4 Proofs in group theory

After working through this section, you should be able to:

(a) understand that the identity in a group is unique;
(b) understand that each element in a group has a unique inverse;
(c) recognise how the uniqueness properties can be proved from the group axioms;
(d) explain the connections between properties of a group table and the group axioms.

The advantage of defining a group $(G, \circ)$ as a general set G, together with a binary operation $\circ$ satisfying the four axioms G1–G4, is that anything we can prove directly from the axioms (in the general case) must apply to any group (any specific case). Thus, by giving one proof, we can simultaneously establish a result that holds for groups of symmetries, modular arithmetic groups, infinite groups of real or complex numbers, and many more.

In this section we introduce some important properties, and show how these can be derived from the group axioms. However, we do not expect you to be able to produce or reproduce these proofs. On your first reading, concentrate on the group properties and examples, and leave detailed study of the proofs until later. When you are familiar with the basic ideas, you should concentrate on the uniqueness proofs in Subsection 4.1, which impart the 'flavour' of proofs in group theory. In general, such proofs are short and, in some senses, simple. However, a beginner in group theory is unlikely to think of them unaided. They involve writing down *what you know*, thinking about *what you want to prove* and trying to *bridge the gap* in an inspired way by using one or more of the group axioms (there are only four from which to choose).

4.1 Uniqueness properties

Uniqueness of the identity element

Axiom G2 states that, in every group $(G, \circ)$, there must be an identity element e such that, for all $g \in G$,

$$g \circ e = g = e \circ g.$$

Each of our examples of groups has contained precisely *one* identity element, and we shall prove now that this must always be the case. We say that the identity in a group is *unique*.

Property 4.1 In any group, the identity element is unique.

As a result of this property we can, and shall, refer to *the* identity element.

The proof of this result is short and not difficult—once you know what to do. We have set out the proof below, with comments to motivate the steps.

Comments	Proof
We use a standard method for proving uniqueness:	
we show that if e and e' are identity elements in G, then they must be equal.	Suppose that e and e' are identity elements in the group $(G, \circ)$.
	We want to show that $e = e'$ is the only possibility.
We write down what we know:	By axiom G2, we know that
e is an identity element	$g \circ e = g = e \circ g \quad$ for all $g \in G$, (4.1)
and	and
e' is an identity element.	$g \circ e' = g = e' \circ g \quad$ for all $g \in G$. (4.2)
We wish to relate e and e'.	
We use particular cases of the general equations (4.1) and (4.2). We put	Equations (4.1) and (4.2) hold for *all* $g \in G$; so, in particular,
$g = e'$ in equation (4.1)	$e' \circ e = e' = e \circ e'$ (4.3)
and	and
$g = e$ in equation (4.2).	$e \circ e' = e = e' \circ e$. (4.4)
We use equations (4.3) and (4.4) to simplify the element $e \circ e'$ in two different ways.	From the right-hand part of equation (4.3), $e' = e \circ e'$, and from the left-hand part of equation (4.4), $e \circ e' = e$.
We now have $e' = e \circ e' = e$, as required.	Thus $e = e'$, so $(G, \circ)$ has a unique identity element. ■

Uniqueness of the inverse element

Axiom G3 states that, for each element g in a group $(G, \circ)$, there must exist an inverse element $g^{-1} \in G$ such that

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

In each group that we have met so far, the inverse of each element is unique: no element has two distinct inverses.

Property 4.2 In any group, each element has a unique inverse.

As a result of this property we can, and shall, refer to *the* inverse of a particular group element.

Again the proof is short: we apply the axiom G4 (associativity) to a particular expression.

Comments	Proof
Again, we use the standard method for proving uniqueness:	
we show that if x and y are inverses of $g \in G$, then they must be equal.	Suppose that $g \in G$ has inverse elements—x and y.
	We want to show that $x = y$ is the only possibility.
	Let e be the identity element in G.
We write down what we know:	By axiom G3, we know that
x is an inverse of g	$g \circ x = e = x \circ g$ (4.5)
and	and
y is an inverse of g.	$g \circ y = e = y \circ g$. (4.6)

We wish to relate x and y.

We consider the element

$$y \circ g \circ x,$$

and simplify it in two different ways.

We have

$$y \circ g \circ x = y \circ (g \circ x),$$

which simplifies to y.

Also

$$y \circ g \circ x = (y \circ g) \circ x,$$

which simplifies to x.

Now we use associativity:

$$y \circ (g \circ x) = (y \circ g) \circ x,$$

which simplifies to $y = x$.

We now have

$$y = x,$$

as required.

