Groups and Geometry
The Second Part
of
Algebra and Geometry

T.W.Körner

April 20, 2007

Small print The syllabus for the course is defined by the Faculty Board Schedules (which are minimal for lecturing and maximal for examining). What is presented here contains some results which it would not, in my opinion, be fair to set as book-work although they could well appear as problems. (A book-work question asks you for material which you are supposed to know. A problem question asks you to use known material to solve a question which you may not have seen before. A typical Cambridge examination question consists of book-work followed by a problem, the so-called 'rider', which makes use of the book-work.) I should **very much** appreciate being told of any corrections or possible improvements and might even part with a small reward to the first finder of particular errors. These notes are written in LaTeX 2_ε and should be available in tex, ps, pdf and dvi format from my home page

http://www.dpmms.cam.ac.uk/~twk/

My e-mail address is `twk@dpmms`. Supervisors can obtain notes on the exercises in the last four sections from the DPMMS secretaries or by e-mailing me for the dvi file.

Contents

1 Preliminary remarks

Convention 1.1. *We shall write $\mathbb{F}$ to mean either $\mathbb{C}$ or $\mathbb{R}$.*

Our motto in this course is 'linear maps for understanding, matrices for computation'. We recall some definitions and theorems from earlier on.

Definition 1.2. *Let $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ be linear and let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ be a basis. Then the matrix $A = (a_{ij})$ of α with respect to this basis is given by the rule*

$$\alpha(\mathbf{e}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{e}_i.$$

We observe that, if $\mathbf{x} = \sum_{j=1}^{n} x_j\mathbf{e}_j$ and $\alpha(\mathbf{x}) = \mathbf{y} = \sum_{i=1}^{n} y_i\mathbf{e}_i$, then

$$y_i = \sum_{j=1}^{n} a_{ij}x_j.$$

Thus coordinates and bases go opposite ways. The definition chosen is conventional but represents a universal convention and must be learnt.

Theorem 1.3. (Change of basis.) *Let $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ be a linear map. If α has matrix $A = (a_{ij})$ with respect to a basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ and matrix $B = (b_{ij})$ with respect to a basis $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n$, then there is an invertible $n \times n$ matrix P such that*

$$B = P^{-1}AP.$$

The matrix $P = (p_{ij})$ is given by the rule

$$\mathbf{f}_j = \sum_{i=1}^{n} p_{ij}\mathbf{e}_i.$$

We recall an important application of this result. Since

$$\det(P^{-1}AP) = (\det P)^{-1} \det A \det P = \det A,$$

we see that all matrix representations of a given linear map $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ have the same determinant. We can thus write $\det \alpha = \det A$ where A is any matrix representation of α.

Although we shall not conduct any explicit calculations, I shall assume that my audience is familiar with the process of Gaussian elimination both as a method of solving linear equations and of inverting square matrices. (If the previous lecturer has not covered these topics, I will.)

The following observation is quite useful.

Example 1.4. *If $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ is the standard basis (that is to say $\mathbf{e}_j$ is the collumn vector with 1 in the jth place and zero elsewhere), then the matrix A of a linear map α with respect to this basis has $\alpha(\mathbf{e}_j)$ as its jth collumn.*

2 Eigenvectors and eigenvalues

Definition 2.1. *If $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ is linear and $\alpha(\mathbf{u}) = \lambda\mathbf{u}$ for some vector $\mathbf{u} \neq \mathbf{0}$ and some $\lambda \in \mathbb{F}$, we say that $\mathbf{u}$ is an eigenvector of α with eigenvalue λ.*

Theorem 2.2. *If $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ is linear, then λ is an eigenvalue of α if and only if $\det(\lambda\iota - \alpha) = 0$.*

Lemma 2.3. *If $n = 3$, then any linear map $\alpha : \mathbb{R}^3 \to \mathbb{R}^3$ has an eigenvector. It follows that there exists some line l through $\mathbf{0}$ with $\alpha(l) \subseteq l$.*

Example 2.4. *Let $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map given by rotation through θ about $\mathbf{0}$. Then R_θ has no eigenvectors unless $\theta \equiv 0 \mod \pi$. If $\theta \equiv \pi \mod 2\pi$, then every vector in $\mathbb{R}^2 \setminus \{\mathbf{0}\}$ is an eigenvector with eigenvalue -1. If $\theta \equiv 0 \mod 2\pi$, then every vector in $\mathbb{R}^2 \setminus \{\mathbf{0}\}$ is an eigenvector with eigenvalue 1.*

Theorem 2.5. (Fundamental Theorem of Algebra.) *If $n \geq 1$ and $a_j \in \mathbb{C}$ $[j = 0, 1, \ldots, n]$ with $a_n \neq 0$, then the equation*

$$\sum_{j=0}^{n} a_j z^j = 0$$

has a solution in $\mathbb{C}$.

The Fundamental Theorem of Algebra is, in fact, a theorem of analysis and its proof is one of the many high spots of the complex variable theory lectures next year. We note the following corollary.

Lemma 2.6. *If $n \geq 1$ and $a_j \in \mathbb{C}$ $[j = 0, 1, \ldots, n-1]$, then we can find ω_1, ω_2, $\ldots$, $\omega_n \in \mathbb{C}$ such that*

$$z^n + \sum_{j=0}^{n-1} a_j z^j = \prod_{j=1}^{n} (z - \omega_j)$$

If $(z-\omega)^k$ is a factor of $z^n + \sum_{j=0}^{n-1} a_j z^j$, but $(z-\omega)^{k+1}$ is not we say that ω is a k times repeated root of $z^n + \sum_{j=0}^{n-1} a_j z^j$.

Lemma 2.7. *Any linear map $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ has an eigenvector. It follows that there exists a one dimensional complex subspace*

$$l = \{w\mathbf{e} : w \in \mathbb{C}\}$$

(where $\mathbf{e} \neq \mathbf{0}$) with $\alpha(l) \subseteq l$.

Theorem 2.8. *Suppose $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ is linear. Then α has diagonal matrix D with respect to a basis $\mathbf{e}_1$, $\mathbf{e}_2$, $\ldots$, $\mathbf{e}_n$ if and only if the $\mathbf{e}_j$ are eigenvectors. The diagonal entries d_{ii} of D are the eigenvalues of the $\mathbf{e}_i$.*

If α has a diagonal matrix with respect to some basis we say that α is diagonalisable.

Theorem 2.9. *If a linear map $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ has n distinct eigenvalues, then the associated eigenvectors form a basis and α has a diagonal matrix with respect to this basis.*

I shall prove this result for $n \leq 3$. It will be obvious from the proof that the result holds for all n, but the general result is best approached via the machinery of next year's linear algebra course.

Theorem 2.9 gives a sufficient but not a necessary condition for a linear map to be diagonalisable. The identity map $\iota : \mathbb{F}^n \to \mathbb{F}^n$ has only one eigenvalue but has the diagonal matrix I with respect to any basis. On the other hand even when we work in $\mathbb{C}^n$ rather than $\mathbb{R}^n$ not every linear map is diagonalisable.

Example 2.10. *Let $\mathbf{e}_1$, $\mathbf{e}_2$ be a basis for $\mathbb{F}^2$. The linear map $\beta : \mathbb{F}^2 \to \mathbb{F}^2$ given by*

$$\beta(x_1\mathbf{e}_1 + x_2\mathbf{e}_2) = x_2\mathbf{e}_1$$

is non-diagonalisable.

Fortunately the map just given is the 'typical' non-diagonalisable linear map for $\mathbb{C}^2$.

Theorem 2.11. *If $\alpha : \mathbb{C}^2 \to \mathbb{C}^2$ is linear, then exactly one of the following three things must happen.*

(i) α has two distinct eigenvalues λ and μ and we can take a basis of eigenvectors $\mathbf{e}_1$, $\mathbf{e}_2$ for $\mathbb{C}^2$. With respect to this basis, α has matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}.$$

(ii) α has only one distinct eigenvalue λ but is diagonalisable. Then $\alpha = \lambda\iota$ and has matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

with respect to any basis.

(iii) α has only one distinct eigenvalue λ and is not diagonalisable. Then there exists a basis $\mathbf{e}_1$, $\mathbf{e}_2$ for $\mathbb{C}^2$ with respect to which α has matrix

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Note that $\mathbf{e}_1$ is an eigenvector with eigenvalue λ but $\mathbf{e}_2$ is not.

The general case of a linear map $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ is substantially more complicated. The possible outcomes are classified using the 'Jordan Normal Form' in a theorem that is easy to state and understand but tricky to prove.

We have the following corollary to Theorem 2.11.

Example 2.12. (Cayley–Hamilton in 2 dimensions.) *If $\alpha : \mathbb{C}^2 \to \mathbb{C}^2$ is a linear map, let us write $Q(t) = \det(t\iota - \alpha)$. Then we have*

$$Q(t) = t^2 + at + b$$

where a, $b \in \mathbb{C}$. The Cayley–Hamilton theorem states that

$$\alpha^2 + a\alpha + b\iota = O$$

or, more briefly[1]*, that $Q(\alpha) = O$.*

We call Q the characteristic polynomial of α and say that α satisfies its own characteristic equation. Once again the result is much harder to prove in higher dimensions. (If you find Example 2.12 hard, note that it is merely an example and not central to the course.)

3 Computation

Let us move from ideas to computation.

Theorem 3.1. *The following two statements about an $n \times n$ matrix A over $\mathbb{F}$ are equivalent.*

(i) If we choose a basis $\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_n$ for $\mathbb{F}^n$ and define a linear map $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ by

$$\alpha(\mathbf{u}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{u}_i,$$

then we can find a basis $\mathbf{e}_1$, $\mathbf{e}_2$, ..., $\mathbf{e}_n$ for $\mathbb{F}^n$ and $d_i \in \mathbb{F}$ such that

$$\alpha(\mathbf{e}_j) = d_j\mathbf{e}_j.$$

(ii) There is a non-singular $n \times n$ matrix P such that $P^{-1}AP$ is diagonal.

If the conditions of Theorem 3.1 hold, we say that A is diagonalisable. (Thus a matrix A is diagonalisable if and only if it represents a diagonalisable linear map with respect to some basis.) As an indication of why diagonalisation is likely to be useful, observe that if A, P, D are $n \times n$ matrices with P invertible, D diagonal and $P^{-1}AP = D$, then

$$A^m = (PDP^{-1})^m = PDP^{-1}PDP^{-1} \dots PDP^{-1} = PD^mP^{-1}$$

and note how easy it is to compute D^m. Here is an example of why it might be useful to compute powers of matrices.

[1]But more confusingly for the novice.

Example 3.2. *Let n towns be called (rather uninterestingly) $1, 2, \ldots, n$. Write $a_{ij} = 1$ if there is a road leading directly from town i to town j and $a_{ij} = 0$ otherwise (we take $a_{ii} = 0$). If we write $A^m = (a_{ij}^{(m)})$ then $a_{ij}^{(m)}$ is the number of routes from i to j of length m. (A route of length m passes through $m + 1$ towns including the starting and finishing towns. If you pass through the same town more than once each visit is counted separately.)*

In the discussion that follows, we take the basis vectors $\mathbf{u}_j$ to be the standard column vectors of length n with entries 0 except in the jth place where we have 1. Recall that any $n \times n$ matrix A gives rise to a linear map α by the rule

$$\alpha(\mathbf{u}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{u}_i.$$

Suppose that we wish to 'diagonalise' such an $n \times n$ matrix. The first step is to look at the roots of the characteristic polynomial

$$P(t) = \det(tI - A).$$

If we work over $\mathbb{R}$ and some of the roots of P are not real, we know at once that A is not diagonalisable (over $\mathbb{R}$). If we work over $\mathbb{C}$ or if we work over $\mathbb{R}$ and all the roots are real, we can move on to the next stage. Either the characteristic polynomial has n distinct roots or it does not. If it does, we know that A is diagonalisable. If we find the n distinct roots (easier said than done outside the artificial conditions of the examination room) $\lambda_1, \lambda_2, \ldots, \lambda_n$ we know without further computation that there exists a non-singular P such that $P^{-1}AP = D$ where D is a diagonal matrix with diagonal entries λ_j. Often knowledge of D is sufficient for our purposes but if not we proceed to find P as follows.

For each λ_j we know that the system of n linear equations in n unknowns given by

$$(A - \lambda_j I)\mathbf{x} = \mathbf{0}$$

(where $\mathbf{x}$ is a column vector of length n, that is to say, with n entries) has non-zero solutions. Let $\mathbf{e}_j$ be one of them so that

$$A\mathbf{e}_j = \lambda_j\mathbf{e}_j.$$

Note that, if P is the $n \times n$ matrix with jth column $\mathbf{e}_j$, then $P\mathbf{u}_j = \mathbf{e}_j$ and

$$P^{-1}AP\mathbf{u}_j = P^{-1}A\mathbf{e}_j = \lambda_j P^{-1}\mathbf{e}_j = \lambda_j\mathbf{u}_j = D\mathbf{u}_j$$

for all $1 \leq j \leq n$ and so

$$P^{-1}AP = D.$$

If we need to know P^{-1}, we calculate it by inverting P in some standard way.

Exercise 3.3. *Diagonalise the matrix*

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

(with θ real) over $\mathbb{C}$.

What if the characteristic polynomial does not have n distinct roots? In this case we do not know, without further investigation, whether A is diagonalisable or not. Example 2.10 gives us

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

as an example of a non-diagonalisable matrix over $\mathbb{C}$. This problem will be looked at further in next year's linear algebra course. Later I will do a simple example (the second matrix of Example 5.8) where the characteristic polynomial has repeated roots.

It cannot be emphasised too strongly that the method described above bears the same relation to real life problems as 'Tom And Wendy Go Shopping' does to 'King Lear'. (But remember that you learn to read by reading 'Tom And Wendy Go Shopping' rather than 'King Lear'.) If $n = 200$ then the characteristic polynomial is likely to be extremely unpleasant.

We can now rewrite Theorem 2.11 as follows.

Theorem 3.4. *If A is a 2×2 complex matrix then exactly one of the following three things must happen.*

(i) We can find a non-singular 2×2 complex matrix P such that

$$P^{-1}AP = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

with $\lambda \neq \mu$.

(ii) $A = \lambda I$ for some λ.

(iii) We can find a non-singular 2×2 complex matrix P such that

$$P^{-1}AP = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

for some λ.

The following result links up with the first year course on differential equations.

Example 3.5. *Consider the simultaneous differential equations*

$$\dot{x}_1 = a_{11}x_1 + a_{12}x_2$$
$$\dot{x}_2 = a_{21}x_1 + a_{22}x_2$$

According as A falls into one of the three cases given in Theorem 3.4:
(i) $x_1(t)$ is a linear combination of $e^{\lambda t}$ and $e^{\mu t}$.
(ii) $x_1(t) = C_1 e^{\lambda t}$, $x_2(t) = C_2 e^{\lambda t}$, with C_1 and C_2 arbitrary.
(iii) $x_1(t)$ is a linear combination of $e^{\lambda t}$ and $te^{\lambda t}$.

4 Distance-preserving linear maps

We start with a trivial example.

Example 4.1. *A restaurant serves n different dishes. The 'meal vector' of a customer is the column vector $\mathbf{x} = (x_1, x_2, \dots, x_n)$ where x_j is the quantity of the jth dish ordered. At the end of the meal, the waiter uses the linear map $P : \mathbb{R}^n \to \mathbb{R}$ to obtain $P(\mathbf{x})$ the amount (in pounds) the customer must pay.*

Although the 'meal vectors' live in $\mathbb{R}^n$ it is not very useful to talk about the distance between two meals. There are many other examples where it is counter-productive to saddle $\mathbb{R}^n$ with things like distance and angle.

Equally there are many other occasions (particularly in the study of the real world) when it makes sense to consider $\mathbb{R}^n$ equipped with the scalar product (inner product)

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{r=1}^{n} x_r y_r,$$

the Euclidean norm

$$||\mathbf{x}|| = \langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$$

(we take the positive square root) and Euclidean distance

$$\text{distance between } \mathbf{x} \text{ and } \mathbf{y} = ||\mathbf{x} - \mathbf{y}||.$$

Definition 4.2. *(i) We say that $\mathbf{a}$ and $\mathbf{b}$ are orthogonal if $\langle \mathbf{a}, \mathbf{b} \rangle = 0$.*
(ii) We say that $\mathbf{e}_1$, $\mathbf{e}_2$, ..., $\mathbf{e}_n$ are orthonormal if

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

for all $1 \leq i, j \leq n$.

Lemma 4.3. *Any system of n orthonormal vectors $\mathbf{e}_1$, $\mathbf{e}_2$, ..., $\mathbf{e}_n$ forms a basis for $\mathbb{R}^n$. (We call this an orthonormal basis.) If $\mathbf{x} \in \mathbb{R}^n$, then*

$$\mathbf{x} = \sum_{r=1}^{n} \langle \mathbf{x}, \mathbf{e}_r \rangle \mathbf{e}_r.$$

It will not have escaped the reader that the standard unit vectors $\mathbf{e}_j$ (with 1 as jth entry, 0 everywhere else) form an orthonormal basis[2]. what

The following remark is used repeatedly in studying inner products.

Lemma 4.4. *If $\langle \mathbf{a}, \mathbf{x} \rangle = \langle \mathbf{b}, \mathbf{x} \rangle$ for all $\mathbf{x}$ then $\mathbf{a} = \mathbf{b}$.*

Our first task will be to study those linear maps which preserve length. Our main tool is a simple and rather pretty equality.

Lemma 4.5. *If $\mathbf{a}$, $\mathbf{b} \in \mathbb{R}^n$, then*

$$||\mathbf{a} + \mathbf{b}||^2 - ||\mathbf{a} - \mathbf{b}||^2 = 4\langle \mathbf{a}, \mathbf{b} \rangle.$$

We shall also need a definition.

Definition 4.6. *If A is the $n \times n$ matrix (a_{ij}), then A^T (the transpose of A) is the $n \times n$ matrix (b_{ij}) with $b_{ij} = a_{ji}$ $[1 \leq i, j \leq n]$.*

Lemma 4.7. *If the linear map $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ has matrix A with respect to some orthonormal basis and $\alpha^* : \mathbb{R}^n \to \mathbb{R}^n$ is the linear map with matrix A^T with respect to the same basis, then*

$$\langle \alpha \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha^* \mathbf{y} \rangle$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Further, if the linear map $\beta : \mathbb{R}^n \to \mathbb{R}^n$ satisfies

$$\langle \alpha \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \beta \mathbf{y} \rangle$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, then $\beta = \alpha^*$.

