Chapter 3

Subgroups and Isomorphisms

For the next two sections, it would be useful to have all of the Cayley diagrams we've encountered in one place for reference. So, before continuing, gather up the following Cayley diagrams:

- $\text{Spin}_{1\times 2}$. There are 3 of these. I drew one for you in Section 2.6 and you discovered two more in Problem 2.68.
- S_2. See Problem 2.71(a).
- R_4. See Problem 2.71(b).
- V_4. See Problem 2.71(c).
- D_3. There are two of these. See Problems 2.71(d) and 2.71(e).
- S_3. See Problem 2.71(f).
- D_4. See Problem 2.71(g).

3.1 Subgroups

Problem 3.1. Recall the definition of "subset." What do you think "subgroup" means? Try to come up with a potential definition. Try not to read any further before doing this.

Problem 3.2. Examine your Cayley diagrams for D_4 (with generating set $\{r,s\}$) and R_4 (with generating set $\{r\}$) and make some observations. How are they similar and how are they different? Can you reconcile the similarities and differences by thinking about the actions of each group?

Hopefully, one of the things you noticed in the previous problem is that we can "see" R_4 inside of D_4. You may have used different colors in each case and maybe even labeled the vertices with different words, but the overall structure of R_4 is there nonetheless.

Problem 3.3. If you ignore the labels on the vertices and just pay attention to the configuration of arrows, it appears that there are two copies of the Cayley diagram for R_4 in the Cayley diagram for D_4. Isolate these two copies by ignoring the edges that correspond to the generator s. Now, paying close attention to the words that label the vertices from the original Cayley diagram for D_4, are either of these groups in their own right?

Recall that the identity must be one of the elements included in a group. If this didn't occur to you when doing the previous problem, you might want to go back and rethink your answer. Just like in the previous problem, we can often "see" smaller groups living inside larger groups. These smaller groups are called **subgroups**.

Definition 3.4. Let G be a group and let H be a subset of G. Then H is a **subgroup** of G, written $H \leq G$, provided that H is a group in its own right under the binary operation inherited from G.

The phrase "under the binary operation inherited from G" means that to combine two elements in H, we should treat the elements as if they were in G and perform the binary operation of G.

In light of Problem 3.3, we would write $R_4 \leq D_4$. The second sub-diagram of the Cayley diagram for D_4 (using $\{r, s\}$ as the generating set) that resembles R_4 cannot be a subgroup because it does not contain the identity. However, since it looks a lot like R_4, we call it a **clone** of R_4. For convenience, we also say that a subgroup is a clone of itself.

Problem 3.5. Let G be a group and let $H \subseteq G$. If we wanted to determine whether H is a subgroup of G, can we skip checking any of the axioms? Which axioms must we verify?

Let's make the observations of the previous problem a bit more formal.

Theorem 3.6 (Two Step Subgroup Test)**.** Suppose G is a group and H is a nonempty subset of G. Then $H \leq G$ if and only if (i) for all $h \in H$, $h^{-1} \in H$, as well, and (ii) H is closed under the binary operation of G.

Notice that one of the hypotheses of Theorem 3.6 is that H be nonempty. This means that if we want to prove that a certain subset H is a subgroup of a group G, then one of the things we must do is verify that H is in fact nonempty. In light of this, the "Two Step Subgroup Test" should probably be called the "Three Step Subgroup Test".

As Theorems 3.7 and 3.9 will illustrate, there are a couple of subgroups that every group contains.

Theorem 3.7. If G is a group, then $\{e\} \leq G$.

The subgroup $\{e\}$ is referred to as the **trivial subgroup**. All other subgroups are called **nontrivial**.

Problem 3.8. Let G be a group. What does the Cayley diagram for the subgroup $\{e\}$ look like? What are you using as your generating set?

Earlier, we referred to subgroups as being "smaller." However, our definition does not imply that this has to be the case.

Theorem 3.9. If G is a group, then $G \leq G$.

We refer to subgroups that are not equal to the whole group as **proper subgroups**. If H is a proper subgroup, then we may write $H < G$.

Recall Theorem 2.51 that states that if G is a group under $*$ and S is a subset of G, then $\langle S \rangle$ is also a group under $*$. Let's take this a step further.

Theorem 3.10. If G is a group and $S \subseteq G$, then $\langle S \rangle \leq G$. In particular, $\langle S \rangle$ is the smallest subgroup of G containing S.

The subgroup $\langle S \rangle$ is called the **subgroup generated by** S. In the special case when S equals a single element, say $S = \{g\}$, then

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\},$$

which is called the (**cyclic**) **subgroup generated by** g. Every subgroup can be written in the "generated by" form. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. In particular, $\langle H \rangle = H$ for $H \leq G$, and as a special case, we have $\langle G \rangle = G$.

Problem 3.11. Consider $\text{Spin}_{1\times 2}$ with generating set $\{s_{11}, s_{22}, s_{12}\}$.

(a) Find the Cayley diagram for the subgroup $\langle s_{11} \rangle$ inside the Cayley diagram for $\text{Spin}_{1\times 2}$. Identify all of the clones of $\langle s_{11} \rangle$ inside $\text{Spin}_{1\times 2}$.

(b) Find the Cayley diagram for the subgroup $\langle s_{11}, s_{22} \rangle$ inside the Cayley diagram of $\text{Spin}_{1\times 2}$. Identify the clones of $\langle s_{11}, s_{22} \rangle$ inside $\text{Spin}_{1\times 2}$.

One of the benefits of Cayley diagrams is that they are useful for visualizing subgroups. However, recall that if we change our set of generators, we might get a very different looking Cayley diagram. The upshot of this is that we may be able to see a subgroup in one Cayley diagram for a given group, but not be able to see it in the Cayley diagram arising from a different generating set.

