- Therefore, the inverse of any 3×3 matrix with integer elements and determinant 1 is also a 3×3 matrix with integer elements.
- Finally, if $\mathbf{A}$ has determinant 1, then $\mathbf{A}^{-1}$ also has determinant 1.
- Therefore, all the group properties are satisfied, and so G forms a group.

a^n notation

It is usual to write a^2 for $a * a$. Similarly, $a * a * a$ is written as a^3.

If n is positive, then a^n means $a * a * \ldots * a$. (Here, there are n copies of a.)

a^0 is taken as the identity element, e.

a^{-n} means $a^{-1} * a^{-1} * \ldots * a^{-1}$. (Here, again, there are n copies of a^{-1}.)

Division in a group

In a group G, we **cannot divide** by a. Instead, we **multiply** by its inverse, a^{-1}, which has the same effect as dividing by a.

When multiplying by a^{-1}, we must ensure that we multiply both sides with a^{-1} in the **same position**. For example, if $b = c$, we have

$$a^{-1} * b = a^{-1} * c \quad \text{and} \quad b * a^{-1} = c * a^{-1}$$

We **cannot** have $a^{-1} * b = c * a^{-1}$.

Permutation groups

Suppose that we are given n objects in a particular order. By switching two objects, we can change that order. Switching the objects in positions 1 and 2 is represented by the notation (1 2) or $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Similarly, the notation for switching the objects in positions 5 and 8 is (5 8) or $\begin{pmatrix} 5 & 8 \\ 8 & 5 \end{pmatrix}$. If we want to move the object in position 1 to position 8, the object in position 8 to position 5, and the object in position 5 back to position 1, the notation for this is (1 8 5) or $\begin{pmatrix} 1 & 8 & 5 \\ 8 & 5 & 1 \end{pmatrix}$. This means '1 to 8, 8 to 5, and 5 to 1'.

Similarly, the notation (1 2) (3 4 5) or $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \end{pmatrix}$ means '1 to 2 and 2 to 1, then 3 to 4, 4 to 5, and 5 to 3'.

This 'language' of permutations is illustrated below.

$$\begin{pmatrix} A & B & C & D & E & F \\ B & A & D & C & F & E \end{pmatrix} \text{ is represented by } \begin{matrix} (1\,2)\,(3\,4)\,(5\,6) \\ \textbf{or} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} \end{matrix}$$

The set which contains all possible permutations of n objects forms a group. The binary operation is the composition of the permutations. We can verify all four group properties.

Closure Composing two permutations of n objects gives another permutation of the n objects.

Associativity The composition of permutations is associative, but we will not prove it.

(One way to prove this is to encode the permutations as an $n \times n$ matrix containing 1s and 0s, and then the composition will correspond to the multiplication of matrices, which we know is associative. However, this technique is beyond the scope of this book.)

We can simply state without proof that the composition of permutations is associative.

Identity The identity permutation which does not interchange any objects is a member of the set.

Inverses The inverse of a typical permutation $(a\,b\,c\ldots d)$ is the permutation $(d\ldots c\,b\,a)$, which is also a member of the set.

Since there are $n!$ ways of arranging n objects, it follows that there are $n!$ different permutations in the permutation group of n elements, which is denoted by S_n.

Generator of a group

If a is a member of a group and $a \neq e$, a^2 is also a member of the group.

If $a^2 \neq e$, $a^2 * a$ or a^3 will also be a member of the group.

If a is a **generator** of a group, then every member of the group may be expressed as a^k for some integer k.

If the group is finite, then $a^r = e$ for some integer r, and the members of the group are

$$a,\ a^2,\ a^3,\ \ldots,\ a^{r-1} \quad \text{and} \quad a^r = e$$

For example, in the group $(\{e, a, a^2, a^3, a^4\}, *)$ with $a^5 = e$, each of a, a^2, a^3 and a^4 is a generator. (See pages 391–2.)

Cyclic groups

Cyclic groups are the simplest type of group. In any cyclic group, there is some element a which **generates** the group. Hence, the elements of the group are

$$\{e, a, a*a, a*a*a, a*a*a*a, \ldots\} \quad \text{or} \quad \{e, a, a^2, a^3, \ldots\}$$

Examples of cyclic and non-cyclic groups

- The group $\{1, i, -1, -i\}$ is cyclic.

  Since, $i^2 = -1$ and $i^3 = -i$, the group can be written as $\{1, i, i^2, i^3\}$.

- The group of integers under addition (mod 4) is also a cyclic group. The elements of this group are $\{0, 1, 2, 3\}$. The group can be written as $\{e, 1, 1^2, 1^3\}$.

  We have already seen that $1^2 = 1 * 1 = 1 + 1 \pmod 4 = 2 \pmod 4$.

Notice that these two cyclic groups are very similar, both having four elements. On page 388, we will find that they are **isomorphic**, since they have identical structures.

- The integers under addition (mod n) always forms a cyclic group, which can always be generated by one element.
- The symmetries of a pentagon are **not** cyclic. If we repeat a rotation again and again, we will **never** get a reflection. If we repeat a reflection again and again, we **only ever** get that reflection and its identity. Therefore, there is no way in which we can repeat the same symmetry over and over again and get **all** the symmetries. So, the group of symmetries of a pentagon cannot be cyclic.

Abelian groups

An **abelian group** is a group in which $a * b = b * a$ for **every** pair of elements a and b. In other words, it does not matter which way round we combine the elements. An abelian group is sometimes called a **commutative group**, since every pair of elements commutes.

We note that a group is abelian when the group table has symmetry in the leading diagonal.

(This class of groups is named after the prodigiously gifted Norwegian mathematician Niels Henrik Abel (1802–29).)

Determining which groups are abelian

Consider the binary operation. Addition is always commutative, and the multiplication of numbers is also always commutative. However, the multiplication of matrices is **not** commutative, since, in general, $\mathbf{AB} \neq \mathbf{BA}$, where **A** and **B** are matrices.

