

Chapter 5

A Formal Approach to Groups

In this chapter we finally introduce the formal definition of a group. From this point on, our focus will shift from developing intuition to studying the abstract properties of groups. However, we should not abandon the intuition we have gained. As we progress, your intuitive understanding of groups will continue to improve and you should rely on this understanding as you try to make sense of the notions that follow. There has been plenty of intentional foreshadowing, so expect to revisit concepts you've already encountered. We'll also encounter plenty of new stuff, too.

It is important to point out that things are about to get quite a bit more difficult for most of you. Be patient and persistent!

5.1 Binary Operations

After learning to count as a child, you likely learned how to add, subtract, multiply, and divide with natural numbers. Loosely speaking, these operations are examples of binary operations since we are combining two objects to obtain a single object. More formally, we have the following definition.

Definition 5.1. A **binary operation** $*$ on a set A is a function from $A \times A$ into A . For each $(a, b) \in A \times A$, we denote the element $*(a, b)$ via $a * b$.

Remark 5.2. Don't misunderstand the use of $*$ in this context. We are not implying that $*$ is the ordinary multiplication of real numbers that you are familiar with. We use $*$ to represent a generic binary operation.

Remark 5.3. Notice that since the codomain of a binary operation on a set A is A , binary operations require that we yield an element of A when combining two elements of A . In this case, we say that A is **closed** under $*$. Binary operations have this closure property by definition. Also, since binary operations are functions, any attempt to combine two elements from A should result in a *unique* element of A . In this case, we say that $*$ is **well-defined**. Moreover, since the domain of $*$ is $A \times A$, it must be the case that $*$ is defined for *all* pairs of elements from A .

Example 5.4. Examples of binary operations include $+$ (addition), $-$ (subtraction), and \cdot (multiplication) on the real numbers. However, \div (division) is not a binary operation on the set of real numbers because all elements of the form $(a, 0)$ are not in the domain $\mathbb{R} \times \mathbb{R}$ since we cannot divide by 0. Yet, \div is a suitable binary operation on $\mathbb{R} \setminus \{0\}$.

Example 5.5. Let C be the set of continuous functions from \mathbb{R} to \mathbb{R} . Then \circ (function composition) is a binary operation on C .

Example 5.6. Consider the 6 actions of D_3 . The composition of these actions is a binary operation on D_3 . In fact, composition of actions for each of the groups that we have seen is a binary operation on the given group. Notice that we never used a symbol for these binary operations, but rather used juxtaposition (i.e., ab is the juxtaposition of a and b).

Example 5.7. Let $M_{2 \times 2}(\mathbb{R})$ be the set of 2×2 matrices with real number entries. Then matrix multiplication is a binary operation on $M_{2 \times 2}(\mathbb{R})$.

Exercise 5.8. Explain why composition of spins is not a binary operation on the set of allowable spins in $\text{Spin}_{3 \times 3}$.

Exercise 5.9. Let $M(\mathbb{R})$ be the set of matrices (of any size) with real number entries. Is matrix addition a binary operation on $M(\mathbb{R})$? How about matrix multiplication?

Exercise 5.10. Determine whether \cup (union) and \cap (intersection) are binary operations on $\mathcal{P}(\mathbb{Z})$ (i.e., the power set of the integers).

Exercise 5.11. Consider the closed interval $[0, 1]$ and define $*$ on $[0, 1]$ via $a * b = \min\{a, b\}$ (i.e., take the minimum of a and b). Determine whether $*$ is a binary operation on $[0, 1]$.

Some binary operations have additional properties.

Definition 5.12. Let A be a set and let $*$ be a binary operation on A .

- (a) We say that $*$ is **associative** if and only if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$.
- (b) We say that $*$ is **commutative** if and only if $a * b = b * a$ for all $a, b \in A$.

Exercise 5.13. Provide at least one example of a binary operation and the corresponding set that is commutative. How about not commutative?

Theorem 5.14. Let A be a set and let F be the set of functions from A to A . Then function composition is an associative binary operation on F .

When the set A is finite, we can represent a binary operation on A using a table in which the elements of the set are listed across the top and the left side (in the same order). The entry in the i th row and j th column of the table represents the output of combining the element that labels the i th row with the element that labels the j th column (order matters).

Example 5.15. Consider the following table.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

This table represents a binary operation on the set $A = \{a, b, c\}$. In this case, $a * b = c$ while $b * a = a$. This shows that $*$ is not commutative.

Exercise 5.16. What property must a table for a binary operation have in order for the operation to be commutative?

Exercise 5.17. Fill in the missing entries in the following table so that $*$ defines an associative binary operation on $\{a, b, c, d\}$.

