5 The Correspondence Theorem

5.1 Review

In the last lecture, we learned about cosets and some of their properties.

Definition 5.1
For a group G and a subgroup $H \leq G$, we define the **left coset** of a to be

$$aH := \{ah : h \in H\} \subseteq G.$$

The left cosets *partition*[22] G into equally sized sets. This provides a useful corollary about the structure of cosets within a group:

Corollary 5.2 (Counting Formula.)
Let $[G : H]$ be the number of left cosets of H, which is called the **index** of H in G. Then $|G| = |H|[G : H]$.

5.2 Lagrange's Theorem

Using cosets provides some additional information about groups.

Guiding Question
What are the possibilities for the structure of a group with order n?

From the Counting Formula, we immediately obtain Lagrange's Theorem as a corollary:

Theorem 5.3 (Lagrange's Theorem.)
For H a subgroup of G, $|H|$ is a divisor of $|G|$.

Several important corollaries follow as a result.

Corollary 5.4
The order of $x \in G$ is $|\langle x\rangle|$. Since the order of any subgroup divides the order of $|G|$, $\mathrm{ord}(x)$ also divides $|G|$.

Corollary 5.5
Any group $|G|$ with prime order p is a cyclic group.

Proof. Take an element $e \neq x \in G$. Since the order of $x \in G$ divides p, and p is prime, $\mathrm{ord}(x) = p$. Then each x^i is distinct for $0 \leq i \leq p - 1$, and since there are only p elements in G, the entire group G is $\langle x\rangle$, the cyclic group generated by x. □

Our result shows that any group of prime order is a cyclic group. In particular, the integers modulo p, $\mathbb{Z}_p$, form a cyclic group of prime order; that is, any group of prime order p is isomorphic to $\mathbb{Z}_p$.

5.3 Results of the Counting Formula

Using Lagrange's Theorem narrows down the possibilities for subgroups.

[22] A partition of a set S is a subdivision of the entire set into disjoint subsets.

Example 5.6 (Groups of order 4.)
What are the possibilities (up to isomorphism) for G if $|G| = 4$?

First, e must be an element of G. Next, consider the other three elements of G. Each of these must have either order 2 or order 4, since those are the divisors of $|G| = 4$. Then there are two possibilities.

- **Case 1.** There exists an element $x \in G$ such that $\mathrm{ord}(x) = 4$. Then we know that $e \neq x \neq x^2 \neq x^3$, and since $|G| = 4$, these are all the elements of G. (The power x^4 is e again.) So G is generated by x, and it is the cyclic group $\langle x \rangle$ of size 4, and must be isomorphic to $\mathbb{Z}_4$[a].
- **Case 2.** All elements of G have order 2. Then, we can take $x \in G$ and $y \neq x \in G$. They have order 2, so $x^2 = e$, which implies that $x = x^{-1}$ and similarly $y = y^{-1}$. Also, the element xy also has order 2, and so $xyx^{-1}y^{-1} = (xy)(xy) = e$, and so x and y commute. Because x and y were chosen arbitrarily, any two elements of the group commute, and so it is abelian.

  This group G is isomorphic to the matrix group
  $$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \leq GL_2(\mathbb{R}).$$

  The non-identity elements each have order 2 and commute with each other. This group is called the Klein-four group, and is denoted K_4.

Up to isomorphism, any order 4 group is either $\mathbb{Z}_2$ or K_4. Note that both of these groups are abelian[b]; the smallest non-abelian group has order 6.

[a] We write $\mathbb{Z}_n$ to denote the group of integers modulo n.
[b] commutative

Exercise 5.7
What are the possible groups of order 6?

The Counting Formula also provides another important corollary.

Corollary 5.8
The size of the group is
$$|G| = |\ker(f)| \cdot |\mathrm{im}(f)|.$$[a]

[a] In linear algebra, the analogous result is the rank-nullity theorem.

