Algebras and Representations
MATH 3193

Andrew Hubery
ahubery@maths.leeds.ac.uk

An **algebra** is a set A which at the same time has the structure of a ring and a vector space in a compatible way. Thus you can add and multiply elements of A, as well as multiply by a scalar. One example is the set of matrices of size n over a field.

A **representation** is an action of an algebra on a vector space, similar to how matrices of size n act on an n-dimensional vector space. It is often the case that information about the algebra can be deduced from knowing enough about its representations. An analogy might be that one can begin to understand a complicated function by computing its derivatives, or more generally a surface by computing its tangent planes.

There are lots of interesting examples of algebras, with applications to mathematics and physics. In this course we will introduce some of these algebras, as well as some of the general theory of algebras and their representations.

Contents

Part I

Algebras

1 Quaternions

1.1 Complex Numbers

Since the work of Wessel (1799) and Argand (1806) we think of complex numbers as formal expressions

$$z = x + yi \quad \text{with } x, y \in \mathbb{R},$$

which we can add and multiply by expanding out, substituting $i^2 = -1$, and collecting terms. In other words, we have a two-dimensional real vector space $\mathbb{C}$ with basis $\{1, i\}$, on which we have defined a multiplication

$$\mathbb{C} \times \mathbb{C} \to \mathbb{C}$$

satisfying the following properties for all $a, b, c \in \mathbb{C}$ and $\lambda \in \mathbb{R}$:

Associative	$a(bc) = (ab)c$.
Unital	there exists $1 \in \mathbb{C}$ with $1a = a = a1$.
Bilinear	$a(b + \lambda c) = ab + \lambda ac$ and $(+\lambda b)c = ac + \lambda bc$.
Commutative	$ab = ba$.

Complex numbers have wonderful properties, for example:

- The conjugate of $z = x + yi$ is $\bar{z} = x - yi$, and its absolute value is $|z| = \sqrt{x^2 + y^2}$. Thus $|\bar{z}| = |z|$ and $z\bar{z} = |z|^2$. Also, $|zw| = |z||w|$ for all complex numbers z, w.
- Every non-zero complex number $z = x + yi$ has an inverse

  $$z^{-1} = (x - yi)/(x^2 + y^2) = \bar{z}/|z|^2,$$

  so they form a field.
- Rotations of the plane correspond to multiplication by complex numbers of absolute value 1.

1.2 Quaternions

Trying to find a way to represent rotations in three dimensions, Sir William Rowan Hamilton invented the quaternions in 1843. He needed four real numbers, not three, and also had to drop commutativity.

Quaternions are expressions $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$. They add and subtract in the obvious way, and multiply by first expanding out (being careful

with the ordering), making the following substitutions

$$\begin{array}{lll} i^2 = -1 & ij = k & ik = -j \\ ji = -k & j^2 = -1 & jk = i \\ ki = j & kj = -i & k^2 = -1 \end{array}$$

and then collecting terms. For example

$$(2+3i)(i-4j) = 2i - 8j + 3i^2 - 12ij = -3 + 2i - 8j - 12k.$$

The set of all quaternions is denoted $\mathbb{H}$.

In other words we have a four-dimensional real vector space $\mathbb{H}$ with basis $\{1, i, j, k\}$, on which we have defined a multiplication

$$\mathbb{H} \times \mathbb{H} \to \mathbb{H}$$

satisfying the following properties for all $a, b, c \in \mathbb{H}$ and $\lambda \in \mathbb{R}$:

Associative	$a(bc) = (ab)c$.
Unital	there exists $1 \in \mathbb{H}$ with $1a = a = a1$.
Bilinear	$a(b + \lambda c) = ab + \lambda ac$ and $(a + \lambda b)c = ac + \lambda bc$.

Remark. Multiplication of quaternions is *not* commutative:

$$ij = k \quad \text{but} \quad ji = -k, \quad \text{so} \quad ij \neq ji.$$

1.3 Basic Definitions

Let $q = a + bi + cj + dk$ be a quaternion.

We say that the **real part** of q is a, and the **imaginary part** is $bi + cj + dk$. A **pure quaternion** is one whose real part is zero.

The **conjugate** of q is $\bar{q} = a - bi - cj - dk$. Thus if a is a real number and p is a pure quaternion, then the conjugate of $a + p$ is $a - p$.

The **absolute value** of q is $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$. Note that $|\bar{q}| = |q|$.