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

5.2 Groups

Without further ado, here is our official definition of a group.

Definition 5.18. A group $(G, *)$ is a set G together with a binary operation $*$ such that the following axioms hold.

- (0) The set G is closed under $*$.
- (1) The operation $*$ is associative.
- (2) There is an element $e \in G$ such that for all $g \in G$, $e * g = g * e = g$. We call e the **identity**.
- (3) Corresponding to each $g \in G$, there is an element $g' \in G$ such that $g * g' = g' * g = e$. In this case, g' is called the **inverse** of g , which we shall denote as g^{-1} .

Remark 5.19. A few comments are in order.

- (a) Notice that a group has two parts to it, namely, a set and a binary operation. For simplicity, if $(G, *)$ is a group, we will often refer to G as being the group. However, you must remember that the binary operation is part of the structure.
- (b) Axiom 2 forces G to be nonempty.
- (c) In the generic case, even if $*$ is not actually multiplication, we will refer to $a * b$ as the **product** of a and b .

- (d) We are not requiring $*$ to be commutative. If $*$ is commutative, then we say that G is **abelian*** (or **commutative**).

Exercise 5.20. Explain why Axiom 0 is unnecessary.

At this time, we have two definitions of a group. The first one was intended to provide an intuitive introduction and Definition 5.18 provides a rigorous mathematical definition. We should confirm that these two definitions are in fact compatible.

Exercise 5.21. Compare and contrast our two definitions of a group. How do the rules and axioms match up?

Exercise 5.22. Quickly verify that $\text{Spin}_{1 \times 2}$, S_2 , R_4 , D_3 , D_4 , V_4 , and Q_8 are groups under composition of actions.

Exercise 5.23. Determine whether each of the following are groups. If the pair is a group, determine whether it is abelian and identify the identity. Explain your answers.

- (a) $(\mathbb{Z}, +)$
- (b) $(\mathbb{N}, +)$
- (c) (\mathbb{Z}, \cdot)
- (d) $(\mathbb{R}, +)$
- (e) (\mathbb{R}, \cdot)
- (f) $(\mathbb{R} \setminus \{0\}, \cdot)$
- (g) $(M_{2 \times 2}(\mathbb{R}), +)$
- (h) $(M_{2 \times 2}(\mathbb{R}), *)$, where $*$ is matrix multiplication.
- (i) $(\{a, b, c\}, *)$, where $*$ is the operation determined by the table in Example 5.15.
- (j) $(\{a, b, c, d\}, *)$, where $*$ is the operation determined by the table in Exercise 5.17.

Notice that in Axiom 2 of Definition 5.18, we said *the* identity and not *an* identity. Implicitly, this implies that the identity is unique.

Theorem 5.24. Let G be a group with binary operation $*$. Then there is a unique identity element in G . That is, there is only one element e in G such that $g * e = e * g = g$ for all $g \in G$.

The following theorem is crucial for proving many theorems about groups.

Theorem 5.25 (Cancellation Law). Let $(G, *)$ be a group and let $g, x, y \in G$. Then $g * x = g * y$ if and only if $x = y$. Similarly, $x * g = y * g$ if and only if $x = y$.[†]

*Commutative groups are called abelian in honor of the Norwegian mathematician Niels Abel (1802–1829).

[†]You only need to prove one of these statements as the proof of the other is symmetric.

Exercise 5.26. Show that (\mathbb{R}, \cdot) fails the Cancellation Law (confirming the fact that it is not a group).

Corollary 5.27. Let G be a group with binary operation $*$. Then each $g \in G$ has a unique inverse.

Theorem 5.28. Let $(G, *)$ be a group and let $g, h \in G$. Then the equations $g * x = h$ and $y * g = h$ have unique solutions for x and y in G .

While proving the previous few theorems, hopefully one of the things you realized is that you can multiply both sides of a group equation by the same element but that you have to do it on the same side of each half. That is, since a group may or may not be abelian, if I multiply one side of an equation on the left by a group element, then we must multiply the other side of the equation on the left by the same group element.

Despite the fact that a group may or may not be abelian, if one product is equal to the identity, then reversing the order yields the same result.

Theorem 5.29. Let G be a group with binary operation $*$. If $g * h = e$, then $h * g = e$.

The upshot of the previous theorem is if we have a “left inverse” then we automatically have a “right inverse” (and vice versa).

The next theorem should not be surprising.

Theorem 5.30. Let $(G, *)$ be a group and let $g \in G$. Then $(g^{-1})^{-1} = g$.