Proof. Let $f : G \to G'$ be a homomorphism, and $\ker(f) \leq G$ be the kernel. For each $y \in G'$, the preimage of y is
$$f^{-1}(y) := \{x \in G : f(x) = y\},$$
which is $\varnothing$ if $y \notin \mathrm{im}(f)$, and a coset of $\ker(f)$ otherwise.[23] □

Then, the number of left cosets of $\ker(f)$ is precisely the number of elements in the image of f, since each of those elements corresponds to a coset of the kernel. So $[G : \ker(f)] = |\mathrm{im}(f)|$, and applying the counting formula with $\ker(f)$ as our subgroup H gives us
$$|G| = |\ker(f)| \cdot |\mathrm{im}(f)|,$$
which is the desired result.

5.4 Normal Subgroups

In this section, we learn about normal subgroups.

[23] Pick $x \in f^{-1}(y)$. Then we claim that $f^{-1}(y) = x\ker(f)$. Take any $x' \in f^{-1}(y)$. We have $y = f(x) = f(x') = f(xx'^{-1})f(x')$, so $f(xx'^{-1}) = e$ and $xx'^{-1} \in \ker(f)$. Thus $x' \in x\ker(f)$.

Guiding Question
The choice of left cosets seems arbitrary — what are the ramifications if *right cosets* are used instead?

Definition 5.9
The **right coset** of a is
$$Ha = \{ha : h \in H\}.$$

In fact, all the same results follow if right cosets are used instead of left cosets. First, let's see an example of right cosets:

Example 5.10
Let H be the subgroup generated by $y \in S_3$. Then the left cosets are
$$\{e, y\}, \{x, xy\}, \{x^2, x^2y\},$$
and the right cosets are
$$\{e, y\}, \{x, x^2y\}, \{x^2, xy\}.$$
So in fact, right cosets give a different partition of S_3, but the number and size of the cosets are the same.[a]

[a] We can think of cosets as "carving up" the group. Using right cosets instead of left cosets is just carving it up in a different way.

In particular, there is a bijection between the set of left cosets and the set of right cosets. It maps
$$C \mapsto C^{-1} = \{x^{-1} : x \in C\}.$$
It is a bijection because $(ah)^{-1} = h^{-1}a^{-1}$, and so $aH = Ha^{-1}$. So the index $[G : H]$ is equal to both the number of right cosets and the number of left cosets.

Guiding Question
For which subsets $H \subseteq G$ do left and right cosets give the **same** partition of G? In other words, for which H is every left coset also a right coset?[a]

[a] If some left coset xH of an element x is equal to some right coset Hy of a different element y, since $x \in Hy$ as well, from a lemma from last week's lecture, $Hy = Hx$, and so in fact the left coset and right coset of the *same* element x must also be equal. So it is sufficient to require that $xH = Hx$.

This question motivates the definition of *normal subgroups.*

Definition 5.11
If $xH = Hx$ for each $x \in G$, $H \subseteq G$ is called a **normal subgroup**. Equivalently, the subgroup H is normal if and only if it is invariant under conjugation by x; that is, $xHx^{-1} = H$. Using the notation from last lecture[a], a subgroup H is normal if and only if $\varphi_x(H) = H$ for all $x \in G$.

[a] The function φ_x takes $g \mapsto xgx^{-1}$.

Let's look at some examples.

Example 5.12 (Non-normal subgroup)
From above, the subgroup $\langle y \rangle$ is *not* normal in S_3.

Example 5.13 (Kernel)
Given a homomorphism $f : G \to G'$, the kernel of f is *always* normal. Take $k \in \ker(f)$. Then

$$f(xkx^{-1}) = f(x)f(k)f(x)^{-1} = f(k) = e_{G'},$$

so $\varphi_x(\ker(f)) = \ker(f)$, and thus $\ker(f)$ is a normal subgroup. In fact, in future lectures, we will see that *all* normal subgroups of a given group G arise as the kernel of some homomorphism $f : G \to G'$ to a group G'.

