# REPRESENTATIONS AND CHARACTERS OF GROUPS

GORDON JAMES AND MARTIN LIEBECK
*Department of Mathematics,*
*Imperial College, London*

Second Edition

CAMBRIDGE
UNIVERSITY PRESS

# 1
# Groups and homomorphisms

This book is devoted to the study of an aspect of group theory, so we begin with a résumé of facts about groups, most of which you should know already. In addition, we introduce several examples, such as dihedral groups and symmetric groups, which we shall use extensively to illustrate the later theory. An elementary course on abstract algebra would normally cover all the material in the chapter, and any book on basic group theory will supply you with further details. One or two results which we shall use only infrequently are demoted to the exercises at the end of the chapter – you can refer to the solutions if necessary.

## Groups

A *group* consists of a set $G$, together with a rule for combining any two elements $g$, $h$ of $G$ to form another element of $G$, written $gh$; this rule must satisfy the following axioms:

(1) for all $g$, $h$, $k$ in $G$,

$$(gh)k = g(hk);$$

(2) there exists an element $e$ in $G$ such that for all $g$ in $G$,

$$eg = ge = g;$$

(3) for all $g$ in $G$, there exists an element $g^{-1}$ in $G$ such that

$$gg^{-1} = g^{-1}g = e.$$

We refer to the rule for combining elements of $G$ as the *product operation* on $G$.

Axiom (1) states that the product operation is *associative*; the element $e$ in axiom (2) is an *identity* element of $G$; and $g^{-1}$ is an *inverse* of $g$ in axiom (3).

It is elementary to see that $G$ has just one identity element, and that every $g$ in $G$ has just one inverse. Usually we write 1, rather than $e$, for the identity element of $G$.

The product of an element $g$ with itself, $gg$, is written $g^2$; similarly $g^3 = g^2 g$, $g^{-2} = (g^{-1})^2$, and so on. Also, $g^0 = 1$.

If the number of elements in $G$ is finite, then we call $G$ a *finite group*; the number of elements in $G$ is called the *order* of $G$, and is written $|G|$.

*1.1 Examples*

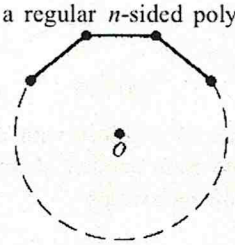
(1) Let $n$ be a positive integer, and denote by $\mathbb{C}$ the set of all complex numbers. The set of $n$th roots of unity in $\mathbb{C}$, with the usual multiplication of complex numbers, is a group of order $n$. It is written as $C_n$ and is called the *cyclic* group of order $n$. If $a = e^{2\pi i/n}$, then

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

and $a^n = 1$.

(2) The set $\mathbb{Z}$ of all integers, under addition, is a group.

(3) Let $n$ be an integer with $n \geqslant 3$, and consider the rotation and reflection symmetries of a regular $n$-sided polygon.




There are $n$ rotation symmetries: these are $\rho_0, \rho_1, \ldots, \rho_{n-1}$ where $\rho_k$ is the (clockwise) rotation about the centre $O$ through an angle $2\pi k/n$. There are also $n$ reflection symmetries: these are reflections in the $n$ lines passing through $O$ and a corner or the mid-point of a side of the polygon.

These $2n$ rotations and reflections form a group under the product operation of *composition* (that is, for two symmetries $f$ and $g$, the product $fg$ means 'first do $f$, then do $g$'). This group is called the *dihedral group* of order $2n$, and is written $D_{2n}$.

Let $A$ be a corner of the polygon. Write $b$ for the reflection in the

line through $O$ and $A$, and write $a$ for the rotation $\rho_1$. Then the $n$ rotations are

$$1, a, a^2, \ldots, a^{n-1}$$

(where 1 denotes the identity, which leaves the polygon fixed); and the $n$ reflections are

$$b, ab, a^2b, \ldots, a^{n-1}b.$$

Thus all elements of $D_{2n}$ are products of powers of $a$ and $b$ – that is, $D_{2n}$ is *generated* by $a$ and $b$.

Check that

$$a^n = 1,\ b^2 = 1 \text{ and } b^{-1}ab = a^{-1}.$$

These relations determine the product of any two elements of the group. For example, we have $ba^j = a^{-j}b$ (using the relation $ba = a^{-1}b$), and hence

$$(a^ib)(a^jb) = a^iba^jb = a^ia^{-j}bb = a^{i-j}.$$

We summarize all this in the presentation

$$D_{2n} = \langle a, b\colon a^n = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1}\rangle.$$

(4) For $n$ a positive integer, the set of all permutations of $\{1, 2, \ldots, n\}$, under the product operation of composition, is a group. It is called the *symmetric group* of degree $n$, and is written $S_n$. The order of $S_n$ is $n!$.

(5) Let $F$ be either $\mathbb{R}$ (the set of real numbers) or $\mathbb{C}$ (the set of complex numbers). The set of all invertible $n \times n$ matrices with entries in $F$, under matrix multiplication, forms a group. This group is called the *general linear group* of degree $n$ over $F$, and is denoted by $\mathrm{GL}(n, F)$. It is an infinite group. The identity of $\mathrm{GL}(n, F)$ is of course the identity matrix, which we denote by $I_n$ or just $I$.

A group $G$ is said to be *abelian* if $gh = hg$ for all $g$ and $h$ in $G$. While $C_n$ and $\mathbb{Z}$ are abelian, most of the other examples given above are non-abelian groups.

## Subgroups

Let $G$ be a group. A subset $H$ of $G$ is said to be a *subgroup* if $H$ is itself a group under the product operation inherited from $G$. We use the notation $H \leqslant G$ to indicate that $H$ is a subgroup of $G$.

It is easy to see that a subset $H$ of a group $G$ is a subgroup if and only if the following two conditions hold:

(1) $1 \in H$, and
(2) if $h, k \in H$ then $hk^{-1} \in H$.

*1.2 Examples*

(1) For every group $G$, both $\{1\}$ and $G$ are subgroups of $G$.

(2) Let $G$ be a group and $g \in G$. The subset

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

is a subgroup of $G$, called the *cyclic subgroup generated by* $g$. If $g^n = 1$ for some $n \geqslant 1$, then $\langle g \rangle$ is finite. In this case, let $r$ be the least positive integer such that $g^r = 1$; then $r$ is equal to the number of elements in $\langle g \rangle$ – indeed,

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{r-1}\}.$$

We call $r$ the *order* of the element $g$.

If $G = \langle g \rangle$ for some $g \in G$ then we call $G$ a *cyclic* group. The groups $C_n$ and $\mathbb{Z}$ in Examples 1.1 are cyclic.

(3) Let $G$ be a group and let $a, b \in G$. Define $H$ to be the subset of $G$ consisting of all elements which are products of powers of $a$ and $b$ – that is, all elements of the form

$$a^{i_1} b^{j_1} a^{i_2} b^{j_2} \ldots a^{i_n} b^{j_n}$$

for some $n$, where $i_k, j_k \in \mathbb{Z}$ for $1 \leqslant k \leqslant n$. Then $H$ is a subgroup of $G$; we call $H$ the subgroup *generated* by $a$ and $b$, and write

$$H = \langle a, b \rangle.$$

Given any finite set $S$ of elements of $G$, we can similarly define $\langle S \rangle$, the subgroup of $G$ generated by $S$.

This construction gives a powerful method of finding new groups as subgroups of given groups, such as general linear or symmetric groups. We illustrate the construction in the next example, and again in Example 1.5 below.

(4) Let $G = \mathrm{GL}(2, \mathbb{C})$, the group of invertible $2 \times 2$ matrices with entries in $\mathbb{C}$, and let

$$A = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Put $H = \langle A, B \rangle$, the subgroup of $G$ generated by $A$ and $B$. Check that

$$A^4 = I,\ A^2 = B^2,\ B^{-1}AB = A^{-1}.$$

Using the third relation, we see that every element of $H$ has the form $A^iB^j$ for some integers $i, j$; and using the first two relations, we can take $0 \leqslant i \leqslant 3$ and $0 \leqslant j \leqslant 1$. Hence $H$ has at most eight elements. Since the matrices

$$A^iB^j \quad (0 \leqslant i \leqslant 3,\ 0 \leqslant j \leqslant 1)$$

are all distinct, in fact $|H| = 8$.

The group $H$ is called the *quaternion group* of order 8, and is written $Q_8$. The above three relations determine the product of any two elements of $Q_8$, so we have the presentation

$$Q_8 = \langle A, B\colon A^4 = I,\ A^2 = B^2,\ B^{-1}AB = A^{-1} \rangle.$$

(5) A *transposition* in the symmetric group $S_n$ is a permutation which interchanges two of the numbers $1, 2, \ldots, n$ and fixes the other $n - 2$ numbers. Every permutation $g$ in $S_n$ can be expressed as a product of transpositions. It can be shown that either all such expressions for $g$ have an even number of transpositions, or they all have an odd number of transpositions; we call $g$ an *even* or an *odd* permutation, accordingly. The subset

$$A_n = \{g \in S_n\colon\ g \text{ is an even permutation}\}$$

is a subgroup of $S_n$, called the *alternating group* of degree $n$.