Problem 3.12. We currently have two different Cayley diagrams for D_3 (see Problems 2.21 and 2.56).

(a) Can you find the Cayley diagram for the trivial subgroup $\langle e \rangle$ in either Cayley diagram for D_3? Identify all of the clones of $\langle e \rangle$ in both Cayley diagrams for D_3.

(b) Can you find the Cayley diagram for the subgroup $\langle r \rangle = R_3$ in either Cayley diagram for D_3? If possible, identify all of the clones of R_3 in the Cayley diagrams for D_3.

(c) Can you find the Cayley diagrams for $\langle s \rangle$ and $\langle s' \rangle$ in either Cayley diagram for D_3? If possible, identify all of the clones of $\langle s \rangle$ and $\langle s' \rangle$ in the Cayley diagrams for D_3.

Problem 3.13. Consider D_4. Let h be the reflection of the square over the horizontal midline and let v be the reflection over the vertical midline. Which of the following are subgroups of D_4? In each case, justify your answer. If a subset is a subgroup, try to find a minimal generating set. Also, determine whether you can see the subgroups in our Cayley diagram for D_4 with generating set $\{r, s\}$.

(a) $\{e, r^2\}$

(b) $\{e, h\}$

(c) $\{e, h, v\}$

(d) $\{e, h, v, r^2\}$

Perhaps you recognized the set in part (d) of the previous problem as being the Klein four-group V_4. It follows that $V_4 \leq D_4$.

Let's introduce a group we haven't seen yet. Define the **quaternion group** to be the group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ having the Cayley diagram with generating set $\{i, j, -1\}$ given in Figure 3.1. In this case, 1 is the identity of the group.

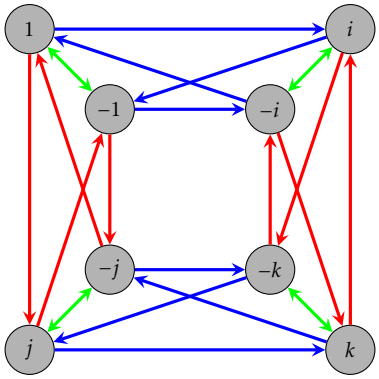

Figure 3.1. Cayley diagram for Q_8 with generating set $\{-1, i, j\}$.

Notice that I didn't mention what the actions actually do. For now, let's not worry about that. The relationship between the arrows and vertices tells us everything we need to know. Also, let's take it for granted that Q_8 actually is a group.

Problem 3.14. Consider the Cayley diagram for Q_8 given in Figure 3.1.

(a) Which arrows correspond to which generators in our Cayley diagram for Q_8?

(b) What is i^2 equal to? That is, what element of $\{1, -1, i, -i, j, -j, k, -k\}$ is i^2 equal to? How about i^3, i^4, and i^5?

(c) What are j^2, j^3, j^4, and j^5 equal to?

(d) What is $(-1)^2$ equal to?

(e) What is ij equal to? How about ji?

(f) Can you determine what k^2 and ik are equal to?

(g) Can you identify a generating set consisting of only two elements? Can you find more than one?

(h) What subgroups of Q_8 can you see in the Cayley diagram in Figure 3.1?

(i) Find a subgroup of Q_8 that you cannot see in the Cayley diagram.

Problem 3.15. Consider $(\mathbb{R}^3, +)$, where $\mathbb{R}^3$ is the set of all 3-entry row vectors with real number entries (e.g., (a, b, c) where $a, b, c \in \mathbb{R}$) and $+$ is ordinary vector addition. It turns out that $(\mathbb{R}^3, +)$ is an abelian group with identity $(0, 0, 0)$.

(a) Let H be the subset of $\mathbb{R}^3$ consisting of vectors with first coordinate 0. Is H a subgroup of $\mathbb{R}^3$? Prove your answer.

(b) Let K be the subset of $\mathbb{R}^3$ consisting of vectors whose entries sum to 0. Is K a subgroup of $\mathbb{R}^3$? Prove your answer.

(c) Construct a subset of $\mathbb{R}^3$ (different from H and K) that is *not* a subgroup of $\mathbb{R}^3$.

Problem 3.16. Consider the group $(\mathbb{Z}, +)$ (under ordinary addition).

(a) Show that the even integers, written $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$, form a subgroup of $\mathbb{Z}$.

(b) Show that the odd integers are not a subgroup of $\mathbb{Z}$.

(c) Show that all subsets of the form $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$ are subgroups of $\mathbb{Z}$.

(d) Are there any other subgroups besides the ones listed in part (c)? Explain your answer.

(e) For $n \in \mathbb{Z}$, write the subgroup $n\mathbb{Z}$ in the "generated by" notation. That is, find a set S such that $\langle S \rangle = n\mathbb{Z}$. Can you find more than one way to do it?

Problem 3.17. Consider the group of symmetries of a regular octagon. This group is denoted by D_8, where the operation is composition of actions. The group D_8 consists of 16 elements (8 rotations and 8 reflections). Let H be the subset consisting of the following clockwise rotations: 0°, 90°, 180°, and 270°. Determine whether H is a subgroup of D_8 and justify your answer.

Problem 3.18. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$. Explain why $\mathbb{R} \setminus \{0\}$ is not a subgroup of $\mathbb{R}$ despite the fact that $\mathbb{R} \setminus \{0\} \subseteq \mathbb{R}$ and both are groups (under the respective binary operations).

Theorem 3.19. If G is an abelian group such that $H \leq G$, then H is an abelian subgroup.

Problem 3.20. Is the converse of the previous theorem true? If so, prove it. Otherwise, provide a counterexample.

