M303

Further pure mathematics

Group theory

This publication forms part of an Open University module. Details of this and other Open University modules can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)845 300 6090; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

Note to reader
Mathematical/statistical content at the Open University is usually provided to students in printed books, with PDFs of the same online. This format ensures that mathematical notation is presented accurately and clearly. The PDF of this extract thus shows the content exactly as it would be seen by an Open University student. Please note that the PDF may contain references to other parts of the module and/or to software or audio-visual components of the module. Regrettably mathematical and statistical content in PDF files is unlikely to be accessible using a screenreader, and some OpenLearn units may have PDF files that are not searchable. You may need additional help to read these documents.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2014. Second edition 2016.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed in the United Kingdom by Halstan & Co. Ltd, Amersham, Bucks.

ISBN 978 1 4730 2036 8

2.1

Contents

1 Direct products **5**
1.1 The external direct product of two groups 5
1.2 Internal direct products 8

2 Cyclic groups **18**
2.1 The classification of cyclic groups 19
2.2 Subgroups and quotient groups of cyclic groups 20
2.3 Direct products of cyclic groups 24

3 Describing groups **32**
3.1 Generators and relations 32
3.2 Dicyclic groups 38

Solutions and comments on exercises **42**

Index **54**

1 Direct products

This section describes how to construct a group called the *direct product* of two given groups, and then describes certain conditions under which a group can be regarded as the direct product of its subgroups.

1.1 The external direct product of two groups

In this subsection, we introduce a method of constructing a new group from two existing ones: their *external direct product*. This method of construction will enable us to use existing groups as building blocks for larger ones. In turn, this will enable us to describe some groups in terms of smaller and possibly less complicated groups. This construction is, therefore, a key tool in our progress towards classifying groups.

First we need the notion of the **Cartesian product** of two sets: if X and Y are two sets, then the Cartesian product $X \times Y$ is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. For example, if $X = \{1, 2, 3\}$ and $Y = \{a, b\}$ then

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

When $X = Y$, the Cartesian product $X \times Y = X \times X$ is also denoted by X^2. More generally, the Cartesian product of n sets $X_1, X_2, \ldots, X_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in X_i$ for all $i = 1, \ldots, n$.

In order to define the direct product of two groups, we need to specify the underlying set and a suitable binary operation. To understand how this is done, it will be useful to examine the familiar example of addition of vectors in the real plane $\mathbb{R} \times \mathbb{R}$ represented by the usual coordinate system.

Example 1.1 *Addition of vectors in $\mathbb{R} \times \mathbb{R}$*

We know that the real numbers with addition are a group, which we denoted by $(\mathbb{R}, +)$ in Chapter 5.

Each point in the plane is represented by an ordered pair (x, y) of real numbers. In other words, the coordinates of points in the plane are elements of the Cartesian product

$$\mathbb{R} \times \mathbb{R} = \{(x, y) : \ x \in \mathbb{R}, \ y \in \mathbb{R}\}.$$

The familiar operation of vector addition on $\mathbb{R} \times \mathbb{R}$ is defined as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Thus, vector addition is defined component by component in terms of addition in $\mathbb{R}$.

It turns out that $\mathbb{R} \times \mathbb{R}$ with addition defined as in Example 1.1 above is a group.

Exercise 1.1

Prove that the set $\mathbb{R} \times \mathbb{R}$ with the operation of vector addition is a group.

We can generalise the definitions of both the real plane as a Cartesian product and component-wise addition of real numbers.

In Example 1.1, $G = H = \mathbb{R}$.

Given two groups $(G, \circ)$ and $(H, *)$, we define the underlying set of a new group to be the Cartesian product of the sets G and H; that is, the set

$$G \times H = \{(g, h) : \; g \in G, \; h \in H\}.$$

In Example 1.1, $\bullet = \circ = * = +$.

As with $\mathbb{R} \times \mathbb{R}$, we can define an operation on this set by applying the original operations to the separate components. Generalising requires a little care because the operations for the two component groups may be different. As the first components come from G, with operation $\circ$, and the second components come from H, with operation $*$, the general definition of the new operation (which we call $\bullet$) is

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

Definition 1.2 *Direct product of two groups*

Let $(G, \circ)$ and $(H, *)$ be two groups. Their **direct product** $(G \times H, \bullet)$ is the group defined as follows.

Set The underlying set of the group is $G \times H$, the Cartesian product of the underlying sets G and H; that is,

$$G \times H = \{(g, h) : \; g \in G, \; h \in H\}.$$

Operation If (g_1, h_1) and (g_2, h_2) are elements of $G \times H$ then

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

This definition does indeed produce a group. Before we prove this, the following exercise will give you some ‘hands-on’ experience of direct products of groups.

Exercise 1.2

Write out the Cayley table of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. Use $+$ for the new operation.

We are now ready to prove that the direct product of any two groups is indeed a group. The proof for the general case is similar to the solution to Exercise 1.1.

To verify that $(G \times H, \bullet)$ is a group, we must check the four group axioms.

To check that the above definition of $\bullet$ produces a closed binary operation on $G \times H$ (that is, it satisfies the closure axiom), we observe the following.

Let (g_1, h_1) and (g_2, h_2) be any two elements of $G \times H$. By the definition of $G \times H$, we know that g_1 and g_2 are elements of G and that h_1 and h_2 are elements of H.

Since G is a group, it is closed under the operation $\circ$, therefore $g_1 \circ g_2$ is in G. Since H is a group, it is closed under the operation $*$, so $h_1 * h_2$ is in H. Therefore, by the definition of $\bullet$, we have

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \in G \times H.$$

The following exercise asks you to check the remaining group axioms for $(G \times H, \bullet)$.

Exercise 1.3

(a) Prove that $\bullet$ is associative (that is, check the associativity axiom).

(b) Let the identity of G be e_G and the identity of H be e_H. Prove that (e_G, e_H) is the identity of $G \times H$ (that is, check the identity axiom).

(c) Let (g, h) be an element of $G \times H$, where g has inverse g^{-1} in G and h has inverse h^{-1} in H. Prove that (g^{-1}, h^{-1}) is the inverse of (g, h) in $G \times H$ (that is, check the inverses axiom).

So far we have carefully distinguished the binary operations of the groups involved in the direct product construction. Now that we have shown that the direct product of two groups is a group, we revert to using either juxtaposition for the operations, or $+$ when both the operations are addition. Some texts refer to the **direct sum** of two groups, rather than direct product, when the groups are abelian and additive notation is used.

Exercise 1.4

Let G and H be abelian groups. Show that their direct product $G \times H$ is abelian.

1.2 Internal direct products

In some cases, a group is isomorphic to the direct product of two more of its subgroups. This is not always obvious, and in this subsection we investigate how to find out whether this is the case.

Consider the group of symmetries of the rectangle, $V = \{e, r, h, v\}$, where r is the half-turn about the centre and h and v are the reflections in the horizontal and vertical axes of symmetry. Recall also that $v = rh$. The Cayley table of V is as follows.

	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

We will show how V can be represented as a direct product of two smaller groups. More specifically, we will show that V is isomorphic to the direct product of two of its subgroups.

By Lagrange's Theorem the only possible orders for subgroups of V are 1, 2 and 4. We aim to express V in the form $V = A \times B$, where A and B are subgroups of V. Now, by the definition of direct products of *any* two groups A and B,

$$|A \times B| = |A||B|.$$

Therefore if either A or B has order 1, then the other must have order 4 and is the whole group. However, this would not be expressing V as a product of smaller groups. Thus, it only makes sense to try to express V as the direct product of two subgroups of order 2. There are three subgroups of order 2, namely

$$H_1 = \{e, r\}, \quad H_2 = \{e, h\} \text{ and } H_3 = \{e, v\}.$$

We pick H_1 and H_2, although any two of the three subgroups would do just as well. The Cayley table for $H_1 \times H_2$ is as follows.

	(e,e)	(r,e)	(e,h)	(r,h)
(e,e)	(e,e)	(r,e)	(e,h)	(r,h)
(r,e)	(r,e)	(e,e)	(r,h)	(e,h)
(e,h)	(e,h)	(r,h)	(e,e)	(r,e)
(r,h)	(r,h)	(e,h)	(r,e)	(e,e)

Since $rh = v$ in V, the Cayley table for V can be rewritten in the following way.

	e	r	h	rh
e	e	r	h	rh
r	r	e	rh	h
h	h	rh	e	r
rh	rh	h	r	e

You may have observed that these two tables have an entirely similar pattern. It follows that the function $\phi : H_1 \times H_2$ defined by

$$\phi : (x, y) \mapsto xy$$

is an isomorphism. Thus V can be represented as – that is, it is isomorphic to – the direct product of two of its subgroups. Since each of these subgroups is cyclic and of order 2, we can also say $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Not all attempts to decompose a group as a direct product of subgroups will work, as the following example shows.

Example 1.3 *A group that is not a non-trivial direct product*

The symmetric group S_3 has six elements:

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

This group is not abelian: consider, for example, the products $(1\,2)(1\,3)$ and $(1\,3)(1\,2)$.

If S_3 could be written as a *non-trivial* direct product – that is, as a direct product in which neither subgroup has order 1 – it would have to be as the direct product of subgroups of orders 2 and 3.

The group S_3 does possess subgroups of orders 2 and 3. For example, $H_1 = \{e, (1\,2)\}$ has order 2 and $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ has order 3.

However, any subgroup of order 2 is cyclic and is isomorphic to $\mathbb{Z}_2$. Equally, any subgroup of order 3 is cyclic and is isomorphic to $\mathbb{Z}_3$. It follows, therefore, that *any* attempt to form a direct product of such subgroups leads to a group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is abelian by Exercise 1.4 and so not isomorphic to S_3.

Example 1.3 shows that, even if subgroups of suitable orders exist, a group may not be isomorphic to a direct product of these subgroups.

In fact, there are precise conditions under which a group is isomorphic to a direct product of two of its subgroups. These conditions form the content of Theorem 1.5 below.

We determine these conditions in two stages: first we establish necessary conditions on the subgroups and then we show that these conditions are also sufficient.

We start by showing that if a group G is the direct product of two of its subgroups, then there are certain restrictions on the subgroups.

This discussion will be the proof of the first half of Theorem 1.5.

So assume that H_1 and H_2 are subgroups of a group G and that $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism. We consider, in turn, the consequences of ϕ being onto, one–one and satisfying the morphism property.

The image set of ϕ consists of all products $h_1 h_2$ of an element of H_1 and an element of H_2. Hence, as ϕ is onto, every element of G is expressible in this form. Using the notation $H_1H_2 = \{h_1h_2 : \ h_1 \in H_1, \ h_2 \in H_2\}$, this says that we must have $G = H_1H_2$. In other words, every element of G is the product of an element of H_1 with an element of H_2. Summing up, we have the following result.

If ϕ is an isomorphism, then $G = H_1H_2$.

Strictly, the correct notation for expressions like $\phi(h_1, h_2)$ is $\phi((h_1, h_2))$. However, for ease of notation we will avoid double brackets where no ambiguity arises and simply write $\phi(h_1, h_2)$.

Let us now look at the consequences of ϕ being one–one. Assume that $\phi(h_1, h_2) = \phi(k_1, k_2)$. Then we know that

$$(h_1, h_2) = (k_1, k_2),$$

which, by the definition of an ordered pair, implies that $h_1 = k_1$ and $h_2 = k_2$.

So $\phi(h_1, h_2) = \phi(k_1, k_2)$ means that $h_1h_2 = k_1k_2$. In other words, the fact that ϕ is one–one means that

$$h_1h_2 = k_1k_2 \quad \text{implies} \quad h_1 = k_1 \text{ and } h_2 = k_2.$$

Thus, because ϕ is one–one, each element of G can be expressed as a *unique* product of the form h_1h_2 with $h_1 \in H_1$ and $h_2 \in H_2$.

Exercise 1.5

Show that the fact that ϕ is one–one implies that $H_1 \cap H_2 = \{e\}$.

Hint: use the fact that $h = he = eh$ for any $h \in G$.

The result of the previous exercise tells us the following.

If ϕ is an isomorphism, then $H_1 \cap H_2 = \{e\}$.

For any two elements (h_1, h_2) and (k_1, k_2) of the direct product, the morphism property of ϕ gives

$$\begin{aligned}
&\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2) \\
&\ \Rightarrow \phi(h_1k_1, h_2k_2) = (h_1h_2)(k_1k_2) \\
&\ \Rightarrow h_1k_1h_2k_2 = h_1h_2k_1k_2 \\
&\ \Rightarrow k_1h_2 = h_2k_1, \qquad \text{using the left and right cancellation rules.}
\end{aligned}$$

What this means is that every element of H_1 commutes with every element of H_2.

We now show that we can deduce that H_1 is a normal subgroup of G. To do so, we show that $aH_1a^{-1} \subseteq H_1$ for each $a \in G$.

