Normal Subgroups and Quotient Groups

The idea here is to find a condition on a subgroup $H$ which makes the set of cosets $G/H$ into a group.

**Example.** Let $G = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and let $H$ be the subgroup $\{0, 4\}$. The cosets of $H$ are

$\{0, 4\}, \quad 1 + \{0, 4\} = \{1, 5\}, \quad 2 + \{0, 4\} = \{2, 6\}, \quad 3 + \{0, 4\} = \{3, 7\}$.

I’m going to make the set of cosets $\mathbb{Z}_8/\{0, 4\}$ into a group. Here’s the addition table:

<table>
<thead>
<tr>
<th>$+$</th>
<th>${0, 4}$</th>
<th>${1, 5}$</th>
<th>${2, 6}$</th>
<th>${3, 7}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${0, 4}$</td>
<td>${0, 4}$</td>
<td>${1, 5}$</td>
<td>${2, 6}$</td>
<td>${3, 7}$</td>
</tr>
<tr>
<td>${1, 5}$</td>
<td>${1, 5}$</td>
<td>${2, 6}$</td>
<td>${3, 7}$</td>
<td>${0, 4}$</td>
</tr>
<tr>
<td>${2, 6}$</td>
<td>${2, 6}$</td>
<td>${3, 7}$</td>
<td>${0, 4}$</td>
<td>${1, 5}$</td>
</tr>
<tr>
<td>${3, 7}$</td>
<td>${3, 7}$</td>
<td>${0, 4}$</td>
<td>${1, 5}$</td>
<td>${2, 6}$</td>
</tr>
</tbody>
</table>

To see how the table was constructed, consider the entry

$\{2, 6\} + \{3, 7\} = \{1, 5\}$.

How was this done?

One way to do this is to use

$\{2, 6\} = 2 + \{0, 4\} \quad $and $\quad \{3, 7\} = 3 + \{0, 4\}$.

You add cosets by adding their representatives — in this case, 2 and 3 — and attaching the sum to the subgroup — in this case, $\{0, 4\}$:

$\{2, 6\} + \{3, 7\} = (2 + \{0, 4\}) + (3 + \{0, 4\}) = (2 + 3) + \{0, 4\} = 5 + \{0, 4\} = \{1, 5\}$.

Another way to do this is to use individual elements. Take an element from $\{2, 6\}$ and an element from $\{3, 7\}$ and add them. Find the coset that contains the sum. That coset is the sum of the cosets.

For example, if I use 6 from $\{2, 6\}$ and 3 from $\{3, 7\}$, I get $6 + 3 = 1$, which is in $\{1, 5\}$. Therefore, $\{2, 6\} + \{3, 7\} = \{1, 5\}$.

What happens if you choose different elements? Take 2 from $\{2, 6\}$ and 7 from $\{3, 7\}$. Then $2 + 7 = 1$, which is in $\{1, 5\}$ again. Just as before, $\{2, 6\} + \{3, 7\} = \{1, 5\}$.

This is what it means to say that coset addition is well-defined: No matter which elements you choose from the two sets, the sum of the elements will always be in the same coset.

The table above is a group table for a group of order 4. There are only two groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Hence, the group above must be isomorphic to one of these groups. In fact, if you replace

$\{0, 4\}$ with 0, $\{1, 5\}$ with 1, $\{2, 6\}$ with 2, and $\{3, 7\}$ with 3,

you get this table:

<table>
<thead>
<tr>
<th>$+$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Thus, \( \mathbb{Z}_8 \setminus \{0, 4\} \cong \mathbb{Z}_4 \). □

Under what conditions will the set of cosets form a group? That is, under what conditions will coset addition (or multiplication, if that is the operation) be well-defined?

**Lemma.** Let \( G \) be a group, and let \( H \) be a subgroup of \( G \). The following statements are equivalent:

1. \( a \) and \( b \) are elements of the same coset of \( H \).
2. \( aH = bH \).
3. \( b^{-1}a \in H \).

**Proof.** To show that several statements are equivalent, I must show that any one of them follows from any other. To do this efficiently, I’ll show that statement 1 implies statement 2, statement 2 implies statement 3, and statement 3 implies statement 1.

(1 \( \Rightarrow \) 2) Suppose \( a \) and \( b \) are elements of the same coset \( gH \) of \( H \). Since \( a \in aH \cap gH \), and since cosets are either disjoint or identical, \( aH = gH \). Likewise, \( b \in bH \cap gH \) implies \( bH = gH \). Therefore, \( aH = bH \).

(2 \( \Rightarrow \) 3) Suppose \( aH = bH \). Since \( 1 \in H \), it follows that \( a = a \cdot 1 \in aH = bH \). Therefore, \( a = bh \) for some \( h \in H \). Hence, \( b^{-1}a = h \in H \).

(3 \( \Rightarrow \) 1) Suppose \( b^{-1}a = h \in H \). Then \( b^{-1}aH = hH = H \), so \( aH = bH \). Therefore, \( a \) and \( b \) are elements of the same coset of \( H \), namely \( aH = bH \).

**Corollary.** \( aH = H \) if and only if \( a \in H \).

**Proof.** The equivalence of the second and third conditions says that \( aH = bH \) if and only if \( b^{-1}a \in H \). Taking \( b = 1 \), this says that \( aH = H \) if and only if \( a \in H \), which is what I wanted to prove. □

In general, the collection \( G/H \) of left cosets of \( H \) in \( G \) is just a set. However, it looks as though you ought to be able to define a binary operation on \( G/H \) by

\[
(aH) \cdot (bH) = (ab)H.
\]

The idea is to use this binary operation to make \( G/H \) into a group. However, a problem arises with the definition of the operation. The cosets \( aH \) and \( bH \) above could be written in terms of other elements (coset representatives). Suppose that \( aH = a'H \) and \( bH = b'H \) for some other elements \( a', b' \). Then

\[
(a'H) \cdot (b'H) = (a'b')H.
\]

The product will not make sense — it won’t be well-defined — unless \( (ab)H = (a'b')H \). This will not be the case for an arbitrary subgroup \( H < G \). The following definition gives a condition on \( H \) which ensures that coset multiplication is well-defined.