As we've seen, some groups are abelian and some are not. If G is a group, then we define the **center** of G to be

$$Z(G) := \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Notice that if G is abelian, then $Z(G) = G$. However, if G is not abelian, then $Z(G)$ will be a proper subset of G. In some sense, the center of a group is a measure of how close G is to being abelian.

Theorem 3.21. If G is a group, then $Z(G)$ is an abelian subgroup of G.

Problem 3.22. Find the center of each of the following groups.

(a) S_2

(b) V_4

(c) S_3

(d) D_3

(e) D_4

(f) R_4

(g) R_6

(h) $\text{Spin}_{1\times 2}$

(i) Q_8

(j) $(\mathbb{Z}, +)$

(k) $(\mathbb{R} \setminus \{0\}, \cdot)$

3.2 Subgroup Lattices

One of the goals of this section is to gain better understanding of the structure of groups by studying their subgroups.

Suppose we wanted to find all of the subgroups of a finite group G. Theorems 3.7 and 3.9 tell us that $\{e\}$ and G itself are subgroups of G, but there may be others. Theorem 3.6 tells us that if we want to find other subgroups of G, we need to find nonempty subsets of G that are closed and contain all the necessary inverses. So, one method for finding subgroups would be to find all possible nonempty subsets of G and then go about determining which subsets are subgroups by verifying whether a given subset is closed under inverses and closed under the operation of G. This is likely to be fairly time consuming.

Another approach would be to utilize the fact that every subgroup H of G has a generating set. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. Given a subset S of G, $\langle S \rangle$ is guaranteed to be closed under inverses and the operation of the group G. So, we could determine all of the subgroups of G by generating groups with various subsets S of G. Of course, one drawback is that it might take a bit of effort to determine what $\langle S \rangle$ actually is. Another drawback is that two different subsets S and T may generate the same subgroup.

Let's make this a bit more concrete by exploring an example. Consider the group R_4. What are the subgroups of R_4? Since the order of R_4 is 4, we know that there are $2^4 - 1 = 15$ nonempty subsets of R_4. Some of these are subgroups, but most of them are not. Theorems 3.7 and 3.9 guarantee that $\{e\}$ and R_4 itself are subgroups of R_4. That's

2 out of 15 so far. Are there any others? Let's do an exhaustive search by playing with generating sets. We can certainly be more efficient, but below we list all of the possible subgroups we can generate using subsets of R_4. As you scan the list, you should take a moment to convince yourself that the list is accurate.

$$\langle e \rangle = \{e\}$$
$$\langle r \rangle = \{e, r, r^2, r^3\}$$
$$\langle r^2 \rangle = \{e, r^2\}$$
$$\langle r^3 \rangle = \{e, r^3, r^2, r\}$$
$$\langle e, r \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r^2 \rangle = \{e, r^2\}$$
$$\langle e, r^3 \rangle = \{e, r^3, r^2, r\}$$
$$\langle r, r^2 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^2 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$

Let's make a few observations. Scanning the list, we see only three distinct subgroups:

$$\{e\}, \{e, r^2\}, \{e, r, r^2, r^3\}.$$

Out of 15 nonempty subsets of R_4, only 3 subsets are subgroups. Our exhaustive search guarantees that these are the only subgroups of R_4. It is also worth pointing out that if a subset contains either r or r^3, then that subset generates all of R_4. The reason for this is that $\{r\}$ and $\{r^3\}$ are each minimal generating sets for R_4. More generally, observe that if we increase the size of the generating subset using an element that was already contained in the subgroup generated by the set, then we don't get anything new. For example, consider $\langle r^2 \rangle = \{e, r^2\}$. Since $e \in \langle r^2 \rangle$, we don't get anything new by including e in our generating set. We can state this as a general fact.

Theorem 3.23. Let G be a group and let $g_1, g_2, \ldots, g_n \in G$. If $x \in \langle g_1, g_2, \ldots, g_n \rangle$, then $\langle g_1, g_2, \ldots, g_n \rangle = \langle g_1, g_2, \ldots, g_n, x \rangle$.

In the previous theorem, we are not claiming that $\{g_1, g_2, \ldots, g_n\}$ is a generating set for G—although this may be the case. Instead, are simply making a statement about the subgroup $\langle g_1, g_2, \ldots, g_n \rangle$, whatever it may be.

We can capture the overall relationship between the subgroups of a group G using a **subgroup lattice**. Given a group G, the **lattice of subgroups** of G is the partially ordered set whose elements are the subgroups of G with the partial order relation being set inclusion. It is common to depict the subgroup lattice for a group using a **Hasse diagram**. The Hasse diagram of subgroup lattice is drawn as follows:

(1) Each subgroup H of G is a vertex.

(2) Vertices corresponding to subgroups with smaller order are placed lower in the diagram than vertices corresponding to subgroups with larger order. In particular,

the vertex for $\{e\}$ is placed at the bottom of the diagram and the vertex for G is placed at the top.

(3) There is an edge going up from H to K if $H \leq K$ and there is no subgroup L such that $H \leq L \leq K$ with $L \neq H, K$.

Notice that there is an upward path of edges in the Hasse diagram from H to K if and only if $H \leq K$. For convenience we will not make a distinction between the subgroup lattice for a group G and the corresponding Hasse diagram.

The Hasse diagram for the subgroup lattice for R_4 is given in Figure 3.2.

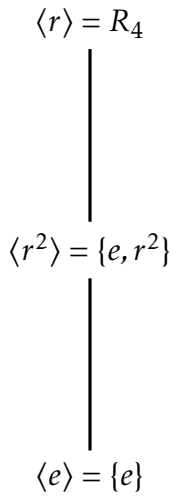

Figure 3.2. Subgroup lattice for R_4.