So suppose that $a \in G$. Since we now know that $G = H_1H_2$, we can write $a = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Now, any element of aH_1a^{-1} is of the form aha^{-1}, where $h \in H_1$. So

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1hh_2h_2^{-1}h_1^{-1} \qquad \text{(since } h \in H_1 \text{ and } h_2 \in H_2 \text{ commute)} \\ &= h_1hh_1^{-1} \in H_1 \qquad \text{(since } h, h_1, h_1^{-1} \in H_1\text{).} \end{aligned}$$

Thus $aH_1a^{-1} \subseteq H_1$ as required.

The following exercise asks you to show that H_2 is also a normal subgroup of G.

Exercise 1.6

Prove that, for any $a \in G$,

$$aH_2a^{-1} \subseteq H_2.$$

Exercise 1.6 and the discussion preceding it give the following result.

If ϕ is an isomorphism, then both H_1 and H_2 are normal subgroups of G.

Summing up, if $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1h_2$$

is an isomorphism, then all three of the following conditions are satisfied:

(a) $G = H_1H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

This completes the proof of the first half of Theorem 1.5 below. Before we state the theorem and complete its proof, we introduce the standard terminology that is used when a group can be expressed as a direct product of subgroups.

Definition 1.4 *Internal direct product*

Let G be a group and let H_1 and H_2 be subgroups of G. Then G is the **internal direct product** of H_1 and H_2 if the map

$$\begin{aligned} \phi : H_1 \times H_2 &\to G \\ \phi : (h_1, h_2) &\mapsto h_1h_2 \end{aligned}$$

is an isomorphism.

The direct product $H_1 \times H_2$ in Definition 1.4 is 'internal' in that H_1 and H_2 are subgroups of G. The next theorem gives necessary and sufficient conditions for a group to be the internal direct product of two given subgroups.

Theorem 1.5 *Internal Direct Product Theorem*

If H_1 and H_2 are subgroups of a group G, then

$$\begin{aligned} \phi &: H_1 \times H_2 \to G \\ \phi &: (h_1, h_2) \mapsto h_1 h_2 \end{aligned}$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of H_1 and H_2.

Proof As remarked above, we have proved that the conditions are necessary; that is, we have proved that if ϕ is an isomorphism, then the three conditions hold. For sufficiency, we need to prove that, if the three conditions hold, then ϕ is an isomorphism.

The three conditions, in turn, give that ϕ is onto, one–one and has the morphism property.

To see that ϕ is onto, recall that $G = H_1 H_2$. Then every $g \in G$ can be written as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$. Hence $g = \phi(h_1, h_2)$ and ϕ is onto.

We now check that ϕ is one–one. Suppose that

$$\phi(h_1, h_2) = \phi(k_1, k_2).$$

Then $h_1 h_2 = k_1 k_2$ for $h_1, k_1 \in H_1$ and $h_2, k_2 \in H_2$. So

$$k_1^{-1} h_1 = k_2 h_2^{-1}.$$

But the left-hand side is an element of H_1 and the right-hand side is an element of H_2. Since both sides are equal, they belong to both H_1 and H_2 and, hence, to the intersection $H_1 \cap H_2$.

However, $H_1 \cap H_2 = \{e\}$.

Thus $k_1^{-1} h_1 = k_2 h_2^{-1} = e$.

It follows that $h_1 = k_1$ and $h_2 = k_2$, and so $(h_1, h_2) = (k_1, k_2)$. Thus ϕ is one–one.

Checking the morphism property is slightly more involved. Let (h_1, h_2) and (k_1, k_2) be elements of $H_1 \times H_2$. We want to show that

$$\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2).$$

But $\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1 k_1, h_2 k_2) = h_1 k_1 h_2 k_2,$ and
$\phi(h_1, h_2)\phi(k_1, k_2) = h_1 h_2 k_1 k_2,$

so the morphism property in this case is equivalent to

$$h_1k_1h_2k_2 = h_1h_2k_1k_2;$$

that is, after using the cancellation laws, to

$$k_1h_2 = h_2k_1.$$

Now consider the product

$$k_1h_2k_1^{-1}h_2^{-1} \in G.$$

Since h_2 is in H_2, so is h_2^{-1}. Since H_2 is normal in G, we have that $k_1h_2k_1^{-1}$ is in H_2. Therefore $k_1h_2k_1^{-1}h_2^{-1}$ is in H_2.

Similarly, $h_2k_1^{-1}h_2^{-1} \in H_1$, so $k_1h_2k_1^{-1}h_2^{-1} \in H_1$.

Therefore $k_1h_2k_1^{-1}h_2^{-1} \in H_1 \cap H_2$. But since $H_1 \cap H_2 = \{e\}$, we have

$$k_1h_2k_1^{-1}h_2^{-1} = e,$$

which is equivalent to $k_1h_2 = h_2k_1$, and therefore also to the morphism property.

This concludes the proof that if conditions (a), (b) and (c) hold, then ϕ is an isomorphism. ■

Theorem 1.5 gives another reason why S_3 is not the direct product of two subgroups isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$: while $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ is a normal subgroup of order 3, we know that S_3 has no normal subgroup of order 2.

Exercise 1.7

Consider the cyclic group $\mathbb{Z}_6$ and denote its underlying set by $\{e, a, a^2, a^3, a^4, a^5\}$. Show that $\mathbb{Z}_6$ has normal subgroups of orders 2 and 3 that satisfy the conditions of Theorem 1.5. Deduce that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

The result you are asked to prove in the following exercise is implicit in the proof of the morphism property for ϕ in Theorem 1.5: in any internal direct product $G \cong H \times K$, the subgroups H and K satisfy a commutativity condition, in the sense that every element of H commutes with every element of K.

Exercise 1.8

Let $G \cong H \times K$ be the internal direct product of subgroups H and K of G. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

Let G and H be two groups with identities e_G and e_H respectively. Then the set

$$\widehat{G} = \{(g, e_H) : g \in G\}$$

is the subset of the direct product $G \times H$ that contains all pairs where the second element is the identity in H. It is not difficult to show – though we will not do so here – that $\widehat{G}$ is a subgroup of $G \times H$ that is isomorphic to G. Similarly, the set

$$\widehat{H} = \{(e_G, h) : h \in H\}$$

forms a subgroup of $G \times H$ that is isomorphic to H.

Then the direct product $G \times H$ is also the internal direct product of its subgroups $\widehat{G}$ and $\widehat{H}$. Thus, the distinction between the external and internal direct products of two groups is simply an indication of whether we regard the factor groups as subgroups of the product group. In the rest of Book B we will usually drop this distinction and simply refer to a *direct product* even when we work with an internal direct product.

Before we move on, it will be useful to consider direct products of more than two groups.

Theorem 1.6

If A, B and C are groups, then:

(a) $A \times B \cong B \times A$

(b) $A \times (B \times C) \cong (A \times B) \times C$.

Proof

(a) Consider the function $\phi : A \times B \to B \times A$ defined by

$$\phi : (a, b) \mapsto (b, a).$$

We claim that ϕ is an isomorphism.

To show that ϕ is one–one, suppose that $\phi(a_1, b_1) = \phi(a_2, b_2)$. Then $(b_1, a_1) = (b_2, a_2)$ by the definition of ϕ. Hence $b_1 = b_2$ and $a_1 = a_2$ by the definition of ordered pairs, and so

$$(a_1, b_1) = (a_2, b_2),$$

which shows that ϕ is one–one.

If (b, a) is any element of the codomain $B \times A$, then $b \in B$ and $a \in A$, so $(a, b) \in A \times B$ and $\phi(a, b) = (b, a)$. Hence ϕ is onto.

To check the morphism property, let (a_1, b_1) and (a_2, b_2) be any two elements of $A \times B$. Then

$$\begin{aligned} \phi((a_1, b_1)(a_2, b_2)) &= \phi(a_1a_2, b_1b_2) \\ &= (b_1b_2, a_1a_2) \\ &= (b_1, a_1)(b_2, a_2) \\ &= \phi(a_1, b_1)\phi(a_2, b_2). \end{aligned}$$

This completes the proof that $A \times B \cong B \times A$.

(b) You are asked to prove the second part of the theorem in the following exercise. ■

Exercise 1.9

Show that the function

$$\begin{aligned} \psi : A \times (B \times C) &\to (A \times B) \times C \\ \psi : (a, (b, c)) &\mapsto ((a, b), c) \end{aligned}$$

is an isomorphism.

The first part of Theorem 1.6 says that if we alter the order of the factor groups in a direct product, we obtain an isomorphic group.

The second part of Theorem 1.6 says that the bracketing of terms in a direct product of three (or more) groups is unnecessary.

So, just as for, say, the multiplication of integers, these 'commutative' and 'associative' laws mean that a direct product of two or more groups may be written in any order, without the need for brackets, since all such expressions produce isomorphic groups. Theorems 1.5 and 1.6 give us the following result concerning the direct product of a finite number of subgroups of a group G. The full proof is omitted.

Corollary 1.7

If H_i are subgroups of a group G for $i = 1, \ldots, n \in \mathbb{N}$, $n \geq 2$, then

$$\begin{aligned} \phi\colon H_1 \times H_2 \times \cdots \times H_n &\to G \\ \phi : (h_1, h_2, \ldots, h_n) &\mapsto h_1 h_2 \cdots h_n \end{aligned}$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2 \cdots H_n$

(b) $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$ for $1 \leq i \leq n$

(c) $H_1, H_2, \ldots, H_n$ are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of $H_1, H_2, \ldots, H_n$.

Notice that condition (b) is stronger than requiring that $H_i \cap H_j = \{e\}$ for $i \neq j$. The next example shows that this extra strength is needed.

Example 1.8 *The Klein group*

Let G be the Klein group,

$$G = \Gamma(\text{▭}) = \{e, r, h, v\}.$$

Let $H_1 = \{e, r\}, H_2 = \{e, h\}$ and $H_3 = \{e, v\}$. Then:

- $e = eee$, $r = ree$, $h = ehe$ and $v = eev$ and so condition (a) from Corollary 1.7 holds
- $H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3 = \{e\}$
- since G is abelian, H_1, H_2, H_3 are all normal in G.

However $G \ncong H_1 \times H_2 \times H_3$, since the order of G is 4, whereas the order of $H_1 \times H_2 \times H_3$ is 8.

Note that condition (b) in Corollary 1.7 does not hold here, since

$$H_1 \cap H_2H_3 = H_1 \cap \{e, h, v, r\} = \{e, r\}.$$

Recall that $HK = \{hk : h \in H \text{ and } k \in K\}$.

When a group G has two subgroups H and K with trivial intersection, we can say quite a lot about the product HK and its relation to the direct product $H \times K$.

Proposition 1.9

Let G be a group with subgroups H and K such that $H \cap K = \{e\}$. Then:

(a) If H and K have finite orders r and s respectively, then HK has rs distinct elements. In particular, if $rs = |G|$ then $G = HK$.

(b) If $kh = hk$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G with $HK \cong H \times K$.

Proof

(a) Suppose that $h_1k_1 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$h_2^{-1}h_1 = k_2k_1^{-1} = e$$

since $H \cap K = \{e\}$. Thus $h_2 = h_1$ and $k_2 = k_1$. This means that HK must have $|H| \times |K| = rs$ distinct elements.

(b) We first apply the subgroup criterion in Chapter 5 to show that HK is a subgroup of G. It is clear that HK is non-empty, so we only need to check that for any elements x, $y \in HK$ the product $x^{-1}y$ is again in HK.

Suppose $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} x^{-1}y &= (h_1k_1)^{-1}h_2k_2 \\ &= k_1^{-1}h_1^{-1}h_2k_2 \\ &= h_1^{-1}h_2k_1^{-1}k_2, \end{aligned}$$

since elements of H commute with elements of K.

But $h_1^{-1}h_2 \in H$ and $k_1^{-1}k_2 \in K$ (because H and K are both subgroups), therefore the product $h_1^{-1}h_2k_1^{-1}k_2 = x^{-1}y$ is in HK, as required.

Thus HK is a subgroup of G.

Now, since $hk = kh$ for all $h \in H$ and $k \in K$, we have

$$\begin{aligned} &hkh^{-1} = k \in K \text{ and} \\ &khk^{-1} = h \in H, \end{aligned}$$

so H and K are both normal subgroups of HK.

Hence, since $H \cap K = \{e\}$, we can apply Theorem 1.5 with $HK = G$ to show that $HK \cong H \times K$ as required. ■

The next exercise gives a useful tip for working with direct products of two groups inside abelian groups.

Exercise 1.10

Let G be an abelian group, and let H_1, H_2 be subgroups of G with

$$H_1 \cap H_2 = \{1\}.$$

Show that if $h_1 \in H_1$ and $h_2 \in H_2$ are such that $h_1h_2 = 1$, then $h_1 = 1$ and $h_2 = 1$.

Finally, we include a result about direct products of direct products.

Proposition 1.10

Let H, K be subgroups of G, and H_1, H_2 be subgroups of H. Suppose that $G \cong H \times K$ and $H \cong H_1 \times H_2$. Then $G \cong H_1 \times H_2 \times K$.