**Definition.** A subgroup \( H < G \) is **normal** if

\[
gHg^{-1} \subseteq H \quad \text{for all} \quad g \in G.
\]

(Since the statement runs over all \( g \in G \), I could just as well say “\( g^{-1}Hg \subseteq H \)”.) Write \( H \triangleleft G \) to mean that \( H \) is a normal subgroup of \( G \).

**Example.** If \( G \) is a group, \( \{1\} \) and \( G \) are normal in \( G \). □
**Example.** If \( G \) is abelian, every subgroup is normal. For if \( g \in G \), then \( gHg^{-1} = Hg_{g^{-1}} = H \).

Let’s see how this works in a particular example. Let \( G = \mathbb{Z}_4 = \{0, 1, 2, 3\} \), and let \( H = \{0, 2\} \). Then

\[
0 + \{0, 2\} + (-0) = \{0, 2\},
\]
\[
1 + \{0, 2\} + (-1) = 1 + \{0, 2\} + 3 = \{0, 2\},
\]
\[
2 + \{0, 2\} + (-2) = 2 + \{0, 2\} + 2 = \{0, 2\},
\]
\[
3 + \{0, 2\} + (-3) = 3 + \{0, 2\} + 1 = \{0, 2\}.
\]

Thus, \( H \) is normal — as it should be, since \( G = \mathbb{Z}_4 \) is abelian.

Note that it isn’t always practical to check that a subgroup is normal by checking the condition for each element in the group! 

---

**Example.** Here’s the multiplication table for \( S_3 \), the group of permutations of \( \{1, 2, 3\} \).

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>(1 2 3)</th>
<th>(1 3 2)</th>
<th>(2 3)</th>
<th>(1 3)</th>
<th>(1 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>id</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(2 3)</td>
<td>(1 3)</td>
<td>(1 2)</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>id</td>
<td>(1 2)</td>
<td>(2 3)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>(1 3 2)</td>
<td>id</td>
<td>(1 2 3)</td>
<td>(1 3)</td>
<td>(1 2)</td>
<td>(2 3)</td>
</tr>
<tr>
<td>(2 3)</td>
<td>(2 3)</td>
<td>(1 3)</td>
<td>(1 2)</td>
<td>id</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 3 2)</td>
<td>id</td>
<td>(1 3 2)</td>
<td>id</td>
</tr>
<tr>
<td>(1 2)</td>
<td>(1 2)</td>
<td>(2 3)</td>
<td>(1 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>id</td>
</tr>
</tbody>
</table>

Consider the subgroup \( H = \{\text{id}, (1 3)\} \). I’ll show that \( H \) is not normal. To do this, I have to find an element \( g \in S_3 \) such that

\[
g[\text{id}, (1 3)]g^{-1} \not\in \{\text{id}, (1 3)\}.
\]

I’ll take \( g = (1 2) \). (I found (1 2) by trial and error.)

\[
(1 2)[\text{id}, (1 3)](1 2)^{-1} = (1 2)[\text{id}, (1 3)](1 2) = \{(1 2)|\text{id}(1 2), (1 2)(1 3)(1 2)\} = \{\text{id}, (2 3)\}.
\]

Since \( \{\text{id}, (2 3)\} \not\subset \{\text{id}, (1 3)\} \), the subgroup \( \{\text{id}, (1 3)\} \) is not normal in \( S_3 \). 

---

**Example.** Consider the group of the quaternions:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>-1</th>
<th>i</th>
<th>-i</th>
<th>j</th>
<th>-j</th>
<th>k</th>
<th>-k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>i</td>
<td>-i</td>
<td>j</td>
<td>-j</td>
<td>k</td>
<td>-k</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-i</td>
<td>i</td>
<td>-j</td>
<td>j</td>
<td>-k</td>
<td>k</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>-i</td>
<td>-1</td>
<td>1</td>
<td>k</td>
<td>-k</td>
<td>-j</td>
<td>j</td>
</tr>
<tr>
<td>-i</td>
<td>-i</td>
<td>i</td>
<td>1</td>
<td>-1</td>
<td>-k</td>
<td>k</td>
<td>j</td>
<td>-j</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-j</td>
<td>-k</td>
<td>k</td>
<td>-l</td>
<td>1</td>
<td>i</td>
<td>-i</td>
</tr>
<tr>
<td>-j</td>
<td>-j</td>
<td>j</td>
<td>-k</td>
<td>-k</td>
<td>1</td>
<td>-l</td>
<td>-i</td>
<td>i</td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>-k</td>
<td>j</td>
<td>-j</td>
<td>i</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>-k</td>
<td>-k</td>
<td>k</td>
<td>-j</td>
<td>j</td>
<td>-i</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>
Consider the subgroup \(\{1, -1, i, -i\}\). To show that it’s normal, I have to compute \(g\{1, -1, i, -i\}g^{-1}\) for each element \(g\) in the group and show that I always get the subgroup \(\{1, -1, i, -i\}\). It’s too tedious to do this for all the elements, so I’ll just do the computation for one of them.

Take \(g = j\). Then \(g^{-1} = -j\) (since \(j(-j) = 1\), so

\[
j\{1, -1, i, -i\}j^{-1} = j\{1, -1, i, -i\}(-j) = \{j \cdot 1 \cdot (-j), j \cdot (-1) \cdot (-j), j \cdot i \cdot (-j), j \cdot (-i) \cdot (-j)\} = \\
\{1, -1, (-k)(-j), k(-j)\} = \{1, -1, -i, i\}.
\]

This is the same set as the original subgroup, so the verification worked with this element.

