

# Chapter 2

## Groups

### 2.1 Symmetries

**Warning!** This section attempts to motivate the topic of this chapter, Groups. As a consequence, you will find it vague and you may find it confusing. If you find it too confusing, ignore it. It is not *necessary* to anything that follows. The same comment applies to the exercises at the end.

We will start with a question.

What are the finite 2-dimensional symmetrical objects?

If you think about this for a while you will probably come to the conclusion that it is a bad question. Let us try to list some of the problems with it:

- What is a finite object? For example, is a square finite? Is a circle finite?
- What does symmetrical mean?
- Assuming we could gain some agreement about the answer to the first two points in this list, how could we list all of the answers?

Let us assume that a square fits into our ideas of a symmetrical object.

- Are two squares of different side length to be listed separately?
- Are two squares of the same side length but with different centres to be listed separately?
- Are two squares of the same side length and the same centre but with different orientations to be listed separately?

The answer to the latter points in the list above are probably no, otherwise our list would be far too complicated to be of any use or interest. So let us try to re-formulate our question. Perhaps our interest should be in the symmetries themselves rather than the objects of which they are symmetries. That would answer most, if not all, of the questions above.

So we try again, with a different question.

What are the finite sets of symmetries of 2-dimensional objects?

This looks more possible; most of our previous problems disappear with this way of formulating the question. There is a very reasonable objection that we have changed the question and we aren't really answering the same question anymore. But this is at least a major step towards providing the sort of information that the first question was seeking.

Let us see what we can say about the new version of the question. Some sorts of finite sets of symmetries of 2-dimensional objects spring to mind fairly quickly.

Start with a square. It has 4 reflectional symmetries and at least 3, possibly 4, rotational symmetries. The uncertainty there is because we have to decide whether to call 'doing nothing' a symmetry. It turns out to be much more convenient if we do. So we have an example. More should come to mind fairly quickly.

- The set of four reflections and four rotations which are symmetries of a square.
- The set of three reflections and three rotations which are symmetries of an equilateral triangle.
- The set of five reflections and five rotations which are symmetries of a regular pentagon.
- The set of six reflections and six rotations which are symmetries of a regular hexagon.
- ...
- ...
- ...
- Keep going until you get tired, or work out a general statement.

So we have a large, but fairly easily described collection of symmetries of 2-dimensional objects. If you think harder about this, you may see that we can get some other examples by going ‘down’ rather than ‘up’ from an equilateral triangle. We can also get the set of two reflections and two rotations which are symmetries of (for example) a non-square rectangle. Finally, we can get the set of one reflection and one rotation which are symmetries of (for example) an isosceles but non-equilateral triangle.

There is another way we can produce new sets of symmetries from the ones we already have. We can try to ‘break’ some, but not all, of the symmetry of the object, such as the regular polygon, used to represent the set of symmetries. For example, with all of the previous examples of polygons, we can put arrowheads, at the centre of each side of the polygon and all pointing in a clockwise direction. The effect of this is to remove the reflectional symmetries and leave only the rotational symmetries. There are other ways of ‘breaking symmetry’ but you will find that the set of symmetries you are left with is the same as some other set you have constructed.

So let us summarise the possibilities we have found as an answer to the second question.

**Answer (but maybe not complete yet)** The following can be finite sets of symmetries of 2-dimensional objects:

- Any set of  $n$  rotations and  $n$  reflections as described above, where  $n = 1, 2, 3, \dots$
- Any set of  $n$  rotations as described above, where  $n = 1, 2, 3, \dots$

It is far from clear that these are the only possibilities. But they are, and we will eventually be able to prove it.

If you found all of this rather easy, what about the same problem for symmetries of three-dimensional objects?

### 2.1.1 Exercises

- (1) Describe the rotational symmetries of a cube. There are 24 in all. It will probably help to have a cube (or something your imagination will allow you to believe is a cube) near at hand. Are there any other symmetries besides these rotations?
- (2) Describe the 12 rotational symmetries of a regular tetrahedron.
- (3) Describe some rotational symmetries of a 4-dimensional cube. (Of course you will first have to work out what a 4-dimensional cube is.)
- (4) What letters in the Roman alphabet display symmetry?

## 2.2 What groups are, and some examples

I hope that you have been convinced in the last section that there is some point in studying sets of symmetries separately from the objects of which they are symmetries. Let us look at the properties which a set of symmetries of some geometric object must have. Firstly, by a *composition* of two symmetries, we mean the effect of applying one after the other. So we can see that the composition of two symmetries of the object is a third symmetry of the object. Also, symmetries are reversible; that is we can find a second symmetry so that the composition leads back to where we started. By agreement, ‘doing nothing’ is a symmetry.

There are many other collections of things, such as the real numbers with ‘addition’ replacing ‘composition’ which have similar properties. This leads us into an abstract definition.

### 2.2.1 Definition of a group

In the following definition, a binary operation on a set  $G$  is simply a function of two variables, from  $G$ , which takes its values in  $G$ . If we used  $f$  for this function and if  $g, h \in G$ , we could therefore write  $f(g, h)$  for the value, in  $G$  of this function. But the examples of such functions in practice are very often functions such as addition or multiplication and most people find it strange to write  $+(a, b)$  or  $\times(a, b)$ . We shall therefore denote the general function by  $*$  (or something similar) and use  $g * h$  rather than  $*(g, h)$  for the value of the function. Later, we will often abbreviate  $g * h$  to  $gh$ .

**Definition 2.2.1.** *A group consists of a set  $G$  together with a binary operation  $*$  which satisfies*

- (0)  $g * h \in G$  for all  $g, h \in G$ ;
- (1)  $g * (h * k) = (g * h) * k$  for all  $g, h, k \in G$ ;
- (2) there is an element  $e_G$  in  $G$  which satisfies  $g * e_G = e_G * g = g$  for all  $g \in G$ : we call  $e_G$  the identity of  $G$ ;
- (3) for each  $g \in G$  there is an element  $g^{-1} \in G$  satisfying  $g * g^{-1} = g^{-1} * g = e_G$ : we call  $g^{-1}$  the inverse of  $g$ .

We said nothing before the definition about rule (1). That was largely because it was too obvious. This will frequently, but not always, be the case. You need to watch out, however, for cases when the property in rule (1) is not a well-known fact.

Note that when we specify a group, we must specify an operation. Identities and inverses are then all taken with respect to this operation. It is possible that an individual element belongs to a different group with a different operation where its ‘inverse’ is quite different.

Before we go on to examples, let us work a little with the definitions. For example,

**Lemma 2.2.1.** (1) *Each group has only one identity;*

(2) *each element has only one inverse;*

(3) *the inverse of  $g * h$  is  $h^{-1} * g^{-1}$ .*

*Proof.* (1) Suppose  $e_G$  and  $f_G$  both satisfy the properties required of an identity for the group  $G$ . Then, as  $e_G$  is an identity,  $e_G * f_G = f_G$ . Also, as  $f_G$  is an identity,  $e_G * f_G = e_G$ . So  $e_G = f_G$ .

(2) Exercise 6.

(3)

$$\begin{aligned}(g * h) * (h^{-1} * g^{-1}) &= g * (h * (h^{-1} * g^{-1})) = g * ((h * h^{-1}) * g^{-1}) \\ &= g * (e_G * g^{-1}) = g * g^{-1} = e_G.\end{aligned}$$

A similar calculation shows that  $(h^{-1} * g^{-1}) * (g * h) = e_G$  and so  $h^{-1} * g^{-1}$  is the inverse of  $g * h$ .  $\square$

**Remark:** Other common symbols for group operations include:

$$g \cdot h, g \circ h, gh, g + h.$$

## 2.2.2 Examples of groups

- (1) The set of all symmetries of a 2-dimensional geometrical figure together with the operation of composition of symmetries. The same will apply in 3 or more dimensions once we formulate more clearly what we mean by a symmetry.
- (2) To give a more precise version of the previous examples, denote by  $D_n$ —called the *dihedral* group of order  $n$ —the set of all symmetries of a regular  $n$ -gon together with the operation of composition. For  $n \geq 3$  there is no problem with this definition. For  $n = 1$  or  $n = 2$  we have, for example, to ‘interpret’ a regular 2-gon as a non-square rectangle and a regular 1-gon as an isosceles but non-equilateral triangle. Then  $D_n$  has  $2n$  elements and comprises  $n$  rotations and  $n$  reflections.

- (3) The group  $(\mathbb{Z}, +)$  of integers together with the operation of addition.
- (4) The groups  $(\mathbb{Q}, +)$  of rational numbers,  $(\mathbb{R}, +)$  of real numbers and  $(\mathbb{C}, +)$  of complex numbers furnished, in each case, with the operation of addition.
- (5)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are **not** groups with multiplication as the operation, since 0 has no inverse.
- (6) The set  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  of non-zero rational numbers furnished with the operation of multiplication is a group. We can similarly form groups  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$  and  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ .
- (7)  $\mathbb{Z} \setminus \{0\}$  is **not** a group under multiplication since only  $\pm 1$  have inverses.
- (8) The group of all  $n \times n$  matrices with entries from the real numbers and the operation of matrix addition.
- (9) The group of all invertible (non-singular) matrices with entries from the real numbers and the operation of matrix multiplication. This is an important example and we shall devote a sub-section to it.

### 2.2.3 Matrix groups

Let  $F$  be a field; for example  $F$  could be the rational numbers, the real numbers, the complex numbers or the integers modulo a prime number  $p$ .

We list here the names of some important groups. In every case the operation is matrix multiplication; we do not list this explicitly each time.

|            |   |
|------------|---|
| $GL(n, F)$ | the collection of all $n \times n$ invertible matrices with entries from $F$                      |
| $O(n)$     | the collection of all $n \times n$ orthogonal matrices (real matrices $A$ such that $A^T A = I$ ) |
| $U(n)$     | the collection of all $n \times n$ unitary matrices (complex matrices $U$ such that $U^* U = I$ ) |
| $SL(n, F)$ | the collection of all $n \times n$ matrices of determinant 1 with entries from $F$                |
| $SO(n)$    | the collection of all $n \times n$ orthogonal matrices of determinant 1                           |
| $SU(n)$    | the collection of all $n \times n$ unitary matrices of determinant 1                              |

There are also many other groups of matrices which have important special properties and corresponding names.

### 2.2.4 Groups with at most 4 elements

First we note some other simple properties of groups.

**Lemma 2.2.2.** (1) *In any group  $G$  we have cancellation laws:*

$$(a) \ g * x = g * y \text{ implies } x = y, \quad (b) \ x * h = y * h \text{ implies } x = y.$$

(2) *We can also solve equations: Given any  $g, h$  in a group  $G$  there are unique  $x, y \in G$  such that*

$$(a) \ g * x = h, \quad (b) \ y * g = h.$$

*Proof.* 1(a) If  $g * x = g * y$ , then  $g^{-1} * (g * x) = g^{-1} * (g * y)$ , so  $(g^{-1} * g) * x = (g^{-1} * g) * y$  by associativity. Hence  $e * x = e * y$  by the property of inverses, so  $x = y$  by the property of the identity element  $e$ . 1(b) is similar.

We leave part (2) as exercise 3. □

**Consequence:** In a group multiplication table each element occurs *exactly once* in each row and each column. For example, 1(a) says that all entries  $gx$  in the row containing  $g$  are different; 2(a) says that every group element occurs in this row.

**Examples:** Using this observation, we see

(1) A group with 2 elements  $\{e, a\}$  has a multiplication table:

|   |   |   |
|---|---|---|
| * | e | a |
| e | e | a |
| a | a | e |

So there is essentially only one possible group with 2 elements;  $(\mathbb{Z}_2, +)$  is such a group. (Two groups are “essentially the same” or *isomorphic* if their multiplication tables are the same after suitable *renaming* of elements.)

(2) For a group with 3 elements  $\{e, a, b\}$  we must have:

|   |   |   |   |
|---|---|---|---|
| * | e | a | b |
| e | e | a | b |
| a | a |   |   |
| b | b |   |   |

Again, there is only one way to fill in the missing entries, so there is essentially only one possible group with 3 elements;  $(\mathbb{Z}_3, +)$  is such a group.

**Exercise:** Find two “different” multiplication tables for groups with 4 elements.

### 2.2.5 Permutations

Most of us have an intuitive idea of what a permutation is; it is a re-arrangement of some sort. We shall need a somewhat more precise version, however, so that we can work in more detail with them.

**Definition 2.2.2.** *A permutation of a set  $S$  is a function  $f : S \rightarrow S$  which is bijective, i.e.  $f$  is one-to-one and onto.*

Thus the function does the ‘re-arrangement’ for us. For example suppose that  $S$  has two elements  $a$  and  $b$ . There are two permutations of  $S$ :

$$\begin{array}{l} a \rightarrow a \\ b \rightarrow b \end{array} \quad \text{and} \quad \begin{array}{l} a \rightarrow b \\ b \rightarrow a \end{array}$$

Now observe that the composition of two bijective functions is bijective and so the composition of two permutations is a permutation. Also the inverse of a bijective function is bijective and so the inverse of a permutation is a permutation. Thus we can see that the set of all permutations of a set  $S$ , together with the operation of composition of functions, gives a group which we will denote  $\text{Sym}(S)$ .

A little thought should convince you that the number of permutations of a set and how they combine together does not depend on the names we give to the elements of the set. So if we want to consider the permutations of a finite set of size  $n$ , we will usually take the set to be  $S = \{1, \dots, n\}$ .

The permutations of  $\{1, 2, 3\}$  are

$$\begin{array}{cccccc} 1 \rightarrow 1 & 1 \rightarrow 2 & 1 \rightarrow 3 & 1 \rightarrow 2 & 1 \rightarrow 3 & 1 \rightarrow 1 \\ 2 \rightarrow 2 & 2 \rightarrow 3 & 2 \rightarrow 1 & 2 \rightarrow 1 & 2 \rightarrow 2 & 2 \rightarrow 3 \\ 3 \rightarrow 3 & 3 \rightarrow 1 & 3 \rightarrow 2 & 3 \rightarrow 3 & 3 \rightarrow 1 & 3 \rightarrow 2 \end{array}$$

We can write a permutation  $f$  without the arrows by writing it in the form

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

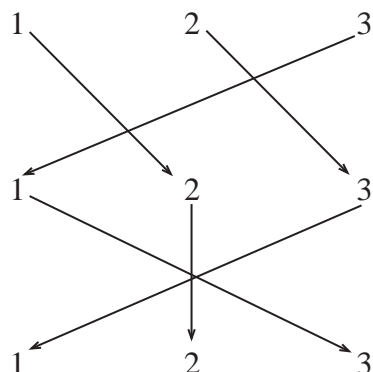
Thus the second permutation above can be written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

and the fifth as

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We can see how to multiply these permutations by drawing a diagram:



We then deduce that

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Note that we write the permutation that is to be applied first on the **right**. This is because we have thought of permutations as functions and by a composite  $fg$  of functions  $f$  and  $g$ , we usually mean ‘first apply  $g$  then apply  $f$ ’.

Similarly, we can calculate that

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

As you can see, this is not a very efficient way to describe permutations. We are writing the top row of the permutation in the same way every time. So we adopt a new notation, called **cycle notation**:

**Example:** Let  $S = \{1, 2, 3, 4, 5\}$ . The permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

acts on  $S$  as shown below:



So  $S$  breaks up into two ‘cycles’ when  $f$  is applied:  $1 \rightarrow 3 \rightarrow 5 \rightarrow 1$  and  $2 \rightarrow 4 \rightarrow 2$ . In *cycle notation* we write:

$$f = (135)(24).$$

In general we describe each permutation as follows:

- (1) Open a left parenthesis;
- (2) write any element of the set;
- (3) after each element write its image under the permutation;
- (4) when you would write an element that has been written before, don't—but write a right parenthesis;
- (5) if there are any elements of the set left unwritten, start again from step 1.

So, for example,  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$  is written as  $(132)(4)$ . We can recover the long form easily enough from the new short form if we need it. Note that the last element before a right parenthesis must be sent to the first element after the previous left parenthesis; in the above example, 2 is sent to 1, for example.

Some more examples

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 7 & 5 & 6 \end{pmatrix} \quad \text{is represented by } (1342)(576)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix} \quad \text{is represented by } (1234567)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 6 & 5 & 7 \end{pmatrix} \quad \text{is represented by } (12)(34)(56)(7)$$

Each string inside a set of parentheses is known as a cycle. In the representation of a permutation, no element of the set can appear in more than one of these cycles. This way of writing permutations is known as expressing them as a *product of disjoint cycles*.

**Note:** Cycle notation for a permutation is *not* unique, for example  $(123) = (231) = (312)$  all represent the permutation taking  $1 \rightarrow 2$ ,  $2 \rightarrow 3$  and  $3 \rightarrow 1$ .

It is not hard to see how to multiply permutations when they are expressed in this form. The main thing is to remember that we must work *from the right*. We then just trace through the images of successive elements and write them according to the rules above. For example

$$(1324)(567) * (143)(5)(267) = (1)(274)(3)(56) \text{ and } (123) * (321) = (1)(2)(3).$$

There is yet another convention that is often used to save space. There is really little difference between  $(123)$  and  $(123)(4)$  so we often omit the

letters that are fixed. With this convention the first product above would be  $(274)(56)$ . The second product above yields an evident problem which we solve by calling it  $(1)$  (rather than  $(\quad)$ ).