## Direct products

We describe a construction which produces a new group from given ones.

Let $G$ and $H$ be groups, and consider

$$G \times H = \{(g, h)\colon g \in G \text{ and } h \in H\}.$$

Define a product operation on $G \times H$ by

$$(g, h)(g', h') = (gg', hh')$$

for all $g, g' \in G$ and all $h, h' \in H$. With this product operation, $G \times H$ is a group, called the *direct product* of $G$ and $H$.

More generally, if $G_1, \ldots, G_r$ are groups, then the direct product $G_1 \times \ldots \times G_r$ is

$$\{(g_1, \ldots, g_r): g_i \in G_i \text{ for } 1 \leqslant i \leqslant r\},$$

with product operation defined by

$$(g_1, \ldots, g_r)(g_1', \ldots, g_r') = (g_1 g_1', \ldots, g_r g_r').$$

If all the groups $G_i$ are finite, then $G_1 \times \ldots \times G_r$ is also finite, of order $|G_1| \ldots |G_r|$.

*1.3 Example*
The group $C_2 \times \ldots \times C_2$ ($r$ factors) has order $2^r$ and all its non-identity elements have order 2.

### Functions

A *function* from one set $G$ to another set $H$ is a rule which assigns a unique element of $H$ to each element of $G$. In this book, we generally apply functions on the *right* – that is, the image of $g$ under a function $\vartheta$ is written as $g\vartheta$, not as $\vartheta g$. We often indicate that $\vartheta$ is a function from $G$ to $H$ by the notation $\vartheta: G \to H$. By an expression $\vartheta: g \to h$, where $g \in G$ and $h \in H$, we mean that $h = g\vartheta$.

A function $\vartheta: G \to H$ is *invertible* if there is a function $\phi: H \to G$ such that for all $g \in G$, $h \in H$,

$$(g\vartheta)\phi = g \text{ and } (h\phi)\vartheta = h.$$

Then $\phi$ is called the *inverse* of $\vartheta$, and is written as $\vartheta^{-1}$. A function $\vartheta$ from $G$ to $H$ is invertible if and only if it is both *injective* (that is, $g_1\vartheta = g_2\vartheta$ for $g_1, g_2 \in G$ implies that $g_1 = g_2$) and *surjective* (that is, for every $h \in H$ there exists $g \in G$ such that $g\vartheta = h$). An invertible function is also called a *bijection*.

### Homomorphisms

Given groups $G$ and $H$, those functions from $G$ to $H$ which 'preserve the group structure' – the so-called homomorphisms – are of particular importance.

If $G$ and $H$ are groups, then a *homomorphism* from $G$ to $H$ is a function $\vartheta: G \to H$ which satisfies

$$(g_1 g_2)\vartheta = (g_1\vartheta)(g_2\vartheta) \quad \text{for all } g_1, g_2 \in G.$$

An invertible homomorphism is called an *isomorphism*. If there is an isomorphism $\vartheta$ from $G$ to $H$, then $G$ and $H$ are said to be *isomorphic*, and we write $G \cong H$; also, $\vartheta^{-1}$ is an isomorphism from $H$ to $G$, so $H \cong G$.

The following example displays a technique which can often be used to prove that certain functions are homomorphisms.

*1.4 Example*
Let $G = D_{2n} = \langle a, b: a^n = b^2 = 1, \ b^{-1}ab = a^{-1} \rangle$, and write the $2n$ elements of $G$ in the form $a^i b^j$ with $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant 1$. Let $H$ be any group, and suppose that $H$ contains elements $x$ and $y$ which satisfy

$$x^n = y^2 = 1, \ y^{-1}xy = x^{-1}.$$

We shall prove that the function $\vartheta: G \to H$ defined by

$$\vartheta: a^i b^j \to x^i y^j \quad (0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant 1)$$

is a homomorphism.

Suppose that $0 \leqslant r \leqslant n-1$, $0 \leqslant s \leqslant 1$, $0 \leqslant t \leqslant n-1$, $0 \leqslant u \leqslant 1$. Then

$$a^r b^s a^t b^u = a^i b^j$$

for some $i$, $j$ with $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant 1$. Moreover, $i$ and $j$ are determined by repeatedly using the relations

$$a^n = b^2 = 1, \ b^{-1}ab = a^{-1}.$$

Since we have $x^n = y^2 = 1$, $y^{-1}xy = x^{-1}$, we can also deduce that

$$x^r y^s x^t y^u = x^i y^j.$$

Therefore,

$$(a^r b^s a^t b^u)\vartheta = (a^i b^j)\vartheta = x^i y^j = x^r y^s x^t y^u$$
$$= (a^r b^s)\vartheta \cdot (a^t b^u)\vartheta,$$

and so $\vartheta$ is a homomorphism.

We now demonstrate the technique of Example 1.4 in action.

*1.5 Example*
Let $G = S_5$ and let $x$, $y$ be the following permutations in $G$:

$$x = (1\ 2\ 3\ 4\ 5), \ y = (2\ 5)(3\ 4).$$

(Here we adopt the usual cycle notation – thus, (1 2 3 4 5) denotes the permutation $1 \to 2 \to 3 \to 4 \to 5 \to 1$, and so on.) Check that

$$x^5 = y^2 = 1,\ y^{-1}xy = x^{-1}.$$

Let $H$ be the subgroup $\langle x, y\rangle$ of $G$. Using the above relations, we see that

$$H = \{x^i y^j \colon 0 \leqslant i \leqslant 4,\ 0 \leqslant j \leqslant 1\},$$

a group of order 10.

Now recall that

$$D_{10} = \langle a, b \colon a^5 = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle.$$

By Example 1.4, the function $\vartheta \colon D_{10} \to H$ defined by

$$\vartheta \colon a^i b^j \to x^i y^j \quad (0 \leqslant i \leqslant 4,\ 0 \leqslant j \leqslant 1)$$

is a homomorphism. Since $\vartheta$ is invertible, it is an isomorphism. Thus, $H = \langle x, y\rangle \cong D_{10}$.

## Cosets

Let $G$ be a group and let $H$ be a subgroup of $G$. For $x$ in $G$, the subset

$$Hx = \{hx \colon h \in H\}$$

of $G$ is called a *right coset* of $H$ in $G$. The distinct right cosets of $H$ in $G$ form a partition of $G$ (that is, every element of $G$ is in precisely one of the cosets).

Suppose now that $G$ is finite, and let $Hx_1, \ldots, Hx_r$ be all the distinct right cosets of $H$ in $G$. For all $i$, the function

$$h \to hx_i \quad (h \in H)$$

is a bijection from $H$ to $Hx_i$, and so $|Hx_i| = |H|$. Since

$$G = Hx_1 \cup \ldots \cup Hx_r, \text{ and}$$

$$Hx_i \cap Hx_j \text{ is empty if } i \neq j,$$

we deduce that

$$|G| = r|H|.$$

In particular, we have

*1.6 Lagrange's Theorem*
*If $G$ is a finite group and $H$ is a subgroup of $G$, then $|H|$ divides $|G|$.*

The number $r$ of distinct right cosets of $H$ in $G$ is called the *index* of $H$ in $G$, and is written as $|G: H|$. Thus

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

when $G$ is finite.

## Normal subgroups

A subgroup $N$ of a group $G$ is said to be a *normal* subgroup of $G$ if $g^{-1}Ng = N$ for all $g \in G$ (where $g^{-1}Ng = \{g^{-1}ng: n \in N\}$); we write $N \lhd G$ to indicate that $N$ is a normal subgroup of $G$.

Suppose that $N \lhd G$ and let $G/N$ be the set of right cosets of $N$ in $G$. The importance of the condition $g^{-1}Ng = N$ (for all $g \in G$) is that it can be used to show that for all $g, h \in G$, we have

$$\{xy: x \in Ng \text{ and } y \in Nh\} = Ngh.$$

Hence we can define a product operation on $G/N$ by

$$(Ng)(Nh) = Ngh \quad \text{for all } g, h \in G.$$

This makes $G/N$ into a group, called the *factor group* of $G$ by $N$.

*1.7 Examples*
(1) For every group $G$, the sub-groups $\{1\}$ and $G$ are normal sub-groups of $G$.

(2) For $n \geqslant 1$, we have $A_n \lhd S_n$. If $n \geqslant 2$ then there are just two right cosets of $A_n$ in $S_n$, namely

$$A_n = \{g \in S_n: g \text{ even}\}, \text{ and}$$
$$A_n(1\ 2) = \{g \in S_n: g \text{ odd}\}.$$

Thus $|S_n: A_n| = 2$, and so $S_n/A_n \cong C_2$.