If I do the same computation with the other elements in \(Q\), I’ll always get the original subgroup back. Therefore, \(\{1, -1, i, -i\}\) is normal.

Note that \(|Q| = 8\) while \(|\{1, -1, i, -i\}| = 4\), so the subgroup has \(\frac{8}{4} = 2\) cosets. \(\Box\)

**Example.** A subgroup of index 2 is always normal. For suppose \((G : H) = 2\). This means that \(H\) has two left cosets and two right cosets. One coset is always \(H\) itself. Take \(g \notin H\). Then \(gH\) is the other left coset, \(Hg\) is the other right coset, and

\[H \cup gH = G = H \cup Hg.\]

But these are disjoint unions, so \(gH = Hg\). By an earlier result, this means that \(H\) is normal. \(\Box\)

**Example.** Let \(G\) and \(H\) be groups. Prove that

\[G \times \{1\} = \{(g, 1) \mid g \in G\}\]

is a normal subgroup of the product \(G \times H\).

First, I’ll show that it’s a subgroup.

Let \((g_1, 1), (g_2, 1) \in G \times \{1\}\), where \(g_1, g_2 \in G\). Then

\[(g_1, 1) \cdot (g_2, 1) = (g_1g_2, 1) \in G \times \{1\}.\]

Therefore, \(G \times \{1\}\) is closed under products.

The identity \((1, 1)\) is in \(G \times \{1\}\).

If \((g, 1) \in G \times \{1\}\), the inverse is \((g, 1)^{-1} = (g^{-1}, 1)\), which is in \(G \times \{1\}\).

Therefore, \(G \times \{1\}\) is a subgroup.

To show that \(G \times \{1\}\) is normal, let \((a, b) \in G \times H\), where \(a \in G\) and \(b \in H\). I must show that

\[(a, b)(G \times \{1\})(a, b)^{-1} \subset G \times \{1\}.\]

I can show one set is a subset of another by showing that an element of the first is an element of the second. An element of \((a, b)(G \times \{1\})(a, b)^{-1}\) looks like \((a, b)(g, 1)(a, b)^{-1}\), where \((g, 1) \in G \times \{1\}\). Now

\[(a, b)(g, 1)(a, b)^{-1} = (a, b)(g, 1)(a^{-1}, b^{-1}) = (aga^{-1}, b(1)b^{-1}) = (aga^{-1}, 1).\]

\(aga^{-1} \in G\), since \(a, g \in G\). Therefore, \((a, b)(g, 1)(a, b)^{-1} \in G \times \{1\}\). This proves that \((a, b)(G \times \{1\})(a, b)^{-1} \subset G \times \{1\}\). Therefore, \(G \times \{1\}\) is normal. \(\Box\)

The next lemma shows that it does no harm to replace the inclusion with equality.

**Lemma.** \(H \triangleleft G\) if and only if \(gHg^{-1} = H\) for all \(g \in G\).
**Proof.** \((\Leftrightarrow)\) If \(gHg^{-1} = H\) for all \(g \in G\), then a fortiori \(gHg^{-1} \subset H\) for all \(g \in G\). Therefore, \(H \triangleleft G\).

\((\Rightarrow)\) Suppose \(H \triangleleft G\). Let \(g \in G\). Then \(gHg^{-1} \subset H\). On the other hand, using \(g^{-1}\) in place of \(g\), I obtain \(g^{-1}Hg \subset H\). Multiply this inclusion on the left by \(g\) and on the right by \(g^{-1}\) to obtain \(H \subset gHg^{-1}\). Therefore, \(gHg^{-1} = H\). \(\square\)

If you know a subgroup is normal, you use the equation form because it is “stronger”. On the other hand, if you’re trying to 

prove that a subgroup \(H\) is normal in a group \(G\), all you need to show is that \(gHg^{-1} \subset H\) for all \(g \in G\) (as opposed to equality).

Now I’ll show that the definition of normality does what I wanted it to.

**Theorem.** Let \(G\) be a group, \(H < G\). The following statements are equivalent:

1. \(H \triangleleft G\)
2. For all \(g \in G\), \(gH = Hg\). (Thus, every left coset is a right coset and every right coset is a left coset.)
3. Coset multiplication is well-defined.

By the third statement, I mean that if \(a_1H = a_2H\) and \(b_1H = b_2H\), then \(a_1b_1H = a_2b_2H\). Once I know that multiplication is well-defined, I can define multiplication of cosets by \((aH)(bH) = abH\).

**Proof.** (1 \(\Rightarrow\) 2) If \(H \triangleleft G\) and \(g \in G\), then \(gHg^{-1} = H\), so \(gHg^{-1}g = Hg\), or \(gH = Hg\).

(2 \(\Rightarrow\) 3) Suppose \(gH = Hg\) for all \(g \in G\). Suppose

\[a_1H = a_2H \quad \text{and} \quad b_1H = b_2H.\]

Then

\[a_1b_1H = a_1b_2H = a_1Hb_2 = a_2Hb_2 = a_2b_2H.\]

(3 \(\Rightarrow\) 1) Suppose coset multiplication is well defined. I want to show \(H \triangleleft G\). Let \(g \in G\). I will show \(gHg^{-1} \subset H\).

Do it with elements. Let \(h \in H\). I will show \(ghg^{-1} \in H\).

By an earlier corollary, \(hH = H\), and surely \(gH = gH\), so (since coset multiplication is well-defined) \(gh = gH\). Again, \(g^{-1}H = g^{-1}H\), so \((gh)g^{-1}H = gg^{-1}H = 1 \cdot H = H\). By another lemma, this shows that \(ghg^{-1} \in H\). Therefore, \(H \triangleleft G\). \(\square\)

The point of all this was to make the set of cosets \(G/H\) into a group via coset multiplication.