Definition 5.31. Let $(G, *)$ be a group and let $g \in G$. Then for $n \in \mathbb{N}$, we define

$$g^n = \underbrace{g * g * \cdots * g}_{n \text{ factors}}$$

and

$$g^{-n} = \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{n \text{ factors}}.$$

Moreover, we define $g^0 = e$.

The good news is that the rules of exponents you are familiar with still hold for groups.

Theorem 5.32. Let $(G, *)$ be a group and let $g \in G$. For $n, m \in \mathbb{Z}$, we have the following:

- (a) $g^n * g^m = g^{n+m}$,
- (b) $(g^n)^{-1} = g^{-n}$.

5.3 Group Tables

Recall that we could represent a binary operation on a finite set using a table. Since groups have binary operations at their core, we can represent a finite group (i.e., a group with finitely many elements) using a table, called a **group table** (or **Cayley table**). For example, below are group tables for D_3 and V_4 , respectively.

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

$*$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

Our convention will be that if x appears in row i and y appears in column j , then row i “times” column j will result in the element determined by xy , where as usual we follow our right to left convention. That is, xy means we apply y first and then x (as in function composition).

Exercise 5.33. Verify that V_4 is an abelian group. What feature of the table makes this clear?

Given an arbitrary group G , we should probably say, “a group table for G ” and not “the group table for G .” The reason for this is that if we chose a different order of the elements (e.g., swap rows 1 and 4—which swaps columns 1 and 4, as well), then the table would look slightly different. Also, if we had chosen a different generating set, then the names of the elements would look different. Regardless, the table still captures the same information about the binary operation. Because every possible table for a given group conveys the same information about the architecture of the group, people may refer to any table for the group as “the” table.

Exercise 5.34. Create group tables for the following groups: S_2 , R_3 , R_4 , D_3 , S_3 , D_4 , and Q_8 . Which groups are abelian?

Perhaps you noticed when creating the tables above that each element of the group appeared exactly once in each row and column, respectively. This is true, in general. Use Theorem 5.28, to prove the following theorem.

Theorem 5.35. Let $(G, *)$ be a finite group. Then each element of G appears exactly once in each row and each column, respectively, in any group table for G .

We can also use tables to define groups. For example, consider the following table on the set $A = \{e, a, b, c\}$.

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

Is this a table for a group? First, we see that the binary operation determined by the table is closed. Second, we see that e is acting as the identity. Since every row and column has the identity element e appearing, we know that every element has an inverse (do you see why that follows?). The only thing left to check is associativity. Imagine for a moment what this entails. It's messy right?! And this is only for a group of order 4.

Thankfully, we can rely on some prior knowledge to help out with associativity. It turns out that if you look closely, the group table for V_4 looks the “same” as the table above. What do we mean by “same” here? The names for elements are different (except for e), but

the product of corresponding elements yields the corresponding result.

To see what I mean, let's color both tables with white, red, blue, and green in such a way that each element corresponds to a unique color. If we choose our colors wisely, it is easy to see that both tables have the same structure.

*	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

↔

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Since we already know that V_4 is a group, we know that the binary operation for V_4 is associative.

Exercise 5.36. Explain why the discussion above implies that the binary operation determined by the table on the right above must be associative. Have we shown that $(A, *)$ is a group?

It is important to point out that if we had not chosen our colors wisely, then perhaps the colorings of the two tables would not agree. Moreover, if we had made the same color choices for elements, but then rearranged columns and rows of one table, the colorings of the two tables would not agree. This doesn't imply anything. The point is whether we *can* get the tables to match.

Exercise 5.37. Draw the Cayley diagram for $(A, *)$ with generators a and b . Explain why this implies that V_4 and A (under their respective binary operations) are isomorphic.

Exercise 5.38. Is it possible to color the group table for R_4 so that it matches the coloring of V_4 ? Explain your answer.

Problem 5.39. Let $(G, *)$ and (G', \circ) be two finite groups. Suppose we can arrange the rows and columns and color elements in such a way that the colorings for the two group tables agree. Explain why this implies that the two groups are isomorphic.

Problem 5.40. Suppose we have a table for $(G, *)$, where G is finite. Further suppose that (i) there is an identity element, and (ii) every element appears exactly once in each row and column, respectively. Explain why the only thing we need to verify in order for $(G, *)$ to be a group is that $*$ is associative.

Problem 5.41. Suppose that $(G, *)$ is a group. Theorem 5.24 guarantees that there is a unique identity in G . When creating the group table for G , what goes wrong if you try to include two different identity elements?

Consider the class of all possible groups. It turns out that “isomorphic” (\cong) determines an equivalence relation. That is, under this relation two groups are related if and only if they are isomorphic. We’ll prove this formally later when we have a more rigorous definition of isomorphic.

