Chapter 5

Cosets, Lagrange's Theorem, and Normal Subgroups

5.1 Cosets

Undoubtably, you've noticed numerous times that if G is a group with $H \leq G$ and $g \in G$, then both $|H|$ and $|g|$ divide $|G|$. The theorem that says this is always the case is called Lagrange's theorem and we'll prove it towards the end of this chapter. We begin with a definition.

Definition 5.1. Let G be a group and let $H \leq G$ and $a \in G$. The subsets

$$aH := \{ah \mid h \in H\}$$

and

$$Ha := \{ha \mid h \in H\}$$

are called the **left** and **right cosets of** H **containing** a, respectively.

To gain some insight, let's tinker with an example. Consider the dihedral group $D_3 = \langle r, s \rangle$ and let $H = \langle s \rangle \leq D_3$. To compute the right cosets of H, we need to multiply all of the elements of H on the right by the elements of G. We see that

$$\begin{aligned}
He &= \{ee, se\} = \{e, s\} = H \\
Hr &= \{er, sr\} = \{r, sr\} \\
Hr^2 &= \{er^2, sr^2\} = \{r^2, rs\} \\
Hs &= \{es, ss\} = \{s, e\} = H \\
Hsr &= \{esr, ssr\} = \{sr, r\} \\
Hrs &= \{ers, srs\} = \{rs, ssr^2\} = \{rs, r^2\}.
\end{aligned}$$

Despite the fact that we made six calculations (one for each element in D_3), if we scan the list, we see that there are only 3 distinct cosets, namely

$$\begin{aligned}
H = He = Hs &= \{e, s\} \\
Hr = Hsr &= \{r, sr\} \\
Hr^2 = Hrs &= \{r^2, rs\}.
\end{aligned}$$

We can make a few more observations. First, the resulting cosets formed a partition of D_3. That is, every element of D_3 appears in exactly one coset. Moreover, all the cosets are the same size—two elements in each coset in this case. Lastly, each coset can be named in multiple ways. In particular, the elements of the coset are exactly the elements of D_3 we multiplied H by. For example, $Hr = Hsr$ and the elements of this coset are r and sr. Shortly, we will see that these observations hold, in general.

Here is another significant observation we can make. Consider the Cayley diagram for D_3 with generating set $\{r, s\}$ that is given in Figure 5.1. Given this Cayley diagram, we can visualize the subgroup H and its clones. Moreover, H and its clones are exactly the 3 right cosets of H. We'll see that, in general, the *right* cosets of a given subgroup are always the subgroup and its clones (see Problem 5.15).

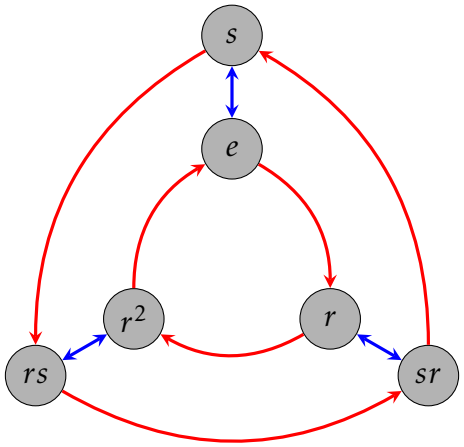

Figure 5.1. Cayley diagram for D_3 with generating set $\{r, s\}$.

Problem 5.2. Consider the group D_3. Find all the left cosets for $H = \langle s \rangle$. Are they the same as the right cosets? Are they the same as the subgroup H and its clones that we can see in the Cayley graph for D_3 with generating set $\{r, s\}$?

As the previous exercise indicates, the collections of left and right cosets may not be the same and when they are not the same, the subgroup and its clones do not coincide with the left cosets.

You might be thinking that somehow right cosets are "better" than left cosets since we were able to visualize them in the Cayley graph. However, this is just a consequence of our convention of composing actions from right to left. If we had adopted a left to right convention, then we would be able to visualize the left cosets in Cayley diagrams.