Thus, for example, the group of $\{0, 1, 2, 3\}$ under addition (mod 4) is abelian, since $a + b = b + a$ for any integers a and b.

To show that the group of 2×2 matrices with integer elements and determinant 1 is **not** an abelian group, we need to find **one** pair of matrices **A** and **B** with $\mathbf{AB} \neq \mathbf{BA}$.

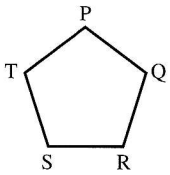
For example, we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$$

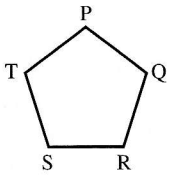
$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

This single example proves that the group of 2×2 matrices with integer elements and determinants is **not** an abelian group.

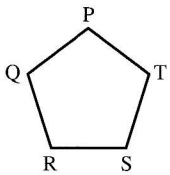
The set of transformations of a pentagon is **not** abelian, since there is a difference between performing a reflection followed by a rotation, and performing a rotation followed by a reflection.



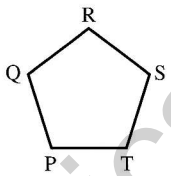
Before transformation.



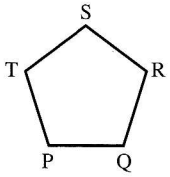
Before transformation.



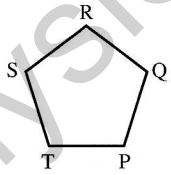
Reflection in the perpendicular bisector of RS, which passes through P.



Rotation anticlockwise through 144°.



Rotation anticlockwise through 144°.



Reflection in the perpendicular bisector of PT, which passes through R.

All cyclic groups are abelian

Proof

We need to prove that $a * b = b * a$, where a and b are any two elements in a cyclic group G. Since G is cyclic, there is some element c which **generates** G. Since c generates G, there are integers n and m for which $c^n = a$ and $c^m = b$.

Hence, we have

$$a * b = c^n * c^m = c^{n+m} = c^m * c^n = b * a$$

$$\Rightarrow \quad a * b = b * a$$

Hence, all cyclic groups are abelian.

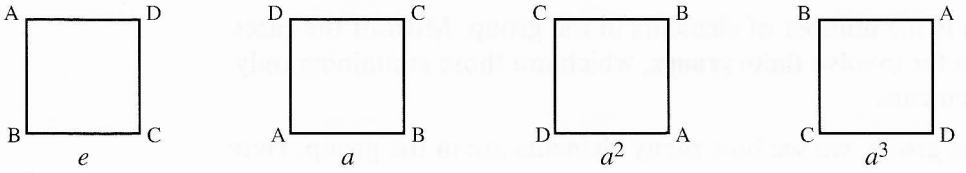
Benefit of abelian groups

It is much easier to calculate in abelian groups than in non-abelian groups. When calculating in non-abelian groups, we always have to ensure that the elements are in their correct positions. Given below is an example of calculating in a non-abelian group.

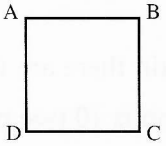
Calculating in a non-abelian group

When a group is not abelian, it is important that we do **not** switch the order of any pair of elements. For example, consider the group of symmetries of a square. This is the dihedral group D_8.

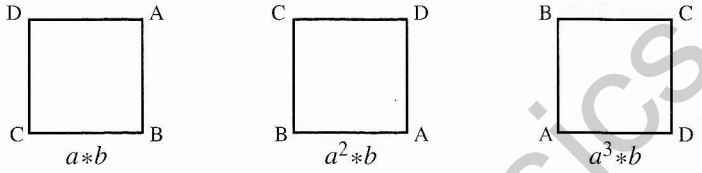
Let a denote rotation by 90° anticlockwise. Then the rotations of the square are a, a^2, a^3 and e ($a^4 = e$), as shown below.



Now let b be the reflection shown below.



The other reflections are given by $a * b$, $a^2 * b$, and $a^3 * b$, as shown below.



We note that $b * a = a^3 * b$, which leads to a way of writing down the group.

The group of symmetries of a square is the group whose elements are $\{e, a, a^2, a^3, a * b, a^2 * b, a^3 * b\}$, with the **stipulations** that $a^4 = e$, $b^2 = e$, $b * a = a^3 * b$.

These relations are enough to find the composition of any two elements. But again, we must be careful – the group is **not** abelian. Hence, we **cannot switch the order of two elements**.

For example, consider $(a * b) * (a^3 * b)$. Using $b * a = a^3 * b$, we obtain

$$(a * b) * (a^3 * b) = (a * b) * (b * a) = a * (b * b) * a$$

Using $b^2 = e$, we obtain

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

Hence, we have

$$(a * b) * (a^3 * b) = a^2$$

Similarly, we have

$$(a * b) * a^2 = a * (b * a) * a = a * (a^3 * b) * a = (a * a^3) * (b * a) =$$
$$= a^4 * (b * a) = e * (b * a) = (e * b) * a = b * a = a^3 * b$$

Because the group is not abelian, we also need to be careful when writing down inverse elements. The inverse of $a * b$ is $b^{-1} * a^{-1}$, since

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$$

Order of a group

The **order** of a group is the number of elements in the group. Most of the cases we have dealt with so far involve **finite groups**, which are those containing only a finite number of elements.

To find the order of a group, we see how many elements are in the group. Here are four examples:

- The order of the group of integers under addition (mod 4) is 4, since the elements are $\{0, 1, 2, 3\}$.
- The order of the group $\{1, i, -1, -i\}$ is 4, since again there are four elements.
- The order of the group of symmetries of a pentagon is 10 (see page 376), since there are five rotations and five reflections.
- The order of the permutation group S_n is $n!$, since there are $n!$ possible arrangements of n objects (see page 382).

Order of an element

In any finite group, any element combined repeatedly with itself must eventually give the identity element. For example, in the group of addition (mod 4), we have

$$1 + 1 + 1 + 1 = 0 \quad \text{and} \quad 2 + 2 = 0$$

In the group of symmetries of a pentagon, a rotation through 72° repeated four more times, returns the pentagon to its original position. So, five rotations through 72° are equivalent to the identity symmetry.

