19

Introduction to Cosets

This chapter introduces a new object called a *coset*, which is obtained by taking a subgroup of a group and multiplying each element of the subgroup by a fixed element. In fact, cosets made a surreptitious appearance in Chapter 18, although they were disguised enough that you likely did not notice them. Despite their relatively simply construction, cosets play a powerful role in group theory. We will use them to prove *Lagrange's theorem* in the next chapter. Cosets will also be used to create a new type of a group called a *quotient group*, which will be the primary focus of the rest of this unit.

19.1 Multiplicative group example

Example 19.1. Consider the multiplicative group $U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ and its subgroup $H = \{1, 3, 9\}$. Choose an element $6 \in U_{13}$. Then the *coset* $6H$ is obtained by multiplying each element of H by 6; i.e., $6H = \{6\cdot 1, 6\cdot 3, 6\cdot 9\} = \{6, 5, 2\}$.

Just as we found $6H$, let's compute the coset aH for each $a \in U_{13}$. Since there are 12 elements in U_{13}, we would expect to obtain 12 cosets:

$$1H = \{1\cdot 1, 1\cdot 3, 1\cdot 9\} = \{1, 3, 9\}, \qquad 7H = \{7\cdot 1, 7\cdot 3, 7\cdot 9\} = \{7, 8, 11\},$$
$$2H = \{2\cdot 1, 2\cdot 3, 2\cdot 9\} = \{2, 6, 5\}, \qquad 8H = \{8\cdot 1, 8\cdot 3, 8\cdot 9\} = \{8, 11, 7\},$$
$$3H = \{3\cdot 1, 3\cdot 3, 3\cdot 9\} = \{3, 9, 1\}, \qquad 9H = \{9\cdot 1, 9\cdot 3, 9\cdot 9\} = \{9, 1, 3\},$$
$$4H = \{4\cdot 1, 4\cdot 3, 4\cdot 9\} = \{4, 12, 10\}, \qquad 10H = \{10\cdot 1, 10\cdot 3, 10\cdot 9\} = \{10, 4, 12\},$$
$$5H = \{5\cdot 1, 5\cdot 3, 5\cdot 9\} = \{5, 2, 6\}, \qquad 11H = \{11\cdot 1, 11\cdot 3, 11\cdot 9\} = \{11, 7, 8\},$$
$$6H = \{6\cdot 1, 6\cdot 3, 6\cdot 9\} = \{6, 5, 2\}, \qquad 12H = \{12\cdot 1, 12\cdot 3, 12\cdot 9\} = \{12, 10, 4\}.$$

There are several duplicates in this list of cosets. Recall that in a set, the order in which the elements are listed does *not* matter. For instance, $4H = \{4, 12, 10\}$, $10H = \{10, 4, 12\}$, and $12H = \{12, 10, 4\}$ are the same set, because they all contain the same elements. More generally, these duplicates occur because the cosets aH and bH can be equal (i.e., they contain the same elements) even when $a \neq b$. For instance, we have $4H = 10H = 12H$, even though 4, 10, and 12 are distinct elements in U_{13}.

Consolidating the duplicates, there are only four *distinct* cosets within the above list:

- $1H = \ 3H = \ 9H = \{1, \ 3, \ 9\}$ (original subgroup).
- $2H = \ 5H = \ 6H = \{2, \ 5, \ 6\}$.
- $4H = 10H = 12H = \{4, 10, 12\}$.
- $7H = \ 8H = 11H = \{7, \ 8, 11\}$.

Aside from the original subgroup (i.e., $1H = 3H = 9H$), none of the other cosets are subgroups of U_{13}. In an exercise, you'll describe which properties of a subgroup are violated by, say, $4H = 10H = 12H$.

Below are observations about these cosets, which will be generalized in Section 19.4.

(1) The coset aH contains the element a. For example, $10H = \{4, 10, 12\}$ contains the element 10.

(2) We have $1H = 3H = 9H = H$, the original subgroup; and 1, 3, 9 are precisely the elements of H.

(3) All cosets have the same size, namely the size of H.

(4) The distinct cosets form a *partition* of U_{13}. Recall from Section 18.3 that "partition" means that the distinct cosets do not overlap and together cover all of U_{13}.

Example 19.2. Consider the group $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and its subgroup $H = \{1, 9\}$. How many *distinct* cosets do we expect to find? Let's compute the coset aH for each $a \in U_{20}$:

$$\begin{aligned} 1H &= \{1 \cdot 1, 1 \cdot 9\} = \{1, 9\}, & 11H &= \{11 \cdot 1, 11 \cdot 9\} = \{11, 19\}, \\ 3H &= \{3 \cdot 1, 3 \cdot 9\} = \{3, 7\}, & 13H &= \{13 \cdot 1, 13 \cdot 9\} = \{13, 17\}, \\ 7H &= \{7 \cdot 1, 7 \cdot 9\} = \{7, 3\}, & 17H &= \{17 \cdot 1, 17 \cdot 9\} = \{17, 13\}, \\ 9H &= \{9 \cdot 1, 9 \cdot 9\} = \{9, 1\}, & 19H &= \{19 \cdot 1, 19 \cdot 9\} = \{19, 11\}. \end{aligned}$$

Again, we see duplicates in this list of cosets. For instance, we have $3H = 7H$, even though 3 and 7 are distinct elements in U_{20}. Consolidating the duplicates, we obtain four distinct cosets:

- $1H = \ 9H = \{1, 9\}$ (original subgroup).
- $3H = \ 7H = \{3, 7\}$.
- $11H = 19H = \{11, 19\}$.
- $13H = 17H = \{13, 17\}$.

The observations that we made about the cosets in Example 19.1 apply here as well. After computing $3H = \{3, 7\}$, it's reasonable to suspect that $7H$ must be the same coset, because $7H$ should contain the element 7. We also have $1H = 9H = \{1, 9\}$, the original subgroup; and 1, 9 are precisely the elements of H. All the cosets have the same size, namely 2 elements each. And these four cosets do form a partition of U_{20}.

Example 19.3. Consider the group $D_4 = \{\varepsilon, r_{90}, r_{180}, r_{270}, h, v, d, d'\}$ and its subgroup $H = \{\varepsilon, d\}$. Since D_4 and H contain 8 and 2 elements, respectively, we would expect four distinct cosets. (Do you see why?) Referring to Appendix B for the group table of D_4, we compute the coset aH for each $a \in D_4$:

$$\begin{aligned}
\varepsilon H &= \{\varepsilon \cdot \varepsilon, \varepsilon \cdot d\} = \{\varepsilon, d\}, & hH &= \{h \cdot \varepsilon, h \cdot d\} = \{h, r_{90}\},\\
r_{90}H &= \{r_{90} \cdot \varepsilon, r_{90} \cdot d\} = \{r_{90}, h\}, & vH &= \{v \cdot \varepsilon, v \cdot d\} = \{v, r_{270}\},\\
r_{180}H &= \{r_{180} \cdot \varepsilon, r_{180} \cdot d\} = \{r_{180}, d'\}, & dH &= \{d \cdot \varepsilon, d \cdot d\} = \{d, \varepsilon\},\\
r_{270}H &= \{r_{270} \cdot \varepsilon, r_{270} \cdot d\} = \{r_{270}, v\}, & d'H &= \{d' \cdot \varepsilon, d' \cdot d\} = \{d', r_{180}\}.
\end{aligned}$$

Consolidating the duplicates, we obtain four distinct cosets, as we had expected:

- $\varepsilon H = dH = \{\varepsilon, d\}$ (original subgroup).
- $r_{90}H = hH = \{r_{90}, h\}$.
- $r_{180}H = d'H = \{r_{180}, d'\}$.
- $r_{270}H = vH = \{r_{270}, v\}$.

We will leave it up to you to verify that the observations that we made about the cosets in Example 19.1 are satisfied in this example as well.

Example 19.4. Consider the matrix group $G(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \alpha \text{ has a multiplicative inverse}\}$. Let $H = S(\mathbb{Z}_{10}) = \{\alpha \in G(\mathbb{Z}_{10}) \mid \det \alpha = 1\}$ and recall from Section 10.3 that $S(\mathbb{Z}_{10})$ is a subgroup of $G(\mathbb{Z}_{10})$.

Fix an element $\mu = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right] \in G(\mathbb{Z}_{10})$ with $\det \mu = 3$. To obtain the coset μH, we multiply each element of H by μ; i.e., $\mu H = \{\mu \cdot h \mid h \in H\}$. For instance, let $h = \left[\begin{smallmatrix} 7 & 2 \\ 5 & 3 \end{smallmatrix}\right]$ with $\det h = 7 \cdot 3 - 2 \cdot 5 = 1$, so that $h \in H$. Thus the following matrix is in the coset μH: $\mu \cdot h = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 7 & 2 \\ 5 & 3 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 9 & 7 \\ 5 & 2 \end{smallmatrix}\right]$. We note that $\det(\mu \cdot h) = \det \left[\begin{smallmatrix} 9 & 7 \\ 5 & 2 \end{smallmatrix}\right] = 9 \cdot 2 - 7 \cdot 5 = 3$, and so $\mu \cdot h$ has determinant 3, just like μ. In fact, you'll show in an exercise that every matrix in the coset μH has determinant 3.

Conversely, you'll also show that every matrix with determinant 3 is in the coset μH. For instance, let $\beta = \left[\begin{smallmatrix} 5 & 7 \\ 1 & 2 \end{smallmatrix}\right]$ and note that $\det \beta = 5 \cdot 2 - 7 \cdot 1 = 3$. Let $h = \left[\begin{smallmatrix} 3 & 2 \\ 9 & 3 \end{smallmatrix}\right]$ with $\det h = 3 \cdot 3 - 2 \cdot 9 = 1$, so that $h \in H$. We have $\mu \cdot h = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 3 & 2 \\ 9 & 3 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 5 & 7 \\ 1 & 2 \end{smallmatrix}\right]$, so that $\mu \cdot h = \beta$. Therefore, $\beta \in \mu H$ as desired. (How did we come up with the matrix h here? That's for you to explore in the exercises!)

19.2 Additive group example

As a default, we assume that an operation of a group is multiplication. But cosets of additive groups will be particularly important when we study *rings* later in the book. So we will take an in-depth look at the additive case in the following examples.

Example 19.5. Consider the additive group $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and its subgroup $H = \{0, 4, 8\}$. Choose $6 \in \mathbb{Z}_{12}$. Then the *coset* $6 + H$ is obtained by adding 6 to each element of H; i.e., $6 + H = \{6 + 0, 6 + 4, 6 + 8\} = \{6, 10, 2\}$. In an exercise, you'll compute the coset $a + H$ for each $a \in \mathbb{Z}_{12}$. You should find that there

are only four *distinct* cosets:

- $0 + H = 4 + H = 8 + H = \{0, 4, 8\}$ (original subgroup).
- $1 + H = 5 + H = 9 + H = \{1, 5, 9\}$.
- $2 + H = 6 + H = 10 + H = \{2, 6, 10\}$.
- $3 + H = 7 + H = 11 + H = \{3, 7, 11\}$.

Aside from the original subgroup $0 + H = 4 + H = 8 + H$, none of the other cosets are subgroups of $\mathbb{Z}_{12}$. Notice again that the duplicates occur, because the cosets $a + H$ and $b + H$ can be equal (i.e., they contain the same elements) even when $a \neq b$. For instance, $5 + H = 9 + H$, even though $5 \neq 9$ in $\mathbb{Z}_{12}$.

Here are some observations about these additive cosets. Note how they're the same as the observations about the cosets in Example 19.1, but written in the language of addition.

(1) The coset $a + H$ contains the element a. For example, $10 + H = \{2, 6, 10\}$ contains the element 10.

(2) We have $0 + H = 4 + H = 8 + H = H$, the original subgroup; and $H = \{0, 4, 8\}$.

(3) All cosets have the same size, namely the size of H.

(4) The distinct cosets form a partition of $\mathbb{Z}_{12}$.

Here is an example of cosets where the group and subgroup have infinitely many elements.

Example 19.6. Consider the additive group $\mathbb{Z}$ and its subgroup

$$H = 5\mathbb{Z} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}.$$

As an example, here's the coset $7 + H$, which is obtained by adding 7 to each element of H:

$$\begin{aligned} 7 + H &= \{7 + h \mid h \in H\} \\ &= \{\ldots, 7 + (-20), 7 + (-15), 7 + (-10), 7 + (-5), \\ &\qquad\qquad 7 + 0, 7 + 5, 7 + 10, 7 + 15, 7 + 20, \ldots\} \\ &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\}. \end{aligned}$$

There are five distinct cosets of H in $\mathbb{Z}$, as shown:

- $\cdots = -5 + H = 0 + H = 5 + H = 10 + H = 15 + H = \cdots$ (original subgroup).
- $\cdots = -4 + H = 1 + H = 6 + H = 11 + H = 16 + H = \cdots$.
- $\cdots = -3 + H = 2 + H = 7 + H = 12 + H = 17 + H = \cdots$.
- $\cdots = -2 + H = 3 + H = 8 + H = 13 + H = 18 + H = \cdots$.
- $\cdots = -1 + H = 4 + H = 9 + H = 14 + H = 19 + H = \cdots$.

The observations made in earlier examples apply here as well. For instance, we have $7+H = 12+H$, even though 7 and 12 are distinct elements in $\mathbb{Z}$. After computing

$$7 + H = \{\ldots, -13, -8, -3, 2, 7, \mathbf{12}, 17, 22, 27, \ldots\},$$

it's reasonable to suspect that $12 + H$ must be the same coset, because $12 + H$ should contain the element 12. We also have $\cdots = -10 + H = -5 + H = 0 + H = 5 + H = 10 + H = 15 + H = \cdots = H$, the original subgroup; and $0, \pm5, \pm10, \pm15, \ldots$ are the elements of H. And these five distinct cosets do form a partition of $\mathbb{Z}$.

19.3 Right cosets

In Section 19.1, we considered *left* cosets of the form aH, where we multiplied each element of H *on the left* by a. We can also consider *right* cosets Ha, as shown in the example below.