Computing left and right cosets using a group table is fairly easy. Hopefully, you figured out in Problem 5.2 that the left cosets of $H = \langle s \rangle$ in D_3 are $H = \{e, s\}$, $srH = \{r^2, sr\}$, and $rsH = \{r, rs\}$. Now, consider the following group table for D_3 that has the rows and columns arranged according to the left cosets of H.

$*$	e	s	sr	r^2	rs	r
e	e	s	sr	r^2	rs	r
s	s	e	r	rs	r^2	sr
sr	sr	r^2	e	s	r	rs
r^2	r^2	sr	rs	r	s	e
rs	rs	r	r^2	sr	e	s
r	r	rs	s	e	sr	r^2

The left coset srH must appear in the row labeled by sr and in the columns labeled by the elements of $H = \{e, s\}$. We've depicted this below.

$*$	e	s	sr	r^2	rs	r
e	e	s	sr	r^2	rs	r
s	s	e	r	rs	r^2	sr
sr	sr	r^2	e	s	r	rs
r^2	r^2	sr	rs	r	s	e
rs	rs	r	r^2	sr	e	s
r	r	rs	s	e	sr	r^2

On the other hand, the right coset Hsr must appear in the column labeled by sr and the rows labeled by the elements of $H = \{e, s\}$:

$*$	e	s	sr	r^2	rs	r
e	e	s	sr	r^2	rs	r
s	s	e	r	rs	r^2	sr
sr	sr	r^2	e	s	r	rs
r^2	r^2	sr	rs	r	s	e
rs	rs	r	r^2	sr	e	s
r	r	rs	s	e	sr	r^2

As we can see from the tables, $srH \neq Hsr$ since $\{sr, r^2\} \neq \{sr, r\}$. If we color the entire group table for D_3 according to which *left* coset an element belongs to, we get the following.

$*$	e	s	sr	r^2	rs	r
e	e	s	sr	r^2	rs	r
s	s	e	r	rs	r^2	sr
sr	sr	r^2	e	s	r	rs
r^2	r^2	sr	rs	r	s	e
rs	rs	r	r^2	sr	e	s
r	r	rs	s	e	sr	r^2

We would get a similar table (but in this case, not identical) if we colored the elements according to the right cosets.

Let's tackle a few more examples.

Problem 5.3. Consider D_3 and let $K = \langle r \rangle$.

(a) Find all of the left cosets of K and then find all of the right cosets of K in D_3. Any observations?

(b) Write down the group table for D_3, but this time arrange the rows and columns according to the left cosets for K. Color the entire table according to which *left* coset an element belongs to. Can you visualize the observations you made in part (a)?

Problem 5.4. Consider Q_8. Let $H = \langle i \rangle$ and $K = \langle -1 \rangle$.

(a) Find all of the left cosets of H and all of the right cosets of H in Q_8.

(b) Write down the group table for Q_8 so that rows and columns are arranged according to the left cosets for H. Color the entire table according to which *left* coset an element belongs to.

(c) Find all of the left cosets of K and all of the right cosets of K in Q_8.

(d) Write down the group table for Q_8 so that rows and columns are arranged according to the left cosets for K. Color the entire table according to which *left* coset an element belongs to.

Problem 5.5. Consider S_4. Find all of the left cosets and all of the right cosets of A_4 in S_4. Instead of doing brute-force, try to be clever. *Hint:* What happens when you compose two even permutations versus an even permutation and an odd permutation?

Problem 5.6. Consider $\mathbb{Z}_8$. Find all of the left cosets and all of the right cosets of $\langle 4 \rangle$ in $\mathbb{Z}_8$. Why do you know the left and right cosets are the same without actually verifying?

Problem 5.7. Consider $(\mathbb{Z}, +)$. Find all of the left cosets and all of the right cosets of $3\mathbb{Z}$ in $\mathbb{Z}$. Why do you know the left and right cosets are the same without actually verifying?

