Chapter 7

Kernels and quotients

Recall that homomorphism between groups $f : G \to Q$ is a map which preserves the operation and identity (which we denote by $\cdot$ and e). It need not be one to one. The failure to be one to one is easy to measure.

Definition 7.1. *Given a homomorphism between groups $f : G \to Q$, the kernel* $\ker f = \{g \in G \mid f(g) = e\}$.

Lemma 7.2. *A homomorphism is one to one if and only if* $\ker f = \{e\}$.

The proof will be given as an exercise. The kernel is a special kind of subgroup. It's likely that you already encountered this notion in linear algebra in the context of linear transformations. There it also called the kernel or sometimes the null space.

Definition 7.3. *A subgroup $H \subset G$ is called normal if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. The operation $h \mapsto ghg^{-1}$ is called conjugation of h by g. So normality of H means that it is closed under conjugation by elements of G.*

Proposition 7.4. *Suppose that $f : G \to Q$ is a homomorphism, then* $\ker f$ *is a normal subgroup.*

Proof. Let $h_1, h_2 \in H$ and $g \in G$. Then $f(h_1 h_2) = f(h_1)f(h_2) = e$, $f(h_1^{-1}) = e$, $f(gh_1g^{-1}) = f(g)f(g)^{-1} = e$. □

Here are some examples.

Example 7.5. *If G is abelian, then any subgroup is normal.*

Example 7.6. *In S_3, $H = \{I, (123), (321)\}$ is a normal subgroup. The subgroup $\{I, (12)\}$ is not normal because* (12) *is conjugate to* (13) *and* (23).

We want to prove that every normal subgroup arises as the kernel of a homomorphism. This involves the quotient construction. Given subsets $H_1, H_2 \subset G$ of a group, define their product by

$$H_1 H_2 = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}$$

Lemma 7.7. *If $H \subseteq G$ is normal, then the product of cosets satisfies $(g_1H)(g_2H) = (g_1g_2)H$.*

Proof. By definition, $(g_1H)(g_2H) = \{g_1h_1g_2h_2 \mid h_1, h_2 \in H\}$. Since H is normal, $h_3 = g_2^{-1}h_1g_2 \in H$. Therefore $g_1h_1g_2h_2 = g_1g_2h_3h_2 \in (g_1g_2)H$. This proves $(g_1H)(g_2H) \subseteq (g_1g_2)H$.

For the reverse inclusion $(g_1g_2)H \subseteq (g_1H)(g_2H)$, observe that if $h \in H$, then $g_1g_2h = (g_1e)(g_2h) \in (g_1H)(g_2H)$.

□

Theorem 7.8. *If $H \subseteq G$ is a normal subgroup, then G/H becomes a group with respect to the product defined above. The map $p(g) = gH$ is a homomorphism with kernel H.*

Proof. By the previous lemma, $(gH)(eH) = gH = (eH)(gH)$, $(gH)(g^{-1}H) = H = (g^{-1}H)(gH)$, and $(g_1H)(g_2Hg_3H) = g_1g_2g_3H = (g_1Hg_2H)(g_3H)$. So G/H is a group. Also $p(g_1g_2) = g_1g_2H = (g_1H)(g_2H) = p(g_1)(g_2)$, so p is a homomorphism. Furthermore, $\ker p = \{g \in G \mid gH = H\} = H$. □

When H is normal, we refer to G/H as the *quotient group*. Quotient groups often show up indirectly as follows.

Lemma 7.9. *Let $f : G \to H$ be a homomorphism with kernel $K = \ker f$. Then the image $f(G) = \{f(g) \mid g \in G\}$ is a subgroup isomorphic to G/K. In particular, H is isomorphic to G/K if f is onto.*

The proof will be given as an exercise. The quotient construction can be used to tie up some loose ends from earlier sections. Let n be a positive integer, and let $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. This is a subgroup. So we can form the quotient $\mathbb{Z}_n^{new} = \mathbb{Z}/n\mathbb{Z}$. The label "new" is temporary, and is there to distinguish it from $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Given an integer x, let $\bar{x} = x + n\mathbb{Z}$. In particular, $x \mapsto \overline{x}$ gives a map from $\mathbb{Z}_n \to \mathbb{Z}_n^{new}$. We leave it as an exercise to show this is a one to one correspondence, and that

$$\overline{x \oplus y} = \overline{x} + \overline{y}$$

where $+$ on the right is addition in the quotient group. Thus, we can conclude that the old and new versions of $\mathbb{Z}_n$ are isomorphic, and we will conflate the two. Recall, in fact, that we never fully completed the proof that the old $\mathbb{Z}_n$ was a group. Now we don't have to!