1.4 Elementary properties

1. If p is a pure quaternion then $p^2 = -|p|^2$. For,

$$\begin{aligned} &(bi + cj + dk)(bi + cj + dk) \\ &\quad = b^2i^2 + c^2j^2 + d^2k^2 + bc(ij + ji) + bd(ik + ki) + cd(jk + kj) \\ &\quad = -(b^2 + c^2 + d^2). \end{aligned}$$

2. Conjugation is a linear map, so

$$\overline{p + \lambda q} = \bar{p} + \lambda \bar{q} \quad \text{for all } p, q \in \mathbb{H} \text{ and } \lambda \in \mathbb{R}.$$

3. Conjugation satisfies

$$\bar{\bar{q}} = q \quad \text{and} \quad \overline{pq} = \bar{q}\,\bar{p} \quad \text{for all} \quad p, q \in \mathbb{H}.$$

The first property is clear, so we just need to prove the second. Since multiplication is bilinear and conjugation is linear, we can reduce to the case when $p, q \in \{1, i, j, k\}$. If $p = 1$ or $q = 1$, then the result is clear, so we may assume that $p, q \in \{i, j, k\}$.

If $p = q$, then $p^2 = -1 = \bar{p}^2$. Otherwise p and q are distinct elements of $\{i, j, k\}$. Let r be the third element. Then $\bar{p} = -p$, and similarly for q and r. Using the multiplication rules we see that $pq = \pm r$ and $qp = \mp r$, so

$$\bar{q}\,\bar{p} = (-q)(-p) = qp = \mp r = \pm\bar{r} = \overline{pq}$$

as required.

4. We have

$$q\bar{q} = \bar{q}q = |q|^2.$$

For, write $q = a + p$ with $a \in \mathbb{R}$ and p a pure quaternion, so that $\bar{q} = a - p$. Then $ap = pa$, so

$$q\,\bar{q} = (a + p)(a - p) = a^2 + pa - ap - p^2 = a^2 - p^2 = (a - p)(a + p) = \bar{q}\,q.$$

Using $p^2 = -|p|^2$ we get

$$q\bar{q} = a^2 - p^2 = a^2 + |p|^2 = |q|^2.$$

5. For any two quaternions p and q we have

$$|pq| = |p||q|.$$

For

$$|pq|^2 = pq\,\overline{pq} = p\,q\,\bar{q}\,\bar{p} = p\,|q|^2\,\bar{p} = |q|^2\,p\,\bar{p} = |q|^2|p|^2.$$

1.5 Lemma

Any non-zero quaternion has a multiplicative inverse; that is, $\mathbb{H}$ is a **division algebra**.

Proof. The inverse of q is $q^{-1} = \bar{q}/|q|^2$. □

1.6 Lemma

Every quaternion can be written in the form

$$q = r\big(\cos(\tfrac{1}{2}\theta) + \sin(\tfrac{1}{2}\theta)n\big)$$

where $r, \theta \in \mathbb{R}$ with $r = |q| \geq 0$ and $\theta \in [0, 2\pi]$, and n is a pure quaternion of absolute value 1.

The use of $\frac{1}{2}\theta$ is traditional; the reason will become clear later.

Proof. If $q = 0$, then this is clear; otherwise $q/|q|$ is a quaternion of absolute value 1.

Now let q have absolute value 1 and write $q = a + p$ with $a \in \mathbb{R}$ and p a pure quaternion. Then

$$1 = |q|^2 = a^2 + |p|^2,$$

so we can write $a = \cos(\frac{1}{2}\theta)$ for some unique $\theta \in [0, 2\pi]$, whence $|p| = \sin(\frac{1}{2}\theta)$. Finally, if $\theta = 0, 2\pi$, then $p = 0$ so we can take n to be arbitrary; otherwise $n = p/|p|$ is a pure quaternion of absolute value 1. □

1.7 Lemma

We may identify the set of pure quaternions $P = \{bi + cj + dk : b, c, d \in \mathbb{R}\}$ with $\mathbb{R}^3$ such that i, j, k correspond respectively to the standard basis vectors e_1, e_2, e_3. We equip $\mathbb{R}^3$ with the usual dot product and cross product. Then

$$pq = -p \cdot q + p \times q \in \mathbb{H} \quad \text{for all } p, q \in P.$$

Note that the dot product of two elements of P is in $\mathbb{R}$, and the cross product is in P, so the sum makes sense in $\mathbb{H}$.

