1. Lagrange’s Theorem

You basically proved Lagrange’s theorem in Homework 17. Let me restate it here, and give you a proof in one piece.

**Lagrange’s Theorem.** If \( H \) is a subgroup of the finite group \( G \), then \( |H| \) divides \( |G| \).

**Proof.** **Step 1.** \(|aH| = |H|\) for all \( a \in G \): Let \( aH \) be a left coset of \( H \), and let \( f : H \to aH \) be a function defined so that \( f(h) = ah \). The function \( f \) is clearly onto. To show that \( f \) is one-to-one, we must show that whenever \( f(h_1) = f(h_2) \), \( h_1 = h_2 \). So suppose \( f(h_1) = f(h_2) \). Then \( ah_1 = ah_2 \), and \( a^{-1}ah_1 = a^{-1}ah_2 \). Therefore, \( h_1 = h_2 \). This establishes the fact that \( f \) is one-to-one. We have, then, a one-to-one, onto function from \( H \) to \( aH \), so \( H \) and \( aH \) must have the same cardinality.

**Step 2.** For any \( a \in G \), \( a \in aH \). It is clear, therefore, that every element of \( G \) lies in at least one left coset of \( H \).

**Step 3.** For any \( a, b \in G \), \( aH = bH \) or \( aH \cap bH = \emptyset \): Let \( aH \) and \( bH \) be two left cosets of \( H \). If they are not disjoint, then there is an element \( x \in G \) such that \( x \in aH \) and \( x \in bH \). It follows that \( x = ah_1 \) for some \( h_1 \in H \) and also that \( x = bh_2 \) for some \( h_2 \in H \). Therefore,

\[
\text{(1)} \quad ah_1 = bh_2,
\]

and

\[
\text{(2)} \quad ah_1h_2^{-1} = b.
\]

Since \( h_1h_2^{-1} \in H \), we see that \( b \in aH \). Furthermore, any element of \( bH \) can be expressed in the form \( bh \) for some \( h \in H \). It follows that

\[
\text{(3)} \quad bh = ah_1h_2^{-1}h,
\]

which is an element of \( aH \), since \( h_1h_2^{-1}h \in H \). We have proven that \( bH \subseteq aH \). A similar argument shows that \( aH \subseteq bH \), so we know that \( aH = bH \).

We have shown that the distinct left cosets of \( H \) partition \( G \) into disjoint sets that are all the same size as \( H \). If there are \( n \) distinct left cosets, then clearly \( |G| = n \cdot |H| \), and this proves the theorem. \( \square \)

2. Homomorphisms

We talked about isomorphisms earlier in the semester. A homomorphism is a function from one group to another that preserves the operation. In other words, a homomorphism is like an isomorphism without the one-to-one and onto conditions. Let’s define this explicitly.

**Definition 1.** Let \( f : G \to H \) be a function from the group \( G \) to the group \( H \). The function \( f \) is a homomorphism, if

\[
\text{(4)} \quad f(a \cdot b) = f(a) \cdot f(b)
\]

for all \( a, b \in G \).

**Example.** Consider the function \( f : \mathbb{Z} \to \mathbb{Z} : z \mapsto -2z \). For example, \( f(5) = -10 \), and \( f(-3) = 6 \). In this particular case,

\[
\text{(5)} \quad f(5 + (-3)) = f(2) = -4,
\]

and

\[
\text{(6)} \quad f(5) + f(-3) = -10 \cdot 6 = -4.
\]

We can prove this in general:

\[
\text{(7)} \quad f(x + y) = -2(x + y) = -2x - 2y = (-2x) + (-2y) = f(x) + f(y).
\]
Example Note that a group with one generator and no relations is going to be isomorphic to $\mathbb{Z}$. If $G$ has generator $s$ with relation $s^n = e$, then $G$ is isomorphic $\mathbb{Z}_n$. If you think about it a little bit, once you know where a homomorphism maps the generators, you can figure out where everything else goes. Because of this, it’s convenient to define homomorphisms by just saying what happens to the generators. For example, consider the homomorphism $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_{12}$ that takes $1$ to $3$. For $f$ to be a homomorphism, we must have $f(2) = f(1 + 1) = f(1) + f(1) = 3 + 3 = 6$. Similarly, $f(3) = 9$. Continuing on, we find that

<table>
<thead>
<tr>
<th>$\mathbb{Z}_8$</th>
<th>$f$</th>
<th>$\mathbb{Z}_{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\mapsto$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>$\mapsto$</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>$\mapsto$</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>$\mapsto$</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>$\mapsto$</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>$\mapsto$</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>$\mapsto$</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>$\mapsto$</td>
<td>9</td>
</tr>
</tbody>
</table>

(8)

We should still check to see that this is a homomorphism, but I’ll just tell you that it is. Note that both 0 and 4 map to 0 $\in \mathbb{Z}_{12}$, and that $\{0, 4\}$ is a subgroup of $\mathbb{Z}_8$. Note also that there are two elements in $\mathbb{Z}_8$ that map to each of the elements in the image. These both reflect general properties of homomorphisms.

Example. A generator can’t be mapped to just any old element. It usually becomes clear when things are not going to work out. Let’s try to make a homomorphism $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_{12}$ that takes 1 to 4. This means that $f(2) = f(1 + 1) = f(1) + f(1) = 4 + 4 = 8$. This leads us to the following.