Let's see what we can do with $V_4 = \{e, v, h, vh\}$. Using an exhaustive search, we find that there are five subgroups:

$\langle e \rangle = \{e\}$

$\langle h \rangle = \{e, h\}$

$\langle v \rangle = \{e, v\}$

$\langle vh \rangle = \{e, vh\}$

$\langle v, h \rangle = \langle v, vh \rangle = \langle h, vh \rangle = \{e, v, h, vh\} = V_4$

For each subgroup above, we've used minimal generating sets to determine the subgroup. The subgroup lattice for V_4 is given in Figure 3.3. Notice that there are no edges among $\langle v \rangle, \langle h \rangle$, and $\langle vh \rangle$. The reason for this is that none of these groups are subgroups of each other.

The next two theorems provide some further insight into the overall structure of subgroups of a group.

Theorem 3.24. If G is a group such that $H, K \leq G$, then $H \cap K \leq G$. Moreover, $H \cap K$ is the largest subgroup contained in both H and K.

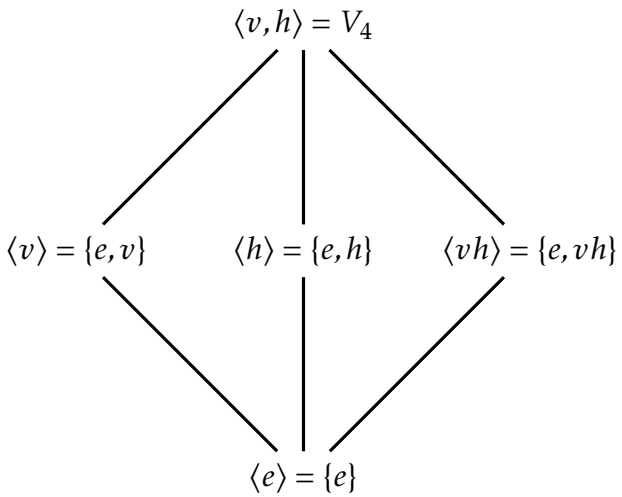

Figure 3.3. Subgroup lattice for V_4.

It turns out that we cannot simply replace "intersection" with "union" in the previous theorem

Problem 3.25. Provide an example of a group G and subgroups H and K such that $H \cup K$ is not a subgroup of G.

Theorem 3.26. If G is a group such that $H, K \leq G$, then $\langle H \cup K\rangle \leq G$. Moreover, $\langle H \cup K\rangle \leq G$ is the smallest subgroup containing both H and K.

Theorems 3.24 and 3.26 justify the use of the word "lattice" in "subgroup lattice". In general, a lattice is a partially ordered set in which every two elements have a unique **meet** (also called a **greatest lower bound** or **infimum**) and a unique **join** (also called a **least upper bound** or **supremum**). In the case of a subgroup lattice for a group G, the meet of subgroups H and K is $H \cap K$ and the join is $\langle H \cup K\rangle$. Figure 3.4 illustrates the meet (Theorem 3.24) and join (Theorem 3.26) in the case when H and K are not comparable.

In the next few problems, you are asked to create subgroup lattices. As you do this, try to minimize the amount of work it takes to come up with all the subgroups.

Problem 3.27. Find all the subgroups of $R_5 = \{e, r, r^2, r^3, r^4\}$ (where r is clockwise rotation of a regular pentagon by 72°) and then draw the subgroup lattice for R_5.

Problem 3.28. Find all the subgroups of $R_6 = \{e, r, r^2, r^3, r^4, r^5\}$ (where r is clockwise rotation of a regular hexagon by 60°) and then draw the subgroup lattice for R_6.

Problem 3.29. Find all the subgroups of $D_3 = \{e, r, r^2, s, sr, sr^2\}$ (where r and s are the usual symmetries of an equilateral triangle) and then draw the subgroup lattice for D_3.

Problem 3.30. Find all the subgroups of $S_3 = \langle s_1, s_2\rangle$ (where s_1 is the action is that swaps the positions of the first and second coins and s_2 is the action that swaps the second and third coins; see Problem 2.58) and then draw the subgroup lattice for S_3. How does your lattice compare to the one in Problem 3.29? You should look back at parts (e) and (f) of Problem 2.71 and ponder what just happened.

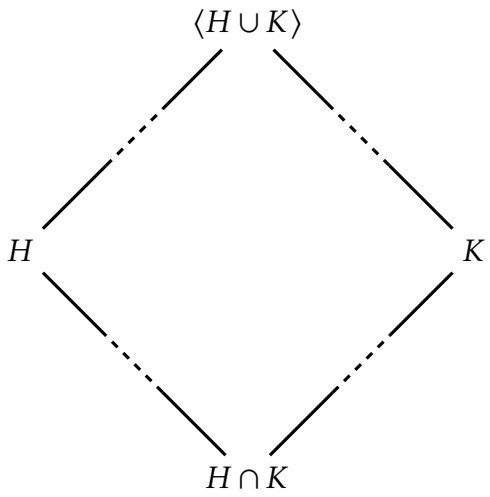

Figure 3.4. Meet and join for subgroups H and K.

Problem 3.31. Find all the subgroups of $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ (where r and s are the usual symmetries of a square) and then draw the subgroup lattice for D_4.

Problem 3.32. Find all the subgroups of $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and then draw the subgroup lattice for Q_8.