Proof We show that the three conditions in Corollary 1.7 hold for G, H_1, H_2 and K.

(a) Since $G \cong H \times K$, we have that $G = HK$ and since $H \cong H_1 \times H_2$, we have that $H = H_1H_2$. It follows that $G = H_1H_2K$.

(b) Since $G \cong H \times K$, we have that $H \cap K = \{e\}$ and so $H_1H_2 \cap K = \{e\}$.

Since $H \cong H_1 \times H_2$, we have $H_1 \cap H_2 = \{e\}$. Suppose $g \in H_1K \cap H_2$. Then

$$g = h_1 k = h_2 \qquad (*)$$

for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$.

But then $k = h_1^{-1}h_2 \in H$ and so $k \in H \cap K$. Thus $k = e$, and $h_1 = h_2$. But $h_1 = h_2$ implies that $h_1 = h_2 = e$ because $H_1 \cap H_2 = \{e\}$. Then equation $(*)$ implies $g = e$, and so

$$H_1K \cap H_2 = \{e\}.$$

The proof that $H_2K \cap H_1 = \{e\}$ is similar.

(c) Since $G \cong H \times K$, by Theorem 1.5 we have that K is normal in G. From Exercise 1.8 we know that:

- $hk = kh$ for all $h \in H$ and $k \in K$
- $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

Now let $h \in H_1$ and $g \in G$. We can write $g = h_1h_2k$ for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$. Then

$$\begin{aligned} ghg^{-1} &= h_1h_2khk^{-1}h_2^{-1}h_1^{-1} \\ &= h_1h_2h_2^{-1}kk^{-1}hh_1^{-1} \\ &= h_1hh_1^{-1} \in H_1. \end{aligned}$$

Thus H_1 is normal in G. Similarly, H_2 is normal in G.

We have shown that the three conditions in Corollary 1.7 are satisfied and hence that $G \cong H_1 \times H_2 \times K$. ■

2 Cyclic groups

We defined cyclic groups in Chapter 5. This section describes the key properties of their structure, starting with a complete description of all cyclic groups.

We will often retain multiplicative notation despite the fact that we know that cyclic groups are abelian.

2.1 The classification of cyclic groups

We are already in a position to describe fully all cyclic groups up to isomorphism. We do so by showing that any cyclic group is isomorphic to one of a list of concrete examples of groups. In fact, the concrete examples are

$$(\mathbb{Z}, +) \quad \text{and} \quad (\mathbb{Z}_n, +_n)$$

for each positive integer n.

The cyclic group with which you are most familiar is $(\mathbb{Z}, +)$, which is generated by the element 1.

$\mathbb{Z}$ is also generated by -1.

Theorem 2.1

(a) All infinite cyclic groups are isomorphic to $(\mathbb{Z}, +)$.

(b) A finite cyclic group of order n is isomorphic to the quotient group $\mathbb{Z}/n\mathbb{Z}$, which is $(\mathbb{Z}_n, +_n)$.

Proof

(a) Let G be an infinite cyclic group. Then G has a generator, a say, so every element of G can be written as a^n for some $n \in \mathbb{Z}$.
Define the function $\phi : G \to \mathbb{Z}$ by

$$a^n \mapsto n.$$

We claim that ϕ is an isomorphism. Since $a^n = a^m \Rightarrow n = m$, we have that ϕ is well defined. For any $m \in \mathbb{Z}$, $\phi(a^m) = m$, so ϕ is onto.

Since $\phi(a^n) = \phi(a^m) \Rightarrow n = m$, we have that

$$\phi(a^n) = \phi(a^m) \Rightarrow a^n = a^m,$$

so ϕ is one–one.

Finally, we check the morphism property, that is, we check that $\phi(a^n) + \phi(a^m) = \phi(a^n a^m)$. The key to this is that we have been using standard power notation when considering elements of groups; that is, we write

$$\underbrace{aa\cdots a}_{n \text{ times}} \text{ as } a^n, \quad \text{and} \quad \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}} \text{ as } a^{-n}.$$

Thus, the familiar power laws apply to products of elements of G, and we get

$$\phi(a^n) + \phi(a^m) = n + m = \phi(a^{n+m}) = \phi(a^n a^m).$$

Therefore the morphism property holds.

(b) Let G be a finite cyclic group of order n. Then G has a generator, a say, so every element of G can be written as a^s for some $s \in \mathbb{Z}$ and, moreover, $a^n = e$.

Now, by the Division Algorithm (see Book A, Chapter 1, Theorem 4.1) we have that $s = kn + r$ where $0 \leq r < n$. Thus

$$a^s = a^{kn+r} = (a^n)^k a^r = a^r.$$

Hence $G = \{e, a, a^2, \dots, a^{n-1}\}$, and these elements are distinct.

Define the function $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ by

$$a^r \mapsto r + n\mathbb{Z}.$$

We show that ϕ is an isomorphism. It is clear that ϕ is onto. To show that ϕ is one–one, we need to check that $\phi(a^r) = \phi(a^s) \Rightarrow a^r = a^s$. Now

$$\begin{aligned}\phi(a^r) = \phi(a^s) &\Rightarrow r + n\mathbb{Z} = s + n\mathbb{Z}\\ &\Rightarrow r - s = kn \text{ for some } k \in \mathbb{Z}\\ &\Rightarrow r = s + kn\\ &\Rightarrow a^r = a^{s+kn} = a^s a^{kn} = a^s \ \ (\text{since } a^n = e),\end{aligned}$$

as required.

Finally, we need to show the morphism property. Suppose that $r, s \in \mathbb{Z}$. Let $t \in \mathbb{Z}$ be such that $0 \leq t < n$ and $t \equiv r + s \pmod{n}$. Then

$$\begin{aligned}\phi(a^r a^s) &= \phi(a^{r+s})\\ &= \phi(a^t) \qquad (\text{since } r + s = t + kn \text{ for some } k \in \mathbb{Z})\\ &= t + n\mathbb{Z}\\ &= r + n\mathbb{Z} + s + n\mathbb{Z}\\ &= \phi(a^r) + \phi(a^s),\end{aligned}$$

so the morphism property holds. ■

2.2 Subgroups and quotient groups of cyclic groups

Chapter 5 showed that subgroups and quotient groups of abelian groups are abelian. A natural question arises as to whether the same is true if ‘abelian’ is replaced by ‘cyclic’. The answer is yes, as will be shown in this subsection.

Although we know, from Theorem 2.1, that cyclic groups can be written in a specific form, namely as $\mathbb{Z}$ or $\mathbb{Z}_n$, it is sometimes convenient to view them in a more abstract way and in multiplicative notation. This more abstract view is adopted in this subsection.

We begin by looking at quotients of cyclic groups.

Theorem 2.2 *Quotients of cyclic groups*

(a) Let G be a cyclic group and let $\phi : G \to H$ be a homomorphism. Then $\phi(G)$ is cyclic.

(b) Let G be a cyclic group generated by a and let H be a subgroup of G. Then the quotient group G/H is cyclic and generated by the coset aH.

Proof

(a) Since G is cyclic, it has a generator g, say. We claim that $\phi(g) \in H$ generates $\phi(G)$.

Let $h \in \phi(G)$. Then $h = \phi(a)$ for some $a \in G$. Since g generates G we know that $a = g^n$ for some $n \in \mathbb{Z}$. Hence

$$h = \phi(a) = \phi(g^n) = (\phi(g))^n.$$

Thus we have shown that every element of $\phi(G)$ can be written in the form $(\phi(g))^n$ for some $n \in \mathbb{Z}$, and so $\phi(G)$ is cyclic with generator $\phi(g)$, as required.

(b) We must show that every element of G/H is of the form $(aH)^k$ for some $k \in \mathbb{Z}$.

Suppose that gH is any element of G/H. Then, since G is generated by a, we know that $g = a^k$ for some integer k. But $(aH)^k = (a^k)H = gH$. Hence aH generates G/H. ■

Before proving that every subgroup of a cyclic group is cyclic, you are asked to work through an exercise that should help you understand what is happening.

Exercise 2.1

Let G be a cyclic group generated by a and let H be a non-trivial subgroup of G. Each element of H must be of the form a^k with $k \geq 0$. Among the elements of H, choose the one with the smallest non-zero exponent and let this exponent be m. Since H is non-trivial, such an m exists.

(a) Suppose that a^k is an element of H. Show that m divides k and hence that $H = \langle a^m \rangle$.

Assume now that G is a finite cyclic group of order n – that is, a has order n.

(b) Deduce that m divides n.

(c) If $n = mq$, show that the order of H is q.

Hint: in part (a), use the Division Algorithm (Book A, Chapter 1, Theorem 4.1).

Exercise 2.1 is a major step towards the proof that every subgroup of a cyclic group is cyclic.

Theorem 2.3

Let G be a cyclic group and let H be a subgroup of G. Then H is cyclic.

Proof If H is the trivial subgroup, that is $H = \{e\}$, then H is generated by e and so it is cyclic.

We therefore consider the case when $H \neq \{e\}$, so that H contains a^t for some integer $t \neq 0$. Then H also contains $a^{-t} = (a^t)^{-1}$. As one of t and $-t$ must be positive, H contains a^k for some positive integer k and we can choose m to be the least such positive integer. Then $H = \langle a^m \rangle$ by Exercise 2.1, and so H is cyclic and generated by a^m. ■

Interpreting this result for the infinite cyclic group $\mathbb{Z}$, using additive notation, gives the following corollary.

Corollary 2.4

The subgroups of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$, $n \geq 0$.

Proof By Theorem 2.3, every subgroup of $\mathbb{Z}$ is cyclic. The cyclic subgroups of $\mathbb{Z}$ are those generated by an element of $\mathbb{Z}$, that is, those of the form $\{nz : z \in \mathbb{Z}\} = n\mathbb{Z}$ for some $n \in \mathbb{Z}, n > 0$, as required. ■

We can summarise the results in Exercise 2.1 and Theorem 2.3 as follows. If

$$G = \langle a : a^n = e \rangle$$

is a finite cyclic group of order n and H is a subgroup of G, then:

- H is cyclic
- H is generated by a^m, where m is the smallest positive exponent of a such that $a^m \in H$
- m divides n
- if $n = mq$ then H has order q.

We have shown that every subgroup of a cyclic group is also cyclic. In fact where the group is finite, we will do rather more. As we have seen, Lagrange's Theorem states that, for finite groups, the order of a subgroup must divide the order of the group. For finite *cyclic* groups we can prove a strong converse to Lagrange's Theorem: for every divisor of the order of the group, not only is there a subgroup having that number of elements, but also this subgroup is unique.

Theorem 2.5 *Subgroups of cyclic groups*

Let $G = \langle a \rangle$ be a finite cyclic group of order n, so that a has order n. If q is a factor of n with $n = mq$, then G has a unique subgroup of order q that is generated by the element a^m.

Proof

We start by proving the existence of subgroups whose orders correspond to factors of the order of the group.

Let H be the subgroup $H = \langle a^m \rangle$. In Exercise 2.1, you showed that the order of H is q. Thus, given a factor q of n, the subgroup generated by a^m, where $n = mq$, has order q.

Finally, we show that the subgroup corresponding to the factor q of n is unique.

Suppose that $n = mq$. Then we know that there *is* a subgroup $\langle a^m \rangle$ of order q. Let H be any subgroup of order q. From Exercise 2.1 and Theorem 2.3, we know that H is cyclic and generated by a^l, where l is the least positive exponent of a occurring among the elements of H. Furthermore, the order of H is k, where $n = lk$. But the order of H is q, so $k = q$ and $mq = n = lk = lq$, and, therefore, $m = l$. Thus H is the subgroup generated by a^m.

This completes the proof of Theorem 2.5. ■

Theorem 2.5 can be regarded as a strong converse to Lagrange's Theorem for cyclic groups. We say 'strong' because not only is there a subgroup for every factor of the order of the group, but, in addition, this subgroup is unique.

Later we will investigate the effect of relaxing the assumptions about the group G. We will first consider the case where G is finite and abelian (instead of cyclic) and then go on to relax the condition further to merely finite. At each stage we will still obtain some sort of converse to Lagrange's Theorem; but, as the conditions on G are relaxed, the conclusions become weaker, although still useful.

We conclude this subsection by interpreting the results that we have obtained so far for our standard finite cyclic groups, that is, the groups $\mathbb{Z}_n$.

At this point, a word is in order about how we think of $\mathbb{Z}_n$. In Theorem 2.1, the group $\mathbb{Z}_n$ was defined as the quotient group $\mathbb{Z}/n\mathbb{Z}$. However, in practice we think of $\mathbb{Z}_n$ as the set $\{0, 1, \ldots, n-1\}$, with addition carried out modulo n.

Since the order of $\mathbb{Z}_n$ is n, by Theorem 2.5 there is a subgroup corresponding to each factor of n. That is, if q is a factor of n, then $\mathbb{Z}_n$ has a cyclic subgroup of order q. Theorem 2.1 tells us that this subgroup must be isomorphic to $\mathbb{Z}_q$.