**Proposition.** If \(H \triangleleft G\), the set of left cosets \(G/H\) becomes a group under coset multiplication.

**Proof.** Associativity:

\[(aH \cdot bH) \cdot cH = (ab)H \cdot cH = (abc)H, \quad aH \cdot (bH \cdot cH) = aH \cdot (bc)H = (abc)H.\]

**Identity:** \(1H \cdot aH = aH = aH \cdot 1H\) for all \(a \in G\).

**Inverses:** \(aH \cdot a^{-1}H = 1H = a^{-1} \cdot aH\) for all \(a \in G\). \(\square\)

**Example.** This is the table for \(D_3\), the group of symmetries of an equilateral triangle. \(r_1\) is rotation through \(\frac{2\pi}{3}\), \(r_2\) is rotation through \(\frac{4\pi}{3}\), and \(m_1\), \(m_2\), and \(m_3\) are reflections through the altitude through vertices 1,
2, and 3, respectively.

\[
\begin{array}{ccccccc}
   & \text{id} & r_1 & r_2 & m_1 & m_2 & m_3 \\
\text{id} & \text{id} & r_1 & r_2 & m_1 & m_2 & m_3 \\
r_1 & r_1 & r_2 & \text{id} & m_2 & m_1 & m_3 \\
r_2 & r_2 & \text{id} & r_1 & m_2 & m_3 & m_1 \\
m_1 & m_1 & m_2 & m_3 & \text{id} & r_1 & r_2 \\
m_2 & m_2 & m_3 & m_1 & r_2 & \text{id} & r_1 \\
m_3 & m_3 & m_1 & m_2 & r_1 & r_2 & \text{id} \\
\end{array}
\]

The rotation subgroup \( H = \{ \text{id}, r_1, r_2 \} \) is a normal subgroup of \( D_3 \). You can check this directly by checking that \( gHg^{-1} \subset H \) for each \( g \in D_3 \). For example,

\[
m_1 H m_1^{-1} = m_1 H m_1 = m_1 [\{ \text{id}, r_1, r_2 \} m_1 = \{ m_1 \text{id} m_1, m_1 r_1 m_1, m_1 r_2 m_1 \} = \{ \text{id}, r_2, r_1 \} = H,
\]

and so on for the other elements.

You can also use the previous example: Since \( H \) has 3 elements, it has index \( \frac{6}{3} = 2 \), so it must be normal.

Finally, you can show it’s normal geometrically, by reasoning about orientation. I’ll do this for \( D_{2n} \) shortly.

In this case, \( D_3/H \) is a group with two elements:

\[
D_3/H = \{ H = \{ \text{id}, \rho_1, \rho_2 \}, m_1 H = \{ m_1, m_2, m_3 \} \}.
\]

For a normal subgroup, every left coset is a right coset: \( gH = Hg \) for all \( g \in G \). This works for \( H = \{ \text{id}, r_1, r_3 \} \); for example,

\[
H m_1 = \{ \text{id} m_1, r_1 m_1, r_3 m_1 \} = \{ m_1, m_3, m_2 \} = m_1 H.
\]

Note that \( \mu_1 H = \mu_2 H = \mu_3 H \) — these are all the same coset.

Here is the group table for \( D_3/H \):

\[
\begin{array}{cc}
   H & m_1 H \\
H & H & m_1 H \\
m_1 H & m_1 H & H \\
\end{array}
\]

Up to notation, this is “the” group of order 2.

(More generally, consider the group \( D_{2n} \) of symmetries of the regular \( n \)-gon. This group has a subgroup of rotations \( H \) consisting of rotations through the angles \( \frac{2\pi k}{n} \), where \( 0 \leq k < n \). This subgroup is normal, since it has index 2. To see this geometrically, observe that if \( \rho \) is a rotation and \( \tau \) is also a rotation, \( \tau \rho \tau^{-1} \) is obviously a rotation. On the other hand, suppose \( \tau \) is a reflection. Then \( \tau \rho \tau^{-1} \) is orientation-preserving, so it must also be a rotation.]

Now consider the subgroup \( H' = \{ \text{id}, m_1 \} \). This subgroup is not normal in \( D_3 \). To prove this, I must find a \( g \in D_3 \) such that \( gH'g^{-1} \neq H' \). Here’s an example:

\[
m_2 \{ \text{id}, m_1 \} m_2^{-1} = m_2 [\{ \text{id}, m_1 \} m_2 = \{ m_2 \text{id} m_2, m_2 m_1 m_2 \} = \{ \text{id}, m_3 \} \neq \{ \text{id}, m_1 \}.
\]

Another way to prove that the subgroup isn’t normal is to compare the left and right cosets. The left cosets are

\[
\{ \text{id}, m_1 \}, m_2 \{ \text{id}, m_1 \} = \{ m_2, r_2 \}, m_3 \{ \text{id}, m_1 \} = \{ m_3, r_1 \}.
\]
The right cosets are
\[ \{\text{id}, m_1\}, \{\text{id}, m_1\} m_2 = \{m_2, r_1\}, \{\text{id}, m_1\} m_3 = \{m_3, r_2\}. \]

As you can see, the left and right cosets are not the same.

Remember that when a subgroup is normal, there is a well-defined multiplication on the set of cosets of the subgroup. Let’s see how this works out for the two subgroup I discussed above.

The first table below is the multiplication table for \(D_3\), the group of symmetries of a triangle. The subgroup \(H = \{\text{id}, r_1, r_2\}\) has two cosets: \(H\) itself and the set \(\{m_1, m_2, m_3\}\). Notice that the row and column headings have been set up with the two cosets one after another.

Get out your coloring pencils! Color the two cosets in the table below in such a way that all the elements of a given coset are the same color, and different cosets have different colors. For example, leave the elements of \(H = \{\text{id}, r_1, r_2\}\) uncolored and color the elements \(\{m_1, m_2, m_3\}\) green.