Example 19.7. Consider again the group U_{13} and its subgroup $H = \{1, 3, 9\}$. The left coset $6H$ is given by $6H = \{6 \cdot 1, 6 \cdot 3, 6 \cdot 9\} = \{6, 5, 2\}$, and we have the right coset $H6 = \{1 \cdot 6, 3 \cdot 6, 9 \cdot 6\} = \{6, 5, 2\}$. Observe that $6H = H6$; i.e., the left and right cosets are equal, because U_{13} is commutative.

As seen in Example 19.7, the distinction between left and right cosets is irrelevant in a commutative group. In particular, additive groups are always commutative, so there is no distinction between the left coset $a + H$ and the right coset $H + a$. Thus, we will only consider left cosets $a + H$ with additive groups.

Here is a non-commutative example, where things get a bit more interesting.

Example 19.8. Let $H = \{\varepsilon, d\}$ be a subgroup of D_4. Let's compute and compare the left coset $r_{90}H$ and the right coset Hr_{90}:

- $r_{90}H = \{r_{90} \cdot \varepsilon, r_{90} \cdot d\} = \{r_{90}, h\}$.
- $Hr_{90} = \{\varepsilon \cdot r_{90}, d \cdot r_{90}\} = \{r_{90}, v\}$.

Therefore, the left and right cosets are not the same; i.e., $r_{90}H \neq Hr_{90}$.

Example 19.9. Let $K = C(h) = \{\varepsilon, r_{180}, h, v\}$ be a subgroup of D_4. (It's the *centralizer* of h in D_4. See Section 5.3.) Let's compute and compare the left coset dK and the right coset Kd:

- $dK = \{d \cdot \varepsilon, d \cdot r_{180}, d \cdot h, d \cdot v\} = \{d, d', r_{270}, r_{90}\}$.
- $Kd = \{\varepsilon \cdot d, r_{180} \cdot d, h \cdot d, v \cdot d\} = \{d, d', r_{90}, r_{270}\}$.

Thus we have a *coset equality* $dK = Kd$, because these sets contain the same four elements. But this does not imply that we have an *element-by-element equality*; i.e., $dk = kd$ for all $k \in K$. Indeed, we have $dh \neq hd$ and $dv \neq vd$, where $h, v \in K$.

You'll show in an exercise at the end of the chapter that $\varepsilon K = K\varepsilon$, $r_{90}K = Kr_{90}$, $r_{180}K = Kr_{180}$, and so on. In fact, it turns out that $aK = Ka$ for all $a \in D_4$, so that left and right cosets are always equal in this example. But be careful: Coset equality does *not* imply element-by-element equality.

Remark. In the next section, we will prove various properties of cosets. The proofs will be written using left cosets. But for each property about left cosets, an analogous theorem holds true for right cosets.

19.4 Properties of cosets

We've seen plenty of examples of cosets thus far, and now we're ready for a general definition.

Definition 19.10 (Coset)**.** Let G be a group, H a subgroup of G, and $a \in G$. Then:

- The set $aH = \{ah \mid h \in H\}$ is the *left coset* of H generated by a.
- The set $Ha = \{ha \mid h \in H\}$ is the *right coset* of H generated by a.

The element a is called the *coset representative* of aH and Ha.

Remark. If G is an *additive* group, then the left and right cosets are $a + H = \{a + h \mid h \in H\}$ and $H + a = \{h + a \mid h \in H\}$, respectively. Recall that we always have $a + H = H + a$, since additive groups are commutative. Given this lack of distinction between left and right cosets, we will only consider left cosets $a + H$ with additive groups.

Below are the first three properties of cosets observed in Examples 19.1 and 19.5. (The fourth property about how the distinct cosets partition the group will be addressed in the next chapter.) While they are stated in the context of left cosets, as will be typical of coset theorems, analogous statements are true for right cosets. Each proof is written for a multiplicative group, and the proofs for an additive group are left for you as an exercise.

The following example motivates the proof of the first theorem.

Example 19.11. Consider again the group U_{13} and its subgroup $H = \{\mathbf{1}, 3, 9\}$. Since H is a subgroup, it must contain the identity element $\mathbf{1}$. Thus the coset $6H$ must contain the element $6 \cdot \mathbf{1}$ or 6; i.e.,

$$6H = \{6 \cdot \mathbf{1}, 6 \cdot 3, 6 \cdot 9\} = \{\mathbf{6}, 5, 2\}.$$

Theorem 19.12. *A coset representative is contained in the coset that it generates. Specifically, let G be a group, H a subgroup of G, and $a \in G$. Then:*

- (*Multiplicative*) *The coset aH contains the element a; i.e., $a \in aH$.*
- (*Additive*) *The coset $a + H$ contains the element a; i.e., $a \in a + H$.*

PROOF. Since H is a subgroup, it contains the identity element ε. Then $a = a\varepsilon \in aH$. ∎

The next theorem says that the elements of G whose cosets are the same as the original subgroup are precisely those elements that are in H. Here are some examples we've seen that illustrate the theorem.

Example 19.13.

- For the group U_{13} and subgroup $H = \{1, 3, 9\}$, we have $1H = 3H = 9H = H$, the original subgroup; and 1, 3, 9 are precisely the elements of H.
- For the group $\mathbb{Z}_{12}$ and subgroup $H = \{0, 4, 8\}$, we have $0+H = 4+H = 8+H = H$, the original subgroup; and 0, 4, 8 are precisely the elements of H.

- For the group D_4 and subgroup $H = \{\varepsilon, d\}$, we have $\varepsilon H = dH = H$, the original subgroup; and ε, d are precisely the elements of H.

Theorem 19.14. *Let G be a group, H a subgroup of G, and $a \in G$. Then:*

- (*Multiplicative*) *$aH = H$ if and only if $a \in H$.*
- (*Additive*) *$a + H = H$ if and only if $a \in H$.*

PROOF. We must prove two implications:

- If $aH = H$, then $a \in H$.
- If $a \in H$, then $aH = H$.

We will prove the second implication. The proof of the first implication is left for you as an exercise.

Assume $a \in H$. To prove $aH = H$, we must show that $aH \subseteq H$ and $H \subseteq aH$. We begin with $aH \subseteq H$. Let $g \in aH$ so that $g = ah$ for some $h \in H$. Since a and h are both in H, we know $ah \in H$ by the closure of H. Then $g \in H$ and thus $aH \subseteq H$. Next, we will show $H \subseteq aH$. Let $g \in H$. To show that $g \in aH$, we must show that $g = ah$ for some $h \in H$. Let $h = a^{-1}g$, which is in H, because a and g are in H. And we have $ah = a(a^{-1}g) = (aa^{-1})g = g$, so that $g = ah \in aH$. This shows that $H \subseteq aH$, so that $aH = H$. ■

Proof know-how. Proofs about cosets often involve a group element contained in a coset. Note how the remarks below are similar to those given after the proof of Theorem 18.6.

- In the first part of the proof, *assuming* that $g \in aH$ allowed us to conclude that $g = ah$ for some $h \in H$. In essence, we're applying the following implication: If $g \in aH$, then $g = ah$ for some $h \in H$.
- Later in the proof, *showing* that $g = ah$ for some $h \in H$ allowed us to conclude that $g \in aH$. Here, we're using the converse of the above implication; namely: If $g = ah$ for some $h \in H$, then $g \in aH$.

Coming up with the element $h = a^{-1}g$ employed the familiar "working backwards" technique. Our goal was to show that $g = ah$ for some $h \in H$, so we solved this equation for h by left-multiplying each side by a^{-1}, which yielded $h = a^{-1}g$. As before, this process of solving for h is scratch work and does *not* belong in the proof. Instead, the focus of the argument is showing that $g = ah$ for $h = a^{-1}g$.

Theorem 19.15. *Let H be a subgroup of a group G. Then all the left cosets of H have the same size, namely the size of H.*

PROOF. Let $a \in G$. We will define a bijection from H to the coset aH. This will show that all cosets of H have the same size as H. Consider the function $f : H \to aH$ where $f(h) = ah$ for all $h \in H$. To show that f is one-to-one, suppose $f(h) = f(k)$ for some $h, k \in H$. Then $ah = ak$ and left cancellation would imply $h = k$. To show that f is onto, let $ah \in aH$ where $h \in H$. Then $f(h) = ah$. ■

Remark. Even if H were infinite, the above proof is valid. It would show that all cosets of H are infinite, each having a bijection from H.

19.5 When are cosets equal?

We have seen that cosets can be equal even when their coset representatives are different. For instance, let's revisit Example 19.1 with the group U_{13} and subgroup $H = \{1, 3, 9\}$. We found $2H = \{2, 6, 5\}$ and $6H = \{6, 5, 2\}$, so that $2H = 6H$, even though $2 \neq 6$ in U_{13}. But could we have determined that $2H = 6H$ *without* computing these cosets? More generally, is there a relationship between the coset representatives a and b that ensures that the cosets aH and bH are equal?

To answer these questions, we study an example whose operation is addition, since additive relationships tend to be easier to detect than their multiplicative counterparts. We revisit Example 19.5 with group $\mathbb{Z}_{12}$ and subgroup $H = \{0, 4, 8\}$. Here is what we found:

- $0 + H = 4 + H = 8 + H = \{0, 4, 8\}$.
- $1 + H = 5 + H = 9 + H = \{1, 5, 9\}$.
- $2 + H = 6 + H = 10 + H = \{2, 6, 10\}$.
- $3 + H = 7 + H = 11 + H = \{3, 7, 11\}$.

For instance, we have $2 + H = 6 + H$, and we seek an additive relationship between the coset representatives 2 and 6. We do have $2 + 6 = 8$, which is contained in the subgroup H. Perhaps the rule is: $a + H = b + H$ if and only if $a + b \in H$. But we also have $3 + H = 11 + H$ where $3 + 11 = 2$ (in $\mathbb{Z}_{12}$), which is not in H. Thus, our conjectured rule does not work in all cases.

Alternatively, we might try *subtracting* the coset representatives. For $2+H = 6+H$, we have $2-6 = 4$ (and $6-2 = 4$), which is in H. For $3+H = 11+H$, we have $3-11 = 4$ and $11 - 3 = 8$, and both differences are in H. Thus, we conjecture the following:

$$a + H = b + H \text{ if and only if } a - b \in H \text{ and } b - a \in H.$$

This rule even works with $5 + H = 5 + H$, since $5 - 5 = 0$ is in H. We also have $3 + H \neq 10 + H$, and $3 - 10 = 5$ and $10 - 3 = 7$, neither of which is in H. Thus, our conjecture seems promising.

Now let's translate this conjecture into the language of multiplicative groups. The expressions $a - b$ and $b - a$ could translate to $a \cdot b^{-1}$ and $b \cdot a^{-1}$. Thus, a conjecture for multiplicative groups may be

$$aH = bH \text{ if and only if } a \cdot b^{-1} \in H \text{ and } b \cdot a^{-1} \in H.$$

Let's verify this with the group U_{13} and subgroup $H = \{1, 3, 9\}$. For $2H = 6H$ (i.e., $a = 2$ and $b = 6$), we note that $2^{-1} = 7$ as $2 \cdot 7 = 1$ modulo 13 and $6^{-1} = 11$ as $6 \cdot 11 = 1$ modulo 13. Thus, $a \cdot b^{-1} = 2 \cdot 6^{-1} = 2 \cdot 11 = 9 \in H$ and $b \cdot a^{-1} = 6 \cdot 2^{-1} = 6 \cdot 7 = 3 \in H$. We also have $2H \neq 4H$, and $2 \cdot 4^{-1} = 2 \cdot 10 = 7$ and $4 \cdot 2^{-1} = 4 \cdot 7 = 2$, neither of which is in H. (Here, $4^{-1} = 10$, because $4 \cdot 10 = 1$ modulo 13.) Thus, the conjecture seems to work, both in concluding that $aH = bH$ and that $aH \neq bH$.

With the multiplicative case, it's instructive to test the conjecture with a non-commutative example. Let's use the group D_4 and subgroup $H = \{\varepsilon, d\}$ from Example 19.3. For $r_{90}H = hH$ (i.e., $a = r_{90}$ and $b = h$), we have $a \cdot b^{-1} = r_{90} \cdot h^{-1} = r_{90} \cdot h = d'$ and $b \cdot a^{-1} = h \cdot r_{90}^{-1} = h \cdot r_{270} = d'$, and yet $d' \notin H$. The conjecture fails, but how can we fix it? In a non-commutative group, the product $a \cdot b^{-1}$ does not necessarily equal $b^{-1} \cdot a$. Likewise, the products $b \cdot a^{-1}$ and $a^{-1} \cdot b$ need not be equal.

As a salvage, therefore, we rewrite $a \cdot b^{-1}$ and $b \cdot a^{-1}$ as $b^{-1} \cdot a$ and $a^{-1} \cdot b$, respectively. This change won't affect commutative groups such as U_{13}. Hence, our revised conjecture is

$$aH = bH \text{ if and only if } b^{-1} \cdot a \in H \text{ and } a^{-1} \cdot b \in H.$$

For $r_{90}H = hH$ (i.e., $a = r_{90}$ and $b = h$), we have $b^{-1} \cdot a = h^{-1} \cdot r_{90} = h \cdot r_{90} = d$ and $a^{-1} \cdot b = r_{90}^{-1} \cdot h = r_{270} \cdot h = d$, and $d \in H$. We also have $r_{90}H \neq vH$, and $v^{-1} \cdot r_{90} = v \cdot r_{90} = d'$ and $r_{90}^{-1} \cdot v = r_{270} \cdot v = d'$, which is not in H. The revised conjecture seems to correctly conclude that $aH = bH$ and that $aH \neq bH$.

We now state the revised conjecture as a theorem. The proof is written for a multiplicative group, and the proof for an additive group is left for you as an exercise.

