence $xkx^{-1} \in \varphi^{-1}(\overline{K})$.

Part (ix) clearly follows from part (v). □

An immediate consequence of (vii) and (viii) of Theorem 10.2.2 is the following important result.

Corollary 10.2.3. *Let $\varphi : G \to \overline{G}$ be a group homomorphism. Then $\operatorname{Ker} \varphi$ is a normal subgroup of G.*

Let us consider some applications of Theorems 10.2.1 and 10.2.2.

Example 10.2.4.

(i) Let $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ be given by $\varphi(x) = x^4$. Then $\operatorname{Ker}\varphi = \{1, -1, i, -i\}$ and φ is a 4-to-1 mapping. Then by (vi) of Theorem 10.2.1, $\varphi^{-1}(2) = \sqrt[4]{2}\operatorname{Ker}\varphi = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}$.

(ii) Consider $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ given by $\varphi(x) = 3x$. Then $\operatorname{Ker}\varphi = \{0, 4, 8\}$ and as $2 \in \varphi^{-1}(6)$, $\varphi^{-1}(6) = 2 + \operatorname{Ker}\varphi = \{2, 6, 10\}$. Also note that $|\,\varphi(2)\,| = |\,6\,| = 2$, which divides $6 = |\,2\,|$. Let $K = \{0, 6\}$. Then $\varphi^{-1}(K) = \{0, 2, 4, 6, 8, 10\}$ (which is a subgroup of $\mathbb{Z}_{12}$).

(iii) We determine all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$. Any homomorphism is completely determined by its action on the generator $1 \in \mathbb{Z}_{12}$. To be precise, if $\varphi(1) = a$, then $\varphi(x) = xa$. Now $|\,a\,| = |\,\varphi(1)\,|$ divides $|\,1\,| = 12$. We also have that $|\,a\,|$ divides 30. Hence $|\,a\,| = 1, 2, 3$ or 6. This gives that $a = 0$ (with order 1), 15 (with order 2), 10 or 20 (with order 3) or 5 or 25 (with order 6).

10.3. **First isomorphism theorem.** The following theorem is a fundamental result in abstract algebra that relates the structure of the kernel and the image of a homomorphism via a quotient group. It causes a systematic collapse of a group to a simpler but closely related group.

Theorem 10.3.1. *Let $\varphi : G \to \overline{G}$ be a group homomorphism. Then 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. We will show that ψ is a well-defined isomorphism. By Theorem 10.2.1, $g\operatorname{Ker}\varphi = h\operatorname{Ker}\varphi$ if and only if $\varphi(g) = \varphi(h)$, so ψ is well-defined and injective. It is clearly onto $\varphi(G)$. It remains to show that ψ is multiplicative. This is true as $\psi\left((g\operatorname{Ker}\varphi)(h\operatorname{Ker}\varphi)\right) = \psi(gh\operatorname{Ker}\varphi) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(g\operatorname{Ker}\varphi)\psi(h\operatorname{Ker}\varphi)$. □

Theorem 10.3.1 is illustrated by the following diagram:

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & \varphi(G) \\ & \searrow^{\gamma} & \uparrow{\scriptstyle \psi} \\ & & {}^{G}\!/_{\operatorname{Ker}\varphi} \end{array}$$

Here the map $\gamma : G \to {}^{G}\!/_{\operatorname{Ker}\varphi}$ given by $\gamma(g) = g\operatorname{Ker}\varphi$ is called the natural or canonical map from G onto ${}^{G}\!/_{\operatorname{Ker}\varphi}$ (verify that it is indeed onto). The relationship between the three maps in the figure is as follows:

$$\psi\gamma = \varphi.$$

The diagram is said to be *commutative* as taking the route from G to $\varphi(G)$ remains the same through the direct route (the right arrow φ) and the "longer route" (take the bottom-right arrow first and then the top arrow: γ followed by ψ).

Corollary 10.3.2. *If $\varphi : G \to \overline{G}$ is a homomorphism and $|\,G\,|$ is finite, then $|\,\varphi(G)\,|$ divides $|\,G\,|$.*

Proof. The result follows as $\frac{|\,G\,|}{|\operatorname{Ker}\varphi|} = \left|\, {}^{G}\!/_{\operatorname{Ker}\varphi} \,\right| = |\,\varphi(G)\,|$. □

We illustrate 10.3.1 with some examples.

Example 10.3.3.