3.3 Isomorphisms

As we have been exploring various groups, I'm sure you've noticed that some groups seem to look and behave the same. For example, if we choose the same colors for our arrows and ignore the labels on the vertices, the Cayley diagram for D_3 with generating set $\{s, s'\}$ looks the same as the Cayley diagram for S_3 with generating set $\{s_1, s_2\}$. That is, if we pick the appropriate colors and set the Cayley diagram for D_3 (with generating set $\{s, s'\}$) on top of the Cayley diagram for S_3 (with generating set $\{s_1, s_2\}$) such that the identities match up, then the two Cayley diagrams are identical up to relabeling the rest of the vertices. Figure 3.5 should make this clear. This act of matching up the Cayley diagrams establishes a correspondence between the elements of the two groups:

$$\begin{aligned} e &\mapsto e \\ s &\mapsto s_1 \\ s' &\mapsto s_2 \\ ss' &\mapsto s_1 s_2 \\ s's &\mapsto s_2 s_1 \\ ss's &\mapsto s_1 s_2 s_1 \end{aligned}$$

Notice that each correspondence is compatible with the correspondence of the generators, namely: $s \mapsto s_1$ and $s' \mapsto s_2$. Given this correspondence, it should not be surprising that the subgroup lattices for D_3 and S_3 have the same structure.

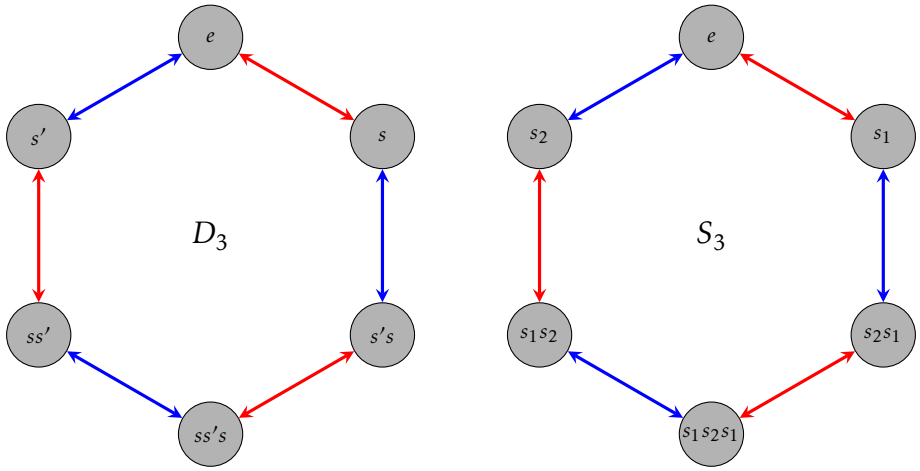

Figure 3.5. Cayley diagrams for D_3 and S_3 with generating sets $\{s, s'\}$ and $\{s_1, s_2\}$, respectively.

The goal of this section is to formalize this phenomenon by introducing the notion of an **isomorphism**. First, let's develop a little more intuition.

If two groups G_1 and G_2 have generating sets T_1 and T_2 such that we can color the edges of the corresponding Cayley diagrams so that the diagrams are identical up to relabeling of the vertices, then we say that there is a **matching** between G_1 and G_2. Above, we showed that D_3 and S_3 have a matching. It's important to emphasize that the existence of a matching between two groups depends on our choice of generating set. If two Cayley diagrams do not look alike, it does not immediately imply that there is not a matching between the groups since it might be the case that choosing different generating sets for the two groups leads to a matching.

Perhaps you've noticed that the Cayley diagram for R_4 with generating set $\{r\}$ looks like the Cayley diagram for the subgroup $\langle j \rangle = \{\pm 1, \pm j\}$ with generating set $\{j\}$ in Q_8. That is, there is a matching between R_4 and $\langle j \rangle$, which we've depicted in Figure 3.6. Similarly, the Cayley diagram for S_2 with generating set $\{s\}$ looks like the Cayley diagram for the subgroup $\langle -1 \rangle = \{\pm 1\}$ with generating set $\{-1\}$ in Q_8. The matching between S_2 and $\langle -1 \rangle$ is depicted in Figure 3.7. It's fairly easy to see that there is also a matching between S_2 and the subgroup $\langle v \rangle = \{e, v\}$ of V_4. Since there is a matching between S_2 and $\langle -1 \rangle$ and a matching between S_2 and $\langle v \rangle$, there is a matching between $\langle -1 \rangle$ and $\langle v \rangle$.

Problem 3.33. We have seen two different Cayley diagrams for D_3, one with generating set $\{s, r\}$ and one with generating set $\{s, s'\}$. As Figure 3.5 illustrates, there is a matching between D_3 and S_3 that relies on the generating sets $\{s, s'\}$ and $\{s_1, s_2\}$, respectively. Find a different matching between D_3 and S_3 that utilizes the generating set $\{r, s\}$ for D_3.

The next theorem follows immediately from the definition of matching.

Theorem 3.34. If there is a matching between G_1 and G_2 using the generating sets T_1 and T_2, respectively, then $|G_1| = |G_2|$ and T_1 and T_2 have the same cardinality.

Unfortunately, the converse of the previous theorem is not true in general. That is, two groups that have the same order may or may not have a matching.

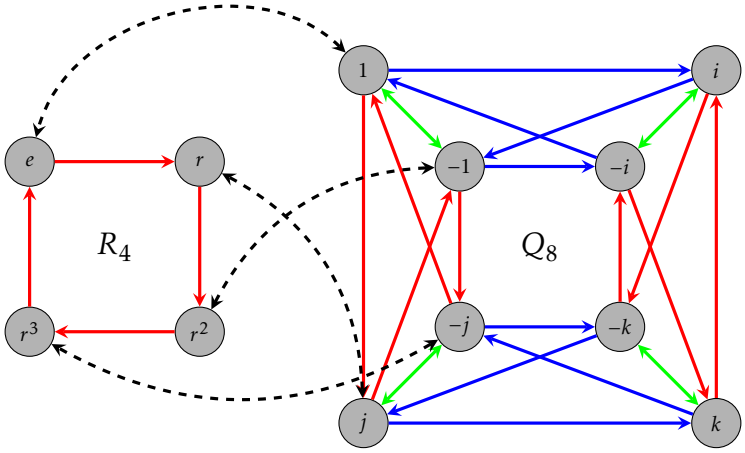

Figure 3.6. A matching between $R_4 = \langle r \rangle$ and $\langle j \rangle \leq Q_8$.

