Exercises from An Inquiry Based Approach to Abstract Algebra

Heather Moore

June 15, 2020

Chapter 4: Subgroups and Isomorphisms

Exercise 4.15

The following diagram shows Q_8 with the generators i, j, and -1.

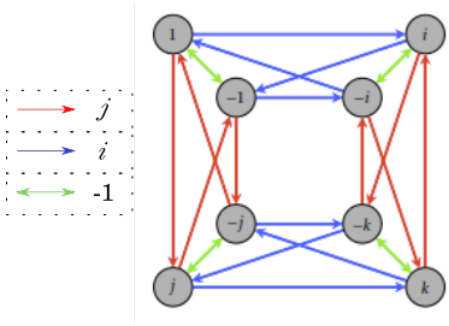


Figure 1: Q_8

By following the arrows around the diagram we can see that $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, and $i^5 = i$. Simlarly, $j^2 = -1$, $j^3 = -j$, $j^4 = 1$, and $j^5 = j$. Also, we have the following:

- $(-1)^2 = 1$
- $ij = k$
- $ji = -k$
- $k^2 = -1$
- $ik = -j$

The entire group can be generated by $< i, j >$ or by $< -i, -j >$, or by $< i, k >$, or by any such combination where one of the generators is $\pm p$ and the other is $\pm q$ where p and q are different elements of $\{i, j, k\}$.

Let's take a look at the subgroups of Q_8. The smallest is the trivial subgroup $\{1\}$. The next smallest is $\{1, -1\}$ which has four clones (including itself). It is generated by $< -1 >$. The subgroups $\{1, -1, i, -i\}$ and $\{1, -1, j, -j\}$ are isomorphic to R_4 and each have another clone on the opposite side of the diagram. They are generated by $< i >$ and $< j >$ respectively (or by $< -i >$ and $< -j >$). The generating set $< k >$ generates a similar subgroup $\{1, -1, k, -k\}$ which cannot be easily seen on the diagram.

Exercise 4.16

The Cayley diagram of D_3 contains two subgroups that are isomorphic to S_2: $\{e, s\}$ and $\{e, s_1\}$.

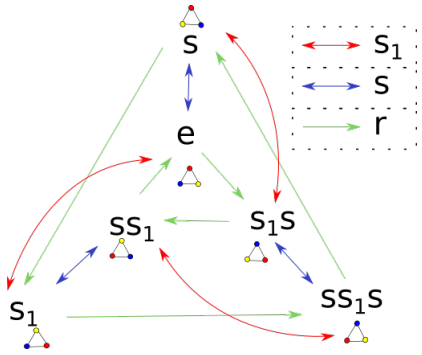


Figure 2: D_3

Definition 4.17

Let G and G_0 be two groups. We say that G and G_0 are isomorphic if there exist generating sets S and S_0 for G and G_0 , respectively, such that the corresponding Cayley diagrams are identical where we ignore the labels on the vertices and recolor the edges if necessary. In this case, we write $G \cong G_0$. Otherwise, we say that G and G_0 are not isomorphic. If G and G_0 are isomorphic, then the one-to-one correspondence determined by matching up the corresponding generators and respecting arrow paths is called an isomorphism.

Definition 4.18

If G is a group with n distinct actions, then we say that G has **order** n and write $|G| = n$. If G contains infinitely many elements, then we say G has infinite order and write $|G| = \infty$.

Exercise 4.19

Here are the orders of some groups we've seen:

- $|S_2| = 2$
- $|\text{Spin}_{1\times 2}| = 8$
- $|\text{Spin}_{3\times 3}| = 9! * 2^9$
- $|R_4| = 4$
- $|D_3| = 6$

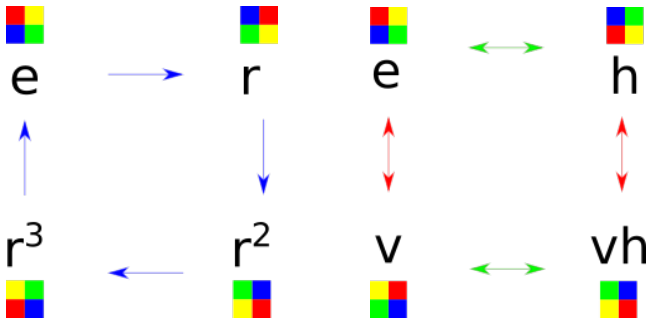
- $|D_4| = 8$
- $|V_4| = 4$
- $|Q_8| = 8$

Theorem 4.20

Suppose G and G_0 are two groups of actions such that $G \cong G_0$. Then $|G| = |G_0|$.

By Definition 4.17 we know that two groups that are isomorphic have a one-to-one correspondence between the vertices and generator arrows. This entails that there be the same number of vertices in each group, and therefore we know that the order of the two groups is the same.

Problem 4.21

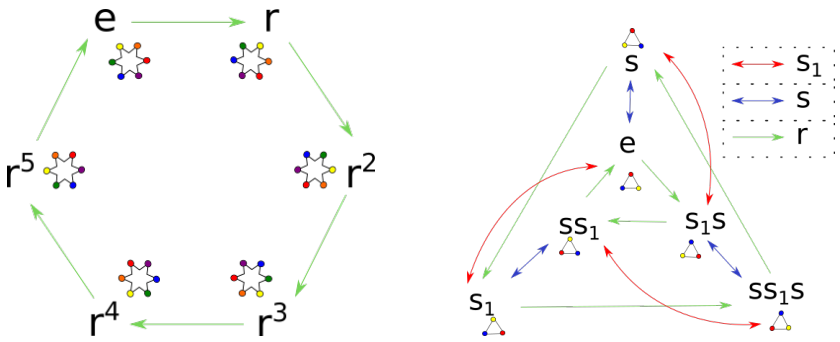


(a) R_4

(b) V_4

The two groups shown above, R_4 and V_4, are not isomorphic because of the behavior of the generating actions. The action r cannot be mapped to either v or h because v and h are their own inverses and r is not.

Problem 4.22



(a) R_6 (b) D_3

These two groups are not isomorphic either. The action r in R_6 requires a minimum of 6 applications to get back to the identity action. None of the actions in D_3 have this property so there is no one to one mapping.