Consider the element

$$y \circ g \circ x.$$

From the left-hand part of equation (4.5),

$$g \circ x = e,$$

so

$$\begin{aligned} y \circ (g \circ x) &= y \circ e \\ &= y, \end{aligned} \tag{4.7}$$

since e is the identity.

From the right-hand part of equation (4.6),

$$y \circ g = e,$$

so

$$\begin{aligned} (y \circ g) \circ x &= e \circ x \\ &= x, \end{aligned} \tag{4.8}$$

since e is the identity.

By axiom G4,

$$y \circ (g \circ x) = (y \circ g) \circ x.$$

By equation (4.7), the left-hand side is y.

By equation (4.8), the right-hand side is x.

Thus

$$y = x,$$

so g has a unique inverse in G. ■

4.2 Properties of inverses

Inverse of the inverse

In our work on groups we have found that some elements are self-inverse, and the remaining elements can be arranged in pairs of elements that are inverses of each other. In other words, if g^{-1} is the inverse of g, then g is the inverse of g^{-1}. We state this as Property 4.3.

Property 4.3 In any group $(G, \circ)$,

if $g \in G$ and g has inverse $g^{-1} \in G$, then g^{-1} has inverse g.

In symbols, we write

$$(g^{-1})^{-1} = g.$$

Proof Let $g \in G$ and let g^{-1} be the inverse of g. By axiom G3,

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

Altering the order of the expressions, we obtain

$$g^{-1} \circ g = e = g \circ g^{-1}.$$

This tells us that g is an inverse of g^{-1}. Hence, by Property 4.2 (uniqueness of the inverse), we have

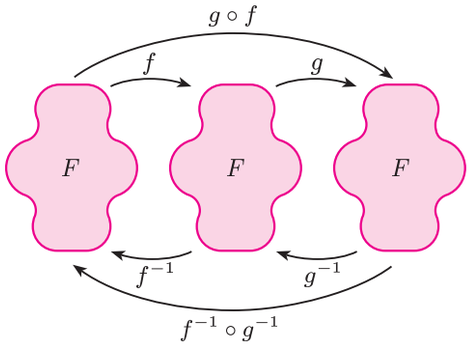
$$(g^{-1})^{-1} = g. \quad ■$$

Inverse of a composite

Our second property of inverses concerns the inverse of a composite.

If f and g are symmetries of a plane figure F, then the inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$.

This result is true of composites in general (whenever inverses exist).



To undo 'f then g', we first undo g, then undo f; that is, we do 'g^{-1} then f^{-1}'.

This result is true for all groups.

Property 4.4 In any group $(G, \circ)$, with $x, y \in G$,

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

The strategy of the proof is identical to that of the proof for Property 4.3. We show that $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$ and then use Property 4.2 (uniqueness of the inverse).

Proof Let $x, y \in G$. First, we compose $x \circ y$ with $y^{-1} \circ x^{-1}$ on the right:

$$\begin{aligned}(x \circ y) \circ (y^{-1} \circ x^{-1}) &= x \circ y \circ y^{-1} \circ x^{-1} \quad \text{(associativity)}\\ &= x \circ (y \circ y^{-1}) \circ x^{-1} \quad \text{(associativity)}\\ &= x \circ e \circ x^{-1} \quad \text{(inverses)}\\ &= x \circ x^{-1} \quad \text{(identity)}\\ &= e \quad \text{(inverses)}.\end{aligned}$$

Next we compose $x \circ y$ with $y^{-1} \circ x^{-1}$ on the left:

$$\begin{aligned}(y^{-1} \circ x^{-1}) \circ (x \circ y) &= y^{-1} \circ x^{-1} \circ x \circ y \quad \text{(associativity)}\\ &= y^{-1} \circ (x^{-1} \circ x) \circ y \quad \text{(associativity)}\\ &= y^{-1} \circ e \circ y \quad \text{(inverses)}\\ &= y^{-1} \circ y \quad \text{(identity)}\\ &= e \quad \text{(inverses)}.\end{aligned}$$

Hence $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$. So, by Property 4.2, it is *the* inverse of $x \circ y$; that is,