Problem 5.42. Explain why all groups with a single element are isomorphic.

In this case, we say that “up to isomorphism” there is only one group with a single element.

Problem 5.43. Consider a group $(G, *)$ of order 2. Suppose that $G = \{e, a\}$. Complete the following group table for G .

$*$	e	a
e		
a		

Explain why every group with 2 elements must be isomorphic to S_2 .

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

Problem 5.44. Consider a group $(G, *)$ of order 3. Suppose that $G = \{e, a, b\}$. Complete the following group table for G .

$*$	e	a	b
e			
a			
b			

Explain why every group with 3 elements must be isomorphic to R_3 .

Problem 5.45. Consider a group $(G, *)$ of order 4. Suppose 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 the cases with b and c are symmetric. Thus, there are two cases: (i) the entry with the question mark is filled with e , (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. Recall that we've seen two non-isomorphic groups of order 2, namely R_4 and 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 general question we will want to address 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 (i.e., rotation group of a regular pentagon).

We've seen three groups of order 6, namely R_6 , D_3 , and S_3 . However, $D_3 \cong S_3$ (see Problem 4.28) while R_6 is not isomorphic to either of these (see Problem 4.22). 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 yes, but why?

The group R_7 is the group of rotations 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 ?

We've encountered four groups of order 8, namely D_4 , $\text{Spin}_{1 \times 2}$, Q_8 , and R_8 . Of these, only D_4 and $\text{Spin}_{1 \times 2}$ are isomorphic. Thus, there are at least three groups up to isomorphism of order 8. However, are these the only ones? It turns out that the answer is no. What are the missing ones?

5.4 Revisiting Cayley Diagrams and Our Original Definition of a Group

Let's begin with a couple of exercises.

Exercise 5.46. Consider the diagram given in Figure 5.1. This is identical to the diagram that appeared in Figure 3.5 that we saw at the end of Chapter 3.

- Consider Rules 1–4 of our original definition of a group (see Definition 2.14). Does the diagram in Figure 5.1 satisfy Rules 1–4?
- Try to convert this diagram into a group table. Does the table represent a group? What goes wrong?

Exercise 5.47. Consider the diagram given in Figure 5.2

- Does the diagram in Figure 5.2 satisfy Rules 1–4 of Definition 2.14?
- Try to convert this diagram into a group table. Does the table represent a group? What goes wrong?

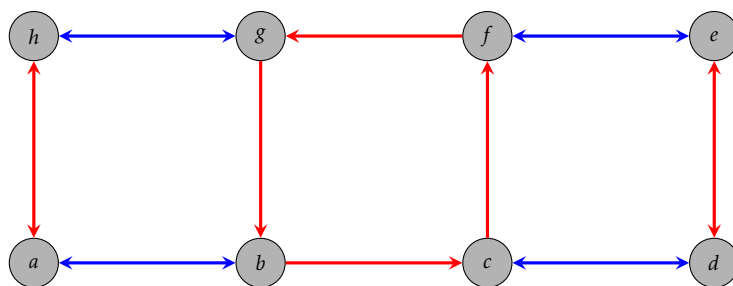


Figure 5.1. Diagram for Exercise 5.46.

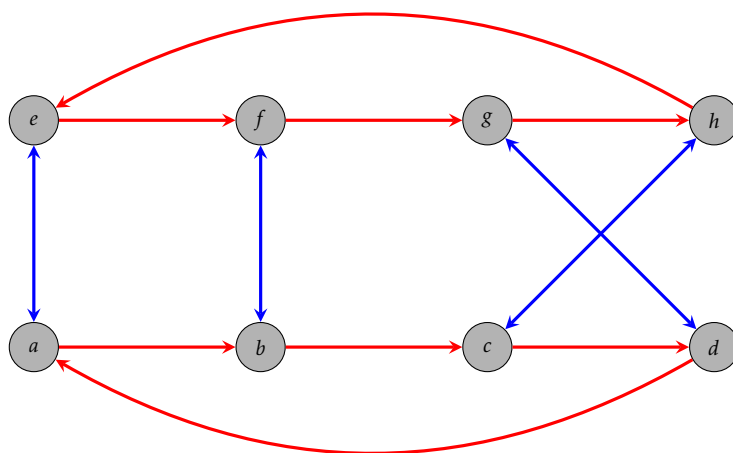


Figure 5.2. Diagram for Exercise 5.47.

As the previous two exercises indicate, the moral of the story is that our original intuitive definition of a group has a weakness. It does not agree with our formal definition of a group given in Definition 5.18. Let's see if we can figure out what goes wrong.