Exercise 4.23

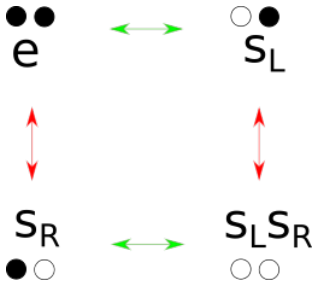


Figure 5: L_4

Problem 4.24

The groups L_2 and V_4 are isomorphic! Here is the mapping:

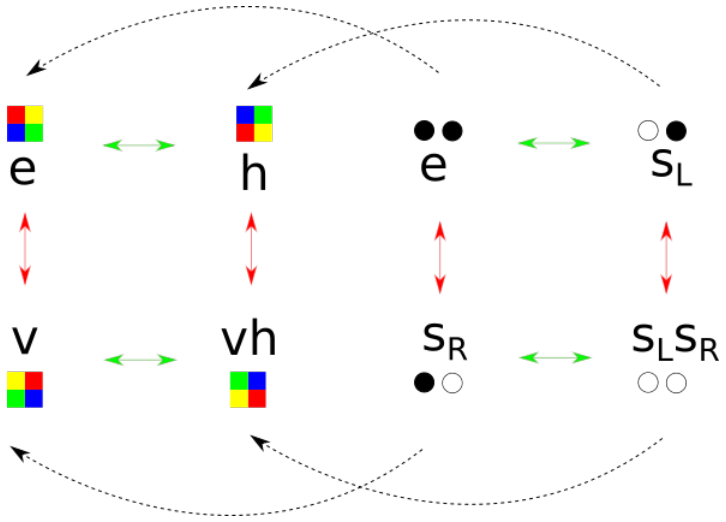
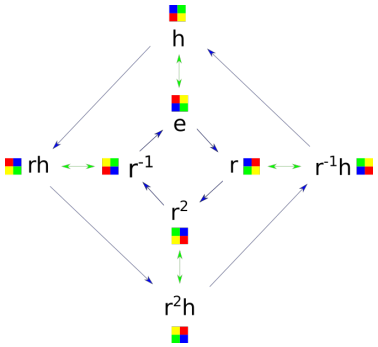
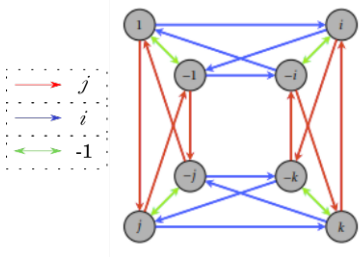


Figure 6: $L_2 \to V_4$

Problem 4.25



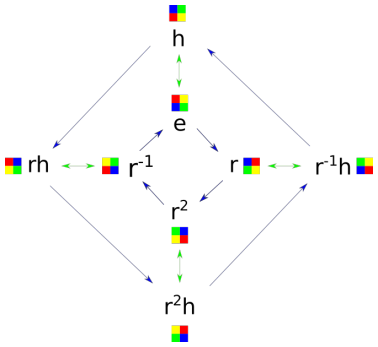
(a) D_4



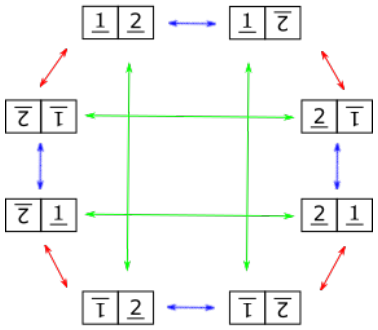
(b) Q_8

The groups D_4 and Q_8 are not isomorphic. In Q_8 there are two subgroups containing e that are each isomorphic to R_4, whereas in D_4 there is only one.

Problem 4.26



(a) D_4



(b) $\mathrm{Spin}_{1\times 2}$

The groups D_4 and $\mathrm{Spin}_{1\times 2}$ are not isomorphic. The action r in D_4 must be applied a minimum of four times to return to e, but in $\mathrm{Spin}_{1\times 2}$ there is no such action.

Exercise 4.27

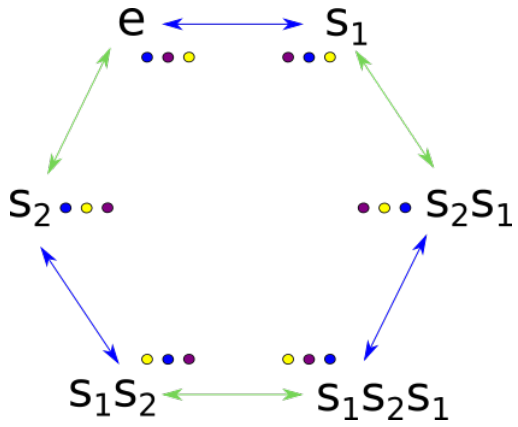
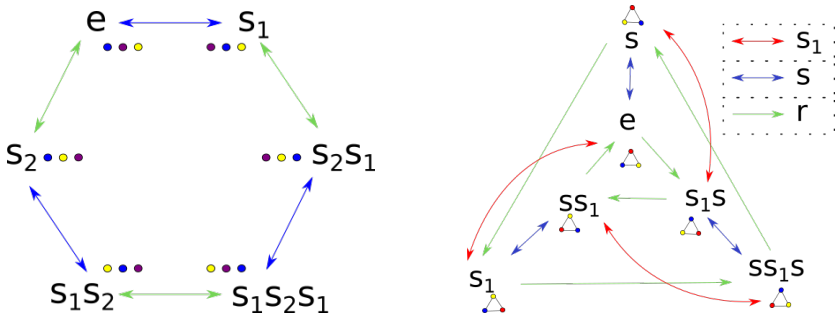


Figure 9: S_3

Problem 4.28



(a) S_3 (b) D_3

The group S_3 is isomorphic with D_3 under the generators s and s_1. Here is the mapping:

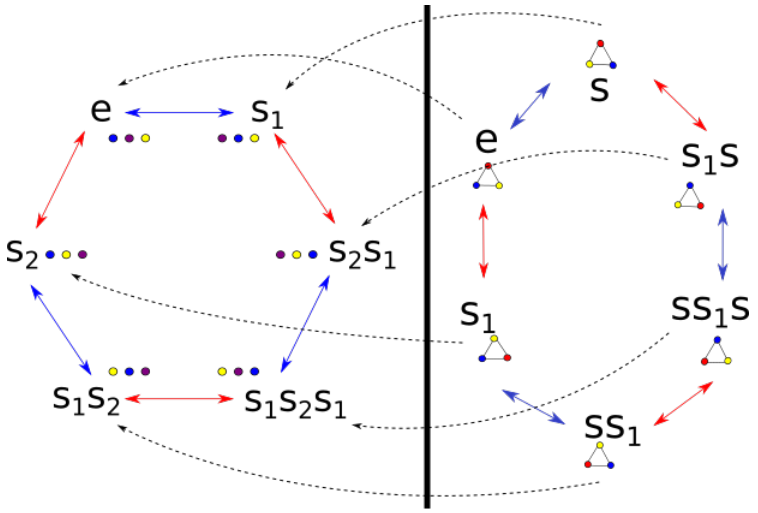


Figure 11: $D_3 \to S_3$

Chapter 5: Formal Groups

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 $a * b$.

Exercise 5.8

Composition of spins is not a binary operation on the set of allowable spins in $\text{Spin}_{3\times3}$ because the net effect of some sequences of spins cannot be reproduced by a single allowable spin. However, composition would be a binary operation on the group of all *actions* in $\text{Spin}_{3\times3}$.

Exercise 5.9

Neither matrix addition nor matrix multiplication on $M(\mathbb{R})$ are binary operations because not all pairs of elements of $M(\mathbb{R})$ are in their domains. However, this problem is circumvented for both operations if we restrict to square matrices of a fixed size $n \times n$.

Exercise 5.10

Both $\cup$ and $\cap$ are binary operations on $\mathcal{P}(\mathbb{Z})$. Taking either the union or the intersection of any two sets of integers will yeild a single set of integers. In other words, $\cup$ and $\cap$ are both closed and well defined on $\mathcal{P}(\mathbb{Z})$.

Exercise 5.11

Consider the closed interval $[0, 1]$ and define $*$ on $[0, 1]$ via $a * b = \min\{a, b\}$. All pairs of numbers within the interval $[a, b]$ are in the domain of the minimum function, which is to say that any pair of numbers has a minimum value. The output will always be a single value; there are never two minimum values in a pair of numbers. Therefore, $*$ is a binary operation.

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

Multiplication on the real numbers is commutative, but matrix multiplication on the set of real number matrices is not.

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.

Exercise 5.16

A table showing the outputs of a binary operation must have reflective symmetry across the middle diagonal of cells (the diagonal that represents each input combined with itself).

$$\begin{array}{ccc} a^2 & a*b & a*c \\ b*a & b^2 & b*c \\ c*a & c*b & c^2 \end{array}$$

Exercise 5.17

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

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}.

Exercise 5.20

Explain why axiom 0 is unnecessary.

It is not necessary to specify that G is closed under $*$ because by definition binary operations have the property of closure.

Exercise 5.21

Let us see how our intuitive definition of a group matches up with our new formal definition. Here is the list of four rules that made up our intuitive definition:

Rule 1: There is a predefined list of actions that never changes.

Rule 2: Every action is reversible.

Rule 3: Every action is deterministic.

Rule 4: Any sequence of consecutive actions is also an action.

It is easy to see that **Rule 2** matches up with the third axiom that requires that each element have an inverse. The second axiom requiring an identity element is a prerequisite for the third axiom, so both these axioms are expressed by **Rule 2**. **Rule 4** is equivalent to saying that the operation is closed which is expressly clarified in axiom 0. The fact that a binary operation is a function guarantees that the operation is well defined, which is **Rule 3**. The associative property guaranteed by the first axiom ensures that function composition is also deterministic. **Rule 1** is covered in the definition of a group as being a binary operation *and a set*, meaning that there is a predefined domain for the operation and that every element of the set is always in the domain for the binary operation.

Exercise 5.22

All of the groups we have considered so far can be verified to satisfy the formal axioms if we can say definitively that all correctly drawn Cayley diagrams guarantee adherence to the axioms.

Associativity is ensured in that following one arrow, followed by the group of two others is always identical to following the first two arrows and then the third.

We can see that a Cayley diagram is closed and well defined by noting that all vertices can be reached by following a sequence of arrows, that vertices have an arrow of each color leaving and arriving, and that no arrows head off into nothingness, but always arrive at another vertex.

Making sure that e is included in the diagram and that paths exist from every vertex to e ensures that the group has an identity and that all of the actions have inverses.

Since we have constructed Cayley diagrams with these properties for all the groups we've considered so far, we can be sure they adhere to our new formal axioms.

Exercise 5.23

Let take a tour of some common sets on binary operations and see if they are groups by our formal definition:

- $(\mathbb{Z}, +)$ is a group. The identity element is 0 and the inverse of an integer n is $-n$. All integers are in the domain of the addition operation, and the result of adding any two integers is another integer. This group is abelian.
- $(\mathbb{N}, +)$ is not a group because without negative numbers included in our group, there are no inverses. This group is abelian.
- $(\mathbb{Z}, \cdot)$ is not a group because multiplicative inverses are non-integer rationals.
- $(\mathbb{R}, +)$ is a group. The identity element is 0 and the inverse of a real number r is $-r$. All real numbers are in the domain of addition and the result of adding any two real numbers is another real number. This group is abelian.
- $(\mathbb{R}, \cdot)$ is not a group because 0 has no multiplicative inverse.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group. The multiplicative inverse of a real number is its reciprocal and without 0 in the mix that covers everybody. The identity element is 1. All non-zero real numbers are in the domain of multiplication and the result of multiplying any two real numbers is another real number. This group is abelian.
- $(M_{2\times 2}(\mathbb{R}), +)$ is a group. The identity element is the 2×2 matrix with 0 in all the cells and the inverse of a matrix m is $-1m$. This group is abelian.
- $(M_{2\times 2}(\mathbb{R}), *)$ where $*$ is matrix multiplication is a group. All pairs of two by two matrices can be combined with matrix multiplcation to produce another two by two matrix. The identity element is the identity matrix and the inverse of a matrix is its inverse matrix! This group is not abelian because matrix multiplication is not commutative.
- $(\{a, b, c\}, *)$ where $*$ is defined by the following table from Exercise 5.15 is not a group because there is no consistent identity element.