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}. \quad \blacksquare$$

4.3 Properties of group tables

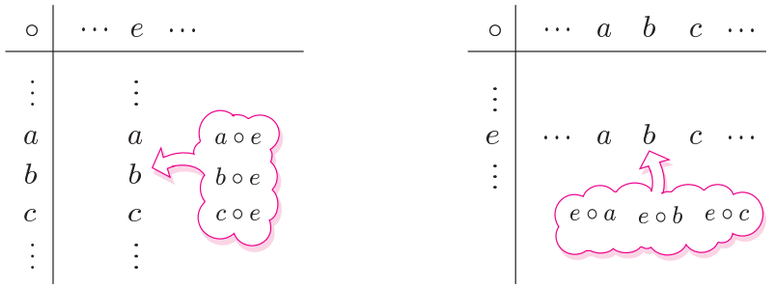
For a small group $(G, \circ)$, we may construct a Cayley table for the binary operation $\circ$. Often, when we know that $(G, \circ)$ is a group and we wish to stress this, we refer to the Cayley table as a *group table*. A group table has a number of properties that correspond directly to the group axioms, so when checking whether a given Cayley table describes a group, we can use these properties to check some of the group axioms. In this subsection we discuss some of the properties of group tables, starting with those linked to the group axioms.

G1 CLOSURE For all $g_1, g_2 \in G$,
$$g_1 \circ g_2 \in G.$$

This means simply that we can complete the body of the Cayley table using the elements of G: no new elements are required to complete the table; that is, no elements from outside G are required.

G2 IDENTITY There exists an identity element $e \in G$ such that, for all $g \in G$,
$$g \circ e = g = e \circ g.$$

The composites $g \circ e$, for all $g \in G$, form the column of the Cayley table labelled by e. Similarly, the composites $e \circ g$, for all $g \in G$, form the row of the Cayley table labelled by e. Hence, if a Cayley table is a group table, then the column and the row corresponding to e must repeat the borders of the table.



When we know which element is the identity, we normally write this label first.

Exercise 4.1 Decide which is the identity element in each of the following group tables.

(a)

	O	E
O	E	O
E	O	E

(b)

	D	I
D	D	I
I	I	D

(c)

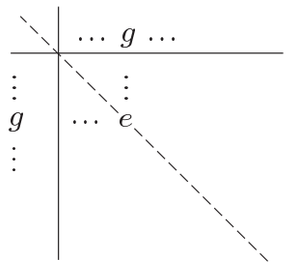
	u	v	w	x
u	w	x	u	v
v	x	w	v	u
w	u	v	w	x
x	v	u	x	w

G3 INVERSES For each $g \in G$, there exists an inverse element $g^{-1} \in G$ such that
$$g \circ g^{-1} = e = g^{-1} \circ g.$$

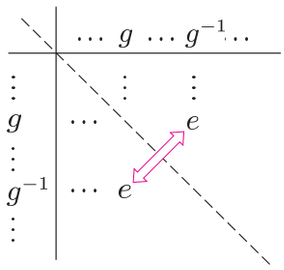
The fact that each element has a unique inverse means that

the identity e must occur exactly once in each row and each column.

However, there is a slightly stronger result. If an element g is self-inverse, then $g \circ g = e$ and so e must occur on the leading diagonal. If g is not self-inverse, then g and g^{-1} are distinct elements which are inverses of each other, so the entries in the Cayley table for $g \circ g^{-1} = e$ and $g^{-1} \circ g = e$ are placed symmetrically with respect to the leading diagonal. These observations are illustrated in the following diagram.



g is self-inverse



g is not self-inverse

Thus a group table has the following property.

Property 4.5 In any group table, the identity e must occur exactly once in each row and each column of the table, and e must occur in symmetrical positions with respect to the leading diagonal.

Exercise 4.2 Given that the following table is a group table, draw up a table of the inverses of the eight elements.

$\circ$	a	b	c	d	e	f	g	h
a	f	e	g	h	a	b	d	c
b	e	f	h	g	b	a	c	d
c	h	g	f	e	c	d	b	a
d	g	h	e	f	d	c	a	b
e	a	b	c	d	e	f	g	h
f	b	a	d	c	f	e	h	g
g	c	d	a	b	g	h	f	e
h	d	c	b	a	h	g	e	f

Exercise 4.3 In the Cayley table below, the identity element e occurs in each row and column, but the table is not a group table. Explain why not.

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	e	c	d	a
c	c	d	e	a	b
d	d	c	a	b	e

G4 ASSOCIATIVITY For all $g_1, g_2, g_3 \in G$,

$$g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3.$$

It is not easy to deduce anything about associativity simply from a Cayley table. (You have to do a lot of checking.) Unfortunately, it is possible for a Cayley table to show the features corresponding to axioms G1, G2 and G3 even when the operation $\circ$ is not associative. This is illustrated by the following table.

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

From this table we find that:

the set is closed under $\circ$,

e is an identity element,

each element is self-inverse.

However, $\circ$ is not associative, as we saw in Frame 15.

Another property of a group table that we mentioned in Frame 15 is the following.

Property 4.6 In a group table, each element of the group occurs exactly once in each row and exactly once in each column.