Moreover, we know a generator of the subgroup. Since $\mathbb{Z}_n$ is generated by 1, the subgroup of order q is generated by $m = \frac{n}{q}$.

Exercise 2.2

(a) Write down the orders of the subgroups of $\mathbb{Z}_{24}$.

(b) For each such subgroup:

(i) state to which $\mathbb{Z}_k$ it is isomorphic

(ii) by using the remark above about how we think of the groups $\mathbb{Z}_n$, give an explicit list of its elements.

The interpretation of our results about quotient groups is also seen quite easily: for each factor q of n, there is a subgroup of $\mathbb{Z}_n$ of order q. This subgroup is normal. The corresponding quotient group is cyclic, by Theorem 2.2, and it has order

$$\frac{|\mathbb{Z}_n|}{q} = \frac{n}{q}.$$

Hence the quotient group $\mathbb{Z}_n/\mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{\frac{n}{q}}$.

2.3 Direct products of cyclic groups

In this subsection we will apply the direct product ideas from Section 1 of this chapter to cyclic groups.

We recall some terminology and results about integers. You saw the details in Book A, Chapter 1, Section 4, so here we restate the results that we need without proof.

Let m and n be two positive integers and let $p_1, p_2, \ldots, p_k$ be the prime numbers occurring in either of their prime factorisations. Then

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

where a_i or b_i, but not both, might be zero.

For example, if $m = 126$ and $n = 120$ then $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ and we have

$$126 = 2 \times 3^2 \times 5^0 \times 7 \text{ and } 120 = 2^3 \times 3 \times 5 \times 7^0.$$

We know that the prime factorisation of mn is

$$p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k},$$

so if p is a prime factor of mn, then p must be a prime factor of either m or n or both.

Recall that the **highest common factor** of m and n, written hcf(m, n), is the largest positive integer h that is a factor of both. If c_i is the smaller of a_i and b_i for each i, then h has prime factorisation

$$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}.$$

For example, $\mathrm{hcf}(126, 120) = 2^1 \times 3^1 \times 5^0 \times 7^0 = 2 \times 3 = 6$.

The **least common multiple** of m and n, written $\mathrm{lcm}(m, n)$, is the smallest positive integer l that is a multiple of both m and n. If d_i is the larger of a_i and b_i for each i, then l has prime factorisation

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

For example, $\mathrm{lcm}(126, 120) = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

Two positive integers m and n are said to be **coprime** if their highest common factor is 1.

Proposition 2.6

Let m and n be two positive integers and let $h = \mathrm{hcf}(m, n)$ and $l = \mathrm{lcm}(m, n)$. Then:

(a) The product of m and n is the product of their highest common factor and least common multiple, that is, $mn = hl$.

(b) If m and n are coprime then their least common multiple is mn.

(c) There are integers a and b such that $am + bn = \mathrm{hcf}(a, b)$. In particular, if m and n are coprime there are integers a and b such that $am + bn = 1$.

This proposition combines the results from Proposition 4.7, Lemma 4.9 and Proposition 4.15 of Book A, Chapter 1.

The results in Proposition 2.6 turn out to be relevant when we calculate the order of the element of a direct product. You can tackle the following exercise using direct calculation, but we will shortly prove a result that will avoid the need for calculations.

Exercise 2.3

(a) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$?

(b) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$?

As promised, we now prove some results that enable us to avoid direct calculations when determining the order of an element in a direct product. The following lemma concerns the order of two commuting elements in any group.

Lemma 2.7

Let a and b be elements of finite orders m and n respectively in a group G. Suppose that $ba = ab$ and that $\langle a \rangle \cap \langle b \rangle = \{e\}$ (that is, the only element of G that can be written both as a power of a and as a power of b is e).

Then the order of ab is the least common multiple of m and n.

Proof Let $l = mp = nq$ be the least common multiple of m and n. Since a and b commute, we have that $(ab)^r = a^r b^r$ for any integer r. Then

$$(ab)^l = a^l b^l = a^{mp} b^{nq} = (a^m)^p (b^n)^q = e^p e^q = e,$$

so the order of ab is at most l. Now let $k > 0$ and suppose that $(ab)^k = e$. Then $a^k b^k = e$ so $a^k = b^{-k}$. But then $a^k \in \langle a \rangle \cap \langle b \rangle$ so $a^k = e$. Similarly, $b^k = e$. By Proposition **??** of Chapter 5, we have that k is a common multiple of m and n, and so $k \geq l$. Thus the order of ab is at least l. We have already seen that the order of ab is at most l, so it must be l. ■

Exercise 2.4

Let G be an abelian group and let $g_1, g_2, \ldots, g_r$ be elements of G that have distinct prime orders $p_1, p_2, \ldots, p_r$ respectively. Show that the order of $g_1 g_2 \cdots g_r$ is $p_1 p_2 \cdots p_r$.

Proposition 2.8

Let G, A, B be groups with $G = A \times B$. Suppose that $a \in A$ has order m and $b \in B$ has order n. Then the order of (a, b) is the least common multiple of m and n.

Proof We consider the elements (a, e) and (e, b) in $A \times B$ and check the hypotheses of Lemma 2.7. Firstly, $(a, e)(e, b) = (a, b) = (e, b)(a, e)$. Secondly $\langle (a, e) \rangle = \{(a^k, e) : k = 0, \ldots, m - 1\}$ and $\langle (e, b) \rangle = \{(e, b^k) : k = 0, \ldots, n - 1\}$, so that

$$\langle (a, e) \rangle \cap \langle (e, b) \rangle = \{(e, e)\}.$$

Since both hypotheses hold, we can conclude that the order of (a, b) is the least common multiple of m and n as required. ■

There is one more result about orders of elements in any group G that will be useful.

Proposition 2.9

If $g \in G$ has order n, then the order of g^m is

$$\frac{l}{m} = \frac{n}{h},$$

where l is the least common multiple of m and n, and h is the highest common factor of m and n. In particular, if m is a factor of n then the order of g^m is $\frac{n}{m}$.

Proof The order of g^m is the least positive integer k such that $g^{mk} = e$. By Exercise **??** of Chapter 5, we know that $g^{mk} = e$ precisely when mk is also a multiple of n. So k is the least positive integer such that mk is a multiple of n, hence mk is the least common multiple of m and n. Then $k = \frac{l}{m}$.

Since $mn = hl$ by Proposition 2.6(a), we also have

$$|g^m| = \frac{l}{m} = \frac{n}{h},$$

as required. ■

We can now proceed to consider direct products of cyclic groups. Firstly, we note that, as observed in Subsection 1.2, irrespective of whether the groups are cyclic or not, the order of the direct product of two finite groups is the product of the orders of the individual groups.

Secondly, if the groups concerned are cyclic, then they are abelian, and hence, by Exercise 1.4, so is their direct product.

On the other hand, we also know that direct products of cyclic groups are not always cyclic. For example, in Subsection 1.2 we showed that $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and V is not cyclic.

We can now also use Proposition 2.8 to obtain results of this kind: the order of $(1,1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$ is the least common multiple of the order of 1 in $\mathbb{Z}_2$ and the order of 1 in $\mathbb{Z}_3$. Since these orders are 2 and 3, with least common multiple 6, $(1,1)$ has order 6.

However, sometimes the direct product of cyclic groups *is* cyclic. For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. In Exercise 2.3 we showed that the order of $(1,1)$ is 6. Since this is the order of $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$, this direct product is indeed cyclic.

So, a direct product of cyclic groups may or may not be cyclic. The aim of this subsection is to determine under what circumstances the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

Exercise 2.5

Show that both of the following direct products are cyclic.

(a) $\mathbb{Z}_3 \times \mathbb{Z}_5$

(b) $\mathbb{Z}_4 \times \mathbb{Z}_5$

In the following exercises you will meet two examples of direct products that are not cyclic even though the factor groups are.

Exercise 2.6

(a) Show that $(1,1)$ does not generate $\mathbb{Z}_2 \times \mathbb{Z}_4$. Why is this insufficient to prove that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic?

(b) Show that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

In the solution to Exercise 2.6, we saw that the maximum order for an element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 4. We could show this directly as follows. If (a, b) is any element of the direct product $\mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$\begin{aligned} 4(a,b) &= (4a, 4b) \\ &= (0,0). \end{aligned}$$

Exercise 2.7

Show that the order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24 and, hence, that this direct product is not cyclic.

Being able to determine the maximum order for any element in a direct product will be useful throughout this chapter, so we generalise the result in Exercises 2.6 and 2.7 in the following proposition.

Proposition 2.10

Let $G = \mathbb{Z}_m \times \mathbb{Z}_n$. Then no element of G can have order greater than the least common multiple of m and n.

Proof Let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Suppose that a has order r and b has order s. Then we have that r divides m and s divides n. Thus r and s both divide $l = \operatorname{lcm}(m, n)$. Hence

$$l(a,b) = (la, lb) = (e, e).$$

Thus the order of (a, b) is at most l, as required. ■

The property in Proposition 2.10 does not necessarily hold for a direct product where the factor groups are not both cyclic.

Exercise 2.8

Let $G = S_3 \times \mathbb{Z}_3$.

(a) What is m, the maximum order of an element of S_3?

(b) What is n, the maximum order of an element of $\mathbb{Z}_3$?

(c) What is the lowest common multiple of m and n?

(d) Write down an element of order 6 in G.

The following exercise asks you to decide whether some direct products are cyclic.

Exercise 2.9

For each of the following direct products, decide whether or not it is cyclic and justify your conclusion.

(a) $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_9$

Inspecting the examples above suggests that the direct product of cyclic groups *of coprime orders* is cyclic, but if the orders are not coprime then the direct product is not cyclic. This is the content of the next theorem. However, first you are asked to attempt the following exercise, which provides part of the proof of the theorem.

Exercise 2.10

Show that, if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Theorem 2.11 *Direct products of cyclic groups*

The direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ of the cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ is cyclic if, and only if, m and n are coprime positive integers.

Proof First we prove that, if m and n are coprime, then the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

The element 1 in $\mathbb{Z}_m$ has order m and the element 1 in $\mathbb{Z}_n$ has order n. It follows by Proposition 2.8 that $(1,1)$ has order $\operatorname{lcm}(m,n)$. By Proposition 2.6, we have that $\operatorname{lcm}(m,n) = mn$. Therefore the order of the element $(1,1)$ in the direct product is mn. However, the direct product has mn elements and so it is cyclic.

We proved the converse statement in Exercise 2.10, where we showed that if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. This is equivalent to showing that if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then m and n are coprime. ■

The next corollary gives an important and useful consequence of Theorem 2.11.

Corollary 2.12

Let m and n be coprime positive integers. Then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Proof We know that the group $\mathbb{Z}_{mn}$ is cyclic and has order mn. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ also has order mn and it is cyclic by Theorem 2.11, we have that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ by Theorem 2.1(b). ■

This corollary is an example of the sort of decomposition result that is our main concern in this book. It leads to the main decomposition theorem for cyclic groups, which we prove later in this subsection.

Exercise 2.11

Show that $\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

If, in Exercise 2.11, we had decomposed 90 in a different manner, taking $90 = 9 \times 10$, for example, we would have obtained

$$\mathbb{Z}_{90} \cong \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

Other decompositions of 90 into a product of pairwise coprime factors produce corresponding direct products. However, Theorem 1.6 ensures that all the resulting direct product decompositions are isomorphic.

Exercise 2.12

Suppose that n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers. Show that

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}$ for $i = 1, \ldots, r$.

Hint: use induction on r.

The solution to Exercise 2.12 provides a decomposition theorem for finite cyclic groups, which we restate as follows.

Theorem 2.13 *Decomposition of finite cyclic groups*

If n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}, \quad i = 1, \ldots, r.$

If we combine Theorem 2.13 with the uniqueness of prime decomposition in $\mathbb{Z}$, we see that the decomposition into cyclic groups of prime power order is unique up to isomorphism.

Since each prime power order is a factor of the order of the group, then by Theorem 2.5 each $\mathbb{Z}_{n_i}$ is (isomorphic to) a subgroup. Thus the decomposition theorem expresses the group as a direct product of normal subgroups.

All subgroups of cyclic groups are normal.

We now have a complete description of all cyclic groups, summarised in the three bullet points below.

- Firstly, we have a list of the familiar cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$ for each positive n. Every cyclic group is isomorphic to one group in this list.
- Secondly, every finite cyclic group can be written as a direct product in which every factor is a cyclic group of prime power order. These cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders. Thus the cyclic groups of prime power order form a collection of fundamental building blocks from which all finite cyclic groups can be constructed.
- Thirdly, we know all about the subgroups of a cyclic group.
  For the infinite cyclic group, $\mathbb{Z}$, the subgroups are precisely the sets $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$, for every non-negative integer n.
  A finite cyclic group has a unique cyclic subgroup corresponding to each factor of its order.

The fact that cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders is a consequence of Theorem 2.11.

In addition, given any group that is a direct product of cyclic groups, we can factorise it as a direct product of cyclic groups of prime power order.