**Definition 2.2.3.** *The set of all permutations of the set  $\{1, \dots, n\}$ , together with the operation of composition of permutations, is called the symmetric group on  $n$  letters and is written  $S_n$ .*

Note that  $S_n$  has  $n!$  elements. In the new notation,  $S_3$  has the elements

$$(1), (123), (132), (12), (13), (23).$$

## 2.2.6 Exercises

- (1) Decide whether the following are groups:
  - (a) the set of positive real numbers with the operation of addition;
  - (b) the set of all  $n \times n$  matrices over the real numbers with the operation of addition;
  - (c) the set of all  $n \times n$  matrices over the real numbers with the operation of multiplication;
- (2) Show that the set of all rotations of the plane about a fixed centre  $P$ , together with the operation of composition of symmetries, form a group. What about all of the reflections for which the axis (or mirror) passes through  $P$ ?
- (3) Suppose that  $x$  and  $y$  are elements of a group. Show that there are elements  $w$  and  $z$  so that  $wx = y$  and  $xz = y$ . Show that  $w$  and  $z$  are unique. Must  $w$  be equal to  $z$ ?
- (4) Let  $n$  be a fixed natural number. Show that the set of complex numbers  $z$  which are  $n$ th roots of unity, that is which satisfy  $z^n = 1$ , together with multiplication of complex numbers, forms a group.
- (5) Show that the set of complex numbers  $z$  which are  $n$ th roots of unity for some (variable) natural number  $n$ , together with multiplication of complex numbers, forms a group.
- (6) Prove part (2) of Lemma 2.2.1.
- (7) Find the product of the following permutations:
  - (a)  $(123)(456) * (134)(25)(6)$ ;

(b)  $(12345) * (1234567)$ ;

(c)  $(123456) * (123) * (123) * (1)$ .

(8) Set  $X = \mathbb{R} \setminus \{0, 1\}$ . Show the following set of functions  $X \rightarrow X$ , together with the operation of composition, form a group.

$$\begin{array}{lll} f(x) = \frac{1}{1-x} & g(x) = \frac{x-1}{x} & h(x) = \frac{1}{x} \\ i(x) = x & j(x) = 1-x & k(x) = \frac{x}{x-1} \end{array}.$$

(9) (Harder) Describe the product of a rotation of the plane with a translation. Describe the product of two (planar) rotations about different axes.

## 2.3 Group discussion; some terminology for groups

### 2.3.1 Subgroups

In a number of the examples of groups given above, the underlying set of one group is a subset of the other and they use the same operation. Such groups are clearly very closely allied.

**Definition 2.3.1.** *A subset  $H$  of a group  $G$  is a subgroup if it is a group in its own right, using the operation of  $G$  restricted to  $H$ . We often write this  $H \leq G$ .*

If we know that  $G$  is a group, then the checking that  $H$  is a subgroup is made somewhat easier than usual. For example, we do not need to check that the operation is associative. In fact, we have the following.

**Lemma 2.3.1.** *Let  $(G, *)$  be a group and let  $H$  be a non-empty subset of  $G$ . Then the following are equivalent:*

- (1)  $H$  is a subgroup;
- (2)  $H$  is closed under  $*$  and inversion: for all  $h_1, h_2 \in H$  we have  $h_1 * h_2 \in H$  and  $h_1^{-1} \in H$ ;
- (3) for all  $h_1, h_2 \in H$  we have  $h_1 * h_2^{-1} \in H$ .

*Proof.* We shall prove this by showing that (1) implies (2), that (2) implies (3) and that (3) implies (1).

It is clear from the definition of subgroup that (1) implies (2). It is not too hard to show that (2) implies (3). The real work is to show that (3) implies (1).

Suppose that (3) is true. Since  $H$  is non-empty it contains some element  $h$ . Setting  $h_1 = h_2 = h$  we deduce that  $e_G = h * h^{-1} \in H$ . Now, if  $k \in H$ , then setting  $h_1 = e_G$  and  $h_2 = k$  we deduce that  $k^{-1} \in H$ . Finally, if  $k_1, k_2 \in H$  then  $k_2^{-1} \in H$  and setting  $h_1 = k_1$  and  $h_2 = k_2^{-1}$ , we deduce that  $k_1 * k_2 \in H$ .

Thus the operation  $*$ , when restricted to  $H$ , gives a well-defined operation. The operation is associative since it is the same as that used for  $G$ . The identity element  $e_G$  of  $G$  lies in  $H$  and is an identity element for the restriction of  $*$  to  $H$ . Finally each element of  $H$  has an inverse, in  $H$ , with respect to the restriction of  $*$  to  $H$ . Thus  $H$ , together with the restriction of  $*$  to  $H$ , forms a group. That is,  $H$  is a subgroup of  $G$ .  $\square$

### Examples:

- (1) The set  $2\mathbb{Z}$  of even integers is a subgroup of the group  $\mathbb{Z}$ .
- (2) The set  $\{e_G\}$  is always a subgroup of  $G$ ;  $G$  is always a subgroup of  $G$ .
- (3) The subset  $\{(1), (123), (132)\}$  is a subgroup of  $S_3$ .
- (4)  $SL(n, F)$  is a subgroup of  $GL(n, F)$ ; in fact all the groups defined in the sub-section on matrix groups are subgroups of the appropriate  $GL(n, F)$ .
- (5) Take any group of symmetries of a geometrical object, for example the group  $D_6$  of a regular hexagon. Colour the edges of the hexagon in some way. Then the set of symmetries which preserve the colours of the edges is a subgroup of  $D_6$ .
- (6) The set of negative integers is **not** a subgroup of  $\mathbb{Z}$ .
- (7) The set  $\{(1), (12), (23), (13)\}$  is **not** a subgroup of  $S_3$ .
- (8) The set of all rotations form a subgroup of  $D_n$ ; the set of all reflections do **not**.
- (9) Let  $G$  be any group,  $g \in G$  any element of  $G$ . Then the set  $\{g^n : n \in \mathbb{Z}\}$  is a subgroup of  $G$ .

The last example is sufficiently important that we devote a whole sub-section to it.

### 2.3.2 Cyclic subgroups

Using the associative law and induction it can be shown that the product of group elements  $g_1, g_2, \dots, g_n$  (in this order) does not depend on how parentheses are inserted. So we can write the product as  $g_1 g_2 \dots g_n$ .

In particular for any element  $g$  of a group, we can define  $g^n$  to be the product of  $n$  copies of  $g$  for  $n = 1, 2, 3, \dots$ . We also define  $g^0 = e$  and  $g^{-n} = (g^{-1})^n$  for  $n = 1, 2, 3, \dots$ .

**Properties of powers in a group:** For all  $n, m \in \mathbb{Z}$ :

(a)  $g^{-n} = (g^n)^{-1}$

(b)  $g^n g^m = g^{n+m}$

(c)  $(g^m)^n = g^{mn}$

We leave this as an exercise.

**Lemma 2.3.2.** *Let  $G$  be a group and  $g \in G$ . The set  $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$  is a subgroup, called the cyclic subgroup generated by  $g$ .*

*Proof.*  $\langle g \rangle$  is closed under the group operation by property (b), and is closed under inversion by property (a) above.  $\square$

For groups with operation  $+$ , we write  $mg$  instead of  $g^m$ . Then  $\langle g \rangle = \{mg : m \in \mathbb{Z}\}$ .

**Definition 2.3.2.** *A group  $G$  is called cyclic if it is equal to one of its cyclic subgroups, i.e.  $G = \langle g \rangle$  for some element  $g \in G$ .*

**Examples:**

(1)  $\mathbb{Z}$  is cyclic;  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ .

(2)  $\mathbb{Z}_n$  is cyclic;  $\mathbb{Z}_n = \langle \bar{1} \rangle$ .

(3) The subgroup  $\{(1), (123), (132)\}$  is cyclic; it equals  $\langle (132) \rangle$ .

(4) The group  $S_3$  is **not** cyclic.

**Definition 2.3.3.** *The order of a group  $G$  is the number of elements in  $G$ . This is written  $|G|$ .*

**Examples:**

- (1)  $|\mathbb{Z}_n| = n$ ,  $|S_n| = n!$ ,  $|D_n| = 2n$ .
- (2)  $|\mathbb{Z}| = \infty$  or “ $\mathbb{Z}$  has infinite order”.

**Definition 2.3.4.** *The order of an element  $g$  of a group  $G$  is the number of elements in the cyclic subgroup  $\langle g \rangle$  that it generates; that is,  $|\langle g \rangle|$ . It is usually written  $|g|$ .*

If  $\langle g \rangle$  is infinite, as is the case with  $1 \in \mathbb{Z}$  for example, we say that  $g$  has infinite order.

**Examples:**

- (1) In  $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ ,  $[0]_4$  has order 1,  $[1]_4$  has order 4,  $[2]_4$  has order 2 and  $[3]_4$  has order 4.
- (2) In  $S_3 = \{(1), (123), (132), (12), (13), (23)\}$ ,  $(1)$  has order 1;  $(123)$  and  $(132)$  have order 3;  $(12)$ ,  $(13)$ ,  $(23)$  have order 2. In particular,  $S_3$  contains no element of order 6, so is not a cyclic group.

**Lemma 2.3.3.** *Let  $g$  be an element of a group  $G$ .*

- (1) *If  $|g|$  is infinite then  $g^m = g^n$  only if  $m = n$ .*
- (2) *If  $|g|$  is finite, say  $|g| = k$ , then  $g^m = g^n$  if and only if  $m \equiv n \pmod{k}$ . In particular,  $|g|$  is the least positive integer so that  $g^k = e_G$ .*

*Proof.* Suppose that  $g^m = g^n$  for some  $m \neq n$ . Then  $g^{m-n} = g^m(g^n)^{-1} = e_G$  and so some non-zero power of  $g$  is the identity. Let  $k$  be the least positive integer such that  $g^k = e_G$ . Using the usual division with remainder of integers, we can write  $(m-n) = qk + r$  with  $q, r \in \mathbb{Z}$  and  $0 \leq r < k$ . Then

$$g^r = g^{(m-n)-qk} = g^{m-n}(g^k)^{-q} = e_G(e_G)^{-q} = e_G.$$

This will contradict the choice of  $k$  as the least positive power of  $g$  which is equal to  $e_G$  unless  $r = 0$ . But then  $m-n$  is a multiple of  $k$ .

In summary, we have shown that if  $g^m = g^n$  for some  $m \neq n$  then  $m \equiv n \pmod{k}$ . It is easy to check that the converse is true; that is, if  $k$  is least such that  $g^k = 1$  and if  $m \equiv n \pmod{k}$  then  $g^m = g^n$ . It follows that the order of  $g$  is  $k$ .

If  $|g|$  is infinite, it follows that  $g^m \neq g^n$  whenever  $m \neq n$  which proves (1). If  $|g|$  is finite, then the proof of (2) follows immediately from what we have done above.  $\square$

**Note:** From part (2) above, the **order** of an element  $g$  is equal to the **least positive integer  $k$  so that  $g^k = e_G$ .**

Subgroups of cyclic groups are particularly easy to understand:

**Lemma 2.3.4.** *Every subgroup of a cyclic group is again cyclic.*

*Proof.* Let  $G = \langle g \rangle$  be a cyclic group and let  $H$  be a subgroup of  $G$ . If  $H = \langle e_G \rangle$  then there is nothing to prove. Suppose therefore that  $H$  contains some element other than the identity. Since  $G$  consists of powers of  $g$ , so also must  $H$ . Let  $g^m$  be the smallest positive power of  $g$  which lies in  $H$ ; we claim that  $H = \langle g^m \rangle$ .

Suppose that  $g^n \in H$ . Use the Euclidean algorithm to write  $n = qm + r$  with  $0 \leq r < m$ . Then  $g^m \in H$  implies  $(g^m)^q = g^{qm} \in H$ . But  $g^n \in H$  and so  $g^n(g^{qm})^{-1} \in H$ . But  $g^n(g^{qm})^{-1} = g^{n-qm} = g^r$  and so  $g^r \in H$ . But  $r$  is positive or zero and  $g^m$  was the smallest positive power of  $g$  lying in  $H$ . Thus  $r$  must be zero. So  $n = qm$  and so  $g^n = (g^m)^q \in \langle g^m \rangle$ . Since  $g^n$  was an arbitrary element of  $H$ , it follows that  $H = \langle g^m \rangle$ .  $\square$

**Definition 2.3.5.** *A group  $G$  is commutative or abelian if  $gh = hg$  for all elements  $g, h$  of  $G$ .*

For example,  $\mathbb{Z}$  is commutative but  $GL(n, F)$  is not when  $n > 1$ . Cyclic groups are commutative.

**Definition 2.3.6.** *Suppose that  $g_1, \dots, g_k$  are elements of a group  $G$ . Then  $\langle g_1, \dots, g_k \rangle$  denotes the smallest subgroup of  $G$  containing  $g_1, \dots, g_k$ . We also say that  $\langle g_1, \dots, g_k \rangle$  is the subgroup generated by  $g_1, \dots, g_k$ . (In fact this consists of all possible products  $g_{i_1}^{n_1} g_{i_2}^{n_2} \dots g_{i_m}^{n_m}$  of powers of  $g_1, \dots, g_k$ .)*

Note that ‘subgroup generated by’ is similar to ‘subspace spanned by’ in vector spaces.

### 2.3.3 Isomorphism

In discussing groups, we are interested only in the operation on the set, not in the names given to the elements. There are many groups of order 2, for example  $\mathbb{Z}_2$ , the subgroup  $\langle (12) \rangle$  of  $S_3$ , the subgroup  $\langle r \rangle$  generated by a reflection  $r$  in  $D_6$ , the subgroup  $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$  of  $GL(2, \mathbb{R})$  are all of order 2. However we saw in section 2.2.4 that they all have essentially the same multiplication table:

|       |       |       |
|-------|-------|-------|
| *     | $e_G$ | $g$   |
| $e_G$ | $e_G$ | $g$   |
| $g$   | $g$   | $e_G$ |

We do not want to distinguish between groups which have, after relabelling, the same multiplication table. We can make this formal as follows.

**Definition 2.3.7.** An isomorphism between groups  $G$  and  $H$  is a bijection (1-1 and onto function)  $f : G \rightarrow H$  such that

$$f(g_1 *_G g_2) = f(g_1) *_H f(g_2)$$

for all elements  $g_1, g_2 \in G$ . If there is an isomorphism between  $G$  and  $H$  we say that  $G$  and  $H$  are isomorphic and write  $G \cong H$ .

Literally, isomorphic groups have ‘the same shape’. After possible relabelling, they will have the same multiplication table.

**Example:** In section 2.2.4 we showed that:

- (a) all groups of order 2 are isomorphic, and
- (b) all groups of order 3 are isomorphic.

**Lemma 2.3.5.** A cyclic group is isomorphic to either  $\mathbb{Z}$  or to  $\mathbb{Z}_n$  for some  $n \geq 1$ .

*Proof.* Let  $G = \langle g \rangle$  be a cyclic group. If  $G$  has infinite order, define a function  $f : \mathbb{Z} \rightarrow G$  by  $f(m) = g^m$ . Part (1) of Lemma 2.3.3 shows that  $f$  is injective. The definition of cyclic group and the notation  $G = \langle g \rangle$  show that  $f$  is surjective. Finally, the fact that  $f$  is an isomorphism simply comes from the fact that  $g^{m+n} = g^m * g^n$ .

If  $G$  has finite order  $k$  the argument is very similar. This time we define  $f$  by  $f : \mathbb{Z}_k \rightarrow G$  by  $f([m]_k) = g^m$ . The extra step in this argument is to show that  $f$  is well-defined. That is, we must show that if  $[m]_k = [n]_k$  then  $g^m = g^n$ . But this follows from (2) of 2.3.3.  $\square$

The following lemma gives some useful some properties of isomorphisms.

**Lemma 2.3.6.** Let  $f : G \rightarrow H$  be an isomorphism between groups. Then

- (1) If  $e_G$  is the identity in  $G$ , then  $f(e_G) = e_H$  is the identity in  $H$ .
- (2) If  $g \in G$ , then  $f(g^{-1}) = f(g)^{-1}$ .
- (3) If  $g \in G$ , then  $|g| = |f(g)|$ .

*Proof.* Exercise 12. □

Isomorphic groups must clearly have the same order. They must also have the same ‘properties of multiplication’. For example, if one of a pair of isomorphic groups is commutative, so must be the other. If one has an element of order 29, so must the other. This is usually the first thing to consider when trying to show that two groups are non-isomorphic.

For example,  $S_3$  is not isomorphic to  $\mathbb{Z}_6$  since the latter is commutative but the former is not. The group  $D_2$  is not isomorphic to  $\mathbb{Z}_4$ ; both are commutative but the latter is cyclic whereas the former is not.

**Examples:**

- (1) What about  $D_3$  and  $S_3$ ? Both are non-commutative and non-cyclic. In fact they are isomorphic. We can set up the isomorphism geometrically. Consider  $D_3$  as the symmetry group of an equilateral triangle  $\mathcal{T}$  and number the vertices with  $\{1, 2, 3\}$ . Each symmetry  $\sigma$  of  $\mathcal{T}$  permutes the vertices and so can be associated with a permutation  $f(\sigma)$  of  $\{1, 2, 3\}$ , that is an element of  $S_3$ . Once we know what  $\sigma$  does to the vertices of  $\mathcal{T}$ , we know what it does to all of  $\mathcal{T}$ . Thus  $f$  is an injective function. Since  $|D_3| = |S_3|$ ,  $f$  must be bijective. It is not difficult now to see that  $f$  must be an isomorphism.

In fact we can try the same sort of thing with  $D_n$  and  $S_n$  but can then only conclude that  $D_n$  is isomorphic to a subgroup of  $S_n$ . We cannot expect  $D_n$  and  $S_n$  to be isomorphic for  $n > 3$  since they have different orders.

- (2) Consider the group  $\mathbb{R}$  of real numbers under addition and the group  $\mathbb{R}_{>0}$  of positive real numbers with multiplication. We claim that they are isomorphic.

The function

$$\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$$

is bijective and  $\exp(a+b) = \exp(a)\exp(b)$  shows that  $\exp$  is an isomorphism.

In general it can be very difficult to decide whether two groups are isomorphic or not — see exercise 15 for some harder examples.

### 2.3.4 Products of groups

There is an easy way to combine groups to produce new groups.

**Definition 2.3.8.** Let  $G_1, G_2$  be groups. Then the direct product  $G_1 \times G_2$  is the group of ordered pairs

$$\{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

with operation:

$$(g_1, g_2) * (h_1, h_2) = (g_1 *_{G_1} h_1, g_2 *_{G_2} h_2)$$

for all  $g_1, h_1 \in G_1$  and  $g_2, h_2 \in G_2$ .