Consider the Cayley diagram for D_3 with generating set $\{r, s\}$ that is given in Figure 5.3. Notice that we labeled the lower right corner of the Cayley diagram with the word r^2s . This means that we first followed a blue arrow out of e and then two red arrows. However, we could also get to this vertex by first doing a red arrow out of e followed by a blue arrow. So, we could also have labeled this vertex with the word sr . The upshot is that $r^2s = sr$. These types of group equations are called **relations**.

We discovered this relation by starting at e and then traveling a sequence of arrows to get to the vertex in the lower right corner. However, notice that following a blue and then two red arrows is *always* the same as following a red arrow and then a blue arrow regardless of which vertex we start at. That is, the relation $r^2s = sr$ holds universally across the entire Cayley diagram.

Cayley diagrams for groups will always have this uniform symmetry. The fancy way of saying this is that Cayley diagrams are **regular**. In other words, a diagram is regular if every internal pattern repeats itself throughout the diagram.

Exercise 5.48. Identify two other relations that the Cayley diagram for D_3 given in Fig-

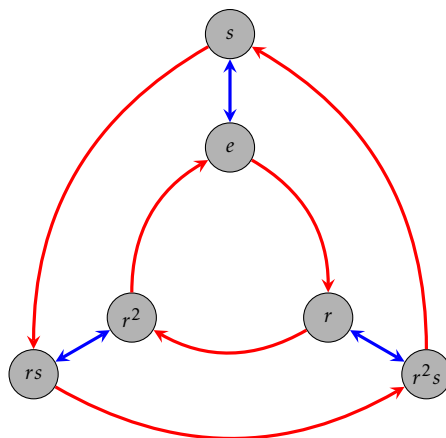


Figure 5.3. Cayley diagram for D_3 with generating set $\{r, s\}$.

ure 5.3 exhibits. Find one that involves both r^{-1} (i.e., following a red arrow backwards) and s . Convince yourself that your relations appear throughout the diagram.

Exercise 5.49. Verify that the diagrams in Exercise 5.46 and 5.47 are not regular.

Problem 5.50. Explain why the Cayley diagram for a group must be regular.

The discussion and exercises above lead us to conclude that one thing missing from our original intuitive definition of a group is regularity. It turns out that this is the only thing missing. That is, if we add the requirement of regularity to our intuitive definition, we could convert it into a rigorous definition that is equivalent to Definition 5.18. However, we won't bother doing this since our intuitive definition served its purpose.

We close this section with a problem that asks you to think about the structure of the Cayley diagrams for an abelian group.

Problem 5.51. Suppose $(G, *)$ is a group and suppose S is a generating set for G . Consider the Cayley diagram for G with generating set S .

- If G is abelian and $a, b \in S$, then what relationship must be true for the arrows in the Cayley diagram corresponding to the elements a and b ?
- Is the converse of your claim true? That is, if every pair of edges in a Cayley diagram for G has the property you stated above, will the group be abelian?

5.5 Revisiting Subgroups

Back in Section 4.1, we introduced the notion of subgroup. In light of our official definition of a group, we more or less have the same definition as before, but let's restate it here using slightly more formal language.

Definition 5.52. 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 G ’s binary operation.

Recall that Theorems 4.6 and 4.8 tell us that $\langle e \rangle = \{e\}$ and G are always subgroups of G . This is still true even using our official definition of a group. The subgroup $\{e\}$ is referred to as the **trivial subgroup**. All other subgroups are called **nontrivial**. If H is a subgroup of a group G with $H \neq G$, then we may write $H < G$ and refer to H as a **proper subgroup** of G .

The next theorem tells us that we don’t need to verify all the axioms of a group to determine whether a nonempty subset is a subgroup.

Theorem 5.53. 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 .

Remark 5.54. Notice that one of the hypotheses of Theorem 5.53 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.

Exercise 5.55. 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 .

Exercise 5.56. 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.

Exercise 5.57. 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.

Exercise 5.58. 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 5.59. Suppose $(G, *)$ is a group and let $H, K \leq G$. Then $H \cap K \leq G$.

Problem 5.60. Can we replace intersection with union in the theorem above? If so, prove the corresponding theorem. If not, then provide a specific counterexample.

Theorem 5.61. Suppose $(G, *)$ is an abelian group and let $H \leq G$. Then H is an abelian subgroup.

Problem 5.62. Is the converse of the previous theorem true? If so, prove it. Otherwise, provide a counterexample.

Theorem 5.63. Suppose $(G, *)$ is a group. Define

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

(called the **center** of G). Then $Z(G)$ is an abelian subgroup of G .