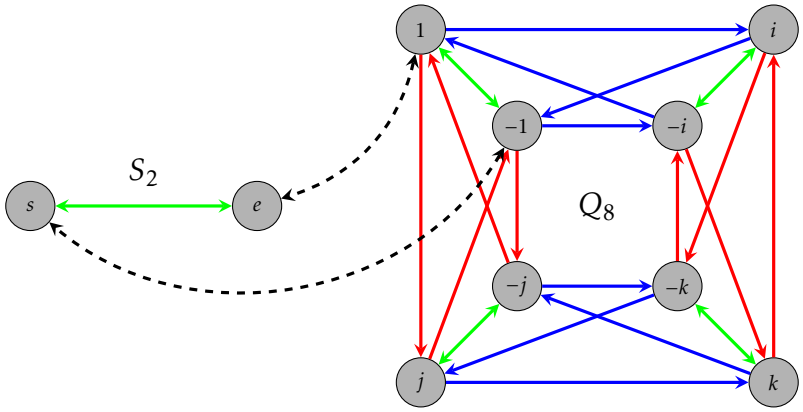

Figure 3.7. A matching between $S_2 = \langle s \rangle$ and $\langle -1 \rangle \leq Q_8$.

Loosely speaking, if two groups have a matching, then the two groups have the same structure and characteristics. In other words, the two groups essentially do the "same kind" of thing. In particular, the corresponding elements in each group have the same characteristics.

On the other hand, if one group has a property that the other does not have, then the two groups cannot have a matching. For example, if one group is abelian and the other is not, then the two groups cannot have a matching. Moreover, for each element g in one group with the property $g^k = e$ for some $k \in \mathbb{Z}$, there must be a corresponding element in the other group with the same property. Otherwise, there cannot be a matching between the two groups.

Problem 3.35. Determine whether there is a matching between D_4 and $\mathrm{Spin}_{1\times 2}$.

Problem 3.36. Determine whether there is a matching between R_4 and V_4.

Problem 3.37. Determine whether there is a matching between D_3 and R_6.

Problem 3.38. Determine whether there is a matching between any pair of the following groups: R_8 (i.e., the group of rotational symmetries of a regular octagon), D_4, Q_8.

Problem 3.39. Consider two light switches on a wall side by side. Consider the group of actions that consists of all possible actions that you can do to the two light switches. For example, one action is toggle the left light switch while leaving the right alone. Let's call this group L_2.

(a) How many distinct actions does L_2 have?

(b) Can you find a minimal generating set for L_2? If so, give these actions names and then write all of the actions of L_2 as words in your generator(s).

(c) Using your generating set from part (b), draw the corresponding Cayley diagram for L_2.

(d) Determine whether there is a matching between L_2 and either of R_4 or V_4.

Problem 3.40. Consider three light switches on a wall side by side. Consider the group of actions that consists of all possible actions that you can do to the three light switches. Let's call this group L_3. It should be easy to see that L_3 has 8 distinct actions.

(a) Can you find a minimal generating set for L_3? If so, give these actions names and then write all of the actions of L_3 as words in your generator(s).

(b) Using your generating set from part (a), draw the corresponding Cayley diagram for L_3.

(c) Is L_3 cyclic? Briefly justify your answer.

(d) Is L_3 abelian? Briefly justify your answer.

(e) Determine whether there is a matching between L_3 and any of R_8, D_4, $\text{Spin}_{1\times 2}$, or Q_8.

Suppose G is a finite group and consider the group table for G. A **coloring** for the group table is an assignment of a unique color to each element of the group. For example, Figure 3.8 depicts a coloring for the group table of V_4.

$\circ$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

Figure 3.8. A coloring for the group table of V_4.

We say that two finite groups have an **identical table coloring**, if we can arrange the rows and columns of each table and choose colorings for each table so that the pattern of colors is the same for both tables. Clearly, this is only possible if the two groups have the same order. In Problem 2.65, we showed that R_4 and V_4 never have an identical table coloring.

Problem 3.41. Determine whether V_4 and L_2 have an identical table coloring.

Problem 3.42. Suppose there is a matching between finite groups G_1 and G_2. Explain why G_1 and G_2 must have an identical table coloring.

Problem 3.43. Is the converse of the previous problem true? That is, if G_1 and G_2 are finite groups that have an identical table coloring, will there be a matching between G_1 and G_2?

Problem 3.44. Suppose there is a matching between G_1 and G_2 and suppose T_1 is a generating set for G_1. Explain why there must be a generating set T_2 for G_2 and an appropriate choice of colors such that the Cayley diagrams for G_1 and G_2 using the generating sets T_1 and T_2, respectively, are identical up to relabeling of the vertices.

The last few problems have led us to the following theorem.

Theorem 3.45. If G_1 and G_2 are two finite groups, then there is a matching between G_1 and G_2 if and only if G_1 and G_2 have an identical table coloring.

As you've likely discovered, matchings and identical table coloring (or the lack thereof) are great for developing intuition about when two groups have identical structure, but the process of finding matchings and identical table colorings is cumbersome. Moreover, it turns out to not be a very useful approach for proving theorems. We need a different approach if we want to develop the general theory any further.