The **order**, or **period**, of an element is the smallest number of times we have to repeat the element before we obtain the identity element. So, in the group G, the order of an element, a, is n, where n is the smallest integer for which $a^n = e$. For example, we have:

- In the group of addition (mod 4), the order of element 1 is 4, since $1 + 1 + 1 + 1 = 0$ (mod 4).
- The order of element 3, under addition (mod 4), is 4, since $3 + 3 + 3 + 3 = 0$ (mod 4).
- The order of element 2 is 2, since we need only combine 2 twice before returning to the identity: $2 + 2 = 0$ (mod 4). The order of 0, which is also the order of every identity element in every group, is 1.

- In the symmetries of a pentagon, the order of any reflection is 2, since combining the same reflection twice returns us to the identity. The order of any rotation in the symmetries of a pentagon is 5, since we need to repeat a rotation four more times before returning to the identity.

Note

- The order of an element **must not be more** than the order of its group.
- The order of a group and the order of an element are **completely different concepts**.

Subgroups

Consider the group $\{0, 1, 2, 3\}$ of integers under addition (mod 4). If we just take the smaller set $\{0, 2\}$ of integers under addition (mod 4), we have another group. (We can confirm this by verifying all of the group properties: closure, associativity, identity and inverses.) Since $\{0, 2\}$ is a group which is wholly contained within the original group, we say that $\{0, 2\}$ is a **subgroup** of $\{0, 1, 2, 3\}$.

That is, if both G and H are groups under the same binary operation, and every member of H is contained within G, then H is a **subgroup** of G.

It is often much easier to check that H is a subgroup of G than to check from scratch that H is a group. Thus, to confirm that H is a subgroup of G, we need to proceed as follows:

1 Check that H contains the identity of G.
2 Check that if a and b are in H, then $a * b$ is also in H.
3 Ensure that for each a in H, a^{-1} is also in H.

We only need to verify that these three conditions are satisfied, since they will ensure that all four group properties are satisfied.

Closure Condition **2** checks that H is closed.

Associativity We know that H must be associative, since it is a subset of G, which is associative.

Identity Condition **1** checks that H has an identity.

Inverses Condition **3** checks that every element in H has an inverse element.

Example 11 Prove that the set H of rotations of a pentagon is a subgroup of the set of all symmetries of a pentagon.

SOLUTION

Applying the three subgroup conditions, we find the following:

1 The identity symmetry, a rotation through 0°, is in H.

2 The composition of two rotations is also a rotation so, if a and b are in H, then $a * b$ is also in H.

3 The inverse of a clockwise rotation through $\alpha°$ is an anticlockwise rotation through $\alpha°$. Therefore, the inverse of any element in H is also in H.

Isomorphic groups

We have already found that the group $G = \{0, 1, 2, 3\}$ under addition (mod 4) and the group $H = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ under multiplication are similar because they are both cyclic of order 4. By drawing their group tables, we can see that they have identical structures.

$+$ (mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	i	-1	$-\mathrm{i}$
1	1	i	-1	$-\mathrm{i}$
i	i	-1	$-\mathrm{i}$	1
-1	-1	$-\mathrm{i}$	1	i
$-\mathrm{i}$	$-\mathrm{i}$	1	i	-1

Two groups which have the same structure are said to be **isomorphic**.

To prove that G and H are isomorphic, we need to identify the way in which we can map elements of G onto elements of H.

In the case above, we can map an integer $n \in G$ onto the complex number $\mathrm{e}^{\pi \mathrm{i} n/2} \in H$. To confirm that a mapping f from G to H is an isomorphism, we must verify each of the following:

1. Each and every element of G is maps onto a **unique** element of H.
2. Each and every element of H is the image of **exactly one** element of G.
3. The image of the identity of G, f(e), is the identity of H.
4. The composition element $\mathrm{f}(a) * \mathrm{f}(b)$ in H is the same element as the image $\mathrm{f}(a * b)$ of the composition element $(a * b)$ in G.

Example 12 Show that the mapping $\mathrm{f}(n) = \mathrm{e}^{\pi \mathrm{i} n/2}$ from $G = \{0, 1, 2, 3\}$ to $H = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ is an isomorphism.

SOLUTION

We need to check that f satisfies all four conditions for isomorphism.

1. f identifies the image of each member of G.
2. Each and every member of H is the image of $\mathrm{f}(n)$ for some n. This is because
$$1 = \mathrm{e}^{0\pi \mathrm{i}/2} \quad \mathrm{i} = \mathrm{e}^{\pi \mathrm{i}/2} \quad -1 = \mathrm{e}^{2\pi \mathrm{i}/2} \quad -\mathrm{i} = \mathrm{e}^{3\pi \mathrm{i}/2}$$
3. The image of the identity of G, 0, is f(0), which is 1. This is the identity of H, which confirms that the identity element in G is mapped onto the identity element in H.
4. We must check that for all integers n and m between 0 and 3
$$\mathrm{f}(n * m) = \mathrm{f}(n) * \mathrm{f}(m)$$
Since the binary operations in G is different from that in H, the equation we have to check becomes
$$\mathrm{f}(n + m) = \mathrm{f}(n) \times \mathrm{f}(m)$$

which gives

$$f(n+m) = e^{\pi i(n+m)/2} = e^{\pi in/2} \times e^{\pi im/2} = f(n) \times f(m)$$

Hence, we have

$$f(n * m) = f(n) * f(m)$$

Since we have proved that all four conditions are satisfied, f is an isomorphism from G to H.

When we have found an isomorphism between two groups, we know that the two groups are essentially the same. The elements are different, the operations are different, but because of condition **4**, they combine in the same way.

These two groups are **isomorphic**.

Lagrange's theorem

Lagrange's theorem states that for a finite group G, of order n, the order m of the subgroup H is a factor of n.

Thus, the subgroups of a group of order 10, have either order 2 or order 5.