Theorem 5.8. Let G be a group and let $H \leq G$. If G is abelian, then for all $a \in G$, $aH = Ha$. That is, if G is abelian, then the left cosets of H are the same as the right cosets of H.

Exercises 5.2 and 5.3 illustrate that if a group is non-abelian, then the cosets of a subgroup may or may not coincide. That is, knowing that the group is non-abelian is not enough to determine whether the left and right cosets are different.

In all of the examples we've seen so far, the left and right cosets partitioned G into equal-sized chunks. We need to prove that this is true in general. To prove that the cosets form a partition, we will define an appropriate equivalence relation.

Theorem 5.9. Let G be a group and let $H \leq G$. Define $\sim_L$ and $\sim_R$ via

$$a \sim_L b \text{ if and only if } a^{-1}b \in H$$

and

$$a \sim_R b \text{ if and only if } ab^{-1} \in H.$$

Then both $\sim_L$ and $\sim_R$ are equivalence relations.*

*You only need to prove that either $\sim_L$ or $\sim_R$ is an equivalence relation as the proof for the other is similar.

Since $\sim_L$ and $\sim_R$ are equivalence relations, the corresponding equivalence classes form a partition of G. If $a \in G$, then the "left" and "right" equivalence classes containing a are given by

$$[a]_{\sim_L} = \{g \in G \mid a \sim_L g\}$$

and

$$[a]_{\sim_R} = \{g \in G \mid a \sim_R g\}.$$

The next theorem tells us that the equivalence classes determined by $\sim_L$ and $\sim_R$ are indeed the left and right cosets of $H \leq G$, respectively.

Theorem 5.10. If G is a group and $H \leq G$, then $[a]_{\sim_L} = aH$ and $[a]_{\sim_R} = Ha$ for all $a \in G$.

Corollary 5.11. If G is a group and $H \leq G$, then the left (respectively, right) cosets of H form a partition of G.

Next, we argue that all of the cosets have the same size.

Theorem 5.12. Let G be a group, $H \leq G$, and $a \in G$. Define $\phi : H \to aH$ via $\phi(h) = ah$. Then ϕ is one-to-one and onto.

Corollary 5.13. Let G be a group and let $H \leq G$. Then all of the left and right cosets of H are the same size as H. In other words $\#(aH) = |H| = \#(Ha)$ for all $a \in G$.[†]

The next theorem provides a useful characterization of cosets. Each part can either be proved directly or by appealing to previous results in this section.

Theorem 5.14. Let G be a group and let $H \leq G$.

(a) If $a \in G$, then $a \in aH$ (respectively, Ha).

(b) We have $b \in aH$ (respectively, Ha) if and only if $aH = bH$ (respectively, $Ha = Hb$).

(c) If $a \in H$, then $aH = H = Ha$.

(d) If $a \notin H$, then for all $h \in H$, $ah \notin H$ (respectively, $ha \notin H$).

The upshot of part (b) of Theorem 5.14 is that cosets can have different names. In particular, if b is an element of the left coset aH, then we could have just as easily called the coset by the name bH. In this case, both a and b are called **coset representatives**.

The final result of this chapter verifies that the clones of a subgroup in a Cayley diagram coincide with the right cosets of the subgroup.

Problem 5.15. Let G be a finite group with generating set S and let H be a proper subgroup of G and suppose we can visualize the subgroup for H in the Cayley diagram for G using S as the generating set.

(a) If $g \in G$, verify that the right coset Hg is a clone of H. *Hint:* Suppose $s \in S$ and $h_1, h_2 \in H$ such that there is an arrow labeled by s that points from h_1 to h_2. Argue that there is an arrow labeled by s pointing from $h_1 g$ to $h_2 g$.

(b) If C is a clone of H, prove that C is a right coset of H.

[†]As you probably expect, $\#(aH)$ denotes the size of aH. Note that everything works out just fine even if H has infinite order.