It is easy to check that this defines a *group*:

- (0)  $G_1 \times G_2$  is closed under  $*$  since  $G_1, G_2$  are closed under their operations.
- (1)  $(e_{G_1}, e_{G_2})$  is an identity element
- (2)  $(g_1, g_2)^{-1} = ((g_1^{-1}, g_2^{-1}))$
- (3) the associative law in  $G_1 \times G_2$  follows from the fact that it holds in  $G_1$  and in  $G_2$ .

Note that:

- (1)  $|G_1 \times G_2| = |G_1| \cdot |G_2|$
- (2)  $G_1 \times G_2$  is abelian if  $G_1, G_2$  are abelian.

Similarly we can define the product

$$G_1 \times G_2 \times \dots \times G_n$$

of  $n$  groups.

**Examples:**

- (1) If  $C_2$  and  $C_3$  are cyclic groups of order 2 and 3, then  $C_2 \times C_3$  is a cyclic group of order 6.
- (2)  $\mathbb{Z}_2 \times \mathbb{Z}_2$  is a non-cyclic abelian group of order 4. It is isomorphic to the dihedral group  $D_2$ .
- (3)  $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$ , and  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  are *non-isomorphic* abelian groups of order 8.

**2.3.5 Exercises**

- (1) Find the order of the following elements
  - (a)  $(123)(4567)(89)$  in  $S_{10}$ ;
  - (b)  $(14)(23567)$  in  $S_7$ ;
  - (c) a reflection;
  - (d) a translation in the group of symmetries of a plane pattern;
  - (e) the elements  $[6]_{20}, [12]_{20}, [11]_{20}, [14]_{20}$  in the additive group of  $\mathbb{Z}_{20}$ ;
  - (f) the elements  $[2]_{13}, [12]_{13}, [8]_{13}$  in the multiplicative group of non-zero elements of  $\mathbb{Z}_{13}$ .
- (2) If  $g$  is an element of a group  $G$ , prove that the orders of  $g$  and  $g^{-1}$  are equal.
- (3) Show that, in a *commutative* group, the product of two elements of finite order again has finite order.
- (4) Can you find an example of two symmetries of finite order where the product is of infinite order?
- (5) Set
$$A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$
Show that  $A$  has order 3, that  $B$  has order 4 and that  $AB$  has infinite order.
- (6) Determine the possible orders of elements in the dihedral group  $D_n$ .
- (7) If  $G$  is a group and  $(gh)^2 = g^2h^2$  for all  $g, h \in G$ , prove that  $G$  is commutative.
- (8) Decide whether the following are subgroups:
  - (a) the positive integers in the additive group of the integers;
  - (b) the set of all rotations in the group of symmetries of a plane tessellation;
  - (c) the set of all permutations which fix 1 in  $S_n$ .
- (9) List all of the subgroups of  $\mathbb{Z}_{12}$ .
- (10) If  $H$  is a subgroup of a group  $G$  and if  $g \in G$ , show that  $gHg^{-1} = \{ghg^{-1} : h \in H\}$  is a subgroup of  $G$ .

(11) If  $G$  is a group and  $g \in G$ , show that the function  $f : G \rightarrow G$  given by

$$f : h \mapsto ghg^{-1}$$

is an isomorphism from  $G$  onto itself.

(12) Prove lemma 2.3.6.

(13) Show that the matrix group  $SO(2)$  is isomorphic to the multiplicative group  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$  of complex number with modulus 1.

(14) (Harder) Show that  $D_m$  is isomorphic to a subgroup of  $D_n$  when  $m$  divides  $n$ .

(15) (Harder) Show that

- (a)  $(\mathbb{R}, +)$  and  $(\mathbb{R}^*, \times)$  are not isomorphic.
- (b)  $(\mathbb{Z}, +)$  and  $(\mathbb{Q}, +)$  are not isomorphic.
- (c) The additive group of rational numbers  $(\mathbb{Q}, +)$  is not isomorphic to the multiplicative group of positive rationals  $(\mathbb{Q}_{>0}, \times)$ .

## 2.4 Lagrange's Theorem

When we construct the 'integers modulo  $n$ ',  $\mathbb{Z}_n$ , we form the elements of  $\mathbb{Z}_n$  by identifying all integers which differ by a multiple of  $n$ . We can state this in more group-theoretical language. The set of multiples of  $n$  is a subgroup  $n\mathbb{Z}$  and we identify  $k$  and  $l$  if  $k - l \in n\mathbb{Z}$ . Alternatively, we identify all of the integers in  $k + n\mathbb{Z} = \{k + ns : s \in \mathbb{Z}\}$ . We are eventually going to make a similar construction with groups in general but firstly we are going to investigate subsets like  $k + n\mathbb{Z}$ .

### 2.4.1 Cosets

**Definition 2.4.1.** Let  $G$  be a group and let  $H$  be a subgroup of  $G$ . A right coset of  $H$  in  $G$  is any set of the form  $Hg = \{hg : h \in H\}$  for some  $g \in G$ . Similarly a left coset of  $H$  in  $G$  is a set of the form  $gH = \{gh : h \in H\}$  for some  $g \in G$ .

Note that  $H = H.e_G$  is always a coset of itself.

**Examples:**

- (1)  $G = \mathbb{Z}$ ;  $H = 2\mathbb{Z}$ . The cosets are  $2\mathbb{Z}$ , the even integers and  $1 + 2\mathbb{Z}$ , the odd integers.
- (2)  $G = D_n$ ,  $H = C_n$  the subgroup of rotations in  $D_n$ . The cosets are  $H$  itself and  $Hg$  where  $g$  is any reflection. Thus  $Hg$  is just the set of reflections in  $G$ .
- (3)  $G = S_3$ ,  $H = \langle(123)\rangle$ . The cosets are  $\{(1), (123), (132)\}$ ,  $\{(12), (23), (13)\}$ .
- (4)  $G = S_3$ ,  $H = \langle(12)\rangle$ . The cosets are  $\{(1), (12)\}$ ,  $\{(123), (23)\}$ ,  $\{(132), (13)\}$ .
- (5)  $G = GL(2, \mathbb{R})$ ,  $H = SL(2, \mathbb{R})$ . The coset  $H \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$  is just the set of all matrices of determinant  $a$  in  $GL(2, \mathbb{R})$ .

Notice that in these examples, the distinct cosets of  $H$  fill up  $G$ , are disjoint, and have the same number of elements as  $H$ . In fact this always happens.

**Lemma 2.4.1.** *Let  $G$  be a group and  $H$  be a subgroup of  $G$ .*

- (1) *If  $a, b \in G$ , then  $Ha = Hb$  if and only if  $ab^{-1} \in H$ .*
- (2) *Each element of  $G$  lies in exactly one coset of  $H$ .*
- (3) *The function  $Ha \rightarrow Hb$  given by  $ha \mapsto hb$  for  $h \in H$  is a bijection between  $Ha$  and  $Hb$ .*

(Similarly for left cosets.)

*Proof.* (1) If  $Ha = Hb$  then  $a = e_G a \in Ha = Hb$  and so  $a = hb$  for some  $h \in H$ . Thus  $h = ab^{-1} \in H$ . Conversely, if  $ab^{-1} = h \in H$  then  $a = hb$  and so, if  $k \in H$ , then  $ka = khb \in Hb$  as  $kh \in H$ . So  $Ha \subseteq Hb$ . For the reverse inclusion (that  $Hb \subseteq Ha$ ) note that  $ba^{-1} = (ab^{-1})^{-1} \in H$  and so we can repeat the previous argument, reversing the roles of  $a$  and  $b$ .

(2) Since  $g \in Hg$  it is clear that every element of  $G$  lies in at least one coset of  $H$ . Suppose that  $g \in Ha$  and  $g \in Hb$ . Then  $g = h_1 a$  and  $g = h_2 b$  for some  $h_1$  and  $h_2$  in  $H$ . So  $ga^{-1} \in H$  and  $gb^{-1} \in H$ . Thus  $(ga^{-1})^{-1} gb^{-1} = ab^{-1} \in H$ . By the first part of the lemma,  $Ha = Hb$  and so the ‘two’ cosets in which  $g$  lies are in fact the same.

(3) Firstly note that each element of  $Ha$  can be expressed *uniquely* in the form  $ha$  with  $h \in H$ . So the function is well defined. The fact that it has an inverse given by  $hb \mapsto ha$  shows that it is a bijection.  $\square$

**Definition 2.4.2.** Let  $G$  be a group and  $H$  a subgroup of  $G$ . The number of different cosets of  $H$  in  $G$  is called the index of  $H$  in  $G$ . It is often written  $|G : H|$ .

**Examples:** In the previous examples:

- (1)  $|\mathbb{Z} : 2\mathbb{Z}| = 2$ ,
- (2)  $|D_n : C_n| = 2$ ,
- (3)  $|S_3 : \langle(123)\rangle| = 2$ ,
- (4)  $|S_3 : \langle(12)\rangle| = 3$ ,
- (5)  $|GL(2, \mathbb{R}) : SL(2, \mathbb{R})| = \infty$ .

## 2.4.2 The Theorem

Next we will look at one of the oldest and most important results about finite groups.

**Theorem 2.4.2 (Lagrange's Theorem).** Let  $G$  be a group of finite order and let  $H$  be a subgroup of  $G$ . Then  $|H|$  divides  $|G|$ . If  $g \in G$  then  $|g|$  divides  $|G|$ .

*Proof.* Firstly note that the second sentence follows easily from the first because  $|g| = |\langle g \rangle|$  and  $\langle g \rangle$  is a subgroup of  $G$ .

By part (2) of Lemma 2.4.1, we can write  $G$  as a non-overlapping union of cosets of  $H$ . By part (3) of Lemma 2.4.1 all cosets have the same order which is therefore also the order of  $H$ . So

$$|G| = |G : H||H|$$

and the theorem follows. □

An immediate consequence is the following.

**Corollary 2.4.3.** If  $G$  is a finite group with  $|G| = n$ , then  $g^n = e$  for all  $g \in G$ .

*Proof.* Let  $|g| = k$ . Then  $k$  divides  $|G| = n$ , so  $n = km$  for some integer  $m$ . Thus

$$g^n = g^{km} = (g^k)^m = e^m = e.$$

□

### 2.4.3 Some applications

One easy application is the following famous result from Number Theory.

**Theorem 2.4.4 (Fermat’s Little Theorem).** *Let  $p$  be a prime number. If  $a$  is any integer which is not a multiple of  $p$ , then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Proof.* The non-zero elements of  $\mathbb{Z}_p$  form a group,  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$ , under multiplication. This follows from the fact, proved at the beginning of the Linear Algebra chapter, that  $\mathbb{Z}_p$  is a field.

The order of the group  $\mathbb{Z}_p^*$  is  $p - 1$ . If  $a$  is any integer which is not a multiple of  $p$  then  $[a]_p \neq [0]_p$  and so  $[a]_p \in \mathbb{Z}_p^*$ . Hence, by the last Corollary,  $[a^{p-1}]_p = [a]_p^{p-1} = [1]_p$  in  $\mathbb{Z}_p^*$ . Thus  $a^{p-1} \equiv 1 \pmod{p}$ , as required.  $\square$

**Remark:** One surprising application of Fermat’s little theorem is to *cryptography* — it is the basis for the “RSA” public key cryptosystem.

Lagrange’s theorem is also important for classifying finite groups. For example:

**Theorem 2.4.5.** *Let  $p$  be a prime number. Then every group of order  $p$  is cyclic, so isomorphic to  $(\mathbb{Z}_p, +)$ .*

*Proof.* Let  $G$  be a group of order  $p$  and choose  $g \in G$  with  $g \neq e_G$ . Then  $\langle g \rangle$  is a subgroup of  $G$  and so  $|\langle g \rangle|$  divides  $|G| = p$ . Since  $p$  is prime,  $|\langle g \rangle| = 1$  or  $|\langle g \rangle| = p$ . Since  $g \neq e_G$  we cannot have only one element in  $\langle g \rangle$  and so  $|\langle g \rangle| = p$ . But then every element of  $G$  is in  $\langle g \rangle$  and so  $G = \langle g \rangle$ ; that is,  $G$  is cyclic.  $\square$

### 2.4.4 Exercises

- (1) If  $H$  and  $K$  are subgroups of a group  $G$  and if  $|H| = 7$  and  $|K| = 29$ , show that  $H \cap K = \{e_G\}$ .
- (2) Let  $G$  be the subgroup of  $GL(2, \mathbb{R})$  of the form

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}; x, y \in \mathbb{R}, x > 0 \right\}.$$

Let  $H$  be the subgroup of  $G$  defined by

$$H = \left\{ \begin{bmatrix} z & 0 \\ 0 & 1 \end{bmatrix}; z \in \mathbb{R}, z > 0 \right\}.$$

Each element of  $G$  can be identified with a point  $(x, y)$  of the  $(x, y)$ -plane. Use this to describe the right cosets of  $H$  in  $G$  geometrically. Do the same for the left cosets of  $H$  in  $G$ .

- (3) Consider the set  $AX = B$  of linear equations, where  $X$  and  $B$  are column matrices,  $X$  is the matrix of unknowns and  $A$  the matrix of coefficients. Let  $W$  be the subspace (and so additive subgroup) of  $\mathbb{R}^n$  which is the set of solutions of the homogeneous equations  $AX = 0$ . Show that the set of solutions of  $AX = B$  is either empty or is a coset of  $W$  in the group  $\mathbb{R}^n$  with addition.
- (4) Let  $H$  be a subgroup of index 2 in a group  $G$ . If  $a, b \in G$  and  $a \notin H$  and  $b \notin H$ , show that  $ab \in H$ .
- (5) (Harder) Let  $H$  be a subgroup of a group  $G$  with the property that if  $a, b \in G$  and  $a \notin H$  and  $b \notin H$ , then  $ab \in H$ . Show that  $H$  has index 2 in  $G$ .
- (6) Let  $D_n$  denote the group of all symmetries of a regular  $n$ -gon. Let  $a$  denote a rotation through  $2\pi/n$  and let  $b$  denote a reflection. Show that

$$a^n = e, \quad b^2 = e, \quad bab^{-1} = a^{-1}.$$

Show that every element of  $D_n$  has a unique expression of the form  $a^i$  or  $a^i b$  where  $i \in \{0, 1, 2, \dots, n-1\}$ . (This exercise is designed to help with future questions which involve dihedral groups.)

- (7) Determine all subgroups of the dihedral group  $D_5$  (of order 10).
- (8) Determine all subgroups of the dihedral group  $D_4$  (of order 8) as follows:
- List the elements of  $D_4$  and hence find all of the cyclic subgroups.
  - Find two non-cyclic subgroups of order 4 in  $D_4$ .
  - Explain why any non-cyclic subgroup of  $D_4$ , other than  $D_4$  itself, must be of order 4 and, in fact, must be one of the two subgroups you have listed in the previous part.
- (9) Let  $G$  denote the group of rotational symmetries of a regular tetrahedron so that  $|G| = 12$ . Show that  $G$  has subgroups of order 1, 2, 3, 4 and 12. (Harder) Show that  $G$  has no subgroup of order 6.
- (10) Let  $G$  be a group of order 841 (which is  $(29)^2$ ). If  $G$  is not cyclic, show that every element  $g$  of  $G$  satisfies  $g^{29} = 1$ .

## 2.5 Quotient groups

When we introduced cosets, it was to mimic the process of ‘equivalence modulo  $n$ ’. This leads to a set  $\mathbb{Z}_n$ . But  $\mathbb{Z}_n$  has a natural addition inherited from  $\mathbb{Z}$ . We now want to see how we can mimic this in general.

Let  $G$  be a group and  $H$  a subgroup of  $G$ . A natural way to attempt to form a product of cosets  $Ha$  and  $Hb$  of  $H$  is to take their representatives and multiply them and then form the corresponding coset; that is, the product of  $Ha$  and  $Hb$  should be  $Hab$ . This is the way the addition of the integers is carried over to the addition of  $\mathbb{Z}_n$ .

There is a possible problem, however. Suppose that  $Ha = Hb$ . Then the product of  $Hc$  with  $Ha$  should equal the product of  $Hc$  with  $Hb$ . That is,  $Hca$  should equal  $Hcb$ . Using (1) of Lemma 2.4.1, we can re-interpret this as saying that

$$\text{if } ab^{-1} \in H \text{ then } (ca)(cb)^{-1} = c(ab^{-1})c^{-1} \in H.$$

For example, if  $b = e_G$  in the above, then we require that  $a \in H$  implies  $cac^{-1} \in H$  for all  $c \in G$ . But this is not true for every subgroup  $H$ . For example, take  $G = S_3$  and  $H = \{(1), (12)\}$ . Then  $(12) \in H$  but

$$(123)(12)(123)^{-1} = (123)(12)(132) = (123)(13) = (23) \notin H.$$

So we cannot expect to make sense of multiplying all cosets of  $H$  in this way. We need to restrict the sort of subgroups we are dealing with.

### 2.5.1 Normal subgroups

**Definition 2.5.1.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . We say that  $H$  is a normal subgroup of  $G$  if*

$$h \in H \text{ and } g \in G \text{ implies } ghg^{-1} \in H.$$

There are two other simple variations of this condition. We introduce some notation. If  $S$  and  $T$  are subgroups of a group  $G$  then  $ST$  denotes  $\{st : s \in S, t \in T\}$ . If  $S = \{s\}$  has only one element, we write  $sT$  rather than  $\{s\}T$ , and similarly. Thus the earlier notation for cosets fits into this notation.

**Lemma 2.5.1.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . The following are equivalent:*

- (1)  $H$  is a normal subgroup of  $G$ .

(2) for every  $g \in G$ ,  $Hg = gH$ .

(3) for every  $g \in G$ ,  $gHg^{-1} = H$ .

*Proof.* Suppose that (1) is true. Let  $k \in Hg$ . Then  $k = hg$  for some  $h \in H$ . Thus

$$k = hg = g(g^{-1}hg) = g(g^{-1}h(g^{-1})^{-1}) \in gH$$

as  $g^{-1}h(g^{-1})^{-1} \in H$  because  $H$  is a normal subgroup. Thus  $Hg \subseteq gH$ . Similarly,  $gH \subseteq Hg$  and so  $gH = Hg$ , proving that (2) holds.