Exercise 2.13

Prove that the following two groups are isomorphic by factorising each of them as a direct product of cyclic groups of prime power order:

$$\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 \text{ and } \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}.$$

Exercise 2.14

Factorise the following groups as a direct product of cyclic groups of prime power order.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75}$

(b) $\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245}$

3 Describing groups

The idea that a single group element *generates* a (cyclic) subgroup by repeated applications of the group operation can be generalised to the case of a finite set of elements. This section introduces the notion of a set of generators of a group and a set of *relations* among the generators. As an example, it looks at a family of finite groups called the dicyclic groups, describing them in terms of generators and relations.

3.1 Generators and relations

A group with 12 elements, such as D_6, the symmetry group of the regular hexagon, is really too large to deal with conveniently by a Cayley table. In this section we formally introduce a way of describing a group using generators. We have been using this approach informally in the previous two chapters, and in this section we will take a more rigorous approach.

Our aim is to find a more succinct way of describing the elements of D_6 than by simply listing all 12 elements. In Chapter 6, we used this approach when working with the action of D_6 on itself by conjugation. We would like this description to aid us with manipulating elements in the same way that in $\mathbb{Z}_7$ (say) we can write any element as a power of a generator a, and can write the composition of two elements a^2 and a^3 (say) as $a^2a^3 = a^5$.

The term 'generators' is an extension of the term 'generator' that you met in the context of cyclic groups. We will start this section by describing D_6 in this way. In the following discussion, you can think of the generators as being the elements involved in our succinct description and of the relations as being the rules we need to carry out manipulations.

It is fairly easy to spot a possible generator for all the rotations: for example, the rotation anticlockwise about the centre through $\frac{\pi}{3}$ can be used to produce all the rotations (including the identity).

Composing rotations with the same centre always produces a rotation and never a reflection. As a consequence, a set of generators of D_6 must contain a reflection, since the whole group does. Consider, for example, the reflection in the line shown in Figure 3.1.

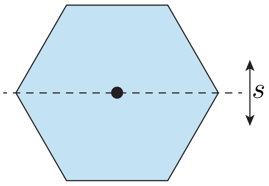


Figure 3.1 Reflection of a hexagon in a given line

Let us label the chosen rotation r and the chosen reflection s. In the following exercise, you are asked to show that these two elements generate D_6. In fact, as you may wish to check, the reflection s is not the only possible choice: *any* reflection will do.

In the notation of M208, $r = r_{\pi/3}$ and $s = q_0$. We have chosen shorter labels for convenience in the calculations that follow.

Exercise 3.1

Let s be the reflection of the hexagon shown in Figure 3.1, and let r be the anticlockwise rotation through $\frac{\pi}{3}$ about the centre of the hexagon.

(a) Express each of the six rotations in D_6 as powers of r.

(b) Express each of the six reflections in D_6 in the form $r^n s$, for suitable integers n.

(c) Since sr must be a group element (by the closure axiom), it must be one of the elements found in the solutions to parts (a) and (b). Which one?

The solution to Exercise 3.1 gives a description of D_6 that will make calculations with its elements much easier. The group D_6 is generated by two elements r and s about which we know the following:

$$r^6 = s^2 = e, \quad sr = r^5 s.$$

Note that the second equation can also be written

$$sr = r^{-1}s.$$

We use these equations to describe the group as follows:

$$D_6 = \langle r, s \,|\, r^6 = s^2 = e,\ sr = r^5 s\rangle.$$

In this description of D_6, the elements r and s are known as the *generators* of the group, and the equations $r^6 = s^2 = e,\ sr = r^5 s$ as the *relations*. We have further information about D_6, namely that every element can be written uniquely in the form

$$r^i s^j \quad \text{for } i = 0, \ldots, 5 \quad \text{and} \quad j = 0, 1.$$

Note that, since $r^0 = s^0 = e$, we usually write $r^i s^0$ as r^i and $r^0 s^j$ as s^j. Thus, elements of D_6 have a **standard form**. The existence of such a standard form enables computations to be made without recourse to a Cayley table.

In practice if, for a given group G, we know

- two generators a and b
- the orders of the two generators
- a relation indicating how to write ba as $a^m b^n$ for some m, n

For an abelian group, for example, we have the relation $ba = ab$.

then we have enough information to write the elements of G in a standard form $a^i b^j$.

This means that we can give an alternative complete and compact description of D_6 as follows:

$$D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}.$$

Note that we have used set notation here, rather than angled brackets. This is because you can read this description of D_6 as ‘the set of expressions of the form $r^i s^j$ where $i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e$ and $sr = r^5 s$'.

The information on the orders of the generators and the relation between them can be used to express any element of D_6 in standard form. As an example, here is how to find the standard form of the product sr^2s.

$$\begin{aligned} sr^2s &= srrs \\ &= r^5srs && \text{using } sr = r^5s \\ &= r^5r^5ss && \text{using } sr = r^5s \text{ again} \\ &= r^{10}e && \text{using } s^2 = e \\ &= r^4 && \text{using } r^6 = e \end{aligned}$$

Exercise 3.2

Let $D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}$.

(a) Use the relations given to express sr^2 and sr^3 in standard form.

(b) Write s^5 in standard form.

The description $D_6 = \langle r, s \mid r^6 = s^2 = e,\ sr = r^5 s\rangle$ is known as a **group presentation**. In general, a group presentation consists of a set of **generators** $g_1, g_2, \ldots, g_n$, say, and a set of equations known as **relations**. Sometimes the relations are given as expressions involving the generators that equate to the identity. Such presentations assume the existence of inverses of the generators as well as the existence of the identity e. It is possible to formally define a group presentation and to define the group described by any such presentation, but we will not do this here. We will just note the properties we need as follows.

Properties of a group presentation

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m\rangle.$$

1. Any element of the group can be written in the form

$$g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s},$$

where $i_1, \ldots, i_s \in \{1, 2, \ldots, n\}$ and $n_i \in \mathbb{Z}$. In this expression there may be repetitions of a generator, and the powers can be both positive and negative.

2. Any equation that holds in the group can be derived from the given relations.

Expressions such as $g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s}$ are known as **words**.

There is a famous issue with this form of presentation, known as the *word problem*, whereby it is not always possible to know whether two words w_1 and w_2 are equal. In other words, it is not always possible to know whether the equality $w_1 = w_2$ can be derived from the given relations. Luckily, the word problem does not arise in the groups we discuss in this module.

For some groups, such as the dihedral groups, elements have a standard form.

Definition 3.1 *Standard form of elements*

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m \rangle.$$

Then we say that elements of G have a **standard form** if every element of G can be written uniquely as a product of powers of the generators according to a specified pattern.

When it is possible to find a standard form for the elements of a certain group, it is also possible to give an alternative presentation of the group whereby the list of generators is replaced by the standard form of the elements of the group. We have done this above for D_6, where we have used the presentation

$$D_6 = \{r^i s^j : \ i = 0, \ldots, 5, \ j = 0, 1; \ r^6 = s^2 = e, \ sr = r^5 s\},$$

where, as remarked earlier, we use set notation rather than angled brackets.

Exercise 3.3

By what names do you know the groups with the following presentations?

(a) $\{r^i : i = 0, \ldots, 5; \ r^6 = e\}$

(b) $\{r^i s^j : i = 0, \ldots, 3, \ j = 0, 1; \ r^4 = s^2 = e, \ sr = r^3 s\}$

(c) $\{r^i s^j : i = 0, 1, \ j = 0, 1; \ r^2 = s^2 = e, \ sr = rs\}$

Recall from Section 1 of Chapter 5 that there is a whole family of dihedral groups, one for each regular polygon. The **dihedral group** D_n is the symmetry group of the regular n-gon, and it has order $2n$. As you can probably see, all dihedral groups can be described in the following way:

$$D_n = \{r^i s^j : i = 0, \ldots, n-1, \ j = 0, 1; \ r^n = s^2 = e, \ sr = r^{n-1} s\}.$$

The next exercise and example are designed to give you practice in working with this type of group presentation. You are asked to work with the dihedral group D_4. Before you start, it is worth convincing yourself that the elements of D_4 may be generated by a rotation r through $\frac{\pi}{2}$ about the centre of the square and a reflection s in an axis through the centre of the square and parallel to two of its sides.

Exercise 3.4

Let G be the group of symmetries of the square, denoted by D_4. In other words,

$$\begin{aligned} G &= \{r^i s^j : i = 0,1,2,3,\ j = 0,1;\ r^4 = s^2 = e,\ sr = r^3 s\} \\ &= \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}. \end{aligned}$$

Let N be the set $\{e, r^2\}$.

(a) Prove that N is a normal subgroup of G.

(b) Find the set of left cosets of N in G in the form aN where $a \in G$.

(c) Using your notation in part (b), write out the Cayley table of the quotient group G/N.

Example 3.2 *D_6 and the Correspondence Theorem*

Let $D_6 = \langle r, s \mid r^6 = s^2 = e, sr = r^5 s = r^{-1} s\rangle$ and let $N = \{e, r^3\}$.

It is not difficult to check that r^3 commutes with every other element of D_6 and that $(r^3)^2 = e$, so N is a normal subgroup of D_6. This implies that the quotient D_6/N is a group, whose elements are

$$\begin{array}{lcccl} N & = & \{e, r^3\} & = & r^3 N, \\ rN & = & \{r, r^4\} & = & r^4 N, \\ r^2 N & = & \{r^2, r^5\} & = & r^5 N, \\ sN & = & \{s, r^3 s\} & = & r^3 sN, \\ rsN & = & \{rs, r^4 s\} & = & r^4 sN, \\ r^2 sN & = & \{r^2 s, r^5 s\} & = & r^5 sN. \end{array}$$

So $D_6/N = \{N, rN, r^2N, sN, rsN, r^2sN\} \cong D_3$. We now apply the Correspondence Theorem to D_6/N to understand the structure of D_6.

You can check that in this copy of D_3, the identity is N, the two non-trivial rotations are rN and r^2N, and sN, rsN, r^2sN are the three reflections.

Now consider the subgroup $H = \{e, r, r^2, r^3, r^4, r^5\}$ of D_6. This subgroup contains N, and it is a normal subgroup of index 2 in D_6.

Thus, by the Correspondence Theorem, H/N is a normal subgroup of D_6/N of index 2 in D_6/N. Since $H/N = \{hN : \ h \in H\}$, the elements of H/N are as follows.

$$\begin{array}{lcl} N & = & \{e, r^3\} \\ rN & = & \{r, r^4\} \\ r^2 N & = & \{r^2, r^5\} \end{array}$$

So $H/N = \{N, rN, r^2N\}$, which is indeed a normal subgroup of D_6/N of index 2: it corresponds to the subgroup of three rotations in D_3 (remember that the identity is a rotation through 0).

Now, the group D_3 has three non-normal subgroups of order 2 and index 3, each of which contains the identity and a reflection.

As a subgroup of D_6/N, one of these three non-normal subgroups is

$$\overline{K} = \{N, sN\}.$$

Since $(sN)^2 = s^2N = eN = N$, we know that sN is self-inverse.

By the Correspondence Theorem, D_6 has a non-normal subgroup K of index 3 that contains N and for which $K/N = \{N, sN\} = \overline{K}$. Thus K is the union of two cosets of N, namely

$$K = N \cup sN = \{e, r^3\} \cup \{s, r^3s\} = \{e, r^3, s, r^3s\}.$$

Confirm this by finding K/N for $K = \{e, r^3, s, r^3s\} \subseteq D_6$.

Finally, note the following.

- K is a subgroup containing N – in fact K is isomorphic to the Klein group, or D_2.
- $|K| = 4$ so the index of K in D_6 is $|D_6|/4 = 12/4 = 3$.
- $rK = \{r, r^4, rs, r^4s\}$ whereas $Kr = \{r, r^4, r^5s, r^2s\} \neq rK$, so K is not normal in D_6.

Exercise 3.5

In the notation of Example 3.2, let $\overline{K}_1$ and $\overline{K}_2$ be the two non-normal subgroups of D_6/N not equal to K.

(a) Write down the elements of $\overline{K}_1$ and $\overline{K}_2$.

(b) Find the subgroups of D_6 that contain N which correspond to $\overline{K}_1$ and $\overline{K}_2$ as in the Correspondence Theorem.

Our findings about the Correspondence Theorem for D_6 in Example 3.2 and Exercise 3.5 are illustrated in Figure 3.2.