There is no necessity for a group of order 10 to have a subgroup of order 2, or a subgroup of order 5, but the **only possible** subgroups **must be** of one of these orders.

Lagrange's theorem helps us understand the structure of groups. The more we can understand how different groups relate to each other, the more we can hope to understand about groups in general.

Examples of Lagrange's theorem

We have found already that $\{0, 2\}$ is a subgroup of the group $\{0, 1, 2, 3\}$ of integers under addition (mod 4). $\{0, 2\}$ has order 2, and $\{0, 1, 2, 3\}$ has order 4. Since we know that 4 is divisible by 2, this example agrees with Lagrange's theorem.

On page 387, we also found that the group of rotations of a pentagon are a subgroup of the symmetries of a pentagon. There are five rotations and ten symmetries of the pentagon. Again, we see that the order of the smaller group (5) is a factor of the order of the larger group (10). This also agrees with Lagrange's theorem.

One consequence of Lagrange's theorem is the following:

The order of an element is a factor of the order of the group.

Take an element a of a group, G, and consider the cyclic group generated by a.

If a has order n, then $a^n = e$. So, the group, H, generated by a is $\{e, a, a^2, a^3, \ldots, a^{n-1}\}$.

Since H is a subgroup of G, we can use Lagrange's theorem, which states that the order of H divides the order of G.

But the order of H is n. Hence, the order of a divides the order of G.

Example 13 A group, G, has subgroups $\{a\}$, $\{a, b, c, d, f\}$, and $\{a, d\}$.

a) What is the identity of G?

b) Could G contain only the five elements $\{a, b, c, d, f\}$? Explain your answer.

c) What is the smallest possible order of G?

SOLUTION

a) The identity of G must be a. This is because every subgroup of G must contain the identity of G, and $\{a\}$ is a subgroup of G.

b) The order of a subgroup divides the order of a group. So, the order of G must be divisible by 1, by 5 and by 2. Therefore, the order of G cannot be 5, and so G cannot contain only the five elements a, b, c, d and f.

c) The smallest order that G could have is the smallest number divisible by 1, 2 and 5. This number is 10.

Groups of order 3

If G is a group of order 3, then the order of every element of G must divide 3. That is, the order of every element of G must be either 1 or 3.

There is only one element of order 1, the identity element e.

Since there are three elements in G, there must be two elements which are not of order 1 and hence must each be of order 3.

Let a be an element of order 3. Then a, a^2 and $a^3 = e$ are three different elements in the group. Since there are only three elements in the group, it follows that a, a^2 and e are **all** the elements in the group, and so G has to be a cyclic group of order 3.

Hence, all groups of order 3 are cyclic. They are also all isomorphic with each other.

Groups of order 4

If G is a group of order 4, then all the elements must have order 1, 2 or 4. One of the elements must have order 1; this is the identity element e. If G has an element a of order 4, then e, a, a^2 and a^3 are the four elements of G, and therefore G must be the cyclic group generated by a.

Thus, if G is **not** the cyclic group generated by a, no element of G has order 4. If G has **no** elements of order 4, then every element apart from e must have order 2. Therefore, the group is $\{e, a, b, c\}$ and $a^2 = b^2 = c^2 = e$.

The only unknown is how different elements combine.

If $a*b=a$, then premultiplying both sides by a^{-1} gives

$$a^{-1}*a=a^{-1}*(a*b),\ =(a^{-1}*a)*b=e*b=b$$

Since $a^{-1}*a=e$, this gives $b=e$. This cannot be true, since e, a, b, c were assumed to be four different elements of the group. Hence $a*b\neq a$.

If $a*b=b$, then by postmultiplying both sides by b^{-1}, we can prove similarly that $a=e$. A third option would be that $a*b=e$, but then premultiplying both sides by a would give $a*a*b=a*e$. Since $a^2=e$, this gives $b=a$, which is also impossible. Since the set is closed and $a*b\neq a$, b or e, we have

$$a*b=c$$

Similarly, we can prove that $b*c=a$, and that $a*c=b$. Therefore, there is only one way in which a group of order 4 can be anything other than cyclic, and this happens if the elements combine as described above. The composition table for this group is then:

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

After filling in the row and the column next to e, and inserting e for a^2, b^2 and c^2, we can complete the composition table very simply by using the rule that each member of the group, e, a, b, c, occurs once and only once in every row and column.

Distinguishing between the two groups of order 4

We have proved that there are only two different groups of order 4. Hence, any group of order 4 is either isomorphic to a cyclic group of order 4, or isomorphic to the group whose composition table is given above.

There are two ways to distinguish between groups of order 4:

- If G contains an element of order 4, then it is cyclic.
- If G contains three elements of order 2, then it is not cyclic.

Groups of order 5

If G is a group of order 5, then the order of every element of G must be a factor of 5. Since 5 is prime, the order of each element must be either 1 or 5. There is only one element of order 1, and that is the identity element.

Select any element other than the identity element, and let this be a. Then a has order 5, and so the five elements of the group must be a, a^2, a^3, a^4 and a^5, which is e. Since the group has only five elements, these are all the elements of the group, and the group is cyclic.

We note that every element excluding the identity element is a generator.

Therefore, **any** group of order 5 is **cyclic**, and **all** groups of order 5 are **isomorphic**.

Groups of order 6

There are only two groups of order 6:

- Type 1: the cyclic group.
- Type 2: the group of symmetries of an equilateral triangle.

If we are given a group of order 6, there are several ways to tell whether it is cyclic.

Distinguishing between types 1 and 2

If G is abelian, then it must be cyclic. The group of symmetries of an equilateral triangle is not abelian.

If G has an element of order 6, then it must be a member of the cyclic group of order 6. There is no symmetry that completely generates the group of symmetries of an equilateral triangle.

If G has three elements of order 2, then it is isomorphic to the group of symmetries of an equilateral triangle. These three elements of order 2 correspond to the three reflections of an equilateral triangle. In the cyclic group of order 6, there is only one element of order 2.