(3) Let $G = D_8 = \langle a, b: a^4 = b^2 = 1, \quad b^{-1}ab = a^{-1}\rangle$ and let $N = \langle a^2\rangle = \{1, a^2\}$. Then $N \lhd G$ and

$$G/N = \{N, Na, Nb, Nab\}.$$

Since $(Na)^2 = (Nb)^2 = (Nab)^2 = N$, we see that $G/N \cong C_2 \times C_2$.

The subgroup $\langle a\rangle$ is also normal in $G$, but the subgroup $H = \langle b\rangle$ is not normal in $G$, since $b \in H$ while $a^{-1}ba = a^2b \notin H$.

## Simple groups

A group $G$ is said to be *simple* if $G \neq \{1\}$ and the only normal subgroups of $G$ are $\{1\}$ and $G$. For example, the cyclic group $C_p$, with $p$ a prime number, is simple. We shall give examples of non-abelian simple groups in later chapters – the smallest one is $A_5$.

If $G$ is a finite group which is not simple, then $G$ has a normal subgroup $N$ such that both $N$ and $G/N$ have smaller order than $G$; and in a sense, $G$ is 'built' out of these two smaller groups. Continuing this process with the smaller groups, we eventually see that $G$ is 'built' out of a collection of simple groups. (This is analogous to the fact that every positive integer is built out of its prime factors.) Thus, simple groups are fundamental to the study of finite groups.

## Kernels and images

To conclude the chapter, we relate normal subgroups and factor groups to homomorphisms. Let $G$ and $H$ be groups and suppose that $\vartheta: G \to H$ is a homomorphism. We define the *kernel* of $\vartheta$ by

$$\operatorname{Ker}\vartheta = \{g \in G: g\vartheta = 1\}. \tag{1.8}$$

Then $\operatorname{Ker}\vartheta$ is a normal subgroup of $G$. Also, the *image* of $\vartheta$ is

$$\operatorname{Im}\vartheta = \{g\vartheta: g \in G\}, \tag{1.9}$$

and $\operatorname{Im}\vartheta$ is a subgroup of $H$.

The following result describes the way in which the kernel and image of $\vartheta$ are related.

*1.10 Theorem*
*Suppose that $G$ and $H$ are groups and let $\vartheta: G \to H$ be a homomorphism. Then*

$$G/\operatorname{Ker}\vartheta \cong \operatorname{Im}\vartheta.$$

*An isomorphism is given by the function*

$$Kg \to g\vartheta \quad (g \in G)$$

*where* $K = \operatorname{Ker}\vartheta$.

*1.11 Example*
The function $\vartheta\colon S_n \to C_2$ given by

$$\vartheta\colon g \to \begin{cases} 1, & \text{if } g \text{ is an even permutation,} \\ -1, & \text{if } g \text{ is an odd permutation,} \end{cases}$$

is a homomorphism. We have $\operatorname{Ker}\vartheta = A_n$, and for $n \geqslant 2$, $\operatorname{Im}\vartheta = C_2$. We know from Example 1.7(2) that $S_n/A_n \cong C_2$, illustrating Theorem 1.10.

## Summary of Chapter 1

1. Examples of groups are

   $C_n = \langle a\colon a^n = 1\rangle$,
   $D_{2n} = \langle a, b\colon a^n = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle$,
   $Q_8 = \langle a, b\colon a^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\rangle$,
   $S_n$ = the symmetric group of degree $n$,
   $A_n$ = the alternating group of degree $n$,
   $\mathrm{GL}(n, \mathbb{C})$ = the group of invertible $n \times n$ matrices over $\mathbb{C}$,
   $G_1 \times \ldots \times G_r$, the direct product of the groups $G_1, \ldots, G_r$.

2. A normal subgroup $N$ of $G$ is a subgroup such that $g^{-1}Ng = N$ for all $g$ in $G$. The factor group $G/N$ consists of the right cosets $Ng$ ($g \in G$), with multiplication

   $$(Ng)(Nh) = Ngh.$$

3. A homomorphism $\vartheta\colon G \to H$ is a function such that

   $$(g_1 g_2)\vartheta = (g_1\vartheta)(g_2\vartheta)$$

   for all $g_1$, $g_2$ in $G$. The kernel, $\operatorname{Ker}\vartheta$, is a normal subgroup of $G$, and the image, $\operatorname{Im}\vartheta$, is a subgroup of $H$. The factor group $G/\operatorname{Ker}\vartheta$ is isomorphic to $\operatorname{Im}\vartheta$.

## Exercises for Chapter 1

1. Show that if $G$ is an abelian group which is simple, then $G$ is cyclic of prime order.
2. Suppose that $G$ and $H$ are groups, with $G$ simple, and that $\vartheta\colon G \to H$ is a surjective homomorphism. Show that either $\vartheta$ is an isomorphism or $H = \{1\}$.

3. Suppose that $G$ is a subgroup of $S_n$, and that $G$ is not contained in $A_n$. Prove that $G \cap A_n$ is a normal subgroup of $G$, and $G/(G \cap A_n) \cong C_2$.
4. Let

$$G = D_8 = \langle a, b: a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle, \text{ and}$$
$$H = Q_8 = \langle c, d: c^4 = 1, c^2 = d^2, d^{-1}cd = c^{-1} \rangle.$$

(a) Let $x$, $y$ be the permutations in $S_4$ which are given by

$$x = (1\ 2),\ y = (3\ 4),$$

and let $K$ be the subgroup $\langle x, y \rangle$ of $S_4$. Show that both the functions $\phi: G \to K$ and $\psi: H \to K$, defined by

$$\phi: a^r b^s \to x^r y^s,$$
$$\psi: c^r d^s \to x^r y^s \quad (0 \leqslant r \leqslant 3, 0 \leqslant s \leqslant 1),$$

are homomorphisms. Find $\operatorname{Ker}\phi$ and $\operatorname{Ker}\psi$.

(b) Let $X$, $Y$ be the $2 \times 2$ matrices which are given by

$$X = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and let $L$ be the subgroup $\langle X, Y \rangle$ of $\mathrm{GL}(2, \mathbb{C})$. Show that just one of the functions $\lambda: G \to L$ and $\mu: H \to L$, defined by

$$\lambda: a^r b^s \to X^r Y^s,$$
$$\mu: c^r d^s \to X^r Y^s \quad (0 \leqslant r \leqslant 3, 0 \leqslant s \leqslant 1),$$

is a homomorphism. Prove that this homomorphism is an isomorphism.

5. Prove that $D_{4m} \cong D_{2m} \times C_2$ if $m$ is odd.
6. (a) Show that every subgroup of a cyclic group is cyclic.

(b) Let $G$ be a finite cyclic group, and let $n$ be a positive integer which divides $|G|$. Prove that

$$\{g \in G: g^n = 1\}$$

is a cylic subgroup of $G$ of order $n$.

(c) If $G$ is a finite cyclic group and $x$, $y$ are elements of $G$ with the same order, show that $x$ is a power of $y$.

7. Show that the set of non-zero complex numbers, under the usual multiplication, is a group. Prove that every finite subgroup of this group is cyclic.
8. Show that every group of even order contains an element of order 2.
9. Find elements $A$ and $B$ of $\mathrm{GL}(2, \mathbb{C})$ such that $A$ has order 8, $B$ has order 4, and

$$B^2 = A^4 \text{ and } B^{-1}AB = A^{-1}.$$

Show that the group $\langle A, B \rangle$ has order 16.
(Hint: compare $Q_8$ in Example 1.2(4).)

10. Suppose that $H$ is a subgroup of $G$ with $|G:H| = 2$. Prove that $H \lhd G$.

# 2
# Vector spaces and linear transformations

An attractive feature of representation theory is that it combines two strands of mainstream mathematics, namely group theory and linear algebra. For reference purposes, we gather the results from linear algebra concerning vector spaces, linear transformations and matrices which we shall use later. Most of the material will be familiar to you if you have taken a first course on linear algebra, so we omit the proofs. An exception occurs in the last section, where we deal with projections; here, we explain in detail how the results work, in case you have not come across projections before.

## Vector spaces

Let $F$ be either $\mathbb{R}$ (the set of real numbers) or $\mathbb{C}$ (the set of complex numbers). A *vector space* over $F$ is a set $V$, together with a rule for adding any two elements $u$, $v$ of $V$ to form an element $u + v$ of $V$, and a rule for multiplying any element $v$ of $V$ by any element $\lambda$ of $F$ to form an element $\lambda v$ of $V$. (The latter rule is called *scalar multiplication*.) Moreover, these rules must satisfy:

(2.1) (a) $V$ is an abelian group under addition;
(b) for all $u$, $v$ in $V$ and all $\lambda$, $\mu$ in $F$,
(1) $\lambda(u + v) = \lambda u + \lambda v$,
(2) $(\lambda + \mu)v = \lambda v + \mu v$,
(3) $(\lambda\mu)v = \lambda(\mu v)$,
(4) $1v = v$.