Exercise 4.8. *Let α, $\beta : \mathbb{R}^n \to \mathbb{R}^n$ be linear.*

(i) $(\alpha\beta)^* = \beta^* \alpha^*$.

(ii) $\alpha^{**} = \alpha$.

---

[2] It will also not have escaped the reader that sometimes I call the standard basis $\mathbf{e}_j$ and sometimes $\mathbf{u}_j$. There is no fixed notation and you should always say explicitly if you wish a particular set of vectors to have a particular property.

Theorem 4.9. *Let $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ be linear. The following statements are equivalent.*

(i) $||\alpha\mathbf{x}|| = ||\mathbf{x}||$ *for all* $\mathbf{x} \in \mathbb{R}^n$.

(ii) $\langle \alpha\mathbf{x}, \alpha\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$ *for all* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

(iii) $\alpha^*\alpha = \iota$.

(iv) If α *has matrix* A *with respect to some orthonormal basis then* $A^T A = I$.

If, as I shall tend to do, we think of the linear maps as central, we refer to the collection of distance preserving linear maps by the name $O(\mathbb{R}^n)$. If we think of the matrices as central, we refer to the collection of real $n \times n$ matrices A with $AA^T = I$ by the name $O(\mathbb{R}^n)$. In practice most people use whichever convention is most convenient at the time and no confusion results. A real $n \times n$ matrix A with $AA^T = I$ is called an orthogonal matrix.

We recall that the determinant of a square matrix can be evaluated by row or by column expansion and so

$$\det A^T = \det A.$$

Lemma 4.10. *If A is an orthogonal matrix, then* $\det A = 1$ *or* $\det A = -1$.

If we think in terms of linear maps, we define

$$SO(\mathbb{R}^n) = \{\alpha \in O(\mathbb{R}^n) : \det \alpha = 1\}.$$

If we think in terms of matrices, we define

$$SO(\mathbb{R}^n) = \{A \in O(\mathbb{R}^n) : \det A = 1\}.$$

(The letter O stands for ‘orthogonal’, the letters SO for ‘special orthogonal’.)

In the rest of this section we shall look at other ways of characterising $O(\mathbb{R}^n)$ and $SO(\mathbb{R}^n)$. We shall think in terms of linear maps. We shall use an approach which, I am told, goes back to Euler.

Definition 4.11. *If* $\mathbf{n}$ *is a vector of norm 1, the map* $R : \mathbb{R}^n \to \mathbb{R}^n$ *given by*

$$R(\mathbf{x}) = \mathbf{x} - 2\langle \mathbf{x}, \mathbf{n}\rangle \mathbf{n}$$

is said to be a reflection in

$$\pi = \{\mathbf{x} : \langle \mathbf{x}, \mathbf{n}\rangle = 0\}.$$

Lemma 4.12. *With the notation of the definition just given:*

(i) There is an orthonormal basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ *with respect to which R has a diagonal matrix D with* $d_{11} = -1$, $d_{ii} = 1$ *for all* $2 \leq i \leq n$.

(ii) $R^2 = \iota$.

(iii) $R \in O(\mathbb{R}^n)$.

(iv) $\det R = -1$.

(v) If $||\mathbf{x}|| = ||\mathbf{y}||$ *and* $\mathbf{x} \neq \mathbf{y}$, *then we can find a unit vector* $\mathbf{n}$ *such that* $R\mathbf{x} = \mathbf{y}$. *Moreover, we can choose* R *in such a way that, whenever* $\mathbf{u}$ *is perpendicular to* $\mathbf{x}$ *and* $\mathbf{y}$, *we have* $R\mathbf{u} = \mathbf{u}$.

Lemma 4.13. *If* $\alpha \in O(\mathbb{R}^n)$, *then* α *is the product of* m *reflections with* $0 \leq m \leq n$. *(If* $m = 0$, $\alpha = \iota$. *Otherwise, we can find reflections* R_1, R_2, $\dots$, R_m *such that* $\alpha = R_1 R_2 \dots R_m$.*) If* m *is even,* $\alpha \in SO(\mathbb{R}^n)$. *If* m *is odd,* $\alpha \notin SO(\mathbb{R}^n)$.

Lemma 4.14. *If* $\alpha \in O(\mathbb{R}^2)$ *then one of two things must happen.*

(i) $\alpha \in SO(\mathbb{R}^2)$ *and we can find* $0 \leq \theta < 2\pi$ *such that, with respect to any orthonormal basis,* α *has one of the two possible matrices*

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ or } \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

(ii) $\alpha \notin SO(\mathbb{R}^2)$ *and we can find an orthonormal basis with respect to which* α *has matrix*

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

To see why we have to allow two forms in part (i), consider an orthonormal basis $\mathbf{e}_1$, $\mathbf{e}_2$ and the related orthonormal basis $\mathbf{e}_1$, $-\mathbf{e}_2$.

Exercise 4.15. *By considering the product of the rotation matrices*

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ and } \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$$

we can recover the addition formulae for cos *and* sin.

Lemma 4.16. *(i) If* $\alpha \in O(\mathbb{R}^3)$ *then we can find an orthonormal basis with respect to which* α *has matrix*

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

(ii) If the plus sign is taken in (i), $\alpha \in SO(\mathbb{R}^3)$. *If the minus sign is taken,* $\alpha \notin SO(\mathbb{R}^3)$.

The traditional way of stating that part of Lemma 4.16 which deals with $SO(\mathbb{R}^3)$ is to say that every rotation has an axis. (Things are more complicated in higher dimensions, but we do not need to go further in this course. If you are interested, look at Exercise 15.17.) It may be worth stating some of our earlier results in the form they we be used in the discussion of Cartesian tensors in next year's mathematical methods course.

Lemma 4.17. *If the matrix $L \in O(\mathbb{R}^3)$, then, using the summation convention,*

$$l_{ik}l_{jk} = \delta_{ij}.$$

Further,

$$\epsilon_{ijk}l_{ir}l_{js}l_{kt} = \pm\epsilon_{rst}$$

with the positive sign if $L \in SO(\mathbb{R}^3)$ and the negative sign otherwise.

We also make the following remark.

Lemma 4.18. *An $n \times n$ real matrix L is orthogonal if and only if its columns are orthonormal column vectors. An $n \times n$ real matrix L is orthogonal if and only if its rows are orthonormal row vectors.*

5 Real symmetric matrices

We say that a real $n \times n$ matrix A is symmetric if $A^T = A$. In this section we deal with the diagonalisation of such matrices. It is not immediately clear why this is important but in the next couple of years the reader will come across the topic in many contexts.

(1) The study of Sturm–Liouville differential equations in the methods course next year runs in parallel with what we do here.

(2) The study of symmetric tensors in the methods course next year will quote our results.

(3) The t-test, F-test and so on in the statistics course next year depend on the diagonalisation of a symmetric matrix.

(4) The study of small oscillations about equilibrium depends on a generalisation of our ideas.

(5) The standard formalism for Quantum Mechanics and the spectral theorem in functional analysis are both deep generalisations of what we do here.

For the moment we note that the covariance matrix $(\mathbb{E}X_iX_j)$ of n random variables and the Hessian matrix

$$\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)$$

of the second partial derivatives of a well behaved function f of n variables are both symmetric matrices. (If one or other or both these matrices make no sense to you, all will become clear next term in the probability and vector calculus courses.)

Lemma 5.1. *Let $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ be linear. The following statements are equivalent.*

(i) $\langle \alpha\mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{x}, \alpha\mathbf{y}\rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

(ii) If α has matrix A with respect to some orthonormal basis, then A is symmetric.

Naturally we call an α, having the properties just described, symmetric. We can also call α a 'real self-adjoint' map.

Theorem 5.2. *If $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is symmetric, then all the roots of the characteristic polynomial* $\det(t\iota - \alpha)$ *are real.*

Theorem 5.3. *If $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is symmetric, then eigenvectors corresponding to distinct eigenvalues are orthogonal.*

Theorem 5.4. *(i) If $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is symmetric and all the roots of the characteristic polynomial* $\det(t\iota-\alpha)$ *are distinct, then there exists an orthonormal basis of eigenvectors of α.*

(ii) If A is a symmetric $n \times n$ matrix and and all the roots of the characteristic polynomial $\det(tI - A)$ *are distinct, then there exists a matrix $P \in SO(\mathbb{R}^n)$ such that $P^T AP$ is diagonal.*

Much more is true.

Fact 5.5. *(i) If $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ is symmetric, then there exists an orthonormal basis of eigenvectors of $\mathbb{R}^n$ with respect to which α is diagonal.*

(ii) If A is a symmetric $n \times n$ matrix, then there exists a matrix $P \in SO(\mathbb{R}^n)$ such that $P^T AP$ is diagonal.

I may sketch a proof for the case $n = 3$ but it will not be examinable. The general case will be proved with more sophisticated techniques in next year's linear algebra course. We note the easy converse results.

Lemma 5.6. *(i) If $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ has an orthonormal basis of eigenvectors, then α is symmetric.*

(ii) If A is an $n \times n$ real matrix and there exists a matrix $P \in SO(\mathbb{R}^n)$ such that $P^T AP$ is diagonal, then A is symmetric.

It is important to think about the various conditions on our results.

Exercise 5.7. *Let*

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Compute PAP^{-1} and observe that it is not a symmetric matrix, although A is. Why does this not contradict Lemma 5.6.

Moving from theory to practice, we see that the diagonalisation of an $n \times n$ symmetric matrix A (using an orthogonal matix) follows the same pattern as ordinary diagonalisation (using an invertible matrix). The first step is to look at the roots of the characteristic polynomial

$$P(t) = \det(tI - A).$$

By Theorem 5.2 we know that all the roots are real. If we can find the n roots (in examinations, n will usually be 2 or 3 and the resulting quadratics and cubics will have nice roots) $\lambda_1, \lambda_2, \dots, \lambda_n$ and the roots are distinct then we know, without further calculation, that there exists an orthogonal matrix P with

$$P^T AP = D,$$

where D is the diagonal matrix with diagonal entries $d_{ii} = \lambda_i$.

For each λ_j we know that the system of n linear equations in n unknowns given by

$$(A - \lambda_j I)\mathbf{x} = \mathbf{0}$$

(with $\mathbf{x}$ a column vector of length n) has non-zero solutions. Let $\mathbf{u}_j$ be one of them so that

$$A\mathbf{u}_j = \lambda_j \mathbf{u}_j.$$

We normalise by setting

$$\mathbf{e}_j = ||\mathbf{u}_j||^{-1}\mathbf{u}_j$$

and, unless we are unusually confident of our arithmetic, check that, as Theorem 5.3 predicts,

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}.$$

If P is the $n \times n$ matrix with jth column $\mathbf{e}_j$ then, from the formula just given, P is orthogonal (i.e., $PP^T = I$ and so $P^{-1} = P^T$). We note that, if we write $\mathbf{v}_j$ for the unit vector with 1 in the jth place, 0 elsewhere, then

$$P^T AP\mathbf{v}_j = P^{-1}A\mathbf{e}_j = \lambda_j P^{-1}\mathbf{e}_j = \lambda_j \mathbf{v}_j = D\mathbf{v}_j$$

for all $1 \le j \le n$ and so

$$P^T AP = D.$$

Our construction gives $P \in O(\mathbb{R}^n)$ but does not guarantee that $P \in SO(\mathbb{R}^n)$. If $\det P = 1$, then $P \in SO(\mathbb{R}^n)$. If $\det P = -1$, then replacing $\mathbf{e}_1$ by $-\mathbf{e}_1$ gives a new P in $SO(\mathbb{R}^n)$.

The strict logic of syllabus construction implies that the reader should not be asked to diagonalise a symmetric matrix when the characteristic equation has repeated roots until she has done next year's linear algebra course. Unfortunately nature is not very obliging and symmetric matrices which appear in physics often have repeated roots. If A is a symmetric 3×3 matrix we proceed as follows. If the characteristic polynomial P has a three times repeated root λ (i.e., $P(t) = (t-\lambda)^3$) then (since A is symmetric, so $A = P^T(\lambda I)P = \lambda I$ for some othogonal P) we have $A = \lambda I$ and there is no problem. If P has a single root μ and a double root λ (i.e., $P(t) = (t-\mu)(t-\lambda)^2$) then, as before, we can find $\mathbf{e}_1$ a column vector of Euclidean length 1 with $A\mathbf{e}_1 = \mu\mathbf{e}_1$. On the other hand, it will turn out that we can find two orthonormal vectors $\mathbf{e}_2$, $\mathbf{e}_3$ such that

$$A\mathbf{e}_2 = \lambda\mathbf{e}_2,\ A\mathbf{e}_3 = \lambda\mathbf{e}_3.$$

If we take P to be the 3×3 matrix with jth column $\mathbf{e}_j$, then P is orthogonal and

$$P^TAP = \begin{pmatrix} \mu & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.$$

Example 5.8. *We shall diagonalise*

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

As I said earlier, most of the applications of the results of this section will occur in later courses but we can give one important one immediately. Let $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ be the standard orthonormal basis of column vectors for $\mathbb{R}^n$. Consider a 'quadratic form' $Q : \mathbb{R}^n \to \mathbb{R}$ given by

$$Q(\mathbf{x}) = \sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j,$$

where $\mathbf{x} = \sum_{i=1}^n x_i\mathbf{u}_i$. It is clear that there is no loss in generality in taking $a_{ij} = a_{ji}$. We then have

$$Q(\mathbf{x}) = \mathbf{x}^TA\mathbf{x}$$

with A the symmetric matrix (a_{ij}). We know that there exists a special orthogonal matrix P such that

$$P^TAP = D$$

with D diagonal. In particular, setting $\mathbf{e}_j = P\mathbf{u}_j$, we see that the $\mathbf{e}_j$ form an orthonormal basis for $\mathbb{R}^n$ such that, if $\mathbf{y} = \sum_{i=1}^n y_i\mathbf{e}_i$, then

$$Q(\mathbf{y}) = \sum_{i=1}^n d_{ii}y_i^2.$$

Example 5.9. *Suppose that $f : \mathbb{R}^2 \to \mathbb{R}$ is given by*

$$f(\mathbf{x}) = ax^2 + 2bxy + cy^2$$

with respect to some orthogonal axes Oxy. Then we can find orthogonal axes OXY with respect to which

$$f(\mathbf{x}) = AX^2 + CY^2,$$

for some A and C. We observe that
(i) If $A, C > 0$, f has a minimum at $\mathbf{0}$.
(ii) If $A, C < 0$, f has a maximum at $\mathbf{0}$.
(iii) If $A < 0 < C$ or $C < 0 < A$ then f has a so-called 'saddle point' (or 'pass') at $\mathbf{0}$.

This result underlies the treatment of stationary points in the vector calculus course next term.

Example 5.10. *The set*

$$\{(x, y) \in \mathbb{R}^2 : ax^2 + 2bxy + cy^2 = d\}$$

is an ellipse, a point, the empty set, a hyperbola, a pair of lines meeting at $(0, 0)$, a pair of parallel lines, a single line or the whole plane.

6 Concrete groups

Although the syllabus does not explicitly require it, life will be simpler if we start with a discussion of functions. Recall that a function $f : A \to B$ assigns to each $a \in A$ a *unique* element $f(a)$ in B. The reader may feel disappointed that we have not defined the concept of function in terms of more primitive concepts but we must start somewhere and I shall assume that the lecture audience and I share the same notion of function. I shall rely strongly on the following key definition.

Definition 6.1. *If $f, g : A \to B$ are functions we say that $f = g$ if $f(a) = g(a)$ for all $a \in A$.*

Again, although the syllabus does not contain the following definitions, it will be convenient to have them readily to hand.

Definition 6.2. *(i) We say that $f : A \to B$ is injective if $f(x) = f(y)$ implies $x = y$.*

(ii) We say that $f : A \to B$ is surjective[3] *if given $b \in B$ there exists an $a \in A$ such that $f(a) = b$.*

(iii) We say that $f : A \to B$ is bijective if f is both injective and surjective.

In other words, f is injective if the equation $f(a) = b$ has at most one solution for each $b \in B$; f is surjective if the equation $f(a) = b$ has at least one solution for each $b \in B$; f is bijective if the equation $f(a) = b$ has exactly one solution for each $b \in B$.

Still more informally, f is injective if different points go to different points and f is surjective if it hits every point in B. (However, it turns out to be genuinely easier to prove things using the definition than by using their informal restatement.)

Definition 6.3. *If X is a set then we write $S(X)$ for the set of bijective maps $\sigma : X \to X$.*

If X is finite then we may picture $S(X)$ as the set of shuffles of an appropriate deck of cards. (By shuffles I mean actions like 'Interchange the 2nd and the 23rd card,' 'Reverse the order of the pack,' and so on.)

Theorem 6.4. *(i) If $\sigma, \tau \in S(X)$ and we write $(\sigma\tau)(x) = \sigma(\tau(x))$, then $\sigma\tau \in S(X)$.*

(ii) If $\sigma, \tau, \rho \in S(X)$, then

$$(\sigma\tau)\rho = \sigma(\tau\rho).$$

(iii) If we define $\iota : X \to X$ by $\iota(x) = x$, then $\iota \in S(X)$. Further,

$$\iota\sigma = \sigma\iota = \sigma$$

for all $\sigma \in S(X)$.

(iv) If $\sigma \in S(X)$, we can define a function $\sigma^{-1} : X \to X$ by $\sigma^{-1}(x) = y$ when $\sigma(y) = x$. The function $\sigma^{-1} \in S(X)$ and

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \iota.$$

[3]The word 'onto' is sometimes used in place of 'surjective'. You should not use the terms 'one-one' or 'one to one' since a a quick trawl with your favourite search engine shows that there is deep confusion about which word means which thing.

We call ι the identity and σ^{-1} the inverse of σ. We call $S(X)$ the 'permutation group of X' (or the 'symmetric group on X').

