4 Isomorphisms and Cosets

4.1 Review

In the last lecture, we learned about subgroups and homomorphisms.

Definition 4.1
We call $f : G \to G'$ a **homomorphism** if for all $a, b \in G$, $f(a)f(b) = f(ab)$.

Definition 4.2
The **kernel** of a homomorphism f is $\{a \in G : f(a) = e_{G'}\}$, and the **image** is the set of elements $b = f(a)$ for some a.

The kernel and image of f are subgroups of G and G', respectively.

4.2 Isomorphisms

Homomorphisms are mappings between groups; now, we consider homomorphisms with additional constraints.

Guiding Question
What information can we learn about groups using mappings between them?

Definition 4.3
We call $f : G \to G'$ an **isomorphism** if f is a bijective homomorphism.

In some sense, if there exists an isomorphism between two groups, they are the *same* group; relabeling the elements of a group using an isomorphism and using the new product law yields the same products as before relabeling. Almost all the time, it is only necessary to consider groups *up to isomorphism*.

Example 4.4
There exists an isomorphism $f : \mathbb{Z}_4 \to \langle i \rangle$ given by $n \mod 4 \mapsto i^n$. In particular, we get

$$\begin{aligned} 0 &\mapsto 1 \\ 1 &\mapsto i \\ 2 &\mapsto -1 \\ 3 &\mapsto -i. \end{aligned}$$

So the group generated by i, which can be thought of as a rotation of the complex plane by $\pi/2$, is essentially "the same" as the integers modulo 4.

Example 4.5
More generally, the group generated by g, $\langle g \rangle = \{e, g, g^2, \cdots, g^{d-1}\}$, where d is the order of g, is isomorphic to $\mathbb{Z}_d = \{0, 1, \cdots, d-1\}$. If the order of g is infinite, then we have $\langle g \rangle \cong \mathbb{Z}$.

Here, the idea that an isomorphism is a "relabeling" of elements makes sense: since $g^a g^b = g^{a+b}$, relabeling g^i with its exponent i retains the important information in this situation. Thinking of $\langle g \rangle$ in this way yields precisely $\mathbb{Z}_d$.

4.3 Automorphisms

An important notion is that of an *automorphism*, which is an isomorphism with more structure.

Definition 4.6
An isomorphism from G to G is called an **automorphism.**

If a homomorphism can be thought of as giving us some sort of "equivalence" between two groups, why do we care about automorphisms? We already *have* an equivalence between G and itself, namely the identity. The answer is that while the identity map $\text{id} : G \to G$ is always an automorphism, more interesting ones exist as well! We can understand more about the symmetry and structure of a group using these automorphisms.

Example 4.7
A non-trivial automorphism from $\mathbb{Z}$ to itself is $f : \mathbb{Z} \to \mathbb{Z}$ taking $n \mapsto -n$.

From the existence of this nontrivial automorphism, we see that $\mathbb{Z}$ has a sort of "reflective" symmetry.[17]

Example 4.8 (Inverse transpose)
Another non-trivial automorphism, on the set of invertible matrices, is the inverse transpose

$$\begin{aligned} f : GL_n(\mathbb{R}) &\to GL_n(\mathbb{R}) \\ A &\mapsto (A^t)^{-1} \end{aligned}$$

Many other automorphisms exist for $GL_n(\mathbb{R})$,[18] since it is a group with lots of structure and symmetry.

Example 4.9 (Conjugation)
A very important automorphism is **conjugation** by a fixed element $a \in G$. We let $\phi_a : G \to G$ be such that

$$\phi_a(x) = axa^{-1}.$$

We can check the conditions to show that conjugation by a is an automorphism:

- **Homomorphism.**
$$\phi_a(x)\phi_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \phi_a(xy).$$
- **Bijection.** We have an inverse function $\phi_{a^{-1}}$:
$$\phi_{a^{-1}} \circ \phi_a = \phi_a \circ \phi_{a^{-1}} = \text{id}.$$

Note that if G is abelian, then $\phi_a = \text{id}$.

Any automorphism that can be obtained by conjugation is called an **inner automorphism**; any group intrinsically has inner automorphisms coming from conjugation by each of the elements (we can always find these automorphisms to work with). Some groups also have **outer automorphisms**, which are what we call any automorphisms that are not inner. For example, on the integers, the only inner automorphism is the identity function, since they are abelian.[19]

4.4 Cosets

Throughout this section, we use the notation $K := \ker(f)$.

Guiding Question
When do two elements of G get mapped to the same element of G'? When does $f(a) = f(b) \in G'$?

Given a subgroup of G, we can find "copies" of the subgroup inside G.