The elements of $V$ are called *vectors*, and those of $F$ are called *scalars*. We write 0 for the identity element of the abelian group $V$ under addition.

*2.2 Examples*

(1) Let $\mathbb{R}^2$ denote the set of all ordered pairs $(x, y)$ where $x$ and $y$ are real numbers. Define addition and scalar multiplication on $\mathbb{R}^2$ by

$$(x, y) + (x', y') = (x + x', y + y'),$$
$$\lambda(x, y) = (\lambda x, \lambda y).$$

Then $\mathbb{R}^2$ is a vector space over $\mathbb{R}$.

(2) More generally, for each positive integer $n$, we consider *row vectors*

$$(x_1, x_2, \ldots, x_n)$$

where $x_1, x_2, \ldots, x_n$ belong to $F$. We denote the set of all such row vectors by $F^n$, and define addition and scalar multiplication on $F^n$ by

$$(x_1, \ldots, x_n) + (x_1', \ldots, x_n') = (x_1 + x_1', \ldots, x_n + x_n'),$$
$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

Then $F^n$ is a vector space over $F$.

## Bases of vector spaces

Let $v_1, \ldots, v_n$ be vectors in a vector space $V$ over $F$. A vector $v$ in $V$ is a *linear combination* of $v_1, \ldots, v_n$ if

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

for some $\lambda_1, \ldots, \lambda_n$ in $F$. The vectors $v_1, \ldots, v_n$ are said to *span* $V$ if every vector in $V$ is a linear combination of $v_1, \ldots, v_n$.

We say that $v_1, \ldots, v_n$ are *linearly dependent* if

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$$

for some $\lambda_1, \ldots, \lambda_n$ in $F$, not all of which are zero; otherwise, $v_1, \ldots, v_n$ are *linearly independent*.

The vectors $v_1, \ldots, v_n$ form a *basis* of $V$ if they span $V$ and are linearly independent.

*Throughout this book, we shall consider only vector spaces $V$ which are finite-dimensional* – this means that $V$ has a basis consisting of finitely many vectors, as above. It turns out that any two bases of $V$ have the same number of vectors. The number of vectors in a basis of $V$ is called the *dimension* of $V$ and is written as $\dim V$. If $V = \{0\}$ then $\dim V = 0$. The vector space $V$ is *n-dimensional* if $\dim V = n$.

*2.3 Example*
Let $V = F^n$. Then

$$(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)$$

is a basis of $V$, so $\dim V = n$. Another basis is

$$(1, 0, 0, \ldots, 0), (1, 1, 0, \ldots, 0), \ldots, (1, 1, 1, \ldots, 1).$$

Given a basis $v_1, \ldots, v_n$ of a vector space $V$, each vector $v$ in $V$ can be written in a *unique* way as

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n,$$

with $\lambda_1, \ldots, \lambda_n$ in $F$. The vector $v$ therefore determines the scalars $\lambda_1, \ldots, \lambda_n$. Except in the case where $V = \{0\}$, there are many bases of $V$. Indeed, the next result says that any linearly independent vectors can be extended to a basis.

(2.4) *If $v_1, \ldots, v_k$ are linearly independent vectors in $V$, then there exist $v_{k+1}, \ldots, v_n$ in $V$ such that $v_1, \ldots, v_n$ form a basis of $V$.*

## Subspaces

A *subspace* of a vector space $V$ over $F$ is a subset of $V$ which is itself a vector space under the addition and scalar multiplication inherited from $V$. For a subset $U$ of $V$ to be a subspace, it is necessary and sufficient that all the following conditions hold:

(2.5) (1) $0 \in U$;
(2) if $u, v \in U$ then $u + v \in U$;
(3) if $\lambda \in F$ and $u \in U$ then $\lambda u \in U$.

*2.6 Examples*
(1) $\{0\}$ and $V$ are subspaces of $V$.

(2) Let $u_1, \ldots, u_r$ be vectors in $V$. We define $\mathrm{sp}(u_1, \ldots, u_r)$ to be the set of all linear combinations of $u_1, \ldots, u_r$; that is,

$$\mathrm{sp}(u_1, \ldots, u_r) = \{\lambda_1 u_1 + \ldots + \lambda_r u_r : \lambda_1, \ldots, \lambda_r \in F\}.$$

By (2.5), $\mathrm{sp}(u_1, \ldots, u_r)$ is a subspace of $V$, and it is called the subspace *spanned* by $u_1, \ldots, u_r$.

Notice that the following fact is a consequence of (2.4).

(2.7) *Suppose that $U$ is a subspace of the vector space $V$. Then* $\dim U \leqslant \dim V$. *Also,* $\dim U = \dim V$ *if and only if* $U = V$.

### Direct sums of subspaces

If $U_1, \ldots, U_r$ are subspaces of a vector space $V$, then the sum $U_1 + \ldots + U_r$ is defined by

$$U_1 + \ldots + U_r = \{u_1 + \ldots + u_r : u_i \in U_i \text{ for } 1 \leqslant i \leqslant r\}.$$

By (2.5), $U_1 + \ldots + U_r$ is a subspace of $V$.

We say that the sum $U_1 + \ldots + U_r$ is a *direct sum* if every element of the sum can be written in a *unique* way as $u_1 + \ldots + u_r$ with $u_i \in U_i$ for $1 \leqslant i \leqslant r$. If the sum is direct, then we write it as

$$U_1 \oplus \ldots \oplus U_r.$$

*2.8 Examples*

(1) Suppose that $v_1, \ldots, v_n$ is a basis of $V$, and for $1 \leqslant i \leqslant n$, let $U_i$ be the subspace spanned by $v_i$. Then

$$V = U_1 \oplus \ldots \oplus U_n.$$

(2) Let $U$ be a subspace of $V$ and let $v_1, \ldots, v_k$ be a basis of $U$. Extend $v_1, \ldots, v_k$ to a basis $v_1, \ldots, v_n$ of $V$ (see (2.4)), and let $W = \mathrm{sp}(v_{k+1}, \ldots, v_n)$. Then

$$V = U \oplus W.$$

From this construction it follows that there are infinitely many subspaces $W$ with $V = U \oplus W$, unless $U$ is $\{0\}$ or $V$.

The next result is frequently useful when dealing with the direct sum of two subspaces. You should consult the solutions to Exercises 2.3 and 2.4 if you have difficulty with the proof.

(2.9) *Suppose that $V = U + W$, that $u_1, \ldots, u_r$ is a basis of $U$ and that $w_1, \ldots, w_s$ is a basis of $W$. Then the following three conditions are equivalent:*

(1) $V = U \oplus W$,
(2) $u_1, \ldots, u_r, w_1, \ldots, w_s$ *is a basis of* $V$,
(3) $U \cap W = \{0\}$.

Our next result, involving the direct sum of several subspaces, can be deduced immediately from the definition of a direct sum.

(2.10) *Suppose that* $U$, $W$, $U_1, \ldots, U_a$, $W_1, \ldots, W_b$ *are subspaces of a vector space* $V$. *If* $V = U \oplus W$ *and also*

$$U = U_1 \oplus \ldots \oplus U_a, \text{ and}$$

$$W = W_1 \oplus \ldots \oplus W_b,$$

*then*

$$V = U_1 \oplus \ldots \oplus U_a \oplus W_1 \oplus \ldots \oplus W_b.$$

We now introduce a construction for vector spaces which is analogous to the construction of direct products for groups.

Let $U_1, \ldots, U_r$ be vector spaces over $F$, and let

$$V = \{(u_1, \ldots, u_r) : u_i \in U_i \text{ for } 1 \leqslant i \leqslant r\}.$$

Define addition and scalar multiplication on $V$ as follows: for all $u_i$, $u_i'$ in $U_i$ $(1 \leqslant i \leqslant r)$ and all $\lambda$ in $F$, let

$$(u_1, \ldots, u_r) + (u_1', \ldots, u_r') = (u_1 + u_1', \ldots, u_r + u_r'),$$

$$\lambda(u_1, \ldots, u_r) = (\lambda u_1, \ldots, \lambda u_r).$$

With these definitions, $V$ is a vector space over $F$. If, for $1 \leqslant i \leqslant r$, we put

$$U_i' = \{(0, \ldots, u_i, \ldots, 0) : u_i \in U_i\}$$

(where the $u_i$ is in the $i$th position), then it is immediate that

$$V = U_1' \oplus \ldots \oplus U_r'.$$

We call $V$ the *external direct sum* of $U_1, \ldots, U_r$, and, abusing notation slightly, we write

$$V = U_1 \oplus \ldots \oplus U_r.$$

## Linear transformations

Let $V$ and $W$ be vector spaces over $F$. A *linear transformation* from $V$ to $W$ is a function $\vartheta : V \to W$ which satisfies

$$(u + v)\vartheta = u\vartheta + v\vartheta \quad \text{for all } u, v \in V, \text{ and}$$

$$(\lambda v)\vartheta = \lambda(v\vartheta) \quad \text{for all } \lambda \in F \text{ and } v \in V.$$

Just as a group homomorphism preserves the group multiplication, so a linear transformation preserves addition and scalar multiplication.