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>(r_1)</th>
<th>(r_2)</th>
<th>(m_1)</th>
<th>(m_2)</th>
<th>(m_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>id</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>(m_1)</td>
<td>(m_2)</td>
<td>(m_3)</td>
</tr>
<tr>
<td>(r_1)</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>id</td>
<td>(m_3)</td>
<td>(m_1)</td>
<td>(m_2)</td>
</tr>
<tr>
<td>(r_2)</td>
<td>(r_2)</td>
<td>id</td>
<td>(r_1)</td>
<td>(m_2)</td>
<td>(m_3)</td>
<td>(m_1)</td>
</tr>
<tr>
<td>(m_1)</td>
<td>(m_1)</td>
<td>(m_2)</td>
<td>(m_3)</td>
<td>id</td>
<td>(r_1)</td>
<td>(r_2)</td>
</tr>
<tr>
<td>(m_2)</td>
<td>(m_2)</td>
<td>(m_3)</td>
<td>(m_1)</td>
<td>(r_2)</td>
<td>id</td>
<td>(r_1)</td>
</tr>
<tr>
<td>(m_3)</td>
<td>(m_3)</td>
<td>(m_1)</td>
<td>(m_2)</td>
<td>(r_1)</td>
<td>(m_2)</td>
<td>id</td>
</tr>
</tbody>
</table>

Consider the product of two elements \(ab\). The coloring shows that the coset containing the product depends only on the cosets containing \(a\) and \(b\). Suppose \(ab\) is in the coset colored green. Take \(a'\) in the same coset as \(a\) and \(b'\) in the same coset as \(b\). Then \(a'b'\) will also be in the coset colored green. This proves that you can multiply cosets by multiplying coset representatives and get a well-defined multiplication.

Here is the same table rearranged to fit the subgroup \(H' = \{\text{id}, m_1\}\) and its cosets \(r_1 H' = \{r_1, m_3\}\) and \(r_2 H' = \{r_2, m_2\}\). Color the elements of the three cosets with different colors as in the last example.

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>(m_1)</th>
<th>(r_1)</th>
<th>(m_3)</th>
<th>(r_2)</th>
<th>(m_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>id</td>
<td>(m_1)</td>
<td>(r_1)</td>
<td>(m_3)</td>
<td>(r_2)</td>
<td>(m_2)</td>
</tr>
<tr>
<td>(m_1)</td>
<td>(m_1)</td>
<td>id</td>
<td>(m_2)</td>
<td>(r_2)</td>
<td>(m_3)</td>
<td>(r_1)</td>
</tr>
<tr>
<td>(r_1)</td>
<td>(r_1)</td>
<td>(m_3)</td>
<td>(r_2)</td>
<td>(m_2)</td>
<td>id</td>
<td>(m_1)</td>
</tr>
<tr>
<td>(m_3)</td>
<td>(m_3)</td>
<td>(r_1)</td>
<td>(m_1)</td>
<td>(id)</td>
<td>(m_2)</td>
<td>(r_2)</td>
</tr>
<tr>
<td>(r_2)</td>
<td>(r_2)</td>
<td>(m_2)</td>
<td>(id)</td>
<td>(m_1)</td>
<td>(r_1)</td>
<td>(m_3)</td>
</tr>
<tr>
<td>(m_2)</td>
<td>(m_2)</td>
<td>(r_2)</td>
<td>(m_3)</td>
<td>(r_1)</td>
<td>(m_1)</td>
<td>id</td>
</tr>
</tbody>
</table>

In this case, the coset containing a product \(a \cdot b\) depends on the particular elements \(a\) and \(b\), not just on the cosets containing \(a\) and \(b\). The coloring produces a table that is not arranged in nice “blocks” like the previous table. For example, \(r_1 \cdot r_1 = r_2\), which is in the third coset. On the other hand, \(m_3 \cdot m_3 = \text{id}\), which is in the first coset. You get different cosets, even though the factors in the two products are all in the second coset. In this case, coset multiplication by multiplication of representatives is not well-defined.

It is natural to see how a new construction interacts with things like unions and intersections. Since the union of subgroups is not a subgroup in general, it’s unreasonable to expect a union of normal subgroups to be a normal subgroup. However, intersections work properly.
Lemma. The intersection of a family of normal subgroups is a normal subgroup.

Proof. Let $G$ be a group, and let $\{H_a\}_{a \in A}$ be a family of normal subgroups of $G$. Let $H = \cap_{a \in A} H_a$. I want to show that $H \triangleleft G$. Since the intersection of a family of subgroups is a subgroup, it remains to show that $H$ is normal.

Let $g \in G$ and let $h \in H$. I must show $ghg^{-1} \in H$. Now $h \in H$ implies $h \in H_a$ for all $a$, so (since $H_a \triangleleft G$ for all $a$) $ghg^{-1} \in H_a$ for all $a$. Therefore, $ghg^{-1} \in \cap_{a \in A} H_a = H$. Therefore, $H$ is normal. □

Definition. Let $G$ be a group, and let $S \subseteq G$. The intersection of all normal subgroups of $G$ containing $S$ is the normal subgroup generated by $S$.

Lemma. Let $\phi : G \to H$ be a group homomorphism.

(a) $\ker \phi \triangleleft G$.

(b) If $H' \triangleleft H$, then $\phi^{-1}(H') \triangleleft G$.

Proof. (a) I showed earlier that $\ker \phi$ is a subgroup of $G$. So I only need to show that $\ker \phi$ is normal. Let $a \in \ker \phi$ (so $\phi(a) = 1$) and let $g \in G$. I need to show that $gag^{-1} \in \ker \phi$.

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1.$$  

Hence, $gag^{-1} \in \ker \phi$, and $\ker \phi \triangleleft G$.