We prove this statement for rows.

The proof for columns is similar.

Proof We prove that any given element, g say, appears exactly once in any given row—the row labelled h, say. This is equivalent to proving that there is a *unique* element of the group, x say, such that

$$h \circ x = g. \tag{4.9}$$

This equation can be 'solved' for the unknown element x by applying the inverse h^{-1} on the left:

$$h^{-1} \circ (h \circ x) = h^{-1} \circ g.$$

Hence

$$(h^{-1} \circ h) \circ x = h^{-1} \circ g \quad \text{(associativity)},$$

so

$$e \circ x = h^{-1} \circ g \quad \text{(inverses)},$$

giving

$$x = h^{-1} \circ g \quad \text{(identity)}.$$

Thus the only possible solution to equation (4.9) is $x = h^{-1} \circ g$, and this is indeed a solution, since

$$h \circ (h^{-1} \circ g) = (h \circ h^{-1}) \circ g = e \circ g = g.$$

By the inverse and closure axioms, $h^{-1} \circ g$ is an element of G.

Thus, in the row labelled h, the element g appears once, in the column labelled by the element $h^{-1} \circ g$. ■

The following Cancellation Laws are also proved using the inverse.

Property 4.7 Cancellation Laws

In any group $(G, \circ)$ with elements a, b and x:

if $x \circ a = x \circ b$, then $a = b$,

if $a \circ x = b \circ x$, then $a = b$.

Exercise 4.4 Prove the Cancellation Laws for a group $(G, \circ)$, namely:

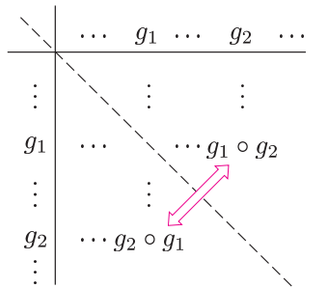
(a) if $x \circ a = x \circ b$, then $a = b$;

(b) if $a \circ x = b \circ x$, then $a = b$.

The last property of group tables that we shall note concerns commutativity.

For any elements g_1 and g_2 of a group G, the entries corresponding to the composites $g_1 \circ g_2$ and $g_2 \circ g_1$ are symmetrically placed with respect to the leading diagonal of the group table (because the order of elements across the top and down the side is the same).

Thus, for an Abelian group, symmetrically-placed entries must be the same.



Property 4.8 For an Abelian group, the group table is symmetrical about the leading diagonal.

The following group tables show that $(\mathbb{Z}_6, +_6)$ is an Abelian group, whereas $(S(\triangle), \circ)$ is not.

$(\mathbb{Z}_6, +_6)$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

symmetrical

$(S(\triangle), \circ)$

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

not symmetrical

For example, in $S(\triangle)$,
$a \circ r = t$ and $r \circ a = s$.

Exercise 4.5 Each of the following tables is a group table for a group of order 8 with identity e. In each case, draw up a table of inverses and state whether the group is Abelian.

(a)

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

(b)

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	b	a	e	c
f	f	d	h	g	c	b	a	e
g	g	f	d	h	e	c	b	a
h	h	g	f	d	a	e	c	b

Further exercises

Exercise 4.6 Given that the following tables are group tables, fill in the missing elements.

(a)

	e	a	b
e	e	a	b
a	a		
b	b		

(b)

	a	b	c	d
a	a	b	c	
b	b			a
c		d		
d	d			c

Exercise 4.7 The following table is a group table.

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	g	d	h	f
b	b	c	e	a	h	g	f	d
c	c	e	a	b	f	h	d	g
d	d	f	h	g	b	c	a	e
f	f	h	g	d	a	b	e	c
g	g	d	f	h	c	e	b	a
h	h	g	d	f	e	a	c	b

(a) Which element is the identity element?

(b) Write down the inverse of each of the elements $e, a, \ldots, h$.

(c) Is this group Abelian?

Exercise 4.8 Explain why each of the following Cayley tables is not a group table.

(a)

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	d	e
b	b	d	a	b
c	c	e	b	a

(b)

$\circ$	e	a	b	c
e	b	e	a	b
a	e	a	b	c
b	c	b	c	a
c	a	c	b	e

(c)

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	e	c	d	a
c	c	d	e	a	b
d	d	c	a	b	e

(d)

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	b	c	d
b	b	d	a	e	f	c
c	c	f	e	d	b	a
d	d	b	c	f	a	e
f	f	c	d	a	e	b

Exercise 4.9 Show that if $(G, \circ)$ is a group with an even number of elements, then there is an element $g \in G$ such that

$$g \circ g = e \quad \text{and} \quad g \neq e.$$