Normal subgroups can be used to break up complicated groups into simpler pieces. For example, in the exercises, we will see that the dihedral group D_n contains a cyclic subgroup C_n, which is normal and the quotient D_n/C_n is also cyclic. Here we look at the related example of the orthogonal group $O(2)$. This is the full symmetry group of the circle which includes rotations and reflection. The rotations form a subgroup $SO(2)$.

Proposition 7.10. *$SO(2)$ is a normal subgroup of $O(2)$.*

We give two proofs. The first, which uses determinants, gets to the point quickly. However, the second proof is also useful since it leads to the formula (7.1).

First Proof. We start with a standard result.

Theorem 7.11. *For any pair of 2×2 matrices A and B, $\det AB = \det A \det B$.*

Proof. A brute force calculation shows that

$$(a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21})$$

and

$$(a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_{11} + a_{22}b_{22})$$

both can be expanded to

$$a_{11}a_{22}b_{11}b_{22} - a_{11}a_{22}b_{12}b_{21} - a_{12}a_{21}b_{11}b_{22} + a_{12}a_{21}b_{12}b_{21}$$

□

Therefore $\det : O(2) \to \mathbb{R}^*$ is a homomorphism, where $\mathbb{R}^*$ denote the group of nonzero real numbers under multiplication. It follows that $SO(2)$ is the kernel. So it is normal. □

Second Proof. We have to show that $AR(\theta)A^{-1} \in SO(2)$ for any $A \in O(2)$. This is true when $A \in SO(2)$ because $SO(2)$ is a subgroup.

It remains to show that conjugating a rotation by a reflection is a rotation. In fact we will show that for any reflection A

$$AR(\theta)A^{-1} = R(-\theta) \tag{7.1}$$

First let A be the reflection $F = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ about the x-axis. Then an easy calculation shows that $FR(\theta)F^{-1} = FR(\theta)F = R(-\theta)$. Now assume that A is a general reflection. Then

$$A = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} = FR(-\phi)$$

So

$$AR(\theta)A^{-1} = FR(-\phi)R(\theta)R(\phi)F = R(-\theta)$$

as claimed. □

So now we have a normal subgroup $SO(2) \subset O(2)$ which we understand pretty well. What about the quotient $O(2)/SO(2)$. This can identified with the cyclic group $\{\pm 1\} \subset \mathbb{R}^*$ using the determinant.

7.12 Exercises

1. Prove lemma 7.2.

2. Determine the normal subgroups of S_3.

3. Prove lemma 7.9. (Hint: first prove that $f(G)$ is subgroup. Then that $\bar{f}(gH) = f(g)$ is a well defined function which gives an isomorphism $G/K \cong f(G)$.)

4. (a) Given a group G and a normal subgroup H. Let $S \subset G$ be a subset with the property that $S \cap gH$ has exactly one element for every $g \in G$. Show that the restriction of p gives a one to one correspondence $S \to G/H$.

   (b) Show that these conditions hold for $G = \mathbb{R}$, $H = 2\pi\mathbb{Z}$ and $S = [0, 2\pi)$.

5. Prove that $\mathbb{Z}_n$ is isomorphic to the quotient group $\mathbb{Z}/n\mathbb{Z}$ as claimed earlier.

6. Check that $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det A = 1\}$ is a normal subgroup of $GL_2(\mathbb{R})$.

7. In an earlier exercise in chapter , you showed that the set of upper triangular matrices
$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$
is a subgroup of $GL_2(\mathbb{R})$. Is it normal?

8. Let $H \subseteq G$ be a normal subgroup $f : G \to K$ be an onto homomorphism, prove that $f(H) = \{f(h) \mid h \in H\}$ is a normal subgroup. What if f is not onto?

9. Given a group G, its *center* $Z(G)$ is the set of elements c which satisfy $cg = gc$ for every $g \in G$.

   (a) Prove that the center is an abelian normal subgroup.

   (b) Does an abelian normal subgroup necessarily lie in the center? (Think about the dihedral group.)

10. Check that the center of S_n, when $n > 2$, is trivial in the sense that it consists of only the identity.