Proof. Each operation is bilinear, so it suffices to check this for $p, q \in \{i, j, k\}$. □

1.8 Theorem

If q is a quaternion of absolute value 1, then the linear transformation

$$R_q \colon P \to P, \quad R_q(p) := qpq^{-1}$$

is a rotation. Explicitly, if $q = \cos(\frac{1}{2}\theta) + \sin(\frac{1}{2}\theta)n$, then $R_q = R_{n,\theta}$ is the rotation about axis n through angle θ.

Two quaternions q, q' of absolute value 1 give the same rotation if and only if $q' = \pm q$.

Proof. Recall that an ordered basis (f_1, f_2, f_3) of $\mathbb{R}^3$ is called a **right-handed orthonormal basis** provided that

$$f_i \cdot f_j = \delta_{ij} \quad \text{and} \quad f_3 = f_1 \times f_2.$$

Also, if $n \in \mathbb{R}^3$ has length 1, then the rotation about axis n through angle θ is the linear map

$$n \mapsto n, \quad u \mapsto \cos(\theta)u + \sin(\theta)v, \quad v \mapsto -\sin(\theta)u + \cos(\theta)v$$

where (n, u, v) is any right-handed orthonormal basis.

Now let q be a quaternion of absolute value 1. By Lemma 1.6 we can write $q = \cos(\frac{1}{2}\theta) + \sin(\frac{1}{2}\theta)n$ with $\theta \in [0, 2\pi]$ and n a pure quaternion of absolute

value 1. Let (n, u, v) be a right-handed orthonormal basis for P. The previous lemma tells us that

$$nu = -n \cdot u + n \times u = v \quad \text{and} \quad un = -u \cdot n + u \times n = -n \times u = -v.$$

Similarly

$$uv = n = -vu \quad \text{and} \quad vn = u = -nv.$$

For simplicity set $c := \cos(\frac{1}{2}\theta)$ and $s := \sin(\frac{1}{2}\theta)$. Now, since $n^2 = -|n|^2 = -1$ we have

$$\begin{aligned} qnq^{-1} &= (c + sn)n(c - sn) = (c + sn)(cn - sn^2) = (c + sn)(cn + s) \\ &= c^2n + cs + csn^2 + s^2n = (cs - cs) + (c^2 + s^2)n = n. \end{aligned}$$

Also

$$\begin{aligned} quq^{-1} &= (c + sn)u(c - sn) = (c + sn)(cu - sun) = (c + sn)(cu + sv) \\ &= c^2u + csv + csnu + s^2nv = (c^2 - s^2)u + 2csv = \cos(\theta)u + \sin(\theta)v \end{aligned}$$

and hence

$$qvq^{-1} = qnuq^{-1} = qnq^{-1}quq^{-1} = \cos(\theta)nu + \sin(\theta)nv = -\sin(\theta)u + \cos(\theta)v.$$

This is the rotation claimed.

Any particular rotation occurs in exactly two ways, as the rotation about axis n through angle θ, and as the rotation about $-n$ through angle $2\pi - \theta$. The latter corresponds to the quaternion

$$\cos(\pi - \tfrac{1}{2}\theta) + \sin(\pi - \tfrac{1}{2}\theta)(-n) = -\cos(\tfrac{1}{2}\theta) - \sin(\tfrac{1}{2}\theta)n = -q. \qquad \square$$

1.9 Remarks (non-examinable)

The set of quaternions of absolute value 1 form a group under multiplication, denoted $Sp(1)$, and it is not hard to see that the map $q \mapsto R_q$ from the previous theorem defines a surjective group homomorphism $R\colon Sp(1) \to SO(3, \mathbb{R})$ to the group of rotations of $\mathbb{R}^3$. This group homomorphism is a *double cover*, meaning that there are precisely two elements of $Sp(1)$ mapping to each rotation in $SO(3, \mathbb{R})$.

In fact, we can say more. A quaternion $q = a + bi + cj + dk$ has absolute value 1 precisely when $a^2 + b^2 + c^2 + d^2 = 1$, so $Sp(1)$ can be thought of as a 3-sphere

$$S^3 = \{(a, b, c, d) \in \mathbb{R}^4 : a^2 + b^2 + c^2 + d^2 = 1\}.$$

Similarly $SO(3, \mathbb{R}) \subset \mathbb{M}_3(\mathbb{R}) \cong \mathbb{R}^9$. Therefore both of these sets have an induced topology on them, and both the multiplication and inversion maps are continuous, so they are *topological groups*. In this set-up the group homomorphism $Sp(1) \to SO(3, \mathbb{R})$ is also continuous.