When X is finite, $S(X)$ has been the object of profitable study both by men with waxed moustaches and wide sleeves and by mathematicians. (In this course we will acquire enough knowledge to handle Exercise 18.12 which interests both classes of humanity.) However, when $X = \mathbb{R}^n$ or even when $X = \mathbb{R}$, $S(X)$ contains objects not merely weirder than we imagine, but, most mathematicians believe, weirder than we can possibly imagine. Under these circumstances it makes sense to study not $S(X)$ itself but smaller 'subgroups'.

Definition 6.5. *If G is a subset of $S(X)$ such that*
(i) $\sigma, \tau \in G$ implies $\sigma\tau \in G$,
(ii) $\sigma \in G$ implies $\sigma^{-1} \in G$,
(iii) $\iota \in G$,
we say that G is a subgroup of $S(X)$. We also say that G is a group acting faithfully[4] *on X, or less precisely that G is a concrete group.*

Conditions (i) to (iii) can be re-expressed in various ways (for example (iii) can be replaced by the condition G non-empty, see also Exercise 16.1 (iii)) but are quite convenient as they stand. If G and H are subgroups of $S(X)$ with $H \subseteq G$, we say that H is a subgroup of G.

Here are some examples of concrete groups.

Example 6.6. *(i) The set $GL(\mathbb{F}^n)$ of invertible linear maps $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ forms a group acting faithfully on $\mathbb{F}^n$. We call it the general linear group.*

(ii) The set $E(\mathbb{R}^n)$ of bijective isometries[5] *$\alpha : \mathbb{R}^n \to \mathbb{R}^n$ forms a group acting faithfully on $\mathbb{R}^n$. We call it the Euclidean group.*

(iii) The set $O(\mathbb{R}^n)$ of linear isometries forms a group acting faithfully on $\mathbb{R}^n$. We call it the orthogonal group[6]*.*

(iv) The set $SL(\mathbb{R}^n)$ of linear maps with determinant 1 forms a group acting faithfully on $\mathbb{R}^n$. We call it the special linear group.

(v) The set $SO(\mathbb{R}^n)$ of linear isometries with determinant 1 forms a group acting faithfully on $\mathbb{R}^n$. We call it the special orthogonal group.

(vi) $GL(\mathbb{R}^n) \supseteq E(\mathbb{R}^n) \cap GL(\mathbb{R}^n) = O(\mathbb{R}^n) \supseteq SO(\mathbb{R}^n)$ and

$$SO(\mathbb{R}^n) = O(\mathbb{R}^n) \cap SL(\mathbb{R}^n).$$

However, if $n \geq 2$, $SL(\mathbb{R}^n) \not\subseteq O(\mathbb{R}^n)$.

[4] We give an alternative but entirely equivalent definition of what it means for a group G to act faithfully on a set X in Definition 7.19.

[5] An isometry is automatically injective and the ideas of Example 6.7 show that an isometry of $\mathbb{R}^n$ is always a bijection, so, if we were prepared to work harder we could leave out the qualifier 'bijective'.

[6] Sometimes called $O(n)$, $O_n(\mathbb{R})$, $O(\mathbb{R}, n)$ or $O(n, \mathbb{R})$. It is always clear what is meant.

Example 6.7. *If $S \in E(\mathbb{R}^n)$ the group of isometries, then we can find a translation $T_{\mathbf{a}}$ (with $T_{\mathbf{a}}(\mathbf{x}) = \mathbf{a} + \mathbf{x}$) and $R \in O(\mathbb{R}^n)$ such that*

$$S = T_{\mathbf{a}} R.$$

(Our treatment of Example 6.7 will be informal.)

Example 6.8. *The collection G of similarity-preserving maps[7] $S : \mathbb{R}^n \to \mathbb{R}^n$ forms a group acting faithfully on $\mathbb{R}^n$. (We call it the similarity group.) If $S \in G$, then we can find a translation $T_{\mathbf{a}}$ (with $T_{\mathbf{a}}(\mathbf{x}) = \mathbf{a} + \mathbf{x}$), a dilation D_λ (with $D_\lambda(\mathbf{x}) = \lambda\mathbf{x}$, $\lambda > 0$) and $R \in O(\mathbb{R}^n)$ such that*

$$S = D_\lambda T_{\mathbf{a}} R.$$

The great German mathematician Klein suggested that geometry was the study of those properties of $\mathbb{R}^n$ which are invariant under the actions of a particular subgroup of $S(\mathbb{R}^n)$. Thus 'Euclidean Geometry' is the study of the properties of $\mathbb{R}^n$ invariant under the actions of the Euclidean group. A particularly interesting example occurs when we consider the collection G of $f \in S(\mathbb{R}^n)$ such that f and f^{-1} are continuous. (The reader may easily check that G is in fact a group.) The study of the properties of $\mathbb{R}^n$ invariant under the actions of G is now called topology. These ideas will be taken up again in Part II.

Continuing the geometric theme, we define the so-called symmetry groups.

Lemma 6.9. *Let X be a set of points in $\mathbb{R}^n$. The collection G of $\sigma \in S(X)$ such that*

$$||\sigma(\mathbf{x}) - \sigma(\mathbf{y})|| = ||\mathbf{x} - \mathbf{y}||$$

for all $\mathbf{x}, \mathbf{y} \in X$ is a subgroup of $S(X)$.

We call G the symmetry group of X. If we pick a random collection of points then, in general, G will consist of the single element ι. However, if X consists of the vertices of a regular polygon or solid, G becomes more interesting. The syllabus used to state rather grandly that the lecturer should talk about 'symmetry groups of regular polygons and solids'. Since Klein devoted an entire book to the study of the symmetry group of the regular icosahedron[8] this was rather tall order and lecturers made only the feeblest attempt to carry it out. In Example 7.14 we shall look at the symmetry group of the regular tetrahedron (this is very easy, can you see why?) and

[7] Maps which preserve angles and straight lines. Our treatment will be informal and the result is not part of the course.

[8] There is a remarkable Open University TV programme on the same subject.

the symmetry group of the cube. There will be a more detailed study of the symmetry groups of the regular solids in a later geometry course. For the moment we look at the symmetry group of the regular polygons in the plane.

Lemma 6.10. *If $n \geq 3$, the symmetry group D_n of the regular n-gon in $\mathbb{R}^2$ has $2n$ elements. If α is a rotation about the centre of the n-gon of $2\pi/n$ and β is a reflection about some axis of symmetry, then the distinct elements of D_n are*

$$\iota,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}, \beta,\ \alpha\beta,\ \alpha^2\beta,\ \ldots,\ \alpha^{n-1}\beta.$$

Further

$$\alpha^n = \iota,\ \beta^2 = \iota,\ \beta\alpha = \alpha^{-1}\beta.$$

(Since the mathematical literature is confused about whether to write D_n or D_{2n} for the group just described, you should always make it clear that you mean the symmetry group of the regular n-gon.)

Students are liable to panic when faced with so many different groups. They should note that the syllabus gives them as *examples* and that, though there is nothing to prevent a rogue examiner suddenly asking for the definition of some named group, a glance through previous examination papers shows that, in practice, examiners give definitions of all but the commonest groups.

7 Abstract groups and isomorphism

Traditional treatments of group theory begin not with concrete but with abstract groups.

Definition 7.1. *We say that $(G, *)$ is an (abstract) group if G is a set and $*$ an operation such that*

(i) If $a, b \in G$, then $a * b \in G$. (Closure)

(ii) If $a, b, c \in G$, then $(a * b) * c = a * (b * c)$. (Associativity)

(iii) There exists an $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (Unit)

(iv) If $a \in G$, then there exists an element $a^{-1} \in G$ with $a^{-1} * a = a * a^{-1} = e$. (Inverse)

The associativity rule means that we can bracket expressions any way we like. Ordinary subtraction is not associative since $(3 - 4) - 5 = -6 \neq 4 = 3 - (4 - 5)$ and so $(\mathbb{Z}, -)$ is not a group.

It will be helpful to get the following results out of the way once and for all.

Lemma 7.2. *(i) The unit of a group* $(G, *)$ *is unique, i.e., if* $e * a = a * e = a$ *and* $e' * a = a * e' = a$ *for all* $a \in G$*, then* $e = e'$.

(ii) The inverse of an element in a group $(G, *)$ *is unique, i.e., if* $b * a = a * b = e$ *and* $c * a = a * c = e$*, then* $b = c$.

Exercise 7.3. *If* $(G, *)$ *is a group and* a, $b \in G$ *then* $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 7.4. *If* $(G, *)$ *is a group and* $H \subseteq G$ *we say that* $(H, *)$ *is a subgroup of* $(G, *)$ *if*

(i) $e \in H$,

(ii) $x \in H$ *implies* $x^{-1} \in H$,

(iii) $x, y \in H$ *implies* $xy \in H$.

(Exercise 16.1 embroiders this a little bit further.)

Lemma 7.5. *If* $(H, *)$ *is a subgroup of* $(G, *)$ *then* $(H, *)$ *is a group.*

Clearly, any concrete group is an abstract group so we already have quite a collection of examples. Here are some more.

Example 7.6. *(i)* $(\mathbb{Z}, +)$ *is a group.*

(ii) $(\mathbb{R}^n, +)$ *with vector addition is a group.*

(iii) If we take $C_n = \{0, 1, 2, \dots, n-1\}$ *and take addition modulo* n*, then* $(C_n, +)$ *is a group (called the cyclic group of order* n*).*

(iv) If $(G, .)$ *and* $(H, .)$ *are groups, then we may define a new group* $(G \times H, .)$ *by*

$$(g_1, h_1).(g_2, h_2) = (g_1.g_2, h_1.h_2).$$

From now on we shall often refer to a group G rather than a group $(G, *)$. We shall usually write $ab = a * b$.

The example of matrix groups like $GL(\mathbb{R}^n)$ for $n \geq 2$ shows us that we cannot assume automatically that $a * b = b * a$.

Definition 7.7. *We say that* G *is a commutative (or an Abelian, or an abelian) group if*

$$g * h = h * g$$

for all $g, h \in G$.

Example 7.8. *(i)* $(\mathbb{Z}, +)$, $(\mathbb{R}^n, +)$, $(C_n, +)$ *and* $SO(\mathbb{R}^2)$ *are commutative.*

(ii) D_n *the group of symmetries of the regular* n*-gon* $[n \geq 3]$, $O(\mathbb{R}^2)$ *and* $SO(\mathbb{R}^3)$ *are non-commutative.*

(iii) If G *and* H *are commutative groups then* $G \times H$ *is commutative.*

We can already see the possibility that what is essentially the same group may turn up under different disguises. We deal with this by introducing the notion of isomorphism.

Definition 7.9. *If $(G, *)$ and $(H, .)$ are groups and $f : G \to H$ is a bijection such that*

$$f(x * y) = f(x).f(y)$$

for all x, $y \in G$ then we say that f is an isomorphism and that $(G, *)$ and $(H, .)$ are isomorphic.

The notion of isomorphism is closely linked with that of homomorphism (or 'group morphism').

Definition 7.10. *If $(G, *)$ and $(H, .)$ are groups and $f : G \to H$ is a map such that*

$$f(x * y) = f(x).f(y)$$

for all x, $y \in G$, then we say that f is a homomorphism.

The following result is trivial but worth noting.

Lemma 7.11. *Let $f : G \to H$ be a homomorphism.*
(i) If G has unit e_G and H unit e_H, then $f(e_G) = e_H$.
(ii) If $x \in G$, then $f(x)^{-1} = f(x^{-1})$.

Normally we write e for both e_G and e_H. Any reader who finds this confusing is free to continue using the unambiguous notation e_G and e_H.

We shall talk a bit about homomorphism later but, for the moment, we concentrate on isomorphism. Those members of my audience who are doing the Numbers and Sets course should note the following remark (the others may ignore it).

Lemma 7.12. *Let us write $G \equiv H$ if G and H are isomorphic. Then, if G, H and K are groups,*
(i) $G \equiv G$.
(ii) $G \equiv H$ implies $H \equiv G$.
(iii) If $G \equiv H$ and $H \equiv K$ then $G \equiv K$.
Thus, isomorphism is an equivalence relation.

Example 7.13. *(i) If G and H are groups, then $G \times H$ is isomorphic to $H \times G$.*
(ii) $C_2 \times C_2$ is not isomorphic to C_4.
(iii) $C_2 \times C_3$ is isomorphic to C_6.

(iv) The set $\mathbb{R} \setminus \{0\}$ *is a group under (ordinary) multiplication which is not isomorphic to* $(\mathbb{R}, +)$.

(v) The set $\{x \in \mathbb{R} : x > 0\}$ *is a group under (ordinary) multiplication which is isomorphic to* $(\mathbb{R}, +)$.

(vi) $S_n = S(\{1, 2, \ldots, n\})$ *is isomorphic to* $S(X)$ *if and only if* X *has* n *elements.*

(vii) S_3 *and* D_3 *are isomorphic.*

In general, to show two groups isomorphic, we look for a 'natural' map between them. To show they are not isomorphic, we look for a 'group property' possessed by one but not the other.

Example 7.14. *(i) The symmetry group of the regular tetrahedron is isomorphic to* S_4.

(ii) The symmetry group of the cube has 48 elements. The subgroup consisting of rotations alone is isomorphic to S_4. *The symmetry group of the cube is isomorphic to* $S_4 \times C_2$.

(iii) The symmetry group of the regular octahedron is isomorphic to the symmetry group of the cube.

The proof of the next result is simple but faintly Zen. (You may be relieved to note that the proof is not in the syllabus.)

Fact 7.15. (Cayley's Theorem.) *Every abstract group* G *is isomorphic to a concrete group (more specifically to a subgroup of* $S(G)$*).*

Thus the study of abstract and concrete groups comes to the same thing in the end.

If we think in terms of abstract groups rather than concrete groups, we have to restate what it means for a group G to act faithfully on a set X.

Definition 7.16. *Suppose* G *is a group and* X *a non-empty set. If there exists a map* $\theta : G \times X \to X$ *such that, writing* $gx = \theta(g, x)$, *we have*

(i) $g(hx) = (gh)x$ *for all* g, $h \in G$ *and* $x \in X$,

(ii) $ex = x$ *for all* $x \in X$,

we say that θ *is an action of* G *on* X, *or, more informally that* G *acts on* X.

Example 7.17. *(i) If* $\theta : \mathbb{Z} \times \mathbb{R} \to \mathbb{R}$ *is given by* $\theta(n, x) = n + x$ *then* θ *is an action of* $(\mathbb{Z}, +)$ *on* $\mathbb{R}$.

(ii) If $\phi : \mathbb{Z} \times \mathbb{R} \to \mathbb{R}$ *is given by* $\phi(n, x) = 2n + x$ *then* ϕ *is an action of* $(\mathbb{Z}, +)$ *on* $\mathbb{R}$.

Exercise 7.18. *If* G *acts on* X *show that, if* $g \in G$, *the map* $x \mapsto gx$ *is a bijection.*

Definition 7.19. *Suppose G is a group acting on a non-empty set X. We say that G acts faithfully on X if the only element g of G with the property $gx = x$ for all $x \in X$ is e itself.*

More compactly 'G acts faithfully on X if and only if the relation $gx = x$ for all $x \in X$ implies $g = e$'.

Exercise 7.20. *Give an example of a group G acting on a set X which does not act faithfully.*

The syllabus only demands that you know Definition 7.16. Example 10.7 sheds some more light on what is going on.

It should be noted that, for any but the smallest groups, checking the associative law on a case by case basis is essentially impossible. Thus the usual way to show that something is a group is to show that it is a subgroup of some other group and often this means showing that it is (isomorphic to) a concrete group. More generally the easiest way to study a particular group is often via some isomorphic concrete group. On the other hand, the general properties common to many groups are frequently best approached by using abstract group theory.

We end with a simple but genuine theorem.

Definition 7.21. *We say that G is cyclic if there exists an $a \in G$ such that every element of G has the form a^r for some integer r.*

Theorem 7.22. *Every cyclic group is isomorphic to $(\mathbb{Z}, +)$ or to C_n for some $n \geq 1$.*

8 Orbits and suchlike

We now return to groups as objects that act on sets.

Definition 8.1. *Suppose G is a group acting on a set X.*

(i) If $x \in X$, the orbit $\mathrm{Orb}(x)$ *of x under G is defined by*

$$\mathrm{Orb}(x) = \{gx : g \in G\}.$$

(ii) If $x \in X$, the stabiliser $\mathrm{Stab}(x)$ *of x is defined by*

$$\mathrm{Stab}(x) = \{g : gx = x\}.$$

We use the following notation in the next lemma and elsewhere.

Definition 8.2. *If F is a finite set we write $|F|$ for the number of elements of F.*

Lemma 8.3. *Suppose G is a group acting on a set X.*

(i) $\bigcup_{x\in X} \operatorname{Orb}(x) = X$.

(ii) If $x, y \in X$, then either $\operatorname{Orb}(x) \cap \operatorname{Orb}(y) = \varnothing$ or $\operatorname{Orb}(x) = \operatorname{Orb}(y)$.

(iii) If X is finite and the distinct orbits under G are $\operatorname{Orb}(x_1)$, $\operatorname{Orb}(x_2)$, ..., $\operatorname{Orb}(x_m)$, then

$$|X| = |\operatorname{Orb}(x_1)| + |\operatorname{Orb}(x_2)| + \cdots + |\operatorname{Orb}(x_m)|.$$

Those students doing the Numbers and Sets course will recognise that Lemma 8.3 could be proved by showing that the relation

$$x \equiv y \text{ if } y \in \operatorname{Orb}(x)$$

is an equivalence relation, but I shall prove it directly.

Lemma 8.4. *If G is a group acting on a set X and $x \in X$ then $\operatorname{Stab}(x)$ is a subgroup of G.*

Example 8.5. *Consider the group $SO(\mathbb{R}^3)$ acting on $\mathbb{R}^3$. If $\mathbf{x} \in \mathbb{R}^3$, then*

$$\operatorname{Orb}(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^3 : ||\mathbf{y}|| = ||\mathbf{x}||\},$$

the sphere with radius $||\mathbf{x}||$ and centre $\mathbf{0}$.

If $\mathbf{x} \neq \mathbf{0}$, then the stabiliser of $\mathbf{x}$ is the subgroup of rotations about an axis through $\mathbf{x}$ and $\mathbf{0}$. The stabiliser of $\mathbf{0}$ is the full group $SO(\mathbb{R}^3)$.

If G is a group and H is a subgroup of G, then H acts on G by the map $(h, g) \mapsto hg$. The orbit of an $x \in G$ is given a special name.