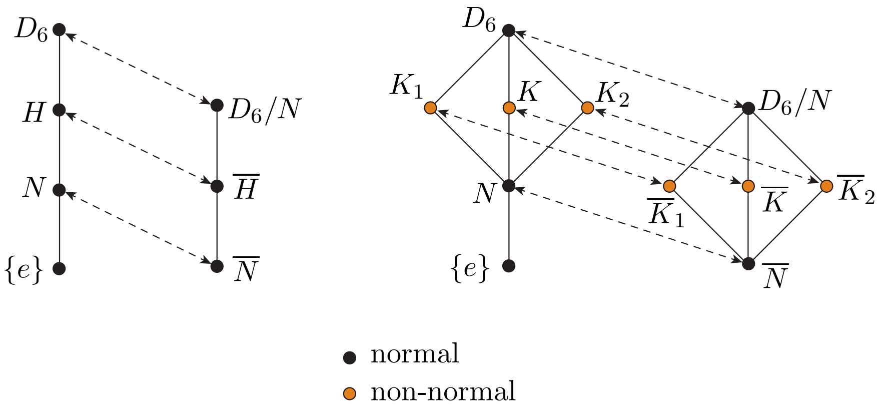


Figure 3.2 D_6 and the Correspondence Theorem

3.2 Dicyclic groups

Consider the group Dic_2 with presentation

$$\mathrm{Dic}_2 = \langle a, b \mid a^4 = e, a^2 = b^2, aba^3b = e\rangle.$$

This is the first in an important family of finite groups whose properties we will explore in this subsection.

Our first task will be to derive some properties of Dic_2 that follow from the relations $a^4 = e$, $a^2 = b^2$ and $aba^3b = e$.

Exercise 3.6

Show that the following hold in the group Dic_2:

(a) $b^4 = e$

(b) b^2 commutes with both a and b

(c) $ba = a^3b$

(d) any element g of Dic_2 can be written in the form
$g = a^r b^s : \ r = 0, \ldots, 3, \ s = 0, 1.$

You may suspect, rightly, that in Exercise 3.6(d) we have found a standard form for the elements of Dic_2. However, to be sure that we really have a standard form we need to show that each element of Dic_2 can be written as $a^r b^s$, for suitable r and s, in a *unique* way.

Note that the expression $a^r b^s$ gives eight elements as r ranges over $0, \ldots, 3$ and s over $0, 1$. Thus, if we can find a group of eight elements with the given presentation, we will know that the expression $a^r b^s$ gives a standard form for its elements. You should be aware that there is no general way of finding such a group.

Consider the diagram in Figure 3.3. You may find it helpful to think of it as a dance formation or as the spokes of two wheels. In Figure 3.4 below, regard a as the dance move where the dancers (or the spokes of the two wheels) rotate anticlockwise through $\frac{\pi}{2}$.

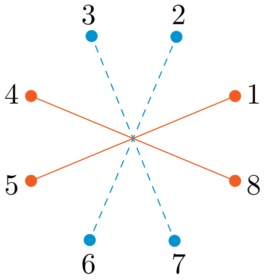


Figure 3.3 A dance formation

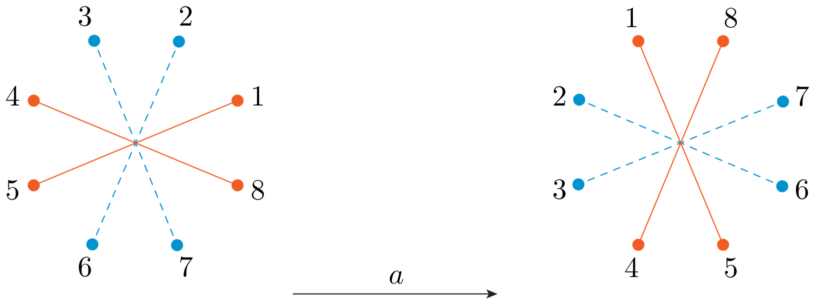


Figure 3.4 The effect of a on the dancers

Now regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 3.5). The dancers (spokes) joined by solid lines move clockwise and the ones joined by a dotted line move anticlockwise.

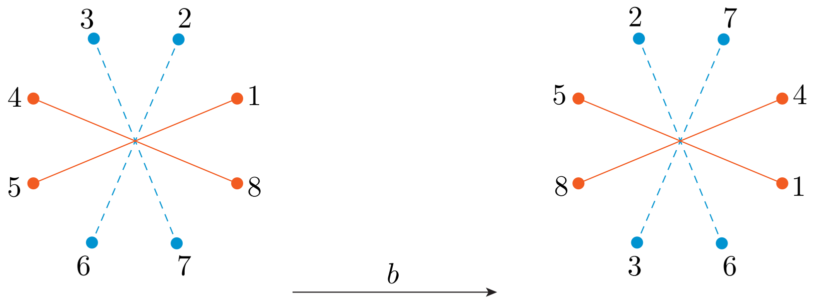


Figure 3.5 The effect of b on the dancers

If we regard a and b as permutations of the set of dancers (or spokes), these descriptions of a and b show that $a^4 = b^4 = e$. They also show that a followed by b is a permutation that reverses the direction of the dancers/spokes in b; that is, the solid lines now move anticlockwise and the dotted lines clockwise. This shows that $ba = ab^{-1} = ab^3$. Finally, you can observe that $a^2 = b^2$ (Figure 3.6).

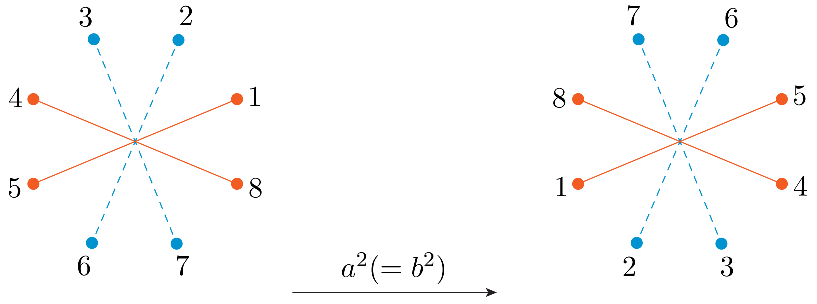


Figure 3.6 The effect of $a^2(= b^2)$ on the dancers

We have thus shown that a and b satisfy the relations in the presentation of the group Dic_2. Since the possible combinations of a and b give rise to eight different permutations of the dancers/spokes, we can see that these permutations form a group of order 8. This group is known as the **dicyclic** group of order 8. It is also known as the **quaternion group**.

In the next exercise you will see another characterisation of the group Dic_2 as a group of matrices over the complex numbers.

Recall that a **complex number** is an expression of the form

$$x + iy,$$

where x and y are real numbers and $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

Exercise 3.7

(a) Let $\mathrm{GL}(2, \mathbb{C})$ be the group of invertible 2×2 matrices over the complex numbers, and let G be the subgroup of $\mathrm{GL}(2, \mathbb{C})$ whose generators are

$$a = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Show that $G \cong \mathrm{Dic}_2$.

(b) Show that G has three normal cyclic subgroups of order 4.

The quaternions are an extension of the complex numbers, and they were first described by the Irish mathematician Sir William Rowan Hamilton (1805–1865). A key fact about this extension is that it is a group where multiplication is not commutative. The quaternion group is the smallest multiplicative subgroup containing the three elements often known as i, j, k, where

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, ki = j.$$

The reason why Dic_2 has two names is that it is the smallest in a family of groups known as the *dicyclic groups*. The dance or wheel pictures help us to describe this family. Consider a dance formation with $4n$ dancers, or a pair of wheels with $4n$ spokes, $2n$ of which are dotted and $2n$ solid. The dancers, or spokes, are divided into four blocks with n dancers or spokes in each, arranged so that the dotted blocks are opposite one another and the solid blocks are opposite one another.

As before, we regard a as the dance move where the dancers, or spokes, rotate anticlockwise by $\frac{\pi}{2}$ (Figure 3.7).

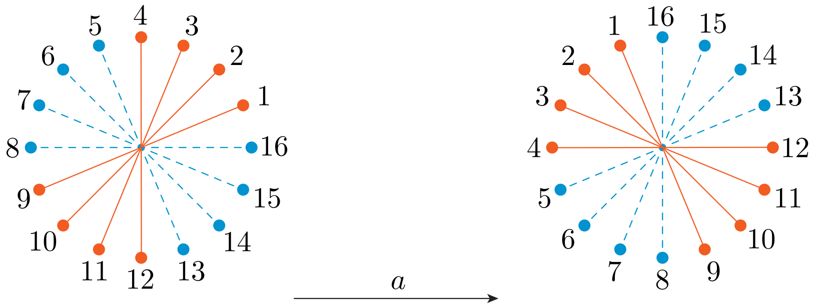


Figure 3.7 The effect of a on a formation of 16 dancers

Again, regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 3.8). The dancers/spokes joined by solid lines move clockwise, and the ones joined by dotted lines move anticlockwise.

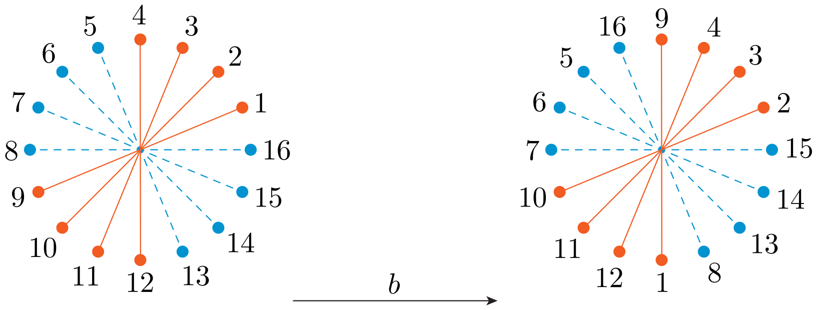


Figure 3.8 The effect of b on a formation of 16 dancers

We can see that in the general case of $4n$ dancers/spokes,

$$a^4 = e, \quad b^{2n} = e \quad \text{and} \quad a^2 = b^n.$$

Some thought may enable you to see that $ab = b^{-1}a$ or, equivalently, $aba^3b = e$. We can therefore give a presentation of the group described using $4n$ dancers/spokes as the **dicyclic group**

$$\underset{n}{\mathrm{Dic}} = \langle a, b \mid a^4 = e, a^2 = b^n, aba^3b = e\rangle.$$

Note that there are $4n$ possible positions of the dancers/spokes, so this group has order $4n$.

Adding dicyclic groups to our list of ‘known’ groups will enable us, by the end of this chapter, to describe all groups of order up to 14.

Exercise 3.8

Show that elements of Dic_n have a standard form given by

$$a^r b^s \quad \text{for } r = 0, \ldots, 3, \ s = 0, \ldots, n-1.$$

Solutions and comments on exercises

Solution to Exercise 1.1

Closure Let (x_1, y_1) and (x_2, y_2) be any two elements of $\mathbb{R} \times \mathbb{R}$. By definition, x_1, y_1, x_2 and y_2 are in $\mathbb{R}$. Since $\mathbb{R}$ is closed under addition, it follows that $x_1 + x_2$ and $y_1 + y_2$ are also in $\mathbb{R}$. By definition,

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

so, by the above, this sum is an element of $\mathbb{R} \times \mathbb{R}$. Therefore the operation $+$ satisfies the closure axiom.

Associativity Let (x_1, y_1), (x_2, y_2) and (x_3, y_3) be three elements of $\mathbb{R} \times \mathbb{R}$. By definition,

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \text{ and}$$
$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1 + (x_2 + x_3),\ y_1 + (y_2 + y_3)).$$

The right-hand sides of these two equations are equal, since addition in $\mathbb{R}$ is associative. Hence

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1, y_1) + ((x_2, y_2) + (x_3, y_3))$$

and so $+$ in $\mathbb{R} \times \mathbb{R}$ is associative.

Identity The element $(0, 0)$ belongs to $\mathbb{R} \times \mathbb{R}$, and

$$(0, 0) + (x, y) = (x, y) + (0, 0) = (x, y)$$

for any (x, y) in $\mathbb{R} \times \mathbb{R}$. Therefore $(0, 0)$ is the identity of $\mathbb{R} \times \mathbb{R}$, and the identity axiom is satisfied.

Inverses If (x, y) is any element of $\mathbb{R} \times \mathbb{R}$ then, as x and y are in $\mathbb{R}$, their additive inverses $-x$ and $-y$ are also in $\mathbb{R}$. So the element $(-x, -y)$ is an element of $\mathbb{R} \times \mathbb{R}$. Furthermore,

$$(x, y) + (-x, -y) = (0, 0) = (-x, -y) + (x, y).$$

So $(-x, -y)$ is the inverse of the element (x, y), and the inverses axiom is satisfied.

Solution to Exercise 1.2

The underlying set is

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_3 &= \{0, 1\} \times \{0, 1, 2\} \\ &= \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}. \end{aligned}$$

The Cayley table is constructed using addition modulo 2 for the first components and addition modulo 3 for the second.