5.2 Lagrange's Theorem

We're finally ready to state Lagrange's Theorem, which is named after the Italian born mathematician Joseph Louis Lagrange. It turns out that Lagrange did not actually prove the theorem that is named after him. The theorem was actually proved by Carl Friedrich Gauss in 1801.

Theorem 5.16 (Lagrange's Theorem)**.** Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

This simple sounding theorem is extremely powerful. One consequence is that groups and subgroups have a fairly rigid structure. Suppose G is a finite group and let $H \leq G$. Since G is finite, there must be a finite number of distinct left cosets, say $H, a_2H, \ldots, a_nH$. Corollary 5.13 tells us that each of these cosets is the same size. In particular, Lagrange's Theorem implies that for each $i \in \{1, \ldots, n\}$, $|a_iH| = |G|/n$, or equivalently $n = |G|/|a_iH|$. This is depicted in Figure 5.2, where each rectangle represents a coset and we've labeled a single coset representative in each case.

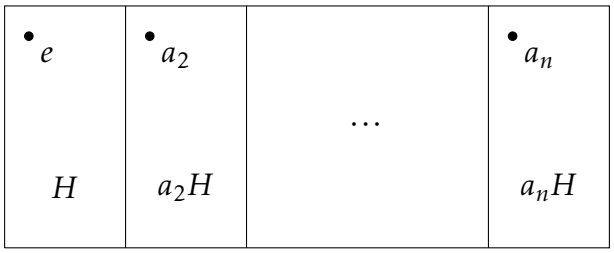

Figure 5.2

One important consequence of Lagrange's Theorem is that it narrows down the possible sizes for subgroups.

Problem 5.17. Suppose G is a group of order 48. What are the possible orders for subgroups of G?

Lagrange's Theorem tells us what the possible orders of a subgroup are, but if k is a divisor of the order of a group, it does not guarantee that there is a subgroup of order k. It's not too hard to show that the converse of Lagrange's Theorem is true for cyclic groups. However, it's not true, in general.

Problem 5.18. Provide an example of a finite group G such that $|G|$ has a divisor k but G does not have a subgroup of order k.

Using Lagrange's Theorem, we can quickly prove both of the following theorems.

Theorem 5.19. Let G be a finite group and let $a \in G$. Then $|a|$ divides $|G|$.

Since the converse of Lagrange's Theorem is not true, the converse of Theorem 5.19 is not true either. However, it is much easier to find a counterexample.

Problem 5.20. Argue that S_4 does not have any elements of order 8.

Theorem 5.21. For every prime p, if G has order p, then $G \cong \mathbb{Z}_p$.

Corollary 5.22. For every prime p, there is a unique group of order p up to isomorphism.

Lagrange's Theorem motivates the following definition.

Definition 5.23. Let G be a group and let $H \leq G$. The **index** of H in G is the number of cosets (left or right) of H in G. Equivalently, if G is finite, then the index of H in G is equal to $|G|/|H|$. We denote the index via $[G : H]$.

Problem 5.24. Let $H = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

(a) Find $[A_4 : H]$.

(b) Find $[S_4 : H]$.

Problem 5.25. Find $[\mathbb{Z} : 4\mathbb{Z}]$.

5.3 Normal Subgroups

We've seen an example where the left and right cosets of a subgroup were different and a few examples where they coincided. In the latter case, the subgroup has a special name.

Definition 5.26. Let G be a group and let $H \leq G$. If $aH = Ha$ for all $a \in G$, then we say that H is a **normal subgroup**. If H is a normal subgroup of G, then we write $H \trianglelefteq G$.

Problem 5.27. Provide an example of group that has a subgroup that is not normal.

Problem 5.28. Suppose G is a finite group and let $H \leq G$. If $H \trianglelefteq G$ and we arrange the rows and columns of the group table for G according to the left cosets of H and then color the corresponding cosets, what property will the table have? Is the converse true? That is, if the table has the property you discovered, will H be normal in G?

There are a few instances where we can guarantee that a subgroup will be normal.