Suppose now that (2) holds. Then

$$gHg^{-1} = (gH)g^{-1} = (Hg)g^{-1} = H$$

as  $gH = Hg$ . Thus (3) holds.

If (3) holds, it is easy to show that (1) holds.

□

### Examples:

- (1) The subgroup  $C_n$  of rotations in  $D_n$  is normal.
- (2) The subgroup  $\{(1), (123), (132)\}$  of  $S_3$  is a normal subgroup. The subgroup  $\{(1), (12)\}$  is not normal.
- (3)  $SL(n, F)$  is a normal subgroup of  $GL(n, F)$ .
- (4)  $\langle e_G \rangle$  and  $G$  are normal subgroups of  $G$ .
- (5) Every subgroup of a commutative group is normal.

Restricting ourselves to normal subgroups gets rid of at least some of the problems associated with taking products of cosets. To see that it works in all cases, we have the following result.

**Lemma 2.5.2.** *Let  $H$  be a normal subgroup of a group  $G$ . Then*

$$HaHb = Hab.$$

*Proof.*

$$HaHb = H(aHa^{-1})ab = HHab = Hab.$$

We have used the facts that  $aHa^{-1} = H$ , because  $H$  is normal, and that  $HH = H$  because  $H$  is a subgroup. □

### 2.5.2 Trivialising subgroups

We now want to complete the process of forming a new group of which the elements are the cosets of some subgroup.

**Definition 2.5.2.** Let  $G$  be a group and  $H$  a normal subgroup of  $G$ . Let  $G/H$  denote the set of right cosets of  $H$  in  $G$ . Define an operation  $\diamond$  on  $G/H$  by  $Ha \diamond Hb = HaHb$  (where  $HaHb$  is interpreted as a product of sets within  $G$ ).

**Theorem 2.5.3.** If  $H$  is a normal subgroup of  $G$ , then the set  $G/H$  with the operation ' $\diamond$ ' gives a group, called 'the quotient group of  $G$  by  $H$ '. The identity  $e_{G/H}$  is the coset  $H$  and the inverse of the coset  $Hg$  is  $Hg^{-1}$ .

*Proof.* By Lemma 2.5.2  $Ha \diamond Hb = HaHb$  is a coset and so the operation is well-defined. (Note that we did not need to use coset representatives to define it). The fact that it is associative is an easy deduction from the fact that the operation  $*$  of  $G$  is associative.

Observe that  $Ha \diamond H = H \diamond Ha = Ha$  and that  $Ha \diamond Ha^{-1} = Ha^{-1} \diamond Ha = H$  and this proves the claims of the last sentence.  $\square$

**Examples:**

(1)  $G = D_4 = \langle a, b : a^4 = 1, b^2 = 1, bab = a^{-1} \rangle, H = \langle a \rangle$

Since  $|G| = 8$  and  $|H| = 4$ , there are two cosets of  $H$  and so two elements in  $G/H$ . We can quickly identify these as  $H$  and  $Hb$ . The multiplication table is

|      |      |      |
|------|------|------|
|      | $H$  | $Hb$ |
| $H$  | $H$  | $Hb$ |
| $Hb$ | $Hb$ | $H$  |

(2)  $G = D_4 = \langle a, b : a^4 = 1, b^2 = 1, bab = a^{-1} \rangle, H = \langle a^2 \rangle$

In this case  $|H| = 2$  and so there are 4 cosets of  $H$ . They are

$$H = \{1, a^2\}, \quad Ha = \{a, a^3\}, \quad Hb = \{b, a^2b\}, \quad Hab = \{ab, a^3b\}.$$

Then we can calculate the multiplication table as

|       |       |       |       |       |
|-------|-------|-------|-------|-------|
|       | $H$   | $Ha$  | $Hb$  | $Hab$ |
| $H$   | $H$   | $Ha$  | $Hb$  | $Hab$ |
| $Ha$  | $Ha$  | $H$   | $Hab$ | $Hb$  |
| $Hb$  | $Hb$  | $Hab$ | $H$   | $Ha$  |
| $Hab$ | $Hab$ | $Hb$  | $Ha$  | $H$   |

The group is isomorphic to  $D_2$ .

- (3) A coset of  $SL(n, F)$  in  $GL(n, F)$  is the set of all matrices which have a given fixed determinant. When we multiply two cosets we obtain a coset corresponding to the product of these determinants. Thus there is one coset for each non-zero element of  $F$  and the product of cosets corresponds to the product of elements of  $F$ . Thus

$$GL(n, F)/SL(n, F) \cong (F \setminus \{0\}, \times)$$

where  $(F \setminus \{0\}, \times)$  is the group of all non-zero elements of  $F$  under the operation of multiplication. We will soon see an easier way to establish this.

### 2.5.3 Homomorphisms

There is an obvious function  $f$  from a group  $G$  to a quotient group  $G/H$  given by

$$f : g \longrightarrow Hg.$$

This function satisfies  $f(g * h) = f(g) \diamond f(h)$  and so looks rather like an isomorphism. But it is certainly not bijective because, for example, every element of  $H$  maps to a single element of  $G/H$ . We need a new definition.

**Definition 2.5.3.** *A homomorphism between groups  $G$  and  $H$  is a function  $f : G \rightarrow H$  such that*

$$f(a *_G b) = f(a) *_H f(b) \quad \text{for all } a, b \in G.$$

Thus homomorphisms are the functions between groups compatible with the group operations; these are analogous to linear transformations between vector spaces.

In particular, an isomorphism is just a bijective homomorphism.

#### Examples:

- (1) Let  $G$  be a group with a normal subgroup  $H$ . The function  $G \rightarrow G/H$  given by  $g \mapsto Hg$  is a homomorphism.
- (2) The function  $\det : GL(n, F) \rightarrow F \setminus \{0\}$  given by taking the determinant of a matrix is a homomorphism.
- (3) The function  $\mathbb{C} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$  given by  $z \mapsto |z|$  is a homomorphism.

Associated with any homomorphism there are two very natural subgroups.

**Definition 2.5.4.** Let  $f : G \rightarrow H$  be a homomorphism. Then

- (1)  $\{g \in G : f(g) = e_H\}$  is called the kernel of  $f$ , written  $\ker f$ .
- (2)  $\{f(g) : g \in G\}$  is called the image of  $f$ , written  $\operatorname{im} f$ .

**Lemma 2.5.4.** Let  $f : G \rightarrow H$  be a homomorphism. Then  $\ker f$  is a normal subgroup of  $G$  and  $\operatorname{im} f$  is a subgroup of  $H$ . Further,  $f$  is injective if and only if  $\ker f = \{e_G\}$ .

*Proof.* We leave the first part of this as Exercise 7. For the second part, observe firstly that if  $f$  is injective then at most one element of  $G$  can be taken, by  $f$ , to  $e_H$ . Since we know that  $f(e_G) = e_H$ , it follows that  $\ker f = \{e_G\}$ .

Suppose that  $\ker f = \{e_G\}$ ; we will show that  $f$  is injective. Let  $g_1$  and  $g_2$  be elements of  $G$  so that  $f(g_1) = f(g_2)$ . Then

$$f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_H.$$

Thus  $g_1g_2^{-1} \in \ker f = \{e_G\}$  and so  $g_1g_2^{-1} = e_G$ . Thus  $g_1 = g_2$  and so  $f$  is injective. □

**Lemma 2.5.5.** Let  $f : G \rightarrow G/H$  be the natural homomorphism given by  $f(g) = Hg$ . Then  $\ker f = H$  and  $\operatorname{im} f = G/H$ .

*Proof.* We leave this as Exercise 8. □

In this section so far we have started with normal subgroups, formed quotient groups, discovered a corresponding homomorphism and then re-discovered the original normal subgroup as the kernel of the homomorphism.

What if we start with a homomorphism from  $G$ ? It has a kernel which is a normal subgroup of  $G$ , we can form a quotient by this normal subgroup and then form a second homomorphism from  $G$  to the quotient group. How does this compare with the original homomorphism? In fact they are essentially the same.

**Theorem 2.5.6 (First Isomorphism Theorem).** Let  $f : G \rightarrow H$  be a homomorphism. Then

$$G/\ker f \cong \operatorname{im} f.$$

In particular, if  $f$  is surjective then  $G/\ker f \cong H$ .

*Proof.* For brevity, set  $\ker f = K$ . We attempt to define a function  $F : G/K \rightarrow \text{im } f$  by  $F(Kg) = f(g)$ . The possible problem with this attempt is that we may have  $Ka = Kb$  with  $a \neq b$ . It will not, in fact, be a problem if we know that  $Ka = Kb$  implies that  $f(a) = f(b)$ .

So suppose that  $Ka = Kb$ . By Lemma 2.4.1,  $ab^{-1} \in K$  and so  $f(ab^{-1}) = e_H$ . But then  $f(a)f(b)^{-1} = e_H$  and so  $f(a) = f(b)$ . Thus  $F$  is a well-defined function.

Now

$$F(Ka \diamond Kb) = F(Kab) = f(ab) = f(a)f(b) = F(Ka)F(Kb).$$

so  $F$  is a homomorphism.

Now,  $F(Kg) = e_H$  if and only if  $f(g) = e_H$  if and only if  $g \in K$  if and only if  $Kg = e_{G/K}$ . By Lemma 2.5.4,  $F$  is injective.

So  $F$  will be an isomorphism of  $G/K$  with the image of  $F$ . But we can easily check that  $\text{im } F = \text{im } f$  and so the proof is complete.  $\square$

### Examples:

- (1)  $\det : GL(n, F) \rightarrow F \setminus \{0\}$  is a homomorphism with kernel  $SL(n, F)$  (see Example 3 of Section 2.5.2). So  $SL(n, F)$  is a normal subgroup of  $GL(n, F)$  and

$$GL(n, F)/SL(n, F) \cong F \setminus \{0\}.$$

- (2) The function  $\mathbb{C} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$  given by  $z \mapsto |z|$  is a homomorphism with image  $\mathbb{R}_{>0}$  and kernel  $\{z : |z| = 1\}$ . Call the latter  $\mathbb{S}^1$  (because it is a ‘one-dimensional sphere’). Then

$$\frac{\mathbb{C} \setminus \{0\}}{\mathbb{S}^1} \cong \mathbb{R}_{>0}.$$

- (3) The function  $\mathbb{R} \rightarrow SO(2, \mathbb{R})$  which maps each real number  $a$  to the matrix representing the rotation, centered at the origin, through an angle of  $a$  can be checked to be a homomorphism. The function is surjective and its kernel is  $2\pi\mathbb{Z}$ , the subgroup of all integral multiples of  $2\pi$ . Thus we have

$$\mathbb{R}/2\pi\mathbb{Z} \cong SO(2, \mathbb{R}).$$

### 2.5.4 Exercises

- (1) Show that the set of matrices

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad \neq 0 \right\}$$

forms a subgroup of  $GL(2, \mathbb{R})$ . Show that the set of matrices

$$K = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\}$$

forms a normal subgroup of  $H$ .

- (2) If  $H$  is a subgroup, prove that  $HH = H$ .
- (3) If  $K$  and  $L$  are normal subgroups of a group  $G$ , show that  $K \cap L$  is also a normal subgroup of  $G$ .
- (4) Let  $G$  be a group and  $n$  a positive integer. If  $H$  is the only subgroup of  $G$  which has order  $n$ , show that  $H$  is a normal subgroup of  $G$ . (Hint: Use Exercise 10 of Section 2.3.)
- (5) Find all of the normal subgroups of  $D_4$ . (It will be a great help if you have done Exercise 8 of the previous section first.)
- (6) The *Quaternion* group  $Q_8$  is the subgroup of  $GL(2, \mathbb{C})$  consisting of the matrices  $\{\pm U, \pm I, \pm J, \pm K\}$  where

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

- (a) Verify that

$$I^2 = J^2 = K^2 = -U, \quad IJ = K, JK = I, KI = J$$

and so that these 8 elements do give a subgroup.

- (b) Find all of the cyclic subgroups of  $Q_8$ .
  - (c) Show that every subgroup of  $Q_8$ , except  $Q_8$  itself, is cyclic.
  - (d) Are  $Q_8$  and  $D_4$  isomorphic?
- (7) Prove the first part of Lemma 2.5.4.
  - (8) Prove Lemma 2.5.5.
  - (9) If  $G$  is an abelian group, show that any quotient  $G/N$  is also abelian.
  - (10) If  $G$  is a cyclic group, show that any quotient  $G/N$  is also cyclic.
  - (11) Show that the cyclic group of order 8 has as homomorphic images the cyclic groups of order 2 and 4 as well as itself and the trivial group.

- (12) Let  $\mathbb{R}$  denote the group of real numbers with the operation of addition and let  $\mathbb{Q}$  and  $\mathbb{Z}$  denote the subgroups of rational numbers and integers, respectively. Show that it is possible to regard  $\mathbb{Q}/\mathbb{Z}$  as a subgroup of  $\mathbb{R}/\mathbb{Z}$  and show that this subgroup consists exactly of the elements of finite order in  $\mathbb{R}/\mathbb{Z}$ .
- (13) Let  $H$  denote the subgroup of  $D_8 = \langle a, b \rangle$  generated by  $a^4$ . Write out the multiplication table of  $D_8/H$ .

## 2.6 Groups that can act

The importance of groups stems from the fact that they occur as ‘generalised symmetries’ of objects. This may occur in many ways apart from the more obvious geometrical ways. The common denominator is that the group will act as *permutations* of some set.

### 2.6.1 Definition and examples

**Definition 2.6.1.** An action of a group  $G$  on a set  $X$  is a function  $G \times X \rightarrow X$ , written  $(g, x) \mapsto g \cdot x$ , which combines elements  $g \in G$ ,  $x \in X$  to give an element  $g \cdot x \in X$  satisfying the properties:

- (a)  $e \cdot x = x$  for all  $x \in X$  where  $e$  is the identity in  $G$ ,
- (b)  $(gh) \cdot x = g \cdot (h \cdot x)$  for all  $g, h \in G$ ,  $x \in X$ .

We also call this a “ $G$ -action on  $X$ ”, and say that “ $G$  acts on  $X$ ”.

**Examples:**

- (1) Let  $G$  be *any* group of bijections  $g : X \rightarrow X$  with composition of functions as the operation. Then  $G$  acts on  $X$  by defining

$$g \cdot x = g(x) \text{ for all } g \in G, x \in X.$$

Many interesting examples arise in this way!

- (2)  $S_n$  acts on  $\{1, \dots, n\}$ .
- (3) The group of symmetries of a polygon  $P$  acts on  $P$ .
- (4)  $GL(n, F)$  acts on the vector space  $F^n$ .
- (5)  $GL(n, F)$  acts on the set of bases of the vector space  $F^n$ .

(6)  $GL(n, F)$  acts on the set of all subspaces of the vector space  $F^n$ .

**Another viewpoint:** Given any  $G$ -action on  $X$ , if we fix  $g \in G$  and let  $x \in X$  vary, then we obtain a function  $\phi(g) : X \rightarrow X$ , taking  $x \mapsto g \cdot x = \phi(g)(x)$ .

Then  $\phi(g)$  is a *permutation* of  $X$  (i.e. a bijection  $X \rightarrow X$ ) since it has an inverse  $\phi(g^{-1})$ : for all  $x \in X$

$$\phi(g^{-1})(\phi(g)(x)) = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = e \cdot x = x$$

using axioms (a) and (b) for a group action. Similarly  $\phi(g)(\phi(g^{-1})(x)) = x$  for all  $x \in X$ .

This gives a function  $\phi : G \rightarrow \text{Sym } X$  where  $\text{Sym } X$  is the group of all permutations of  $X$  furnished with the operation of composition. Further,  $\phi$  is a *homomorphism*, since

$$\phi(g_1 g_2)(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi(g_1)(\phi(g_2)(x))$$

for all  $x \in X$ , i.e.  $\phi(g_1 g_2) = \phi(g_1) \phi(g_2)$ .

Conversely, any homomorphism  $\phi : G \rightarrow \text{Sym } X$  gives a group action as defined above, with  $g \cdot x = \phi(g)(x)$ . (Exercise: check this.) Sometimes this is taken as the definition of a group action.

## 2.6.2 Orbits and stabilizers

**Definition 2.6.2.** Suppose that a group  $G$  acts on a set  $X$ .

(1) The orbit of  $x \in X$  is

$$G \cdot x = \{g \cdot x : g \in G\}.$$

It is a subset of  $X$ .

(2) The stabilizer of  $x \in X$  is

$$\text{Stab } x = G_x = \{g \in G : g \cdot x = x\}.$$

It is a subset of  $G$ , in fact a subgroup of  $G$ .

**Lemma 2.6.1.** Suppose that the group  $G$  acts on the set  $X$ . Then the stabilizer of  $x \in X$  is a subgroup of  $G$ .

*Proof.* Suppose that  $g, h \in \text{Stab } x$  so that  $g \cdot x = x$  and  $h \cdot x = x$ . Then  $h^{-1} \cdot h \cdot x = h^{-1} \cdot x$  and so  $x = e_G \cdot x = h^{-1} \cdot x$ . Thus

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$$

and so  $gh^{-1} \in \text{Stab } x$ . Thus  $\text{Stab } x$  is a subgroup of  $G$ .  $\square$

**Examples:**

- (1) Consider  $G = S_3$  acting on  $\{1, 2, 3\}$ . The stabilizer of 2 is  $\langle(13)\rangle$ ; the orbit of 2 is  $\{1, 2, 3\}$ .
- (2) Set  $G = \langle(12)\rangle$ , a subgroup of  $S_3$ . Then  $G$  acts on  $\{1, 2, 3\}$ . The orbit of 1 (or of 2) is  $\{1, 2\}$ . The orbit of 3 is  $\{3\}$ . The stabilizer of 1 or of 2 is the identity subgroup. The stabilizer of 3 is  $G$  itself.
- (3) Consider  $SO(2, \mathbb{R})$  acting on the plane  $\mathbb{R}^2$ . The orbit of any point is the circle, centered at the origin, which passes through that point. The stabilizer of any point, other than the origin, is the identity subgroup; the stabilizer of the origin is the whole group.
- (4) Consider  $SO(3, \mathbb{R})$  acting on  $\mathbb{R}^3$ . The orbit of any point is the sphere, centered at the origin, which passes through that point. The stabilizer of any point, other than the origin, is the set of rotations which have as axis the line passing through the origin and the chosen point.