If two finite groups G_1 and G_2 have an identical table coloring, then

the product of corresponding elements yields the corresponding result.

This is the essence of what it means for two groups to have the same structure.

Let's try to make this a little more precise. Suppose $(G_1,*)$ and $(G_2,\odot)$ are two finite groups that have an identical table coloring and let $x_1, y_1 \in G_1$. Then these two elements have corresponding elements in the group table for G_2, say x_2 and y_2, respectively. In other words, x_1 and x_2 have the same color while y_1 and y_2 have the same color. Since G_1 is closed under its binary operation $*$, there exists $z_1 \in G_1$ such that $z_1 = x_1 * y_1$. But then there must exist a $z_2 \in G_2$ such that z_2 has the same color as z_1. What must be true of $x_2 \odot y_2$? Since the two tables exhibit the same color pattern, it must be the case that $z_2 = x_2 \odot y_2$. This is what it means for the product of corresponding elements to yield the corresponding result. Figure 3.9 illustrates this phenomenon for group tables.

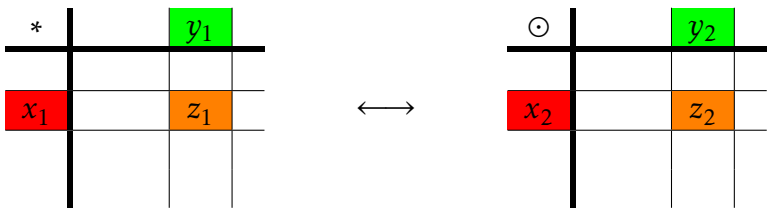

Figure 3.9

We can describe the identical table matching between G_1 and G_2 using a function. Let $\phi : G_1 \to G_2$ be the one-to-one and onto function that maps elements of G_1 to their corresponding elements in G_2. Then $\phi(x_1) = x_2$, $\phi(y_1) = y_2$, and $\phi(z_1) = z_2$. Since $z_2 = x_2 \odot y_2$, we obtain

$$\phi(x_1 * y_1) = \phi(z_1) = z_2 = x_2 \odot y_2 = \phi(x_1) \odot \phi(y_1).$$

In summary, it must be the case that

$$\phi(x_1 * y_1) = \phi(x_1) \odot \phi(y_1).$$

We are now prepared to state a formal definition of what it means for two groups to be isomorphic.

Definition 3.46. Let $(G_1, *)$ and $(G_2, \odot)$ be two groups. Then G_1 is **isomorphic** to G_2, written $G_1 \cong G_2$, if and only if there exists a one-to-one and onto function $\phi : G_1 \to G_2$ such that

$$\phi(x * y) = \phi(x) \odot \phi(y). \tag{3.1}$$

The function ϕ is referred to as an **isomorphism**. Equation 3.1 is often referred to as the **homomorphic property**.

It should be clear from the development that two finite groups are isomorphic if and only if they have an identical table coloring. Moreover, since two finite groups have an identical table coloring if and only if there is a matching between the two groups, it must be the case that two groups are isomorphic if and only if there is a matching between the two groups. The upshot is that we have three different ways to think about what it means for two groups to be isomorphic:

(1) There exists generating sets for the two groups such that the respective Cayley diagrams are identical up to relabeling of the vertices.

(2) There exists a choice of colors and an arrangement of the rows and columns of the group tables such that the two tables exhibit the same pattern of colors.

(3) There exists a bijective function between the two groups that satisfies the homomorphic property.

Problem 3.47. Using the work that you did earlier in this section, determine which of the following groups are isomorphic to each other: S_2, $\langle -1 \rangle$ in Q_8, R_3, R_4, V_4, L_2, $\langle i \rangle$ in Q_8, $\langle sr, sr^2 \rangle$ in D_4, R_5, R_6, D_3, S_3, R_7, R_8, D_4, $\text{Spin}_{1\times 2}$, Q_8, L_3.

Problem 3.48. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where $\mathbb{R}^+$ is the set of positive real numbers. It turns out that these two groups are isomorphic, but this would be difficult to discover using our previous techniques because the groups are infinite. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ via $\phi(r) = e^r$ (where e is the natural base, not the identity). Prove that ϕ is an isomorphism.

Problem 3.49. For each of the following pairs of groups, determine whether the given function is an isomorphism from the first group to the second group.

(a) $(\mathbb{Z},+)$ and $(\mathbb{Z},+)$, $\phi(n) = n+1$.

(b) $(\mathbb{Z},+)$ and $(\mathbb{Z},+)$, $\phi(n) = -n$.

(c) $(\mathbb{Q},+)$ and $(\mathbb{Q},+)$, $\phi(x) = x/2$.

Problem 3.50. Show that the groups $(\mathbb{Z},+)$ and $(2\mathbb{Z},+)$ are isomorphic.

Perhaps one surprising consequence of the previous problem is that when dealing with infinite groups, a group can have a proper subgroup that it is isomorphic to. Of course, this never happens with finite groups.

Once we know that two groups are isomorphic, there are lots of interesting things we can say. The next theorem tells us that isomorphisms map the identity element of one group to the identity of the second group. This was already clear using Cayley diagrams and groups tables, but you should try to prove the theorem directly using Definition 3.46.

Theorem 3.51. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1,*)$ to the group $(G_2,\odot)$. If e_1 and e_2 are the identity elements of G_1 and G_2, respectively, then $\phi(e_1) = e_2$.

The next theorem tells us that isomorphisms respect inverses.

Theorem 3.52. If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1,*)$ to the group $(G_2,\odot)$, then $\phi(g^{-1}) = [\phi(g)]^{-1}$.