Definition 8.6. *If H is a subgroup of a group G and $x \in G$, we write*

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

and call Hx a right coset of H. The left coset xH is defined similarly[9].

Example 8.7. *Consider D_3 the group of symmetries of an equilateral triangle. If H is a subgroup $\{\iota, \rho\}$ with ρ a reflection and σ is a non-trivial rotation, then $H\sigma \neq \sigma H$.*

[9]The reader is warned that some mathematicians reverse this convention and call xH a left coset.

We constantly make use of simple remarks of the type illustrated in the next lemma.

Lemma 8.8. *If H is a subgroup of a group G and $a, b \in G$, then the following three statements are equivalent.*
(i) $aH = bH$,
(ii) $b^{-1}a \in H$,
(iii) $b^{-1}aH = H$.

Expressions of the type PAP^{-1} occur throughout mathematics. In the context of group theory we talk of conjugation.

Definition 8.9. *(i) If G is a group and and $x, y \in G$, we say that x and y are conjugate if there exists an $a \in G$ such that*

$$x = aya^{-1}.$$

(ii) If G is a group and and H and K are subgroups, we say that H and K are conjugate if there exists an $a \in G$ such that

$$H = aKa^{-1}.$$

or, more formally,

$$H = \{aka^{-1} : k \in K\}.$$

Definition 8.9 (ii) is supplemented by the following easy observation.

Lemma 8.10. *If G is a group, $a \in G$ and K a subgroup, then aKa^{-1} is a subgroup.*

The following remarks are easy but useful.

Lemma 8.11. *(i) If we consider conjugacy of elements of a group G and write $x \equiv y$ whenever x and y are conjugate then*
(a) $x \equiv x$,
(b) $x \equiv y$ *implies* $y \equiv x$,
(c) If $x \equiv y$ *and* $y \equiv z$, *then* $x \equiv z$.
(ii) Similar results hold if we consider conjugacy of subgroups of a group G.

Example 8.12. *If G is a group acting on a set X then points in the same orbit have conjugate stabilisers.*

9 Lagrange's theorem

Algebraists call the number of elements in a finite group G the order of G. The following theorem can be proved using the language of orbits but, in view of its importance, I shall give a self contained proof.

Theorem 9.1. (Lagrange's Theorem.) *If G is finite group and H a subgroup, then the order of H divides the order of G.*

The proof of this theorem is book-work and frequently asked for in exams. Example 12.14 gives an example of a group of order 12 with no subgroup of order 6.

The next result (the 'orbit-stabiliser theorem') is also an old examination favourite.

Theorem 9.2. *Suppose that G is a group acting on a set X and that $x \in X$.*

(i) There is a bijection between $\operatorname{Orb}(x)$ and the left cosets of $\operatorname{Stab} x$.

(ii) If G is finite, then $|\operatorname{Orb}(x)| = |G|/|\operatorname{Stab} x|$.

(iii) If G is finite, then the number of elements in $\operatorname{Orb}(x)$ divides the order of G.

Exercise 9.3. *(i) Verify the orbit-stabiliser theorem for the full group of isometries of the cube.*

(ii) Let X be a regular 6-gon with centre O and one vertex A. Consider the group G of symmetries of X generated by rotation through $2\pi/3$ about O and reflection in the line OA. Verify the orbit-stabiliser theorem for G acting on X.

Definition 9.4. *If $a \in G$ a group, then*

(i) If $a = e$, we say a has order 1.

(ii) If $a \neq e$ and there exists an $r \neq 0$ such that $a^r = e$, we say that a has order

$$\min\{r > 0 : a^r = e\}.$$

(iii) If the equation $a^r = e$ has no solution with $r \neq 0$, we say that a has infinite order.

Theorem 9.5. *If G is finite group then the order of any $a \in G$ divides the order of G. In particular, $a^{|G|} = e$.*

Note that $C_2 \times C_2 \times C_2$ has order 8 but contains no elements of order 4.

Lemma 9.6. *If p is a prime, all groups of order p are isomorphic to C_p.*

Anyone who believes that the study of finite commutative groups is trivial should test their belief against the next collection of groups.

Definition 9.7. *We define $(R_n, .)$ to be the set of integers r with $1 \leq r \leq n$ and r coprime to n with multiplication modulo n. We write $\phi(n) = |R_n|$. (We call ϕ Euler's totient function.)*

It is not even trivial to show that R_n is indeed a group. We shall use the following result (proved as a consequence of Euclid's Algorithm in the Numbers and Sets course for those of my audience who attend that course) without proof.

Fact 9.8. *If integers n and m are coprime, then there exist a and b integers such that $an + bm = 1$.*

Lemma 9.9. *$(R_n, .)$ is a commutative group.*

Example 9.10. (Euler-Fermat Theorem.) *If r and n are coprime, then*

$$r^{\phi(n)} \equiv 1 \mod n.$$

Example 9.11. (Fermat's Little Theorem.) *If p is a prime and $1 \leq r \leq p-1$, then*

$$r^{p-1} \equiv 1 \mod p.$$

Example 9.13, below, is not important in itself (indeed if time presses I shall omit it) but provides useful revision of much of our discussion of abstract finite groups. We need a preliminary remark.

Lemma 9.12. *If G is a group in which every element has order 1 or 2 then G is the product of cyclic groups of order 2.*

Example 9.13. *Up to isomorphism the only groups of order 8 or less are*
(i) $\{e\}$ (isomorphic to S_1 and C_1),
(ii) C_2,
(iii) C_3,
(iv) C_4, $C_2 \times C_2$ (isomorphic to the symmetry group of the rectangle),
(v) C_5,
(vi) $C_2 \times C_3$ (isomorphic to $C_3 \times C_2$ and C_6), D_3 (isomorphic to S_3),
(vii) C_7
(viii) C_8, $C_2 \times C_4$ (isomorphic to $C_4 \times C_2$), $C_2 \times C_2 \times C_2$, D_4 and possibly a further group Q.
All these groups are non-isomorphic unless specified otherwise.

Our next task is to satisfy ourselves that the putative group Q does in fact exist.

Example 9.14. *Consider the* 2×2 *matrices*

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

together with I, $-I$, $-\mathbf{i}$, $-\mathbf{j}$ *and* $-\mathbf{k}$. *The set*

$$Q = \{I, -I, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$$

forms a subgroup Q *of* $GL(\mathbb{C}^2)$ *of order 8 with*

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I, \ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \ \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Example 9.15. *Continuing with the notation of the previous example, let us consider the collection* $\mathcal{Q}$ *of matrices*

$$\mathbf{x} = x_0 I + x_1 \mathbf{i} + x_2 \mathbf{j} + x_3 \mathbf{k}.$$

If we add or multiply matrices in $\mathcal{Q}$ *we obtain matrices in* $\mathcal{Q}$. *Further, if we write*

$$\mathbf{x}^* = x_0 I - x_1 \mathbf{i} - x_2 \mathbf{j} - x_3 \mathbf{k},$$

then

$$\mathbf{x}\mathbf{x}^* = \mathbf{x}^*\mathbf{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2 = ||\mathbf{x}||^2, \textit{say},$$

and so, if $\mathbf{x} \neq \mathbf{0}$, *we may set* $\mathbf{x}^{-1} = ||\mathbf{x}||^{-2}\mathbf{x}^*$ *and obtain*

$$\mathbf{x}^{-1}\mathbf{x} = \mathbf{x}\mathbf{x}^{-1} = I.$$

Thus we obtain the system $\mathcal{Q}$ of Hamilton's quaternions which behaves much like $\mathbb{R}$ and $\mathbb{C}$ although multiplication is not commutative ($\mathbf{ij} \neq \mathbf{ji}$). The quaternions form a fascinating system but further discussion would take us too far afield.

10 A brief look at quotient groups

The notion of a quotient group (like the notion of quotients in general) is extremely useful but also fairly subtle.

If we consider a group G with a subgroup H, then it is natural to try and put a group structure on the collection of left cosets gH. The 'natural definition' is to write $g_1H.g_2H = g_1g_2H$. BUT THIS DOES NOT ALWAYS WORK.

Theorem 10.1. *Let G be a group and H a subgroup of G. The following two statements are equivalent*

(i) $g_1H = g_1'H,\ g_2H = g_2'H\ \Rightarrow g_1g_2H = g_1'g_2'H$,

(ii) $ghg^{-1} \in H$ *whenever* $g \in G,\ h \in H$.

In view of this, we make the following definitions.

Definition 10.2. *If H is a subgroup of a group G we say that H is* normal *if $ghg^{-1} \in H$ whenever $g \in G$, $h \in H$.*

This is sometimes restated as 'H is normal if $gHg^{-1} \subseteq H$ for all $g \in G$' or (using the next lemma) 'H is normal if the only subgroup conjugate to H is H itself'.

Lemma 10.3. *Let H is a subgroup of a group G. Then H is normal if and only if $gH = Hg$ for all $g \in G$.*

Since left and right cosets agree for H normal, we shall refer, in this case, to 'cosets' rather than left cosets.

Definition 10.4. *If H is a normal subgroup of a group G, the set G/H of cosets gH with multiplication defined by $g_1H.g_2H = g_1g_2H$ is called a quotient group.*

Theorem 10.5. *Quotient groups are groups.*

I reiterate the warning above:

QUOTIENT GROUPS EXIST ONLY FOR NORMAL SUBGROUPS.

Example 10.6. *(i) Subgroups of Abelian groups are always normal.*

(ii) If D_3 is the symmetry group of the equilateral triangle, then no subgroup of order 2 is normal.

(iii) If H is a subgroup of the finite group G and $|H| = |G|/2$, then H is normal in G.

Here is a natural example of the use of quotient groups.

Example 10.7. *Suppose that G is a group acting on a non-empty set X and we write*

$$H = \{g \in G : gx = x \text{ for all } x \in X\}.$$

Then H is a normal subgroup of G and, if we take

$$(gH)x = gx,$$

then G/H acts faithfully on X.

Quotient groups and homomorphisms are intimately linked.

Definition 10.8. *If $\theta : G \to H$ is a homomorphism we define the image $\theta(G)$ of θ by*

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

and the kernel $\ker(\theta)$ *of θ by*

$$\ker(\theta) = \theta^{-1}(e) = \{g \in G : \theta(g) = e\}.$$

Lemma 10.9. *Let $\theta : G \to H$ be a homomorphism.*

(i) $\theta(G)$ is a subgroup of H.

(ii) $\ker(\theta)$ *is a subgroup of G.*

(iii) $\ker(\theta)$ *is a normal subgroup of G.*

(iv) The equation $\theta(g) = h$ with $h \in H$ has a solution in G if and only if $h \in \theta(G)$.

(v) If $g_1 \in G$ is a solution of $\theta(g) = h$ with $h \in H$, then $g_2 \in G$ is a solution if and only if $g_2 \in g_1 \ker(\theta)$.

Theorem 10.10. (The isomorphism theorem.) *If $\theta : G \to H$ is a homomorphism, then $G/\ker\theta$ is isomorphic to $\theta(G)$.*

Example 10.11. *(i) Consider the additive group $(\mathbb{Z}, +)$ and the cyclic group $(C_n, .)$ generated by a, say. If $\theta : \mathbb{Z} \to C_n$ is given by*

$$\theta(r) = a^r,$$

then θ is a homomorphism,

$$\ker(\theta) = \{r : r \equiv 0 \mod n\} = n\mathbb{Z} \text{ and } \theta(\mathbb{Z}) = C_n.$$

Thus $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to C_n.

(ii) Consider D_3 generated by a and b with $a^3 = e$, $b^2 = e$ and $ba = a^{-1}b$ and the cyclic group C_2 generated by c with $c^2 = e$. If we set

$$\theta(a^r b^s) = c^s,$$

then $\theta : D_3 \to C_2$ is a homomorphism, $\theta(D_3) = C_2$ and $\ker(\theta)$ *is isomorphic to C_3.*

(iii) Consider the cyclic group C_6 generated by a with $a^6 = e$, and the cyclic group C_2 generated by c with $c^2 = e$. If we set

$$\theta(a^r) = c^r,$$

then $\theta : C_6 \to C_2$ is a homomorphism, $\theta(C_6) = C_2$ and $\ker(\theta)$ *is isomorphic to C_3.*

(iv) If p and q are distinct primes, then the only homomorphism $\theta : C_p \to C_q$ is the trivial map $\theta(g) = e$ for all $g \in C_p$.

Notice that every normal subgroup can be obtained a kernel.

Example 10.12. *If H is a normal subgroup of a group G, then the map $\theta : G \to G/H$ given by*

$$\theta(g) = gH$$

is a homomorphism with kernel H.

11 The Möbius group

At the beginning of the course you briefly looked at the Möbius map $\tilde{T}$

$$\tilde{T}(z) = \frac{az+b}{cz+d},$$

where $ad - bc \neq 0$. This is 'almost a well defined bijective map on $\mathbb{C}$' but, if $c \neq 0$, there are two problems. The first is that $\tilde{T}(-d/c)$ is not defined and the second is that there is no $w \in \mathbb{C}$ with $\tilde{T}(w) = a/c$. We get round this by adding a new point ∞ ('the point at infinity' in old fashioned language) to $\mathbb{C}$.

Definition 11.1. *If $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$ we define the Möbius map T which will be written informally as*

$$T(z) = \frac{az+b}{cz+d}$$

by the following formal rules.

(i) If $c \neq 0$, then

$$\begin{aligned} T(z) &= \frac{az+b}{cz+d} \qquad \textit{when } z \in \mathbb{C} \setminus \{-d/c\}, \\ T(-d/c) &= \infty, \\ T(\infty) &= a/c. \end{aligned}$$

(ii) If $c = 0$, then

$$\begin{aligned} T(z) &= \frac{az+b}{cz+d} \qquad \textit{when } z \in \mathbb{C}, \\ T(\infty) &= \infty. \end{aligned}$$

Henceforward, when we talk about a Möbius map we shall use this definition. Möbius maps will reappear in geometry courses and play an important rôle throughout complex variable theory. The following result will be the key to our treatment of Möbius maps.

Lemma 11.2. *Every Möbius map is the composition of Möbius maps of the following three forms* $[\alpha, \lambda \in \mathbb{C},\ \lambda \neq 0]$

$$\begin{aligned} S_1(z) &= z + \alpha && \textit{(Translation)},\\ S_2(z) &= \lambda z && \textit{(Rotation and dilation)},\\ S_3(z) &= \frac{1}{z}. \end{aligned}$$

Theorem 11.3. *The collection* $\mathcal{M}$ *of Möbius maps forms a group acting on* $\mathbb{C} \cup \{\infty\}$.

Lemma 11.4. *The general equation of a circle or straight line in* $\mathbb{C}$ *is*

$$Azz^* + Bz^* + B^*z + C = 0$$

with A *and* C *real and* $|B|^2 > AC$. *We have a straight line if and only if* $A = 0$. *We have a locus through* 0 *(i.e. the set defined by our equation contains* 0*) if and only if* $C = 0$.

Theorem 11.5. *The Möbius transform* T *given by* $Tz = z^{-1}$ *takes circles and straight lines to circles and straight lines. Any straight line is taken to a circle or straight line through* 0. *Any circle or straight line through* 0 *is taken to a straight line.*

Theorem 11.6. *Möbius transforms take circles and straight lines to circles and straight lines.*

Example 11.7. (Inversion.) *(i) If* $k > 0$, *the map* $T : \mathbb{R}^2 \cup \{\infty\} \to \mathbb{R}^2 \cup \{\infty\}$ *given, in polars, by* $T(r, \theta) = (kr^{-1}, \theta)$ *for* $r \neq 0$, $T\mathbf{0} = \infty$, $T\infty = \mathbf{0}$ *takes circles and straight lines to circles and straight lines.*

(ii) If $k > 0$, *the map* $T : \mathbb{R}^3 \cup \{\infty\} \to \mathbb{R}^3 \cup \{\infty\}$ *given by* $T\mathbf{r} = kr^{-2}\mathbf{r}$ *for* $\mathbf{r} \neq \mathbf{0}$, $T\mathbf{0} = \infty$, $T\infty = \mathbf{0}$ *takes spheres and planes to spheres and planes.*

Example 11.8. (Peaucellier's Inversor.) *Consider a set of jointed rods with* OB, OD *of equal length and* AB, BC, CD, DA *of equal length. If* O *is a fixed point but the rest of the framework is free to move in a plane then, if* A *describes part of a circle through* O, C *will describe part of a straight line.*

Definition 11.9. *If* z_1, z_2, z_3 *and* z_4 *are distinct complex numbers, we write*

$$[z_1, z_2, z_3, z_4] = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_4 - z_3)(z_2 - z_1)}.$$

and call $[z_1, z_2, z_3, z_4]$ *the cross ratio of* z_1, z_2, z_3 *and* z_4.

As might be expected, different authors permute the suffices in different ways so you should always state which definition you use[10]. (All the theorems remain unaltered whichever definition is used.)

Theorem 11.10. *(i) Cross ratio is unaltered by Möbius transformation. Thus, if z_1, z_2, z_3 and z_4 are distinct complex numbers and T is a Möbius transform,*

$$[Tz_1, Tz_2, Tz_3, Tz_4] = [z_1, z_2, z_3, z_4].$$

(ii) If T is a Möbius map with $T0 = 0$, $T1 = 1$ and $T\infty = \infty$, then $T = I$.

(iii) If z_1, z_2 and z_3 are distinct complex numbers, then there exists a unique Möbius transform T such that

$$Tz_1 = 0,\ Tz_2 = 1,\ Tz_3 = \infty.$$

(iv) If z_1, z_2 and z_3 are distinct complex numbers and w_1, w_2 and w_3 are distinct complex numbers, then there exists a unique Möbius transform T such that

$$Tz_1 = w_1,\ Tz_2 = w_2,\ Tz_3 = w_3.$$

Example 11.11. *The distinct complex numbers z_1, z_2, z_3 and z_4 lie on a circle (or straight line) if and only if their cross ratio $[z_1, z_2, z_3, z_4]$ is real.*

Note that this gives us an alternative proof of Theorem 11.6[11].

It is interesting to apply some of our general ideas on groups to the specific group $\mathcal{M}$.