Theorem 19.16. *Let G be a group, H a subgroup of G, and $a, b \in G$. Then:*

- *(Multiplicative) $aH = bH$ if and only if $b^{-1} \cdot a \in H$ and $a^{-1} \cdot b \in H$.*
- *(Additive) $a + H = b + H$ if and only if $a - b \in H$ and $b - a \in H$.*

Remark. The elements $b^{-1} \cdot a$ and $a^{-1} \cdot b$ are multiplicative inverses of each other. (Think socks-shoes.) Thus, they're both in H or neither is in H. Therefore, Theorem 19.16 could be stated as follows: *$aH = bH$ if and only if $b^{-1} \cdot a \in H$*. But, as we saw above with the group D_4 and subgroup $H = \{\varepsilon, d\}$, we cannot use the conditions $a \cdot b^{-1} \in H$ and $b \cdot a^{-1} \in H$.

PROOF. We must prove two implications:

- If $aH = bH$, then $b^{-1} \cdot a \in H$ and $a^{-1} \cdot b \in H$.
- If $b^{-1} \cdot a \in H$ and $a^{-1} \cdot b \in H$, the $aH = bH$.

We will prove the second implication. The proof of the first implication is left for you as an exercise.

Assume $b^{-1}a \in H$ and $a^{-1}b \in H$. To prove $aH = bH$, we will show that $aH \subseteq bH$ and $bH \subseteq aH$.

We start with $aH \subseteq bH$. Let $g \in aH$ so that $g = ah$ for some $h \in H$. (We must show that $g \in bH$). Moreover, since $b^{-1}a \in H$, we have $b^{-1}a = j$ for some $j \in H$. Left-multiplying both sides of $b^{-1}a = j$ by b, we obtain $a = bj$. Combining $g = ah$ and $a = bj$, we find $g = ah = (bj)h = b(jh) \in bH$, where $jh \in H$. Therefore, $g \in bH$ so that $aH \subseteq bH$.

By symmetry, we can deduce that $bH \subseteq aH$. Hence, we conclude that $aH = bH$, as desired. ∎

Proof know-how. The above proof contains the sentence, "By symmetry, we can deduce that $bH \subseteq aH$." This means that the argument for $bH \subseteq aH$ is *identical* to that for $aH \subseteq bH$, with the roles of a and b swapped. For instance, the first step in the argument would be "Let $g \in bH$ so that $g = bh$ for some $h \in H$." Rather than repeating what is essentially the same argument, we invoked the phrase "By symmetry." This proof-writing technique is often called *proof by symmetry*.

In Theorem 19.16, it's easy to get confused between the conditions $b^{-1} \cdot a,\ a^{-1} \cdot b \in H$ (which is correct) and $a \cdot b^{-1},\ b \cdot a^{-1} \in H$ (which is incorrect). Here's a mnemonic

device that can help. Starting with $aH = bH$, left-multiply both sides by b^{-1} to obtain $b^{-1}aH = b^{-1}bH$, which simplifies to $(b^{-1}a)H = H$. Then Theorem 19.14 implies that $b^{-1}a \in H$. Likewise, starting with $aH = bH$ and left-multiplying both sides by a^{-1} results in $a^{-1}b \in H$. We caution that this is merely a mnemonic for remembering the correct condition, and it does *not* constitute a proof of Theorem 19.16. In particular, the coset equality $b^{-1}aH = b^{-1}bH$ would require a more rigorous justification in an actual proof.

Example 19.17. Consider again the additive group $\mathbb{Z}$ and it subgroup $H = 5\mathbb{Z}$. Theorem 19.16 implies the following:

$$a + H = b + H \iff a - b \in H \iff 5 \mid (a - b) \iff a = b \text{ in } \mathbb{Z}_5.$$

Here, the symbol $\iff$ is a shorthand for "if and only if." Therefore, the cosets $a + H$ and $b + H$ are related in a way that resembles how a and b are related in $\mathbb{Z}_5$. We'll dig much more into this soon!

Exercises

When working with the group D_4, refer to Appendix B for its group table.

1. Consider the group U_{13} and its subgroup $H = \{1, 3, 9\}$. Then the coset $4H = \{4, 12, 10\}$ is *not* a subgroup of U_{13}. Describe all the group properties that are violated by $4H$.

2. A group G has 100 elements and its subgroup H has 5 elements. Determine the number of distinct cosets of H. Explain your reasoning.

3. Can a group G with 100 elements have a subgroup H with 12 elements? Why or why not? (This exercise is referenced in Chapter 20.)

4. Let $\alpha \in S_5$ be defined by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}.$$

   Let $H = \langle \alpha \rangle$, i.e., the cyclic subgroup generated by α. Find the number of distinct cosets of H.

5. Let $H = \{0, 4, 8\}$ be a subgroup of $\mathbb{Z}_{12}$. For each $a \in \mathbb{Z}_{12}$, compute the coset $a + H$. (See Example 19.5.)

6. Let $H = \{0, 5, 10\}$ be a subgroup of $\mathbb{Z}_{15}$.

   (a) How many distinct cosets of H do you expect? Explain your reasoning.

   (b) For each $a \in \mathbb{Z}_{15}$, compute the coset $a + H$.

   (c) Verify Theorems 19.12, 19.14, 19.15, and 19.16 using the cosets you computed in part (b).

   (d) Verify that the distinct cosets of H form a partition of $\mathbb{Z}_{15}$.

7. Consider the multiplicative group U_{28} and its subset $H = \{1, 9, 25\}$.
   (a) Verify that H is indeed a subgroup of U_{28}.
   (b) How many distinct cosets of H do you expect? Explain your reasoning.
   (c) For each $a \in U_{28}$, compute the coset aH.
   (d) Verify Theorems 19.12, 19.14, 19.15, and 19.16 using the cosets you computed in part (c).
   (e) Verify that the distinct cosets of H form a partition of U_{28}.

8. Consider the additive group $\mathbb{Z}$ and its subgroup $H = 5\mathbb{Z}$. (See Example 19.6.)
   (a) Compute the cosets $12 + H$, $-1 + H$, $203 + H$, $-25 + H$, and $101 + H$.
   (b) Find all distinct cosets of H.
   (c) Verify that the distinct cosets of H form a partition of $\mathbb{Z}$.

9. Consider the additive group $\mathbb{Z}$ and its subgroup $H = 5\mathbb{Z}$. Determine whether or not the following cosets of H are equal.
   (a) $436 + H$ and $721 + H$.
   (b) $-43 + H$ and $111 + H$.
   (c) $317 + H$ and $532 + H$.

10. Consider the multiplicative group U_{35} and its subset $H = \{1, 8, 22, 29\}$.
    (a) Verify that H is indeed a subgroup of U_{35}.
    (b) How many distinct cosets of H do you expect? Explain your reasoning.
    (c) Without computing these cosets, determine if $11H = 18H$. (**Hint:** $18 \cdot 2 = 1$ modulo 35.)
    (d) Without computing these cosets, determine if $9H = 13H$. (**Hint:** $9 \cdot 4 = 1$ modulo 35.)
    (e) Without computing these cosets, determine if $3H = 24H$. (**Hint:** $3 \cdot 12 = 1$ modulo 35.)

11. Let $H = \{\varepsilon, v\}$ be a subgroup of D_4.
    (a) How many distinct cosets of H do you expect? Explain your reasoning.
    (b) For each $a \in D_4$, compute the left coset aH.
    (c) Find a pair of distinct elements $a, b \in D_4$ for which $aH = bH$. Verify that $b^{-1} \cdot a,\ a^{-1} \cdot b \in H$.
    (d) Find $a, b \in D_4$ for which $aH = bH$, but $b \cdot a^{-1}, a \cdot b^{-1} \notin H$.
    Note: So, you should be careful when using Theorem 19.16.

12. Write the proofs of Theorems 19.12, 19.14, 19.15, and 19.16 when the group operations is *addition*.

13. (a) For Theorem 19.16, give an analogous statement for right cosets.
    (b) Using an example, verify that the statement in part (a) correctly concludes that $Ha = Hb$ and that $Ha \neq Hb$.
    Note: It's recommended that you work on Exercise #14 in conjunction with this one.

    (This exercise is referenced in Chapter 20, Exercise #2.)

14. Again, let $H = \{\varepsilon, v\}$ be a subgroup of D_4.

    (a) For each $a \in D_4$, compute the right coset Ha.

    (b) Verify Theorems 19.12, 19.14, 19.15, and 19.16 (that are appropriately restated for right cosets) using the cosets you computed in part (a).
    Note: It's recommended that you work on Exercise #13 in conjunction with this one.

    (c) **True or False:** $aH = Ha$ for all $a \in D_4$.

    (This exercise is referenced in Example 24.14.)

15. Let $K = C(h) = \{\varepsilon, r_{180}, h, v\}$ be a subgroup of D_4. (See Example 19.9.)

    (a) For each $a \in D_4$, compute the left and right cosets aK and Ka.

    (b) Verify that $aK = Ka$ for all $a \in D_4$.

    (c) **True or False:** $aK = Ka$ means $ak = ka$ for each $k \in K$ (i.e., element-by-element equality).

    (This exercise is referenced in Example 24.5.)

16. Repeat Exercise #15 with $K = \{\varepsilon, r_{90}, r_{180}, r_{270}\}$. (This exercise is referenced in Example 24.9 and Chapter 24, Exercise #5.)

17. Consider the group U_{13} and its subgroup $H = \{1\}$.

    (a) How many distinct cosets of H do you expect?

    (b) For each $a \in U_{13}$, compute the coset aH.

    (c) Using your result in part (b), complete this statement: $aH = bH$ if and only if _____.

18. Consider the group U_{13} and its subgroup $H = U_{13}$.

    (a) How many distinct cosets of H do you expect?

    (b) For each $a \in U_{13}$, compute the coset aH.

    (c) Using your result in part (b), complete this statement: $aH = bH$ if and only if _____.

19. Let G be a group and H its subgroup. Restate Theorem 19.16 for the cases $H = \{\varepsilon\}$ and $H = G$. How do your restatements compare with your answers in Exercises #17 and #18?

20. Let's generalize our work from Example 19.4. Consider the matrix group $G(\mathbb{Z}_{10})$ and its subgroup $H = S(\mathbb{Z}_{10}) = \{\alpha \in G(\mathbb{Z}_{10}) \mid \det \alpha = 1\}$. Define the following two sets:

    - Coset μH where μ is a fixed element $\mu = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right] \in G(\mathbb{Z}_{10})$ with $\det \mu = 3$.
    - Set $T = \{\beta \in G(\mathbb{Z}_{10}) \mid \det \beta = 3\}$, i.e., the set of all matrices in $G(\mathbb{Z}_{10})$ with determinant 3.

    (a) Choose an element of the coset μH, i.e., a product $\mu \cdot h$ where $h \in H$. Show that this product is in set T by showing that it has determinant 3.

(b) Choose an element of set T, i.e., a matrix β with determinant 3. Show that β is in the coset μH by finding $h \in H$ such that $\beta = \mu \cdot h$.

Note: You must create examples that are different from the ones we used in Example 19.4.

21. Consider the matrix group $G(\mathbb{Z}_{10})$ and its subgroup $H = S(\mathbb{Z}_{10})$. Let $\mu \in G(\mathbb{Z}_{10})$ be a fixed element with $\det \mu = 3$, and define $T = \{\beta \in G(\mathbb{Z}_{10}) \mid \det \beta = 3\}$. Prove that $\mu H = T$. (This exercise is referenced in Section 25.2.)

Note: You must let μ be a general element of $G(\mathbb{Z}_{10})$ with $\det \mu = 3$, not a specific one like $\mu = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right]$.

22. **Prove:** Let H and K be subgroups of a group G. If $aH \subseteq bK$ for some $a, b \in G$, then $H \subseteq K$.

23. Complete the proof of Theorem 19.14 by proving its first implication.

24. Complete the proof of Theorem 19.16 by proving its first implication.

20

Lagrange's Theorem

Chapter 19, Exercise #3 asked the following:

> Can a group G with 100 elements have a subgroup H with 12 elements? Why or why not?

Here is a related question:

> Suppose there are lots of eggs and lots of dozen egg cartons, like the one shown in the figure below. If all the eggs are in cartons and all the cartons are full, can there be 100 eggs? Why or why not?

The answer to both questions is "No," and understanding the reason behind it will be the focus of this chapter. In particular, we will prove Lagrange's theorem, which states that if H is a subgroup of G with $\#H$ and $\#G$ elements, respectively, then $\#H$ is a divisor of $\#G$. Cosets will play a prominent role in proving this theorem, one of the most important results about finite groups.

20.1 Motivating Lagrange's theorem

Let G be a *finite* group, and let H be a subgroup of G. Denote the number of elements of G and H by $\#G$ and $\#H$, respectively. Then *Lagrange's theorem*, named after Joseph-Louis Lagrange, states that $\#H$ is a divisor of $\#G$. In this section, we will review several examples that motivate this theorem, highlighting the aspects of those examples that will play a role in its proof.

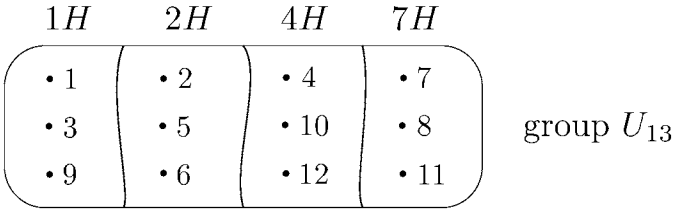
Example 20.1. Consider the group U_{13} and its subgroup $H = \{1, 3, 9\}$. In Example 19.1, we computed the cosets aH for each $a \in U_{13}$, i.e., $1H$, $2H$, $3H$, …, $12H$. We found several duplicates, and after consolidating those duplicates, we found four *distinct* cosets:

- $1H = \{1, 3, 9\}$.
- $2H = \{2, 5, 6\}$.
- $4H = \{4, 10, 12\}$.
- $7H = \{7, 8, 11\}$.

To say that these are the distinct cosets of H means that *any* coset of H must be equal to one of these. For instance, the coset $8H$ (which isn't on the above list) is equal to $7H$. More generally, a coset aH, where $a \in U_{13}$, must be equal to one of $1H$, $2H$, $4H$, or $7H$.

We recall two observations about these distinct cosets that will help in proving Lagrange's theorem. First, all cosets of H have the same size; namely $\#H = 3$. In fact, this was proved in Theorem 19.15.