(b) I showed earlier that $\phi^{-1}(H')$ is a subgroup of $G$. I only need to show that if $H'$ is normal in $H$, then $\phi^{-1}(H')$ is normal in $G$.

Let $a \in \phi^{-1}(H')$, so $\phi(a) \in H'$, and let $g \in G$. I must show that $gag^{-1} \in \phi^{-1}(H')$. Apply $\phi$ and see if it winds up in $H'$.

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in \phi(g)H'\phi(g)^{-1} \subseteq H'.$$

(The last inclusion follows from normality of $H'$.) Hence, $gag^{-1} \in \phi^{-1}(H')$, and $\phi^{-1}(H') \triangleleft G$. □

Remark. It’s not true in general that the image of a normal subgroup is normal. It is true if the map is a surjection. (Try it yourself!) □

Let $H \triangleleft G$. Then $G/H$ becomes a group under coset multiplication. Define the quotient map (or canonical projection) $\pi : G \to G/H$ by

$$\pi(g) = gH.$$  

It’s easy to verify that $\pi$ is a homomorphism: If $a, b \in G$, then

$$\pi(ab) = (ab)H = aH \cdot bH = \pi(a)\pi(b).$$

Obviously, if $gH \in G/H$, then $\pi(g) = gH$. Hence, $\pi$ is surjective.

Finally, I claim that $\ker \pi = H$. If $h \in H$, then $\pi(h) = hH = H$, and $H$ is the identity in $G/H$. Therefore, $h \in \ker \pi$, i.e. $H \subseteq \ker \pi$.

Conversely, suppose $g \in \ker \pi$. Then $\pi(g) = H$, so $gH = H$, so $g \in H$. Therefore, $\ker \pi \subseteq H$, and hence $H = \ker \pi$.

To summarize:

- If $H \triangleleft G$, the quotient map $\pi : G \to G/H$ is a surjective homomorphism with kernel $H$.

In other words, every normal subgroup is the kernel of a homomorphism (namely the canonical projection onto the quotient). On the other hand, the kernel of a homomorphism is a normal subgroup. Hence:

- Normal subgroups are exactly the kernels of group homomorphisms.
Normality was defined with the idea of imposing a condition on subgroups which would make the set of cosets into a group. Now an apparently independent notion — that of a homomorphism — gives rise to the same idea! This strongly suggests that the definition of a normal subgroup was a good one.

You can think of quotient groups in an even more subtle way. The general theme is something like this. In modern mathematics, it is important to study not only objects — like groups — but the maps between objects — in this case, group homomorphisms. The maps, after all, describe the relationships between different objects. (This theme is elaborated in a branch of mathematics called category theory.)

It turns out that more is true. In a sense, the maps carry all of the information about the objects; one could even be perverse and “build up” objects out of maps! I won’t go to such extremes, but in some cases, an object can be characterized by certain maps. Here’s an important example.

**Theorem. (Universal Property of the Quotient)** Let \( H \triangleleft G \), and let \( \phi : G \to K \) be a group homomorphism such that \( H \subseteq \ker \phi \). Then there is a unique homomorphism \( \tilde{\phi} : G/H \to K \) such that the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{\pi} & G/H \\
\downarrow \phi & & \downarrow \tilde{\phi} \\
K & & K
\end{array}
\]

(To say that the diagram commutes means that \( \tilde{\phi} \cdot \pi = \phi \).)

**Proof.** Define \( \tilde{\phi} : G/H \to K \) by

\[
\tilde{\phi}(gH) = \phi(g).
\]

This is forced by the requirement that \( \tilde{\phi} \pi = \phi \), since plugging \( g \in G \) into both sides yields \( \tilde{\phi} \pi(g) = \phi(g) \), or \( \tilde{\phi}(gH) = \phi(g) \).

I need to check that this map is well-defined. The point is that a given coset \( gH \) may in general be written as \( g'H \), where \( g \neq g' \). I must verify that the result \( \phi(g) \) or \( \phi(g') \) is the same regardless of how I write the coset.

(If \( \phi(g) \neq \phi(g') \) in this situation, then a single input — the coset \( gH = g'H \) — produces different outputs, which contradicts what it means to be a function.)

Suppose then that \( gH = g'H \), so \( g = g'h \) for some \( h \in H \).

\[
\tilde{\phi}(gH) = \phi(g) = \phi(g'h) = \phi(g') \phi(h) = \phi(g') \cdot 1 = \phi(g') = \tilde{\phi}(g'H).
\]

This shows that \( \tilde{\phi} \) is indeed well-defined.

I was forced to define \( \tilde{\phi} \) as I did in order to make the diagram commute. Hence, \( \tilde{\phi} \) is unique.

Now I’ll show that \( \tilde{\phi} \) is a homomorphism. Let \( a, b \in G \). Then

\[
\tilde{\phi}((aH)(bH)) = \tilde{\phi}((ab)H) = \phi(ab) = \phi(a) \phi(b) = \tilde{\phi}(aH) \tilde{\phi}(bH).
\]

Therefore, \( \tilde{\phi} \) is a homomorphism. \( \Box \)

The universal property of the quotient is an important tool in constructing group maps.
• To define a map out of a quotient group \( G/H \), define a map out of \( G \) which maps \( H \) to 1.

\[
\begin{array}{c}
G \\
\downarrow \\
H
\end{array}
\quad 
\begin{array}{c}
G' \\
\downarrow \\
1
\end{array}
\]

\[ \varphi \]

The map you construct goes from \( G \) to \( G' \); the universal property automatically constructs a map \( G/H \to G' \) for you. The advantage of using the universal property rather than defining a map out of \( G/H \) directly is that you don’t repeat the verification that the map is well-defined — it’s been done once and for all in the proof above.

Should you ever need to know how the magic map \( \tilde{\varphi} \) is defined, refer to the proof (and the commutativity of the diagram).