Lemma 11.12. *The collection $GL(\mathbb{C}^n)$ of invertible $n \times n$ complex matrices forms a group under matrix multiplication. The set*

$$SL(\mathbb{C}^n) = \{A \in GL(\mathbb{C}^n) : \det A = 1\}$$

is a subgroup.

Lemma 11.13. *(i) The map $\theta : GL(\mathbb{C}^2) \to \mathcal{M}$ given by*

$$\theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az+b}{cz+d}$$

[10] The particular choice we made has the property that, if we write, $Tw = [z_1, z_2, z_3, w]$ then $Tz_1 = 0$, $Tz_2 = 1$ and $Tz_3 = \infty$.

[11] To avoid circularity we have to give an alternative proof of Example 11.11. One way of obtaining such a proof is to use the fact that (provided we choose their sign appropriately) angles on the same chord of a circle are equal modulo π.

is a surjective homomorphism with kernel the subgroup

$$\{\lambda I : \lambda \in \mathbb{C},\ \lambda \neq 0\}.$$

(ii) The map $\theta : SL(\mathbb{C}^2) \to \mathcal{M}$ given by

$$\theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az+b}{cz+d}$$

is a surjective homomorphism with kernel the subgroup $\{I, -I\}$.

We note that a simple modification of Theorem 3.4 gives the following lemma.

Lemma 11.14. *If $A \in SL(\mathbb{C}^2)$, then exactly one of the following three things must happen.*

(i) We can find $P \in SL(\mathbb{C}^2)$ such that

$$P^{-1}AP = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

for some $\lambda \in \mathbb{C}$ with $\lambda \neq 1, -1, 0$.

(ii) $A = \pm I$.

(iii) We can find $P \in SL(\mathbb{C}^2)$ such that

$$P^{-1}AP = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

with $\lambda = \pm 1$.

Using Lemma 11.13 (ii) this gives us the following result on Möbius maps.

Lemma 11.15. *If $T \in \mathcal{M}$, then one of the following three things must happen.*

(i) T is conjugate to a map S of the form $Sz = \mu z$ (i.e., a rotation and dilation) with $\mu \neq 1$.

(ii) $T = \iota$ (i.e., $Tz = z$ for all z).

(iii) T is conjugate to the map S given by $Sz = z \pm 1$ (a translation).

Note that we seperate (i) and (ii) because T behaves very differently in the two cases. In Lemma 11.17 we see that the two maps $Sz = z \pm 1$ are, in fact, conjugate.

We say that a map $F : X \to X$ has $x \in X$ as a fixed point if $f(x) = x$.

Lemma 11.16. *If $T \in \mathcal{M}$, then $T = \iota$ or T has one or two fixed points.*

If we are interested in the behaviour of $T^n z$, then (by conjugating with the Möbius map S given by $Sz = 1/z$ in (i) and by a similar trick in (iii)) we can obtain a slightly more refined version of Lemma 11.15.

Lemma 11.17. *If $T \in \mathcal{M}$ then one of the following four things must happen.*

(ia) T is conjugate to a map S of the form $Sz = \mu z$ with $|\mu| > 1$.

(ib) T is conjugate to a map S of the form $Sz = \mu z$ with $|\mu| = 1$ (pure rotation) with $\mu \neq 1$.

(ii) $T = \iota$ (i.e., $Tz = z$ for all z).

(iii) T is conjugate to the map S given by $Sz = z + 1$ (a translation).

Thus, given a $T \in \mathcal{M}$, we can find $Q \in \mathcal{M}$ such that $S = QTQ^{-1}$ takes one of the simple forms above. Since

$$T^n z = Q^{-1}(S^n(Q(z))),$$

study of $S^n w$ with $w = Q(z)$ tells us about $T^n z$.

Exercise 18.17 outlines a direct proof of Lemma 11.17 which does not depend on looking at $SL(\mathbb{C}^2)$.

12 Permutation groups

We now return to the study of the finite permutation group

$$S_n = S(\{1, 2, \ldots, n\}),$$

Definition 12.1. *If $\sigma \in S_n$ has the property that there exist distinct $a_1, a_2, \ldots, a_m$ such that*

$$\begin{aligned} \sigma(a_j) &= a_{j+1} \qquad [1 \leq j \leq m-1], \\ \sigma(a_m) &= a_1, \\ \sigma(x) &= x \qquad \textit{if } x \notin \{a_1, a_2, \ldots, a_m\}, \end{aligned}$$

we say that σ is a cycle of length m and write

$$\sigma = (a_1 a_2 \ldots a_m).$$

If $\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, b_p\} = \varnothing$ we say that the cycles $(a_1 a_2 \ldots a_m)$ and $(b_1 b_2 \ldots b_p)$ are disjoint.

Lemma 12.2. *(i) $(a_1 a_2 \ldots a_m) = (a_m a_1 \ldots a_{m-1}) = (a_{m-1} a_m \ldots a_{m-2}) = \ldots$ (i.e., cycles can be cycled).*

(ii) If σ and τ are disjoint cycles then $\sigma\tau = \tau\sigma$ (i.e., disjoint cycles commute).

(iii) $(a) = \iota$ for all $a \in \{1, 2, \ldots, n\}$.

Theorem 12.3. *Every $\sigma \in S_n$ can be written as the product of disjoint cycles. The representation is unique subject to the variations allowed by Lemma 12.2.*

Example 12.4. *(i) If σ is the product of disjoint cycles of length n_1, n_2, $\dots$, n_k, then σ has order $\operatorname{lcm}(n_1, n_2, \dots, n_k)$.*

(ii) If a pack of N cards is repeatedly shuffled using exactly the same shuffle, then the pack will return to its initial state after at most

$$\max\{\operatorname{lcm}(n_1, n_2, \dots, n_k) : n_1 + n_2 + \dots + n_k = N\}$$

shuffles.

The following results are very useful in later work (but experience shows that by the time the results are needed they will have been forgotten and need to be painfully relearned).

Lemma 12.5. *(i) If $\sigma \in S_n$, then*

$$\sigma(a_1 a_2 \dots a_m)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\dots\sigma(a_m)).$$

(ii) If the $(a_{1j}a_{2j}\dots a_{m(j)j})$ are disjoint cycles and $\sigma \in S_n$, then

$$\sigma\left(\prod_{j=1}^{s}(a_{1j}a_{2j}\dots a_{m(j)j})\right)\sigma^{-1} = \prod_{j=1}^{s}(\sigma(a_{1j})\sigma(a_{2j})\dots\sigma(a_{m(j)j}))$$

(iii) Two elements of S_n are conjugate if and only if they are the product of the same number of disjoint cycles of each length (have the same 'cycle type').

When thinking about results like (iii) we must be careful to treat cycles of length 1 consistently.

The next lemma is obvious. We refer to cycles of length 2 as transpositions.

Lemma 12.6. *Every $\sigma \in S_n$ is the product of transpositions.*

What is much less obvious is the next result.

Lemma 12.7. *The product of an even number of transpositions cannot be written as the product of an odd number of transpositions and vice versa.*

We obtain this result as the consequence of an equivalent statement.

Theorem 12.8. (Existence of Signature.) *(i) If $n \geq 2$ there exists a non-trivial homomorphism ζ from S_n to the multiplicative group $(\{-1,1\},\times)$.*

(ii) There is only one non-trivial homomorphism ζ from S_n to the multiplicative group $(\{-1,1\},\times)$ $[n \geq 2]$. If σ is the product of m transpositions, then $\zeta(\sigma) = (-1)^m$.

(Exercise 18.18 sheds some light on our proof of Theorem 12.8.) We call the ζ of Theorem 12.8 the signature. It will be used in the treatment of the determinant in the linear algebra course and in the treatment of alternating forms in later algebra. The signature also appears (via the alternating group A_n defined below in Definition 12.11) in the discussion of the symmetry groups of regular polyhedra in later geometry courses and in Galois Theory.

The following example, which is emphatically outside the schedules, shows that the existence of a signature is not obvious.

Example 12.9. *Suppose $\theta : S(\mathbb{Z}) \to \{-1,1\}$ is a homomorphism. Extending our notation from the finite case, suppose that*

$$\sigma = (12)(34)(56)\dots$$

and that τ is the shift map given by $\tau(j) = j+1$ for all $j \in \mathbb{Z}$.

(i) $\tau^2\sigma\tau^{-2} = (34)(56)(78)\dots$.

(ii) $\sigma\tau^2\sigma\tau^{-2} = (12)$.

(iii) $\theta((12)) = 1$.

(iv) If μ is the product of a finite number of cycles of finite length then $\theta(\mu) = 1$.

Computation of signatures is made easy by the following observation.

Lemma 12.10. *(i) $(a_1a_{m+1})(a_1a_2\dots a_m) = (a_1a_2\dots a_ma_{m+1})$.*

(ii) A cycle of length k has signature $(-1)^{k+1}$.

Definition 12.11. *If $n \geq 2$ and $\zeta : S_n \to \{-1,1\}$ is the signature, we write $A_n = \ker(\zeta)$ and call A_n the alternating group.*

Lemma 12.12. *(i) S_n has order $n!$.*

(ii) A_n is a normal subgroup of S_n. S_n/A_n is isomorphic to C_2.

(iii) A_n has order $n!/2$.

Exercise 12.13. *Use the orbit-stabiliser theorem to prove that S_n has order $n!$ and A_n has order $n!/2$.*

The following result is interesting in itself and will give us some practice in working with A_n.

Example 12.14. *A_4 has order 12 but has no subgroup of order 6.*

13 Trailers

(The contents of this section are not part of the course and I will not lecture on them unless there is time at the end.)

One of the main topics in my treatment of this course was the subject of distance preserving linear maps, that is linear maps $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ such that if $\alpha\mathbf{x} = \mathbf{x}'$ then

$$x_1^2 + x_2^2 + \cdots + x_n^2 = x_1'^2 + x_2'^2 + \cdots + x_n'^2.$$

In Einstein's Special Theory of Relativity, which is the subject of a course in the third term, particular interest is attached to those linear maps on $\mathbb{R}^3 \times \mathbb{R}$ (that is 'space-time') which leave

$$x^2 + y^2 + z^2 - (ct)^2$$

unchanged. Normalising and generalising, this suggests that we should study the linear maps $\alpha : \mathbb{R}^n \to \mathbb{R}^n$ such that if $\alpha\mathbf{x} = \mathbf{x}'$, then

$$\begin{aligned} &x_1^2 + x_2^2 + \cdots + x_m^2 - x_{m+1}^2 - x_{m+2}^2 - \cdots - x_n^2 \\ &\qquad = x_1'^2 + x_2'^2 + \cdots + x_m'^2 - x_{m+1}'^2 - x_{m+2}'^2 - \cdots - x_n'^2. \end{aligned}$$

This is too much of a challenge for the moment (it will be easier after next year's linear algebra course) so we study the simplest case.

Example 13.1. *The collection $\mathcal{L}$ of linear maps $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ such that, if $\alpha\mathbf{x} = \mathbf{x}'$, then*

$$x_1^2 - x_2^2 = x_1'^2 - x_2'^2$$

forms a group $\mathcal{L}$. If we write $\mathcal{L}_0$ for the set of linear maps $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ which have matrix

$$\begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix},$$

with respect to the standard basis then:

(i) $\mathcal{L}_0$ is a subgroup of $\mathcal{L}$.

(ii) $\mathcal{L}$ is the union of the four disjoint cosets $E_j\mathcal{L}_0$ with

$$E_1 = I,\ E_2 = -I,\ E_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ E_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(iii) $\mathcal{L}_0$ is normal.

(iv) $\mathcal{L}_0$ is isomorphic to $(\mathbb{R}, +)$.

(v) $\{E_j : 1 \le j \le 4\}$ is a subgroup of $\mathcal{L}$ isomorphic to $C_2 \times C_2$ but $\mathcal{L}$ is not commutative and so, in particular, not isomorphic to $C_2 \times C_2 \times \mathbb{R}$.

Groups like $\mathcal{L}$ are called Lorentz groups after the great Dutch physicist who first formulated the transformation rules which underlie the Special Theory of Relativity.

Next year's linear algebra course contain generalisations of the notions of orthogonal and symmetric matrices and maps from the real to the complex case. When people become algebraists they have to swear a terrible oath never to reveal that their subject has applications to other parts of mathematics and the linear algebra course has been designed with this in mind. However the generalisations are used in classical and, particularly, in modern physics.

We start by defining an inner product on $\mathbb{C}^n$ by

$$\langle \mathbf{z}, \mathbf{w} \rangle = \sum_{r=1}^{n} z_r w_r^*.$$

Lemma 13.2. *If* $\mathbf{z}, \mathbf{w}, \mathbf{u} \in \mathbb{C}^n$ *and* $\lambda \in \mathbb{C}$, *then*

(i) $\langle \mathbf{z}, \mathbf{z} \rangle$ *is always real and positive.*

(ii) $\langle \mathbf{z}, \mathbf{z} \rangle = 0$ *if and only if* $\mathbf{z} = \mathbf{0}$.

(iii) $\langle \lambda\mathbf{z}, \mathbf{w} \rangle = \lambda\langle \mathbf{z}, \mathbf{w} \rangle$.

(iv) $\langle \mathbf{z} + \mathbf{u}, \mathbf{w} \rangle = \langle \mathbf{z}, \mathbf{w} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$.

(v) $\langle \mathbf{w}, \mathbf{z} \rangle = \langle \mathbf{z}, \mathbf{w} \rangle^*$.

Rule (v) is a warning that we must tread carefully with our new complex inner product and not expect it to behave quite as simply as the old real inner product. However, it turns out that

$$||\mathbf{z}|| = \langle \mathbf{z}, \mathbf{z} \rangle^{1/2}$$

behaves just as we wish it to behave. (This is not really surprising, if we write $z_r = x_r + iy_r$ with x_r and y_r real, we get

$$||\mathbf{z}||^2 = \sum_{r=1}^{n} x_r^2 + \sum_{r=1}^{n} y_r^2$$

which is clearly well behaved.)

We can take over Definition 4.2 and Lemma 4.3 directly.

Definition 13.3. *(i) We say that* $\mathbf{a}$ *and* $\mathbf{b}$ *are orthogonal if* $\langle \mathbf{a}, \mathbf{b} \rangle = 0$.

(ii) We say that $\mathbf{e}_1$, $\mathbf{e}_2$, $\dots$, $\mathbf{e}_n$ *are orthonormal if*

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}$$

for all $1 \leq i, j \leq n$.

Lemma 13.4. *Any system of n orthonormal vectors $\mathbf{e}_1$, $\mathbf{e}_2$, …, $\mathbf{e}_n$ forms a basis for $\mathbb{C}^n$. (We call this an orthonormal basis.) If $\mathbf{x} \in \mathbb{C}^n$, then*

$$\mathbf{x} = \sum_{r=1}^{n} \langle \mathbf{x}, \mathbf{e}_r \rangle \mathbf{e}_r.$$

If we now ask which linear maps preserve our new distance, we get results and definitions which parallel the sequence from Lemma 4.5 to Lemma 4.10.

Lemma 13.5. *If $\mathbf{a}$, $\mathbf{b} \in \mathbb{C}^n$, then*

$$||\mathbf{a}+\mathbf{b}||^2 - ||\mathbf{a}-\mathbf{b}||^2 + i||\mathbf{a}+i\mathbf{b}||^2 - i||\mathbf{a}-i\mathbf{b}||^2 = 4\langle \mathbf{a}, \mathbf{b} \rangle.$$

Definition 13.6. *If A is the $n \times n$ complex matrix (a_{ij}), then A^* (the adjoint of A) is the $n \times n$ matrix (b_{ij}) with $b_{ij} = a_{ji}^*$ $[1 \leq i, j \leq n]$.*

Theorem 13.7. *Let $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ be linear. The following statements are equivalent.*

(i) $||\alpha \mathbf{x}|| = ||\mathbf{x}||$ for all $\mathbf{x} \in \mathbb{C}^n$.

(ii) $\langle \alpha \mathbf{x}, \alpha \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$.

(iii) If α has matrix A with respect to some orthonormal basis, then $AA^* = I$.

A complex $n \times n$ matrix A with $AA^* = I$ is called a unitary matrix.

If we think of the linear maps as central, we refer to the collection of norm-preserving linear maps by the name $U(n)$. If we think of the matrices as central, we refer to the collection of complex $n \times n$ matrices A with $AA^* = I$ by the name $U(n)$.

Lemma 13.8. *If A is a unitary matrix then $|\det A| = 1$.*

If we think in terms of linear maps, we define

$$SU(n) = \{\alpha \in U(n) : \det \alpha = 1\}.$$

If we think in terms of matrices, we define

$$SU(n) = \{A \in U(n) : \det A = 1\}.$$

(The letter U stands for 'unitary', the letters SU for 'special unitary'.)

Lemma 13.9. *$U(n)$ is a group and $SU(n)$ a subgroup of $U(n)$.*

Not surprisingly, the generalisation of the symmetric matrix from the real case turns out to involve * rather than ^{T}. The reader should have no difficulty in proving the following parallel to Lemma 5.1.

Lemma 13.10. *Let $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ be linear. The following statements are equivalent.*

(i) $\langle \alpha\mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{x}, \alpha\mathbf{y}\rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$.

(ii) If α has matrix A with respect to some orthonormal basis, then $A = A^*$.

We call an α, having the properties just described, Hermitian. We can also call α a 'self-adjoint' map.

Again, the reader should have no problems proving the following versions of Theorems 5.2 and 5.3

Theorem 13.11. *If $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ is Hermitian, then all the roots of the characteristic polynomial* $\det(t\iota - \alpha)$ *are real.*

Theorem 13.12. *If $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ is Hermitian, then eigenvectors corresponding to distinct eigenvalues are orthogonal.*

As we might expect, the linear algebra course will contain a proof of the following result (compare Fact 5.5).

Fact 13.13. *(i) The map $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ is Hermitian if and only if there exists an orthonormal basis of eigenvectors of $\mathbb{C}^n$ with respect to which α has a diagonal matrix with real entries.*

(ii) The $n \times n$ complex matrix A is Hermitian if and only if there exists a matrix $P \in SU(n)$ such that P^*AP is diagonal with real entries.

In order to keep things simple for the rest of the discussion, we shall confine ourselves to the two dimensional space $\mathbb{C}^2$, but almost everything carries over to higher dimensions.