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

- $(\{a, b, c, d\}, *)$ where $*$ is defined by the following table from Exercise 5.17 is also not a group because while a appears to be an identity element, c and d have no inverse.

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

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 $g \in G$.

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 $x = y$.

Suppose that $g * x = g * y$.
Then, $g^{-1} * (g * x) = g^{-1} * (g * y)$ because $*$ is deterministic.
Therefore, $(g^{-1} * g) * x = (g^{-1} * g) * y$ because $*$ is associative.
Finally, $e * x = e * y$ and so $x = y$.

Exercise 5.26

To see that $(\mathbb{R}, \cdot)$ fails the Cancellation Law consider that $5 \cdot 0 = \pi \cdot 0 = 0$. By the Cancellation Law, 5 should then be equal to π. Since this is not the case, the Cancellation Law does not hold.

Corollary 5.27

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

Suppose that a and b are both inverses of g. Then, $g * a = g * b = e$. Therefore, by the Cancellation Law, $a = b$.

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 $x, y \in G$.

Suppose that both x_1 and x_2 are solutions to the equation $g * x = h$. Then, $g * x_1 = g * x_2 = h$, and so by the Cancellation Law $x_1 = x_2$. We also know that such a solution exists because x, g and h are all members of the group, so there must be some element x that results in h when applied to g.

A symmetric argument shows the same for y.

Theorem 5.29

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

If $g * h = e$, then h and g are inverses. By definition, $g * g^{-1} = g^{-1} * g = e$. So, $h * g = g * h = e$.

Theorem 5.30

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

For any element $g \in G$, we have that $g^{-1} * g = e$.
So, $(g^{-1})^{-1} * g^{-1} = e$.
Since $g * g^{-1} = e$ as well, we know that $(g^{-1})^{-1}$ and g are identical.

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 $g^0 = e$.

Theorem 5.32

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

(a) $g^n * g^m = \underbrace{g * g * \cdots * g}_{n \text{ factors}} * \underbrace{g * g * \cdots * g}_{m \text{ factors}}$

Therefore, $g^n * g^m = g^{n+m}$

(b) By definition, $g^n * (g^n)^{-1} = e$.
Also, by part (a), $g^n * g^{-n} = g^{n+(-n)} = g^0 = e$.
So, $g^n * (g^n)^{-1} = g^n * g^{-n} = e$.
And therefore, $(g^n)^{-1} = g^{-n}$.

Exercise 5.33

The table has symmetry across the diagonal from the upper left to the lower right. This reveals that V_4 is abelian.

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

Exercise 5.34

Table 1: S_2

$*$	e	s
e	e	s
s	s	e

Table 2: R_3

$*$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

Table 3: R_4

$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

Table 4: D_3

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

Table 5: S_3

$*$	e	s_1	s_2s_1	$s_1s_2s_1$	s_1s_2	s_2
e	e	s_1	s_2s_1	$s_1s_2s_1$	s_1s_2	s_2
s_1	s_1	e	$s_1s_2s_1$	s_2s_1	s_2	s_1s_2
s_2s_1	s_2s_1	s_2	s_1s_2	s_1	e	$s_1s_2s_1$
$s_1s_2s_1$	$s_1s_2s_1$	s_1s_2	s_2	e	s_1	s_2s_1
s_1s_2	s_1s_2	$s_1s_2s_1$	e	s_2	s_2s_1	s_1
s_2	s_2	s_2s_1	s_1	s_1s_2	$s_1s_2s_1$	e

Table 6: D_4

$*$	e	r	r^2	r^3	h	rh	r^2h	hr
e	e	r	r^2	r^3	h	rh	r^2h	hr
r	r	r^2	r^3	e	rh	r^2h	hr	h
r^2	r^2	r^3	e	r	r^2h	hr	h	rh
r^3	r^3	e	r	r^2	hr	h	rh	r^2h
h	h	hr	r^2h	rh	e	r^3	r^2	r
rh	rh	h	hr	r^2h	r	e	r^3	r^2
r^2h	r^2h	rh	h	hr	r^2	r	e	r^3
hr	hr	r^2h	rh	h	r^3	r^2	r	e

Table 7: Q_8

$*$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Of the groups shown, only S_2, R_3 and R_4 are abelian.

Theorem 5.35

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

Proof. Suppose that an element g appeared twice in a single column. That would mean that both $x * y_1 = g$ **and** $x * y_2 = g$ for any $y_1, y_2 \in G$ where $y_1 \neq y_2$. But then,

$$\begin{aligned} x^{-1} * x * y_1 &= x^{-1} * g \\ y_1 &= x^{-1} * g \end{aligned}$$

and

$$\begin{aligned} x^{-1} * x * y_2 &= x^{-1} * g \\ y_2 &= x^{-1} * g \end{aligned}$$

By the definition of a group we know that $x^{-1} \in G$ and therefore Theorem 5.28 guarantees that $x^{-1} * g$ must have a unique solution. So, $y_1 = y_2$ and g does not appear twice in the same column after all.

A symmetric argument can be made showing that g cannot appear twice in the same row either.

Now, a group table for G contains a column and a row for each element, and therefore has the same number of columns and rows as the number of elements in G. Each cell in a row or column must be occupied by an element of the group. But, since an element cannot appear twice in a row or column, each element must appear exactly once in every row and column. □

Exercise 5.36

The discussion in the book shows that there is a way to draw the group tables for V_4 and the group A such that the product of corresponding elements yields the corresponding result. We could, in other words, replace all the vertices in a Cayley diagram for V_4 with the corresponding elements from A. We have already seen that when you follow sequences of arrows around a Cayley diagram the way you group the sequences doesn't change where you end up. So, associativity is present for V_4 and for any group that can be shown to have an equivalent structure in this way.

Exercise 5.37

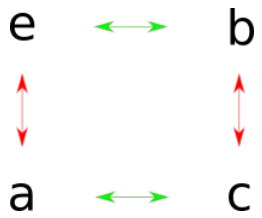


Figure 12: $A \cong V_4$

There is a one to one mapping between each arrow and each vertex in A to a corresponding arrow or vertex in V_4, so the two are isomorphic.