Example 14 The symmetries of a square form the dihedral group, D_8. Find

a) any subgroups of D_8 of order 3
b) all the subgroups of D_8 of order 4.

SOLUTION

a) Since D_8 has order 8, there can be no subgroups of order 3, since 3 does not divide 8.

b) Let H be a subgroup of order 4.

If there is a rotation of 90° in H, then H must be the set of **all** rotations of a square. This is because a rotation of 90° generates all four rotations of a square, and because H has only four elements.

If a reflection in a diagonal is in H, then the only other reflection in H is the reflection in the other diagonal.

If we were to include any other reflection, then H must contain **all** the reflections. Thus, H must contain all four reflections **and** the identity element, which is **impossible**, since H has order 4.

Similarly, if a reflection which is not in a diagonal is included, the other reflection which is not a reflection in either diagonal, must be in the subgroup.

Therefore, the only subgroups of D_8 of order 4 are:

- All four rotations (cyclic subgroup).
- One rotation of 180°, together with the two reflections in the diagonals and the identity.
- One rotation of 180°, together with the two reflections which are **not** reflections in the diagonals and the identity.

Example 15 G is the group of symmetries of a square. Find all the solutions to the equation $x^3 = x$ in the group G.

SOLUTION

We really want to divide both sides of this equation by x. However, we cannot divide in groups, and so we must first multiply both sides of the equation by x^{-1}. Since the group is not abelian, we must specify whether we are going to pre- or postmultiply by x^{-1}. We will pick postmultiplication (although either way works in this case), which gives

$$\begin{aligned} & x^3 = x \\ \Rightarrow \quad & x * x * x = x \\ \Rightarrow \quad & (x * x * x) * x^{-1} = x * x^{-1} \\ \Rightarrow \quad & (x * x) * (x * x^{-1}) = x * x^{-1} \\ \Rightarrow \quad & x * x * e = e \\ \Rightarrow \quad & x * x = e \\ \Rightarrow \quad & x^2 = e \end{aligned}$$

Therefore, the solution is all symmetries which, done twice, give the identity.

Such transformations are called **self inverse**, since they are their own inverses. (See also page 375.)

In the group of symmetries of a square, these transformations are all four reflections, a rotation through 180°, and the identity transformation.

Exercise 17B

1 Consider the two groups:

G_1: $(\mathbb{R}^+, \times)$, the set of positive real numbers under multiplication

G_2: $(\mathbb{R}, +)$, the set of real numbers under addition

i) What are the identity elements in each of the two groups?

ii) Why must zero be excluded from the set of elements in G_1?

Consider the mapping

$$f: \mathbb{R}^+ \to \mathbb{R}$$

$$f(x) = \log_e(x)$$

iii) Explain why this mapping defines an isomorphism from G_1 to G_2. (NICCEA)

2 Consider the following three groups.

G_1: $(\{1, 3, 7, 9\}, \times_{10})$, i.e. the set $\{1, 3, 7, 9\}$ under multiplication mod 10

G_2: $(\{1, 5, 7, 11\}, \times_{12})$

G_3: $(\{1, 3, 5, 7\}, \times_8)$

Draw up the group tables for G_1, G_2 and G_3 and use them to:

i) find which two are isomorphic to each other and write down an isomorphism between them

ii) solve the equation $x^3 = x$ in each of the three groups. (NICCEA)

3 Show that the set of all matrices of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, where n is an integer, forms a group under the operation of matrix multiplication. (You may assume the associativity of matrix multiplication.) Describe the geometrical transformation represented by the matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. (OCR)

4 i) The set of integers $\{1, 3, 5, 7\}$, together with the operation of multiplication modulo 8, forms a group G. Show the operation table for G.

ii) Identify three proper subgroups of G.

iii) The functions f, g, h, k are defined, for $x \neq 0$, as follows:

$$f: x \mapsto x \qquad g: x \mapsto \frac{1}{x} \qquad h: x \mapsto -x \qquad k: x \mapsto -\frac{1}{x}$$

The set $\{f, g, h, k\}$ under the operation of composition of functions forms a group H. Show the operation table for H.

iv) State, with a reason, whether or not G and H are isomorphic. (OCR)

5 a) Let $G = \{1, 3, 5, 7\}$. Construct the Cayley table for G with respect to multiplication (mod 8), and determine whether or not G is a group with respect to this operation.

b) Explain why the set $\mathbb{Z}_8 - \{0\}$ is **not** a group under multiplication (mod 8).

c) For which values of n does $\mathbb{Z}_n - \{0\}$ form a group under multiplication (mod n)?

(SQA/CSYS)

6 Show that the set of all matrices of the form $\begin{pmatrix} 1-n & n \\ -n & 1+n \end{pmatrix}$, where n is an integer (positive, negative or zero), forms a group G under the operation of matrix multiplication. (You may assume that matrix multiplication is associative.)

The subset of G which consists of those elements for which n is an even integer (positive, negative or zero) is denoted by H. Determine whether or not H is a subgroup of G, justifying your answer. (OCR)

7 a) It is given that x and y are elements of a multiplicative group G with identity e, and that $x^2 = e$, $y^2 = e$ and $(xy)^2 = e$. Show that $xy = yx$.

b) The multiplicative group H is commutative. Two elements a and b of H are such that a has order 2 and b has order 3. Show that ab has order 6. (OCR)

8 The group G consists of the set of six matrices **I**, **A**, **B**, **C**, **D**, **E** defined below, under the operation of matrix multiplication.

$$\mathbf{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \mathbf{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \mathbf{D} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \mathbf{E} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

i) Copy and complete the following group table for G.

	I	**A**	**B**	**C**	**D**	**E**
I	**I**	**A**	**B**	**C**	**D**	**E**
A	**A**	**B**	**I**	**E**	**C**	
B	**B**	**I**	**A**	**D**	**E**	
C	**C**	**D**	**E**			
D	**D**	**E**	**C**			
E						

ii) Show that G is not cyclic.

iii) Find all the proper subgroups of G.

iv) The group H consists of the six elements 1, 2, 3, 4, 5, 6 under multiplication modulo 7. The multiplicative group K consists of the six elements i, a, a^2, b, ab, a^2b, where i is the identity, $a^3 = b^2 = i$ and $ba = a^2b$. Determine whether

a) H is isomorphic to G

b) K is isomorphic to G

c) H is isomorphic to K.