[17] In particular, this automorphism f corresponds to reflection of the number line across 0.
[18] For example, just the transpose or just the inverse are automorphisms, and in fact they are commuting automorphisms, since the transpose and inverse can be taken in either order.
[19] For an abelian group, $axa^{-1} = aa^{-1}x = x$.

Definition 4.10
Given $H \subseteq G$ a subgroup, a **left coset** of H is a subset of the form

$$aH \coloneqq \{ax : x \in H\}$$

for some $a \in G$.

Let's start with a couple of examples.

Example 4.11 (Cosets in S_3)
Let's use our favorite non-abelian group, $G = S_3 = \langle (123), (12) \rangle = \langle x, y \rangle$, and let our subgroup H be $\{e, y\}$. Then

$$eH = H = \{e, y\} = yH;$$

$$xH = \{x, xy\} = xyH;$$

and

$$x^2 H = \{x^2, x^2 y\} = x^2 yH.$$

We have three different cosets, since we can get each coset one of two ways.

Example 4.12
If we let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$, we get

$$0 + H = 2\mathbb{Z} = \text{evens} = 2 + H = \cdots,$$

and

$$1 + H = 1 + 2\mathbb{Z} = \text{odd integers} = 3 + H = \cdots.$$

In this example, the odd integers are like a "copy" of the even integers, shifted over by 1. From these examples, we notice a couple of properties about cosets of a given subgroup.

Proposition 4.13
All cosets of H have the same order as H.

Proof. We can prove this by taking the function $f_a : H \to aH$ which maps $h \mapsto ah$. This is a bijection because it is invertible; the inverse is $f_{a^{-1}}$.[20] □

Proposition 4.14
Cosets of H form a **partition** of the group G.[a]

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

To prove this, we use the following lemma.

Lemma 4.15
Given a coset $C \subset G$ of H, take $b \in C$. Then, $C = bH$.

Proof. If C is a coset, then $C = aH$ for some $a \in G$. If $b \in C$, then $b = ah$ for some $h \in H$, and $a = bh^{-1}$. Then

$$bH = \{bh' : h' \in H\} = \{ahh' | h' \in H\} \subseteq aH.$$

Using $a = bh^{-1}$, we can similarly show that $aH \subseteq bH$, and so $aH = bH$.[21] □

[20] I can undo any f_a in a **unique** way by multiplying again on the left by a^{-1}. This is something that breaks down with monoids or semigroups or other more complicated structures.
[21] So for a given coset C, we can use any of the elements in it as the representative a such that $C = aH$.

Proof. Now, we prove our proposition.

- Every $x \in G$ is in some coset. Take $C = xH$. Then $x \in C$.
- Cosets are disjoint. If not, let C, C' be distinct cosets, and take y in their intersection. Then $yH = C$ and $yH = C'$ by Lemma 4.15, and so $C = C'$.

□

With this conception of *cosets*, we have the answer to our question:

Answer. *If $f(a) = f(b)$, then $f(a)^{-1}f(b) = e_{G'}$. In particular, $f(a^{-1}b) = e_{G'}$, so $a^{-1}b \in K$, the kernel of f. Then, we have that $b \in aK$, or $b = ak$ where $f(k) = e_{G'}$. So $f(a) = f(b)$ if a is in the same left coset of the kernel as b.*

4.5 Lagrange's Theorem

In fact, thinking about cosets gives us quite a restrictive result on subgroups, known as Lagrange's Theorem.

Guiding Question
What information do we automatically have about subgroups of a given group?

Definition 4.16
The **index** of $H \subseteq G$ is $[G : H]$, the number of left cosets.

Theorem 4.17
We have
$$|G| = [G : H]|H|.$$

Proof. This is true because each of the cosets have the same number of elements and partition G.

So we have
$$|G| = \sum_{\text{left cosets } C} |C| = \sum_{\text{left cosets } C} |H| = [G : H]|H|.$$

That is, the order of G is the number of left cosets multiplied by the number of elements in each one (which is just $|H|$). □

Example 4.18
For S_3, we have $6 = 3 \cdot 2$.

From our theorem, we get Lagrange's Theorem:

Corollary 4.19 (Lagrange's Theorem.)
For H a subgroup of G, $|H|$ is a divisor of $|G|$.

We have an important corollary about the structure of cyclic groups.

Corollary 4.20
If $|G|$ is a prime p, then G is a cyclic group.

Proof. Pick $x \neq e \in G$. Then $\langle x \rangle \subseteq G$. Since the order of x cannot be 1, since it is not the identity, the order of x has to be p, since p is prime. Therefore, $\langle x \rangle = G$, and so G is cyclic, generated by x. □

In general, for $x \in G$, the order of x is the size of $\langle x \rangle$, which divides G. So the order of any element divides the size of the group.