Exercise 5.38

$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

Table 8: R_4

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

Table 9: V_4

It is not possible to color these two tables so that they match. They are not isomorphic. There are many ways to see this, but one is to consider that none

of the elements in R_4 are their own inverses, but all of the elements in V_4 are their own inverses.

Problem 5.39

Let $(G, *)$ and $(G', \circ)$ be two finite groups. If we can arrange the rows and columns and color the elements in such a way that the colorings for the two group tables agree, that means that the sequences of actions you must take to move between the elements of the groups are identical and so the two groups are isomorphic. If the group tables map in this way, it is equivalent to the Cayley diagrams having a one-to-one mapping, and so either comparison is a valid method of establishing isomorphism.

Problem 5.40

Suppose we have a table for $(G, *)$, where G is finite. If we know that there is an identity element, and that every element appears exactly once in each row and in each column, we have almost all we need to establish that G is a group. We know that $*$ is a binary operation because the table shows an output for any combination of two inputs and all of those outputs are elements of G. Also, we know that every element of G has an inverse because the identity element appears in every row and column and so there is a "path" from every element to the identity. The only remaining property of a group to establish is associativity.

Problem 5.41

If you try to create a group table with two identities the cell where the two identities combine must meet two conflicting requirements. An identity element does not change any element it combines with, but it cannot help but do so in the case of two different identities combining. Let us say the first identity is e and the second is e_1. The cell where they combine would have to be e_1 because otherwise e would be changing e_1 when applied to it. But the reverse is also true. The cell must be e because otherwise e_1 would be changing e when combined with it and would not be an identity element. Thus, it is impossible to create a consistent group table with two identity elements.

Problem 5.42

All groups with a single element are isomorphic because there is only one way for such a group to be. The element is an identity and it is its own inverse and there is no other structure that a single element group could take on.

Problem 5.43

$*$	e	a
e	e	a
a	a	e

The table above shows the only possible group table for a group of order two. The cells in the e column and the e row are determined by e being the identity. There is only one remaining cell which must be filled in by e for at least two reasons. First, e needs to appear in row two and column two. Secondly, a needs an inverse. The identity cannot be the inverse of a and so a must be its own inverse.

This is the group table for S_2 and so all groups of order two are isomorphic to it.

Problem 5.44

For a group of order three, there are only two possible ways to fill in the identity element in the table. Either a and b are their own inverses, or they are the inverses of each other. If they are their own inverses, we have the following situation:

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

There is no way to consistently fill in the third element of the second row, since filling it in with b would result in b appearing twice in that column. A symmetric conflict arises for the second cell in the third row.

So, a and b must be the inverses of each other and we have the following table, which is the table for R_3.

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

All groups of order three must therefore be isomorphic to R_3.

Problem 5.45

Here are the two possible ways to fill out group tables of order 4:

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

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

The one on the left is isomorphic to V_4. Notice that all the actions in the group are their own inverses. The table on the right is isomorphic with R_4 with b mapping on to r^2 and a and c being inverses of each other just like r and r^3.

Since these are the only two possibilities, all groups of order 4 are isomorphic to either D_4 or R_4.

Exercise 5.46

Does the following diagram satisfy all the rules of our informal definition of a group? It depends on what is meant by Rule 1: There is a basic set of actions that never changes. The diagram in figure 5.1 satisfies the restriction that all vertices have an arrow of each color leaving and arriving, but sometimes the action represented by the red arrow is its own inverse and sometimes it is not. A strict interpretation of what it means for an action to change would disqualify this diagram.

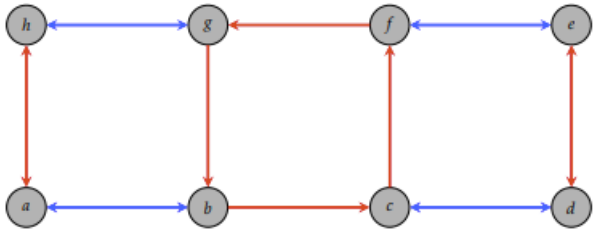


Figure 5.1

Trying to convert the diagram to a group table reveals a problem that disqualifies it as a group. Starting from c, taking the red arrow action results in f. But, you can also arrive at f from c by following blue, then red, then blue. Regardless of how you choose the identity, some action in the group will correspond to this blue-red-blue path. So, we can get from c to f either by taking the action corresponding to the red arrow, or by the action corresponding to blue-red-blue. This causes f to appear twice in the c column.

Exercise 5.47

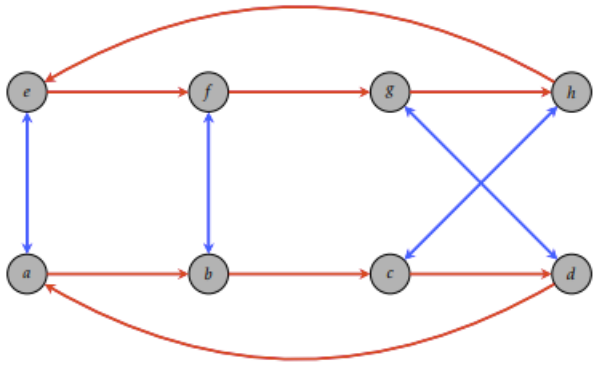


Figure 5.2

This time the red and blue arrow generators are at least consistently single or double arrows. But the assymetry between the left and right hand side of the diagram is suspicious.

It turns out that there are problems that arise if you try to make this diagram into a group table. One way of seeing the problems is to notice that some combinations of the generators do not have a consistent inverse. Starting from a, an inverse of blue-red-red is blue-red. But, if you start from d and following blue-red-red and then blue-red, you wind up at b instead of back at d like you would be if the inverse relation still held.

In the group table, this means that the path of generators you pick to stand in for an action sometimes makes a difference and only one of the paths will create a consistent table. For a diagram to truly be a group, it shouldn't matter how you name an action in terms of the generators, it will always come out the same.

