Normal Subgroups and Quotient Groups

- A subgroup $H < G$ is **normal** if $gHg^{-1} \subset H$ for all $g \in G$. Notation: $H \triangleleft G$.
- Every subgroup of an abelian group is normal. Every subgroup of index 2 is normal.
- If $H \triangleleft G$, the set $G/H$ of left cosets becomes a group under **coset multiplication**: $(aH)(bH) = (ab)H$. In this case, $G/H$ is the **quotient group** (or **factor group**) of $G$ by $H$.
- The kernel of a group map is a normal subgroup. The image of a normal subgroup is a normal subgroup, provided that the group map is surjective.

What condition on a subgroup $H$ will make set of cosets $G/H$ into a group?

**Example. (Adding cosets)** 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

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

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 
\[
\{0, 4\} \text{ with } 0, \quad \{1, 5\} \text{ with } 1, \quad \{2, 6\} \text{ with } 2, \quad \text{ and } \{3, 7\} \text{ with } 3,
\]
you get this table:

\[
\begin{array}{cccc}
+ & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

Thus, \( \mathbb{Z}_{8/\{0, 4\}} \cong \mathbb{Z}_4 \). ❍

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:

(a) \( a \) and \( b \) are elements of the same coset of \( H \).

(b) \( aH = bH \).

(c) \( b^{-1}a \in H \).

**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 (a) implies statement (b), statement (b) implies statement (c), and statement (c) implies statement (a).

((a) \( \Rightarrow \) (b)) 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, \( aH = bH \).

((b) \( \Rightarrow \) (c)) 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, \( b^{-1}a = h \in H \).

((c) \( \Rightarrow \) (a)) 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

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

(Since the statement runs over all \(g \in G\), I could just as well say “\(g^{-1}Hg \subset H\”).) The notation \(H \trianglelefteq G\) means that \(H\) is a normal subgroup of \(G\).

To check that one set is contained in another, you can check that every element of the first set is contained in the second. In this case, \(H \trianglelefteq G\) means that if \(g \in G\) and \(h \in H\), then \(ghg^{-1} \in H\).

**Example.** (The trivial subgroup and the whole group are normal) If \(G\) is a group, \(\{1\}\) and \(G\) are normal in \(G\).

To show that \(\{1\}\) is normal, let \(g \in G\). The only element of \(\{1\}\) is 1, and \(g \cdot 1 \cdot g^{-1} = 1 \in \{1\}\). Therefore, \(\{1\}\) is normal.

To show that \(G\) is normal, let \(g \in G\) and let \(h \in G\). Then \(ghg^{-1} \in G\), because \(g, h, \text{ and } g^{-1}\) are all in \(G\), and \(G\) must be closed under its operation.

**Example.** (Subgroups of abelian groups are normal) If \(G\) is abelian, every subgroup is normal. For if \(g \in G\), then \(ghg^{-1} = HgH^{-1} = H\).

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.** (Showing a subgroup is not normal) Here’s the multiplication table for \(S_3\), the group of permutations of \(\{1, 2, 3\}\).
Consider the subgroup \( H = \{ \text{id}, (1 3) \} \). I'll show that \( H \) is \emph{not} normal. To do this, I have to find an element \( g \in S_3 \) such that
\[
g\{ \text{id}, (1 3) \} g^{-1} \not\subset \{ \text{id}, (1 3) \}.
\]
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. (A normal subgroup of the quaternions) Consider the group of the quaternions:

\[
\begin{array}{cccccccc}
1 & -1 & i & -i & j & -j & k & -k \\
1 & 1 & -1 & i & -i & j & -j & k \\
-1 & -1 & 1 & -i & i & -j & j & -k \\
i & i & -i & 1 & -1 & -k & k & j \\
i & -i & i & 1 & -1 & k & -k & j \\
j & j & -j & -k & k & -1 & 1 & i \\
j & -j & j & k & -k & 1 & -1 & -i \\
k & k & -k & j & -j & -i & 1 & 1 \\
k & -k & k & -j & j & i & -i & 1 \\
\end{array}
\]

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.

Example. (Subgroups of index 2 are normal) 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.

Example. (Checking normality in a product) Let \( G \) and \( H \) be groups. Let

\[
G \times \{ 1 \} = \{ (g,1) \mid g \in G \}.
\]
Prove that \( G \times \{1\} \) 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.** \((\Leftarrow)\) 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, \( gHg^{-1} = H \). \(\Box\)

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, \( H \triangleleft G \). The following statements are equivalent:

(a) \( H \triangleleft G \)

(b) For all \( g \in G \), \( gH = Hg \). (Thus, every left coset is a right coset and every right coset is a left coset.)

(c) Coset multiplication is well-defined.

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

\((b) \Rightarrow (c))\) Suppose \( gH = Hg \) for all \( g \in G \). Suppose

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

Then

\[
a_1b_1H = a_1b_2H = a_1Hb_2 = a_2Hb_2 = a_2b_2H.
\]
Suppose coset multiplication is well defined. I want to show \( H \trianglelefteq G \). Let \( g \in G \). I will show \( gHg^{-1} \subset H \).