Exercise 5.64. 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) $(\mathbb{R} \setminus \{0\}, \cdot)$

The following definition formalizes Definition 4.9.

Definition 5.65. Let $(G, *)$ be a group and let S be a nonempty subset of G . Then we define $\langle S \rangle$ to be the set consisting of all possible (finite) products of elements from S and their inverses. The set $\langle S \rangle$ is called the **subgroup generated by S** . The elements of S are called **generators** of $\langle S \rangle$.

Note that S may be finite or infinite. Moreover, even if S is finite, $\langle S \rangle$ may be infinite. Also, it is important to point out that we are not putting any restrictions about efficiency on S in the definition above. That is, it is possible that some elements are included in S that are not necessary to generate all of the elements of $\langle S \rangle$.

In cases when we know what the elements of S actually are, then we will list them inside the angle brackets without the set braces. For example, if $S = \{a, b, c\}$, then we will write $\langle a, b, c \rangle$ instead of $\langle \{a, b, c\} \rangle$. In the special case when S equals a single element, say $S = \{a\}$, then

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\},$$

which is called the **subgroup generated by a** .

The set $\langle S \rangle$ is called the “subgroup generated by S ”, so it better be a subgroup!

Theorem 5.66. Let $(G, *)$ be a group and let $S \subseteq G$, where $S \neq \emptyset$. Then $\langle S \rangle \leq G$. In particular, $\langle S \rangle$ is the smallest subgroup of G containing S .

Exercise 5.67. In Exercise 5.56 we introduced the notation $n\mathbb{Z}$. Write these subgroups 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?

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, $\langle H \rangle = H$.

Let’s explore a couple of examples. First, consider the group R_4 (where the operation is composition of actions). What are the subgroups of R_4 ? Theorems 4.6 and 4.8 tell us that $\{e\}$ and R_4 itself are subgroups of R_4 . Are there any others? Theorem 5.53 tells us that if we want to find other subgroups of R_4 , we need to find nonempty subsets of R_4 that are closed and contain all the necessary inverses. However, the previous paragraph indicates that we can find all of the subgroups of R_4 by forming the subgroups generated by various combinations of elements from R_4 . We can certainly be more efficient, but below we list all of the possible subgroups we can generate using subsets of R_4 . We are assuming that r is rotation by 90° clockwise. As you scan the list, you should take a moment to convince yourself that the list is accurate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let's make a few observations. Scanning the list, we see only three distinct subgroups: $\{e\}$, $\{e, r^2\}$, $\{e, r, r^2, r^3\}$. 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 generators for R_4 , respectively. Also, observe that if we increase the size of the subset using an element that was already contained in the subgroup generated by the smaller 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 5.68. Let $(G, *)$ be a group and let $g_1, g_2, \dots, g_n \in G$. If $x \in \langle g_1, g_2, \dots, g_n \rangle$, then $\langle g_1, g_2, \dots, g_n \rangle = \langle g_1, g_2, \dots, g_n, x \rangle$.

It is important to point out that in the theorem above, we are not saying that $\{g_1, g_2, \dots, g_n\}$ is a generating set for G —although this may be the case. Instead, we are simply making a statement about the subgroup $\langle g_1, g_2, \dots, g_n \rangle$, whatever it may be.

Let's return to our example involving R_4 . We have three subgroups, namely the two trivial subgroups $\{e\}$ and R_4 itself, together with one nontrivial subgroup $\{e, r^2\}$. Notice that $\{e\}$ is also a subgroup of $\{e, r^2\}$. We can capture the overall relationship between the subgroups using a **subgroup lattice**, which we depict in Figure 5.4 case of R_4 .

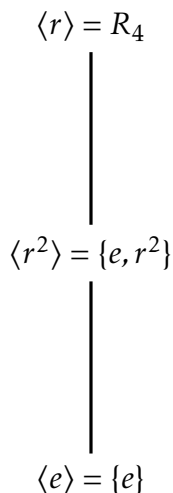


Figure 5.4. Subgroup lattice for R_4 .

In general, subgroups of smaller order are towards the bottom of the lattice while larger subgroups are towards the top. Moreover, an edge between two subgroups means that the smaller set is a subgroup of the larger set.

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 group. (Note that minimal generating sets are generating sets where we cannot remove any elements and still obtain the same group. Two minimal generating sets for the same group do not have to have the same number of generators.) In this case, we get the subgroup lattice in Figure 5.5.