Let us fix a pure quaternion n of absolute value 1. Then, as θ increases from 0 to 2π, we get a sequence of rotations starting and ending at the identity. The sequence of quaternions, however, starts at 1 but ends at -1. We therefore only

get 4π-periodicity for the quaternions. This is relevant in quantum mechanics for 'spin 1/2' particles like electrons.

We can visualise this by rotating a book held in a hand: a 2π rotation returns the book to its original position, but a 4π rotation is needed to return both the book and the hand to their original positions.

You can read about the 'quaternion machine' in J. Conway and R. Guy, The book of numbers.

2 Algebras

2.1 Definition

Fix a base field K, for example $\mathbb{R}$ or $\mathbb{C}$.

An **algebra over** K, or **K-algebra**, consists of a K-vector space A together with a multiplication

$$A \times A \to A, \quad (a, b) \mapsto ab,$$

satisfying the following properties for all $a, b, c \in A$ and $\lambda \in K$:

Associative	$a(bc) = (ab)c$.
Unital	there exists $1 \in A$ such that $1a = a = a1$.
Bilinear	$a(b + \lambda c) = ab + \lambda(ac)$ and $(a + \lambda b)c = ac + \lambda(bc)$.

Aside. If you have seen the definition of a ring, then you will see that the distributivity axiom has been replaced by the stronger bilinearity axiom. We can do this since our algebra is *a priori* a vector space.

An alternative description would therefore be that A is both a vector space and a ring, and that these structures are compatible in the sense that scalars can always be brought to the front, so $a(\lambda b) = \lambda(ab)$.

2.2 Remarks

1. In the literature, the algebras we consider might be called *unital, associative algebras*. There are other types: *Banach algebras* are usually non-unital; *Lie algebras* and *Jordan algberas* are non-associative.

2. Recall that a vector space V is *finite dimensional* if it has a finite basis. Not all of our algebras will be finite dimensional.

3. There is a very rich theory of *commutative* algebras, where one assumes that the multiplication is commutative, so $ab = ba$ for all $a, b \in A$. This is related to, amongst other things, algebraic geometry and algebraic number theory. In this course we will be concerned with general, non-commutative, algebras.

2.3 Examples

1. K is a 1-dimensional algebra over itself.
2. $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-algebra with basis $\{1, i\}$ as a vector space over $\mathbb{R}$. (It is also a 1-dimensional $\mathbb{C}$-algebra, as in Example 1.)
3. $\mathbb{H}$ is a 4-dimensional $\mathbb{R}$-algebra with basis $\{1, i, j, k\}$. Even though it contains a copy of $\mathbb{C}$, for example with basis $\{1, i\}$, it cannot be considered as a $\mathbb{C}$-algebra since i does not commute with j and k.

2.4 Division algebras

A **division algebra** is a non-zero algebra A in which every non-zero element has a multiplicative inverse; that is, for all $a \neq 0$ there exists a^{-1} such that $aa^{-1} = 1 = a^{-1}a$.

2.5 Lemma

A division algebra has no zero divisors: $ab = 0$ implies $a = 0$ or $b = 0$.

Proof. If $ab = 0$ and $a \neq 0$, then $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$, so $b = 0$. $\square$

2.6 Example

A field is the same as a commutative division algebra. The quaternions form a division algebra, but are not commutative so do not form a field.

2.7 Characteristic

The **characteristic** of a field K is the smallest positive integer n such that $n \cdot 1 = 0 \in K$. If no such n exists, we define the characteristic to be zero.

Examples.

1. The fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic zero.
2. If $p \in \mathbb{Z}$ is a prime, then $\mathbb{F}_p = \mathbb{Z}_p$ is a field of characteristic p.
3. The characteristic of a field is either zero or a prime number. For, if $\mathrm{char}(K) = n$ and $n = ab$ with $1 < a, b < n$, then $ab = n = 0 \in K$, whence either $a = 0 \in K$ or $b = 0 \in K$, contradicting the minimality of n.

2.8 Algebras given by a basis and structure coefficients

One immediate question which arises is how to describe an algebra. We shall give two answers to this question, both having their advantages and disadvantages.

The first answer starts from the fact that A is a vector space, so has a basis $\{e_i : i \in I\}$, and we need to define a bilinear multiplication on A.

Recall that to define a linear map f, we just need to specify the images of a basis, since then $f(\sum_i \lambda_i e_i) = \sum_i \lambda_i f(e_i)$.