Second, these distinct cosets form a *partition* of U_{13}, which means that the distinct cosets do not overlap and together cover all of U_{13}. This second observation is depicted in the figure below. Note how each element of U_{13} is contained in *exactly one* of the distinct cosets.



Example 20.2. Consider the group D_4 and its subgroup $H = \{\varepsilon, d\}$. In Example 19.3, we found the distinct left cosets of H, which are listed below along with the distinct right cosets of H.

Distinct left cosets of H:

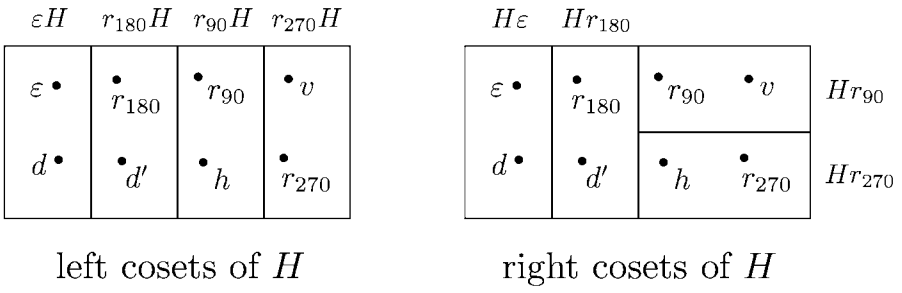
- $\varepsilon H = \{\varepsilon, d\}$.
- $r_{90}H = \{r_{90}, h\}$.
- $r_{180}H = \{r_{180}, d'\}$.
- $r_{270}H = \{r_{270}, v\}$.

Distinct right cosets of H:

- $H\varepsilon = \{\varepsilon, d\}$.
- $Hr_{90} = \{r_{90}, v\}$.
- $Hr_{180} = \{r_{180}, d'\}$.
- $Hr_{270} = \{r_{270}, h\}$.

As we observed in Example 19.8, the same coset representative can generate different left and right cosets, such as $r_{90}H \neq Hr_{90}$. This isn't too surprising, since D_4 is a *non-commutative* group. Nonetheless, all left and right cosets of H have the same size, namely $\#H = 2$, and the number of distinct left cosets equals the number of distinct right cosets (i.e., there are four of each type). The distinct left cosets of H form a partition of D_4, and the distinct right cosets of H do so as well. However, the manner in

which D_4 is partitioned differs between the left and right cosets, as shown in the figure below:



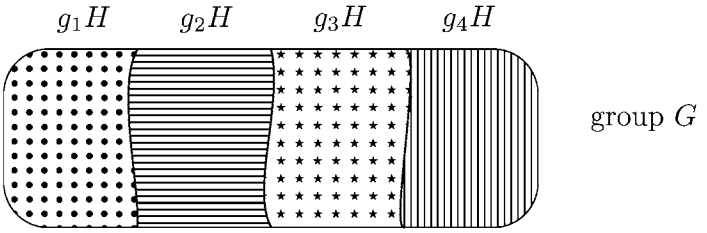
20.2 Proving Lagrange's theorem

We are now ready to prove Lagrange's theorem, which says: If H is a subgroup of a finite group G, then $\#H$ is a divisor of $\#G$. (Recall that $\#H$ and $\#G$ denote the number of elements of H and G, respectively.) Here are the key ingredients needed for its proof:

(1) All the cosets of H have the same size, namely $\#H$. (Proved in Theorem 19.15.)

(2) The distinct cosets of H form a *partition* of G; i.e., they cover all of G without overlapping.

Let's see why these two ingredients suffice to prove Lagrange's theorem. Suppose g_1H, g_2H, g_3H, …, g_nH are the distinct left cosets of H. The case of $n = 4$, i.e., four distinct cosets, is shown in the figure below:



Since these cosets form a partition of G, the number of elements in G equals the sum of the number of elements in each coset; i.e., $\#G = \#(g_1H) + \#(g_2H) + \#(g_3H) + \cdots + \#(g_nH)$. But all the cosets of H have the same size, namely $\#H$, and thus we obtain

$$\#G = \underbrace{\#H + \#H + \#H + \cdots + \#H}_{n \text{ terms}} = n \cdot \#H,$$

where n is the number of left cosets of H. Hence $\#G = n \cdot \#H$, so that $\#H$ is a divisor of $\#G$.

Remark. A helpful analogy is to think of the cosets of H as "tiling" the group G. And if the cosets of H were to tile G without any overlap, then it must be the case that $\#H$ is a divisor of $\#G$.

It remains to show that the distinct cosets of H form a *partition* of G. Thus, we will prove the following:

- Every element of G is contained in one of these cosets.
- Distinct cosets of H do not overlap with each other.

Remark. Like the theorems in Chapter 19, Theorems 20.3 and 20.4 below are stated in terms of left cosets. Analogous statements are true for right cosets (which you'll prove in an exercise at the end of the chapter), as well as for groups whose operation is addition.

Theorem 20.3. *Let H be a subgroup of a finite group G, and suppose g_1H, g_2H, g_3H, …, g_nH are the distinct left cosets of H. Then every element of G is contained in one of these cosets.*

PROOF. Consider an element $a \in G$. Then $a \in aH$ by Theorem 19.12. Moreover, aH must be equal to one of $g_1H, g_2H, g_3H, \ldots, g_nH$, say $aH = g_iH$. Since $a \in aH$, we have $a \in g_iH$ as desired. ∎

Next, we will show that distinct cosets of H do not overlap with each other. In other words, given cosets aH and bH, we must prove the following: If $aH \neq bH$, then aH and bH do not share any common element. Instead, we will prove the contrapositive; namely: If aH and bH do share a common element, then $aH = bH$.

Proof know-how. Why prove the contrapositive? Inequalities such as $aH \neq bH$ can be difficult to work with, since they indicate a *lack* of something. Instead, the hypothesis of the contrapositive, "aH and bH do share a common element," gives us something concrete to use, namely an element common to aH and bH.

Theorem 20.4. *Let H be a subgroup of a finite group G. If cosets aH and bH share a common element, then $aH = bH$.*

Remark. The last step of the proof below uses Theorem 19.16; i.e., $aH = bH$ if and only if $b^{-1}a \in H$.

PROOF. Assume aH and bH share a common element. Let g be an element contained in aH and bH. Thus, $g = ah$ and $g = bk$ for some $h, k \in H$, so that $ah = bk$. Take the equation $ah = bk$ and left-multiply by b^{-1} and right-multiply by h^{-1} to obtain $b^{-1}a = kh^{-1}$. Since $h, k \in H$ and H is a subgroup, we have $kh^{-1} \in H$. Hence $b^{-1}a \in H$, from which we conclude $aH = bH$. ∎

Proof know-how. In the above proof, one might wonder how we knew to take the equation $ah = bk$ and left-multiply by b^{-1} and right-multiply by h^{-1}. Our goal was to show $aH = bH$. Due to Theorem 19.16, that meant showing $b^{-1}a \in H$. Once we determined our goal (i.e., show that $b^{-1}a \in H$), the proof boiled down to manipulating the equation $ah = bk$ to solve for $b^{-1}a$ (and show that it's in H).

With its proof complete, we now state Lagrange's theorem.

Theorem 20.5 (Lagrange's theorem)**.** *Let H be a subgroup of a finite group G. Then $\#H$ is a divisor of $\#G$.*

Example 20.6. At the beginning of this chapter, we asked, "Can a group G with 100 elements have a subgroup H with 12 elements?" The answer is "No," because 12 is not a divisor of 100, and thus such a group and subgroup would violate Lagrange's theorem.

Consider a finite group G and its subgroup H. In the proof of Lagrange's theorem, we found that $\#G = n \cdot \#H$ where n is the number of distinct left cosets of H. Therefore, we concluded that $\#H$ is a divisor of $\#G$. From $\#G = n \cdot \#H$, we obtain the formula $n = \frac{\#G}{\#H}$. But we could have proved Lagrange's theorem using *right* cosets instead and derived the same conclusions. Thus, the same formula $n = \frac{\#G}{\#H}$ also applies to the number of distinct right cosets of H.

The above discussion prompts the following definition and theorem.

Definition 20.7 (Index of a subgroup)**.** Let G be a group, and let H be a subgroup of G. Then the *index* of H in G, denoted $[G : H]$, is the number of distinct left (or right) cosets of H in G.

Theorem 20.8. *Let H be a subgroup of a finite group G. Then $[G : H] = \frac{\#G}{\#H}$.*

Remark. Using the tiling analogy again, the index tells us how many cosets of H are needed to tile G.

We end the section with some examples of index calculations.

Example 20.9. In Example 19.1, we considered the group U_{13} and its subgroup $H = \{1, 3, 9\}$. There are four distinct left cosets of H, and so $[U_{13} : H] = 4$. Note that $\frac{\#U_{13}}{\#H} = \frac{12}{3} = 4$, which confirms Theorem 20.8.

Example 20.10. In Example 19.6, we computed the distinct cosets of $5\mathbb{Z}$ in $\mathbb{Z}$. Since $\mathbb{Z}$ is an infinite group, Theorem 20.8 does not apply. However, we found five distinct cosets, so that $[\mathbb{Z} : 5\mathbb{Z}] = 5$.

Example 20.11. In Example 20.2, we considered the group D_4 and its subgroup $H = \{\varepsilon, d\}$. We found four distinct left cosets and four distinct right cosets, and thus $[D_4 : H] = 4$. Note that $\frac{\#D_4}{\#H} = \frac{8}{2} = 4$, which confirms Theorem 20.8.

20.3 Applications of Lagrange's theorem

Lagrange's theorem is a powerful result that can provide many insights into the structure of finite groups. For instance, here is a conjecture that we had made in earlier chapters, which can now be proved using Lagrange's theorem. (See Chapter 4, Exercise #11; Chapter 5, Exercise #10; Chapter 6, Exercise #7.)

Theorem 20.12. *Let G be a finite group, and let $g \in G$. Then* $\operatorname{ord}(g)$ *is a divisor of $\#G$.*

PROOF. Let $n = \operatorname{ord}(g)$. By Theorem 13.17, the cyclic subgroup $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ contains n distinct elements; namely $\langle g \rangle = \{\varepsilon, g^1, g^2, g^3, \ldots, g^{n-1}\}$. Since $\langle g \rangle$ is a subgroup of G, Lagrange's theorem implies that $\#\langle g \rangle$ is a divisor of $\#G$. Thus, $n = \operatorname{ord}(g)$ is a divisor of $\#G$, as desired. ∎

Example 20.13. Suppose a group G contains p elements, where p is prime. Let $g \in G$ be a non-identity element; i.e., $g \neq \varepsilon$. By Theorem 20.12, $\text{ord}(g)$ is a divisor of $\#G = p$. Since p is prime, its only positive divisors are 1 and p. And since $g \neq \varepsilon$, we know that $\text{ord}(g) \neq 1$. Thus we must have $\text{ord}(g) = p$, which implies that the cyclic subgroup $\langle g \rangle$ contains p elements; namely $\langle g \rangle = \{\varepsilon, g^1, g^2, g^3, \ldots, g^{p-1}\}$. Since G also has p elements, we have $G = \langle g \rangle$, so that G is cyclic with generator g.

The result of Example 20.13 is summarized in the following theorem.

Theorem 20.14. *Let G be a group with p elements, where p is prime. Then G is cyclic with $G = \langle g \rangle$, where g is any non-identity element of G.*

The next theorem is a direct consequence of Theorem 20.14. Moreover, its proof introduces a new proof-writing technique, which is described in the Proof know-how below. (**Note:** Recall that $H \cap K$ is the *intersection* of H and K, i.e., the set of elements that are contained in both subgroups.)

Theorem 20.15. *Let G be a group with subgroups H and K. Suppose $\#H = \#K = p$, where p is prime. Then $H = K$ or $H \cap K = \{\varepsilon\}$.*

Proof know-how. In this theorem, we must prove an "or" statement; i.e., we must prove that (1) $H = K$ or (2) $H \cap K = \{\varepsilon\}$. Here is a possible approach. We know that conclusion (2) is either true or false. If it's true, then we're done with the proof. Thus, we will *assume* that (2) is false and *prove* that (1) is true. In other words, we will prove the following implication: If (2) is false, then (1) is true. In the actual proof, we typically leave out the rationale behind this approach, i.e., about how (2) is either true or false and we're done with the proof if (2) is true. Instead, we start right away with the assumption that (2) is false.

Now, we could also assume that (1) is false and prove that (2) is true, which happens to be the contrapositive of "if (2) is false, then (1) is true." In this case, it turns out that "if (2) is false, then (1) is true" is easier to prove. Like many aspects of proof writing, a feel for choosing which implication to prove comes with lots of experience. If you're not sure which one to prove, try both and see what happens!

PROOF. Assume that $H \cap K \neq \{\varepsilon\}$. Hence, there is a non-identity element g that is contained in both H and K. We will show that $H = K$. Since H has p elements, Theorem 20.14 implies that it is cyclic with $H = \langle g \rangle$. Likewise, we have $K = \langle g \rangle$. Therefore $H = K$, as both are equal to $\langle g \rangle$. ■

Example 20.16. Let G be a group with 35 elements. We'll prove that G contains an element of order 5. Let $g \in G$ be a non-identity element. By Theorem 20.12, $\text{ord}(g)$ is a divisor of $\#G = 35$. The positive divisors of 35 are 1, 5, 7, and 35. Since $g \neq \varepsilon$, we have $\text{ord}(g) = 5$, 7, or 35. If $\text{ord}(g) = 5$, then we're done with our proof. If $\text{ord}(g) = 35$, then $\text{ord}(g^7) = 5$ by Theorem 12.7 and we're also done.

But what if all 34 non-identity elements of G have order 7? We'll show this isn't possible, and thus G must have an element of order 5. Suppose $g_1 \in G$ has order 7. Then the cyclic subgroup $\langle g_1 \rangle$ contains 6 non-identity elements, each with order 7. Next, let $g_2 \in G$ have order 7, with $g_2 \notin \langle g_1 \rangle$. Then $\langle g_2 \rangle$ also contains 6 non-identity

elements, each with order 7. Moreover, Theorem 20.15 implies that $\langle g_1 \rangle \cap \langle g_2 \rangle = \{\varepsilon\}$. Therefore, elements of order 7 come in disjoint "clumps" of 6 elements. Since 6 is not a divisor of 34, there cannot be 34 elements of order 7 in G.

