KERNELS AND QUOTIENTS

A hopelessly broad problem is:

Classify all groups.

A variant of the problem is:

Given a group, try to study it by breaking it into smaller pieces.

A group can arise, for example, as a *description* of solving a problem, so that decomposing the group gives a *process* to solve the problem. This was Galois's original idea.

1. Two Associate Kinds of Structure

Given a group G, we have learned about two associated group structures:

- Subgroups H of G.
- Homomorphic images $f(G)$ of G.

While the homomorphic image of a group somehow reflects some structure of the original group, the image is emphatically *not* a substructure. Indeed, it often fails to distinguish among some distinct elements of the group. For example,

- $|\ | : \mathbb{C}^\times \longrightarrow \mathbb{R}^+$ has positive real numbers as its output-values, taking many nonzero complex numbers to the same positive real number.
- $\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ has nonzero real numbers as its output-values, taking many different invertible matrices to the same number.
- Similarly, $\deg : k(X)^\times \longrightarrow \mathbb{Z}$ has integers as its output-values, with many different rational functions having the same degree.
- $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$ takes all even permutations to 1 and all odd permutations to -1.
- $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ takes all integers that leave remainder r upon division by n to the single equivalence class $r \bmod n$.

In each case,

The image-group gives a **coarse** *rendition of the structure of the* **entire** *original group, in contrast to how a subgroup gives the* **precise** *structure of* **part** *of the original group.*

Since subgroups and homomorphic images give incomplete descriptions of the original group in somehow-opposite ways, the natural question is,

In each case, is there a complementary structure?

2. The Complement of an Image

In the case of a homomorphic image $f(G)$ of G, there is indeed a complementary structure: it is the subgroup $\ker(f)$ of G. Specifically, we have a *short exact sequence*

$$1 \longrightarrow \ker(f) \longrightarrow G \longrightarrow f(G) \longrightarrow 1.$$

Here "1" denotes the trivial group, and *exact* means that the image of each map is the kernel of the next one. Of course, all of the maps are homomorphisms. Thus exactness at the first *joint* $\ker(f)$ says simply that the inclusion map $\ker(f) \longrightarrow G$ is injective: there is only one homomorphism from 1 to $\ker(f)$, taking the identity element of the trivial group to e_G; and we recall that a homomorphism is injective if and only if its kernel is trivial. Similarly, because there is only one homomorphism from $f(G)$ to 1, taking all of $f(G)$ to the identity element of the trivial group, exactness at the third joint $f(G)$ restates the fact that $f : G \longrightarrow f(G)$ is surjective.

In sum,

The complement of an image is a kernel subgroup.

3. The Complement of a Subgroup

By contrast, in the case of a subgroup H of G, there is not always a complementary structure. As discussed above, the complementary structure should be a group that somehow views all of H as a single element, and that bunches other collections of elements of G together into single elements as well.

For an example of a subgroup that has a complementary structure, take G to be the nonabelian group of order 6,

$$G = \{e, a, a^2, b, ab, a^2b\},$$

where as usual $a^3 = b^2 = e$ and $ba = a^2b$. (Incidentally, this group is yet another semidirect product like the homework problem and the parabolic matrix group from class.) Consider a subgroup

$$H = \{e, a, a^2\}.$$

View G as the symmetry group of the triangle, with a being counterclockwise rotation one-third of the way around and b being reflection through the vertical axis. Imagine the triangle painted red on its front and blue on its back. Then H is exactly the symmetries that preserve which color of the triangle we see, while the other three symmetries exchange which color we see. The obvious complementary structure to H in G is a group of two elements,

$$\{\text{moves that preserve color},\ \text{moves that exchange color}\} \approx \mathbb{Z}/2\mathbb{Z},$$

where the group operation is clear:

$$\begin{aligned}
\text{preserve} \circ \text{preserve} &= \text{preserve},\\
\text{preserve} \circ \text{reverse} &= \text{reverse},\\
\text{reverse} \circ \text{preserve} &= \text{reverse},\\
\text{reverse} \circ \text{reverse} &= \text{preserve}.
\end{aligned}$$

Equivalently, the complementary structure is a group each of whose two elements is a subset of G,

$$\big\{\{e, a, a^2\},\ \{b, ab, a^2b\}\big\} = \{H,\ Hb\},$$

and the operation is

$$H \cdot H = H, \quad H \cdot Hb = Hb, \quad Hb \cdot H = Hb, \quad Hb \cdot Hb = H.$$

For an example of a subgroup that does not have a complementary structure, again view the nonabelian group G of order 6 as the symmetry group of the triangle, and let N, W, and E (for *north*, *west*, and *east*) denote the three triangle vertices, with N the apex and W and E at either end of the base. Consider a subgroup of G,

$$H' = \{e, b\}.$$

This is the subgroup that fixes N. The obvious attempt at a complementary structure is

$$\{N, W, E\} = \{H', H'a, H'a^2\},$$

where W now denotes the moves that take N to W and similar for E. Since a takes N to W and a^2 takes N to E, the multiplication law in the complementary structure must be

$$W^2 = E.$$

But also a^2b takes N to W, while $(a^2b)^2 = a^2ba^2b = a^6b^2 = e$ leaves N in place. Thus the multiplication law in the complementary structure must also be

$$W^2 = N.$$

In sum, no multiplication law on $\{N, W, E\}$ is compatible with the original group, if we interpret N, W, and E as above.