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

By an earlier corollary, \( hH = H \), and surely \( gH = gH \), so (since coset multiplication is well-defined) \( ghH = gH \). 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, \( H \trianglelefteq G \).

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

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

**Proof.** I’ll check that axioms. For associativity, note that
\[
(aH \cdot bH) \cdot cH = (ab)H \cdot cH = (abc)H \quad \text{and} \quad aH \cdot (bH \cdot cH) = aH \cdot (bc)H = (abc)H.
\]
I have
\[
1H \cdot aH = aH = aH \cdot 1H \quad \text{for all} \quad a \in G.
\]
Hence, \( H = 1H \) is the identity for coset multiplication.
Finally
\[
aH \cdot a^{-1}H = 1H = a^{-1} \cdot aH \quad \text{for all} \quad a \in G.
\]
Therefore, \( (aH)^{-1} = a^{-1}H \), and every coset has an inverse. \( \square \)

**Definition.** Let \( G \) be a group, and let \( H \trianglelefteq G \). The set \( G/H \) of left cosets under coset multiplication is the quotient group (or factor group) of \( G \) by \( H \).

Because coset multiplication (or addition) is independent of the choice of representatives, you do computations in quotient groups by doing the corresponding computations on coset representatives. The next two examples illustrate this idea.

**Example.** The cosets of the subgroup \( \langle 19 \rangle \) in \( U_{20} \) are
\[
\langle 19 \rangle = \{1, 19\} \\
3 \cdot \langle 19 \rangle = \{3, 17\} \\
7 \cdot \langle 19 \rangle = \{7, 13\} \\
9 \cdot \langle 19 \rangle = \{9, 11\}
\]

(a) Compute \( \{3, 17\} \cdot \{9, 11\} \).

Take an element (it doesn’t matter which one) from each coset, say \( 3 \in \{3, 17\} \) and \( 11 \in \{9, 11\} \).
Perform the operation on the elements you chose. In this case, it’s multiplication:
\[
3 \cdot 11 = 33 = 13.
\]
Find the coset containing the answer: \( 13 \in \{7, 13\} \).
Hence,
\[
\{3, 17\} \cdot \{9, 11\} = \{7, 13\}. \quad \square
\]
(b) Compute \( \{3, 17\}^{-1} \).

Take an element (it doesn’t matter which one) from the coset, say \( 3 \in \{3, 17\} \).
Perform the operation on the elements you chose. In this case, it’s finding the inverse (use the Extended Euclidean Algorithm, or trial and error):
\[
3^{-1} = 7.
\]
Find the coset containing the answer: \( 7 \in \{7, 13\} \).
Hence,
\[
\{3, 17\}^{-1} = \{7, 13\}. \quad \square
\]

(c) Compute \( \{9, 11\}^3 \).

Take an element (it doesn’t matter which one) from the coset, say \( 11 \in \{9, 11\} \).
Perform the operation on the elements you chose. In this case, it’s cubing:
\[
11^3 = 1331 = 11.
\]

Find the coset containing the answer: \( 11 \in \{9, 11\} \).
Hence,
\[
\{9, 11\}^3 = \{9, 11\}. \quad \square
\]

(d) Construct a multiplication table for the quotient group \( \frac{U_{20}}{\langle 19 \rangle} \). Determine whether the quotient group is isomorphic to \( \mathbb{Z}_4 \) or to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

To save writing, I’ll use \( 1, 3, 7, \) and \( 9 \) to represent the cosets. I did the multiplications to construct the table the way I did the multiplication in (a) above.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>7</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>1</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

I can see that \( \{3, 17\} \) has order 4. Therefore, \( \frac{U_{20}}{\langle 19 \rangle} \approx \mathbb{Z}_4 \). \( \square \)

**Example.** The cosets of \( \langle (1, 3) \rangle \) in \( \mathbb{Z}_4 \times \mathbb{Z}_4 \) are
\[
\langle (1, 3) \rangle = \{(0, 0), (1, 3), (2, 2), (3, 1)\}
\]
\[
(0, 1) + \langle (1, 3) \rangle = \{(0, 1), (1, 0), (2, 3), (3, 2)\}
\]
\[
(0, 2) + \langle (1, 3) \rangle = \{(0, 2), (1, 1), (2, 0), (3, 3)\}
\]
\[
(0, 3) + \langle (1, 3) \rangle = \{(0, 3), (1, 2), (2, 1), (3, 0)\}
\]

(a) Compute \([0, 2] + \langle (1, 3) \rangle + [0, 3] + \langle (1, 3) \rangle \).