Notice that if $\vartheta: V \to W$ is a linear transformation and $v_1, \ldots, v_n$ is a basis of $V$, then for $\lambda_1, \ldots, \lambda_n$ in $F$ we have

$$(\lambda_1 v_1 + \ldots + \lambda_n v_n)\vartheta = \lambda_1(v_1\vartheta) + \ldots + \lambda_n(v_n\vartheta).$$

Thus, $\vartheta$ is determined by its action on a basis. Furthermore, given any basis $v_1, \ldots, v_n$ of $V$ and any $n$ vectors $w_1, \ldots, w_n$ in $W$, there is a unique linear transformation $\phi: V \to W$ such that $v_i\phi = w_i$ for all $i$; the linear transformation $\phi$ is given by

$$(\lambda_1 v_1 + \ldots + \lambda_n v_n)\phi = \lambda_1 w_1 + \ldots + \lambda_n w_n.$$

We sometimes construct a linear transformation $\phi: V \to W$ in this way, by specifying the values of $\phi$ on a basis of $V$, and then saying 'extend the action of $\phi$ to be linear'.

## Kernels and images

Suppose that $\vartheta: V \to W$ is a linear transformation. The kernel of $\vartheta$ (written $\operatorname{Ker}\vartheta$) and the image of $\vartheta$ (written $\operatorname{Im}\vartheta$) are defined as follows:

$$\operatorname{Ker}\vartheta = \{v \in V: v\vartheta = 0\}, \tag{2.11}$$

$$\operatorname{Im}\vartheta = \{v\vartheta: v \in V\}.$$

Using (2.5), it is easy to check that $\operatorname{Ker}\vartheta$ is a subspace of $V$ and $\operatorname{Im}\vartheta$ is a subspace of $W$. Their dimensions are connected by the following equation, which is known as the Rank–Nullity Theorem:

$$\dim V = \dim(\operatorname{Ker}\vartheta) + \dim(\operatorname{Im}\vartheta). \tag{2.12}$$

*2.13 Examples*

(1) If $\vartheta: V \to W$ is defined by $v\vartheta = 0$ for all $v \in V$, then $\vartheta$ is a linear transformation, and

$$\operatorname{Ker}\vartheta = V, \quad \operatorname{Im}\vartheta = \{0\}.$$

(2) If $\vartheta: V \to V$ is defined by $v\vartheta = 3v$ for all $v \in V$, then $\vartheta$ is a linear transformation, and

$$\operatorname{Ker}\vartheta = \{0\}, \quad \operatorname{Im}\vartheta = V.$$

(3) If $\vartheta: \mathbb{R}^3 \to \mathbb{R}^2$ is given by

$$(x, y, z)\vartheta = (x + 2y + z, -y + 3z)$$

for all $x, y, z \in \mathbb{R}$, then $\vartheta$ is a linear transformation; we have

$$\operatorname{Ker}\vartheta = \operatorname{sp}((7, -3, -1)), \quad \operatorname{Im}\vartheta = \mathbb{R}^2,$$

so $\dim(\operatorname{Ker}\vartheta) = 1$ and $\dim(\operatorname{Im}\vartheta) = 2$.

### Invertible linear transformations

Again, let $V$ and $W$ be vector spaces over $F$. A linear transformation $\vartheta$ from $V$ to $W$ is injective if and only if $\operatorname{Ker}\vartheta = \{0\}$, and hence $\vartheta$ is invertible precisely when $\vartheta$ is surjective and $\operatorname{Ker}\vartheta = \{0\}$. It turns out that the inverse of an invertible linear transformation is also a linear transformation (see Exercise 2.1).

If there exists an invertible linear transformation from $V$ to $W$, then $V$ and $W$ are said to be *isomorphic* vector spaces. By applying (2.12), we see that isomorphic vector spaces have the same dimension. By also taking (2.7) into account, we obtain the next result (see Exercise 2.2).

(2.14) *Let $\vartheta$ be a linear transformation from $V$ to itself. Then the following three conditions are equivalent*:

(1) *$\vartheta$ is invertible*;
(2) $\operatorname{Ker}\vartheta = \{0\}$;
(3) $\operatorname{Im}\vartheta = V$.

### Endomorphisms

A linear transformation from a vector space $V$ to itself is called an *endomorphism* of $V$.

Suppose that $\vartheta$ and $\phi$ are endomorphisms of $V$ and $\lambda \in F$. We define the functions $\vartheta + \phi$, $\vartheta\phi$ and $\lambda\vartheta$ from $V$ to $V$ by

(2.15)
$$v(\vartheta + \phi) = v\vartheta + v\phi,$$
$$v(\vartheta\phi) = (v\vartheta)\phi,$$
$$v(\lambda\vartheta) = \lambda(v\vartheta),$$

for all $v \in V$. Then $\vartheta + \phi$, $\vartheta\phi$ and $\lambda\vartheta$ are endomorphisms of $V$. We write $\vartheta^2$ for $\vartheta\vartheta$.

*2.16 Examples*

(1) The identity function $1_V$ defined by

$$1_V: v \to v \quad \text{for all } v \in V$$

is an endomorphism of $V$. If $\vartheta$ is an endomorphism of $V$, then so is $\vartheta - \lambda 1_V$, for all $\lambda \in F$. Note that

$$\mathrm{Ker}(\vartheta - \lambda 1_V) = \{v \in V: v\vartheta = \lambda v\}.$$

(2) Let $V = \mathbb{R}^2$, and let $\vartheta$, $\phi$ be the functions from $V$ to $V$ defined by

$$(x, y)\vartheta = (x + y, x - 2y),$$

$$(x, y)\phi = (x - 2y, -2x + 4y).$$

Then $\vartheta$ and $\phi$ are endomorphisms of $V$, and $\vartheta + \phi$, $\vartheta\phi$, $3\vartheta$ and $\vartheta^2$ are given by

$$(x, y)(\vartheta + \phi) = (2x - y, -x + 2y),$$

$$(x, y)(\vartheta\phi) = (-x + 5y, 2x - 10y),$$

$$(x, y)(3\vartheta) = (3x + 3y, 3x - 6y),$$

$$(x, y)\vartheta^2 = (2x - y, -x + 5y).$$

## Matrices

Let $V$ be a vector space over $F$, and let $\vartheta$ be an endomorphism of $V$. Suppose that $v_1, \ldots, v_n$ is a basis of $V$ and call it $\mathscr{B}$. Then there are scalars $a_{ij}$ in $F$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ such that for all $i$,

$$v_i\vartheta = a_{i1}v_1 + \ldots + a_{in}v_n.$$

*2.17 Definition*

The $n \times n$ matrix $(a_{ij})$ is called the matrix of $\vartheta$ *relative to the basis* $\mathscr{B}$, and is denoted by $[\vartheta]_{\mathscr{B}}$.

*2.18 Examples*

(1) If $\vartheta = 1_V$ (so that $v\vartheta = v$ for all $v \in V$), then $[\vartheta]_{\mathscr{B}} = I_n$ for all bases $\mathscr{B}$ of $V$, where $I_n$ denotes the $n \times n$ *identity matrix*.

(2) Let $V = \mathbb{R}^2$ and let $\vartheta$ be the endomorphism $(x, y) \to (x + y, x - 2y)$ of $V$. If $\mathscr{B}$ is the basis $(1, 0)$, $(0, 1)$ of $V$ and $\mathscr{B}'$ is the basis

$(1, 0)$, $(1, 1)$ of $V$, then

$$[\vartheta]_{\mathscr{B}} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}, \quad [\vartheta]_{\mathscr{B}'} = \begin{pmatrix} 0 & 1 \\ 3 & -1 \end{pmatrix}.$$

If we wish to indicate that the entries in a matrix $A$ come from $F$, then we describe $A$ as a *matrix over* $F$.

Given two $m \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$ over $F$, their sum $A + B$ is the $m \times n$ matrix over $F$ whose $ij$-entry is $a_{ij} + b_{ij}$ for all $i$, $j$; and for $\lambda \in F$, the matrix $\lambda A$ is the $m \times n$ matrix over $F$ obtained from $A$ by multiplying all the entries by $\lambda$.