Exercise 5.48

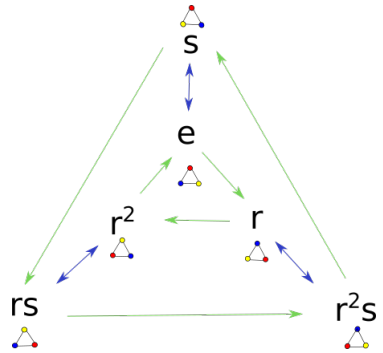


Figure 13: D_3

Here are some relations that hold throughout the diagram:

- $srsr = e$
- $sr^{-1}sr = r^2$

Exercise 5.49

In Figure 5.1, blue-red-blue sometimes equals red, but sometimes equals backwards red. We already saw how Figure 5.2 was not regular in Exercise 5.47.

Problem 5.50

There are many ways to think about why a Cayley diagram for a group must be regular. The basic idea is that actions, and therefore sequences of actions must always do the "same thing". One way to link this to the formal definition is to consider that if a relation does not hold throughout the group, an action will not always have a consistent inverse.

Problem 5.51

Suppose $(G, *)$ is a group and S is a generating set for G. If G is abelian and $a, b \in S$, then any sequence of n arrows representing a and m arrows representing b must be equivalent, regardless of the order of the arrows.

The converse of this statement is also true. This ability to arrange the arrows in any order is essentially what it means to be commutative or abelian.

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.

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.

Proof. First, let us recall the 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}.

It is clear that if either conditions (i) or (ii) do not hold then H cannot be a group in its own right. We need to show that they are sufficient, given that H is defined to be a subset of G.

We can check the axioms one by one. Axiom 0 is guaranteed directly by part (ii). Axiom 1 holds because we already know $*$ is associative from the knowledge that G is a group. Axiom 3 is guaranteed by (i) directly.

All that is left to show is that there is an identity element in H. If part (i) holds, then there is an inverse for every member of the group. Combining a given element h with it's inverse h^{-1} results in e. And if (ii) holds, then closure implies that e must then be in the set as well. And so axiom 2 is satisfied.

□

Exercise 5.55

Consider $(\mathbb{R}^3, +)$, where $\mathbb{R}^3$ is the set of all 3-entry row vectors with real number entries and $+$ is ordinary vector addition.

Let H be the subset of $\mathbb{R}^3$ consisting of vectors with first coordinate 0. H is a subgroup of $\mathbb{R}^3$.

Proof. By Theorem 5.53, we need only show that every element in H has an inverse and that it is closed over vector addition.

For all $y, z \in \mathbb{R}$ the inverse of an element $(0, y, z)$ is $(0, -y, -z)$, which has a first coordinate of 0 and so is an element of H.

Also, for any $a, b, c, d \in \mathbb{R}$ adding $(0, a, b) + (0, c, d)$ results in a new vector $(0, a + c, b + d)$ which still has a first coordinate of 0 and so is an element of H. □

Let K be the subset of $\mathbb{R}^3$ consisting of vectors whose entries sum to 0. K is also a subgroup of $\mathbb{R}^3$.

Proof. Again we need to show that every element in K has an inverse that is also in K and that K is closed under vector addition.

Let M be the vector (x, y, z) for any $x, y, z \in \mathbb{R}^3$ where $x + y + z = 0$. Then $M \in K$ and the inverse of M is $(-x, -y, -z)$. Now, $-x + (-y) + (-z) = -(x + y + z) = -(0) = 0$, so M^{-1} is also an element of K.

Let N be a second vector in K with coordinates (a, b, c). Then $M + N = (x + a, y + b, z + c)$ and so the sum of the coordinates of this new vector is $(x + a) + (y + b) + (z + c) = (x + y + z) + (a + b + c) = 0 + 0 = 0$. So, the new vector is also a member of K, and K is closed under vector addition. □

Let L be the subset of $\mathbb{R}^3$ consisting of vectors whose entries sum to 1. L is not a subgroup of $\mathbb{R}^3$. To see why, consider that the inverse of an element of L will have coordinates that sum to -1 and so will not be a member of L.

Exercise 5.56

The even integers are a subgroup of the integers under addition because for any $n \in \mathbb{Z}$, the inverse of $2n$ is $-2n$ and adding any two even integers results in another even integer.

However, adding two odd integers results in an even integer, so the odd integers are not a subgroup of the integers under addition. (They are, however, a *clone* of the even integer subgroup!)

The proof for $n\mathbb{Z}$ is the same as for $2n$.

There are no other subgroups of $\mathbb{Z}$ The simplest generating set is $1, -1$. For $2n$ you take two of each of these at once for a generating set of $2, -2$. This has the effect of stretching out the number line but preserving the symmetry and structure of the group. If there were another subgroup we would need a smaller or alternate generating set with which to generate the subgroup.

Exercise 5.57

In D_8 the subset consisting of rotations by $0°, 90°, 180°$ and $270°$ is a subgroup. The $90°$ and $270°$ rotations are inverses of each other and $180°$ is its own inverse. They are all multiples of $90°$. Combining any two results in another multiple of $90°$.

Exercise 5.58

The definition of a subgroup requires that the subgroup be a group under the same binary operation of the original group. We can see that $(\mathbb{R} \setminus 0, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$ by noting that it lacks the identity and so is not a group in its own right under addition.

Theorem 5.59

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

Proof. Any element that is in both H and K will have an inverse in both H and K as well. Therefore, if an element is in $H \cap K$ its inverse will be as well. We can conclude from this that all elements in $H \cap K$ have an inverse in $H \cap K$.

Let $g, h \in H \cap K$. Since both H and K are closed under $*$, any combination of h and g is contained in both H and K and so will also be in the intersection. Therefore,$H \cap K$ is closed under $*$.

By Theorem 5.53, these two conditions are sufficient for showing that $H \cap K$ is a group. □

Problem 5.60

We cannot replace intersection with union in the previous theorem. To see a counterexample, consider $V_4 = \{e, v, h, vh\}$ and two of its subgroups $< v >$ and $< h >$. The union of these two subgroups is $\{e, v, h\}$ which lacks the element vh. The union, therefore, is not closed and so is not a group in its own right.

Theorem 5.61

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

Proof. Let $g, h \in H$. By definition, G is abelian if and only if $a * b = b * a$ for all $a, b \in G$. Since H is a subgroup of G we know that $g, h \in G$. So we have that $g * h = h * g$. Therefore, H is abelian. □

Problem 5.62

The converse of the previous theorem is not true. Consider the counter-example D_3. The group R_3 is a subgroup of D_3. R_3 is abelian, but D_3 is not.