It turns out that "isomorphic" ($\cong$) determines an equivalence relation on the class of all possible groups. The next two theorems justify that $\cong$ is symmetric and transitive.

Theorem 3.53. If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1,*)$ to the group $(G_2,\odot)$, then the function $\phi^{-1} : G_2 \to G_1$ is an isomorphism.

Theorem 3.54. If $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are isomorphisms from the groups $(G_1,*)$ to $(G_2,\odot)$ and $(G_2,\odot)$ to $(G_3,\star)$, respectively, then the composite function $\psi \circ \phi$ is an isomorphism of G_1 and G_3.

The only thing left to do in order to justify the next theorem is prove that $\cong$ is reflexive.

Theorem 3.55. If $\mathcal{G}$ is any nonempty collection of groups, then the relation $\cong$ is an equivalence relation on $\mathcal{G}$.

Mathematicians love to classify things. In particular, mathematicians want to classify groups. One can think of this pursuit as a taxonomy of groups. In order to simplify the task, one can classify isomorphism classes (i.e., the equivalence classes determined by $\cong$) instead of classifying groups. If two groups are isomorphic, then we say that the groups are **the same up to isomorphism**. If there are k isomorphism classes of order n, then we say that there are k **groups of order** n **up to isomorphism**.

Problem 3.56. Explain why all groups with a single element are isomorphic. Justify your answer using group tables.

In light of the previous problem, we say that there is one group of order one up to isomorphism.

Problem 3.57. Suppose that $(G,*)$ is a group of order 2 such that $G = \{e, a\}$. Complete the following group table for G.

$*$	e	a
e		
a		

Explain why every group of order 2 must be isomorphic to S_2.

The previous problem implies that up to isomorphism, there is only one group of order 2.

Problem 3.58. Suppose $(G,*)$ is a group of order 3 such that $G = \{e, a, b\}$. Complete the following group table for G.

$*$	e	a	b
e			
a			
b			

Explain why every group of order 3 must be isomorphic to R_3.

Problem 3.59. Suppose $(G,*)$ is a group of order 4 such that $G = \{e, a, b, c\}$. Assuming that e is the identity, the first row and first column of the corresponding group table must be completed as follows.

$*$	e	a	b	c
e	e	a	b	c
a	a	?		
b	b			
c	c			

The cell with the question mark cannot be filled with an a. So, this entry must be either e, b, or c. However, it should be easy to see that the cases with b and c are symmetric. Thus, there are two cases: (i) the entry with the question mark is filled with e, or (ii) the entry with the question mark is without loss of generality filled with b. Complete the group table in each of these two cases. Are either of the resulting groups isomorphic to R_4 or V_4. What conclusion can you make about groups of order 4?

So far we've seen that there are unique groups up to isomorphism of orders 1, 2, and 3, but that there are two groups up to isomorphism of order 4. A natural question to ask is: how many groups are there of order n?

In a future chapter we will be able to prove that there is only one group up to isomorphism of order 5, namely those groups isomorphic to R_5.

We've seen three groups of order 6, namely R_6, D_3, and S_3. However, $D_3 \cong S_3$ while R_6 is not isomorphic to either of these. So, we can conclude that there are at least two groups up to isomorphism of order 6. But are there others? It turns out that the answer is no, but why?

The group R_7 is the group of rotational symmetries of a regular 7-sided polygon. This group has order 7. Are there other groups of order 7 that are not isomorphic to R_7? It turns out that the answer is no, but why?

We've encountered several groups of order 8, namely D_4, $\text{Spin}_{1\times 2}$, Q_8, R_8, and L_3. Of these, only D_4 and $\text{Spin}_{1\times 2}$ are isomorphic. Thus, there are at least four groups up to isomorphism of order 8. Are these the only isomorphism types? It turns out that there are five groups of order 8 up to isomorphism.

Let's return to proving some general statements about isomorphisms.

Theorem 3.60. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. If G_1 is cyclic, then G_2 is cyclic.

Problem 3.61. Is the converse of Theorem 3.60 true? That is, if $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$ and G_2 is cyclic, is G_1 necessarily cyclic? If the converse is true, then prove it. If the converse is false, provide a counterexample.

Theorem 3.62. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. If G_1 is abelian, then G_2 is abelian.

If $\phi : G_1 \to G_2$ is a function, not necessarily an isomorphism, and $X \subseteq G_1$, then the set

$$\phi(X) := \{y \in G_2 \mid \text{there exists } x \in X \text{ such that } \phi(x) = y\}.$$

is called the **image** of X. The next theorem tells us that the image of a subgroup under an isomorphism is also a subgroup.

Theorem 3.63. If $\phi : G_1 \to G_2$ is an isomorphism and $H \leq G_1$, then $\phi(H) \leq G_2$.

Suppose G is a group and let $g \in G$. Define $\phi_g : G \to G$ via $\phi(x) = gxg^{-1}$. The map ϕ_g is called **conjugation** by g.

Theorem 3.64. If G is a group and $g \in G$, then conjugation by g is an isomorphism from G to G.

Now that you've proved the above theorems, it's a good idea to review the key themes. If you were really paying attention, you may have noticed that in a few of the proofs, we did not use the fact that the function was one-to-one and onto despite assuming that the function was an isomorphism.

Problem 3.65. For which of the recent theorems could we remove either the assumption that the function is one-to-one or the assumption that the function is onto?

A function that satisfies the homomorphic property and may or may not be one-to-one or onto is called a **homomorphism** and will be the subject of a future chapter.

Problem 3.66. What claims can be made about the subgroup lattices of two groups that are isomorphic? What claims can be made about the subgroup lattices of two groups that are not isomorphic? What claims can be made about two groups if their subgroup lattices look nothing alike?