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Solution to Exercise 1.3

(a) Let (g_1,h_1), (g_2,h_2) and (g_3,h_3) be any three elements of $G\times H$. Then

$$\begin{aligned}
&((g_1,h_1)\bullet(g_2,h_2))\bullet(g_3,h_3)\\
&\quad=(g_1\circ g_2,h_1*h_2)\bullet(g_3,h_3) && \text{by the definition of }\bullet\\
&\quad=((g_1\circ g_2)\circ g_3,(h_1*h_2)*h_3) && \text{by the definition of }\bullet\\
&\quad=(g_1\circ(g_2\circ g_3),h_1*(h_2*h_3)) && \text{by the associativity axiom for } G \text{ and } H\\
&\quad=(g_1,h_1)\bullet((g_2\circ g_3),(h_2*h_3)) && \text{by the definition of }\bullet\\
&\quad=(g_1,h_1)\bullet((g_2,h_2)\bullet(g_3,h_3)) && \text{by the definition of }\bullet.
\end{aligned}$$

(b) Let (g,h) be any element of the direct product $G\times H$. Then

$$\begin{aligned}
(e_G,e_H)\bullet(g,h)&=(e_G\circ g,e_H*h) && \text{by the definition of }\bullet\\
&=(g,h) && \text{by the identity axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g,h)\bullet(e_G,e_H)=(g,h).$$

Hence (e_G,e_H) is the identity element of the direct product.

(c) Applying the inverse properties for the groups G and H, we have

$$\begin{aligned}
(g,h)\bullet(g^{-1},h^{-1})&=(g\circ g^{-1},h*h^{-1}) && \text{by the definition of }\bullet\\
&=(e_G,e_H) && \text{by the inverses axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g^{-1},h^{-1})\bullet(g,h)=(e_G,e_H).$$

Hence (g^{-1},h^{-1}) is the inverse of (g,h).

Solution to Exercise 1.4

Let $(g_1,h_1),(g_2,h_2)\in G\times H$. Then

$$\begin{aligned}
(g_1,h_1)(g_2,h_2)&=(g_1g_2,h_1h_2)\\
&=(g_2g_1,h_2h_1)
\end{aligned}$$

since G and H are both abelian. But

$$(g_2g_1,h_2h_1)=(g_2,h_2)(g_1,h_1),$$

so the direct product $G\times H$ is abelian.

Solution to Exercise 1.5

Assume that $h \in H_1 \cap H_2$. We can express h in two ways as an element of $H_1 H_2$, namely

$$\begin{aligned} &h = he, \text{ with } h \in H_1,\ e \in H_2, \text{ and} \\ &h = eh, \text{ with } e \in H_1,\ h \in H_2. \end{aligned}$$

Hence $\phi(h, e) = \phi(e, h)$, and, since ϕ is one–one, we have

$$(h, e) = (e, h).$$

Then $h = e$ by the definition of an ordered pair. Thus the only element in $H_1 \cap H_2$ is the identity, as required.

Solution to Exercise 1.6

As before, we write $a = h_1 h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Let aha^{-1} be any element of aH_2a^{-1}, where $h \in H_2$. Then

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1(h_2hh_2^{-1})h_1^{-1} \\ &= h_1h'h_1^{-1} \qquad (\text{where } h' = h_2hh_2^{-1} \in H_2) \\ &= h'h_1h_1^{-1} \qquad (\text{since } h_1 \in H_1 \text{ and } h' \in H_2 \text{ commute}) \\ &= h' \in H_2, \end{aligned}$$

and so $aH_2a^{-1} \subseteq H_2$.

Solution to Exercise 1.7

We can define the subgroups as follows:

$$\begin{aligned} &H_1 = \langle a^3 \rangle = \{e, a^3\}, \\ &H_2 = \langle a^2 \rangle = \{e, a^2, a^4\}. \end{aligned}$$

Note that $H_1 \cong \mathbb{Z}_2$ and $H_2 \cong \mathbb{Z}_3$.

Since e, a^2, a^3, a^4, a^5 are all in H_1H_2 and

$$a^3a^4 = a^7 = a,$$

we see that $\mathbb{Z}_6 = H_1H_2$.

Next, by inspection, $H_1 \cap H_2 = \{e\}$.

Lastly, we must check that H_1 and H_2 are both normal in $\mathbb{Z}_6$. But $\mathbb{Z}_6$ is abelian, so every subgroup is normal.

Hence H_1 and H_2 satisfy the conditions in Theorem 1.5, and we can conclude that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, as required.

Solution to Exercise 1.8

Let $g = h^{-1}k^{-1}hk$. Since K is a normal subgroup of $G, h^{-1}k^{-1}h \in K$; and so, since $k \in K, g \in K$. Since H is a normal subgroup of G, $k^{-1}hk \in H$; and so, since $h \in H, g \in H$. Thus $g \in H \cap K = \{e\}$ and so $g = e$. That is, $h^{-1}k^{-1}hk = e$, and so by multiplying on the left by kh we see that $hk = kh$.

Solution to Exercise 1.9

Suppose that $\psi(a_1, (b_1, c_1)) = \psi(a_2, (b_2, c_2))$. By the definition of ψ,

$$((a_1, b_1), c_1) = ((a_2, b_2), c_2).$$

By the definition of ordered pairs, $(a_1, b_1) = (a_2, b_2)$ and $c_1 = c_2$. Applying the definition of ordered pairs again, we get $a_1 = a_2$ and $b_1 = b_2$. Hence $(a_1, (b_1, c_1)) = (a_2, (b_2, c_2))$. This shows that ψ is one–one.

To see that ψ is onto, let $((a, b), c)$ be any element of the codomain. Then $a \in A, b \in B, c \in C$, and so $(a, (b, c)) \in A \times (B \times C)$ and $\psi(a, (b, c)) = ((a, b), c)$. Hence ψ is onto.

To check the morphism property, let $(a_1, (b_1, c_1))$ and $(a_2, (b_2, c_2))$ be any two elements of the domain. Then

$$\begin{aligned}\psi((a_1, (b_1, c_1))(a_2, (b_2, c_2))) &= \psi(a_1a_2, ((b_1, c_1)(b_2, c_2)))\\ &= \psi(a_1a_2, (b_1b_2, c_1c_2))\\ &= ((a_1a_2, b_1b_2), c_1c_2)\\ &= ((a_1, b_1)(a_2, b_2), c_1c_2)\\ &= ((a_1, b_1), c_1)((a_2, b_2), c_2)\\ &= \psi(a_1, (b_1, c_1))\psi((a_2, (b_2, c_2)).\end{aligned}$$

This completes the proof that ψ is an isomorphism.

Solution to Exercise 1.10

Since G is abelian, the elements of H_1 and H_2 commute, so we can apply Proposition 1.9(b) to conclude that $H_1H_2 \cong H_1 \times H_2$ via the isomorphism $\psi : H_1H_2 \to H_1 \times H_2$ defined by

$$x_1x_2 \mapsto (x_1, x_2).$$

If $h_1h_2 = 1$, then $(h_1, h_2) = \psi(h_1h_2) = \psi(1)$. Since ψ must map the identity in H_1H_2 to the identity in $H_1 \times H_2$, we must have $(h_1, h_2) = (1, 1)$, which gives the required result.

Solution to Exercise 2.1

(a) Since m is the least positive exponent such that a^m is in H, we have $k \geq m$ and we can use the Division Algorithm (Book A, Chapter 1, Theorem 4.1) to write $k = mq + r$ where $0 \leq r < m$. Hence $r = k - mq$, and so

$$\begin{aligned}a^r &= a^{k-mq}\\ &= a^k a^{-mq}\\ &= a^k(a^m)^{-q}.\end{aligned}$$

Since a^k and a^m belong to H, so does a^r.

Now, m was chosen as the least *positive* exponent appearing in H, so we must have $r = 0$, and hence $m \mid k$. We have shown that every element a^k of H is a power $a^k = a^{mq} = (a^m)^q$ of a^m, which completes the proof that $H = \langle a^m \rangle$.

(b) Since $a^n = e$, which is an element of H, from part (a) we have that $m \mid n$.

(c) Let $n = mq$. We first observe that $e = a^n = a^{mq} = (a^m)^q$. So q is a positive power of a^m that produces the identity. It remains to prove that q is the smallest such power of a^m.

Consider a positive power k of a^m that is the identity; that is, $e = (a^m)^k = a^{mk}$. Since the order of a is n, this can only be true if $mk \geq n = mq$. Hence $k \geq q$. Therefore q is the least power of a^m that gives the identity. Hence the order of a^m, and therefore the order of H, is q.

Solution to Exercise 2.2

(a) The divisors of 24 are $1, 2, 3, 4, 6, 8, 12$ and 24, so $\mathbb{Z}_{24}$ will have a subgroup of each of these orders.

(b) (i) The subgroups are isomorphic to $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ and $\mathbb{Z}_{24}$, respectively.

(ii) The first subgroup in the list is the trivial subgroup, generated by $\frac{24}{1} \equiv 0 \pmod{24}$.

The remaining ones have generators $12, 8, 6, 4, 3, 2$ and 1, respectively.

We list the generators, the elements generated and the cyclic group to which the subgroup is isomorphic in the table below.

Generator (mod 24)	Elements generated	Isomorphic group
$\frac{24}{1} \equiv 0$	$\{0\}$	$\mathbb{Z}_1$
$\frac{24}{2} \equiv 12$	$\{0, 12\}$	$\mathbb{Z}_2$
$\frac{24}{3} \equiv 8$	$\{0, 8, 16\}$	$\mathbb{Z}_3$
$\frac{24}{4} \equiv 6$	$\{0, 6, 12, 18\}$	$\mathbb{Z}_4$
$\frac{24}{6} \equiv 4$	$\{0, 4, 8, 12, 16, 20\}$	$\mathbb{Z}_6$
$\frac{24}{8} \equiv 3$	$\{0, 3, 6, 9, 12, 15, 18, 21\}$	$\mathbb{Z}_8$
$\frac{24}{12} \equiv 2$	$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$	$\mathbb{Z}_{12}$
$\frac{24}{24} \equiv 1$	$\{0, 1, \ldots, 23\}$	$\mathbb{Z}_{24}$

Solution to Exercise 2.3

We use additive notation so that $(0,0)$ denotes the identity in both cases, and we write $n(x,y)$ for $\underbrace{(x,y)+\cdots+(x,y)}_{n \text{ times}}$.

(a) We have $(1,1)=(1,1)$, $2(1,1)=(0,2)$, $3(1,1)=(1,0)$,
$4(1,1)=(0,1)$, $5(1,1)=(1,2)$, $6(1,1)=(0,0)$.

Hence $(1,1)$ has order 6.

(b) We have $1(1,1)=(1,1)$ and $2(1,1)=(0,0)$. Hence $(1,1)$ has order 2.

Solution to Exercise 2.4

We use induction on r, the number of elements in the product. For $r=2$, the result follows from Lemma 2.7, since G is abelian and p_1 and p_2 are distinct primes, so that $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$.

Suppose the result is true for $r=k$; that is, if $g_1, g_2, \ldots, g_k$ are elements of G that have distinct prime order $p_1, p_2, \ldots, p_r$ respectively, then the order of $g_1 g_2 \cdots g_k$ is $p_1 p_2 \cdots p_k$.

Let g_{k+1} be an element of G of order p_{k+1}, where p_{k+1} is prime and distinct from $p_1, p_2, \ldots, p_k$. Then

$$\langle g_1 g_2 \cdots g_k\rangle \cap \langle g_{k+1}\rangle = \{e\}$$

since no elements of $\langle g_1 g_2 \cdots g_k\rangle$ can have order p_{k+1}, and so we can apply Lemma 2.7 to obtain that the order of $g_1 g_2 \cdots g_{k+1}$ is $p_1 p_2 \cdots p_{k+1}$.

The result follows by induction.

Solution to Exercise 2.5

By Proposition 2.8, the order of the element $(1,1)$ in the direct product is the least common multiple of the orders of the element 1 in each of the factor groups.

(a) The order of 1 in $\mathbb{Z}_3$ is 3 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(3,5)=15$, the element $(1,1)$ has order 15 in $\mathbb{Z}_3 \times \mathbb{Z}_5$.
As $\mathbb{Z}_3 \times \mathbb{Z}_5$ has 15 elements, it is cyclic.

(b) The order of 1 in $\mathbb{Z}_4$ is 4 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(4,5)=20$, the element $(1,1)$ has order 20 in $\mathbb{Z}_4 \times \mathbb{Z}_5$.
As $\mathbb{Z}_4 \times \mathbb{Z}_5$ has 20 elements, it is cyclic.

Solution to Exercise 2.6

(a) The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_4$ is 4.
Since $\operatorname{lcm}(2,4)=4$, the element $(1,1)$ has order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_4$.
As $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 8 elements, it is not generated by $(1,1)$.

All we have done is to show that $(1,1)$ is not a generator. To show that the direct product is not cyclic, we would have to show that *none* of the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ generates the whole group.

(b) If (a, b) is any element of $\mathbb{Z}_2 \times \mathbb{Z}_4$, then a has order 1 or 2 and b has order 1, 2 or 4. The only possible least common multiples of the orders of a and b are 1, 2 and 4. Hence no element of the direct product has order 8, and so $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

Solution to Exercise 2.7

Let $a \in \mathbb{Z}_6$. Then $6a = 0$. Similarly, if $b \in \mathbb{Z}_8$, then $8b = 0$. Hence for any element (a, b) in $\mathbb{Z}_6 \times \mathbb{Z}_8$, we have

$$\begin{aligned} 24(a, b) &= (24a, 24b) \\ &= (4(6a), 3(8b)) \\ &= (0, 0). \end{aligned}$$

So the maximum order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24. Since this direct product has order 48, it cannot be cyclic.