Give reasons for your conclusions. (OCR)

9 The multiplicative group G has eight elements $e, a, b, c, ab, ac, bc, abc$, where e is the identity. The group is commutative, and the order of each of the elements a, b, c is 2.

i) State the orders of the elements ab and abc.

ii) Find four subgroups of G of order 4.

iii) Give a reason why no group of order 8 can have a subgroup of order 3.

The group H has elements $0, 1, 2, \ldots, 7$ with group operation addition modulo 8.

iv) Find the order of each element of H.

v) Determine whether G and H are isomorphic and justify your conclusion. (OCR)

10 The multiplication tables for G, a cyclic group of order 6, and H, a non-cyclic group of order 6, are shown below.

G

	e	g	g^2	g^3	g^4	g^5
e	e	g	g^2	g^3	g^4	g^5
g	g	g^2	g^3	g^4	g^5	e
g^2	g^2	g^3	g^4	g^5	e	g
g^3	g^3	g^4	g^5	e	g	g^2
g^4	g^4	g^5	e	g	g^2	g^3
g^5	g^5	e	g	g^2	g^3	g^4

H

	i	h_1	h_2	h_3	h_4	h_5
i	i	h_1	h_2	h_3	h_4	h_5
h_1	h_1	h_2	i	h_5	h_3	h_4
h_2	h_2	i	h_1	h_4	h_5	h_3
h_3	h_3	h_4	h_5	i	h_1	h_2
h_4	h_4	h_5	h_3	h_2	i	h_1
h_5	h_5	h_3	h_4	h_1	h_2	i

i) Give the order of each element of G.
ii) Give the order of each element of H and write down all the proper subgroups of H.
iii) The group M has elements $1, 3, 4, 9, 10, 12$ with operation multiplication modulo 13. State to which of G and H the group M is isomorphic. For the two groups which are isomorphic, write down a correspondence between the elements. (OCR)

11 The group $G = \{e, p_1, p_2, p_3, q_1, q_2, q_3, q_4\}$ has order 8 and its multiplication table is shown below.

	e	p_1	p_2	p_3	q_1	q_2	q_3	q_4
e	e	p_1	p_2	p_3	q_1	q_2	q_3	q_4
p_1	p_1	p_2	p_3	e	q_4	q_3	q_1	q_2
p_2	p_2	p_3	e	p_1	q_2	q_1	q_4	q_3
p_3	p_3	e	p_1	p_2	q_3	q_4	q_2	q_1
q_1	q_1	q_3	q_2	q_4	e	p_2	p_1	p_3
q_2	q_2	q_4	q_1	q_3	p_2	e	p_3	p_1
q_3	q_3	q_2	q_4	q_1	p_3	p_1	e	p_2
q_4	q_4	q_1	q_3	q_2	p_1	p_3	p_2	e

i) Find the orders of p_1 and p_3.
ii) Find two subgroups of order 4.
iii) State whether G has any subgroups of order 6 and justify your answer.
iv) The group H has elements $e^{\frac{1}{4}k\pi i}$, where $k = 0, 1, \ldots, 7$, and the group operation is complex multiplication. Show that H is cyclic.
v) The set $K = \{i, a, a^2, a^3, b, ab, a^2b, a^3b\}$ is a commutative multiplicative group of order 8. The identity element is i and $a^4 = b^2 = i$. Determine whether any two of G, H, K are isomorphic to each other and justify your conclusions. (OCR)

12 **a)** Explain why $4 \times 14 = 2$ for multiplication modulo 18.

b) Complete the group table shown below for multiplication modulo 18.

	2	4	8	10	14	16
2	4	8	16	2	10	14
4	8	16	14	4	2	10
8	16	14	10	8	4	2
10	2	4				
14	10	2				
16	14	10				

c) State the identity element. Find a subgroup of order 2 and a subgroup of order 3.

d) State, with a reason, whether the group in part **b** is isomorphic to the group of symmetries of an equilateral triangle. (NEAB/SMP 16–19)

13 Consider the matrices

$$\mathbf{A} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \quad \mathbf{E}_1 = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix} \quad \mathbf{E}_2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \quad \mathbf{E}_3 = \begin{pmatrix} 1 & 0 \\ 0 & \frac{3}{10} \end{pmatrix}$$

$$\mathbf{E}_4 = \begin{pmatrix} 1 & -\frac{2}{3} \\ 0 & 1 \end{pmatrix}$$

i) Describe the geometrical transformations which correspond to $\mathbf{E}_1$ and $\mathbf{E}_2$.

ii) Calculate the three products: $\mathbf{E}_1\mathbf{A}$, $\mathbf{E}_2(\mathbf{E}_1\mathbf{A})$, $\mathbf{E}_3(\mathbf{E}_2\mathbf{E}_1\mathbf{A})$. Verify that $\mathbf{E}_4(\mathbf{E}_3\mathbf{E}_2\mathbf{E}_1\mathbf{A}) = \mathbf{I}$.

iii) Find the inverse matrices $\mathbf{E}_1^{-1}, \mathbf{E}_2^{-1}, \mathbf{E}_3^{-1}$ and $\mathbf{E}_4^{-1}$.

iv) State how $\mathbf{A}$ can be written as a product of these inverse matrices. Describe fully the geometrical transformation corresponding to $\mathbf{A}$ in terms of a composition of shears and stretches, giving the scale factors and relevant directions in each case. (NICCEA)

14 **i)** Form the combination table for the set $\{3, 6, 9, 12\}$ under the operation multiplication modulo 15. Write down any elements which are self-inverse.

ii) A binary operation $*$ is defined on $\mathbb{R}$ by

$$r * s = r + s + rs$$

Given that $S = \{x : x \in \mathbb{R}, x \neq -1\}$, show that S forms a group under the operation $*$.