Similarly, to define a bilinear map $A \times A \to A$, we just need to specify the products $e_i e_j$ for all i, j. We can then multiply arbitrary elements of A by expanding out:

$$\Big(\sum_i \lambda_i e_i\Big)\Big(\sum_j \mu_j e_j\Big) = \sum_{i,j} \lambda_i \mu_j (e_i e_j).$$

We may display this information in the multiplication table, having rows and columns indexed by the basis elements, writing the product $e_i e_j$ in the i-th row and j-th column. This is essentially what we did when describing the quaternions.

More precisely, each product $e_i e_j$ again lies in A, so can be expressed uniquely as a linear combination of the basis elements. Thus one only needs to define the scalars $c_{ij}^k \in K$, called the **structure coefficients**, such that

$$e_i e_j = \sum_k c_{ij}^k e_k.$$

We next need to ensure that the multiplication is associative and has a unit.

Using that the multiplication is bilinear, it is enough to check associativity for all triples of basis elements. So, our multiplication is associative if and only if $(e_i e_j)e_k = e_i(e_j e_k)$ for all i, j, k. Note that we can express this entirely in terms of the structure constants as

$$\sum_p c_{ij}^p c_{pk}^l = \sum_p c_{ip}^l c_{jk}^p \quad \text{for all } i, j, k, l.$$

Similarly, to check that an element $x = \sum_i \lambda_i e_i$ is a unit, we just need to show that $xe_j = e_j = e_j x$ for all j. In practice, however, it is common to specify in advance that the unit is one of the basis elements, as we did when describing the complex numbers and quaternions.

This method of describing an algebra is analogous to the method of describing a group by giving the set of elements and the multiplication table, and for large-dimensional algebras it is just as unwieldy as it is for large groups.

2.9 Examples

1. The vector space with basis $\{e, f\}$ has a bilinear multiplication given by

   $$ee = e, \quad ef = 0, \quad fe = 0, \quad ff = f.$$

   Is it an algebra? It is associative: we have $e(ee) = e = (ee)e$ and $f(ff) = f = (ff)f$; all other possibilities are zero. It has a unit, namely $e + f$. So yes.

2. The vector space with basis $\{1, a, b\}$ has a bilinear multiplication given by

$$a^2 = a, \quad b^2 = b, \quad ab = 0, \quad ba = b + 1$$

and with 1 a unit. Is it an algebra? We have

$$b(ba) = b(b + 1) = b^2 + b = 2b \quad \text{but} \quad (bb)a = ba = b + 1$$

so no: it is not associative.

2.10 Polynomials

The set $K[X]$ of polynomials in an indeterminate X with coefficients in K forms an algebra by the usual addition and multiplication of polynomials.

This has basis $\{1, X, X^2, X^3, \ldots\}$ (so is infinite dimensional) and multiplication $X^m X^n = X^{m+n}$.

More generally, let A be an algebra. Then there is an algebra $A[X]$ whose elements are polynomials in the indeterminate X with coefficients in A, so of the form $a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$ with $a_i \in A$, and multiplication

$$(a_0 + a_1 X + \cdots + a_m X^m)(b_0 + b_1 X + \cdots + b_n X^n) = \sum_{r=0}^{m+n} \big(\sum_{s=0}^{r} a_s b_{r-s} \big) X^r.$$

Observe that if A has basis e_i and structure coefficients c_{ij}^k, then $A[X]$ has basis $e_i X^m$ and multiplication

$$e_i X^m \cdot e_j X^n = \sum_k c_{ij}^k e_k X^{m+n}.$$

In particular, we can inductively define the polynomial algebra $K[X_1, \ldots, X_r]$ to be $\big(K[X_1, \ldots, X_{r-1}]\big)[X_r]$. This has basis the set of **monomials**

$$\{X_1^{m_1} X_2^{m_2} \cdots X_r^{m_r} : m_1, \ldots, m_r \geq 0\},$$

and multiplication

$$\big(X_1^{m_1} \cdots X_r^{m_r}\big) \cdot \big(X_1^{n_1} \cdots X_r^{n_r}\big) = X_1^{m_1+n_1} \cdots X_r^{m_r+n_r}.$$

2.11 Matrix algebras

The set of all $n \times n$ matrices with entries in K forms an algebra $\mathbb{M}_n(K)$. For $a \in \mathbb{M}_n(K)$ we write $a = (a_{pq})$, where $a_{pq} \in K$ and $1 \leq p, q \leq n$. Addition, scalar multiplication and matrix multiplication are as usual:

$$(a + \lambda b)_{pq} = a_{pq} + \lambda b_{pq}, \quad (ab)_{pq} = \sum_r a_{pr} b_{rq}.$$

The unit is the identity matrix, denoted 1 or I, or 1_n or I_n if we want to emphasise the size of the matrices.