As you know, the product of two matrices is defined in a less transparent way. Given an $m \times n$ matrix $A = (a_{ij})$ and an $n \times p$ matrix $B = (b_{ij})$, their product $AB$ is the $m \times p$ matrix whose $ij$-entry is

$$\sum_{k=1}^{n} a_{ik} b_{kj}.$$

*2.19 Example*
Let

$$A = \begin{pmatrix} -1 & 2 \\ 3 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & -4 \\ 2 & -1 \end{pmatrix}.$$

Then

$$A + B = \begin{pmatrix} -1 & -2 \\ 5 & 0 \end{pmatrix}, 3A = \begin{pmatrix} -3 & 6 \\ 9 & 3 \end{pmatrix}, AB = \begin{pmatrix} 4 & 2 \\ 2 & -13 \end{pmatrix},$$

$$BA = \begin{pmatrix} -12 & -4 \\ -5 & 3 \end{pmatrix}.$$

The matrix of the sum or product of two endomorphisms (relative to some basis) is related to the matrices of the individual endomorphisms in the way you would expect:

(2.20) *Suppose that $\mathscr{B}$ is a basis of the vector space $V$, and that $\vartheta$ and $\phi$ are endomorphisms of $V$. Then*

$$[\vartheta + \phi]_{\mathscr{B}} = [\vartheta]_{\mathscr{B}} + [\phi]_{\mathscr{B}}, \text{ and}$$

$$[\vartheta\phi]_{\mathscr{B}} = [\vartheta]_{\mathscr{B}}[\phi]_{\mathscr{B}}.$$

*Also, for all scalars* $\lambda$,

$$[\lambda\vartheta]_{\mathscr{B}} = \lambda[\vartheta]_{\mathscr{B}}.$$

We showed you in (2.17) how to get a matrix from an endomorphism of a vector space $V$, given a basis of $V$. It is easy enough to reverse this process and use a matrix to define an endomorphism. We concentrate on a particular way of doing this. Suppose that $A$ is an $n \times n$ matrix over $F$, and let $V = F^n$, the vector space of row vectors $(x_1, \ldots, x_n)$ with each $x_i$ in $F$. Then for all $v$ in $V$, the matrix product $vA$ also lies in $V$. The following remark is easily justified.

(2.21) *If* $A$ *is an* $n \times n$ *matrix over* $F$, *then the function*

$$v \to vA \quad (v \in F^n)$$

*is an endomorphism of* $F^n$.

*2.22 Example*
Let

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

Then $A$ gives us an endomorphism $\vartheta$ of $F^2$, where

$$(x, y)\vartheta = (x, y)\begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} = (x + 3y, -x + 2y).$$

**Invertible matrices**

An $n \times n$ matrix $A$ is said to be *invertible* if there exists an $n \times n$ matrix $B$ with $AB = BA = I_n$. Such a matrix $B$, if it exists, is unique; it is called the *inverse* of $A$ and is written as $A^{-1}$. Write $\det A$ for the determinant of $A$. Then a necessary and sufficient condition for $A$ to be invertible is that $\det A \neq 0$.

The connection between invertible endomorphisms and invertible matrices is straightforward, and follows from (2.20): given a basis $\mathscr{B}$ of $V$, an endomorphism $\vartheta$ of $V$ is invertible if and only if the matrix $[\vartheta]_{\mathscr{B}}$ is invertible.

Invertible matrices turn up when we relate two bases of a vector space. An invertible matrix converts one basis into another, and this same matrix is used to describe the way in which the matrix of an

endomorphism depends upon the basis. The precise meaning of these remarks is revealed in the definition (2.23) and the result (2.24) below.

*2.23 Definition*
Let $v_1, \ldots, v_n$ be a basis $\mathscr{B}$ of the vector space $V$, and let $v_1', \ldots, v_n'$ be a basis $\mathscr{B}'$ of $V$. Then for $1 \leqslant i \leqslant n$,

$$v_i' = t_{i1}v_1 + \ldots + t_{in}v_n$$

for certain scalars $t_{ij}$. The $n \times n$ matrix $T = (t_{ij})$ is invertible, and is called the *change of basis matrix* from $\mathscr{B}$ to $\mathscr{B}'$.

The inverse of $T$ is the change of basis matrix from $\mathscr{B}'$ to $\mathscr{B}$.

(2.24) *If $\mathscr{B}$ and $\mathscr{B}'$ are bases of $V$ and $\vartheta$ is an endomorphism of $V$, then*

$$[\vartheta]_{\mathscr{B}} = T^{-1}[\vartheta]_{\mathscr{B}'}T,$$

*where $T$ is the change of basis matrix from $\mathscr{B}$ to $\mathscr{B}'$.*

*2.25 Example*
Suppose that $V = \mathbb{R}^2$. Let $\mathscr{B}$ be the basis $(1, 0)$, $(0, 1)$ and $\mathscr{B}'$ the basis $(1, 0)$, $(1, 1)$ of $V$. Then

$$T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

If $\vartheta$ is the endomorphism

$$\vartheta\colon (x, y) \to (x + y, x - 2y)$$

of $V$, as in Example 2.18(2), then

$$[\vartheta]_{\mathscr{B}} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = T^{-1}[\vartheta]_{\mathscr{B}'}T.$$

## Eigenvalues

Let $V$ be an $n$-dimensional vector space over $F$, and suppose that $\vartheta$ is an endomorphism of $V$. The scalar $\lambda$ is said to be an *eigenvalue* of $\vartheta$ if $v\vartheta = \lambda v$ for some non-zero vector $v$ in $V$. Such a vector $v$ is called an *eigenvector* of $\vartheta$.

Now $\lambda$ is an eigenvalue of $\vartheta$ if and only if $\mathrm{Ker}(\vartheta - \lambda 1_V) \neq \{0\}$, which occurs if and only if $\vartheta - \lambda 1_V$ is not invertible. Therefore, if $\mathscr{B}$ is a basis of $V$, then the eigenvalues of $\vartheta$ are those scalars $\lambda$ in $F$ which satisfy the equation

$$\det([\vartheta]_{\mathscr{B}} - \lambda I_n) = 0.$$

Solving this equation involves finding the roots of a polynomial of degree $n$. Since every non-constant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$, we deduce the following result.

(2.26) *Let $V$ be a non-zero vector space over $\mathbb{C}$, and let $\vartheta$ be an endomorphism of $V$. Then $\vartheta$ has an eigenvalue.*

*2.27 Examples*

(1) Let $V = \mathbb{C}^2$ and let $\vartheta$ be the endomorphism of $V$ which is given by

$$(x, y)\vartheta = (-y, x).$$

If $\mathscr{B}$ is the basis $(1, 0)$, $(0, 1)$ of $V$, then

$$[\vartheta]_{\mathscr{B}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We have $\det([\vartheta]_{\mathscr{B}} - \lambda I_2) = \lambda^2 + 1$, so i and $-$i are the eigenvalues of $\vartheta$. Corresponding eigenvectors are $(1, -\mathrm{i})$ and $(1, \mathrm{i})$. Note that if $\mathscr{B}'$ is the basis $(1, -\mathrm{i})$, $(1, \mathrm{i})$ of $V$, then

$$[\vartheta]_{\mathscr{B}'} = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}.$$

(2) Let $V = \mathbb{R}^2$ and let $\vartheta$ again be the endomorphism which is given by

$$(x, y)\vartheta = (-y, x).$$

This time, $V$ is a vector space over $\mathbb{R}$, and $\vartheta$ has no eigenvalues in $\mathbb{R}$. Thus we depend upon $F$ being $\mathbb{C}$ in result (2.26).

For an $n \times n$ matrix $A$ over $F$, the element $\lambda$ of $F$ is said to be an eigenvalue of $A$ if $vA = \lambda v$ for some non-zero row vector $v$ in $F^n$. The eigenvalues of $A$ are those elements $\lambda$ of $F$ which satisfy

$$\det(A - \lambda I_n) = 0.$$

*2.28 Example*
We say that an $n \times n$ matrix $A = (a_{ij})$ is *diagonal* if $a_{ij} = 0$ for all $i$ and $j$ with $i \neq j$. We often display such a matrix in the form

$$A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

which indicates, in addition, that $a_{ii} = \lambda_i$ for $1 \leqslant i \leqslant n$. For this diagonal matrix $A$, the eigenvalues are $\lambda_1, \ldots, \lambda_n$.

## Projections

If a vector space $V$ is a direct sum of two subspaces $U$ and $W$, then we can construct a special endomorphism of $V$ which depends upon the expression $V = U \oplus W$:

*2.29 Proposition*
*Suppose that $V = U \oplus W$. Define $\pi: V \to V$ by*

$$(u + w)\pi = u \quad \text{for all } u \in U, w \in W.$$

*Then $\pi$ is an endomorphism of $V$. Further,*

$$\operatorname{Im}\pi = U, \operatorname{Ker}\pi = W \text{ and } \pi^2 = \pi.$$

*Proof* Since every vector in $V$ has a *unique* expression in the form $u + w$ with $u \in U$, $w \in W$, it follows that $\pi$ is a function on $V$.