**Lemma 2.6.2.** *Suppose that the group  $G$  acts on the set  $X$ . Then every element of  $X$  lies in one and only one orbit.*

*Proof.* Since  $x \in G \cdot x$ , every element of  $X$  lies in at least one orbit. Suppose that  $z \in G \cdot x$  and  $z \in G \cdot y$ ; we need to show that  $G \cdot x = G \cdot y$ ; it will follow that different orbits can contain no element in common.

Since  $z \in G \cdot x$  and  $z \in G \cdot y$ , we can write  $z = a \cdot x$  and  $z = b \cdot y$  for some  $a, b \in G$ . Let  $w$  be any element of  $G \cdot x$ , say  $w = g \cdot x$ . Then

$$w = g \cdot x = g \cdot (a^{-1}) \cdot z = (ga^{-1}) \cdot z = (ga^{-1}) \cdot (b \cdot y) = (ga^{-1}b) \cdot y \in G \cdot y.$$

Thus  $G \cdot x \subseteq G \cdot y$ . To show that  $G \cdot y \subseteq G \cdot x$  and so that  $G \cdot x = G \cdot y$ , just reverse the roles of  $x$  and  $y$  in this argument.  $\square$

Next we come to the key relationship between orbits and stabilizers.

**Theorem 2.6.3 (The Orbit-Stabilizer Relation).** *Suppose that the group  $G$  acts on the set  $X$ . Then, for each  $x \in X$ , there is a bijective correspondence between the (left) cosets of  $\text{Stab } x$  and the elements of the orbit  $G \cdot x$ . Thus the size of any orbit  $|G \cdot x|$  is equal to the index  $|G : \text{Stab}(x)|$  of the stabilizer  $\text{Stab}(x)$  in  $G$ .*

*In particular, if  $G$  is finite then*

$$|G| = |G \cdot x| \cdot |\text{Stab } x|,$$

*and so  $|G \cdot x|$  divides  $|G|$ .*



defines an action of the additive group of the real numbers on  $X$ . Give a geometrical description of the orbits.

- (3) Let  $G$  be the subgroup of  $S_{15}$  generated by the three permutations

$$(1, 12)(3, 10)(5, 13)(11, 15) \quad (2, 7)(4, 14)(6, 10)(9, 13) \\ (4, 8)(6, 10)(7, 12)(9, 11).$$

Find the orbits in  $S = \{1, \dots, 15\}$  under the action of  $G$ . Deduce that  $G$  has order which is a multiple of 60.

- (4) If a group  $G$  of order 5 acts on a set  $X$  with 11 elements, must there be an element of the set  $X$  which is left fixed by every element of the group  $G$ ? What if  $G$  has order 15 and  $X$  has 8 elements?

## 2.7 Groups acting on themselves

One of the most powerful techniques of finite group theory involves the consideration of groups acting on themselves. That is, the set  $X$  on which the group  $G$  acts is just the set of elements of  $G$ . We shall consider two examples and apply them to prove results about the groups themselves.

### 2.7.1 Left multiplication

Any group  $G$  acts on  $X = G$  by *left multiplication*:

$$g \cdot x = gx \text{ for all } g \in G, x \in X = G,$$

where the right hand side is group multiplication. This gives a group action since

- (a)  $e \cdot x = ex = x$   
 (b)  $(gh) \cdot x = (gh)x = g(hx) = g \cdot (h \cdot x)$ .

Similarly  $G$  acts on itself by *right multiplication*:  $g \cdot x = xg^{-1}$ . (Exercise.)

As usual, this group action gives us a homomorphism  $\alpha : G \rightarrow \text{Sym } G$ . This describes how left multiplication permutes the rows of the multiplication table for the group  $G$ :

**Example:** Consider the group  $D_2 = \langle a, b : a^2 = e, b^2 = e, ab = ba \rangle$  and the action by left multiplication. The group  $D_2$  has 4 elements  $\{e, a, b, ab\}$  and its multiplication table is:

|      | $e$  | $a$  | $b$  | $ab$ |
|------|------|------|------|------|
| $e$  | $e$  | $a$  | $b$  | $ab$ |
| $a$  | $a$  | $e$  | $ab$ | $b$  |
| $b$  | $b$  | $ab$ | $e$  | $a$  |
| $ab$ | $ab$ | $b$  | $a$  | $e$  |

Left multiplication permutes the group elements as follows:

$$\begin{aligned} \alpha(e) & \quad \text{the identity permutation} \\ \alpha(a) & \quad \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix} \\ \alpha(b) & \quad \begin{pmatrix} e & a & b & ab \\ b & ab & e & a \end{pmatrix} \\ \alpha(ab) & \quad \begin{pmatrix} e & a & b & ab \\ ab & b & a & e \end{pmatrix} \end{aligned}$$

If we wish, we could re-name the elements of  $D_2$  via  $(e, a, b, ab) \rightarrow (1, 2, 3, 4)$  and we would then have an isomorphism between  $D_2$  and a subgroup of  $S_4$ :

$$\begin{aligned} e & \rightarrow (1) & a & \rightarrow (12)(34) \\ b & \rightarrow (13)(24) & ab & \rightarrow (14)(23) \end{aligned}$$

The same method gives the following general result.

**Theorem 2.7.1 (Cayley's Theorem).** *Every group  $G$  is isomorphic to a subgroup of a permutation group. If  $G$  has finite order  $n$  then  $G$  is isomorphic to a subgroup of  $S_n$ .*

*Proof.* The action of  $G$  on itself by left multiplication gives a homomorphism  $\alpha : G \rightarrow \text{Sym } G$  where  $\alpha(g)(x) = g \cdot x = gx$ . We show that  $\alpha$  is injective (or 1-1) so that  $G$  is isomorphic to  $\text{im } \alpha$  which is a subgroup of the permutation group  $\text{Sym } G$ . If  $G$  has  $n$  elements then  $\text{Sym } G$  will be isomorphic to  $S_n$  so that the second sentence follows.

We need to show that  $\alpha$  is injective. Suppose that, for some  $a, b \in G$ ,  $\alpha(a) = \alpha(b)$ . Then, for any  $x \in G$ ,  $\alpha(a)(x) = \alpha(b)(x)$ ; that is,  $ax = bx$ . But then  $a = b$  and so  $\alpha$  is injective.  $\square$

## 2.7.2 Conjugation

Each group  $G$  acts on itself by *conjugation*:

$$g \cdot x = gxg^{-1} \text{ for all } g \in G, x \in G.$$

This is a group action since

- (a)  $e \cdot x = exe^{-1} = x$
- (b)  $(gh) \cdot x = (gh)x(gh)^{-1} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} = g \cdot (h \cdot x)$ .

The case where a group acts on itself by conjugation has particular importance and acquires its own notation rather than the general notation of ‘orbit’ and ‘stabilizer’.

**Definition 2.7.1.** *Let  $G$  be a group, and let  $x \in G$ . Then*

- (1) *a conjugate of  $x$  is any element of the form  $gxg^{-1}$  where  $g \in G$ .*
- (2) *the conjugacy class of  $x$  is the set of all elements of  $G$  of the form  $gxg^{-1}$  for  $g \in G$ .*
- (3) *the centralizer of  $x$ , written  $C_G(x)$ , is the subgroup of  $G$  of all elements  $g$  satisfying  $gxg^{-1} = x$  or, equivalently,  $gx = xg$ .*

Observe that a conjugacy class is just an orbit and a centralizer is just a stabilizer when we consider  $G$  acting on itself by conjugation. Thus we can translate the orbit-stabilizer relation into this context.

**Theorem 2.7.2.** *Let  $G$  be a finite group. Then the number of elements in a conjugacy class is equal to the number of cosets of the centralizer of any element of the conjugacy class. Thus the number of conjugates of  $g \in G$  is  $|G|/|C_G(g)|$ , so divides  $|G|$ .*

**Examples:** We shall work out the conjugacy classes of  $G = D_4 = \langle a, b : a^4 = b^2 = e, bab^{-1} = a^{-1} \rangle$ .

Before we proceed with the details we mention briefly the general line of approach. We pick an element that we have not yet assigned to a conjugacy class. We note any obvious conjugates and so get a lower bound on the size of the conjugacy class. We then try to find elements in the centralizer of the element. This will give us a lower bound on the size of the centralizer and so, using Theorem 2.7.2, an upper bound on the size of the conjugacy class. With luck the lower and upper bounds on the size of the conjugacy class are

the same; if not, then we need to find more conjugates or more elements in the centralizer to refine our bounds.

Firstly,  $\{e\}$  is a conjugacy class.

Let us calculate the conjugacy class containing  $a$ . Observe that  $a \in C_G(a)$  and so  $\langle a \rangle \leq C_G(a)$ . Thus, as  $|\langle a \rangle| = 4$ ,  $C_G(a)$  has at least 4 elements. Thus it has at most  $8/4 = 2$  cosets. So the conjugacy class of  $a$  has at most 2 elements. The relation  $bab^{-1} = a^{-1}$  above tells us that  $a^{-1}$  is a conjugate of  $a$ . So this conjugacy class is  $\{a, a^{-1}\}$ . Note that  $a^{-1} = a^3$ .

We will now calculate the conjugacy class containing  $a^2$ . Observe that  $a \in C_G(a)$  and so  $\langle a \rangle \leq C_G(a)$ . Also,  $ba^2b^{-1} = (bab^{-1})(bab^{-1}) = (a^{-1})^2 = a^2$  and so  $b \in C_G(a)$ . Hence  $C_G(a^2) = G$  and the conjugacy class containing  $a^2$  has one element. So this conjugacy class is  $\{a^2\}$ .

We will now calculate the conjugacy class containing  $b$ . Observe that  $b \in C_G(b)$ . In the previous paragraph we showed that  $ba^2b^{-1} = a^2$  and so that  $ba^2 = a^2b$ . This also implies that  $a^2b(a^2)^{-1} = b$  and so  $a^2 \in C_G(b)$ . Thus  $C_G(b)$  contains at least two different non-identity elements and so must have order at least 4 (recall that its order must divide 8, by Lagrange's theorem). So the conjugacy class containing  $b$  can have at most 2 elements. Since

$$aba^{-1} = b^2aba^{-1}b^2 = b(bab^{-1})a^{-1} = b(a^{-1})a^{-1} = ba^{-2} = ba^2 = a^2b$$

we have that  $a^2b$  is a conjugate of  $b$ . So this conjugacy class is  $\{b, a^2b\}$ .

A similar argument shows that the final class is  $\{ab, a^3b\}$ .

Thus the conjugacy classes of  $D_4$  are

$$\{e\}, \{a^2\}, \{a, a^3\}, \{b, a^2b\}, \{ab, a^3b\}.$$

Note how little hard calculation we had to do in order to find these conjugacy classes.

### 2.7.3 Some consequences for group theory

The elements of the group which form a conjugacy class on their own clearly play a special role.

**Definition 2.7.2.** *Let  $G$  be a group. The centre of  $G$ , written  $Z(G)$ , is the set of elements  $x \in G$  such that  $gx = xg$  for all  $g \in G$ .*

**Examples:**

- (1) The centre of  $D_4$  is  $\{e, a^2\}$  (this needs some checking).
- (2) The element  $e_G$  always lies in the centre of  $G$ .
- (3) The centre of  $S_3$  is just  $\{(1)\}$  (this needs some checking).
- (4) The centre of  $GL(n, F)$  is the subgroup of scalar matrices  $\{aI : a \in F^*\}$  (this needs a lot of checking).

**Lemma 2.7.3.** *The centre of a group  $G$  is a normal subgroup of  $G$ .*

*Proof.* We leave this as Exercise 6. □

As we have seen, the centre of a group may contain only the identity element. But there is one case where we can guarantee that it contains more than this.

**Theorem 2.7.4.** *Let  $p$  be a prime and let  $G$  be a group of order  $p^n$  for some integer  $n \geq 1$ . Then the centre of  $G$  contains more than the identity element.*

*Proof.* Recall that in studying the centre, we are looking at elements which form a conjugacy class on their own.

Write  $G$  as a disjoint union of conjugacy classes:

$$G = C_1 \cup C_2 \cup \cdots \cup C_k$$

and recall that the size of each conjugacy class has order dividing  $|G|$ . Now group the one element conjugacy classes together to form the centre  $Z$ . Thus we have

$$G = Z \cup C_l \cup C_{l+1} \cup \cdots \cup C_k$$

where we have renamed the classes so that  $C_l, \dots, C_k$  are exactly the classes with more than one element. Thus, looking at sizes,

$$|G| = p^n = |Z| + |C_l| + |C_{l+1}| + \cdots + |C_k|.$$

But  $|C_l|, \dots, |C_k|$  are all divisors of  $|G|$  and are all bigger than one. Thus they are all powers of  $p$  and, in particular, are all multiples of  $p$ . Thus the equation becomes:  $p^n = |Z| + pm$  where  $|C_l| + \cdots + |C_k| = pm$ . So  $p$  divides  $|Z|$  and so  $|Z|$  must be bigger than 1. □

One application of this result is the following.

**Theorem 2.7.5.** *If  $p$  is prime, then every group of order  $p^2$  is isomorphic to  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$ .*

A proof is outlined in exercises 7,9 and 10.

We will finish this section with a partial converse to Lagrange's theorem. We know that the order of any element in a group  $G$  divides  $|G|$ , but if  $n$  divides  $|G|$  there may be no element of order  $n$  in  $G$ . However we have:

**Theorem 2.7.6 (Cauchy's Theorem).** *Let  $G$  be a finite group of order divisible by a prime number  $p$ . Then  $G$  has an element of order  $p$ .*

*Proof.* We need to find  $x \in G$ , with  $x \neq e$ , such that  $x^p = e$ .

Consider the set

$$X = \{(x_1, x_2, \dots, x_p) : x_i \in G, x_1 x_2 \dots x_p = e\},$$

i.e. all ordered  $p$ -tuples of elements in  $G$  whose product is the identity.

First we determine the size of  $X$ . We can choose *arbitrary* elements  $x_1, \dots, x_{p-1}$  from  $G$ . Then  $(x_1, \dots, x_{p-1}, x_p) \in X$  if and only if  $x_p = (x_1 \dots x_{p-1})^{-1}$ . Hence  $|X| = |G|^{p-1}$ . In particular,

$$p \text{ divides } |X|, \tag{1}$$

since  $p$  divides  $|G|$  and  $p - 1 \geq 1$ .

Now the group  $\mathbb{Z}_p$  acts on  $X$  by cyclically permuting the  $p$ -tuples: for  $m = 0, 1, \dots, p - 1$ , define

$$[m] \cdot (x_1, x_2, \dots, x_p) = (x_{m+1}, x_{m+2}, \dots, x_p, x_1, \dots, x_m).$$

Each orbit for this action has 1 or  $p$  elements, since the size of each orbit divides  $|\mathbb{Z}_p| = p$ . Clearly, the orbit of  $(e, e, \dots, e)$  has 1 element. If every other orbit has  $p$  elements then

$$|X| = \text{sum of orbit sizes}$$

would not be divisible by  $p$  contradicting (1).

Hence there is  $(x_1, x_2, \dots, x_p) \in X$  other than  $(e, e, \dots, e)$  which is *fixed* by every element of  $\mathbb{Z}_p$ . Then  $x_1 = x_2 = \dots = x_p = x \neq e$ , and  $x^p = e$ .  $\square$

This can be used to prove:

**Theorem 2.7.7.** *If  $p$  is an odd prime, then each group of order  $2p$  is isomorphic to the cyclic group  $C_{2p}$  or the dihedral group  $D_p$ .*

We leave this as exercise 12.

**2.7.4 Exercises**

- (1) Find the conjugacy classes in the quaternion group described in Exercise 6 of Section 2.5.
- (2) Find the conjugates of
  - (a)  $(123)$  in  $S_3$ ;
  - (b)  $(123)$  in  $S_4$ ;
  - (c)  $(1234)$  in  $S_4$ ;
  - (d)  $(1234)$  in  $S_n$  where  $n \geq 4$ ;
  - (e)  $(12 \dots m)$  in  $S_n$  where  $n \geq m$ .
- (3) (Harder) Let  $\tau$  be a permutation in  $S_n$ . Suppose that  $\sigma = (12 \dots k)$ . Show that  $\tau\sigma\tau^{-1} = (\tau(1)\tau(2) \dots \tau(k))$ . What is the result if  $\sigma$  is replaced by a general element of  $S_n$ ? Use this to describe the conjugacy classes of  $S_n$ .
- (4) Suppose that  $g$  and  $h$  are conjugate elements of a group  $G$ . Show that  $C_G(g)$  and  $C_G(h)$  are conjugate subgroups of  $G$ .
- (5) Determine the centralizer in  $GL(3, \mathbb{R})$  of the following matrices:

$$(a) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

$$(b) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$(c) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$(d) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$(e) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

- (6) Prove Lemma 2.7.3.
- (7) Suppose that  $G$  is a group with centre  $Z$  and so that  $G/Z$  is a cyclic group. Show that there must be an element  $h \in G$  so that every element of  $G$  can be written in the form  $g = h^n z$  with  $n \in \mathbb{Z}$  and  $z \in Z$ . Deduce that  $G$  is commutative.
- (8) Describe the finite groups with exactly one or exactly two or exactly three conjugacy classes (the last of these is harder).

- (9) If  $p$  is a prime, use Lemma 2.7.4 and Exercise 7 to show that a group of order  $p^2$  is commutative.
- (10) (Harder) If  $p$  is a prime, use the previous exercise to help show that each group of order  $p^2$  is isomorphic to either  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$ .
- (11) If  $p$  is a prime number, show that any group of order  $2p$  must have a subgroup of order  $p$  and that this subgroup must be normal.
- (12) Show that, up to isomorphism, there are two groups of order  $2p$  for every prime number  $p$ .