Lemma 13.14. *(i) If $\alpha \in U(2)$, then we can find an orthonormal basis for $\mathbb{C}^2$ with respect to which α has matrix*

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

with $\theta, \phi \in \mathbb{R}$. Conversely, any α with such a matrix representation is in $U(2)$.

(ii) If $\alpha \in SU(2)$, then we can find an orthonormal basis for $\mathbb{C}^2$ with respect to which α has matrix

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

with $\theta \in \mathbb{R}$. Conversely, any α with such a matrix representation is in $SU(2)$.

(iii) If $\beta : \mathbb{C}^2 \to \mathbb{C}^2$ is Hermitian, then we can find an orthonormal basis for $\mathbb{C}^2$ with respect to which β has matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

with $\lambda, \mu \in \mathbb{R}$. Conversely, any β with such a matrix representation is Hermitian.

(Note that we can prove (iii) directly without appealing to Fact 13.13.)

The discussion now takes off into the wild blue yonder. Readers who are already confused should stop reading here (indeed they could throw away the whole of this last section without real loss). Those who read on can treat what follows as a formal exercise (though, rather surprisingly, it is actually rigorous).

Lemma 13.15. *If $\alpha : \mathbb{C}^2 \to \mathbb{C}^2$ is linear, then*

(i) We can find a K such that

$$||\alpha \mathbf{x}|| \leq K||\mathbf{x}||$$

for all $\mathbf{x} \in \mathbb{C}^2$.

(ii) With the notation of (i),

$$||\alpha^n \mathbf{x}|| \leq K^n||\mathbf{x}||.$$

(iii) If $\mathbf{x} \in \mathbb{C}^2$, then $\sum_{n=0}^{\infty} \alpha^n \mathbf{x}/n!$ converges to a limit which we call $\exp(\alpha)\mathbf{x}$. More formally, we can find $\exp(\alpha)\mathbf{x} \in \mathbb{C}^2$ such that

$$\left|\left|\sum_{n=0}^{N} \frac{1}{n!}\alpha^n \mathbf{x} - \exp(\alpha)\mathbf{x}\right|\right| \to 0$$

as $N \to \infty$.

(iv) With the notation of (iii), $\exp(\alpha) : \mathbb{C}^2 \to \mathbb{C}^2$ is a linear map.

(v) If α has matrix A with respect to a given basis, then, with respect to the same basis, $\exp(\alpha)$ has matrix

$$\exp(A) = \sum_{n=0}^{\infty} \frac{1}{n!} A^n$$

with the sum taken in the obvious (component by component) way.

IMPORTANT WARNING In general $\exp(\alpha)\exp(\beta) \neq \exp(\alpha + \beta)$.

Before stating our final result we need a definition and an accompanying remark.

Definition 13.16. *If $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ is linear, then the trace* $\operatorname{tr}(\alpha)$ *is defined to be minus the coefficient of t^{n-1} in the characteristic polynomial* $\det(t\iota - \alpha)$.

Lemma 13.17. *If the linear map $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ has matrix A with respect to some basis then*

$$\operatorname{tr}(\alpha) = \sum_{j=1}^{n} a_{jj}.$$

We call $\sum_{j=1}^{n} a_{jj}$ the trace of A and write it $\operatorname{tr} A$. The trace will be discussed again in the linear algebra course.

Lemma 13.18. *(i) The map $\alpha \in SU(2)$ if and only if $\alpha = e^{i\beta}$ with β Hermitian of trace 0.*

(ii) The 2×2 matrix A is in $SU(2)$ (considered as a matrix group) if and only if

$$A = \exp(i(a_1 S_1 + a_2 S_2 + a_3 S_3))$$

with a_1, a_2, a_3 real and

$$S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ S_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ S_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The matrices S_1, S_2 and S_3 are called the Pauli spin matrices. They will turn up together with the group $SU(2)$ in the Part II Quantum Mechanics courses. Had we gone through the argument above with $SU(3)$ in place of $SU(2)$, we would have obtained eight real parameters $a_1, a_2, \dots, a_8$ in place of the three just found, and so heard a distant echo of the famous eight-fold way of Gell-Mann and Ne'eman.

14 Books

Professor Beardon has just brought out a book *Algebra and Geometry* which is very close in spirit and content to this course. If you want just one algebra text to see you through Parts 1A and 1B then C. W. Norman *Undergraduate Algebra* is very user friendly. P. M. Cohn's *Algebra* (Volume 1) is a more highbrow text but will appeal to future algebraists. All three books should be in your college library. (If not the librarian will be pleased to order them.) In general you should first consult textbooks in your library and only buy one when you have used it successfully for some time.

15 First exercise set

Most of the exercises in these exercise sets are taken from earlier sheets of Professor Beardon. In each case, the first five or so exercises are intended to be short and any exercises after the first twelve are for enthusiasts. (The extra questions may come in handy for revision, or your supervisor may choose a different selection of questions or one of the extra questions such as Exercise 15.17 or 18.18 may catch your fancy.)

We will take $\mathbf{e}_1, \mathbf{e}_2 \dots, \mathbf{e}_n$ to be the standard basis of $\mathbb{R}^n$. Unless otherwise stated, matrices act on $\mathbb{R}^n$ with respect to this basis.

Exercise 15.1. (a) Find a 3×3 real matrix with eigenvalues 1, i, $-i$. [Think geometrically.]

(b) Construct a 3×3 non-zero real matrix which has all three eigenvalues zero.

Exercise 15.2. (a) Let A be a square matrix such that $A^m = 0$ for some integer m. Show that every eigenvalue of A is zero.

(b) Let A be a real 2×2 matrix which has non-zero non-real eigenvalues. Show that the non-diagonal elements of A are non-zero, but that the diagonal elements may be zero.

Exercise 15.3. Suppose that A is an $n \times n$ square matrix and that A^{-1} exists. Show that if A has characteristic equation $a_0 + a_1 t + \dots + a_n t^n = 0$, then A^{-1} has characteristic equation

$$(-1)^n \det(A^{-1})(a_n + a_{n-1}t + \dots + a_0 t^n) = 0.$$

[**Note** : take $n = 3$ in this question if you wish, but treat the general case if you can. It should be clear that λ is an eigenvalue of A if and only if $1/\lambda$ is an eigenvalue of A^{-1}, but this result says more than this (about multiplicities of eigenvalues). You should use properties of the determinant to solve this problem, for example, $\det(A)\det(B) = \det(AB)$. You should also state explicitly why we do not need to worry about zero eigenvalues.]

Exercise 15.4. Show that the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$$

has characteristic equation $(t-2)^3 = 0$. Explain (without doing any further calculations) why A is not diagonalisable.

Exercise 15.5. (i) Find a, b and c such that the matrix

$$\begin{pmatrix} 1/3 & 0 & a \\ 2/3 & 1/\sqrt{2} & b \\ 2/3 & -1/\sqrt{2} & c \end{pmatrix}$$

is orthogonal. Does this condition determine a, b and c, uniquely?

(ii) (Exercise 5.7) Let

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Compute PAP^{-1} and observe that it is not a symmetric matrix, although A is. Why does this not contradict Lemma 5.6.

Exercise 15.6. Let

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

Find the characteristic equation for A. Verify[12] that $A^2 = 2A - I$. Is A diagonalisable ?

Show by induction that A^n lies in the two-dimensional subspace (of the space of 2×2 real matrices) spanned by A and I, so that there exists real numbers α_n and β_n with

$$A^n = \alpha_n A + \beta_n I.$$

Use the fact that $A^{n+1} = AA^n$ to find a recurrence relation (i.e., a difference equation) for α_n and β_n. Solve these and hence find an explicit formula for A^n. Verify this formula by induction.

Exercise 15.7. For each of the three matrices below,

(a) compute their eigenvalues (as often happens in exercises and seldom in real life each eigenvalue is a small integer);

(b) for each real eigenvalue λ compute the dimension of the eigenspace $\{\mathbf{x} \in \mathbb{R}^3 \,:\, A\mathbf{x} = \lambda\mathbf{x}\}$;

(c) determine whether or not the matrix is diagonalisable as a map of $\mathbb{R}^3$ into itself.

$$\begin{pmatrix} 5 & -3 & 2 \\ 6 & -4 & 4 \\ 4 & -4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{pmatrix}, \quad \begin{pmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{pmatrix}.$$

[12] See Example 2.12.

Exercise 15.8. Determine the eigenvalues and eigenvectors of the symmetric matrix
$$A = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Use an identity of the form $PAP^T = D$, where D is a diagonal matrix, to find A^{-1}.

Exercise 15.9. The object of this exercise is to show why finding eigenvalues of a large matrix is not just a matter of finding a large fast computer.

Consider the $n \times n$ complex matrix $A = (a_{ij})$ given by

$$\begin{aligned} a_{j\,j+1} &= 1 && \text{for } 1 \leq j \leq n-1 \\ a_{n1} &= \kappa^n \\ a_{ij} &= 0 && \text{otherwise,} \end{aligned}$$

where $\kappa \in \mathbb{C}$ is non-zero. Thus, when $n = 2$ and $n = 3$, we get the matrices

$$\begin{pmatrix} 0 & 1 \\ \kappa^2 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \kappa^3 & 0 & 0 \end{pmatrix}.$$

(i) Find the eigenvalues and associated eigenvectors of A for $n = 2$ and $n = 3$. (Note that we are working over $\mathbb{C}$ so we must consider complex roots.)

(ii) By guessing and then verifying your answers, or otherwise, find the eigenvalues and associated eigenvectors of A for for all $n \geq 2$.

(iii) Suppose that your computer works to 15 decimal places and that $n = 100$. You decide to find the eigenvalues of A in the cases $\kappa = 2^{-1}$ and $\kappa = 3^{-1}$. Explain why at least one (and more probably) both attempts will deliver answers which bear no relation to the true answers.

Exercise 15.10. (a) Let
$$A = \begin{pmatrix} 2 & -2 \\ -2 & 5 \end{pmatrix}$$

Find an orthogonal matrix P such that P^TAP is diagonal and use P to diagonalise the quadratic form

$$Q(x, y) = 2x^2 - 4xy + 5y^2.$$

(b) Diagonalise the quadratic form

$$(a\cos^2\theta + b\sin^2\theta)x^2 + 2(a-b)(\sin\theta\cos\theta)xy + (a\sin^2\theta + b\cos^2\theta)y^2.$$

Exercise 15.11. Find all eigenvalues, and an orthonormal set of eigenvectors, of the matrices

$$A = \begin{pmatrix} 5 & 0 & \sqrt{3} \\ 0 & 3 & 0 \\ \sqrt{3} & 0 & 3 \end{pmatrix} \text{ and } B = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2. \end{pmatrix}$$

Hence sketch the surfaces

$$5x^2 + 3y^2 + 3z^2 + 2\sqrt{3}xz = 1 \text{ and } x^2 + y^2 + z^2 - xy - yz - zx = 1.$$

Exercise 15.12. Use Gaussian elimination to solve the following two systems of integer *congruences* modulo 7.

$$\begin{aligned} x + y + z &\equiv 3 \\ x + 2y + 3z &\equiv 1 \\ x + 4y + 2z &\equiv 1. \end{aligned}$$

Do the same for

$$\begin{aligned} x + y + 6z &\equiv 2 \\ x + 2y + 5z &\equiv 4 \\ x + 4y + 3z &\equiv 1. \end{aligned}$$

Write down a third equation which makes the system

$$\begin{aligned} x + y + 6z &\equiv 2 \\ x + 2y + 5z &\equiv 4 \end{aligned}$$

insoluble and show that you have done so.

Exercise 15.13. (a) Suppose that a 3×3 real matrix A acting on $\mathbb{R}^3$ has eigenvalues λ, μ and $\bar{\mu}$, where λ is real, μ is complex and non-real, and $\bar{\mu}$ is the complex conjugate of μ. Suppose also that $\mathbf{u}$ is a real eigenvector for λ and that $\mathbf{v}$ is a complex eigenvector for μ, where $\mathbf{v} = \mathbf{v}_1 + i\mathbf{v}_2$, and $\mathbf{v}_1$ and $\mathbf{v}_2$ are real vectors. Show that $\mathbf{v}_1 - i\mathbf{v}_2$ is a complex eigenvector for $\bar{\mu}$.

Assume that the vectors $\mathbf{u}$, $\mathbf{v}_1$, $\mathbf{v}_2$ are linearly independent. Show that A maps the plane Π in $\mathbb{R}^3$ spanned by $\mathbf{v}_1$ and $\mathbf{v}_2$ into itself, and that Π contains no eigenvectors of A.

(b) Illustrate the previous paragraph with the case of a rotation of $\mathbb{R}^3$ of angle $\pi/4$ about the axis along $\mathbf{e}_1$.

(c) Illustrate (a) again by taking

$$A = \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix},$$

and show that in this case Π has equation $2x - 2y + z = 0$.

Exercise 15.14. Let Σ be the surface in $\mathbb{R}^3$ given by

$$2x^2 + 2xy + 4yz + z^2 = 1.$$

By writing this equation as

$$\mathbf{x}^T A \mathbf{x} = 1,$$

with A a real symmetric matrix, show that there is an orthonormal basis such that, if we use coordinates (u, v, w) with respect to this new basis, Σ takes the form

$$\lambda u^2 + \mu v^2 + \nu w^2 = 1.$$

Find λ, μ and ν and hence find the minimum distance between the origin and Σ. [It is **not** necessary to find the basis explicitly.]

Exercise 15.15. (This is another way of proving $\det AB = \det A \det B$. You may wish to stick to the case $n = 3$.)

If $1 \le r, s \le n$, $r \ne s$ and λ is real, let $E(\lambda, r, s)$ be an $n \times n$ matrix with (i, j) entry $\delta_{ij} + \lambda \delta_{ir} \delta_{js}$. If $1 \le r \le n$ and μ is real, let $F(\mu, r)$ be an $n \times n$ matrix with (i, j) entry $\delta_{ij} + (\mu - 1)\delta_{ir}\delta_{jr}$.

(i) Give a simple geometric interpretation of the linear maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ associated with $E(\lambda, r, s)$ and $F(\mu, r)$.

(ii) Give a simple account of the effect of pre-multiplying an $n \times m$ matrix by $E(\lambda, r, s)$ and by $F(\mu, r)$. What is the effect of post-multiplying an $m \times n$ matrix?

(iii) If A is an $n \times n$ matrix, find $\det(E(\lambda, r, s)A)$ and $\det(F(\mu, r)A)$ in terms of $\det A$.

(iv) Show that every $n \times n$ matrix is the product of matrices of the form $E(\lambda, r, s)$ and $F(\mu, r)$ and a diagonal matrix with entries 0 or 1.

(v) Use (iii) and (iv) to show that, if A and B are $n \times n$ matrices, then $\det A \det B = \det AB$.

Exercise 15.16. Show that a rotation about the z axis through an angle θ corresponds to the matrix

$$\mathbf{R} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Write down a real eigenvector of $\mathbf{R}$ and give the corresponding eigenvalue.

In the case of a matrix corresponding to a general rotation, how can one find the axis of rotation?

A rotation through $45°$ about the x-axis is followed by a similar one about the z-axis. Show that the rotation corresponding to their combined effect has its axis inclined at equal angles

$$\cos^{-1}\frac{1}{\sqrt{(5-2\sqrt{2})}}$$

to the x and z axes.

Exercise 15.17. (i) If $\beta : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal map which fixes two orthonormal vectors $\mathbf{e}_1$ and $\mathbf{e}_2$, show that if, $\mathbf{x}$ is perpendicular to $\mathbf{e}_1$ and $\mathbf{e}_2$, then $\beta\mathbf{x}$ is perpendicular to $\mathbf{e}_1$ and $\mathbf{e}_2$.

(ii) Use the ideas of Lemma 4.16 and the surrounding lemmas to show that, if $n \geq 3$, then there is an orthonormal basis of $\mathbb{R}^n$ with respect to which β has matrix

$$\begin{pmatrix} C & O_{2,n-2} \\ O_{n-2,2} & B \end{pmatrix}$$

where $O_{r,s}$ is a $r \times s$ matrix of zeros, B is an $(n-2)\times(n-2)$ orthogonal matrix and

$$C = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

for some real θ.

(iii) Show that, if $n = 4$, then, if β is special orthogonal, we can find an orthonormal basis of $\mathbb{R}^4$ with respect to which β has matrix

$$\begin{pmatrix} \cos\theta_1 & -\sin\theta_1 & 0 & 0 \\ \sin\theta_1 & \cos\theta_1 & 0 & 0 \\ 0 & 0 & \cos\theta_2 & -\sin\theta_2 \\ 0 & 0 & \sin\theta_2 & \cos\theta_2 \end{pmatrix},$$

for some real θ_1 and θ_2, whilst, if β is not special orthogonal, we can find an orthonormal basis of $\mathbb{R}^4$ with respect to which β has matrix

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & \sin\theta & \cos\theta \end{pmatrix},$$

for some real θ.

(iv) What happens if we take $n = 5$? What happens for general n? Prove your statements.

16 Second exercise set

Most of the exercises in these exercise sets are taken from earlier sheets of Professor Beardon. In each case, the first five or so exercises are intended to be short and any exercises after the first twelve are for enthusiasts. (The extra questions may come in handy for revision, or your supervisor may choose a different selection of questions or one of the extra questions such as Exercise 15.17 or 18.18 may catch your fancy.)

Exercise 16.1. Throughout this question $(G, *)$ will be set G with a multiplication $*$ such that $a * b \in G$ whenever a, $b \in G$ whilst

$$a * (b * c) = (a * b) * c \text{ for all } a,\ b,\ c \in G.$$

(i) Suppose that there exist e_R and e_L in G such that

$$a * e_R = e_L * a = a \text{ for all } a \in G.$$

Show that $e_R = e_L$. How does this show that the unit in a group is unique?

(ii) Suppose that there exists an $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. Show that, if $x \in G$ and we can find x_R and x_L in G such that

$$x * x_R = x_L * x = e,$$

then $x_R = x_L$. How does this show that the inverse of any element in a group is unique?

(iii) Suppose now that $(G, *)$ is a group. If H is a non-empty subset of G such that $ab^{-1} \in H$ whenever a, $b \in H$, show that H is a subgroup of G.

Exercise 16.2. Let $\mathbf{Z}$ be the group of integers under addition. What is the subgroup of $\mathbf{Z}$ generated

(i) by 530 and 27?

(ii) by 531 and 27?