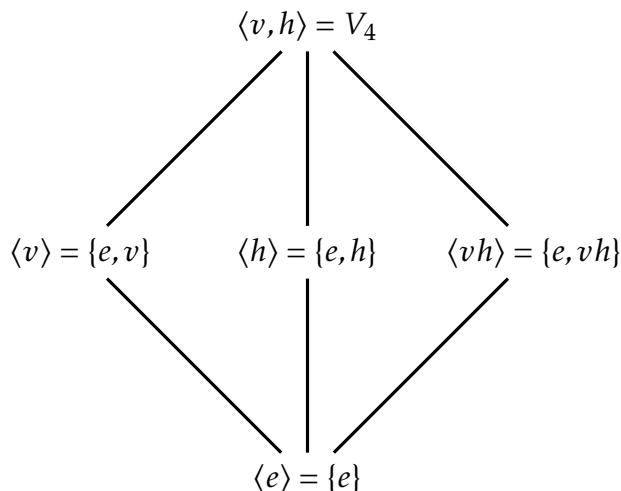


Figure 5.5. Subgroup lattice for V_4 .

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. We already know that R_4 and V_4 are not isomorphic, but this becomes even more apparent if you compare their subgroup lattices.

In the next few exercises, 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. In particular, I do *not* recommend taking a full brute-force approach like we did for R_4 .

Exercise 5.69. Find all the subgroups of $R_5 = \{e, r, r^2, r^3, r^4\}$ (where r is rotation clockwise of a regular pentagon by 72°) and then draw the subgroup lattice for R_5 .

Exercise 5.70. Find all the subgroups of $R_6 = \{e, r, r^2, r^3, r^4, r^5\}$ (where r is rotation clockwise of a regular hexagon by 60°) and then draw the subgroup lattice for R_6 .

Exercise 5.71. Find all the subgroups of $D_3 = \{e, r, r^2, s, sr, sr^2\}$ (where r and s are the usual actions) and then draw the subgroup lattice for D_3 .

Exercise 5.72. 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 Exercise 4.27) and then draw the subgroup lattice for S_3 . How does your lattice compare to the one in Exercise 5.71? You should look back at Exercise 4.28 and ponder what just happened.

Exercise 5.73. 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 actions) and then draw the subgroup lattice for D_4 .

Exercise 5.74. Find all the subgroups of $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and then draw the subgroup lattice for Q_8 .

Problem 5.75. 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? *Hint:* The answers to two of these questions should be obvious, but the answer to the remaining question should be something like, “we don’t have enough information to make any claims.”

Here are two final problems to conclude this section.

Problem 5.76. Several times we’ve referred to the fact that some subgroups are visible in a Cayley diagram for the parent group and some subgroups are not. Suppose $(G, *)$ is a group and let $H \leq G$. Can you describe a process for creating a Cayley diagram for G that “reveals” the subgroup H inside of this Cayley diagram?

Problem 5.77. Suppose $(G, *)$ is a finite group and let $H \leq G$. Can you describe a process that “reveals” the subgroup H inside the group table for G ? Where will the clones for H end up?

5.6 Revisiting Isomorphisms

Suppose $(G_1, *)$ and (G_2, \circ) are two groups. Recall that G_1 and G_2 are isomorphic, written $G_1 \cong G_2$, provided that we can choose generating sets for G_1 and G_2 , respectively, so that the Cayley diagrams for both groups are identical (ignoring the labels on the vertices). When two groups are isomorphic, it means that they have identical structure up to relabeling the names of the elements of the group.

One consequence of two groups being isomorphic is that there is a one-to-one correspondence between the elements of the group. This correspondence is referred to as an isomorphism. In other words, an isomorphism is a one-to-one and onto function that preserves the structure of the two groups.

Having an isomorphism between two groups immediately implies that they have the same order, i.e., $|G_1| = |G_2|$ (see Theorem 4.20). However, it is extremely important to remember that two groups having the same order does *not* imply that the two groups are isomorphic. Said another way, having a one-to-one correspondence between two groups does not imply that the two groups are isomorphic. They must also have the same structure!

Exercise 5.78. Provide an example of two groups that have the same order but are not isomorphic.

After we introduced groups tables, we also discussed the fact that $G_1 \cong G_2$ exactly when we can arrange the rows and columns and color elements in such a way that the