(i) Consider $\varphi : D_4 \to D_4$ given by $\varphi(r_0) = \varphi(r_2) = r_0$, $\varphi(r_1) = \varphi(r_3) = s_0$, $\varphi(s_0) = \varphi(s_2) = r_2$, $\varphi(s_1) = \varphi(s_3) = s_2$. Then φ is a homomorphism with $\operatorname{Ker}\varphi = \{r_0, r_2\}$. Now $\psi : {}^{D_4}\!/_{\operatorname{Ker}\varphi} \to \varphi(D_4) = \{r_0, r_2, s_0, s_2\}$ given by $\psi(r_0 \operatorname{Ker}\varphi) = r_0, \psi(r_1 \operatorname{Ker}\varphi) = s_0, \psi(s_0 \operatorname{Ker}\varphi) = r_2, \psi(s_1 \operatorname{Ker}\varphi) = s_2$ is an isomorphism.

(ii) Recall the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ in part (iv) of Example 10.1.3 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 10.3.1, ${}^{\mathbb{Z}}\!/_{\langle n \rangle} \cong \mathbb{Z}_n$.

(iii) Let H be a subgroup of G. Recall the subgroups $N(H) = \{x \in G \mid xHx^{-1} = H\}$ (the *normalizer* of H) and $C(H) = \{x \in G \mid xhx^{-1} = h \ \forall h \in H\}$ (the *centralizer* of H). Recall also that $C(H) \leq N(H)$. Define $\chi : N(H) \to \operatorname{Aut}(H)$ by $\chi(g) = \varphi_g$, the inner automorphism induced by g. Then χ is a homomorphism. To verify this, first note that for all $h \in H$, $\varphi_g(h) = ghg^{-1} \in H$ because $g \in N(H)$. Further, we have already seen that $\varphi_{gh} = \varphi_g\varphi_h$, so χ is a homomorphism. To find the kernel of χ, note that $\varphi_g = \varphi_e$ (the identity in $\operatorname{Aut}(H)$) if and only if $ghg^{-1} = ehe^{-1}$ for all $h \in H$, that is, $ghg^{-1} = h$ for all $h \in H$. This is precisely the criterion for $g \in C(H)$, so $\operatorname{Ker}\chi = C(H)$. Hence, by Theorem 10.3.1, ${}^{N(H)}\!/_{C(H)}$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$. This is sometimes called the ${}^{N}\!/_{C}$ theorem.

(iv) We illustrate an application of the N/C theorem. Let G be a group of order 35. We will show that G is cyclic. Every non-identity element of G has either order $5, 7$ or 35. Now, not all elements can have order 5, as elements of order 5 appear in groups of 4 (as if x has order 5, so does x^2, x^3 and x^4) and 4 does not divide $35 - 1 = 34$. Similarly, all elements cannot have order 7 as these elements appear in groups of 6, which also does not divide 34. Hence G has both elements of order 7 and 5.

Hence G has a subgroup of order 7, say H. We claim that H is the only subgroup of order 7, for if $K \leq G$ with $|K| = 7$ and $K \neq H$, then $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{7 \times 7}{1} = 49$ which is impossible in a group of order 35 (Note: $|H \cap K| = 1$ as it cannot have order 7). Hence, for all $a \in G$, $aHa^{-1} = H$, so that $N(H) = G$. Now as $|H| = 7$, H is cyclic and thus Abelian. Hence $H \leq C(H)$. This implies that 7 divides the order of $C(H)$ and as $|C(H)|$ divides 35, either $|C(H)| = 7$ or $|C(H)| = 35$. In the first case, $\left| {}^{N(H)}\!/_{C(H)} \right| = \frac{35}{7} = 5$. But this quotient group must be isomorphic to a subgroup of $\operatorname{Aut}(\mathbb{Z}_7) \cong U(7)$ (Theorem 6.4.9) which has order 6, and of course, 5 does not divide 6. On the other hand, if $C(H) = G$, then taking $x = hk$ with h a non-identity element of H (and hence of order 7) and $k \in G$ with order 5 gives $|x| = |hk| = 35$ as h and k commute and h and k have orders 7 and 5 respectively.

We end the lecture with an important result which gives the converse of the statement "the kernel of a homomorphism is a normal subgroup".

Theorem 10.3.4. *Every normal subgroup N of a group G is the kernel of a homomorphism of G. Namely, $N = \operatorname{Ker}\gamma$ for $\gamma : G \to {}^{G}\!/_{N}$ given by $\gamma(g) = gN$.*

Proof. Clearly, γ is well-defined. It is multiplicative as $\gamma(gh) = (gh)N = gNhN = \gamma(g)\gamma(h)$ for $g, h \in G$. The kernel of γ is given by $\{g \in G \mid gN = N\}$ which is precisely equal to $\{g \in G \mid g \in N\} = N$. □

References

[1] Chapter 10. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.