[Recall that the subgroup generated by a subset E of a group is the smallest subgroup of G containing E. Consider the greatest common divisor.]

Exercise 16.3. Show that if H and K are subgroups of a group G, then $H \cap K$ is also a subgroup of G. Show also that, if H and K have orders p and q, respectively, where p and q are coprime, then $H \cap K$ contains only the identity element e of G.

Exercise 16.4. Show that the set G of matrices of the form

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix},$$

where z and w are complex numbers with $|z|^2 + |w|^2 \neq 0$, is a non-Abelian group under multiplication.

Show that the set H of matrices of the form

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix},$$

where z and w are complex numbers with $|z|^2 + |w|^2 = 1$, is a subgroup of G. Is H a normal subgroup of G? [Think determinants. H is normal if $ABA^{-1} \in H$ whenever $A \in G$ and $B \in H$.] Is H Abelian? Is H infinite? In each case, give reasons.

Exercise 16.5. Let G be the set of complex numbers of the form $\exp i\pi q$ with q rational. Show that G is an Abelian group under multiplication. Show that G is infinite but that every element of G is of finite order.

Can you find an infinite group in which every element except the identity is of infinite order? Give reasons.

Exercise 16.6. Let $\mathcal{P}$ be a solid triangular prism with an equilateral triangle as cross-section and ends orthogonal to the longitudinal axis of the prism (a 'Toblerone' bar). Find the group of rotations which leaves $\mathcal{P}$ invariant. Can you show that it is isomorphic to a standard group? [It may be helpful to proceed as follows. First find the number of elements in the group. Now find generators for the group and relations between them. Now see if you can identify the group as isomorphic to one you already know.] Find the group of rotations and reflections which leaves $\mathcal{P}$ invariant. Can you show that it is isomorphic to a standard group?

Exercise 16.7. Suppose G is group in which every element other than the identity has order 2. By evaluating $x(xy)^2y$ in two ways, show that $xy = yx$ for all $x, y \in G$. If the identity e, x and y are all distinct, show that the set $\{e, x, y, xy\}$ is a subgroup of G of order exactly 4.

Use Lagrange's theorem to show that any group of order $2p$, where p is an odd prime, must contain an element of order p.

Exercise 16.8. Consider the four matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Compute $\mathbf{i}^2$, $\mathbf{j}^2$, $\mathbf{k}^2$, $\mathbf{ij}$, $\mathbf{jk}$, $\mathbf{ki}$, $\mathbf{ji}$, $\mathbf{kj}$, $\mathbf{ik}$ and show that the four matrices generate a group $\mathbf{Q}$ of order 8. Is the group $\mathbf{Q}$ Abelian? How many subgroups of order 4 does it have?

Exercise 16.9. (a) Consider the functions $f : A \to B$, $g : B \to C$ and their composition $g \circ f : A \to C$ given by $g \circ f(a) = g(f(a))$. Prove the following results.

(i) If f and g are surjective, then so is $g \circ f$.

(ii) If f and g are injective, then so is $g \circ f$.

(iii) If $g \circ f$ is injective, then so is f.

(iv) If $g \circ f$ is surjective, then so is g.

(b) Give an example where $g \circ f$ is injective and surjective but f is not surjective and g is not injective.

(c) If any of your proofs of parts (i) to (iv) of (a) involved contradiction, reprove them without such arguments[13].

(d) Have you given the simplest possible example in (b)? (If you feel that this is not a proper question, let us ask instead for the smallest possible sets A and B.)

Exercise 16.10. Three fixed lines a, b, c are the sides of an equilateral triangle, and $\mathbf{A}$, $\mathbf{B}$ $\mathbf{C}$ denote the operations of reflection in a, b, c respectively. Describe the operations $\mathbf{AB}$, $\mathbf{CB}$, $\mathbf{CBAB}$. (You should use the composition law $(fg)(x) = f(g(x))$.)

Show that there exists an infinite group G containing elements p, q, r such that

(i) G is generated by p, q, r;

(ii) $p^2 = q^2 = r^2 = (qr)^3 = (rp)^3 = (pq)^3 = e$.

Exercise 16.11. For any two sets A and B the symmetric difference $A \triangle B$ of A and B is the set of elements in *exactly one* of A and B. Let Ω be a non-empty set and let G be the set of subsets of Ω (note that G includes both the empty set $\varnothing$ and Ω). Show that G with the operation $\triangle$ is an abelian group. [*Hint* : the identity element is likely to be either $\varnothing$ or Ω as no other 'special' element presents itself. *Remark* : this is an example in which the associative law is not entirely trivial.]

Let $\Omega = \{1, \ldots, 7\}$ and let $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$, $C = \{5, 6, 7\}$. Find X in G such that $A \triangle X \triangle B = C$.

Exercise 16.12. Let C_n be the cyclic group with n elements and D_{2n} the dihedral group with $2n$ elements (i.e., the group of symmetries of the regular n-gon[14]). If n is odd and $f : D_{2n} \to C_n$ is a homomorphism, show that $f(x) = e$ for all $x \in D_{2n}$. What can we say if n is even?

Find all the homomorphisms from the cyclic group C_n of order n generated by a, say, to C_m the cyclic group generated by b, say. If $n = m$, show that there are $\phi(n)$ isomorphisms, where $\phi(n)$ is the number of integers between 0 and $n - 1$ coprime to n (Euler's totient function).

---

[13] Conway refers to arguments of the form 'Assume X is true but Y is false. Since X implies Y it follows that Y is true. This contradicts our original assumption. Thus X implies Y.' as 'absurd absurdums'.

[14] Observe my inability to keep to a consistent choice between D_n and D_{2n}.

Exercise 16.13. (This question will be accessible to those who are doing the course 'Numbers and Sets', it may or may not be accessible to others.) State what is meant by an *equivalence relation* between members of a set E and show that an equivalence relation defines a partition of E into disjoint sets.

A relation $\sim$ between $m \times n$ matrices A and B is defined as follows: $A \sim B$ if there exists a non-singular $m \times m$ matrix P and a non-singular $n \times n$ matrix Q such that

$$PAQ = B.$$

Show that this is an equivalence relation.

State a criterion for A to be equivalent to

$$\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix},$$

where I_r is the unit $r \times r$ matrix, and deduce the number of equivalence classes.

Exercise 16.14. Giving adequate justification for your answers, state which of the following sets of $n \times n$ matrices are groups under the usual operation of matrix multiplication (in each case $n \geq 2$)

(i) the matrices A with $a_{11} = 1$;
(ii) the set consisting of the zero matrix only;
(iii) the matrices with a positive non-zero determinant;
(iv) the matrices with determinant zero;
(v) the matrices whose determinant is a non-zero integer;
(vi) the matrices A such that a_{ij} is an integer for all (i, j) and $\det A = 1$.

Exercise 16.15. We work in $\mathbb{R}^2$. Let R_1 be the rectangle with vertices $(0, 0)$, $(1, 0)$, $(1, 2)$, $(0, 2)$ and let R_2 be the rectangle with vertices $(0, 0)$, $(2, 0)$, $(2, 1)$, $(0, 1)$. Find all the isometries which map R_1 to R_2 and show that you have indeed found all of them.

Exercise 16.16. Throughout this question G is a group and K a non-empty subset of G.

(i) Give an example of a finite group G and a non-empty subset K such that $x^{-1}Kx = K$ for all $x \in G$ but K is not a normal subgroup of G.

(ii) Show that if K is finite and $Kx \subseteq K$ for some $x \in G$, then $Kx = K$.

(iii) Give an example to show that (ii) is false if we drop the condition K finite.

(iv) If $Kx = K$ for all $x \in G$, show that $K = G$.

Exercise 16.17. From time to time the lecturer and your supervisor may mention the notion of 'a group generated by certain elements' (eg in the hint to Exercise 16.6). It is not necessary to make this notion precise at 1A level. If you are interested, this exercise shows how it can be made precise. The arguments are easy but not worth doing unless you formulate them carefully.

(i) Let G be a group and let $\{H_\alpha : \alpha \in A\}$ be a non-empty collection of subgroups of G. Show that $\bigcap_{\alpha\in A} H_\alpha$ is a subgroup of G.

(ii) Let G be a group and X a non-empty subset of G. Explain why the collection $\mathcal{G}_X$ of subgroups of G containing X is non-empty. We call

$$\operatorname{gen} X = \bigcap_{H\in\mathcal{G}_X} H$$

the subgroup of G generated by X.

(iii) Show that if G and X are as in (ii), then there is unique subgroup K of G containing X with the property that, if H is a subgroup of G containing X, then $H \supseteq K$. Show also that $K = \operatorname{gen} X$.

(iv) If G and X are as in (ii), show that $\operatorname{gen} X$ consists of the unit e together with all elements

$$\prod_{i=1}^{N} g_i^{\epsilon_i} = g_1^{\epsilon_1} g_2^{\epsilon_1} \dots g_N^{\epsilon_N}$$

with $\epsilon_i = \pm 1$, $g_i \in X$ $[1 \le i \le N]$ and $N \ge 1$.

(v) [In the remainder of this question we use the notion of generator to bound the number of non-isomorphic groups of order n. You should worry less about dotting i's and crossing t's.] If E contains n elements explain why there are exactly n^{n^2} distinct functions $f : E \times E \to E$ and use this fact to show that there are at most n^{n^2} non-isomorphic groups of order n.

(vi) If H is a subgroup of a finite group G and $x \notin H$ show that $\{x\} \cup H$ generates a subgroup of order at least twice the order of H. Deduce that that a group of order n has a set of generators with at most $\log_2 n$ elements. (That is to say, we can find X a subset of G with at most $\log_2 n$ elements and $\operatorname{gen} X = G$. We define $\log_2 n$ by the equation $2^{\log_2 n} = n$.)

(v) Suppose that X generates a group G. Explain how, given the values of xg and $x^{-1}g$ for every $x \in X$ and $g \in G$, we may compute uv for every $u, v \in G$. Deduce that there are at most $n^{2n \log_2 n}$ non-isomorphic groups of order n.

17 Third exercise set

Most of the exercises in these exercise sets are taken from earlier sheets of Professor Beardon. In each case, the first five or so exercises are intended to be short and any exercises after the first twelve are for enthusiasts. (The extra questions may come in handy for revision, or your supervisor may choose a different selection of questions or one of the extra questions such as Exercise 15.17 or 18.18 may catch your fancy.)

Exercise 17.1. Show that if a group G is generated by two elements a and b, where $a^{-1}ba = b^2$ and $b^{-1}ab = a^2$, then G contains only one element. [Recall that 'G is generated by two elements a and b' means that every element of G is the product of terms of the form a, b, a^{-1} and b^{-1}.]

Exercise 17.2. The dihedral group D_{2n} is the full symmetry group of a regular plane n-gon. Show that, if the integer m divides $2n$, then D_{2n} has a subgroup of order m.

If $n \geq m \geq 3$, show that D_{2m} is isomorphic to a subgroup of D_{2n} if and only if m divides n.

Exercise 17.3. Show that the set of real non-singular 3×3 upper-triangular[15] matrices form a group under matrix multiplication. Does this group contain any elements of order two which are not diagonal matrices?

Exercise 17.4. Let G the group of orthogonal 2×2 real matrices and let N be a normal subgroup of G that contains a reflection in some line through the origin. Show that N contains all reflections and deduce that $N = G$.

Exercise 17.5. Show that the set of real 2×2 upper triangular matrices of positive determinant is a group G under matrix multiplication. Show that the map θ given by

$$\theta \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \log ad$$

is a homomorphism of G onto the additive group $\mathbb{R}$. What is the kernel K of θ?

Exercise 17.6. Let G be the set of all 3×3 real matrices of determinant 1 of the form

$$\begin{pmatrix} a & 0 & 0 \\ b & x & y \\ c & z & w \end{pmatrix}.$$

[15]If you come across a word which you do not know like 'upper-triangular' you have various choices. You can not do the question OR you can ask a friend OR go and look in the index in the algebra books in your college library. Which of these three choices is the stupidest? Actually an upper triangular matrix (a_{ij}) is one with $a_{ij} = 0$ whenever $i > j$ i.e., one with all elements below the diagonal zero.

Show that G is a group under matrix multiplication. Find[16] a homomorphism from G onto the group of all non-singular 2×2 real matrices and find its kernel.

Exercise 17.7. Let $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ be the additive groups of integers, rational and real numbers respectively. Show that every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order. Show that every element of the quotient group $\mathbb{R}/\mathbb{Q}$ (apart from the identity) has infinite order. Show that some elements of $\mathbb{R}/\mathbb{Z}$ have infinite order and some non-identity elements do not.

Exercise 17.8. The group of 2×2 real non-singular matrices is the General Linear Group $GL(2,\mathbb{R})$; the subset of $GL(2,\mathbb{R})$ consisting of matrices of determinant 1 is called the Special Linear Group $SL(2,\mathbb{R})$. Show that $SL(2,\mathbb{R})$ is, indeed, a subgroup of $GL(2,\mathbb{R})$ and that it is, in fact, normal. Show that the quotient group $GL(2,\mathbb{R})/SL(2,\mathbb{R})$ is isomorphic to the multiplicative group of non-zero real numbers. [The neatest way to do this question is to reflect on the isomorphism theorem (Theorem 10.10).]

Exercise 17.9. Let G and H be groups and $\phi : G \to H$ a homomorphism with kernel K. Show that, if $K = \{e, a\}$, then $x^{-1}ax = a$ for all $x \in G$.

Show that:–

(i) There is a homomorphism from $O(3)$, the orthogonal group of 3×3 real matrices, onto a group of order 2 with kernel the special orthogonal group $SO(3)$.

(ii) There is a homomorphism from S_3 the symmetry group on 3 elements to a group of order 2 with a kernel of order 3.

(iii) There is a homomorphism from $O(3)$ onto $SO(3)$ with kernel of order 2.

(iv) There is no homomorphism from S_3 to a group of order 3 with a kernel of order 2.

Exercise 17.10. For a combinatorialist a *graph* is a finite set of points called *vertices* and some *edges*. Each edge joins two vertices and there is at most one edge $[ab] = [ba]$ joining any two vertices a and b. (Think of airports with at most one route joining any two airports.) Two such graphs with vertices labelled 1 to 6 are shown in Figure 1.
Graph A has edges [12], [23], [34], [45], [56], [61], [35], [31] and [51].
Graph B has edges [12], [23], [34], [45], [56], [61], [35], [26], [63] and [52].

A *symmetry* ρ of the graph is a permutation of $\{1, \dots, 6\}$ such that $(\rho a, \rho b)$ is an edge if and only if (a, b) is an edge. Show that the symmetries of a graph form a subgroup of S_6.

[16] That is to say, guess, and then verify that your guess is correct. Guessing is an essential part of mathematics. Very good guessers are very good mathematicians (provided they understand the difference between a guess and a proof).

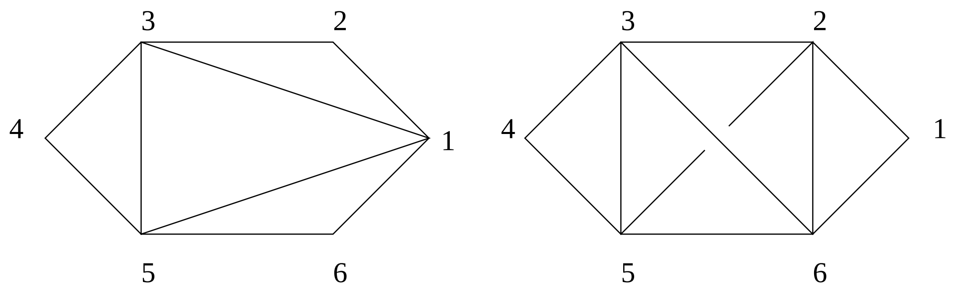

Figure 1: Graphs A and B

For each of graphs A and B
(a) find the symmetry group of the graph;
(b) find the orbit and stabiliser for each vertex;
(c) verify the orbit-stabiliser theorem for each vertex.

Exercise 17.11. Let G be a finite group and X the set of its subgroups. Show that $g(L) = gLg^{-1}$ $[g \in G,\ L \in X]$ defines an action of G on X. If H is a proper subgroup of G show that the orbit of H has at most $|G|/|H|$ elements and, by considering overlapping, or otherwise, show that there is an element of G which does not belong to any conjugate of H.

Exercise 17.12. In each case, give reasons for your answer.

(i) Is it true that, if a finite group G acts on a finite set X, then every $g \in G$ has a fixed point? [Recall that x is a fixed point for g if $gx = x$.]

(ii) Is it true that, if a finite group G with more than one element acts faithfully on a finite set X with more than one element, then there exists a $g \in G$ with no fixed point?

(iii) Can an infinite group have a finite subgroup with more than one element?

(iv) Let a and b be elements of an Abelian group. If a and b have order 2, what are the possible orders of ab?

(v) Is every subgroup of a normal subgroup of a group G itself normal in G?

(vi) Let G_1 and G_2 be arbitrary groups. Does there exist a group G with subgroups H_1 and H_2 such that H_1 is isomorphic to G_1 and H_2 is isomorphic to G_2?

(vii) [For those who have done the course 'Numbers and Sets' or know about countability from other sources.] Does there exist an uncountable set of finite groups no two of which are isomorphic?

Exercise 17.13. Let G be a group acting faithfully on a finite set X.

(i) We say that G acts transitively on X if there is only one orbit. Show that G acts transitively if and only if given x, $y \in X$ we can find a $g \in G$ with $gx = y$.

(ii) Suppose that G acts transitively on X. Define a function $T : G \times X \to \mathbb{Z}$ by $T(g, x) = 1$ if $gx = x$, $T(g, x) = 0$ otherwise. By evaluating $\sum_{x \in X} \sum_{g \in G} T(g, x)$ in two different ways, show that

$$\frac{1}{|G|} \sum_{g \in G} I(g) = 1,$$

where $I(g)$ is the number of elements fixed by g.

(iii) Deduce that, if G acts transitively on X and X has more than one element, then there must exist a $g \in G$ with no fixed point.

(iv) Suppose now that we do not assume that G acts transitively. Find and prove a formula along the lines of (ii) for the number N of distinct orbits. [The formula you find is called the Cauchy–Frobenius formula. If your supervisor is a combinatorialist or a group theorist you may expect an impassioned speech on the many uses of this result, but, alas, there is not room in 1A for all that we would like to teach.]