Example 5.14
In S_3, the subgroup $\langle y \rangle$ is not normal, but $\langle x \rangle$ is normal. In particular, it is the kernel of the sign homomorphism $\text{sign} : S_3 \to \mathbb{R}$.[a]

[a] A given permutation σ can be written as a product of i transpositions, where i is unique up to parity. The sign homomorphism maps σ to $(-1)^i$.

5.5 The Correspondence Theorem

Ealier in this lecture, we noticed that homomorphisms give us some information about subgroups. Can we make this more concrete?

Guiding Question
Let f be a homomorphism from G to G'. Is there a relationship between the subgroups of G and the subgroups of G'?

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{subgroups of } G'\}$$

Answer. *In fact, we see that there is!*

- *Given a subgroup of G, a subgroup of G' can be produced as follows. Let f with the domain restricted to H be denoted as $f|_H$. Then a subgroup $H \leq G$ maps to $\text{im}(f|_H) = f(H) \subseteq G'$, which is a subgroup of G'.*
- *Now, given $H' \leq G'$ and a subgroup of G can be produced by taking the preimage*

  $$f^{-1}(H') = \{x \in G : f(x) \in H'\}.$$

  Is this subset of G is actually a subgroup? It is! Let's just check that it's closed under composition. If $x, y \in f^{-1}(H)$, then $f(x), f(y) \in H'$, so $f(x)f(y) \in H'$, since H' is closed under multiplication. Then $f(xy) \in H'$, so $xy \in f^{-1}(H)$.

  If $H' = e_{G'}$, then its preimage is the kernel, and if $H' = G'$, then the preimage is all of G. In general, the preimage is a subgroup somewhere in-between the kernel and the whole domain.

Are these maps bijective, or inverses of each other? It can be easily seen that they are not; in particular, if G is the trivial group and G' is some more complicated group with many subgroups, every subgroup of G' must always still map to the trivial group. It makes sense that these maps are not bijective, since f is not an isomorphism, just an arbitrary homomorphism with no more restrictions.

Two issues arise with these maps that make them non-bijective:

- Any subgroup of G must map to some subgroup of G' that is contained within the image of f, by construction, since $f(H) \subseteq \text{im}(f)$.
- The kernel $\ker(f) = f^{-1}(e_{G'}) \subseteq f^{-1}(H')$, so any subgroup not contained within the kernel cannot be mapped to by any subgroup of G'.

However, these are actually the only issues! If we are willing to put some restrictions on the homomorphism f and the types of subgroups we look at, there *is* actually a bijection between certain subgroups of G and certain subgroups of G'.

In order to make things a little easier for now, we take a surjective homomorphism $f : G \to G'$. The first issue then is no longer consequential, because the image is all of G'. Now, let's restrict the subgroups of G to subgroups that contain $\ker(f)$. Then our maps (as described above) provide a bijection.

Theorem 5.15 (Correspondence Theorem)
For a surjective homomorphism f with kernel K, there is a bijective correspondence:

$$\{\text{subgroups of } G \text{ containing } K\} \leftrightarrow \{\text{subgroups of } G'\},$$

where

$$\begin{aligned} \text{a subset of } G, H \supseteq K &\rightsquigarrow \text{its image } f(H) \leq G' \\ H' \leq G' &\rightsquigarrow \text{its preimage } f^{-1}(H') \leq G. \end{aligned}$$

Example 5.16 (Roots of Unity)
Take

$$\begin{aligned} G = \mathbb{C}^* &\xrightarrow{f} G' = \mathbb{C}^* \\ z &\mapsto z^2, \end{aligned}$$

which is a homomorphism because G is abelian.

The kernel is $\ker(f) = \{\pm 1\}$. We have a correspondence between $\mathbb{R}^\times \rightsquigarrow \mathbb{R}_{>0}$.

For example, the eighth roots of unity correspond to the fourth roots of unity under this map.

$$H = \{e^{\frac{2\pi i k}{8}}\} \leftrightsquigarrow H' = \{\pm 1, \pm i\}.$$