Solution to Exercise 2.8

(a) The maximum order of an element of S_3 is 3.

(b) The maximum order of an element of $\mathbb{Z}_3$ is 3.

(c) The lowest common multiple is 3.

(d) $((1\,2), 1)$ has order 6.

Solution to Exercise 2.9

(a) The group $\mathbb{Z}_4 \times \mathbb{Z}_6$ is not cyclic.

The maximum order of an element in $\mathbb{Z}_4$ is 4 and the maximum order for an element of $\mathbb{Z}_6$ is 6. Since $\operatorname{lcm}(4, 6) = 12$, the maximum order for any element is at most 12.

Therefore the direct product, of order 24, is not cyclic.

(b) The group $\mathbb{Z}_2 \times \mathbb{Z}_9$ is cyclic.

Previous examples suggest that $(1, 1)$ should be a generator, which we can confirm as follows.

The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_9$ is 9. Since $\operatorname{lcm}(2, 9) = 18$, the element $(1, 1)$ has order 18 in the direct product. As the direct product has 18 elements, it is cyclic.

Solution to Exercise 2.10

By Proposition 2.10, no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ can have order greater than the least common multiple of m and n.

Since m and n are not coprime, we have that $\operatorname{lcm}(m, n) < mn$, the order of the direct product. Hence no element can generate the whole of the direct product, and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Solution to Exercise 2.11

We have $90 = 2 \times 45$. Since 2 and 45 are coprime, we can deduce from Corollary 2.12 that

$$\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_{45}.$$

Similarly, since $45 = 9 \times 5$ and these factors are coprime, we have

$$\mathbb{Z}_{45} \cong \mathbb{Z}_9 \times \mathbb{Z}_5.$$

Combining these results gives

$$\begin{aligned} \mathbb{Z}_{90} &\cong \mathbb{Z}_2 \times \mathbb{Z}_{45} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5. \end{aligned}$$

Solution to Exercise 2.12

We use induction on r, the number of distinct prime factors, and generalise the argument used in the solution to Exercise 2.11.

Firstly, if $r = 1$ the result is immediate. Now suppose that the result is true for $r - 1$ and write

$$\begin{aligned} n &= p_1^{k_1} (p_2^{k_2} \cdots p_r^{k_r}) \\ &= n_1(n_2 \cdots n_r), \end{aligned}$$

where, because all the p_i are distinct, the factors n_1 and $n_2 \cdots n_r$ are coprime. By Corollary 2.12, we have

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2 \cdots n_r}.$$

But $\mathbb{Z}_{n_2 \cdots n_r} \cong \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ by the inductive hypothesis, hence the result holds for $\mathbb{Z}_n$ by Proposition 1.10.

Solution to Exercise 2.13

We apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$. For example, since $154 = 2 \times 7 \times 11$, we have

$$\mathbb{Z}_{154} \cong \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}.$$

Hence $\begin{aligned}[t] \mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 &\cong (\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_5) \times \mathbb{Z}_5 \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$

Note that 4 is a prime power and it cannot be factorised into distinct primes.

Similarly, we apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$. This gives

$$\begin{aligned} \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10} &\cong (\mathbb{Z}_5 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_7) \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$$

Thus the two groups $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$ and $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$ are isomorphic to the same direct product and hence to one another.

Solution to Exercise 2.14

(a)
$$\begin{aligned}\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75} &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_{25})\\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{25}\\ &= (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{5^2}.\end{aligned}$$

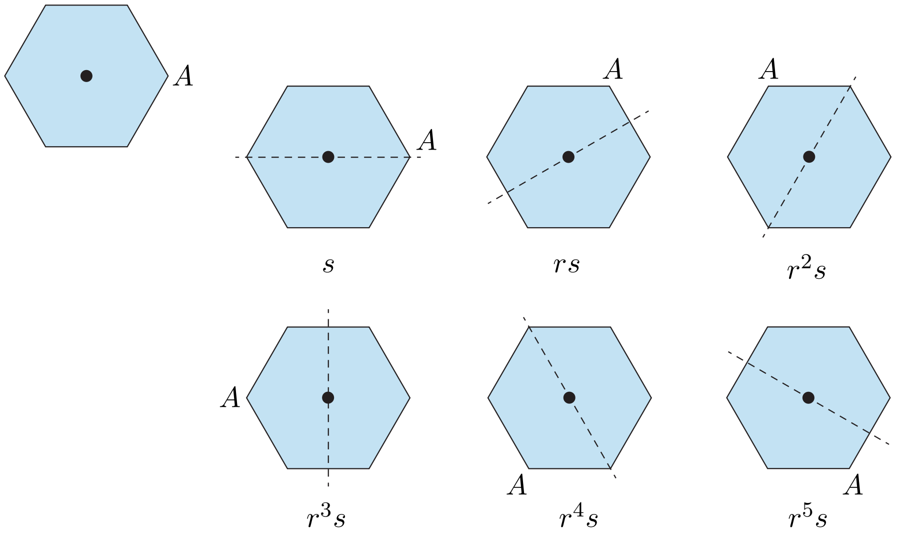
(b)
$$\begin{aligned}\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245} &\cong \mathbb{Z}_9 \times (\mathbb{Z}_3 \times \mathbb{Z}_7) \times (\mathbb{Z}_5 \times \mathbb{Z}_{49})\\ &\cong (\mathbb{Z}_3 \times \mathbb{Z}_9) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{49})\\ &= (\mathbb{Z}_3 \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{7^2}).\end{aligned}$$

Solution to Exercise 3.1

(a) All the rotations in D_6 are obtained by repeating r a sufficient number of times. Thus the rotations are

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6 = r^0 = e.$$

(b) The easiest way to find out which reflection corresponds to each expression of the form $r^n s$ is to keep track of what happens to the vertices of the hexagon under each composite transformation. These transformations are illustrated in the figure below.



s $\quad$ rs $\quad$ r^2s

r^3s $\quad$ r^4s $\quad$ r^5s

(c) By inspection, we find that $sr = r^5s$.

You may have expressed this element in the form $r^{-1}s$, which is the same because $r^{-1} = r^5$.

Solution to Exercise 3.2

(a) $sr^2 = srr = r^5sr = r^5r^5s = r^{10}s = r^4s$

$sr^3 = sr^2r = r^4sr = r^4r^5s = r^9s = r^3s$

The second result should be no surprise as r^3 is rotation through π and so commutes with all the elements of D_6. If you spotted this and used it in your solution, well done!

(b) $s^5 = s$

Solution to Exercise 3.3

(a) This is the cyclic group $\mathbb{Z}_6$.

(b) This is the dihedral group D_4 – the symmetry group of a square.

(c) This is the Klein group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The relation $sr = rs$ means that the two generators commute. A little thought might convince you that this implies the group is abelian. In addition, the standard form shows the group has four elements, and it is not hard to see that no element has order greater than 2. These conditions are enough to show that the group is isomorphic to V.

Solution to Exercise 3.4

(a) Firstly we show that N is a subgroup of G.

Closure The only non-trivial product to check is $r^2r^2 = e$. So N satisfies the closure axiom.

Identity As e is in N, the identity axiom is satisfied.

Inverses As $e^{-1} = e$ and $\left(r^2\right)^{-1} = r^2$, the inverses axiom is satisfied.

Hence N is a subgroup of G.

Alternatively, simply note that $N = \langle r^2 \rangle$.

Next, we must show that N is normal. We need to check that aNa^{-1} is a subset of N for each a in G.

As $aea^{-1} = e \in N$ for each a in G, we only have to check that ar^2a^{-1} is in N. Using the relations $r^4 = s^2 = e$ and $sr = r^3s$ gives the following.

$$\begin{aligned}
er^2e^{-1} &= r^2\\
rr^2r^{-1} &= r^2\\
(r^2)r^2(r^2)^{-1} &= r^2\\
(r^3)r^2(r^3)^{-1} &= r^2\\
sr^2s^{-1} &= r^2\\
(rs)r^2(rs)^{-1} &= r^2\\
(r^2s)r^2(r^2s)^{-1} &= r^2\\
(r^3s)r^2(r^3s)^{-1} &= r^2
\end{aligned}$$

This completes the proof that N is a normal subgroup of G.

(b) The distinct left cosets of $N = \{e, r^2\}$ are

$$\begin{aligned}
eN &= r^2N = N,\\
rN &= r^3N = \{r, r^3\},\\
sN &= r^2sN = \{s, r^2s\},\\
rsN &= r^3sN = \{rs, r^3s\}.
\end{aligned}$$

(c) The Cayley table of G/N is as follows.

$\circ$	N	rN	sN	rsN
N	N	rN	sN	rsN
rN	rN	N	rsN	sN
sN	sN	rsN	N	rN
rsN	rsN	sN	rN	N

Solution to Exercise 3.5

(a) $\overline{K}_1 = \{N, rsN\},\ \overline{K}_2 = \{N, r^2sN\}$.

(b) $K_1 = \{e, r^3, rs, r^4s\},\ K_2 = \{e, r^3, r^2s, r^5s\}$.

Solution to Exercise 3.6

(a) $b^4 = (b^2)^2 = a^4 = e$

(b) $b^2a = a^2a = a^3 = aa^2 = ab^2 \quad$ and $\quad b^2b = b^3 = bb^2$

(c)
$$\begin{aligned} aba^3b = e &\Rightarrow aaba^3b = a \\ &\Rightarrow ba^2ba^3b = ba \\ &\Rightarrow b^4a^3b = ba && \text{using } a^2 = b^2 \\ &\Rightarrow a^3b = ba && \text{using } a^4 = e \text{ and } a^2 = b^2 \end{aligned}$$

(d) The result in part (c) means that in any word involving a and b we can successively move all the bs to the right. This will give us a word of the form $\alpha\beta$, where α is a word containing only as and β is a word containing only bs.

We can then use $a^4 = e$ and $b^4 = e$ to reduce α and β to a^r and b^s respectively for some $r, s \in \{0, 1, 2, 3\}$.

Lastly, we can use $b^2 = a^2$ and $b^3 = a^2b$ to write an element g of Dic_2 in the form $g = a^rb^s : \ r = 0, \ldots, 3,\ s = 0, 1$.

Solution to Exercise 3.7

(a) We have

$$a^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and}$$

$$b^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

so $a^2 = b^2$. Moreover, $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, that is, $(a^2)^2 = a^4 = e$.

Another matrix calculation shows that $aba^3b = e$.

Calculation also shows that the eight matrices

$$a^rb^s : \ r = 0, \ldots, 3,\ s = 0, 1$$

are distinct, and the required result follows.

(b) Both $\langle a\rangle$ and $\langle b\rangle$ are cyclic subgroups of order 4. Moreover, the product $ab = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$ also generates a cyclic subgroup of order 4. Since $|G| = 8$, these three subgroups of order 4 have index 2 in G, and so they are normal.

Solution to Exercise 3.8

Since $a^4 = e$, we have $a^3 = a^{-1}$.

Since $a^2 = b^n$ and $a^4 = e$, we have $a^4 = (b^n)^2 = b^{2n} = e$, hence

$$b^{2n-1} = b^{-1}.$$

Now

$$\begin{aligned} aba^3b = e &\Rightarrow ba^3b = a^{-1} = a^3 \\ &\Rightarrow ba^3 = a^3b^{-1} = a^3b^{2n-1} \\ &\Rightarrow ba^3 = a^3a^2b^{n-1} = ab^{n-1} \\ &\Rightarrow ba = ab^{n-1}a^2 = a^3b^{n-1}. \end{aligned}$$

We can use this relation to rewrite any word in a, b as a word in a followed by a word in b, that is, a power of a followed by a power of b. We then use

$$a^4 = e, \quad a^2 = b^n$$

to ensure that the power of a is one of $a^0 (= e), a, a^2, a^3$ and the power of b is one of $b^0 (= e), b, \ldots, b^{n-1}$.

This shows that every element of Dic_n can be written in the required form. Since this form gives $4n$ elements and Dic_n has order $4n$, we have a standard form.

Index

action by conjugation, 36
action by left multiplication, 44

Cartesian product, 5
Cauchy's Theorem, 47
Cayley's Theorem, 45
classification of cyclic groups, 19
coprime, 25

decomposition of $\mathbb{Z}_{mn}$, 29
decomposition theorem for finite cyclic groups, 30
direct product of groups, 6
direct products of cyclic groups, 29
direct sum of groups, 7

external direct product of groups, 6

group action, 32

highest common factor, 24

internal direct product of groups, 11
Internal Direct Product Theorem, 12

least common multiple, 25

Orb(x), the orbit of x, 38
Orbit–Stabiliser Theorem, 43

quotients of cyclic groups, 21

Stab(x), the stabiliser of x, 40
subgroups of cyclic groups, 23