Exercise 17.14. If G is a group, we call an isomorphism $\alpha : G \to G$ an *automorphism*. Show that the automorphisms of G form a group under composition.

Consider $\mathbb{Q}$ (the rationals) as an additive group. Show that, if r and s are non-zero rationals, there is a unique automorphism α with $\alpha(r) = s$. Deduce that the group of automorphisms of $\mathbb{Q}$ is isomorphic to the multiplicative group of $\mathbb{Q} \setminus \{0\}$.

Exercise 17.15. You are skiing on the border of Syldavia. By mistake you cross into Borduria and are arrested. The border guard turns out to be an old Trinity man and agrees to let you go provided that you prove you are indeed a mathematician by classifying all groups of order 10. Do so.

Exercise 17.16. (i) Consider the collection $\mathcal{A}$ of maps $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$T\mathbf{x} = \alpha(\mathbf{x}) + \mathbf{u}$$

where α is a non-singular linear map (i.e. $\alpha \in GL(\mathbb{R}^2)$) and $\mathbf{u} \in \mathbb{R}^2$. Show that $\mathcal{A}$ forms a group under composition.

(ii) Show that the set of isometries, that is to say, T such that

$$\|T\mathbf{x} - T\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|,$$

for all $\mathbf{x}$, $\mathbf{y} \in \mathbb{R}^2$ forms a subgroup of $\mathcal{A}$. [You may assume that any isometry which fixes $\mathbf{0}$ is linear.]

(iii) In what follows we seek to characterise the set $\mathcal{B}$ of $T \in \mathcal{A}$ such that $T^2 = I$, the identity map. Suppose

$$T\mathbf{x} = \alpha(\mathbf{x}) + \mathbf{u}$$

where $\alpha \in GL(\mathbb{R}^2)$ and $\mathbf{u} \in \mathbb{R}^2$. Show that $T \in \mathcal{B}$ if and only if $\alpha^2 = I$ and $\alpha\mathbf{u} = -\mathbf{u}$.

(iv) Suppose that $\alpha \in GL(\mathbb{R}^2)$ and $\alpha^2 = I$. Show that either $\alpha = I$, or $\alpha = -I$, or there exists a basis $\mathbf{f}_1$, $\mathbf{f}_2$ with respect to which α has matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(v) Suppose that $\alpha \in GL(\mathbb{R}^2)$ and $\alpha^2 = I$. Show that either $\alpha = I$, or $\alpha = -I$, or there exists a orthonormal basis $\mathbf{e}_1$, $\mathbf{e}_2$ with respect to which α has matrix

$$\begin{pmatrix} -1 & k \\ 0 & 1 \end{pmatrix}$$

for some real k.

(vi) Show that $T \in \mathcal{B}$ if and only if

$$T\mathbf{x} = \mathbf{x}$$

for all $\mathbf{x} \in \mathbb{R}^2$, or

$$T\mathbf{x} = -\mathbf{x} + \mathbf{u}$$

for all $\mathbf{x} \in \mathbb{R}^2$ and some fixed $\mathbf{u} \in \mathbb{R}^2$, or if, after an appropriate rotation of axes,

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ 0 \end{pmatrix}$$

for some fixed k, $u \in \mathbb{R}$.

(vii) Show that, if $T \in \mathcal{B}$, then T leaves some line l through the origin fixed (that is to say, $Tl = l$).

(viii) Is $\mathcal{B}$ a subgroup of $\mathcal{A}$?

(xi) Show that, if T is an isometry and $T^2 = I$, then T is a reflection in some line (not necessarily through the origin), or a rotation through π about some point (not necessarily the origin) or the identity map.

18 Fourth exercise set

Most of the exercises in these exercise sets are taken from earlier sheets of Professor Beardon. In each case, the first five or so exercises are intended to be short and any exercises after the first twelve are for enthusiasts. (The extra questions may come in handy for revision, or your supervisor may choose a different selection of questions or one of the extra questions such as Exercise 15.17 or 18.18 may catch your fancy.)

Exercise 18.1. Let $X = \{0, 1, 2, \ldots, 16\}$. Express each of the following permutations of X as a product of cycles and decide whether it is even or odd.

(a) The function defined by $f_1(x) \equiv 2x \mod 17$.
(b) The function defined by $f_2(x) \equiv x + 5 \mod 17$.
(c) The function defined by $f_3(x) \equiv 3x \mod 17$.

Explain why the function defined by $f_4(x) \equiv x^2 \mod 17$ is not a permutation.

Exercise 18.2. What is the largest possible order of an element in S_5?

What is the largest possible order of an element in S_9?

What is the largest possible order of an element in S_{16}? [You may need to run through several possibilities.]

Show that every element in S_{10} of order 14 is odd.

Exercise 18.3. Show that any subgroup of S_n which is not contained in A_n contains an equal number of odd and even elements.

Exercise 18.4. Let $g(z) = (z + 1)/(z - 1)$. By considering the points $g(0)$, $g(\infty)$, $g(1)$ and $g(i)$, find the image of the real axis $\mathbb{R}$ and the imaginary axis (in each case with ∞ attached) under g. What is the image under g of $\{x + iy : x > 0, y > 0\}$?

Exercise 18.5. Express the Möbius transformation $z \mapsto (2z + 3)/(z - 4)$ as the composition of maps of the form $z \mapsto az$, $z \mapsto z + b$ and $z \mapsto 1/z$. Hence show that $z \mapsto (2z + 3)/(z - 4)$ maps the circle $|z - 2i| = 2$ onto the circle

$$\left| z + \left(\frac{6 + 11i}{8} \right) \right| = \frac{11}{8}.$$

Exercise 18.6. (i) Show that, if z_1, z_2, z_3 and w_1, w_2, w_3 are two triples of distinct points in $\mathbb{C} \cup \{\infty\}$, there exists a unique Möbius transformation that takes z_j to w_j $[j = 1, 2, 3]$. Hence show that 4 distinct points z_1, z_2, z_3 and z_4 lie on a circle or a straight line if and only if the cross ratio $CR(z_1, z_2, z_3, z_4)$ is real.

(ii) If z_1, z_2, z_3 and z_4 are distinct and $CR(z_1, z_2, z_3, z_4) = \lambda$ write down the possible values of $CR(z_{\sigma 1}, z_{\sigma 2}, z_{\sigma 3}, z_{\sigma 4})$ when $\sigma \in S_4$, proving your assertion.

(iii) Use cross-ratios to prove Ptolemy's theorem:– 'For any quadrilateral whose vertices lie on a circle the product of the lengths of the diagonals is the sum of the products of the lengths of pairs of opposite sides.'

Exercise 18.7. Let G be the subgroup of those Möbius transformations which map the set $\{0, 1, \infty\}$ onto itself. Show that the only elements of G are the functions

$$f_0(z) = z,\ f_1(z) = 1-z,\ f_2(z) = \frac{1}{z},\ f_3(z) = \frac{z}{z-1},\ f_4(z) = \frac{1}{1-z},\ f_5(z) = \frac{z-1}{z}.$$

To which standard group is G isomorphic?

Find the group of Möbius transformations which map the set $\{0, 2, \infty\}$ onto itself.

Exercise 18.8. Show that if $|a| \neq 1$ the map

$$T_a z = \frac{z-a}{a^* z - 1}$$

takes the unit circle $\{z : \ |z| = 1\}$ to itself. What are $T_a 0$ and $T_a a$? What does T_a take the unit disc $D = \{z : \ |z| < 1\}$ to (i) if $|a| < 1$, (ii) if $|a| > 1$? What happens if $|a| = 1$?

Show that the only Möbius map S with $S0 = 0$, $S1 = 1$ and $SD = D$ is the identity map. Hence, or otherwise, show that the most general Möbius map R with $RD = D$ is given by

$$Rz = \exp(i\theta)\frac{z-a}{a^* z - 1},$$

where θ is real and $|a| < 1$.

Find the most general Möbius map which takes the half-plane $\{z : \ \operatorname{Im}(z) > 0\}$ to the unit disc D. (You may leave your result in the form of a composition.)

Exercise 18.9. Show that every Möbius transform has at least one fixed point.

Identify the stabiliser G of ∞. Find all the $T \in G$ which have only one fixed point and show that

$$T^n z \to \infty \quad \text{as } |n| \to \infty$$

for all such T and all $z \in \mathbb{C}$. Hence show that, if S is any Möbius map with a unique fixed point z_0, then

$$S^n z \to z_0 \quad \text{as } |n| \to \infty$$

for all $z \in \mathbb{C} \cup \{\infty\}$.

Identify the subgroup H of Möbius maps which leave 0 and ∞ fixed and the subgroup H' of Möbius maps which leave the set $\{0, \infty\}$ fixed. Describe, in general terms, the orbits under $T \in H$ (that is to say, the orbit of a point z under the cyclic group generated by T) if T does not leave the circle $\{z \in \mathbb{C} : \ |z| = 1\}$ fixed. Give an example of a Möbius map for which the orbit of every point with two exceptions has four elements.

Show that every Möbius transform, with exactly one exception, has exactly one fixed point or exactly two fixed points.

Exercise 18.10. The *cycle type* of an element σ of the symmetric group S_n is defined to be the collection of lengths of disjoint cycles that form σ. (For example $(1754)(268)(3)(9) \in S_9$ has cycle type 4, 3, 1, 1.)

(i) Show that σ_1 and σ_2 in S_n have the same cycle type if and only if there exists a $\tau \in S_n$ such that $\sigma_1 = \tau^{-1}\sigma_2\tau$.

(ii) Find the number of elements of each cycle type in S_5. Which of them belong to A_5?

Exercise 18.11. (i) Show that S_n is generated by transpositions of the form $(1j)$ with $2 \leq j \leq n$.

(ii) Show that S_n is generated by transpositions of the form $(j-1\,j)$ with $2 \leq j \leq n$.

(iii) Show that S_n is generated by the two elements (12) and $(123\dots n)$.

(iv) For which values of n is S_n generated by a single element? Prove your answer.

(v) Calculate the product $(12)(13)$ in S_n for $n \geq 3$. Calculate the product $(123)(124)$ in S_n for $n \geq 4$. Show that, if $n \geq 3$, A_n is generated by the set of all cycles of length 3 in S_n. What happens if $n = 2$ or $n = 1$?

Exercise 18.12. By dint of constant practice, the well known man about town Simon Wendel Indler has reached the point where, given a pack of $2n$ cards, he can execute a 'perfect shuffle' in which the card in rth position in the pack moves to the $2r$th position for $1 \leq r \leq n$ and to the $2(r-n)-1$st position for $n+1 \leq r \leq 2n$.

(i) By using the cycle notation, find how many shuffles does it take him to return the pack to its initial state when $n = 1, 2, 3, 4, 5, 6, 7$? Are there any remarks about particular things for particular n that might be helpful to Mr Indler? Remember that even a small amount of extra information gives a card player a substantial advantage.

(ii) Why does Mr Indler prefer a shuffle in which the card in rth position in the pack moves to the $2r-1$th position for $1 \leq r \leq n$ and to the $2(r-n)$st position for $n+1 \leq r \leq 2n$? (This is called an 'out-shuffle'. The shuffle described in the first paragraph is called an 'in-shuffle'.)

(iii) Show that the in-shuffle can be described using modular arithmetic by saying that the card in position r goes to position k where

$$k \equiv 2r \mod 2n+1.$$

Explain why the pack returns to its original order after $\phi(2n+1)$ shuffles where ϕ is Euler's totient function. Apply this result to a standard pack of 52 cards.

(iv) Now consider the out-shuffle. Show that, if we ignore the first and last cards and renumber the remainder so that what was the $r+1$st card is now the rth card, then the effect of the out-shuffle can be described using modular arithmetic by saying that the card in position r goes to position k where

$$k \equiv 2r \mod 2n-1.$$

Explain why the pack returns to its original order after $\phi(2n-1)$ shuffles where ϕ is Euler's totient function. Apply this result to a standard pack of 52 cards.

(v) Show that, in fact, out-shuffling returns a standard pack of 52 cards to it original state in 8 shuffles (making it a particularly useful shuffle for Mr Indler and for stage magicians). Why is this consistent with the result of (iv)?

(vi) Show that in-shuffling does require at least 52 shuffles to return the pack to its original order. (You should only need 26 easy calculations, or less, to show this. Cunning can replace computation but thinking of cunning tricks takes effort.)

(vii) Is it true that every orbit for an in-shuffle is the same size? Is it true that every orbit for an in-shuffle has a size dividing the size of the orbit of the first card? Can you give an infinite set of integers n such that every orbit for an in-shuffle is the same size? Give reasons.

[Remark: Provided that your in-shuffling is not quite accurate, in-shuffling is a very good way of randomising packs. It has been shown that seven imperfect in-shuffles are sufficient. The study of imperfect shuffles only began a few years ago. It requires probability theory and group theory.]

Exercise 18.13. Consider the following groups:– $(\mathbb{R}\setminus\{0\},\times)$ the non-zero reals under multiplication, $(\mathbb{R}^+,\times)$ the strictly positive reals under multiplication, $(\mathbb{R},+)$ the reals under addition, $(\mathbb{Z},+)$ the integers under addition, $(\mathbb{R}/\mathbb{Z},+)$, $SO(\mathbb{R},2)$ the group of 2×2 orthogonal real matrices of determinant 1 under matrix multiplication, $O(\mathbb{R},2)$ the group of orthogonal real matrices under matrix multiplication. Establish which are isomorphic and which are not.

Exercise 18.14. Let $\mathcal{M}$ be the group of Möbius maps acting on $\mathbb{C}\cup\{\infty\}$. If $\alpha(z)=z^{-1}$ and $\beta z = z+2$, show that $0<|\alpha\beta^r(z)|<1$ whenever $|z|<1$ and r is a non-zero integer. Deduce that, if t is a strictly positive integer and

$r_1, r_2, \ldots, r_t$ are non-zero integers, then $\alpha\beta^{r_1}\alpha\beta^{r_2}\ldots\alpha\beta^{r_t}$ does not lie in the stabiliser of 0.

Does the group generated by α and β contain a non-identity element which lies in the stabiliser of 0? Give a proof or counter-example.

Exercise 18.15. If H is a subgroup of a finite group G and G has twice as many elements as H, show that H is normal in G.

How many elements does the group G_1 of isometries of the cube have, how many does the group G_2 of rotations of a cube have? How many elements does the group G_3 of isometries of the regular tetrahedron have, how many does the group G_4 of rotations of a regular tetrahedron have? Give reasons. By considering the effect of rotations on the diagonals of the cube, or otherwise, show that G_2 is isomorphic to S_4. Give, with reasons, similar isomorphisms of G_3 and G_4 with permutation groups or subgroups.

By colouring opposite faces of the cube in the same colour but otherwise using different colours find a surjective homomorphism from G_2 to S_3 and so a surjective homomorphism from S_4 to S_3. Deduce that S_4 has a normal subgroup with 4 elements.

Exercise 18.16. For each integer c, define $f_c : \mathbb{Z} \to \mathbb{Z}$ by $f_c(k) = k + (-1)^k c$. Show that $\{f_c : c \in \mathbb{Z}\}$ is a subgroup of the group of permutations of $\mathbb{Z}$.

Exercise 18.17. Here is another proof of Lemma 11.17.

(i) Show that every Möbius map has a fixed point. Deduce that every Möbius map is conjugate to a Möbius map which fixes ∞.

(ii) Show that every Möbius map which fixes ∞ either has another fixed point or has the form $z \mapsto z + a$. Deduce that every Möbius map is either conjugate to a Möbius map which fixes ∞ and 0, or is conjugate to map of the form $z \mapsto z + a$.

(iii) Show that every Möbius map is either the identity or is conjugate to map of the form $z \mapsto z + 1$ or is conjugate to map of the form $z \mapsto \lambda z$ with $|\lambda| \geq 1$. Why is the map $z \mapsto z+1$ not conjugate to map of the form $z \mapsto \lambda z$ with $|\lambda| \geq 1$?

(iv) Suppose that $Tz = \lambda z$, $Sz = \mu z$, R is Möbius map and $T = RSR^{-1}$. Show that $Rz = az$ or $Rz = a/z$ (for some $a \neq 0$). Deduce that if $|\mu|$, $|\lambda| \geq 1$ and μ, $\lambda \neq 1$ then either $\lambda = \mu$ or $|\lambda| = |\mu| = 1$ and $\lambda = \mu^*$.

Exercise 18.18. **(The Vandermonde determinant.)** (i) Consider the function $F : \mathbb{R}^3 \to \mathbb{R}$ given by

$$F(x, y, z) = \det \begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{pmatrix}.$$

Explain why F is a multinomial of degree 3. By considering $F(x, x, z)$, show that F has $x-y$ as a factor. Explain why $F(x, y, z) = A(x-y)(y-z)(z-x)$ for some constant A. By looking at the coefficient of yz^2, or otherwise, show that $F(x, y, z) = (x-y)(y-z)(z-x)$.

(ii) Consider the $n \times n$ matrix V with $v_{rs} = x_s^{r-1}$. Show that, if we set

$$F(x_1, x_2, \dots, x_n) = \det V,$$

then

$$F(x_1, x_2, \dots, x_n) = \prod_{i>j} (x_i - x_j).$$

(iii) If $\sigma \in S_n$ and all the x_r are distinct, we set

$$\zeta(\sigma) = \frac{F(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})}{F(x_1, x_2, \dots, x_n)}.$$

Use the rules for calculating determinants to find $\zeta(\sigma)$ when σ is a transposition and when σ is the product of k transpositions.
[Part (iii) shows that we could define signature using determinants but it is more common to define determinants using signature and we must be careful to avoid circularity.]

Exercise 18.19. (i) Show that, if $n \geq 5$, then S_n is generated by 4-cycles (that is to say, cycles of length 4). Can the identity can be written as the product of an odd number of 4-cycles?

(ii) Let $n \geq 3$ and let X be the subset of S_n consisting of those σ with $\sigma 1 = 2$. Show that S_n is generated by X. Can we define a function $\Omega : S_n \to \{-1, 1\}$ by taking $\Omega(\sigma) = (-1)^n$ if σ is the product of n elements of X and their inverses?

(iii) If G is an Abelian group and $T : S_n \to G$ is a homomorphism, what can you say about the image $T(S_n)$?