Exercises

1. Consider the group D_4 and its subgroup $H = \{\varepsilon, r_{180}, d, d'\}$.

   Note: We have $H = C(d)$, i.e., the *centralizer* of d in D_4. Thus, H is indeed a subgroup.

   (a) Find $[D_4 : H]$.

   (b) Let $a \in H$. *Without* using the group table for D_4, compute the left coset aH and right coset Ha.

   (c) Repeat part (b) for $a \notin H$. Explain your reasoning.

   (d) Explain why $aH = Ha$ for all $a \in D_4$.

2. For Theorems 20.3 and 20.4, write analogous statements for right cosets and prove them.

   Note: For Theorem 20.4, you should first complete Chapter 19, Exercise #13.

3. Let G be a finite group, H a subgroup of G, and K a subgroup of H (thus $K \subseteq H \subseteq G$). Prove that $[G : K] = [G : H] \cdot [H : K]$.

4. Let G be a group, and let H and K be its subgroups. Define $M = H \cap K = \{g \in G \mid g \in H \text{ and } g \in K\}$; i.e., M is the *intersection* of H and K. If $\#H = 15$ and $\#K = 28$, find $\#M$. Explain your reasoning.

   Hint: See Chapter 11, Exercise #13.

5. **Prove:** Suppose G is a group and H and K are subgroups of G containing m and n elements, respectively. If $\gcd(m, n) = 1$, then $H \cap K = \{\varepsilon\}$.

   Note: Compare with Chapter 14, Exercise #24.

6. Prove each of the following statements.

   (a) If the group U_m contains k elements, then $a^k = 1$ for all $a \in U_m$. (See Chapter 4, Exercise #10.)

   (b) If a group G contains k elements, then $g^k = \varepsilon$ for all $g \in G$.

7. **Prove:** Let G be a group with k elements. Suppose $\gcd(k, n) = 1$. If $g \in G$ and $g^n = \varepsilon$, then $g = \varepsilon$.

   Hint: Use Theorem 3.9, i.e., the GCD theorem.

8. Consider the prime number $p = 3$.

   (a) Choose an integer a, compute $a^p - a$, and verify that p is a divisor of $a^p - a$.

   (b) Repeat part (a) with another integer a of your choice.

   (c) Repeat part (a) again, this time with a negative integer a.

9. (a) Repeat Exercise #8 with prime $p = 5$; with prime $p = 7$; with prime $p = 11$.
   (b) Repeat Exercise #8 with one more prime number of your choice.
   (c) What conjecture do you have?

10. **(Fermat's little theorem)** Let p be a prime number. Prove that p is a divisor of $a^p - a$ for all $a \in \mathbb{Z}$.

11. Let G be a group with 15 elements, and let H be a *proper* subgroup of G. Explain why H is cyclic.

    Note: A *proper* subgroup of G is a subgroup that is not G itself.

12. Repeat Exercise #11 for a group G with 21 elements; with 33 elements; with 91 elements.

13. **Prove:** Suppose G is a group with pq elements, where p and q are distinct prime numbers. If H is a proper subgroup of G, then H is cyclic.

14. Prove each of the following statements.
    (a) If G is a group with 27 elements, then there exists an element $g \in G$ with $\text{ord}(g) = 3$.
    (b) Suppose G is a group with p^n elements, where p is a prime number and n is a positive integer. Then there exists an element $g \in G$ with $\text{ord}(g) = p$.

15. Let G be a group with 49 elements. If G is *not* cyclic, what can you say about the order of each element in G?

16. (a) Repeat Exercise #15 for a group with 25 elements; with 169 elements; with 289 elements.
    (b) Write a statement that generalizes part (a). Then prove your statement.

17. Let G be a group with 55 elements.
    (a) For $g \in G$, find the possible values of $\text{ord}(g)$.
    (b) **Prove:** There exists an element of G with order 11.

18. Let G be a group with 40 elements.
    (a) For $g \in G$, find the possible values of $\text{ord}(g)$.
    (b) **Prove:** There exists an element of G with order 2.

19. **Prove:** Let G be a group with $p \cdot 2^n$ elements, where p is an odd prime and n is a positive integer. Then there exists an element $g \in G$ with $\text{ord}(g) = 2$.

20. **Prove:** Let G be a group with n elements. If n is odd, then G has no element of order 2.

21. **Prove:** Let G be a commutative group with n elements. Let a be the product of all elements of G. If n is odd, then $a = \varepsilon$.

22. Let G be a commutative group with 21 elements. Consider the function $\theta : G \to G$ where $\theta(g) = g^{16}$ for all $g \in G$. Show that θ is an isomorphism.

23. Let G be a commutative group with n elements. Consider the function $\theta : G \to G$ where $\theta(g) = g^m$ for all $g \in G$. If $\gcd(m, n) = 1$, then show that θ is an isomorphism.

21

Multiplying/Adding Cosets

In Chapter 20, we saw the instrumental role that cosets play in the proof of Lagrange's theorem. As noted in the introduction to this unit, I often tell students, "If proving Lagrange's theorem is all that cosets are good for, then cosets would still hold a special place in group theory." However, cosets can do so much more, and we'll learn about their further exploits in the next few chapters.

Given a group G and its subgroup H, the distinct cosets of H form a group called a *quotient group*, provided that H meets a certain condition (TBA). In this chapter, we'll learn the group operation for the quotient group, i.e., how to multiply (or add) cosets.

21.1 Turning a set of cosets into a group

We begin by revisiting Example 19.1. Let $H = \{1, 3, 9\}$ be a subgroup of U_{13}. The distinct cosets of H are the following:

- $1H = \{1, \ 3, \ 9\} = \ 3H = \ 9H$.
- $2H = \{2, \ 6, \ 5\} = \ 6H = \ 5H$.
- $4H = \{4, 12, 10\} = 12H = 10H$.
- $7H = \{7, \ 8, 11\} = \ 8H = 11H$.

We can use the property $a \in aH$ (Theorem 19.12) and that distinct cosets do not overlap (Theorem 20.4) when finding these coset representatives. For instance, once we compute $2H = \{2 \cdot 1, 2 \cdot 3, 2 \cdot 9\} = \{2, 6, 5\}$, then we know that this coset also equals $6H$ and $5H$, because 6 and 5 are contained in $2H$.

Notation. We define U_{13}/H (read "U_{13} mod H") to be the set of distinct cosets of H. Thus,

$$U_{13}/H = \{1H, \ 2H, \ 4H, \ 7H\}.$$

Since different coset representatives can generate the same coset (e.g., $2H = 6H$), we could have written U_{13}/H slightly differently, perhaps like this:

$$U_{13}/H = \{1H, \ 6H, \ 10H, \ 11H\}.$$

It does make sense to use $1H$ instead of $3H$ or $9H$, given that $1 \in U_{13}$ is a special element, namely the multiplicative identity. (We'll soon see the special role that $1H$ plays in U_{13}/H.) However, using $2H$ instead of $6H$ is simply a matter of choice.

Here's a crazy idea: We wish to turn the set U_{13}/H into a *group*. That means we need an *operation*, i.e., a way to "multiply" a pair of cosets. For instance, what would $2H \cdot 4H$ equal? By closure, it would have to equal $1H$, $2H$, $4H$, or $7H$. But which one? To answer this question, we begin by defining what it means to multiply two subsets of a group. (**Recall:** This was first defined in Chapter 8, Exercise #9.)

Definition 21.1. Let S and T be subsets of a group G. Then the *set product* of S and T is the set

$$S \cdot T = \{s \cdot t \mid s \in S,\ t \in T\},$$

where the multiplication $s \cdot t$ is done in G.

Example 21.2. Let $H = \{1, 3, 9\}$ be a subgroup of U_{13}. To compute the set product $2H \cdot 4H$, we multiply every element of $2H = \{2, 6, 5\}$ by every element of $4H = \{4, 12, 10\}$, as shown below:

$$\begin{aligned} 2H \cdot 4H &= \{2, 6, 5\} \cdot \{4, 12, 10\} \\ &= \{2 \cdot 4,\ 2 \cdot 12,\ 2 \cdot 10,\ 6 \cdot 4,\ 6 \cdot 12,\ 6 \cdot 10,\ 5 \cdot 4,\ 5 \cdot 12,\ 5 \cdot 10\} \\ &= \{8, 11, 7, 11, 7, 8, 7, 8, 11\}. \end{aligned}$$

Since $2H$ and $4H$ contain 3 elements each, it may seem that $2H \cdot 4H$ would contain 9 elements of U_{13}. But we see several duplicates in the set product, and duplicate elements are not counted in a set. After consolidating the duplicates, we obtain $2H \cdot 4H = \{7, 8, 11\}$. Therefore, $2H \cdot 4H = 7H$.

Example 21.3. Consider again the subgroup $H = \{1, 3, 9\}$ of U_{13}. Let's compute the set product $4H \cdot 2H$ and compare the result with $2H \cdot 4H$, which we found in Example 21.2 above:

$$\begin{aligned} 4H \cdot 2H &= \{4, 12, 10\} \cdot \{2, 6, 5\} \\ &= \{4 \cdot 2,\ 4 \cdot 6,\ 4 \cdot 5,\ 12 \cdot 2,\ 12 \cdot 6,\ 12 \cdot 5,\ 10 \cdot 2,\ 10 \cdot 6,\ 10 \cdot 5\} \\ &= \{8, 11, 7, 11, 7, 8, 7, 8, 11\} \\ &= \{7, 8, 11\} \\ &= 7H. \end{aligned}$$

We obtain $4H \cdot 2H = 7H$, so that $2H \cdot 4H = 4H \cdot 2H$. Perhaps this was expected, since multiplication of cosets in this example and in Example 21.2 is based on multiplication in U_{13}, which is commutative. In an exercise at the end of the chapter, you'll prove that if a group G is commutative, then the corresponding coset multiplication is also commutative; i.e., $aH \cdot bH = bH \cdot aH$.

Example 21.4. For the subgroup $H = \{1, 3, 9\}$ of U_{13}, we have the set of distinct cosets

$$U_{13}/H = \{1H, 2H, 4H, 7H\}.$$

We'll now see the special role that $1H$ plays in coset multiplication. Consider the set product:

$$\begin{aligned} 1H \cdot 4H &= \{1, 3, 9\} \cdot \{4, 12, 10\} \\ &= \{1 \cdot 4, 1 \cdot 12, 1 \cdot 10, 3 \cdot 4, 3 \cdot 12, 3 \cdot 10, 9 \cdot 4, 9 \cdot 12, 9 \cdot 10\} \\ &= \{4, 12, 10, 12, 10, 4, 10, 4, 12\} \\ &= \{4, 10, 12\} \\ &= 4H. \end{aligned}$$

Therefore, $1H \cdot 4H = 4H$. Based on Example 21.3, we also have $4H \cdot 1H = 4H$. In an exercise at the end of the chapter, you'll show that $1H \cdot aH = aH$ and $aH \cdot 1H = aH$ for all cosets aH. Hence, $1H$ is the multiplicative identity element of U_{13}/H.

Example 21.5. Let $H = \{1, 3, 9\}$ be a subgroup of U_{13} and consider the set of distinct cosets

$$U_{13}/H = \{1H, 2H, 4H, 7H\}.$$

We'll leave it up to you to verify the following set products: $1H \cdot 1H = 1H$, $2H \cdot 7H = 1H$ (and hence $7H \cdot 2H = 1H$), and $4H \cdot 4H = 1H$. Since $1H$ is the multiplicative identity of U_{13}/H (see Example 21.4), we conclude that $2H$ and $7H$ are an inverse pair and $1H$ and $4H$ are self-inverses.

After computing all the set products, we obtain the following table for $U_{13}/H = \{1H, 2H, 4H, 7H\}$ where the operation is coset multiplication:

$\cdot$	$1H$	$2H$	$4H$	$7H$
$1H$	$1H$	$2H$	$4H$	$7H$
$2H$	$2H$	$4H$	$7H$	$1H$
$4H$	$4H$	$7H$	$1H$	$2H$
$7H$	$7H$	$1H$	$2H$	$4H$

We use this table to verify the group properties for U_{13}/H.

(1) U_{13}/H is closed under coset multiplication. We can see this from the table, since every entry in the table (i.e., all possible "products") is an element of U_{13}/H.

(2) Coset multiplication is associative. See Theorem 21.6 below for a justification.

(3) U_{13}/H contains the multiplicative identity element $1H$, where $1H \cdot aH = aH$ (first row of the table) and $aH \cdot 1H = aH$ (first column of the table) for all $aH \in U_{13}/H$.

(4) Every element in U_{13}/H has a multiplicative inverse. $2H$ and $7H$ are multiplicative inverses of each other, and $1H$ and $4H$ are self-inverses.

Thus, U_{13}/H is a group under coset multiplication.

Remark. The key here is that we are treating each coset aH as an *element* of U_{13}/H.

Using the group table, we can compute the order of each $aH \in U_{13}/H$, i.e., the smallest number of times we multiply aH by itself to obtain the multiplicative identity $1H$.

- $\text{ord}(1H) = 1$, because $(1H)^1 = 1H$.
- $\text{ord}(2H) = 4$, because $(2H)^1 = 2H$, $(2H)^2 = 4H$, $(2H)^3 = 7H$, and $(2H)^4 = 1H$.
- $\text{ord}(4H) = 2$, because $(4H)^1 = 4H$ and $(4H)^2 = 1H$.
- $\text{ord}(7H) = 4$, because $(7H)^1 = 7H$, $(7H)^2 = 4H$, $(7H)^3 = 2H$, and $(7H)^4 = 1H$.

Therefore, U_{13}/H is a *cyclic* group with generators $2H$ and $7H$; i.e., $U_{13}/H = \langle 2H \rangle = \langle 7H \rangle$.