Theorem 5.29. Suppose G is a group. Then $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.

Theorem 5.30. If G is an abelian group, then all subgroups of G are normal.

A group does not have to be abelian in order for all the proper subgroups to be normal.

Problem 5.31. Argue that all of the proper subgroups of Q_8 are normal in Q_8.

Theorem 5.32. Suppose G is a group and let $H \leq G$ such that $[G : H] = 2$. Then $H \trianglelefteq G$.

It turns out that normality is not transitive.

Problem 5.33. Consider $\langle s \rangle = \{e, s\}$ and $\langle r^2, sr^2 \rangle = \{e, r^2, sr^2, s\}$. It is clear that

$$\langle s \rangle \leq \langle r^2, sr^2 \rangle \leq D_4.$$

Show that $\langle s \rangle \trianglelefteq \langle r^2, sr^2 \rangle$ and $\langle r^2, sr^2 \rangle \trianglelefteq D_4$, but $\langle s \rangle \not\trianglelefteq D_4$.

The previous problem illustrates that $H \trianglelefteq K \trianglelefteq G$ does not imply $H \trianglelefteq G$.

Definition 5.34. Suppose G is a group and let $H \leq G$. For $g \in G$, we define the **conjugate of H by g** to be the set

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}.$$

Theorem 5.35. Suppose G is a group and let $H \leq G$. Then $H \trianglelefteq G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

Another way of thinking about normal subgroups is that they are "closed under conjugation." It's not too hard to show that if $gHg^{-1} \subseteq H$ for all $g \in G$, then we actually have $gHg^{-1} = H$ for all $g \in G$. This implies that $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in G$. This seemingly stronger version of Theorem 5.35 is sometimes used as the definition of normal subgroup. This discussion motivates the following definition.

Definition 5.36. Let G be a group and let $H \leq G$. The **normalizer of H in G** is defined via

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Theorem 5.37. If G is a group and $H \leq G$, then $N_G(H)$ is a subgroup of G.

Theorem 5.38. If G is a group and $H \leq G$, then $H \trianglelefteq N_G(H)$. Moreover, $N_G(H)$ is the largest subgroup of G in which H is normal.

It is worth pointing out that the "smallest" $N_G(H)$ can be is H itself—certainly a subgroup is a normal subgroup of itself. Also, the "largest" that $N_G(H)$ can be is G, which happens precisely when H is normal in G.

Problem 5.39. Find $N_{D_4}(V_4)$.

Problem 5.40. Find $N_{D_3}(\langle s \rangle)$.

We conclude this chapter with a few remarks. We've seen examples of groups that have subgroups that are normal and subgroups that are not normal. In an abelian group, all the subgroups are normal. It turns out that there are examples of groups that have no normal subgroups. These groups are called **simple groups**. The smallest simple group is A_5, which has 60 elements and lots of proper nontrivial subgroups, none of which are normal.

The classification of the finite simple groups is a theorem stating that every finite simple group belongs to one of four categories:

1. A cyclic group with prime order;
2. An alternating group of degree at least 5;
3. A simple group of Lie type, including both
   (a) the classical Lie groups, namely the simple groups related to the projective special linear, unitary, symplectic, or orthogonal transformations over a finite field;

(b) the exceptional and twisted groups of Lie type (including the Tits group);

4. The 26 sporadic simple groups.

These groups can be seen as the basic building blocks of all finite groups, in a way reminiscent of the way the prime numbers are the basic building blocks of the natural numbers.

The classification theorem has applications in many branches of mathematics, as questions about the structure of finite groups (and their action on other mathematical objects) can sometimes be reduced to questions about finite simple groups. Thanks to the classification theorem, such questions can sometimes be answered by checking each family of simple groups and each sporadic group. The proof of the theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004.

The classification of the finite simple groups is a modern achievement in abstract algebra and I highly encourage you to go learn more about it. You might be especially interested in learning about one of the sporadic groups called the **Monster Group**.