Theorem 5.63

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

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

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

Proof. □

Exercise 5.64

- $Z(S_2) = S_2$
- $Z(V_4) = V_4$
- $Z(S_3) = \{e\}$
- $Z(D_3) = \{e\}$
- $Z(D_4) = \{e, r^2\}$
- $Z(R_4) = R_4$
- $Z(R_6) = R_6$
- $Z(\mathrm{Spin}_{1\times 2}) = \{e, t_1 t_2\}$
- $Z(Q_8) = \{1, -1\}$
- $Z((\mathbb{Z}, +)) = (\mathbb{Z}, +)$
- $Z((\mathbb{R} \setminus 0, \cdot)) = (\mathbb{R} \setminus 0, \cdot)$

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 $\langle S \rangle$.

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.

Proof. We need to show that $\langle S \rangle$ is a group in its own right, and that no smaller subgroups containing S exist.

By Definition 5.65, all possible products of elements from S are contained in $\langle S \rangle$, so $\langle S \rangle$ is closed. Also by that definition, the inverses of these products are in S. We have therefore satisfied both conditions required by Theorem 5.53, and so $\langle S \rangle$ is a group in its own right.

Since S is a subset of G and a group in its own right, S is a subgroup of G.

Now we turn to whether $\langle S \rangle$ is the smallest subgroup of G containing S. Let $H \leq G$ such that every element of S is contained in H and H is smaller than $\langle S \rangle$. Then there exists at least one element g such that $g \in \{\langle S \rangle \setminus H\}$. Since H is defined to contain all the original elements of S, g must not be an element of S. The only other elements in $\langle S \rangle$ are possible products of the elements in S, so g must be one of these possible products. But g is not contained in H, so H is lacking one of the possible products of the elements of S. Therefore, H is not closed under $*$. Thus, H cannot exist and $\langle S \rangle$ is the smallest subgroup of G containing S. □

Exercise 5.67

The only two generating sets for $n\mathbb{Z}$ seem to be $\langle n \rangle = n\mathbb{Z}$ or $\langle -n \rangle = n\mathbb{Z}$. Larger multiples of n won't generate n itself.

Theorem 5.68

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 $\langle g_1, g_2, \ldots, g_n \rangle = \langle g_1, g_2, \ldots, g_n, x \rangle$.

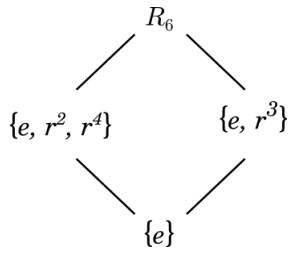
Proof. Since $x \in \langle g_1, g_2, \ldots, g_n \rangle$, we know that $x = g_i * g_j$ for some $g_i, g_j \in \{g_1, g_2, \ldots, g_n\}$. So, for all $g \in \{g_1, g_2, \ldots, g_n\}$, $x * g = (g_i * g_j) * g$. But $(g_i * g_j) * g$ is one possible product of the elements in $\{g_1, g_2, \ldots, g_n\}$ and so is already contained in $\langle g_1, g_2, \ldots, g_n \rangle$. Thus, all elements in $\langle g_1, g_2, \ldots, g_n, x \rangle$ are also in $\langle g_1, g_2, \ldots, g_n \rangle$ and therefore $\langle g_1, g_2, \ldots, g_n \rangle = \langle g_1, g_2, \ldots, g_n, x \rangle$. □

Exercise 5.69

The only subgroups of R_5 are R_5 itself and $\{e\}$.

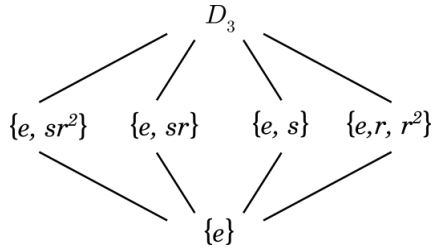
Exercise 5.70

The subgroups of R_6 are R_6 itself, $\{e, r^2, r^4\}$, $\{e, r^3\}$ and $\{e\}$.



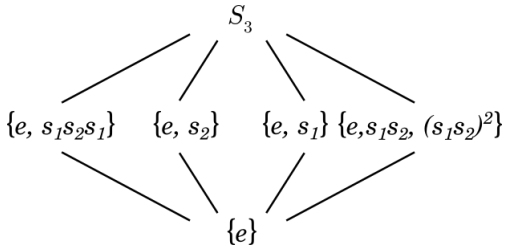
Exercise 5.71

There are four non-trivial subgroups of D_3: $\langle r \rangle = \{e, r, r^2\}$, $\{e, s\}$, $\{e, sr\}$, $\{e, sr^2\}$.



Exercise 5.72

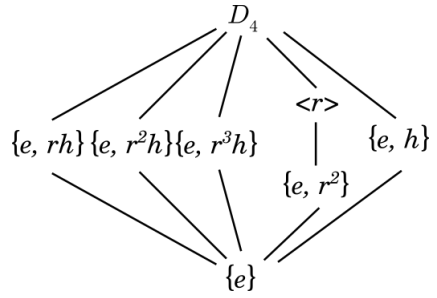
There are four non-trivial subgroups of S_3: $\langle s_1 s_2 \rangle = \{e, s_1 s_2, (s_1 s_2)^2\}$, $\{e, s_1\}$, $\{e, s_2\}$, $\{e, s_1 s_2 s_1\}$.



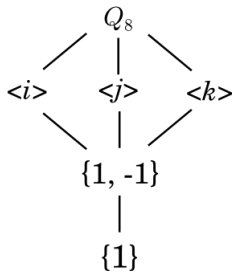
Hey, look! It's isomorphic to D_3! Drawing the subgroup lattice makes the isomorphism apparent even if different generators are used.

Exercise 5.73

There are six non-trivial subgroups of D_4: $\langle r \rangle = \{e, r, r^2, r^3\}$, $\{e, r^2\}$, $\{e, h\}$, $\{e, rh\}$, $\{e, r^2 h\}$, $\{e, r^3 h\}$.



Exercise 5.74



Problem 5.75

If two groups are isomorophic, their subgroup lattices will have the same structure. It follows that if the subgroup lattices of two groups look nothing alike, they cannot be isomorphic. On the other hand, if two groups are not isomorphic we don't know how their subgroup lattices will compare. They might be similar and simply have different kind of subgroups.