<table>
<thead>
<tr>
<th>$\mathbb{Z}_8$</th>
<th>$f$</th>
<th>$\mathbb{Z}_{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\mapsto$</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>$\mapsto$</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>$\mapsto$</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>$\mapsto$</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>$\mapsto$</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>$\mapsto$</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>$\mapsto$</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>$\mapsto$</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>$\mapsto$</td>
<td>8</td>
</tr>
</tbody>
</table>

(9)

Since $8 \equiv_8 0$, we have 0 mapping to both 0 and 8 in $\mathbb{Z}_{12}$. Functions can’t do that, so there is no such homomorphism. It’s slightly easier to show something is not a homomorphism than it is to show a function is a homomorphism.

1. Find as many homomorphisms as you can of the form $f : D_4 \rightarrow D_4$.

3. Some terminology

For any function $f : A \rightarrow B$, the set $A$ is called the domain, and the set $B$ is called the codomain, although some might call $B$ the range. The set of elements in $B$ that actually get mapped to is called the image of $f$. The image is also sometimes called the range, so the word range should be spoken and heard with care. Let me give a more general (and specific) definition for image.

Definition 2. Let $f : A \rightarrow B$, and let $S \subset A$. The image of $S$, denoted $f(S)$, is the set

$$ f(S) = \{ f(a) \in B \mid a \in S \}.$$

(10)

If we just say image of $f$, we mean $f(A)$.

We want to go the other way, as well.
**Definition 3.** Let \( f : A \to B \), and let \( R \subseteq B \). The **preimage** of \( R \), denoted \( f^{-1}(R) \), is the set
\[
  f^{-1}(R) = \{ a \in A \mid f(a) \in R \}
\]
The preimage of \( R \) is the collection of domain elements that map into \( R \).

One last definition. With homomorphisms, we’re going to be interested in the set of things in the domain that map to the identity.

**Definition 4.** Let \( f : G \to H \) be a homomorphism from the group \( G \) to the group \( H \). The **kernel** of \( f \), denoted \( \ker(f) \), is the set
\[
  \ker(f) = \{ a \in G \mid f(a) = e \}
\]
In other words, the \( \ker(f) \) is the preimage of the set \( \{ e \} \).

1. Suppose \( f : A \to B \) is a function. What is \( f^{-1}(B) \)?
2. Let \( f : \mathbb{Z}_3 \to \mathbb{Z}_6 \) be the homomorphism that maps \( 1 \mapsto 2 \). Find the image of \( f \) (i.e., \( f(\mathbb{Z}_3) \)) and \( \ker(f) \).
3. Let \( f : \mathbb{Z}_6 \to D_3 \) be the homomorphism that maps \( 1 \mapsto 120^\circ \). Find the image of \( f \) and \( \ker(f) \).
4. Let \( f : \mathbb{Z}_{12} \to \mathbb{Z}_6 \) be the homomorphism that maps \( 1 \mapsto 2 \). Find the image of \( f \) and \( \ker(f) \).

**4. Homework 18**

For problems 1-3, let \( f : \mathbb{Z}_8 \to \mathbb{Z}_2 \) be the homomorphism that maps \( 1 \mapsto 1 \).

1. What are the elements in image of \( f \).
2. What are the elements in \( \ker(f) \).
3. What are \( |\mathbb{Z}_8|, |f(\mathbb{Z}_8)| \), and \( |\ker(f)| \)? That is, how many elements are in each of these sets? Write your answer like \( 4,7,2 \) with no spaces.

For problems 4-6, let \( f : \mathbb{Z}_9 \to \mathbb{Z}_9 \) be the homomorphism that maps \( 1 \mapsto 3 \).

4. What are the elements in image of \( f \).
5. What are the elements in \( \ker(f) \).
6. What are \( |\mathbb{Z}_9|, |f(\mathbb{Z}_9)| \), and \( |\ker(f)| \)? That is, how many elements are in each of these sets? Write your answer like \( 4,7,2 \) with no spaces.

For problems 7-9, let \( f : \mathbb{Z}_4 \to \mathbb{Z}_{12} \) be the homomorphism that maps \( 1 \mapsto 9 \).

7. What are the elements in image of \( f \).
8. What are the elements in \( \ker(f) \).
9. What are \( |\mathbb{Z}_4|, |f(\mathbb{Z}_4)| \), and \( |\ker(f)| \)? That is, how many elements are in each of these sets? Write your answer like \( 4,7,2 \) with no spaces.

For problems 10-12, let \( f : \mathbb{Z}_{12} \to \mathbb{Z}_4 \) be the homomorphism that maps \( 1 \mapsto 2 \).

10. What are the elements in image of \( f \).
11. What are the elements in \( \ker(f) \).
12. What are $|\mathbb{Z}_{12}|$, $|f(\mathbb{Z}_{12})|$, and $|\ker(f)|$? That is, how many elements are in each of these sets? Write your answer like $4, 7, 2$ with no spaces.

For problems 13-15, you should have noticed a pattern in the relationship between $|G|$, $|f(G)|$, and $|\ker(f)|$.
Conjecture: For a homomorphism $f: G \to H$, $A \cdot B = C$.

13. What goes in for $A$ and $B$?

14. What goes in for $C$?

Bye.