Alternatively we might treat W as the moves that take W to N (rather than taking N to W as before), and similarly for E. Now we have

$$\{N, W, E\} = \{H', a^2H', aH'\}.$$

No multiplication structure works compatibly with G here either. But now we can begin to see why the first example, H, allows a complementary structure, while the second example, H', does not.

In the first example, the crucial point is that *the left-translate of H by b is also the right-translate*,

$$bH = \{b, ba, ba^2\} = \{b, a^2b, a^4b\} = \{b, ab, a^2b\} = Hb.$$

Thus we see that the calculations from before really are valid calculations rather than just heuristics, e.g.,

$$\begin{aligned} Hb \cdot H &= H \cdot bH = H \cdot Hb = Hb, \\ Hb \cdot Hb &= H \cdot bH \cdot b = H \cdot Hb \cdot b = H. \end{aligned}$$

(Here it may be worth a moment to convince oneself that $H \cdot H = H$ for any group H, where literally $H \cdot H = \{h \cdot h' : h, h' \in H\}$.) By contrast, in the second example we compute that the left-translates of H' are

$$\{H', aH', a^2H'\} = \big\{\{e, b\},\ \{a, ab\},\ \{a^2, a^2b\}\big\}$$

while the right-translates are

$$\{H', H'a, H'a^2\} = \big\{\{e, b\},\ \{a, ba\},\ \{a^2, ba^2\}\big\} = \big\{\{e, b\},\ \{a, a^2b\},\ \{a^2, ab\}\big\}.$$

And we see that the left-translates are not the right-translates.

This is the key point.

> *For the set of left-translates of a subgroup, or the set of right-translates of a subgroup, to have a group-structure compatible with the full group, the left-translates and its right-translates must be equal.*

Indeed, if G is a group and H is a subgroup such that $gH = Hg$ for all $g \in G$ then the product of two translates of H is

$$gH \cdot g'H = g \cdot Hg' \cdot H = g \cdot g'HH = gg'H.$$

The translates of a subgroup are called *cosets*.

Definition 3.1. *Let G be a group and let N be a subgroup. Then N is a* **normal** *subgroup if its left cosets and its right cosets are equal,*

$$gN = Ng \quad \textit{for all } g \in G.$$

An equivalent condition for a subgroup to be normal

$$gNg^{-1} = N \quad \text{for all } g \in G,$$

That is,

A normal subgroup is a subgroup whose normalizer is the full group.

And in hindsight, all of this was serendipitous: not only is the complement of an image a normal subgroup (because kernel subgroups are normal), but also the normal subgroups are the subgroups with complementary structures. Other equivalent conditions for a subgroup to be normal are

$$gNg^{-1} \subset N \quad \text{for all } g \in G,$$

or

$$gNg^{-1} \supset N \quad \text{for all } g \in G.$$

Now we formalize the complementary structure of a normal subgroup.

Definition 3.2. *Let G be a group and let N be a normal subgroup. The* **quotient** *group of G by N is the set of cosets,*

$$G/N = \{gN : g \in G\}$$

with multiplication rule

$$gN \cdot g'N = gg'N.$$

The quotient group is indeed a group. As with the particular quotient group $\mathbb{Z}/n\mathbb{Z}$ from the introductory unit on the integers, the immediate question is whether its operation *makes sense*. It does. Specifically, if

$$gN = \gamma N \quad \text{and} \quad g'N = \gamma' N$$

then

$$gg'N = gg'NN = gNg'N = \gamma N\gamma' N = \gamma\gamma' NN = \gamma\gamma' N.$$

Now the group laws for G/N follow immediately, e.g.,

$$\begin{aligned}(gN\, g'N)g''N = gg'N\, g''N &= (gg')g''N \\ &= g(g'g'')N = gN\, g'g''N = gN(g'N\, g''N).\end{aligned}$$

And similarly, N is the identity and $(gN)^{-1} = g^{-1}N$.

4. The Natural Projection

Recall that

Every kernel is a normal subgroup.

Now we want to show that conversely,

Every normal subgroup is a kernel.

So, let G be a group and let N be a normal subgroup. The map

$$\pi : G \longrightarrow G/N, \quad g \longmapsto gN$$

is a surjective homomorphism whose kernel is N. Thus we have a short exact sequence with left joint N as desired,

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1.$$

5. An Example to Consider

The alternating group on four letters,

$$\begin{aligned} A_4 = \{e,\ &(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3), \\ &(1\,2\,3),\ (1\,3\,2),\ (1\,2\,4),\ (1\,4\,2), \\ &(1\,3\,4),\ (1\,4\,3),\ (2\,3\,4),\ (2\,4\,3)\}, \end{aligned}$$

contains its *Klein four-subgroup*,

$$V = \{e,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}.$$

The exercise has two parts. First, viewing A_4 as the rotation group of the tetrahedron, find a geometric argument that V is a normal subgroup. It follows that the quotient space

$$A_4/V = \{\sigma V : \sigma \in A_4\},$$

whose coset-elements are worth writing out explicitly, carries the structure of the group of three elements (there is only one such group). For the second part of the exercise, what aspect of A_4 as the tetrahedral rotation group (i.e., what geometry of the rotations) is coarsely reflected in the structure of the three-element quotient group?