The theorem below shows that coset multiplication is associative, for any group G and its subgroup H. Note that we must show the set equality $(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$, which entails showing the set inclusions $(aH \cdot bH) \cdot cH \subseteq aH \cdot (bH \cdot cH)$ and $aH \cdot (bH \cdot cH) \subseteq (aH \cdot bH) \cdot cH$.

Theorem 21.6 (Associativity of coset multiplication)**.** *Let G be a group, H a subgroup of G, and $a, b, c \in G$. Then $(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$.*

PROOF. Let $(\alpha \cdot \beta) \cdot \gamma \in (aH \cdot bH) \cdot cH$ where $\alpha \in aH$, $\beta \in bH$, and $\gamma \in cH$. But α, β, and γ are elements of G. So we use the associativity of multiplication in G to get

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma) \in aH \cdot (bH \cdot cH).$$

Therefore, $(aH \cdot bH) \cdot cH \subseteq aH \cdot (bH \cdot cH)$. The argument for the other set inclusion follows similarly. Thus, $(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$, as desired. ■

21.2 Coset multiplication shortcut

As we saw in Examples 21.2, 21.3, and 21.4, coset multiplication can be a tedious process. Fortunately, there is a shortcut. To motivate this shortcut, let's examine the earlier examples in more depth.

Example 21.7. Consider the subgroup $H = \{1, 3, 9\}$ of U_{13}. We found the coset product $2H \cdot 4H = 7H$. But $7H$ can be written as $8H$ (i.e., they're the same coset). Thus $2H \cdot 4H = 8H$, where we observe that $2 \cdot 4 = 8$ in U_{13}. We also found that $1H \cdot 4H = 4H$, where $1 \cdot 4 = 4$ in U_{13}. For the product $4H \cdot 4H = 1H$, we observe that $1H$ can also be written as $3H$. Hence we have $4H \cdot 4H = 3H$, where $4 \cdot 4 = 3$ in U_{13}.

Example 21.7 above suggests that to find the coset product $aH \cdot bH$ in G/H, we can simply multiply their coset representatives in G; i.e., $aH \cdot bH = (ab)H$. The theorem below is for the case when G is commutative, such as $G = U_{13}$. Its proof is left for you as an exercise at the end of the chapter.

Theorem 21.8 (Coset multiplication shortcut)**.** *Let G be a* commutative *group, H a subgroup of G, and $a, b \in G$. Define the coset product by $aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH, \beta \in bH\}$. Then $aH \cdot bH = (ab)H$.*

Example 21.9. Consider again the cosets $2H = \{2, 6, 5\}$ and $4H = \{4, 12, 10\}$ of U_{13}. Rather than multiplying every element of $2H$ by every element of $4H$, we use the coset multiplication shortcut to compute $2H \cdot 4H$. Note that the shortcut applies in this case, because U_{13} is commutative. We have

$$2H \cdot 4H = (2 \cdot 4)H = 8H.$$

But $8H = 7H$, so that $2H \cdot 4H = 7H$ as before.

Remark. In Example 21.9 above, we have the the equality $2H \cdot 4H = (2 \cdot 4)H$. There's a subtle distinction between the multiplication symbol $\cdot$ in each side of the equation. On the left side, the expression $2H \cdot 4H$ denotes a product of cosets, i.e., multiplication in U_{13}/H. In the expression $(2 \cdot 4)H$, the product $2 \cdot 4$ depicts a product of coset representatives, which occurs in U_{13}.

Example 21.10 (Non-example)**.** Let's look at a non-commutative example. Consider the group D_4 and its subgroup $H = \{\varepsilon, \upsilon\}$. To compute the set product $r_{90}H \cdot d'H$, we multiply every element of $r_{90}H = \{r_{90}, d\}$ by every element of $d'H = \{d', r_{270}\}$, as shown below:

$$\begin{aligned} r_{90}H \cdot d'H &= \{r_{90}, d\} \cdot \{d', r_{270}\} \\ &= \{r_{90} \cdot d', r_{90} \cdot r_{270}, d \cdot d', d \cdot r_{270}\} \\ &= \{\upsilon, \varepsilon, r_{180}, h\}. \end{aligned}$$

Thus, $r_{90}H \cdot d'H = \{\upsilon, \varepsilon, r_{180}, h\}$. But $(r_{90} \cdot d')H = \upsilon H = \{\upsilon, \varepsilon\}$, so we see that $r_{90}H \cdot d'H \neq (r_{90} \cdot d')H$. The coset multiplication shortcut fails! In fact, the set product $r_{90}H \cdot d'H$ contains 4 elements, and therefore it's not even a coset of H.

Based on Example 21.10 above, it's natural to ask: Does the coset multiplication shortcut in G/H hold *only* when G is commutative? Not quite. You'll see in the exercises at the end of this chapter that the shortcut can hold in D_4/H for some subgroups H, even though D_4 is non-commutative. The precise condition for when the coset multiplication shortcut holds will be revealed in Chapter 24. Stay tuned!

21.3 Cosets of $H = 5\mathbb{Z}$ in $\mathbb{Z}$ revisited

Consider the additive group $\mathbb{Z}$ and its subgroup $H = 5\mathbb{Z}$. We saw in Example 19.6 that the distinct cosets of H in $\mathbb{Z}$ are as follows:

- $\cdots = -5 + H = \mathbf{0} + \boldsymbol{H} = 5 + H = 10 + H = 15 + H = \cdots$ (original subgroup).
- $\cdots = -4 + H = \mathbf{1} + \boldsymbol{H} = 6 + H = 11 + H = 16 + H = \cdots$.
- $\cdots = -3 + H = \mathbf{2} + \boldsymbol{H} = 7 + H = 12 + H = 17 + H = \cdots$.
- $\cdots = -2 + H = \mathbf{3} + \boldsymbol{H} = 8 + H = 13 + H = 18 + H = \cdots$.
- $\cdots = -1 + H = \mathbf{4} + \boldsymbol{H} = 9 + H = 14 + H = 19 + H = \cdots$.

We define $\mathbb{Z}/H$ (read "$\mathbb{Z}$ mod H") to be the set of distinct cosets of H. Thus,

$$\mathbb{Z}/H = \{0 + H, 1 + H, 2 + H, 3 + H, 4 + H\}.$$

As with U_{13}/H in Section 21.1, we could have written $\mathbb{Z}/H$ slightly differently, since different coset representatives can generate the same coset (e.g., $2+H = 7+H$). Here is one possibility:

$$\mathbb{Z}/H = \{0+H,\ 11+H,\ 7+H,\ -2+H,\ 1049+H\}.$$

However, $\mathbb{Z}/H = \{0+H,\ 1+H,\ 2+H,\ 3+H,\ 4+H\}$ is a natural choice, as we will see below.

We will now show that $\mathbb{Z}/H$ is an (additive) group under coset addition. To add, for example, the cosets $2+H$ and $3+H$, we add every element of $2+H$ to those of $3+H$. Thus, we have

$$\begin{aligned}(2+H)+(3+H)&\\ &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} + \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}\\ &= \{\ldots, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, 30, 35, \ldots\}\\ &= 0+H.\end{aligned}$$

When computing $(2+H)+(3+H)$, we encounter duplicates, infinitely many of them, in fact. For instance, the integer 20 in the coset sum is obtained by $-13+33$, $-8+28$, $-3+23$, $2+18$, $7+13$, and so on, each of which is the sum of an element in $2+H$ and an element in $3+H$.

You might have noticed that $(2+H)+(3+H) = (2+3)+H$. This is true not only in $\mathbb{Z}/H$, but also in any G/H where G is an additive group. Below is the additive version of the coset multiplication shortcut (Theorem 21.8). Note that additive groups are always commutative, so that the shortcut should hold.

Theorem 21.11 (Coset addition shortcut)**.** *Let G be an additive group, H a subgroup of G, and $a, b \in G$. Define the coset sum by $(a+H)+(b+H) = \{\alpha+\beta \mid \alpha \in a+H,\ \beta \in b+H\}$. Then $(a+H)+(b+H) = (a+b)+H$.*

PROOF. To show this set equality, we must show that

$$(a+H)+(b+H) \subseteq (a+b)+H \quad \text{and} \quad (a+b)+H \subseteq (a+H)+(b+H).$$

First, let $\alpha+\beta \in (a+H)+(b+H)$, where $\alpha \in a+H$ and $\beta \in b+H$. Thus, $\alpha = a+h$ and $\beta = b+k$ for some $h, k \in H$. Since additive groups are commutative,

$$\alpha+\beta = (a+h)+(b+k) = (a+b)+(h+k) \in (a+b)+H.$$

Thus $\alpha+\beta \in (a+b)+H$, so that $(a+H)+(b+H) \subseteq (a+b)+H$.

Next, let $\gamma \in (a+b)+H$ so that $\gamma = (a+b)+h$ for some $h \in H$. Then,

$$\gamma = (a+b)+h = (a+0)+(b+h) \in (a+H)+(b+H).$$

Thus $\gamma \in (a+H)+(b+H)$, so that $(a+b)+H \subseteq (a+H)+(b+H)$.

Therefore, $(a+H)+(b+H) = (a+b)+H$ as desired. ∎

Proof know-how. In the above proof, we showed $\gamma = (a+b)+h = (a+0)+(b+h)$ by rewriting a as $a+0$. This "inserting the (additive) identity" technique allowed us to conclude that γ is in $(a+H)+(b+H)$, since $a+0 \in a+H$ and $b+h \in b+H$. (Compare this with the proofs of Theorems 9.6 and 17.9.)

Using the shortcut, we create a group table for $\mathbb{Z}/H$:

$+$	$0+H$	$1+H$	$2+H$	$3+H$	$4+H$
$0+H$	$0+H$	$1+H$	$2+H$	$3+H$	$4+H$
$1+H$	$1+H$	$2+H$	$3+H$	$4+H$	$0+H$
$2+H$	$2+H$	$3+H$	$4+H$	$0+H$	$1+H$
$3+H$	$3+H$	$4+H$	$0+H$	$1+H$	$2+H$
$4+H$	$4+H$	$0+H$	$1+H$	$2+H$	$3+H$

Then we use the table to verify the group properties for $\mathbb{Z}/H$.

(1) $\mathbb{Z}/H$ is closed under coset addition, since every entry in the table is an element of $\mathbb{Z}/H$.

(2) Coset addition is associative. The proof looks similar to that of Theorem 21.6. You'll fill in the details in an exercise at the end of the chapter.

(3) $\mathbb{Z}/H$ contains the identity element $0+H$, where $(0+H)+(a+H)=a+H$ (first row of the table) and $(a+H)+(0+H)=a+H$ (first column of the table) for all $a+H \in \mathbb{Z}/H$.

(4) Every element in $\mathbb{Z}/H$ has an additive inverse, because each row (and column) of the table contains the additive identity element $0+H$.

Thus, $\mathbb{Z}/H$ is a group. To which familiar group is it isomorphic? (**Hint:** Ignore the "$+H$" in the table.)

Exercises

When working with the group D_4, refer to Appendix B for its group table.

1. Let $H=\{1,\ 3,\ 9\}$ be a subgroup of U_{13}. We saw in Example 21.4 that $1H \cdot 4H = 4H$.
   (a) Compute the coset product $1H \cdot 1H$ by multiplying each element of $1H$ by those of $1H$.
   (b) Repeat part (a) to compute $1H \cdot 2H$.
   (c) Repeat part (a) to compute $1H \cdot 7H$.
   (d) What conclusion can you make about the element $1H$ in U_{13}/H?

2. Let $H=\{1,\ 3,\ 9\}$ be a subgroup of U_{13}. We saw in Exercise #1 that $1H \cdot 1H = 1H$.
   (a) Compute the coset $2H \cdot 7H$ by multiplying each element of $2H$ by those of $7H$.
   (b) Repeat part (a) to compute $7H \cdot 2H$.
   (c) Repeat part (a) to compute $4H \cdot 4H$.
   (d) What conclusion can you make about the pair $2H$ and $7H$? About $4H$ itself?

3. In Chapter 8, Exercise #9, we computed set products using the following subsets of U_7:
   $$E=\{1,\ 6\},\ S=\{2,\ 5\},\ T=\{3,\ 4\}.$$
   One of these is a subgroup of U_7 and the other two are cosets of that subgroup. Find the subgroup (call it H) and write the other two sets as cosets of H.

4. Let G be a group, H a subgroup of G, and $a, b \in G$. Define the coset product by

$$aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH,\ \beta \in bH\}.$$

Prove: If G is commutative, then $aH \cdot bH = bH \cdot aH$. (See Example 21.3.)

5. Prove Theorem 21.6 when the group operation is addition: Let G be an *additive* group, H a subgroup of G, and $a, b, c \in G$. Then $(aH + bH) + cH = aH + (bH + cH)$.

6. Let $H = \{1, 3, 9\}$ be a subgroup of U_{13}. Shown below is the table for $U_{13}/H = \{1H,\ 2H,\ 4H,\ 7H\}$, where the operation is coset multiplication. Use this table to verify the coset multiplication shortcut for each pair $aH, bH \in U_{13}/H$. (See Example 21.9.)

$\cdot$	$1H$	$2H$	$4H$	$7H$
$1H$	$1H$	$2H$	$4H$	$7H$
$2H$	$2H$	$4H$	$7H$	$1H$
$4H$	$4H$	$7H$	$1H$	$2H$
$7H$	$7H$	$1H$	$2H$	$4H$

7. Consider the subgroup $Z = \{\varepsilon, r_{180}\}$ of D_4. Recall that $Z = \{z \in G \mid zg = gz \text{ for all } g \in D_4\}$ is the *center* of D_4, i.e., the set of elements of D_4 that commute with all elements of D_4.

   (a) Quick! How many distinct left (or right) cosets of Z are there? Explain how you know.
   (b) For each $a \in D_4$, compute the left and right cosets aZ and Za.
   (c) Verify that $aZ = Za$ for all $a \in D_4$.
   (d) Elizabeth says, "Since Z is the center of D_4, it's not surprising to see that the left and right cosets were the same in part (c)." What might she mean?