Take an element (it doesn’t matter which one) from the cosets, say \((0, 2) \in (0, 2) + \langle (1, 3) \rangle \) and \((0, 3) \in (0, 3) + \langle (1, 3) \rangle \). (I’ll just use the coset representatives, but again, I could choose any elements from the two cosets.)
Perform the operation on the elements you chose. In this case, it’s addition:
\[
(0, 2) + (0, 3) = (0, 1).
\]
Find the coset containing the answer:
\[
(0, 1) \in \{(0, 1), (1, 0), (2, 3), (3, 2)\} = (0, 1) + \langle (1, 3) \rangle.
\]
Hence,
\[
[0, 2] + \langle (1, 3) \rangle + [0, 3] + \langle (1, 3) \rangle = (0, 1) + \langle (1, 3) \rangle. \quad \square
\]
(b) Construct an addition table for the quotient group \( \mathbb{Z}_4 \times \mathbb{Z}_4 \langle (1, 3) \rangle \). Determine whether the quotient group is isomorphic to \( \mathbb{Z}_4 \) or to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

To save writing, I’ll use \((0,0), (0,1), (0,2), \) and \((0,3)\) to represent the cosets. I did the additions to construct the table the way I did the addition in (a) above.

<table>
<thead>
<tr>
<th></th>
<th>(0,0)</th>
<th>(0,1)</th>
<th>(0,2)</th>
<th>(0,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(0,3)</td>
</tr>
<tr>
<td>(0,1)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(0,3)</td>
<td>(0,0)</td>
</tr>
<tr>
<td>(0,2)</td>
<td>(0,2)</td>
<td>(0,3)</td>
<td>(0,0)</td>
<td>(0,1)</td>
</tr>
<tr>
<td>(0,3)</td>
<td>(0,3)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
</tr>
</tbody>
</table>

I can see that \((0,1) + \langle (1, 3) \rangle\) has order 4, so \( \mathbb{Z}_4 \times \mathbb{Z}_4 \langle (1, 3) \rangle \approx \mathbb{Z}_4 \) .

Example. (A quotient group of a dihedral group) 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.

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

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,

\[ m_1HM_1^{-1} = m_1Hm_1 = m_1\{\text{id}, r_1, r_2\}m_1 = \{m_1 \text{id} m_1, m_1r_1m_1, m_1r_2m_1\} = \{\text{id}, r_2, r_1\} = H, \]

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:

\[ D_3/H = \{H = \{\text{id}, r_1, r_2\}, m_1H = \{m_1, m_2, m_3\}\}. \]

For a normal subgroup, every left coset is a right coset: \( gH = Hg \) for all \( g \in G \). This works for \( H = \{\text{id}, r_1, r_2\} \); for example,

\[ Hm_1 = \{\text{id} m_1, r_1m_1, r_2m_1\} = \{m_1, m_3, m_2\} = m_1H. \]

Note that \( \mu_1H = \mu_2H = \mu_3H \) — these are all the same coset.
Here is the group table for $D_3/H$:

<table>
<thead>
<tr>
<th></th>
<th>$H$</th>
<th>$m_1H$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$H$</td>
<td>$m_1H$</td>
</tr>
<tr>
<td>$m_1H$</td>
<td>$m_1H$</td>
<td>$H$</td>
</tr>
</tbody>
</table>

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:

$$m_2\{\text{id}, m_1\}m_2^{-1} = m_2\{\text{id}, m_1\}m_2 = \{m_2\text{id}m_2, m_2m_1m_2\} = \{\text{id}, m_3\} \neq \{\text{id}, m_1\}.$$  

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>$r_2$</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 \( g h g^{-1} \in H \). Now \( h \in H \) implies \( h \in H_a \) for all \( a \), so (since \( H_a \triangleleft G \) for all \( a \)) \( g h g^{-1} \in H_a \) for all \( a \). Therefore, \( g h g^{-1} \in \cap_{a \in A} H_a = H \). 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 \( S \)**.

Why are normal subgroups and quotient groups important? The idea is that you might be able to understand groups by taking them apart into pieces, the way that you can factor a positive integer into a product of primes. If you’re trying to understand a group \( G \), you try to find a normal subgroup \( H \). This allows you to decompose \( G \) into smaller groups \( H \) and \( G/H \). Now you try to find normal subgroups of \( H \) and of \( G/H \), and you keep going.

At some point, you may be unable to find any normal subgroups (other than \( \{1\} \) and the group itself).

**Definition.** A group \( G \) is **simple** if its only normal subgroups are \( \{1\} \) and \( G \).

Thus, simple groups are to groups as prime numbers are to positive integers.

**Example.** (Cyclic groups of prime order are simple) If \( p \) is a prime number, then \( \mathbb{Z}_p \) is simple. The order of a subgroup must divide the order of the group (by Lagrange’s theorem), and the only positive divisors of \( p \) are 1 and \( p \). Therefore, the only subgroups — and hence the only normal subgroups — are \( \{0\} \) and \( \mathbb{Z}_p \).
The hope is that if you know all the possible simple groups, and you know all the ways of putting them together, then you’ll know all about groups. In its complete generality, this ideal is unattainable. However, progress has been made in this endeavor for finite groups. The finite simple groups were completely classified around 1980; estimates suggested that the complete proof (pieces of which were finished by many people over the course of decades) ran to thousands of pages.

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

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

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

**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 $\ker \phi \trianglelefteq G$.

(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 $\phi^{-1}(H') \trianglelefteq G$.  

**Remarks.**

1. 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!)

2. The lemma above says that kernels of group maps are normal subgroups. In fact, the converse is true, and I’ll prove it later: Every normal subgroup is the kernel of a group map.  

©2014 by Bruce Ikenaga