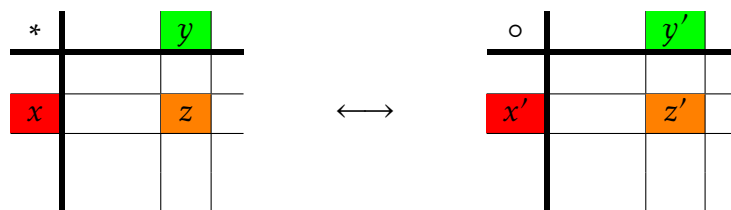


Figure 5.6

colorings for the two group tables agree (see Problem 5.39). The upshot of this is that if $G_1 \cong G_2$, 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 a little more sense of this. Suppose that $G_1 \cong G_2$ and imagine we have arranged the rows and columns of their respective group tables and colored the elements in such a way that the colorings for the two group tables agree. Now, let $x, y \in G_1$. Then these two elements have corresponding elements in the group table for G_2 , say x' and y' , respectively. In other words, x and x' have the same color while y and y' have the same color. Since G_1 is closed under its binary operation $*$, there exists $z \in G_1$ such that $z = x * y$. There must exist a $z' \in G_2$ such that z' has the same color as z . What must be true of $x' \circ y'$? Since the two tables exhibit the same color pattern, it must be the case that $z' = x' \circ y'$. This is what it means for the product of corresponding elements to yield the corresponding result. Figure 5.6 depicts this phenomenon for group tables.

We can describe the isomorphism between G_1 and G_2 using a function. Let $\phi : G_1 \rightarrow G_2$ be the one-to-one and onto function that maps elements of G_1 to their corresponding elements in G_2 . Then $\phi(x) = x'$, $\phi(y) = y'$, and $\phi(z) = z'$. Since $z' = x' \circ y'$, we can obtain

$$\phi(x * y) = \phi(z) = z' = x' \circ y' = \phi(x) \circ \phi(y).$$

In summary, it must be the case that

$$\phi(x * y) = \phi(x) \circ \phi(y).$$

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

Definition 5.79. Let $(G_1, *)$ and (G_2, \circ) 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 $\phi : G_1 \rightarrow G_2$ such that

$$\phi(x * y) = \phi(x) \circ \phi(y). \quad (5.1)$$

The function ϕ is referred to as an **isomorphism**. Equation 5.1 is often referred to as the **homomorphic property**.

You should definitely take a few minutes to convince yourself that the above definition agrees with our previous informal approach to isomorphisms. For those of you that have

had linear algebra, notice that our homomorphic property looks a lot like the requirement for a function on vector spaces to be a linear transformation. Linear transformations preserve the algebraic structure of vector spaces while the homomorphic property is preserving the algebraic structure of groups.

We've seen several instances of two groups being isomorphic, but now that we have a formal definition, we can open the door to more possibilities.

Problem 5.80. 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 $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$ via $\phi(r) = e^r$ (where e is the natural base, not the identity). Prove that ϕ is an isomorphism.

Exercise 5.81. 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 5.82. 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. It was already clear that this was the case using our informal definition of isomorphic. Prove the next theorem using Definition 5.79

Theorem 5.83. Suppose $\phi : G_1 \rightarrow G_2$ is an isomorphism from the group $(G_1, *)$ to the group (G_2, \circ) . If e and e' are the identity elements of G_1 and G_2 , respectively, then $\phi(e) = e'$.

Theorem 5.84. Suppose $\phi : G_1 \rightarrow G_2$ is an isomorphism from the group $(G_1, *)$ to the group (G_2, \circ) . Then $\phi(g^{-1}) = [\phi(g)]^{-1}$.

Theorem 5.85. Suppose $\phi : G_1 \rightarrow G_2$ is an isomorphism from the group $(G_1, *)$ to the group (G_2, \circ) . If G_1 is abelian, then G_2 is abelian.

Theorem 5.86. Suppose $\phi : G_1 \rightarrow G_2$ is an isomorphism from the group $(G_1, *)$ to the group (G_2, \circ) . Then the function $\phi^{-1} : G_2 \rightarrow G_1$ is an isomorphism.

Theorem 5.87. Suppose $\phi : G_1 \rightarrow G_2$ and $\psi : G_2 \rightarrow G_3$ 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 .

Theorem 5.88. Let \mathcal{G} be any nonempty collection of groups. Then the relation \cong of being isomorphic is an equivalence relation.

Theorem 5.89. Suppose $\phi : G_1 \rightarrow G_2$ is an isomorphism from the group $(G_1, *)$ to the group (G_2, \circ) . If $H \leq G_1$, then $\phi(H) \leq G_2$, where

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

Note that $\phi(H)$ is called the **image** of H .

Theorem 5.90. Suppose $(G, *)$ is a group and let $g \in G$. Define $\phi_g : G \rightarrow G$ via $\phi(x) = g^{-1}xg$. Then ϕ_g is an isomorphism from G to G . Note that the map ϕ_g is called **conjugation** by 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 5.91. For which of the recent theorems could we remove the assumption that the function is one-to-one and onto and only assume that it satisfies the homomorphic property? Such functions are called **homomorphisms** and will be the subject of a future chapter.