## 2.8 Keeping our distance; isometries

### 2.8.1 Definition and basic properties

We want to consider ‘symmetries’ of the standard Euclidean plane. To avoid confusion with the vector space  $\mathbb{R}^2$ , we shall denote the Euclidean plane by  $\mathbb{E}^2$ . The points of  $\mathbb{R}^2$  and of  $\mathbb{E}^2$  are the same but  $\mathbb{E}^2$  is a *geometric* object, equipped with the usual notions of distance and angle in Euclidean geometry. Further all points of  $\mathbb{E}^2$  are considered identical; there is no ‘origin’.

We begin with a precise version of what we mean by a ‘symmetry’.

**Definition 2.8.1.** *A function  $f : \mathbb{E}^2 \rightarrow \mathbb{E}^2$  is an isometry if, for any pair of points  $P, Q \in \mathbb{E}^2$ , we have  $|PQ| = |f(P)f(Q)|$ .*

Here  $|PQ|$  denotes the distance  $d(P, Q)$  between the points  $P$  and  $Q$ .

**Examples:**

- (1) A reflection in a line;
- (2) a rotation about a point;
- (3) a translation;
- (4) a glide reflection.

Since many of you may not know what the last is, here is a definition.

**Definition 2.8.2.** *A glide reflection is the combination of a translation followed by a reflection in an axis parallel to the direction of translation.*

**Lemma 2.8.1.** *If an isometry fixes two points, it fixes all points of the line on which they lie. If an isometry fixes three points which do not all lie on a line, then it fixes all of  $\mathbb{E}^2$ .*

*Proof.* The proof involves some elementary Euclidean geometry. For example, if a point lies on the line between two fixed points then it is uniquely determined by its distances from those two points, and so must also be fixed.. We leave the details to Exercise 7.  $\square$

We need some information about multiplication of different kinds of isometries. Once we have used this to establish Theorem 2.8.3, it will become easier to calculate the result of other combinations.

**Lemma 2.8.2.** (1) *Let  $\sigma_1$  and  $\sigma_2$  be reflections in axes  $L_1$  and  $L_2$ . The product  $\sigma_1\sigma_2$  is either,*

- (a) *a rotation about the point of intersection of  $L_1$  and  $L_2$ , with angle of rotation twice the angle between  $L_1$  and  $L_2$ , if  $L_1$  and  $L_2$  intersect;*
- (b) *a translation in a direction perpendicular to  $L_i$  with a magnitude equal to twice the distance between  $L_1$  and  $L_2$ , if  $L_1$  and  $L_2$  are parallel.*

(2) *The product of three reflections in parallel axes is a further reflection.*

(3) *The product of three reflections in axes which are not parallel and which do not intersect in a point is a glide reflection.*

*Proof.* Perhaps the easiest (but not the most elegant) way to do (1) and (2) is to choose co-ordinate axes suitably and to represent the reflections by specific functions of the co-ordinates. For example, to consider reflections in two parallel axes, choose co-ordinate axes so that one of the axes of reflection is the  $x$ -axis and the other is the line  $y = a$ . Then the two reflections are given by the functions

$$f : (x, y) \mapsto (x, -y) \quad \text{and} \quad g : (x, y) \mapsto (x, a/2 - y).$$

The composite  $g \circ f$  of these two functions is then the function  $(x, y) \mapsto (x, a/2 + y)$  which is easily seen to be a translation. We leave the rest of (1) and (2) as Exercise 8.

We turn to (3); call the product  $\rho_1\rho_2\rho_3$ . Consider the reflections  $\rho_2, \rho_3$ . If their axes are parallel, then this product is a translation  $\tau$  and we must consider  $\rho_1\tau$ . If their axes intersect, then the product of these two reflections is a rotation about the point of intersection  $P$  of the axes. But this rotation can be represented by any product of reflections which both have axes passing through  $P$  and lying at an angle which is the same as the angle between the two original axes. Thus we can replace  $\rho_2\rho_3$  by a product  $\rho'_2\rho'_3$  of reflections

so that the axis of  $\rho'_2$  is parallel to the axis of  $\rho_1$ . Then  $\rho_1\rho'_2$  is a translation  $\tau'$  and we must consider  $\tau'\rho_3$ .

Thus we must consider either a translation followed by a reflection or a reflection followed by a translation. The two cases are, not surprisingly, very similar, and we shall consider only the second. Choose axes so that the axis of the reflection is the  $y$ -axis. In co-ordinates the reflection is then given by  $(x, y) \mapsto (-x, y)$ . The translation will be of the form  $(x, y) \mapsto (a + x, b + y)$ . The composite is therefore

$$(x, y) \mapsto (-x, y) \mapsto (a - x, b + y).$$

But we can represent this composite in the form

$$(x, y) \mapsto (a - x, y) \mapsto (a - x, y) + (0, b)$$

which shows that it is the combination of a reflection  $(x, y) \mapsto (a - x, y)$  in the line  $x = a/2$  with a translation parallel to the  $y$  axis and so to the line of reflection. It is therefore a glide reflection. □

## 2.8.2 What isometries are there?

It is surprisingly easy to describe all isometries of the plane. We do it by looking at successively smaller sets of fixed points.

**Theorem 2.8.3.** *The set of fixed points of an isometry is one of the following:*

- (1) *All of  $\mathbb{E}^2$ ; in this case, the isometry is the identity.*
- (2) *A line in  $\mathbb{E}^2$ ; in this case, the isometry is the reflection in that line.*
- (3) *A single point; in this case, the isometry is a rotation about that point and can be expressed as the product of two reflections.*
- (4) *empty; in this case, the isometry is either a translation and can be expressed as the product of two reflections or a glide reflection and can be expressed as the product of three reflections.*

*Proof.* There is nothing to prove if the isometry  $\phi$  fixes all of  $\mathbb{E}^2$ . So suppose that it does not. Then, by Lemma 2.8.1, it must fix no more than a line of points. Suppose that it fixes exactly a line; call this line  $L$ . Let  $P, Q$  be points on  $L$  and let  $R$  be a point which is not on  $L$ . Then  $|RP| = |\phi(R)\phi(P)| = |\phi(R)P|$  and, similarly,  $|RQ| = |\phi(R)\phi(P)| = |\phi(R)Q|$ . A

little school geometry will now tell you that  $\phi(R)$  is either  $R$  or the reflection of  $R$  in  $L$ . We have assumed, however, that  $\phi$  fixes points only on  $L$  and so  $\phi(R) \neq R$ . Let  $\rho$  be the reflection in  $L$ . Then  $\phi(R) = \rho(R)$ . Thus  $\rho^{-1} \circ \phi$  fixes all of  $P, Q$  and  $R$ . By Lemma 2.8.1,  $\rho^{-1} \circ \phi$  fixes  $\mathbb{E}^2$  and so is the identity. Hence  $\phi = \rho$  and  $\phi$  is a reflection, as claimed.

Suppose now that  $\phi$  does not fix any line. By Lemma 2.8.1, it can fix no more than a point. Suppose that it fixes a point,  $P$  say. Let  $Q$  be any point different from  $P$  and let  $L$  be the perpendicular bisector of  $Q$  and  $\phi(Q)$ . Since  $Q$  and  $\phi(Q)$  must have the same distance from the fixed point  $P$ , it follows that  $P$  must lie on  $L$ . Also, the reflection in  $L$ , call it  $\rho$  say, must send  $Q$  to  $\phi(Q)$ . Thus  $\rho^{-1} \circ \phi$  fixes both  $P$  and  $Q$  and so, by what we have done so far, is either the identity or a reflection. We can easily see that it cannot be the identity if  $\phi$  is to fix no more than one point. Thus  $\rho^{-1} \circ \phi$  is a reflection, say  $\rho_1$ , and so  $\phi = \rho \circ \rho_1$ . Since the axes of  $\rho$  and  $\rho_1$  intersect at  $P$ , it follows from Lemma 2.8.2 that  $\phi$  is a rotation about  $P$ .

Suppose finally that  $\phi$  fixes no points. Then if  $P$  is any point, we have  $P \neq \phi(P)$ . Let  $L$  be the perpendicular bisector of  $P$  and  $\phi(P)$  and let  $\rho$  be the reflection in  $L$ . Then  $\rho^{-1} \circ \phi$  fixes  $P$  and so  $\rho^{-1} \circ \phi$  is either a rotation about  $P$  or a reflection fixing  $P$ . Thus, using the result of the last case,  $\phi$  is a product of at most three reflections in this case.

It remains to show that  $\phi$  is either a translation or a glide reflection. If  $\rho^{-1} \circ \phi$  is a reflection fixing  $P$  then  $\phi$  is a product of two reflections and so must be a translation, by Lemma 2.8.1. If  $\rho^{-1} \circ \phi$  is a rotation about  $P$  then  $\phi$  is the product of three reflections. If the axes of all three of these reflections are parallel then, by Lemma 2.8.1,  $\phi$  is a reflection, which is impossible. If not, then the axes cannot meet in a point, since that point would then be fixed by  $\phi$ . Thus the axes are not all parallel and do not meet in a point and so, by Lemma 2.8.1,  $\phi$  is a glide reflection.  $\square$

So we have described *all* isometries on  $\mathbb{E}^2$ . We can use this to help us describe the group of all isometries.

**Definition 2.8.3.** *The group of all isometries of  $\mathbb{E}^2$  will be denoted by  $\mathcal{I}$ .*

Before we go on, we make a few observations about conjugates in  $\mathcal{I}$ . If  $\phi$  is an isometry, and  $X$  is the set of fixed points of  $\phi$  then it is not too hard to check that, for some other isometry  $\sigma$ , the set of fixed points of  $\sigma\phi\sigma^{-1}$  is  $\sigma(X)$ . This shows us immediately that if  $\phi$  is a reflection then any conjugate of  $\phi$  is also a reflection because the set of fixed points of the conjugate must also be a line. Similarly a conjugate of a rotation is another rotation. By this method we know that a conjugate of a translation is either a translation or a glide reflection. But a translation is a product of two reflections and then

its conjugate will be the product of two conjugates of reflections and so itself the product of two reflections. Thus its conjugate is another translation. Similarly, a conjugate of a glide reflection is a glide reflection. We leave to Exercise 6 the question of determining all of the conjugacy classes exactly.

**Theorem 2.8.4.** (1) *The set of translations forms a normal subgroup  $\mathcal{T}$  of  $\mathcal{I}$ .*

(2) *Let  $P$  be a point of  $\mathbb{E}^2$ ; the set of isometries of  $\mathcal{I}$  which fix  $P$  forms a subgroup  $\mathcal{O}_P$ .*

(3) *If  $P, Q \in \mathbb{E}^2$  then  $\mathcal{O}_P$  and  $\mathcal{O}_Q$  are conjugate subgroups of  $\mathcal{I}$ . In particular, they are isomorphic. item Let  $P$  be a point of  $\mathbb{E}^2$ ; every element of  $\mathcal{I}$  can be uniquely expressed as a product of a translation and an isometry fixing  $P$ .*

(4) *Let  $P$  be a point of  $\mathbb{E}^2$ ; there is a surjective homomorphism  $\pi_P : \mathcal{I} \rightarrow \mathcal{O}_P$ .*

*Proof.* (1) It is easy to check that  $\mathcal{T}$  is a subgroup of  $\mathcal{I}$ . We have just shown, in the discussion preceding the statement of the theorem, that a conjugate of a translation is another translation. Thus  $\mathcal{T}$  is a normal subgroup.

(2) is an easy check.

(3) Choose any  $\phi \in \mathcal{I}$  satisfying  $\phi(P) = Q$ . For example,  $\phi$  could be a translation. We claim that  $\phi\mathcal{O}_P\phi^{-1} = \mathcal{O}_Q$ . Let  $\psi \in \phi\mathcal{O}_P\phi^{-1}$ ; say  $\psi = \phi\nu\phi^{-1}$  with  $\nu \in \mathcal{O}_P$ . Then

$$\psi(Q) = \phi\nu\phi^{-1}(Q) = \phi\nu(P) = \phi(P) = Q.$$

Thus  $\psi \in \mathcal{O}_Q$  and so  $\phi\mathcal{O}_P\phi^{-1} \subseteq \mathcal{O}_Q$ ; the reverse inclusion is similar.

(4) Suppose that  $\phi \in \mathcal{I}$ . Set  $Q = \phi(P)$ . Then there is a translation  $\tau$  which takes  $P$  to  $Q$ . Also  $\tau^{-1}\phi(P) = \tau^{-1}(Q) = P$ . If we set  $\tau^{-1}\phi = \mu$ , then  $\mu \in \mathcal{I}$  and  $\phi = \tau\mu$  with  $\tau \in \mathcal{T}$  and  $\mu$  an isometry fixing  $P$ . It remains to show the uniqueness. Suppose that  $\phi = \tau_1\mu_1$  with  $\tau_1 \in \mathcal{T}$  and  $\mu_1 \in \mathcal{O}_P$ . Then  $\tau\mu = \tau_1\mu_1$  and so  $\tau_1^{-1}\tau = \mu_1\mu^{-1}$ . But  $\tau_1^{-1}\tau$  is a translation and  $\mu_1\mu^{-1}$  fixes the point  $P$ . Thus they must both be the identity. That is,  $\tau = \tau_1$  and  $\mu = \mu_1$ .

(5) If  $\phi \in \mathcal{I}$ , we can write  $\phi = \tau\mu$  with  $\tau \in \mathcal{T}$  and  $\mu \in \mathcal{O}_P$ . Define  $\pi_P(\phi) = \mu$ . This is a well-defined function by the previous part. We must show that it is a homomorphism. Suppose that  $\phi_1 = \tau_1\mu_1$  and  $\phi_2 = \tau_2\mu_2$ . Then

$$\phi_1\phi_2 = \tau_1\mu_1\tau_2\mu_2 = \tau_1(\mu_1\tau_2\mu_1^{-1})\mu_1\mu_2$$

and  $\mu_1\mu_2 \in \mathcal{O}_P$  and  $\tau_1(\mu_1\tau_2\mu_1^{-1}) \in \mathcal{T}$  (using part (1)). Thus

$$\pi_P(\phi_1\phi_2) = \mu_1\mu_2 = \pi_P(\phi_1)\pi_P(\phi_2)$$

and  $\pi_P$  is a homomorphism.  $\square$

We have shown that  $\mathcal{I}$  has a normal subgroup  $\mathcal{T}$  and a subgroup  $\mathcal{O}_P$  (not unique) which satisfy  $\mathcal{T} \cap \mathcal{O}_P = \{e_I\}$  and  $\mathcal{T}\mathcal{O}_P = \mathcal{I}$ . This kind of structure is quite common; we say that  $\mathcal{I}$  is a *semi-direct product* of  $\mathcal{T}$  by  $\mathcal{O}_P$ .

The fact that  $\mathcal{O}_P$  and  $\mathcal{O}_Q$  are conjugate via a translation shows that the homomorphism  $\pi_P$  need not depend on  $P$ . Thus we shall simply regard it as a homomorphism

$$\pi : \mathcal{I} \longrightarrow \mathcal{O}$$

where  $\mathcal{O}$  is the set of elements in  $\mathcal{I}$  which fix a given (unnamed) point. Note that, if we identify  $\mathbb{E}^2$  with  $\mathbb{R}^2$  in such a way that the point  $P$  becomes the origin of  $\mathbb{R}^2$  then all of these elements are linear transformations of  $\mathbb{R}^2$  and so  $\mathcal{O} \cong O(2, \mathbb{R})$ .

### 2.8.3 Classification of finite symmetry groups

**Theorem 2.8.5.** *The only finite groups of isometries of  $\mathbb{E}^2$  are the cyclic groups and the dihedral groups.*

*Proof.* We have already seen that the groups described are finite groups of isometries; we must show that there are no more. Suppose that  $G$  is a finite group of isometries of  $\mathbb{E}^2$ .

We claim first that  $G$  has a fixed point. Suppose that  $G = \{g_1, \dots, g_n\}$  and let  $P$  be any point of  $\mathbb{E}^2$ . Consider the set of points  $S = \{g_1(P), \dots, g_n(P)\}$ . If  $g \in G$  then

$$g(S) = g(\{g_1(P), \dots, g_n(P)\}) = \{gg_1(P), \dots, gg_n(P)\} = S$$

as  $\{gg_1, \dots, gg_n\}$  is just  $G$ , but listed in a different order. Thus the set  $S$  of points is left fixed by each element of  $G$  and so the centroid (centre of gravity) of  $S$  is also left fixed by each element of  $G$ . Thus we have the required fixed point; call it  $O$ .

By Theorem 2.8.3,  $G$  consists of reflections and rotations. It is clear that the rotations form a subgroup  $H$ .

Let  $k \in H$  be the rotation in  $H$  of least possible positive angle  $\theta$  and let  $h \in H$  be an arbitrary element of  $H$ , with angle  $\eta$ . Then we can write  $\eta = n\theta + \zeta$  with  $n \in \mathbb{Z}$  and  $0 \leq \zeta < \theta$ . So  $hk^{-n}$  will have angle  $\eta - n\theta = \zeta$ . But  $hk^{-n} \in H$  and this will contradict the choice of  $\theta$  as the least possible

angle of any element of  $H$  unless  $\zeta = 0$ . Thus  $\zeta = 0$  and so  $hk^{-n} = e_H$ . Hence  $h = k^n$  and  $H = \langle k \rangle$ , showing that  $H$  is cyclic. If  $G = H$ ,  $G$  is thus the cyclic group.

Otherwise,  $G$  must contain reflections. By Lemma 2.8.2, the product of any two reflections is a rotation. Thus, if we take two reflection  $\rho_1$  and  $\rho_2$  in  $G$ , then  $\rho_2\rho_1^{-1} \in H$ . Hence  $\rho_2 \in H\rho_1$ . Hence all cosets containing a reflection coincide; in fact they are just the complement of  $H$  in  $G$ . That is, the only coset of  $H$ , apart from  $H$  itself, is the complement of  $H$  in  $G$  and consists of all of the reflections. Also, if  $\rho$  is any reflection and  $\sigma$  is a rotation through  $\theta$ , it is an easy exercise to check that  $\rho\sigma\rho^{-1}$  is a rotation through  $-\theta$ . Thus  $\rho\sigma\rho^{-1} = \sigma^{-1}$ . It is now relatively easy to check that  $G$  is a dihedral group.  $\square$

Thus the natural symmetry groups we discussed at the beginning of this section are the only possibilities.