Let $v$ and $v'$ belong to $V$. Then $v = u + w$ and $v' = u' + w'$ for some $u$, $u'$ in $U$ and $w$, $w'$ in $W$. We have

$$\begin{aligned}(v + v')\pi &= (u + u' + w + w')\pi = u + u' \\ &= (u + w)\pi + (u' + w')\pi \\ &= v\pi + v'\pi.\end{aligned}$$

Also, for $\lambda$ in $F$,

$$(\lambda v)\pi = (\lambda u + \lambda w)\pi = \lambda u = \lambda(v\pi).$$

Therefore, $\pi$ is an endomorphism of $V$.

Clearly $\operatorname{Im}\pi \subseteq U$; and since $u\pi = u$ for all $u$ in $U$, we have $\operatorname{Im} = U$. Also,

$$(u + w)\pi = 0 \Leftrightarrow u = 0 \Leftrightarrow u + w \in W,$$

and so $\operatorname{Ker}\pi = W$.

Finally,

$$(u + w)\pi^2 = u\pi = u = (u + w)\pi,$$

and so $\pi^2 = \pi$. ∎

*2.30 Definition*
An endomorphism $\pi$ of a vector space $V$ which satisfies $\pi^2 = \pi$ is called a *projection* of $V$.

*2.31 Example*
The endomorphism

$$(x, y) \to (2x + 2y, -x - y)$$

of $\mathbb{R}^2$ is a projection.

We now show that every projection can be constructed using a direct sum, as in Proposition 2.29.

*2.32 Proposition*
*Suppose that $\pi$ is a projection of a vector space $V$. Then*

$$V = \operatorname{Im}\pi \oplus \operatorname{Ker}\pi.$$

*Proof* If $v \in V$ then $v = v\pi + (v - v\pi)$. Clearly the first term $v\pi$ belongs to $\operatorname{Im}\pi$; and the second term $v - v\pi$ lies in $\operatorname{Ker}\pi$, since

$$(v - v\pi)\pi = v\pi - v\pi^2 = v\pi - v\pi = 0.$$

This establishes that $V = \operatorname{Im}\pi + \operatorname{Ker}\pi$.

Now suppose that $v$ lies in $\operatorname{Im}\pi \cap \operatorname{Ker}\pi$. As $v \in \operatorname{Im}\pi$, we have $v = u\pi$ for some $u \in V$. Therefore

$$v\pi = u\pi^2 = u\pi = v.$$

Since $v \in \operatorname{Ker}\pi$, it follows that $v = v\pi = 0$. Thus

$$\operatorname{Im}\pi \cap \operatorname{Ker}\pi = \{0\},$$

and (2.9) now shows that $V = \operatorname{Im}\pi \oplus \operatorname{Ker}\pi$. ∎

*2.33 Example*
If $\pi: (x, y) \to (2x + 2y, -x - y)$ is the projection of $\mathbb{R}^2$ which appears in Example 2.31, then

$$\operatorname{Im}\pi = \{(2x, -x): x \in \mathbb{R}\}, \operatorname{Ker}\pi = \{(x, -x): x \in \mathbb{R}\}.$$

## Summary of Chapter 2

1. All our vector spaces are finite-dimensional over $F$, where $F = \mathbb{C}$ or $\mathbb{R}$. For example, $F^n$ is the set of row vectors $(x_1, \ldots, x_n)$ with each $x_i$ in $F$, and $\dim F^n = n$.
2. $V = U_1 \oplus \ldots \oplus U_r$ if each $U_i$ is a subspace of $V$, and every element $v$ of $V$ has a unique expression of the form $v = u_1 + \ldots + u_r$ $(u_i \in U_i)$.
   Also, $V = U \oplus W$ if and only if $V = U + W$ and $U \cap W = \{0\}$.
3. A linear transformation $\vartheta: V \to W$ satisfies
   $$(u + v)\vartheta = u\vartheta + v\vartheta \text{ and } (\lambda v)\vartheta = \lambda(v\vartheta)$$
   for all $u$, $v$ in $V$ and all $\lambda$ in $F$. $\operatorname{Ker}\vartheta$ is a subspace of $V$ and $\operatorname{Im}\vartheta$ is a subspace of $W$, and
   $$\dim V = \dim(\operatorname{Ker}\vartheta) + \dim(\operatorname{Im}\vartheta).$$
4. A linear transformation $\vartheta: V \to W$ is invertible if and only if $\operatorname{Ker}\vartheta = \{0\}$ and $\operatorname{Im}\vartheta = W$.
5. Given a basis $\mathscr{B}$ of the $n$-dimensional vector space $V$, there is a correspondence between the endomorphisms $\vartheta$ of $V$ and the $n \times n$ matrices $[\vartheta]_{\mathscr{B}}$ over $F$.
   Given two bases $\mathscr{B}$ and $\mathscr{B}'$ of $V$, and an endomorphism $\vartheta$ of $V$, there exists an invertible matrix $T$ such that
   $$[\vartheta]_{\mathscr{B}} = T^{-1}[\vartheta]_{\mathscr{B}'}T.$$
6. Eigenvalues $\lambda$ of an endomorphism $\vartheta$ satisfy $v\vartheta = \lambda v$ for some non-zero $v$ in $V$.
7. A projection is an endomorphism $\pi$ of $V$ which satisfies $\pi^2 = \pi$.

## Exercises for Chapter 2

1. Show that if $V$ and $W$ are vector spaces and $\vartheta: V \to W$ is an invertible linear transformation then $\vartheta^{-1}$ is a linear transformation.

2. Suppose that $\vartheta$ is an endomorphism of the vector space $V$. Show that the following are equivalent:

   (1) $\vartheta$ is invertible;
   (2) $\operatorname{Ker}\vartheta = \{0\}$;
   (3) $\operatorname{Im}\vartheta = V$.

3. Let $U$ and $W$ be subspaces of the vector space $V$. Prove that $V = U \oplus W$ if and only if $V = U + W$ and $U \cap W = \{0\}$.

4. Let $U$ and $W$ be subspaces of the vector space $V$. Suppose that $u_1, \ldots, u_r$ is a basis of $U$ and $w_1, \ldots, w_s$ is a basis of $W$. Show that $V = U \oplus W$ if and only if $u_1, \ldots, u_r, w_1, \ldots, w_s$ is a basis of $V$.

5. (a) Let $U_1$, $U_2$ and $U_3$ be subspaces of a vector space $V$, with $V = U_1 + U_2 + U_3$. Show that

   $$V = U_1 \oplus U_2 \oplus U_3 \Leftrightarrow$$

   $$U_1 \cap (U_2 + U_3) = U_2 \cap (U_1 + U_3) = U_3 \cap (U_1 + U_2) = \{0\}.$$

   (b) Give an example of a vector space $V$ with three subspaces $U_1$, $U_2$ and $U_3$ such that $V = U_1 + U_2 + U_3$ and

   $$U_1 \cap U_2 = U_1 \cap U_3 = U_2 \cap U_3 = \{0\},$$

   but $V \neq U_1 \oplus U_2 \oplus U_3$.

6. Suppose that $U_1, \ldots, U_r$ are subspaces of the vector space $V$, and that $V = U_1 \oplus \ldots \oplus U_r$. Prove that

   $$\dim V = \dim U_1 + \ldots + \dim U_r.$$

7. Give an example of a vector space $V$ with endomorphisms $\vartheta$ and $\phi$ such that $V = \operatorname{Im}\vartheta \oplus \operatorname{Ker}\vartheta$, but $V \neq \operatorname{Im}\phi \oplus \operatorname{Ker}\phi$.

8. Let $V$ be a vector space and let $\vartheta$ be an endomorphism of $V$. Show that $\vartheta$ is a projection if and only if there is a basis $\mathscr{B}$ of $V$ such that $[\vartheta]_{\mathscr{B}}$ is diagonal, with all diagonal entries equal to 1 or 0.

9. Suppose that $\vartheta$ is an endomorphism of the vector space $V$ and $\vartheta^2 = 1_V$. Show that $V = U \oplus W$, where

   $$U = \{v \in V : v\vartheta = v\}, \; W = \{v \in V : v\vartheta = -v\}.$$

   Deduce that $V$ has a basis $\mathscr{B}$ such that $[\vartheta]_{\mathscr{B}}$ is diagonal, with all diagonal entries equal to $+1$ or $-1$.