Solve the equation

$$(x * 2) * x = 3 * (4 * x)$$ (EDEXCEL)

15 A non-abelian group G consists of eight 2×2 matrices, and the binary operation is matrix multiplication. The eight distinct elements of G can be written as

$$G = \{\mathbf{I}, \mathbf{A}, \mathbf{A}^2, \mathbf{A}^3, \mathbf{B}, \mathbf{AB}, \mathbf{A}^2\mathbf{B}, \mathbf{A}^3\mathbf{B}\} \qquad (*)$$

where $\mathbf{I}$ is the identity matrix, and $\mathbf{A}$, $\mathbf{B}$ are 2×2 matrices such that

$$\mathbf{A}^4 = \mathbf{I} \quad \mathbf{B}^2 = \mathbf{I} \quad \text{and} \quad \mathbf{BA} = \mathbf{A}^3\mathbf{B}$$

i) Show that $(\mathbf{A}^2\mathbf{B})(\mathbf{AB}) = \mathbf{A}$ and $(\mathbf{AB})(\mathbf{A}^2\mathbf{B}) = \mathbf{A}^3$.

ii) Evaluate the following products, giving each one as an element of G as listed in $(*)$,

$$(\mathbf{AB})(\mathbf{A}) \quad (\mathbf{AB})(\mathbf{AB}) \quad (\mathbf{B})(\mathbf{A}^2)$$

iii) Find the order of each element of G.
iv) Show that $\{\mathbf{I}, \mathbf{A}^2, \mathbf{B}, \mathbf{A}^2\mathbf{B}\}$ is a subgroup of G.
v) Find the other two subgroups of G which have order 4.
vi) For each of the three subgroups of order 4, state whether or not it is a cyclic subgroup.

(MEI)

16 Four of the subgroups of a group, $\mathbf{X}$, are $\{A\}$, $\{A, B, C, D\}$, $\{A, C\}$ and $\{A, E\}$.

a) Explain why $\mathbf{X}$ must contain more than the five elements given above. State the minimum number of extra elements which $\mathbf{X}$ must have.
b) The subgroup $\{A, B, C, D\}$ is cyclic. State possible geometrical transformations which could correspond to the elements A, B, C and D and construct a table for this subgroup.

(NEAB/SMP 16–19)

17 The matrix $\mathbf{M}(\alpha)$ is defined by

$$\mathbf{M}(\alpha) = \begin{pmatrix} \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \end{pmatrix}$$

a) Show that the set $G = \{\mathbf{M}(\alpha) : \alpha \in \mathbb{C}, \alpha \neq 0\}$ forms a group under the operation of matrix multiplication, which may be assumed to be associative.
b) Find the order of $\mathbf{M}(\frac{1}{3}\mathrm{i})$ and hence find a subgroup of G of order 4 and a subgroup of G of order 2.
c) Show that the set $H = \{\mathbf{M}(\alpha) : \alpha = 3^k, k \in \mathbb{Z}\}$ is a subgroup of G.
d) Explain why the set $S = \{\mathbf{M}(\alpha) : \alpha = \frac{1}{3}k, k \in \mathbb{Z}, k \neq 0\}$ is not a subgroup of G.

(EDEXCEL)

18 a) Show that if $M = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ then $M^2 = I$, where I is the 2×2 identity matrix.

By choosing two different values of θ, exhibit two matrices A, B such that $A^2 = I$ and $B^2 = I$ but $(AB)^2 \neq I$.

b) Prove that if C and D are $n \times n$ matrices such that $C^2 = I$, $D^2 = I$ **and** C **and** D **commute**, then $(CD)^2 = I$.
c) Let G be an abelian group, and define H by

$$H = \{g \in G : g^2 = e\}$$

where e is the identity element of G. Show that H is a subgroup of G.
d) The following is the multiplication table of the group D_8.

	e	a	b	c	p	q	r	s
e	e	a	b	c	p	q	r	s
a	a	b	c	e	q	r	s	p
b	b	c	e	a	r	s	p	q
c	c	e	a	b	s	p	q	r
p	p	s	r	q	e	c	b	a
q	q	p	s	r	a	e	c	b
r	r	q	p	s	b	a	e	c
s	s	r	q	p	c	b	a	e

i) Determine whether or not D_8 is abelian.
ii) Determine whether or not $\{g \in D_8 : g^2 = e\}$ is a subgroup of D_8. (SQA/CSYS)

19 The six permutations of the set $\{1, 2, 3\}$ are

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

i) If $\circ$ denotes the composition of permutations, show that $\pi_5 \circ \pi_3 = \pi_6$.
ii) Show that $\pi_3 \circ (\pi_5 \circ \pi_2) = (\pi_3 \circ \pi_5) \circ \pi_2$.
iii) Draw up a table for the group formed by $\circ$ operating on the set of these six permutations.
iv) State a group which is isomorphic to this group of six permutations. (NICCEA)

20 Consider the binary operation $\otimes$ as defined by

$$a \otimes b = a + b + ab$$

i) Show that

$$a \otimes (b \otimes c) = a + b + c + ab + bc + ac + abc$$

ii) Prove $\otimes$ is associative.

Consider the algebraic system consisting of the set of real numbers, $\mathbb{R}$, and the operation $\otimes$.

iii) Find the identity element for this binary operation.
iv) By considering the inverse of the element a, show that this system is **not** a group.
v) A group can be formed using this operation and a subset of $\mathbb{R}$. State how $\mathbb{R}$ can be amended to form this subset. (NICCEA)

Real vector spaces

Groups have one binary operation. In **vector spaces**, there are two operations: addition and multiplication. The simplest, interesting real vector space is the two-dimensional vector space $\mathbb{R}^2$.

Just as with groups, to check that we have a real vector space, we need to verify that certain properties are satisfied.