The elementary matrices E_{pq} have a 1 in the (p,q)-th place and 0s elsewhere. They form a basis for $\mathbb{M}_n(K)$, so this algebra has dimension n^2. The multiplication is then given by $E_{pq}E_{rs} = \delta_{qr}E_{ps}$.

More generally, if A is an algebra, then the set of $n \times n$ matrices with elements in A forms an algebra $\mathbb{M}_n(A)$. The addition and multiplication are given by the same formulae, but where we now take $a_{pq} \in A$. If A has basis $\{e_i : i \in I\}$ and structure coefficients c_{ij}^k, then $\mathbb{M}_n(A)$ has basis the matrices e_iE_{pq}, having the single non-zero entry e_i in position (p,q), and multiplication

$$e_iE_{pq} \cdot e_jE_{rs} = \sum_k c_{ij}^k \delta_{qr} e_k E_{ps}.$$

Note that if A is finite dimensional, then $\dim \mathbb{M}_n(A) = n^2 \dim A$.

2.12 Endomorphism algebras

More abstractly let V be a vector space. Recall that, after fixing a basis for V, we can represent every linear map $f\colon V \to V$ as a matrix. It is sometimes convenient not to have to choose a basis, in which case we consider the set of all such linear maps, called **endomorphisms** and denoted $\mathrm{End}(V)$. This is again a vector space, with addition and scalar multiplication given by

$$(f + \lambda g)(v) := f(v) + \lambda g(v) \quad \text{for all } v \in V,$$

where $f, g \in \mathrm{End}(V)$ and $\lambda \in K$.

Composition of linear maps now defines a bilinear multiplication on $\mathrm{End}(V)$, so

$$(fg)(v) = f(g(v)) \quad \text{for } f, g \in V \text{ and } v \in V.$$

This is an algebra with unit the identity map $\mathrm{id}_V(v) = v$. (It is associative since composition of functions is always associative.)

2.13 Group algebras

One interesting way of defining an algebra is to start with a group G and take KG to be the vector space with basis indexed by the elements of G, so the set $\{e_g : g \in G\}$. We now use the multiplication on G to define a bilinear multiplication on KG:

$$e_g \cdot e_h := e_{gh}.$$

Since the multiplication for G is associative, it is easy to see that the multiplication for KG is also associative. Moreover, the unit for KG is the basis element indexed by the identity element of G, so $1 = e_1$.

This is easiest to see in an example. Let G be the cyclic group of order 3 with generator g, so that $G = \{1, g, g^2\}$ with $g^3 = 1$. Then the elements of KG are linear combinations $\lambda + \mu e_g + \nu e_{g^2}$ with $\lambda, \mu, \nu \in K$, and as an example of the multiplication we have

$$\begin{aligned}(1 + 2e_g + 5e_{g^2})(2 + e_{g^2}) &= 2 + 4e_g + 10e_{g^2} + e_{g^2} + 2e_ge_{g^2} + 5e_{g^2}e_{g^2} \\ &= 2 + 4e_g + 10e_{g^2} + 2 + 5e_g \\ &= 4 + 9e_g + 11e_{g^2}.\end{aligned}$$

In general we can compute that

$$(\lambda 1 + \mu e_g + \nu e_{g^2}) \cdot (\lambda' 1 + \mu' e_g + \nu' e_{g^2}) \\ = (\lambda\lambda' + \mu\nu' + \nu\mu')1 + (\lambda\mu' + \mu\lambda' + \nu\nu')e_g + (\lambda\nu' + \mu\mu' + \nu\lambda')e_{g^2}.$$

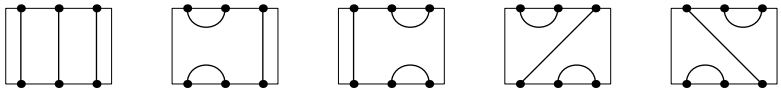
2.14 Temperley-Lieb algebras

Another interesting way of defining algebras is to index the basis elements by certain types of diagrams and then to describe the multiplication in terms of these diagrams. Such algebras are referred to as **diagram algebras**.