8. In Exercise #7, we found that the distinct left cosets of Z are $D_4/Z = \{\varepsilon Z,\ r_{90}Z,\ hZ,\ dZ\}$.

   Note: Using, for example, hZ instead of vZ (they're the same coset) is simply a matter of choice.

   (a) Compute the coset product $r_{90}Z \cdot hZ$ by multiplying each element of $r_{90}Z$ by those of hZ. You may *not* use the coset multiplication shortcut (i.e., Theorem 21.8).
   (b) Verify that the product in part (a) is indeed equal to $(r_{90} \cdot h)Z$.

   (This exercise and Exercise #9 below are referenced in Sections 22.3 and 23.1.)

9. Repeat Exercise #8, but now verify the following:

   (a) $hZ \cdot r_{90}Z = (h \cdot r_{90})Z$.
   (b) $\varepsilon Z \cdot dZ = (\varepsilon \cdot d)Z$.
   (c) $dZ \cdot hZ = (d \cdot h)Z$.

   Note: The coset multiplication shortcut does hold in D_4/Z; i.e., $aZ \cdot bZ = (ab)Z$ for all $aZ, bZ \in D_4/Z$, even though D_4 is *not* commutative (so Theorem 21.8 doesn't apply). We'll soon see why this is true.

10. Consider again the subgroup $Z = \{\varepsilon, r_{180}\}$ of D_4.

    (a) Complete the group table below:

$\cdot$	εZ	$r_{90}Z$	hZ	dZ
εZ				
$r_{90}Z$				
hZ				
dZ				

    (b) Use the table to verify that D_4/Z is a group under coset multiplication.

    (c) Is D_4/Z commutative or non-commutative?

    (d) Find the order of each $aZ \in D_4/Z$. Is the group cyclic?

    (This exercise is referenced in Example 23.2.)

11. Let $H = \{\varepsilon, h\}$ be a subgroup of D_4. (This exercise is referenced in Exercise #18 below.)

    (a) Compute the cosets $r_{90}H$ and dH.

    (b) Compute the coset product $r_{90}H \cdot dH$ by multiplying each element of $r_{90}H$ by those of dH.

    (c) Does the coset multiplication shortcut work here? What's going on?!

12. Consider the group D_4 and its subgroup $H = \{\varepsilon, r_{180}, d, d'\}$.

    Note: We have $H = C(d)$, i.e., the *centralizer* of d in D_4. Thus, H is indeed a subgroup.

    (a) Compute the coset product $r_{90}H \cdot dH$ by multiplying each element of $r_{90}H$ by those of dH.

    (b) Verify that the product in part (a) is indeed equal to $(r_{90} \cdot d)H$.

13. Repeat Exercise #12, but now verify the following:

    (a) $dH \cdot r_{90}H = (d \cdot r_{90})H$.

    (b) $\varepsilon H \cdot dH = (\varepsilon \cdot d)H$.

    (c) $hH \cdot r_{270}H = (h \cdot r_{270})H$.

    Note: Indeed, the coset multiplication shortcut holds in this setting as well. We'll see why soon.

14. Consider again the subgroup $H = \{\varepsilon, r_{180}, d, d'\}$ of D_4.

    (a) Create the group table for D_4/H and verify that it's a group under coset multiplication.

    (b) Is D_4/H commutative or non-commutative?

15. Let $H = \{0, 4, 8\}$ be a subgroup of the (additive) group $\mathbb{Z}_{12}$.

    (a) Find the distinct left cosets of H.

    (b) Compute the coset sum $(2 + H) + (3 + H)$ by adding each element of $2 + H$ to those of $3 + H$.

    (c) Verify that the sum in part (b) is indeed equal to $(2 + 3) + H$.

16. Repeat Exercise #15, but now verify the following:
    (a) $(3 + H) + (2 + H) = (3 + 2) + H$.
    (b) $(0 + H) + (3 + H) = (0 + 3) + H$.
    (c) $(2 + H) + (2 + H) = (2 + 2) + H$.

17. Consider again the subgroup $H = \{0, 4, 8\}$ of $\mathbb{Z}_{12}$.
    (a) Create the group table for $\mathbb{Z}_{12}/H$ and verify that it's a group under coset addition.
    (b) Find the order of each $a + H \in \mathbb{Z}_{12}/H$. Is the group cyclic?

18. We've seen examples where the coset multiplication shortcut fails.
    (a) With subgroup $H = \{\varepsilon, v\}$ of D_4, we saw that $r_{90}H \cdot d'H \neq (r_{90} \cdot d')H$. (See Example 21.10.)
    (b) With subgroup $H = \{\varepsilon, h\}$ of D_4, we saw that $r_{90}H \cdot dH \neq (r_{90} \cdot d)H$. (See Exercise #11.)

    In each of those cases, verify that the set inclusion $(ab)H \subseteq aH \cdot bH$ still holds.

19. Let G be a group (not necessarily commutative), H a subgroup of G, and $a, b \in G$. Define the coset product by $aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH,\ \beta \in bH\}$. Prove that $(ab)H \subseteq aH \cdot bH$. (This exercise is referenced in the proof of Theorem 23.5. It is also the statement of Theorem 24.2.)

20. Let G be a *commutative* group, H a subgroup of G, and $a, b \in G$. Define the coset product by $aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH,\ \beta \in bH\}$. Prove that $aH \cdot bH \subseteq (ab)H$. (This exercise is referenced in Example 24.3.)

    Note: Combined with the result of Exercise #19, this shows that $aH \cdot bH = (ab)H$ when G is commutative, hence completing the proof of Theorem 21.8.

21. Consider the homomorphism $\delta : G(\mathbb{Z}_{10}) \to U_{10}$ where $\delta(\alpha) = \det \alpha$ for all $\alpha \in G(\mathbb{Z}_{10})$, and let $K = \ker \delta$ be the kernel of δ; i.e., $K = \{\alpha \in G(\mathbb{Z}_{10}) \mid \delta(\alpha) = 1\}$.
    (a) Let $\alpha = \left[\begin{smallmatrix} 7 & 2 \\ 5 & 3 \end{smallmatrix}\right] \in G(\mathbb{Z}_{10})$. Verify that $\alpha \in K$.
    (b) Let $g = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right] \in G(\mathbb{Z}_{10})$ so that $g \cdot \alpha$ is in the left coset gK. Find $\beta \in K$ for which $g \cdot \alpha = \beta \cdot g$.
    (c) Explain why $g \cdot \alpha$ is also contained in the right coset Kg.

22. Let $\theta : G \to H$ be a group homomorphism, and let $K = \ker \theta = \{a \in G \mid \theta(a) = \varepsilon_H\}$. Show that $gK = Kg$ for all $g \in G$. (This exercise is referenced in Example 24.13.)

    Hint: Be careful! $\theta(gk) = \theta(kg)$ does *not* necessarily imply that $gk = kg$.

22

Quotient Group Examples

In Chapter 21, we learned how to multiply (or add) a pair of cosets, as well as the coset multiplication shortcut; namely $aH \cdot bH = (ab)H$. This allowed us to form a new type of group, called a *quotient group*, whose elements are cosets. In this chapter, we'll formalize the notion of the quotient group. In particular, let G be a group, H a subgroup of G, and G/H (read "G mod H") the set of distinct cosets of H. We will show that if the coset multiplication shortcut holds in G/H, then G/H satisfies the group properties and thus is a group under coset multiplication. We will begin writing some proofs about G/H, with more proofs to come in the next chapter (which is aptly named "Quotient Group Proofs").

22.1 Quotient group U_{13}/H revisited

We begin by reviewing the main example from Chapter 21. Let $H = \{1, 3, 9\}$ be a subgroup of U_{13}. The set of distinct cosets of H is $U_{13}/H = \{1H, 2H, 4H, 7H\}$. Moreover, the set U_{13}/H (read "U_{13} mod H") turned out to be a group under coset multiplication. To multiply a pair of cosets such as $2H = \{2, 5, 6\}$ and $7H = \{7, 8, 11\}$, we multiply every element of $2H$ by every element of $7H$, as shown:

$$\begin{aligned} 2H \cdot 7H &= \{2, 5, 6\} \cdot \{7, 8, 11\} \\ &= \{2 \cdot 7, 2 \cdot 8, 2 \cdot 11, 5 \cdot 7, 5 \cdot 8, 5 \cdot 11, 6 \cdot 7, 6 \cdot 8, 6 \cdot 11\} \\ &= \{1, 3, 9, 9, 1, 3, 3, 9, 1\} \\ &= \{1, 3, 9\} \\ &= 1H \end{aligned}$$

Therefore, $2H \cdot 7H = 1H$.

Rather than performing this tedious computation, we found the *coset multiplication shortcut*; namely, $aH \cdot bH = (ab)H$. In Theorem 21.8, we proved that this shortcut holds in G/H when G is commutative (such as when $G = U_{13}$). Thus, $2H \cdot 7H = (2 \cdot 7)H = 14H = 1H$ as before.

In Section 21.1, we verified that U_{13}/H satisfies the group properties under coset multiplication. In particular, $1H$ is its multiplicative identity element, where $1H \cdot aH = aH$ and $aH \cdot 1H = aH$ for all $aH \in U_{13}/H$. Thus, $2H \cdot 7H = 1H$ and $7H \cdot 2H = 1H$ imply that $2H$ and $7H$ are multiplicative inverses of each other. In symbols, we write $7H = (2H)^{-1}$; i.e., $7H$ is the multiplicative inverse of $2H$. Likewise, we write $2H = (7H)^{-1}$, which says that $2H$ is the multiplicative inverse of $7H$.

22.2 Quotient group U_{37}/H

Consider the multiplicative group $U_{37} = \{1, 2, 3, \ldots, 35, 36\}$ and its subgroup $H = \{1, 10, 26\}$. You will verify in an exercise at the end of the chapter that H is equal to $\langle 10 \rangle = \{10^k \mid k \in \mathbb{Z}\}$, i.e., the cyclic subgroup generated by 10. Thus, H is indeed a subgroup of U_{37}. Since U_{37} and H contain 36 and 3 elements, respectively, there are $\frac{36}{3} = 12$ distinct cosets of H. And as U_{37} is commutative, Theorem 21.8 ensures that the coset multiplication shortcut holds in U_{37}/H.

Note that in all of the examples in this section, the subgroup H of U_{37} refers to $H = \{1, 10, 26\}$.

Example 22.1. Let $4H, 11H \in U_{37}/H$, where $4H = \{4, 3, 30\}$ and $11H = \{11, 36, 27\}$. While the shortcut does hold in U_{37}/H, we'll find $4H \cdot 11H$ as a set product, to remind us of the underlying computation. To ease the calculation somewhat, we will write some numbers in the cosets $4H$ and $11H$ using negative values modulo 37; i.e., $4H = \{4, 3, -7\}$ and $11H = \{11, -1, -10\}$. Thus, we have

$$\begin{aligned}
4H \cdot 11H &= \{4, 3, -7\} \cdot \{11, -1, -10\} \\
&= \{4 \cdot 11,\ 4 \cdot (-1),\ 4 \cdot (-10),\ 3 \cdot 11,\ 3 \cdot (-1),\ 3 \cdot (-10),\ -7 \cdot 11,\ -7 \cdot (-1),\ -7 \cdot (-10)\} \\
&= \{44, -4, -40, 33, -3, -30, -77, 7, 70\} \\
&= \{7, 33, 34, 33, 34, 7, 34, 7, 33\} \\
&= \{7, 33, 34\} \\
&= 7H.
\end{aligned}$$

Therefore, $4H \cdot 11H = 7H$. Using the shortcut, we have $4H \cdot 11H = (4 \cdot 11)H = 44H = 7H$, which matches the result obtained by a more tedious calculation.

Example 22.2. We compute the set product once more, in order to find $1H \cdot 11H$. To ease the calculation somewhat, we'll write $1H = \{1, 10, -11\}$ and $11H = \{11, -1, -10\}$.

$$\begin{aligned}
1H \cdot 11H &= \{1, 10, -11\} \cdot \{11, -1, -10\} \\
&= \{1 \cdot 11,\ 1 \cdot (-1),\ 1 \cdot (-10),\ 10 \cdot 11,\ 10 \cdot (-1),\ 10 \cdot (-10),\ -11 \cdot 11,\ -11 \cdot (-1),\ -11 \cdot (-10)\} \\
&= \{11, -1, -10, 110, -10, -100, -121, 11, 110\} \\
&= \{11, 36, 27, 36, 27, 11, 27, 11, 36\} \\
&= \{11, 27, 36\} \\
&= 11H.
\end{aligned}$$

Therefore, $1H \cdot 11H = 11H$. The shortcut confirms that $1H \cdot 11H = (1 \cdot 11)H = 11H$.

As Example 22.2 suggests, $1H$ is the multiplicative identity element of U_{37}/H. Next, let's consider multiplicative inverses in U_{37}/H and how they relate to multiplicative inverses in U_{37}.

Example 22.3. The coset multiplication shortcut implies $2H \cdot 19H = (2 \cdot 19)H = 1H$, since $2 \cdot 19 = 1$ in U_{37}. Thus, $2H \cdot 19H = 1H$. Symbolically, we write the following:

- In U_{37}, $2 \cdot 19 = 1$ implies $2^{-1} = 19$; i.e., the multiplicative inverse of 2 is 19.
- In U_{37}/H, $2H \cdot 19H = 1H$ implies $(2H)^{-1} = 19H$; i.e., the multiplicative inverse of $2H$ is $19H$.

Combining these two, we obtain $(2H)^{-1} = 19H = 2^{-1}H$, so that $(2H)^{-1} = 2^{-1}H$.

We use the coset multiplication shortcut to "verify" the group properties for U_{37}/H. Here, we write "verify" (in quotes), since exhibiting a few examples as we do below is not enough to justify these group properties. For a complete justification, see Section 22.3 below.

(1) U_{37}/H is closed under coset multiplication. In Example 22.1 above, we saw that

$$4H \cdot 11H = (4 \cdot 11)H = 44H = 7H$$

so that the product of $4H$ and $11H$ is another element of U_{37}/H.

(2) Coset multiplication is associative. This was proved in Theorem 21.6.

(3) U_{37}/H contains the identity element $1H$. In Example 22.2, we saw that $1H \cdot 11H = (1 \cdot 11)H = 11H$.