### 2.8.4 Isometries of Euclidean space $\mathbb{E}^n$

Let  $\mathbb{E}^n$  denote  $n$ -dimensional Euclidean space, that is  $\mathbb{R}^n$  together with its usual Euclidean notion of distance: the distance between points  $x$  and  $y$  in  $\mathbb{R}^n$  is  $d(x, y) = \|x - y\| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}$ . This is just the usual distance defined in terms of the dot product on  $\mathbb{R}^n$  since  $\|x\| = \sqrt{x \cdot x}$ .

An **isometry** of  $\mathbb{E}^n$  is a distance preserving function, i.e. a function  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  such that  $d(x, y) = d(f(x), f(y))$  for all  $x, y$  in  $\mathbb{R}^n$ .

**Examples:**

- (1) If  $A \in O(n)$  is an orthogonal matrix (i.e.  $A^T A = I$ ), then the linear transformation  $f_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  defined by  $f_A(x) = Ax$  is an isometry.
- (2) If  $b \in \mathbb{R}^n$ , then *translation by  $b$*  is an isometry  $t_b : \mathbb{R}^n \rightarrow \mathbb{R}^n$ ,  $t_b(x) = x + b$ . Further the inverse of  $t_b$  is  $t_{-b}$ .
- (3) Compositions of isometries are isometries.

In fact, every isometry of  $\mathbb{E}^n$  is a composition of a translation and an orthogonal transformation.

**Lemma 2.8.6.** *Let  $f$  be an isometry of  $\mathbb{E}^n$  such that  $f(\mathbf{0}) = \mathbf{0}$ . Then  $f$  is a linear transformation,  $f(x) = Ax$  where  $A \in O(n)$  is an orthogonal matrix, and  $x \in \mathbb{R}^n$  is a column vector.*

*Proof.* We have a function  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  such that

(i)  $f(\mathbf{0}) = \mathbf{0}$  and (ii)  $\|f(x) - f(y)\| = \|x - y\|$  for all  $x, y$  in  $\mathbb{R}^n$ .

**Step 1.**  $f$  preserves dot products.

For all  $x, y$  we have

$$\|x - y\|^2 = (x - y) \cdot (x - y) = x \cdot x - 2x \cdot y + y \cdot y = \|x\|^2 - 2x \cdot y + \|y\|^2. \quad (1)$$

Hence we also have

$$\|f(x) - f(y)\|^2 = \|f(x)\|^2 - 2f(x) \cdot f(y) + \|f(y)\|^2. \quad (2)$$

Since  $f$  preserves distances, we have  $\|x - y\| = \|f(x) - f(y)\|$  for all  $x, y$ . Taking  $y = \mathbf{0}$  in this gives  $\|x\| = \|x - \mathbf{0}\| = \|f(x) - f(\mathbf{0})\| = \|f(x) - \mathbf{0}\| = \|f(x)\|$  for all  $x$ , and similarly  $\|y\| = \|f(y)\|$  for all  $y$ . Using these facts together with (1) and (2) then gives  $x \cdot y = f(x) \cdot f(y)$  for all  $x, y$ .

**Step 2.** If  $\{e_1, \dots, e_n\}$  is the standard basis for  $\mathbb{R}^n$  then  $\{f(e_1), \dots, f(e_n)\}$  is an orthonormal basis for  $\mathbb{R}^n$ .

Since  $e_1, \dots, e_n$  are orthonormal vectors, step 1 implies that  $f(e_1), \dots, f(e_n)$  are also orthonormal vectors. Since orthonormal vectors are linearly independent and  $\dim \mathbb{R}^n = n$  it follows that  $\{f(e_1), \dots, f(e_n)\}$  is an orthonormal basis for  $\mathbb{R}^n$ .

**Step 3.**  $f$  is a linear transformation.

Let  $x$  be any vector in  $\mathbb{R}^n$ . Then we can write

$$x = x_1 e_1 + \dots + x_n e_n$$

where  $x_i = x \cdot e_i$ , since  $\{e_1, \dots, e_n\}$  is an orthonormal basis. Similarly

$$f(x) = (f(x) \cdot f(e_1))f(e_1) + \dots + (f(x) \cdot f(e_n))f(e_n)$$

since  $\{f(e_1), \dots, f(e_n)\}$  is an orthonormal basis. But  $f(x) \cdot f(e_i) = x \cdot e_i = x_i$  by step 1. Hence we have

$$f(x_1 e_1 + \dots + x_n e_n) = x_1 f(e_1) + \dots + x_n f(e_n)$$

for all  $x_1, \dots, x_n$ . It follows  $f$  is a linear transformation.

**Step 4.** The matrix  $A$  of  $f$  with respect to the standard basis satisfies  $A^T A = I$ , so  $A$  is orthogonal.

The standard matrix of  $A$  has columns  $f(e_1), \dots, f(e_n)$  (we regard these as column vectors). Then the  $(i, j)$  entry in the matrix  $A^T A$  is

$$f(e_i)^T f(e_j) = f(e_i) \cdot f(e_j) = e_i \cdot e_j = \delta_{ij}.$$

So  $A^T A$  is the identity matrix. □

**Corollary 2.8.7.** *Every isometry  $f$  of  $\mathbb{E}^n$  has the form  $f(x) = Ax + b$  where  $A \in O(n)$  and  $b \in \mathbb{R}^n$ . (We write  $f = (A, b)$  for short.)*

*Proof.* If  $f(\mathbf{0}) = b$ , then  $t_b^{-1} \circ f = t_{-b} \circ f$  is an isometry fixing  $\mathbf{0}$ . Hence, by the previous lemma,  $f(x) - b = t_{-b} \circ f(x) = Ax$  for some  $A \in O(n)$ .  $\square$

### 2.8.5 Exercises

- (1) Let  $\mathcal{I}_+$  denote the subset of  $\mathcal{I}$  consisting of all translations together with all rotations. Show that  $\mathcal{I}_+$  is a subgroup of  $\mathcal{I}$ .
- (2) Show that  $\mathcal{I}_+$  has index 2 in  $\mathcal{I}$ ; deduce that  $\mathcal{I}_+$  is normal. The isometries in  $\mathcal{I}_+$  are called *orientation preserving*.
- (3) Show that an isometry is orientation preserving precisely if it is a product of an even number of reflections.
- (4) Identify  $\mathbb{E}^2$  with the complex plane. Then each point can be represented by a complex number. Show that every isometry can be represented in the form  $z \mapsto e^{i\theta}z + u$  or the form  $z \mapsto e^{i\theta}\bar{z} + u$  for some real number  $\theta$  and some complex number  $u$ . Show that the former type correspond to orientation preserving isometries.
- (5) Let  $D_\infty$  be the set of isometries consisting of all translations of  $\mathbb{R}^2$  which are parallel to the  $x$ -axis and through an integer distance together with all reflections in a line  $x = n/2$  for  $n$  an integer. Show that  $D_\infty$  is a subgroup of the group of all isometries. Show that  $D_\infty$  acts on the  $x$ -axis and find the orbit and stabilizer of  $(1, 0)$ ,  $(\frac{1}{2}, 0)$ ,  $(\frac{1}{3}, 0)$ .
- (6) Describe the conjugacy classes in the group  $\mathcal{I}$ .
- (7) Prove Lemma 2.8.1.
- (8) Complete the proof of parts (1) and (2) of Lemma 2.8.2.

## 2.9 Wallpaper groups

We want to study the different possible types of repeating 2-dimensional patterns. It needs some thought, however, to work out what we really mean by ‘repeating 2-dimensional patterns’. We do not want too much symmetry, otherwise we are not able to obtain sensible patterns; we do not want too little, otherwise we do not obtain enough of what we would regard as sensible answers.

### 2.9.1 Lattices and point groups

**Definition 2.9.1.** (1) A subgroup of  $\mathcal{T}$  generated by two independent translations is called a lattice.

(2) If  $W$  is a subgroup of  $\mathcal{I}$ , then  $\pi(W)$  is called the point group of  $W$ .

(3) A subgroup  $W$  of  $\mathcal{I}$  is said to be a wallpaper or crystallographic group if the translation subgroup  $W \cap \mathcal{T}$  is a lattice and if the point group  $\pi(W)$  is finite.

Note that the point group need not be a subgroup of  $W$ . For example, the group  $W$  generated by a glide reflection is the infinite cyclic group which has no elements of finite order other than the identity. But the point group has order 2 because when we choose a point  $P$  and write the glide reflection as a product of a translation and a symmetry fixing  $P$ , the latter is a reflection. The point group is then the group generated by this reflection. This point group cannot be isomorphic to a subgroup of  $W$  since  $W$  is isomorphic to the infinite cyclic group and has no elements of order 2.

Each translation can be identified with the two-dimensional vector which has starting point an arbitrary point and finish point the image, under the translation, of the starting point. If  $\tau$  is a translation, we shall denote this vector by  $\text{vec}(\tau)$ .

Because  $\mathcal{T} \cap W$  is generated by two independent translations, say  $\tau_1$  and  $\tau_2$ , every element is uniquely expressible in the form  $\tau_1^a \tau_2^b$  for integers  $a$  and  $b$ . Then  $\text{vec}(\mathcal{T} \cap W)$  is a set of vectors in the plane each of which is expressible as a linear combination, with integer coefficients, of two independent vectors. If  $\mathcal{T} \cap W$  is a lattice, we shall also call  $\text{vec}(\mathcal{T} \cap W)$  a lattice.

**Lemma 2.9.1.** If  $W$  is a wallpaper group then the point group of  $W$  acts on the translation subgroup of  $W$ . More precisely, if  $\rho \in \pi(W)$ , define

$$f : \pi(W) \rightarrow \text{Sym}(\mathcal{T} \cap W)$$

by

$$f(\rho)[\tau] = \phi\tau\phi^{-1}$$

where  $\tau \in \mathcal{T} \cap W$  and  $\phi$  satisfies  $\pi(\phi) = \rho$ .

This action agrees with the action of  $\pi(W)$  on the plane in the sense that, for  $\rho \in \pi(W)$ ,

$$\text{vec}(f(\rho)[\tau]) = \rho(\text{vec}(\tau)) \text{ for all } \tau \in \mathcal{T} \cap W.$$

*Proof.* We show firstly that the action defined in the statement of the lemma is well-defined. The problem is that a choice of  $\phi$  has been made. Suppose then that  $\pi(\phi_1) = \pi(\phi_2) = \rho$ . Then  $\pi(\phi_1^{-1}\phi_2) = e$  and so  $\phi_1^{-1}\phi_2 \in \ker \pi = \mathcal{T}$ . Hence  $\phi_2 = \phi_1\nu$  for some translation  $\nu$ . Thus, if  $\tau \in \mathcal{T}$ ,

$$\phi_2\tau\phi_2^{-1} = \phi_1\nu\tau\nu^{-1}\phi_1^{-1} = \phi_1\tau\phi_1^{-1}$$

because  $\nu\tau\nu^{-1} = \tau$  since both  $\tau$  and  $\nu$  lie in the commutative group  $\mathcal{T}$ . Thus  $f$  does not depend on the particular choice of  $\phi$  satisfying  $\pi(\phi) = \rho$ .

If  $\phi \in W$  and  $\tau \in \mathcal{T} \cap W$  then clearly  $\phi\tau\phi^{-1} \in W$ . Also,  $\phi\tau\phi^{-1}$  lies in  $\mathcal{T}$  as  $\mathcal{T}$  is a normal subgroup of  $\mathcal{I}$ . Thus  $\phi\tau\phi^{-1} \in \mathcal{T} \cap W$ .

Suppose that  $\rho_1, \rho_2 \in \pi(W)$ . Then

$$\begin{aligned} f(\rho_1\rho_2)[\tau] &= \rho_1\rho_2\tau(\rho_1\rho_2)^{-1} \\ &= \rho_1\rho_2\tau\rho_2^{-1}\rho_1^{-1} = \rho_1(\rho_2\tau\rho_2^{-1})\rho_1^{-1} \\ &= f(\rho_1)[\rho_2\tau\rho_2^{-1}] \\ &= f(\rho_1)[f(\rho_2)[\tau]] \end{aligned}$$

Thus  $f(\rho_1\rho_2) = f(\rho_1) \circ f(\rho_2)$  and  $f$  is a homomorphism. It follows easily that  $f(\rho)$  has inverse  $f(\rho^{-1})$  and so  $f(\rho)$  is an element of  $\text{Sym}(T)$ . Thus  $f$  gives an action of  $\pi(W)$  on  $T$ .

For the final statement of the lemma, note firstly that, if  $P$  is any point of the plane,  $\tau$  is a translation and  $\tau(P) = Q$  then  $\text{vec}(\tau)$  can be expressed as the vector  $\overrightarrow{PQ}$ . Now, fix a point  $O$  and set  $\phi^{-1}(O) = R$  and  $\tau(R) = S$  so that  $\text{vec}(\tau) = \overrightarrow{RS}$ . Then

$$\begin{aligned} \rho(\text{vec}(\tau)) &= \phi(\text{vec}(\tau)) = \phi(\overrightarrow{RS}) \\ &= \overrightarrow{\phi(R)\phi(S)} = \overrightarrow{OQ} \end{aligned}$$

where  $Q = \phi(S) = \phi\tau(R) = \phi\tau\phi^{-1}(O)$  and

$$\overrightarrow{OQ} = \text{vec}(\phi\tau\phi^{-1}) = \text{vec}(\rho.\tau).$$

□

This action will be very useful when we attempt to classify the wallpaper groups. We can think of a wallpaper group as consisting of several parts. These include the point group, the translation subgroup (which is always isomorphic to  $\mathbb{Z}^2$ ) and the action of the former on the latter. But these may fit together in different ways.

## 2.9.2 Simple properties of wallpaper groups

We shall not prove the next lemma. Its proof is somewhat outside the scope of this course.

**Lemma 2.9.2.** *In a lattice of  $\mathbb{E}^2$ , there is a non-zero translation of least length. Any set of two shortest independent vectors generates the lattice*

**Lemma 2.9.3.** (1) *If  $\pi(\rho)$  is a rotation through  $\theta \neq 0$  then so also is  $\rho$ .*

(2) *If  $W$  is a wallpaper group with point group consisting entirely of rotations, then  $W = (W \cap \mathcal{T})(W \cap \mathcal{O}_P)$  for some point  $P$ .*

*Proof.* (1) Recall that  $\pi(\rho)$  is given by  $\rho = \tau\pi(\rho)$  where  $\tau$  is a translation and  $\pi(\rho)$  is an isometry fixing some chosen point. If  $\pi(\rho)$  is a rotation then we can write it as a product of two reflections, the first of which has axis perpendicular to the direction of translation. The translation can be written as a product of two reflections, each of which has axis perpendicular to the direction of translation. Further we can take the second of these reflections to co-incide with the first of the reflections which make up the rotation. Thus these two reflections will cancel leaving  $\rho$  as a product of two reflections with axes inclined at an angle of  $\theta/2$  and so a rotation through an angle  $\theta$ .

(2) Suppose that  $\pi(W)$  is the cyclic group of order  $n$ . The argument in the previous paragraph shows that  $W$  contains a rotation through  $2\pi/n$ . Suppose the centre of this is  $P$ . Then  $\pi_P(W) \subseteq W$ . Thus when we write  $\phi \in W$  in the form  $\phi = \tau\rho$  with  $\rho \in \mathcal{O}_P$  we have  $\rho \in W$  and so  $\tau \in W$ . Thus  $W = (W \cap \mathcal{T})(W \cap \mathcal{O}_P)$ .  $\square$

What this shows is that, when the point group of  $W$  consists of rotations, there is a point  $P$  in the plane so that the subgroup of  $W$  consisting of those isometries which fix  $P$  is isomorphic to the point group of  $W$  (via  $\pi$ ). Thus the rather tricky idea of the point group is not really needed here.

The reason that there are not too many essentially different wallpaper patterns is the following.

**Theorem 2.9.4 (The crystallographic restriction).** *The order of a rotation in a wallpaper group  $W$ , is 1, 2, 3, 4 or 6.*

*Proof.* Let  $\tau$  be a translation of shortest non-zero length in  $W$  and let  $v_\tau = \text{vec}(\tau)$ . Suppose that  $W$  contains a rotation  $\rho$  through  $2\pi/n$ ; that is, a rotation of order  $n$ . Then  $\rho\tau\rho^{-1}$  will be a translation with corresponding vector  $\rho(v_\tau)$ . The angle between the vectors  $v_\tau$  and  $\rho(v_\tau)$  is  $2\pi/n$  since  $\rho(v_\tau)$  is obtained from  $v_\tau$  by rotating it through  $2\pi/n$ . Thus the translation

corresponding to the difference of these vectors lies in  $W$ . But a little elementary trigonometry tells us that the difference of the two vectors has length  $2 \sin(\pi/n)|v_\tau|$ . This is less than  $|v_\tau|$  if  $\sin(\pi/n) < 1/2$ ; that is, if  $n > 6$ . Thus we must have  $n \leq 6$ .

If  $n = 5$ , then form the difference of  $\rho^2(v_\tau)$  and  $-v_\tau$ . The angle between these two vectors is  $\pi/5$  and so again the difference would be of shorter length. Thus  $n \neq 5$ . A little consideration of chessboard and honeycomb patterns should convince you that  $n = 1, 2, 3, 4, 6$  are possible.  $\square$

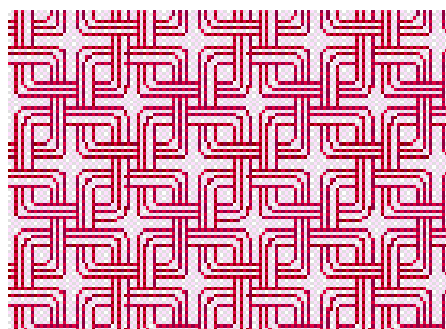
### 2.9.3 Exercises

(1) For the following wallpaper patterns:

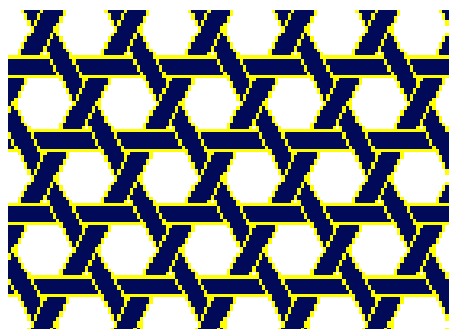
- find two generating translation vectors;
- find a complete set of centres of rotation (so that any other centre of rotation can be found by applying a translation of the group);
- find a complete set of axes of reflection ;
- find a complete set of axes of glide reflection;
- find the point group.