The Temperley-Lieb algebra $TL_n(\delta)$ for $n \geq 1$ and $\delta \in K$ has basis indexed by diagrams having two rows of n dots, one above the other, connected by n non-intersecting curves. Two such diagrams are considered equal if the same vertices are connected.

To define the multiplication ab of two basis elements, we first stack the diagram for a on top of that for b, and then concatenate the curves. The resulting diagram may contain some loops which we must remove, and we multiply by the scalar δ for each such loop that we remove.

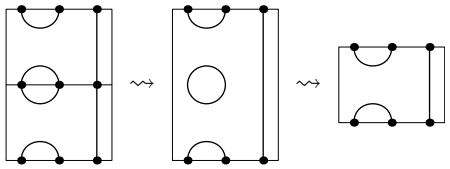
This is again easiest to understand once we have seen an explicit example. For the algebra $TL_3(\delta)$ we have the following diagrams



1 u_1 u_2 p q

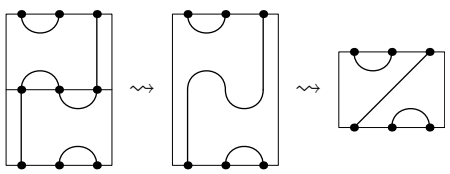
We have written the corresponding basis elements under the diagrams, so $TL_3(\delta)$ has basis $\{1, u_1, u_2, p, q\}$.

To compute the product u_1^2 we take two copies of the appropriate diagram, stacked one above the other, then join curves and remove loops:



Since we had to remove one loop, we deduce that $u_1^2 = \delta u_1$.

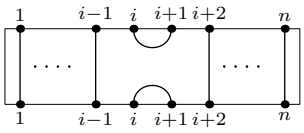
Similarly $u_1 u_2 = p$, since



It is hopefully clear that the basis element 1 is indeed a unit for the algebra. In general the unit is the basis element indexed by the diagram given by joining the dots vertically, so the i-th dot on the top row is joined to the i-th dot on the bottom row.

We can also use the diagrams to see that the multiplication is associative; for, if we take three diagrams stacked one on top of the other, then joining the curves of the top two diagrams, and then joining them with the third is the same as joining the bottom two together, and then joining with the top diagram. In fact, both operations agree with simply joining all three diagrams together in one go. This proves that the multiplication is associative when restricted to three basis elements, and hence is associative.

In general we define $u_i \in TL_n(\delta)$ for $1 \leq i < n$ to be the diagram



so we have joined togther the i-th and $(i+1)$-st dots on the top row, and the same on the bottom row; all other dots on the top row are joined to their counterparts on the bottom row.

Then the following relations always hold

$$u_i^2 = \delta u_i, \quad u_i u_{i\pm 1} u_i = u_i \quad \text{and} \quad u_i u_j = u_j u_i \text{ if } |i-j| > 1.$$

In fact, in a certain sense (which we will make precise later), these relations are sufficient to completely determine the Temperley-Lieb algebra. (See Exercise Sheet 1, Question 6.)

Remark. The Temperley-Lieb algebra was invented to study Statistical Mechanics (see for example Paul Martin's homepage). It is now also important in Knot Theory, and Vaughan Jones won a Fields Medal in 1990 for his work in this area.

2.15 Direct Product of Algebras

Let A and B be algebras. Since they are *a priori* vector spaces, we may form their Cartesian product, or direct product, $A \times B$ and this is again a vector space, with addition and scalar multiplication given by

$$(a,b) + \lambda(a',b') = (a + \lambda a', b + \lambda b').$$

We give $A \times B$ the structure of an algebra via the following multiplication

$$(a,b)(a',b') = (aa', bb').$$

It is easy to check that this is associative and bilinear. Moreover the multiplication is unital, with unit $1 = (1_A, 1_B)$.

3 Homomorphisms and Subalgebras

3.1 Homomorphisms

A map $f : A \to B$ between algebras is an **(algebra) homomorphism** if

(a) f is a linear map.

(b) $f(aa') = f(a)f(a')$ for all $a, a' \in A$.

(c) $f(1_A) = 1_B$.

In other words, f is a linear map which **respects the multiplication** and **preserves the unit**.

Note that if (b) holds, then condition (c) is equivalent to:

(c') There is some $a \in A$ with $f(a) = 1_B$.