A **real vector space** consists of a set of vectors V, which admit of two operations, $+$ and $.$, and have the following six properties:

- $(V, +)$ is an **abelian group**. The identity of this group is the zero vector $\mathbf{0}$.
- If $\mathbf{v}$ is a vector in V and $\lambda \in \mathbb{R}$, then $\lambda \,.\, \mathbf{v}$ is a vector in V.
- If $\mathbf{v}$ and $\mathbf{w}$ are vectors in V and $\lambda \in \mathbb{R}$, then $\lambda \,.\, (\mathbf{v} + \mathbf{w}) = \lambda \,.\, \mathbf{v} + \lambda \,.\, \mathbf{v}$.
- If $\mathbf{v} \in V$ and $\lambda, \mu \in \mathbb{R}$, then $(\lambda + \mu) \,.\, \mathbf{v} = \lambda \,.\, \mathbf{v} + \mu \,.\, \mathbf{v}$.
- If $\mathbf{v} \in V$ and $\lambda, \mu \in \mathbb{R}$, then $\lambda(\mu \,.\, \mathbf{v}) = (\lambda\mu) \,.\, \mathbf{v}$.
- For any $\mathbf{v} \in V$, $1 \,.\, \mathbf{v} = \mathbf{v}$.

The last four properties define the operation of multiplication by scalars, which we have already used with geometric vectors (see page 94).

Three-dimensional space

Let V be the three-dimensional vector space $\mathbb{R}^3$. We can define any vector in terms of **i**, **j** and **k**. For example, $2\mathbf{i} + 3\mathbf{k}$ is a vector in this space. We know how to perform addition in this vector space: we just add the components separately. We also know how to multiply a vector by a real scalar. All of the real vector space properties are satisfied.

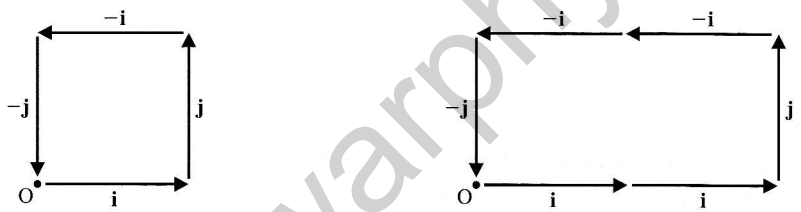
Complex numbers

The set of all complex numbers can be treated as a real vector space. We can write any complex number in the form $a + b\mathrm{i}$, where a and b are real numbers. Addition is performed in the normal way, and we know how to multiply any complex number by a **real** scalar. Again, we verify that the real vector space properties are satisfied.

Linearly independent sets

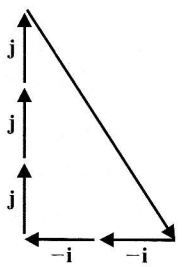
Let V be a vector space. We say that $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a **linearly independent** set if, whenever $\sum_{k=1}^{n} \lambda_k \mathbf{v}_k = 0$, we can deduce that $\lambda_k = 0$ for every k.

Let us consider the vectors **i** and **j** in normal two-dimensional space. And let us imagine that we are trying to follow paths from the origin back to itself by following the vectors **i** and **j**. Two examples are shown below.



In both cases, the total number of components of vector **i** we follow is 0. Similarly, the total number of components of vector **j** we follow is 0. Now, the only way that $a\mathbf{i} + b\mathbf{j} = 0$ is if $a = b = 0$. So, **i** and **j** are linearly independent.

On the other hand, the vectors **i**, **j** and $2\mathbf{i} - 3\mathbf{j}$ are **not** linearly independent. The diagram on the right shows that $-2\mathbf{i} + 3\mathbf{j} + 1(2\mathbf{i} - 3\mathbf{j}) = \mathbf{0}$.



Any three vectors in two-dimensional space are **not** linearly independent.

Spanning sets and basis vectors

Let V be a vector space. The set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is called a **spanning set** if we can write any element $\mathbf{v}$ of V as a sum,

$$\mathbf{v} = \sum_{k=1}^{n} \lambda_k \mathbf{v}_k$$

A **basis** is a spanning set that is also a linearly independent set. A basis exists in any real vector space. Any two bases of the same vector space have the same number of elements.

The vectors **i**, **j**, and **k** form a basis for three-dimensional space.

The number of elements in a basis of V is called the **dimension** of V.

The vectors 1 and i form a basis for the set of all complex numbers. Thus, the set of all complex numbers have dimension two when regarded as a real vector space.

Linear mappings

A linear mapping $\mathrm{T} : V \to V$ is one which satisfies

$$\mathrm{T}(\lambda \mathbf{v}) = \lambda \mathrm{T}(\mathbf{v}) \quad \text{for every } \lambda \in \mathbb{R}, \mathbf{v} \in V$$

and

$$\mathrm{T}(\mathbf{v} + \mathbf{w}) = \mathrm{T}(\mathbf{v}) + \mathrm{T}(\mathbf{w})$$

Linear mappings are completely determined by their effect on a basis.

For example, consider an anticlockwise rotation of 90° in $\mathbb{R}^2$. This moves vector **i** onto **j**, and it also moves **j** onto $-\mathbf{i}$. It follows that the vector $2\mathbf{i} + 3\mathbf{j}$ is carried to $2\mathbf{j} + 3(-\mathbf{i})$.

Now, if we use $\mathbf{e}_1$ to denote **i**, the first basis element, and $\mathbf{e}_2$ to denote **j**, the second basis element, we have

$$\mathrm{T}(\mathbf{e}_1) = \mathbf{e}_2 \qquad \mathrm{T}(\mathbf{e}_2) = -\mathbf{e}_1$$

For convenience, we represent $\mathbf{e}_1$ by the column vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $\mathbf{e}_2$ by the column vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

We can then represent T by the matrix

$$\mathbf{T} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

which gives

$$\mathrm{T}(\mathbf{e}_1) = \mathbf{T}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{e}_2$$

and

$$\mathrm{T}(\mathbf{e}_2) = \mathbf{T}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = -\mathbf{e}_1$$

We note that T depends on our choice of basis.

Example 16 illustrates the difference that a change of basis can make to a transformation matrix.