(4) Every element in U_{37}/H has an inverse. In Example 22.3, we found that $2H \cdot 19H = (2 \cdot 19)H = 1H$, and so the multiplicative inverse of $2H$ is $19H$; i.e., $(2H)^{-1} = 19H$.

22.3 Quotient group G/H (generalization)

Let G be a group, and let H be a subgroup of G. Suppose that G/H (the set of distinct cosets of H) satisfies the coset multiplication shortcut; i.e., $aH \cdot bH = (ab)H$ for all aH, $bH \in G/H$. Then we'll show that G/H is a group under coset multiplication.

(1) G/H **is closed.** Let $aH, bH \in G/H$, where $a, b \in G$. Then $aH \cdot bH = (ab)H$. Since G is closed, we have $ab \in G$. Thus $(ab)H$ is the coset of H that is generated by the element $ab \in G$. Therefore, $(ab)H \in G/H$, which implies that $aH \cdot bH \in G/H$. Hence, G/H is closed.

(2) **Coset multiplication is associative.** This was proved in Theorem 21.6.

(3) G/H **contains an identity.** Consider $\varepsilon H \in G/H$, where ε is the identity of G. We have

$$\varepsilon H \cdot aH = (\varepsilon a)H = aH \quad \text{and} \quad aH \cdot \varepsilon H = (a\varepsilon)H = aH$$

for all $aH \in G/H$. Thus, εH is a multiplicative identity of G/H.

(4) G/H **contains inverses of its elements.** Let $aH \in G/H$, where $a \in G$. Since G is a group, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = \varepsilon$ and $a^{-1} \cdot a = \varepsilon$. Thus $a^{-1}H \in G/H$, and

$$aH \cdot a^{-1}H = (a \cdot a^{-1})H = \varepsilon H \quad \text{and} \quad a^{-1}H \cdot aH = (a^{-1}a)H = \varepsilon H.$$

Thus, the multiplicative inverse of aH is $a^{-1}H$. Symbolically, we write $(aH)^{-1} = a^{-1}H$.

Proof know-how. An element of G/H has the form aH where $a \in G$ is the coset representative. Often, a proof about G/H involves working with these coset representatives (which are elements of G) and relies on what we know about the group G. For instance, when showing that G/H is closed, we used the closure of G to conclude that $ab \in G$, and hence $(ab)H \in G/H$.

We have just proved the following theorem.

Theorem 22.4. *Let G be a group, and let H be a subgroup of G. If G/H satisfies the coset multiplication shortcut, then G/H is a group under coset multiplication.*

Definition 22.5 (Quotient group)**.** The group G/H in Theorem 22.4 is called a *quotient group*.

Example 22.6. Let $H = \{1, 10, 26\}$ be a subgroup of U_{37}. Then U_{37}/H is a quotient group containing $\frac{36}{3} = 12$ elements. The key here is that we treat each coset aH as an *element* of U_{37}/H.

Example 22.7. Let G be a group, and let H be its subgroup. Assume G/H satisfies the coset multiplication shortcut. Given $aH \in G/H$ where $a \in G$, we'll compute $(aH)^n$ for integer exponents n.

First, consider a positive value of n, say $n = 3$. The shortcut implies

$$(aH)^3 = aH \cdot aH \cdot aH = (a \cdot a \cdot a)H = a^3H,$$

so that $(aH)^3 = a^3H$.

In any group, we define an element raised to the 0^{th} power to be the identity element. In G/H, this implies $(aH)^0 = \varepsilon H$, since εH is the multiplicative identity of G/H. In G, we have $a^0 = \varepsilon$. Thus, $(aH)^0 = \varepsilon H = a^0H$, so that $(aH)^0 = a^0H$.

With a negative exponent, say $n = -3$, we have

$$\begin{aligned}(aH)^{-3} &= ((aH)^{-1})^3 \\ &= (aH)^{-1} \cdot (aH)^{-1} \cdot (aH)^{-1} \\ &= a^{-1}H \cdot a^{-1}H \cdot a^{-1}H \\ &= (a^{-1})^3H \\ &= a^{-3}H.\end{aligned}$$

Therefore, $(aH)^{-3} = a^{-3}H$.

Example 22.7 suggests the following theorem, whose proof is left for you as an exercise.

Theorem 22.8. *Let G be a group, and let H be its subgroup. Assume G/H satisfies the coset multiplication shortcut. Given $aH \in G/H$, we have $(aH)^n = a^nH$ for all integer exponents n.*

Here is an example of an additive group. Recall that Theorem 21.11 (i.e., the coset addition shortcut), which states $(a+H)+(b+H) = (a+b)+H$, holds for any additive group G and its subgroup H, since additive groups are always commutative.

Example 22.9. Consider the subgroup $H = \{0, 4, 8\}$ of the additive group $\mathbb{Z}_{12}$. In Example 19.5, we found the following distinct cosets of H:

- $0 + H = 4 + H = 8 + H = \{0, 4, 8\}$ (original subgroup).
- $1 + H = 5 + H = 9 + H = \{1, 5, 9\}$.
- $2 + H = 6 + H = 10 + H = \{2, 6, 10\}$.
- $3 + H = 7 + H = 11 + H = \{3, 7, 11\}$.

Thus, $\mathbb{Z}_{12}/H = \{0 + H, 1 + H, 2 + H, 3 + H\}$. For instance, $(2 + H) + (3 + H) = (2 + 3) + H = 1 + H$, since $5 + H = 1 + H$. Hence, the coset sum $(2 + H) + (3 + H)$ is contained in $\mathbb{Z}_{12}/H$.

The additive identity element of $\mathbb{Z}_{12}/H$ is $0 + H$. For all $a + H \in \mathbb{Z}_{12}/H$, we have

$$(0 + H) + (a + H) = (0 + a) + H = a + H$$

and

$$(a + H) + (0 + H) = (a + 0) + H = a + H.$$

For additive inverses in $\mathbb{Z}_{12}/H$, consider the following. We have $(3+H)+(9+H) = (3 + 9) + H = 0 + H$, since $3 + 9 = 0$ in $\mathbb{Z}_{12}$. Symbolically, we write the following:

- In $\mathbb{Z}_{12}$, $3 + 9 = 0$ implies $-3 = 9$; i.e., the additive inverse of 3 is 9.
- In $\mathbb{Z}_{12}/H$, $(3 + H) + (9 + H) = 0 + H$ says $-(3 + H) = 9 + H$; the additive inverse of $3 + H$ is $9 + H$.

Combining these two, we obtain $-(3+H) = 9+H = -3+H$, so that $-(3+H) = -3+H$.

Example 22.9 above can be generalized as follows, whose proof is left for you as an exercise.

Theorem 22.10. *Let G be an additive group, and let H be a subgroup of G. Then G/H satisfies the coset addition shortcut and is a group under coset addition.*

We end the chapter with the following observation. Theorem 22.4 says:

$$\boxed{\text{The coset multiplication shortcut holds in } G/H} \implies \boxed{G/H \text{ is a quotient group}}.$$

We might ask, "When does the shortcut hold?" A possible answer is, "When G is commutative," as proved in Theorem 21.8. But in Chapter 21, Exercises #8 and #9, we saw that the shortcut also holds in D_4/Z, where $Z = \{\varepsilon, r_{180}\}$, even though D_4 is *non-commutative*. So the story is a bit more complicated!

Exercises

1. Consider the subgroup $H = \{0, 4, 8\}$ of the additive group $\mathbb{Z}_{12}$. For each $a \in \mathbb{Z}_{12}$, find and compare the orders of $a \in \mathbb{Z}_{12}$ and $a + H \in \mathbb{Z}_{12}/H$. What conjecture do you have?
2. Consider the subgroup $H = \{1, 3, 9\}$ of the multiplicative group U_{13}. For each $a \in U_{13}$, find and compare the orders of $a \in U_{13}$ and $aH \in U_{13}/H$. What conjecture do you have?

3. Consider the subgroup $H = \{1, 10, 26\}$ of U_{37}. Verify that H is equal to $\langle 10 \rangle = \{10^k \mid k \in \mathbb{Z}\}$, i.e., the cyclic subgroup generated by 10. (This computation is referred to in Section 22.2.)

4. Consider the subgroup $H = \{1, 10, 26\}$ of U_{37}.
   (a) Find and compare the orders of $6 \in U_{37}$ and $6H \in U_{37}/H$.
   (b) Repeat part (a) with $34 \in U_{37}$ and $34H \in U_{37}/H$. It might help to write 34 as -3 modulo 37.
   (c) Repeat part (a) with $4 \in U_{37}$ and $4H \in U_{37}/H$.
   (d) What conjecture do you have?

5. Consider the subgroup $H = \{1, 10, 26\}$ of U_{37}. Let $a \in U_{37}$ with $\text{ord}(a) = 18$. Show that $(aH)^{18} = 1H$. What does this say about the order of aH in U_{37}/H? Explain.

6. Our friends are working on Exercise #4:

   Elizabeth: Phew! I just found that $\text{ord}(4) = 18$ in U_{37}.

   Anita: Great! So $\text{ord}(4H)$ must be 18 as well, since $(4H)^{18} = 4^{18}H = 1H$.

   Elizabeth: But do we know if 18 is the *smallest* positive exponent for $4H$?

   Anita: Sure. If n is less than 18, then $(4H)^n = 4^nH$ can't equal $1H$, because $4^n \neq 1$.

   How would you respond to Anita?

7. **Prove:** Consider the subgroup $H = \{1, 10, 26\}$ of U_{37}. Let $aH \in U_{37}/H$ where $a \in U_{37}$. Then $\text{ord}(aH)$ in U_{37}/H is a divisor of $\text{ord}(a)$ in U_{37}.

8. Consider the subgroup $H = \{1, 10, 26\}$ of U_{37}.
   (a) Find $(15H)^{-1}$, i.e., the multiplicative inverse of $15H$ in U_{37}/H.
   (b) Find $(28H)^{-1}$.
   (c) Find $(3H)^{-1}$.

9. Consider the subgroup $H = \{1, 7\}$ of U_{16}.
   (a) Quick! How many distinct left (or right) cosets of H are there? Explain how you know.
   (b) Find the quotient group U_{16}/H.
   (c) Create the group table for U_{16}/H and verify that it's a group under coset multiplication.
   (d) Find the order of each $aH \in U_{16}/H$. Is the group cyclic?

10. Consider the subgroup $H = \{1, 9\}$ of U_{16}.
    (a) Find the quotient group U_{16}/H and determine if it's cyclic.
    (b) Compare your work in part (a) with Exercise #9. Are you surprised by the results?
    (c) U_{16} has another subgroup K with two elements. Find it and determine if U_{16}/K is cyclic.

11. Consider the additive group $\mathbb{Q}$ of rational numbers and its subgroup $\mathbb{Z}$.
    (a) Describe the elements of $\mathbb{Q}$ that are contained in the coset $\frac{1}{5} + \mathbb{Z}$.
    (b) Find all $\alpha \in \mathbb{Q}$ such that $\alpha + \mathbb{Z} = \frac{1}{5} + \mathbb{Z}$.
    (c) Find 10 distinct cosets in $\mathbb{Q}/\mathbb{Z}$.
    (d) Explain why $\mathbb{Q}/\mathbb{Z}$ contains infinitely many cosets.

12. (a) Find the order of $\frac{2}{5} + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$.
    (b) Find the order of $\frac{6}{11} + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$.
    (c) Find the order of $-\frac{3}{4} + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$.
    (d) Explain why every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

13. Consider the additive group $\mathbb{R}$ of real numbers and its subgroup $\mathbb{Z}$. Does every element of $\mathbb{R}/\mathbb{Z}$ have finite order? Explain why or why not.

14. Let G be a (multiplicative) group, and let H be its subgroup. Suppose G/H satisfies the coset multiplication shortcut. Consider a function $\theta : G \to G/H$ where $\theta(a) = aH$ for all $a \in G$. Prove that θ is a homomorphism.

    Remark. Recall from Section 17.1 that homomorphisms provide a *unifying language* to talk about familiar algebraic properties (e.g., exponent rules, distributive law, etc.). Here's another such instance. This time, we described the coset multiplication shortcut using the language of homomorphisms.

15. Let θ be the homomorphism from Exercise #14; i.e., $\theta : G \to G/H$ where $\theta(a) = aH$ for all $a \in G$.
    (a) Explain why θ is onto.
    (b) Is θ necessarily one-to-one? If so, prove it. If not, provide a counterexample.
    (c) **Prove:** θ is one-to-one if and only if $H = \{\varepsilon\}$.

16. Let G be a cyclic group, and let H be a subgroup of G. Explain why G/H satisfies the coset multiplication shortcut, which in turn implies that G/H is a quotient group.

17. Recall from Example 13.4 that U_{13} is cyclic with generator 2; i.e., $U_{13} = \langle 2 \rangle$. With the subgroup $H = \{1, 3, 9\}$ of U_{13}, verify that U_{13}/H is cyclic with generator $2H$. (This exercise and Exercises #18 and #19 below are referenced in Chapter 23, Exercise #9.)

18. Observe that $\mathbb{Z}_{12}$ is cyclic with generator 1; i.e., $\mathbb{Z}_{12} = \langle 1 \rangle$. With the subgroup $H = \{0, 4, 8\}$ of $\mathbb{Z}_{12}$, verify that $\mathbb{Z}_{12}/H$ is cyclic with generator $1 + H$.

19. It turns out that U_{37} is cyclic with generator 2; i.e., $U_{37} = \langle 2 \rangle$. With the subgroup $H = \{1, 10, 26\}$ of U_{37}, is the quotient group U_{37}/H cyclic? Explain your reasoning.

20. In Example 22.7, we used the interpretation $(aH)^{-3} = ((aH)^{-1})^3$ to show that $(aH)^{-3} = a^{-3}H$. This time, use the interpretation $(aH)^{-3} = ((aH)^3)^{-1}$ to obtain the same result.

21. Prove Theorem 22.8.

    Hint: When n is negative, write it as $n = -(-n)$ where $-n$ is positive.

22. Prove Theorem 22.10.