The best way to do all but the last part is probably to mark them directly onto the pattern (or a photocopy).

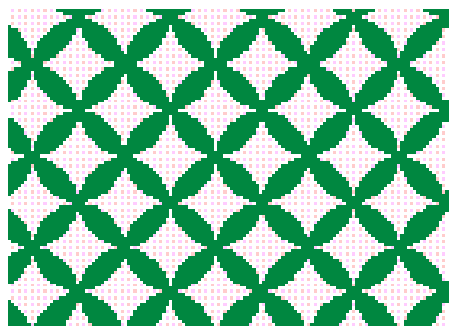
(a)



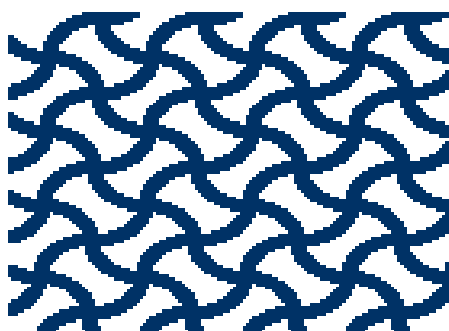
(b)



(c)



(d)



- (2) For each of the preceding patterns, describe the action of the point group by matrices. You should first choose as basis the generating set of translations that you described centered at one of the points which are centres of rotation for a rotation of greatest order. It will be sufficient to give matrices only for this rotation of greatest order and for a single reflection (if there are any).

## 2.10 Classifying wallpaper groups

### 2.10.1 The point groups and the lattices

A combination of Theorem 2.8.5 with Theorem 2.9.4 enables us to classify the possible point groups of wallpaper groups

**Theorem 2.10.1.** *The following are the possible point groups for a crystallographic group:*

- *The trivial group;*
- *The cyclic rotation group  $C_2$  of order 2;*
- *The cyclic rotation group  $C_3$  of order 3;*
- *The cyclic rotation group  $C_4$  of order 4;*
- *The cyclic rotation group  $C_6$  of order 6;*
- *The dihedral group  $D_1$  of order 2 (containing one reflection and the identity);*
- *The dihedral group  $D_2$  of order 4 (containing two reflections with axes at right angles);*
- *The dihedral group  $D_3$  of order 6 (the full symmetry group of a triangle);*
- *The dihedral group  $D_4$  of order 8 (the full symmetry group of a square);*
- *The dihedral group  $D_6$  of order 12 (the full symmetry group of a hexagon).*

We can then deal with separately with each type of point group and investigate the corresponding possibilities for wallpaper groups. If there are no reflections, this is relatively straightforward, since by Lemma 2.9.3, the wallpaper group contains a faithful copy of the point group. If, however, there are also reflections in the point group, then there may or may not be corresponding reflections in the wallpaper group and the situation becomes a little more complicated.

We shall attempt to give the flavour of the classification of the wallpaper groups by doing one non-trivial example. Thus, for the remainder of this section, **we shall assume that  $W$  is a wallpaper group for which the point group contains a four-fold rotation.** Thus, by Lemma 2.9.3  $W$  itself also contains a four-fold rotation. We shall call it  $\rho$ . Denote the translation subgroup of  $W$  by  $T(W)$ .

### 2.10.2 Understanding the rotations in $W$

Recall that we have been thinking of the plane  $\mathbb{E}^2$  as ‘bare’; that is, without origin or axes. We shall now choose these to make our description easier. Choose the origin  $O$  to be the centre of the rotation  $\rho$ .

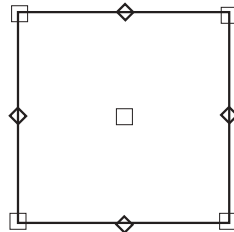
Let  $\tau$  be a non-identity translation in  $T(W)$  of least magnitude. By Lemma 2.9.1,  $\text{vec}(\rho\tau\rho^{-1}) = \rho(\text{vec}(\tau))$  and so  $\rho\tau\rho^{-1}$  has the same magnitude as  $\tau$ . Thus, by Lemma 2.9.2,  $\tau$  and  $\rho\tau\rho^{-1}$  generate  $T(W)$ . We shall take their vectors, which are orthogonal, as the unit vectors for a set of axes based at  $O$ . Thus every element of  $\text{vec}(T(W))$  can be represented as  $(a, b)$  for suitable integers  $a$  and  $b$ . In particular,  $\text{vec}(\tau)$  will be represented as  $(1, 0)$  and  $\text{vec}(\rho\tau\rho^{-1})$  will be represented as  $(0, 1)$ . The action of  $\rho$  on  $T(W)$  can then be represented as a rotation and the matrices of the powers of  $\rho$  are as follows:

$$\rho \sim \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \rho^2 \sim \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \rho^3 \sim \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Suppose that  $\tau$  is a translation with  $\text{vec}(\tau)$  represented by  $(a, b)$ . Then the effect of  $\tau\rho$  is given by  $\tau\rho : (x, y) \mapsto (-y, -x) \mapsto (-y + a, -x + b)$ . We know that this is a rotation through  $\pi/2$  and to find its center, we must solve the equations  $x = -y + a, y = -x + b$ . Continuing in this way, we find all possibilities for a product of  $\tau$  with a power of  $\rho$ .

| name         | type                      | centre                   |
|--------------|---------------------------|--------------------------|
| $\tau$       | translation               | not applicable           |
| $\tau\rho$   | rotation through $\pi/2$  | $((a - b)/2, (a + b)/2)$ |
| $\tau\rho^2$ | rotation through $\pi$    | $(a/2, b/2)$             |
| $\tau\rho^3$ | rotation through $3\pi/2$ | $((a + b)/2, (a - b)/2)$ |

There are, of course, infinitely many such centres of rotation. But we can describe them by listing those that occur in the ‘unit square’.



We have used a small square to represent a centre of four-fold rotation and a small diamond to represent a centre of two-fold rotation.

We have now listed all of the elements of  $W$  which do not involve a reflection. If the point group of  $W$  is  $C_4$  then the description of  $W$  is complete.

### 2.10.3 Classifying the cases when the point group contains a reflection

Let us suppose now that the point group of  $W$  is  $D_4$ . Then the point group of  $W$  will contain reflections. Recall that the point group acts on the image of the translation group in the plane. Thus  $T(W)$  will contain translations corresponding to the images, by these reflections in the point group, of the basis vectors  $(1, 0)$  and  $(0, 1)$ . If there is an axis of reflection which is neither along the axes nor makes an angle of  $\pi/4$  with them then it is easy to see that we can produce a translation in  $T(W)$  for which the vector makes an angle of less than  $\pi/6$  with one of the axes. But then the triangle formed by this vector and the closest unit vector along an axis will have a third side (also corresponding to an element of  $T(W)$ ) which has lesser length. By assumption, this does not happen. Thus there is a reflection in  $\pi(W)$  which has axis either along an axis or making an angle of  $\pi/4$  with the axes.

It is now easy to check by multiplying this reflection by powers of the rotation  $\rho$  that we must have in  $\pi(W)$  the four reflections in the axes and in the two lines making an angle of  $\pi/4$  with the axes. The matrices for these reflections are:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

### 2.10.4 The case when $\pi(W)$ is $D_4$ and $W$ contains a corresponding reflection

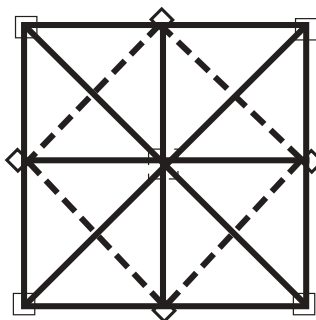
We shall suppose now that  $W$  itself contains a reflection in the  $x$ -axis. We call this reflection  $\sigma$ . Then  $\sigma$  and  $\rho$  will generate a copy of  $D_4$  within  $W$  and  $W$  will be generated by this copy and  $T(W)$ . The other reflections fixing  $O$  will be  $\sigma\rho, \sigma\rho^2, \sigma\rho^3$  and their matrices will be as above (in the same order).

Thus the elements of  $W$  which we have not listed so far will be of the form  $\tau\sigma\rho^i$  with  $\tau \in T(W)$  and  $i = 0, 1, 2, 3$ . We now give a description of each of these types. For each one we will describe it as a glide reflection in the form  $\tau_1\sigma_1$  where  $\tau_1$  is a translation and  $\sigma_1$  is a reflection with axis parallel to  $\tau_1$ . In the following list, we give the vector of  $\tau_1$ , the axis of  $\sigma_1$ , what conditions are needed to make  $\tau_1\sigma_1$  a genuine reflection (that is with trivial associated translation) and whether the product ‘splits’; that is, whether  $\tau_1$  and  $\sigma_1$  lie in  $W$ .

We assume that  $\text{vec}(\tau) = (a, b)$ .

|                    | $\text{vec}(\tau_1)$     | Axis of $\sigma_1$  | Reflection? | splits?      |
|--------------------|--------------------------|---------------------|-------------|--------------|
| $\tau\sigma$       | $(a, 0)$                 | $y = b/2$           | $a = 0$     | always       |
| $\tau\sigma\rho$   | $((a - b)/2, (b - a)/2)$ | $x + y = (a + b)/2$ | $a = b$     | $a + b$ even |
| $\tau\sigma\rho^2$ | $(0, b)$                 | $x = a/2$           | $b = 0$     | always       |
| $\tau\sigma\rho^3$ | $((a + b)/2, (a + b)/2)$ | $y - x = (b - a)/2$ | $a = -b$    | $a + b$ even |

We can summarise this by drawing the axes of reflections or glide reflections which appear in the unit square formed by the basis vectors.



### 2.10.5 The case when $\pi(W)$ is $D_4$ and $W$ does not contain a corresponding reflection

We now suppose that  $W$  does not contain the reflection  $\sigma$  in the  $x$ -axis, even though  $\pi(W)$  does. It follows from the definition of  $\pi$  that  $W$  must contain some element of the form  $\tau\sigma$  where  $\tau$  is a reflection with  $\text{vec}(\tau) = (\alpha, \beta)$ , say.

Note that

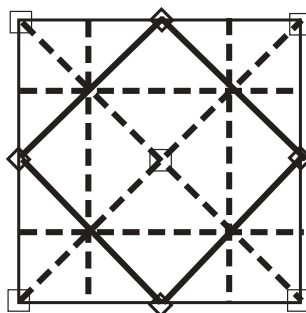
$$(\tau\sigma)^2 = \tau\sigma\tau\sigma = \tau(\sigma\tau\sigma^{-1})$$

and this is a translation in  $W$  with vector  $(\alpha, \beta) + \sigma(\alpha, \beta) = (2\alpha, 0)$ . Thus  $2\alpha$  must be an integer. Now repeat this argument with  $\tau\sigma\rho^i$  ( $i = 1, 2, 3$ ) replacing  $\tau\sigma\rho$ . We will be able to deduce that  $(\alpha + \beta, \alpha + \beta)$ ,  $(0, 2\beta)$  and  $(\alpha - \beta, \beta - \alpha)$  all lie in  $W$ . Thus  $2\alpha, 2\beta, \alpha + \beta, \alpha - \beta$  are all integers. It follows easily that either  $\alpha$  and  $\beta$  are integers or each is an integer plus  $1/2$ . We can now multiply  $\tau\sigma$  on the left by a translation in  $W$  and obtain that  $\tau_0\sigma \in W$  where  $\text{vec}(\tau_0) = (1/2, 1/2)$ . Set  $\sigma_0 = \tau_0\sigma$ .

Since  $\pi(\sigma_0) = \sigma$ , it follows that  $W$  is generated by  $T(W)$ ,  $\rho$  and  $\sigma_0$ . It remains to look at the nature of the elements  $\tau\sigma_0\rho^i$  where  $\tau$  is a translation, with  $\text{vec}(\tau) = (a, b)$  and  $i = 0, 1, 2, 3$ . We make the table as in the last section. Recall that the chosen isometry is written in the form  $\tau_1\sigma_1$  where  $\tau_1$  is a translation and  $\sigma_1$  is a reflection with axis parallel to  $\tau_1$ .

|                      | $\text{vec}(\tau_1)$                 | Axis of $\sigma_1$        | Reflection?        | splits?      |
|----------------------|--------------------------------------|---------------------------|--------------------|--------------|
| $\tau\sigma_0$       | $(a + \frac{1}{2}, 0)$               | $y = \frac{2b+1}{4}$      | $a = -\frac{1}{2}$ | never        |
| $\tau\sigma_0\rho$   | $(\frac{a-b}{2}, \frac{b-a}{2})$     | $x + y = \frac{a+b+1}{2}$ | $a = b$            | $a + b$ odd  |
| $\tau\sigma_0\rho^2$ | $(0, b + \frac{1}{2})$               | $x = \frac{2a+1}{4}$      | $b = -\frac{1}{2}$ | never        |
| $\tau\sigma_0\rho^3$ | $(\frac{a+b+1}{2}, \frac{a+b+1}{2})$ | $y - x = \frac{b-a}{2}$   | $a + b = -1$       | $a + b$ even |

We can again summarise this by drawing the axes of reflections or glide reflections which appear in the unit square formed by the basis vectors.



We have now completed the classification of wallpaper groups which contain a four-fold rotation.

### 2.10.6 Summary of the classification

We shall simply list all of the seventeen possibilities for wallpaper groups. The list can be obtained by more of the sort of analysis we have just described. In the following, the ‘Name’ is from a standard naming system—it helps to know that ‘m’ stands for mirror (that is, a reflection) and ‘g’ stands for glide reflection. The third column describes the general shape of the translation lattice. The fourth column asks whether the group contains a subgroup of isometries fixing some point  $P$  which is isomorphic to the point group. The final column gives the name which this wallpaper group is assigned in the program ‘Kali’.

## Wallpaper Groups

| Name | Point Group | Lattice       | Contains point group? | Kali Name |
|------|-------------|---------------|-----------------------|-----------|
| p1   | id          | parallelogram | yes                   | o         |
| pm   | $D_1$       | rectangular   | yes                   | **        |
| pg   | $D_1$       | rectangular   | no                    | xx        |
| cm   | $D_1$       | rhombic       | yes                   | *x        |
| p2   | $C_2$       | parallelogram | yes                   | 222       |
| pmm  | $D_2$       | rectangular   | yes                   | *222      |
| pmg  | $D_2$       | rectangular   | no                    | 22*       |
| pgg  | $D_2$       | rectangular   | no                    | 22x       |
| cmm  | $D_2$       | rhombic       | yes                   | 2*2       |
| p3   | $C_3$       | hexagonal     | yes                   | 333       |
| p3m1 | $D_3$       | hexagonal     | yes                   | 3*3       |
| p31m | $D_3$       | hexagonal     | yes                   | *333      |
| p4   | $C_4$       | square        | yes                   | 442       |
| p4m  | $D_4$       | square        | yes                   | *442      |
| p4g  | $D_4$       | square        | no                    | 4*2       |
| p6   | $C_6$       | hexagonal     | yes                   | 632       |
| p6m  | $D_6$       | hexagonal     | yes                   | *632      |

## 2.10.7 Exercises

The aim of this (long) exercise is to classify the wallpaper groups which have point group  $D_1$ . Recall that  $D_1$  is the group consisting of the identity and a reflection; call the reflection  $\rho$ .

Let  $W$  denote a wallpaper group with  $\pi(W) = D_1$  and with translation subgroup  $T(W)$ .

- (1) Suppose that  $\text{vec}(T(W))$  contains a shortest non-zero vector  $v_0$  which is neither parallel nor perpendicular to the axis of  $\rho$ .
  - (a) Show that  $v_0$  and  $v_1 = \rho(v_0)$  generate the lattice  $\text{vec}(T(W))$ .
  - (b) We know that  $\tau\rho \in W$  for some translation  $\tau$ . If  $\text{vec}(\tau) = av_0 + bv_1$  for some  $a, b \in \mathbb{R}$ , show by considering  $(\tau\rho)^2$  that  $a + b \in \mathbb{Z}$ .
  - (c) Show that, for some  $\tau_2 \in W$ ,  $\tau_2\tau\rho$  is a reflection.
  - (d) Deduce that, after taking suitable axes, we can regard  $W$  as being generated by translations with vectors  $(a, b)$ ,  $(a, -b)$  and a reflection in the  $x$ -axis.

- (e) Show that every element of  $W$  is either a translation or a reflection in a line  $y = mb$  or a glide reflection in a line  $y = (m + 1/2)b$  where  $m$  is an arbitrary integer.
- (2) Now suppose that any shortest non-zero vector in  $\text{vec}(T(W))$  is either parallel to or perpendicular to the axis of  $\rho$ .
- (a) Show that the two generating vectors of  $\text{vec}(T(W))$  are perpendicular to each other, leading to a rectangular lattice for  $\text{vec}(T(W))$ . Write the generating vectors as  $(a, 0)$  and  $(0, b)$  so that  $\rho$  is now a reflection in the  $x$ -axis
- (3) Now suppose, as well as (2) above, that  $W$  contains a reflection  $\sigma$ . Choose axes so that the  $x$ -axis coincides with the axis of  $\sigma$ .
- (a) Show that the elements of  $W$  are either translations or reflections in a line  $y = mb/2$  with  $m$  an integer.
- (4) Finally suppose that, as well as (2) above,  $W$  does not contain a reflection.
- (a) Show that if  $\tau\rho \in W$  for some translation  $\tau$  then  $\text{vec}(\tau)$  must take the form  $(m + 1/2)a, nb$ .
- (b) Deduce that every element of  $W$ , in this case, is either a translation or a glide reflection in a line  $y = mb/2$  with  $m$  an arbitrary integer.