# 3
# Group representations

A representation of a group $G$ gives us a way of visualizing $G$ as a group of matrices. To be precise, a representation is a homomorphism from $G$ into a group of invertible matrices. We set out this idea in more detail, and give some examples of representations. We also introduce the concept of equivalence of representations, and consider the kernel of a representation.

## Representations

Let $G$ be a group and let $F$ be $\mathbb{R}$ or $\mathbb{C}$. Recall from the first chapter that $\mathrm{GL}(n, F)$ denotes the group of invertible $n \times n$ matrices with entries in $F$.

*3.1 Definition*
A *representation* of $G$ over $F$ is a homomorphism $\rho$ from $G$ to $\mathrm{GL}(n, F)$, for some $n$. The *degree* of $\rho$ is the integer $n$.

Thus if $\rho$ is a function from $G$ to $\mathrm{GL}(n, F)$, then $\rho$ is a representation if and only if

$$(gh)\rho = (g\rho)(h\rho) \quad \text{for all } g, h \in G.$$

Since a representation is a homomorphism, it follows that for every representation $\rho\colon G \to \mathrm{GL}(n, F)$, we have

$$1\rho = I_n, \text{ and}$$

$$g^{-1}\rho = (g\rho)^{-1} \quad \text{for all } g \in G,$$

where $I_n$ denotes the $n \times n$ identity matrix.

*3.2 Examples*

(1) Let $G$ be the dihedral group $D_8 = \langle a, b: a^4 = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle$. Define the matrices $A$ and $B$ by

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and check that

$$A^4 = B^2 = I,\ B^{-1}AB = A^{-1}.$$

It follows (see Example 1.4) that the function $\rho: G \to \mathrm{GL}(2, F)$ which is given by

$$\rho: a^i b^j \to A^i B^j \quad (0 \leqslant i \leqslant 3,\ 0 \leqslant j \leqslant 1)$$

is a representation of $D_8$ over $F$. The degree of $\rho$ is 2.

The matrices $g\rho$ for $g$ in $D_8$ are given in the following table:

| $g$ | $1$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| $g\rho$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ |

| $g$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
|---|---|---|---|---|
| $g\rho$ | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ |

(2) Let $G$ be any group. Define $\rho: G \to \mathrm{GL}(n, F)$ by

$$g\rho = I_n \quad \text{for all } g \in G,$$

where $I_n$ is the $n \times n$ identity matrix, as usual. Then

$$(gh)\rho = I_n = I_n I_n = (g\rho)(h\rho)$$

for all $g,\ h \in G$, so $\rho$ is a representation of $G$. This shows that every group has representations of arbitrarily large degree.

## Equivalent representations

We now look at a way of converting a given representation into another one.

Let $\rho\colon G \to \mathrm{GL}(n, F)$ be a representation, and let $T$ be an invertible $n \times n$ matrix over $F$. Note that for all $n \times n$ matrices $A$ and $B$, we have

$$(T^{-1}AT)(T^{-1}BT) = T^{-1}(AB)T.$$

We can use this observation to produce a new representation $\sigma$ from $\rho$; we simply define

$$g\sigma = T^{-1}(g\rho)T \quad \text{for all } g \in G.$$

Then for all $g, h \in G$,

$$\begin{aligned}(gh)\sigma &= T^{-1}((gh)\rho)T \\ &= T^{-1}((g\rho)(h\rho))T \\ &= T^{-1}(g\rho)T \cdot T^{-1}(h\rho)T \\ &= (g\sigma)(h\sigma),\end{aligned}$$

and so $\sigma$ is, indeed, a representation.

*3.3 Definition*
Let $\rho\colon G \to \mathrm{GL}(m, F)$ and $\sigma\colon G \to \mathrm{GL}(n, F)$ be representations of $G$ over $F$. We say that $\rho$ is *equivalent* to $\sigma$ if $n = m$ and there exists an invertible $n \times n$ matrix $T$ such that for all $g \in G$,

$$g\sigma = T^{-1}(g\rho)T.$$

Note that for all representations $\rho$, $\sigma$ and $\tau$ of $G$ over $F$, we have (see Exercise 3.4):

(1) $\rho$ is equivalent to $\rho$;
(2) if $\rho$ is equivalent to $\sigma$ then $\sigma$ is equivalent to $\rho$;
(3) if $\rho$ is equivalent to $\sigma$ and $\sigma$ is equivalent to $\tau$, then $\rho$ is equivalent to $\tau$.

In other words, equivalence of representations is an equivalence relation.

*3.4 Examples*
(1) Let $G = D_8 = \langle a, b\colon a^4 = b^2 = 1, b^{-1}ab = a^{-1}\rangle$, and consider the representation $\rho$ of $G$ which appears in Example 3.2(1). Thus $a\rho = A$

and $b\rho = B$, where

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Assume that $F = \mathbb{C}$, and define

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{pmatrix}.$$

Then

$$T^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -\mathrm{i} \\ 1 & \mathrm{i} \end{pmatrix}.$$

In fact, $T$ has been constructed so that $T^{-1}AT$ is diagonal; we have

$$T^{-1}AT = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad T^{-1}BT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and so we obtain a representation $\sigma$ of $D_8$ for which

$$a\sigma = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad b\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The representations $\rho$ and $\sigma$ are equivalent.

(2) Let $G = C_2 = \langle a: a^2 = 1 \rangle$ and let

$$A = \begin{pmatrix} -5 & 12 \\ -2 & 5 \end{pmatrix}.$$

Check that $A^2 = I$. Hence $\rho: 1 \to I$, $a \to A$ is a representation of $G$. If

$$T = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix},$$

then

$$T^{-1}AT = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and so we obtain a representation $\sigma$ of $G$ for which

$$1\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and $\sigma$ is equivalent to $\rho$.

There are two easily recognized situations where the only representation which is equivalent to $\rho$ is $\rho$ itself; these are when the degree of $\rho$ is 1, and when $g\rho = I_n$ for all $g$ in $G$. However, there are usually lots of representations which are equivalent to $\rho$.

## Kernels of representations

We conclude the chapter with a discussion of the kernel of a representation $\rho$: $G \to \mathrm{GL}(n, F)$. In agreement with Definition 1.8, this consists of the group elements $g$ in $G$ for which $g\rho$ is the identity matrix. Thus

$$\mathrm{Ker}\,\rho = \{g \in G\colon g\rho = I_n\}.$$

Note that $\mathrm{Ker}\,\rho$ is a normal subgroup of $G$.

It can happen that the kernel of a representation is the whole of $G$, as is shown by the following definition.

*3.5 Definition*
The representation $\rho$: $G \to \mathrm{GL}(1, F)$ which is defined by

$$g\rho = (1) \quad \text{for all } g \in G,$$

is called the *trivial* representation of $G$.

To put the definition another way, the trivial representation of $G$ is the representation where every group element is sent to the $1 \times 1$ identity matrix.

Of particular interest are those representations whose kernel is just the identity subgroup.

*3.6 Definition*
A representation $\rho$: $G \to \mathrm{GL}(n, F)$ is said to be *faithful* if $\mathrm{Ker}\,\rho = \{1\}$; that is, if the identity element of $G$ is the only element $g$ for which $g\rho = I_n$.

*3.7 Proposition*
*A representation $\rho$ of a finite group $G$ is faithful if and only if* $\mathrm{Im}\,\rho$ *is isomorphic to $G$.*

*Proof* We know that $\operatorname{Ker}\rho \lhd G$ and by Theorem 1.10, the factor group $G/\operatorname{Ker}\rho$ is isomorphic to $\operatorname{Im}\rho$. Therefore, if $\operatorname{Ker}\rho = \{1\}$ then $G \cong \operatorname{Im}\rho$. Conversely, if $G \cong \operatorname{Im}\rho$, then these two groups have the same (finite) order, and so $|\operatorname{Ker}\rho| = 1$; that is, $\rho$ is faithful. ■

*3.8 Examples*

(1) The representation $\rho$ of $D_8$ given by

$$(a^i b^j)\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^j$$

as in Example 3.2(1) is faithful, since the identity is the only element $g$ which satisfies $g\rho = I$. The group generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is therefore isomorphic to $D_8$.

(2) Since $T^{-1}AT = I_n$ if and only if $A = I_n$, it follows that all representations which are equivalent to a faithful representation are faithful.

(3) The trivial representation of a group $G$ if faithful if and only if $G = \{1\}$.

In Chapter 6 we shall show that every finite group has a faithful representation.

The basic problem of representation theory is to discover and understand representations of finite groups.

## Summary of Chapter 3

1. A representation of a group $G$ is a homomorphism from $G$ into $\mathrm{GL}(n, F)$, for some $n$.
2. Representations $\rho$ and $\sigma$ of $G$ are equivalent if and only if there exists an invertible matrix $T$ such that for all $g \in G$,
$$g\sigma = T^{-1}(g\rho)T.$$
3. A representation is faithful if it is injective.