**Remarks.**

1. Many other constructions are characterized by universal properties. In each case, one finds that the appropriate conditions imply the existence of a unique map with certain properties.

2. The use of diagrams of maps — particularly commutative ones — is pervasive in modern mathematics. They are a powerful language, and another outgrowth of the categorical point of view. In general, one says a diagram commutes if following the “paths” indicated by the arrows (maps) in different ways between two objects produces the same result. For example, to say that

\[
\begin{array}{c}
A \\
\downarrow \\
C
\end{array}
\quad 
\begin{array}{c}
B \\
\downarrow \\
D
\end{array}
\]

\[ f \quad g \quad i \quad h \]

commutes means that \( h \cdot f = i \cdot g \).

**Example.** To illustrate how the universal property is used, suppose you wanted to construct a homomorphism from the quotient group \( \mathbb{Z} \times \mathbb{Z} / \langle (5, 2) \rangle \) to \( \mathbb{Z} \). How would you do it?

The universal property tells me to construct a group map from \( \mathbb{Z} \times \mathbb{Z} \) to \( \mathbb{Z} \) which contains \( \langle (5, 2) \rangle \) in its kernel — that is, which sends \( \langle (5, 2) \rangle \) to 0. Now \( \langle (5, 2) \rangle \) consists of all multiples of \( (5, 2) \), so what I’m looking for is a group map which sends \( (5, 2) \) to 0.

To ensure that what I get is a group map, I should probably guess a linear function — something like

\[ f(x, y) = ax + by. \]

If \( f(5, 2) = 0 \), then \( 5a + 2b = 0 \). There is no question of solving this equation for \( a \) and \( b \), since there is one equation and two variables. But I just need some \( a \) and \( b \) that work — and one “obvious” way to do this is to set \( a = 2 \) and \( b = -5 \), since

\[ 5(2) + 2(-5) = 0. \]
Theorem. (The First Isomorphism Theorem) Let $\phi : G \to H$ be a group map, and let $\pi : G \to G/\ker \phi$ be the quotient map. There is an isomorphism $\tilde{\phi} : G/\ker \phi \to \text{im } \phi$ such that the following diagram commutes:

$$
\begin{array}{ccc}
G & \xrightarrow{\pi} & G/\ker \phi \\
\downarrow & & \downarrow \tilde{\phi} \\
& \text{im } \phi & \\
\end{array}
$$
**Proof.** Since \( \phi \) maps \( G \) onto \( \text{im} \) \( \phi \) and \( \ker \phi \subset \ker \phi \), the universal property of the quotient yields a map \( \hat{\phi} : G / \ker \phi \to \text{im} \hat{\phi} \) such that the diagram above commutes. Since \( \phi \) is onto, so is \( \hat{\phi} \); in fact, if \( \hat{\phi}(g) \in \text{im} \hat{\phi} \), by commutativity \( \hat{\phi}(\pi(g)) = \phi(g) \).

It remains to show that \( \hat{\phi} \) is injective.

By the previous lemma, it suffices to show that \( \ker \hat{\phi} = \{1\} \). Since \( \hat{\phi} \) maps out of \( G / \ker \phi \), the “1” here is the identity element of the group \( G / \ker \phi \), which is the subgroup \( \ker \phi \). So I need to show that \( \ker \hat{\phi} = \{\ker \phi\} \).

However, this follows immediately from commutativity of the diagram. For \( g \ker \phi \in \ker \hat{\phi} \) if and only if \( \hat{\phi}(g \ker \phi) = 1 \). This is equivalent to \( \hat{\phi}(\pi(g)) = 1 \), or \( \phi(g) = 1 \), or \( g \in \ker \phi \) — i.e. \( \ker \hat{\phi} = \{\ker \phi\} \). \( \Box \)

---

**Example.** Use the First Isomorphism Theorem to prove that

\[
\mathbb{R}^* / \{1, -1\} \cong \mathbb{R}^+.
\]

\( \mathbb{R}^* \) is the group of nonzero real numbers under multiplication. \( \mathbb{R}^+ \) is the group of positive real numbers under multiplication. \( \{1, -1\} \) is the group consisting of 1 and \(-1\) under multiplication (it’s isomorphic to \( \mathbb{Z}_2 \)).

I’ll define a group map from \( \mathbb{R}^* \) onto \( \mathbb{R}^+ \) whose kernel is \( \{1, -1\} \).

Define \( \phi : \mathbb{R}^* \to \mathbb{R}^+ \) by

\[
\phi(x) = |x|.
\]

Since

\[
\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y),
\]

\( \phi \) is a group map. If \( z \in \mathbb{R}^+ \) is a positive real number, then

\[
\phi(z) = |z| = z \quad \text{since } z \text{ is positive.}
\]

Therefore, \( \phi \) is surjective: \( \text{im} \phi = \mathbb{R}^+ \).

Finally, \( \phi \) clearly sends 1 and \(-1\) to the identity \( 1 \in \mathbb{R}^+ \), and those are the only two elements of \( \mathbb{R}^* \) which map to 1. Therefore, \( \ker \phi = \{1, -1\} \).

By the First Isomorphism Theorem,

\[
\mathbb{R}^* / \{1, -1\} = \mathbb{R}^* / \ker \phi \cong \text{im} \phi \cong \mathbb{R}^+.
\]

Note that I didn’t construct a map \( \mathbb{R}^* / \{1, -1\} \to \mathbb{R}^+ \) explicitly; the First Isomorphism Theorem constructs the isomorphism for me. \( \Box \)

---

**Example.** Define \( \phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) by

\[
\phi(m, n) = m - 3n.
\]

\( \phi \) is a homomorphism:

\[
\phi[(m_1, n_1) + (m_2, n_2)] = \phi(m_1 + m_2, n_1 + n_2) = (m_1 + m_2) - 3(n_1 + n_2) = (m_1 - 3n_1) + (m_2 - 3n_2) = \phi(m_1, n_1) + \phi(m_2, n_2).
\]

\( \text{im} \phi \subset \mathbb{Z} \), because \( \phi(m, 0) = m \) for all \( m \in \mathbb{Z} \).

