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

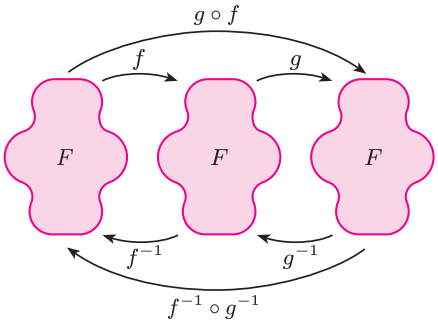
$$(g^{-1})^{-1} = g. \quad ■$$

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.