Problem 5.76

To generate a Cayley diagram that reveals a particular subgroup, construct the diagram by using the generators of that subgroup as generators for the diagram.

Problem 5.77

To construct a group table that reveals a subgroup, generate the columns by applying the generator of the subgroup repeatedly so that the first series of columns are all headed by members of that subgroup. Every time you add a new column after that, make sure to apply the same generator to create the head of the next column. In this way, the subgroup will be visible in the upper left hand corner of the group table and clones will show up in adjacent blocks of the table.

Section 5.6

Exercise 5.78

The groups R_4 and V_4 both have an order of 4, but they are not 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 $\phi : G_1 \to G_2$ such that

$$\phi(x * y) = \phi(x) \circ \phi(y) \tag{1}$$

The function ϕ is referred to as an **isomorphism**. Equation (1) is often referred to as the **homomorphic property**.

Problem 5.80

For the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ define $\phi : \mathbb{R} \to \mathbb{R}^+$ to be $\phi(r) = e^r$ for all $r \in \mathbb{R}$. Then ϕ is an isomorphism.

Proof. Note that, by the properties of exponents, $e^{(x+y)} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}$. Rewriting in terms of ϕ we have $\phi(x + y) = \phi(x) \cdot \phi(y)$. This matches the condition in Definition 5.79 and so ϕ is an isomorphism.

□

Exercise 5.81

(a) No, $\phi(n) = n + 1$ is not an isomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ under addition. $\phi(x + y) = \phi(x) + \phi(y) - 1$.

(b) However, $\phi(n) = -n$ is an isomorphism under the conditions in (a) because $-(x + y) = -x + (-y)$.

(c) Yes, $\phi(x) = x/2$ is an isomorhpism from $\mathbb{Q}$ to $\mathbb{Q}$ under addition because $\frac{x+y}{2} = \frac{x}{2} + \frac{y}{2}$.

Problem 5.82

The groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic.

Proof. Define $\phi : \mathbb{Z} \to 2\mathbb{Z}$ to be $\phi(n) = 2n$. For all $x, y \in \mathbb{Z}$, $2(x + y) = 2x + 2y$ and so $\phi(x + y) = \phi(x) + \phi(y)$. Therefore ϕ is an isomorphism for the two groups, showing that they are isomorphic. □

Theorem 5.83

Suppose $\phi : G_1 \to G_2$ 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 $\phi(e) = e'$.

Proof. Since ϕ is an isomorphism, we have that $\phi(x * y) = \phi(x) \circ \phi(y)$ for any $x, y \in G_1$. So, $\phi(x * e) = \phi(x) \circ \phi(e)$. And since $x * e = x$, $\phi(x) = \phi(x) \circ \phi(e)$. But the only element in a group that gives back the same element it is combined with is the identity element. And so we see that $\phi(e)$ must be e' the identity element for G_2. □

Theorem 5.84

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

Proof. By definition, we know that $\phi(g * g^{-1}) = \phi(g) \circ \phi(g^{-1})$. The left side is equivalent to $\phi(e)$, which by the previous theorem is just the identity element for G_2, or e'. So we see that $\phi(g^{-1})$ is the element that combines with $\phi(g)$ to get the identity. That is, $\phi(g^{-1})$ is the inverse of $\phi(g)$, or $\phi(g^{-1}) = [\phi(g)]^{-1}$.
□

Theorem 5.85

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

Proof. By definition we know both that $\phi(x * y) = \phi(x) \circ \phi(y)$ and $\phi(y * x) = \phi(y) \circ \phi(x)$. Since G_1 is abelian, $x * y = y * x$ and so the two lefthand sides of the above equations are equal. That is, $\phi(x * y) = \phi(y * x)$. Therefore the two righthand sides of the equations are equal so that $\phi(x) \circ \phi(y) = \phi(y) \circ \phi(x)$ which means that G_2 is abelian. □

Theorem 5.86

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

Proof. Let $\phi^{-1} : G_2 \to G_1$ be the inverse function of ϕ so that $\phi^{-1}(\phi(g)) = g$ for any $g \in G_1$ and $\phi(\phi^{-1}(g')) = g'$ for any $g' \in G_2$. We can be sure such an inverse function exists because ϕ is one to one.

By the definition of an isomorphism, we know that $\phi(x * y) = \phi(x) \circ \phi(y)$. Applying ϕ^{-1} to both sides of the equation, we have $\phi^{-1}(\phi(x*y)) = \phi^{-1}(\phi(x) \circ \phi(y))$.

The right side of the equation is equivalent to $x*y$, which is in turn equivalent to $\phi^{-1}(\phi(x)) * \phi^{-1}(\phi(y))$. So we have

$$\phi^{-1}(\phi(x)) * \phi^{-1}(\phi(y)) = \phi^{-1}(\phi(x) \circ \phi(y)) \tag{2}$$

Equation (2) satisfies Definition 5.79 and so the function $\phi^{-1} : G_2 \to G_1$ is an isomorphism. □

Theorem 5.87

Suppose $\phi : G_1 \to G_2$ 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.

Proof. By the definition of an isomorphism we know that $\phi(a * b) = \phi(a) \odot \phi(b)$ and $\psi(g \odot h) = \psi(g) \star \psi(h)$ for all $a, b \in G_1$ and all $g, h \in G_2$. If we apply the function ψ to both sides of the first equation we have

$$\psi(\phi(a * b)) = \psi(\phi(a) \odot \phi(b))$$

and by the second equation, the right side can be re-written as follows.

$$\psi(\phi(a * b)) = \psi(\phi(a)) \star \psi(\phi(b))$$

And rewriting with function composition notation,

$$\psi \circ \phi(a * b) = \psi \circ \phi(a) \star \psi \circ \phi(b).$$

This fulfills Definition 5.79 and therefore the composite function $\psi \circ \phi$ is an isomorphism from G_1 to 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.

Proof. A binary relation is an equivalence relation if and only if it is reflexive ($a = a$), symmetric (if $a = b$ then $b = a$) and transitive (if $a = b$ and $b = c$ then $a = c$).

The relation of being isomorphic is reflexive because □