\( \ker \phi = \langle (3, 1) \rangle \). First,

\[
\phi[k \cdot (3, 1)] = \phi(3k, k) = 3k - 3k = 0.
\]

12
Thus, \( \langle (3, 1) \rangle \subseteq \ker \phi \).

Conversely, if \((m, n) \in \ker \phi\), then \(\phi(m, n) = 0\), so \(m - 3n = 0\), or \(m = 3n\). Then \((m, n) = (3n, n) = n \cdot (3, 1)\), and the latter is an element of \(\langle (3, 1) \rangle \). Thus, \(\ker \phi \subseteq \langle (3, 1) \rangle\), so \(\ker \phi = \langle (3, 1) \rangle\).

Hence, the First Isomorphism Theorem says that

\[
\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (3, 1) \rangle} \cong \mathbb{Z}.
\]

A coset of \(\langle (3, 1) \rangle\) in \(\mathbb{Z} \times \mathbb{Z}\) consists of the lattice points on the line \(y = \frac{1}{3}x + \frac{1}{3}n\). The isomorphism essentially maps this coset to the \(x\)-intercept \(-n \in \mathbb{Z}\).

For example, consider the point \((2, 1) \in \mathbb{Z} \times \mathbb{Z}\). Since

\[
(2, 1) - (3, 1) = (-1, 0),
\]

\((2, 1)\) and \((-1, 0)\) are in the same coset of \(\langle (3, 1) \rangle\).

![Graph showing lattice points and line through points (2,1) and (-1,0).]

What is the line through \((2, 1)\) and \((-1, 0)\)? It has slope \(\frac{1}{3}\), so its equation is

\[
y = \frac{1}{3}(x + 1) = \frac{1}{3}x + \frac{1}{3}.
\]

The \(x\)-intercept is \(-1\) — and sure enough,

\[
\phi(2, 1) = 2 - 3 \cdot 1 = -1. \quad \Box
\]

**Lemma.** If \(\phi : G \to H\) is a surjective group map and \(K \triangleleft G\), then \(\phi(K) \triangleleft H\).

**Proof.** \(1 \in K\), so \(1 = \phi(1) \in \phi(K)\), and \(\phi(K) \neq \emptyset\).

Let \(a, b \in K\), so \(\phi(a), \phi(b) \in \phi(K)\). Then

\[
\phi(a) \phi(b)^{-1} = \phi(a) \phi(b^{-1}) = \phi(ab^{-1}) \in \phi(K), \text{ since } ab^{-1} \in K.
\]

Therefore, \(\phi(K)\) is a subgroup.

(Notice that this does not use the fact that \(K\) is normal. Hence, I’ve actually proved that the image of a subgroup is a subgroup.)

Now let \(h \in H, a \in K\), so \(\phi(a) \in \phi(K)\). I want to show that \(h \phi(a) h^{-1} \in \phi(K)\). Since \(\phi\) is surjective, \(h = \phi(g)\) for some \(g \in G\). Then

\[
h \phi(a) h^{-1} = \phi(g) \phi(a) \phi(g)^{-1} = \phi(gag^{-1}).
\]
But $gag^{-1} \in K$ because $K$ is normal. Hence, $\phi(gag^{-1}) \in \phi(K)$. It follows that $\phi(K)$ is a normal subgroup of $H$. \[\square\]

**Theorem. (The Second Isomorphism Theorem)** Let $K, H \triangleleft G$, $K < H$. Then

$$\frac{G}{K} \cong \frac{G/H}{K}.$$ 

**Proof.** Note that a typical element of the left side looks like $(gK)(H/K)$, where $g \in G$.

If $\phi : G \to G/K$ is the quotient map, $\phi(H) = H/K$. Since $H \triangleleft G$, it follows that $H/K \triangleleft G/K$, by the preceding lemma. Therefore, the left side really is a quotient group!

I will construct maps going both ways which are inverses. The construction will make heavy use of the Universal Property of the Quotient.

First, the quotient map $\pi : G \to G/H$ sends $K < H$ to the identity. By the Universal Property of the Quotient, there is an induced map $\phi : G/K \to G/H$ defined by

$$\phi(gK) = gH.$$ 

Now if $g \in H$, then $\phi(gK) = gH = H$, which is the identity coset in $G/H$. Since $\phi$ kills $H$, the Universal Property of the Quotient implies the existence of a map $\psi : (G/K)/(H/K) \to G/H$ defined by

$$\psi[(gK)(H/K)] = gH.$$ 

Thus, I've constructed a map from the left side to the right side.

Next, consider the composite $\sigma : G \to G/K \to (G/K)/(H/K)$ made up of two quotient maps. It is $\sigma(g) = (gK)(H/K)$. If $g \in H$, then $\sigma(g) = (gK)(H/K) = H/K$, which is the identity coset in $(G/K)/(H/K)$. Hence, $\sigma$ kills $H$, and the Universal Property of the Quotient implies the existence of a map $\tau : G/H \to (G/K)/(H/K)$ given by

$$\tau(gH) = (gK)(H/K).$$ 

Now I have a map from the right side to the left side.

$\psi$ and $\tau$ are visibly inverses, so they are isomorphisms. \[\square\]

Notice the ease with which the Universal Property of the Quotient allowed me to construct the maps. Nowhere did I need to check that a map was well defined, or that a map was a homomorphism! All the work was done in the proof of the Universal Property.

There is a Third Isomorphism Theorem (sometimes called the Modular Isomorphism, or the Noether Isomorphism). It asserts that if $H < G$ and $K \triangleleft G$, then

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$