For, if $f(a) = 1_B$, then

$$1_B = f(a) = f(a1_A) = f(a)f(1_A) = 1_B f(1_A) = f(1_A).$$

If $f\colon A \to B$ and $g\colon B \to C$ are algebra homomorphisms, then so too is their composition $gf\colon A \to C$.

An **isomorphism** is a homomorphism $f\colon A \to B$ which has an inverse, so there is a homomorphism $g\colon B \to A$ with both $gf = \mathrm{id}_A$ and $fg = \mathrm{id}_B$. It is a useful fact that f is an isomorphism if and only if it is a bijection.

If there is an isomorphism $A \to B$, we say that A and B are **isomorphic** and write $A \cong B$.

3.2 Subalgebras

A **subalgebra** B of an algebra A, written $B \leq A$, is a vector subspace **closed under multiplication** and **containing the unit**:

(a) B is a subspace.

(b) $bb' \in B$ for all $b, b' \in B$.

(c) $1_A \in B$.

It follows that, using the induced multiplication, B is an algebra in its own right.

3.3 Lemma

If $f\colon B \to A$ is an algebra homomorphism, then its image $\mathrm{Im}(f)$ is a subalgebra of A. Conversely, if $B \leq A$ is a subalgebra, then the inclusion map $B \hookrightarrow A$ is an algebra homomorphism.

In other words, subalgebras are the same as images of algebra homomorphisms.

Proof. Let $f\colon B \to A$ be an algebra homomorphism. Since f is a linear map, we know that its image is a subspace. It contains the identity since $f(1_B) = 1_A$, and it is closed under multiplication since $f(a)f(a') = f(aa')$.

Conversely, let $B \leq A$ be a subalgebra. Then the inclusion map $B \hookrightarrow A$ is the restriction to B of the identity map $\mathrm{id}_A\colon A \to A$, and hence is an algebra homomorphism. □

3.4 Example

If K is a field and A a K-algebra, then there is a unique algebra homomorphism $K \to A$, sometimes called the **structure map**. This sends the scalar $\lambda \in K$ to the element $\lambda 1_A \in A$.

For example, if $A = \mathbb{M}_n(K)$, then the structure map sends λ to the diagonal matrix λI_n.

3.5 Example

The set of upper-triangular matrices

$$U = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in \mathbb{M}_2(K) : x, y, z \in K \right\}$$

is a subalgebra of $\mathbb{M}_2(K)$. For

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} + \lambda \begin{pmatrix} x' & y' \\ 0 & z' \end{pmatrix} = \begin{pmatrix} x + \lambda x' & y + \lambda y' \\ 0 & z + \lambda z' \end{pmatrix} \in U$$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} x' & y' \\ 0 & z' \end{pmatrix} = \begin{pmatrix} xx' & xy' + yz' \\ 0 & zz' \end{pmatrix} \in U$$

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

Two more examples of subalgebras of $\mathbb{M}_2(K)$ are

$$B = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} : x, y \in K \right\} \quad \text{and} \quad C = \left\{ \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} : x, z \in K \right\}.$$

In fact, B and C are both subalgebras of U.

3.6 Example

Let $A \leq \mathbb{M}_m(K)$ and $B \leq \mathbb{M}_n(K)$ be subalgebras. Then the direct product $A \times B$ is isomorphic to the subalgebra of $\mathbb{M}_{m+n}(K)$ consisting of block-diagonal matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \mathbb{M}_{m+n}(K), \quad a \in \mathbb{M}_m(K) \text{ and } b \in \mathbb{M}_n(K).$$

3.7 Examples

1. Recall that we can view $\mathbb{C}$ as an algebra over $\mathbb{Q}$. Given any element $z \in \mathbb{C}$ there is a $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}[X] \to \mathbb{C}$ sending $X^n \mapsto z^n$. This is called the **evaluation map** and is denoted ev_z.

2. Recall that both $\mathbb{C}$ and $\mathbb{H}$ are algebras over $\mathbb{R}$. Then the $\mathbb{R}$-linear map $\mathbb{C} \to \mathbb{H}$ sending $x + yi \in \mathbb{C}$ to $x + yi \in \mathbb{H}$ is an $\mathbb{R}$-algebra homomorphism. In fact, if $p \in \mathbb{H}$ is any pure quaternion of absolute value 1, then there is an algebra homomorphism $\mathbb{C} \to \mathbb{H}$ such that $i \mapsto p$.

3. Let A and B be algebras, and consider their direct product $A \times B$. The projection map
$$\pi_A \colon A \times B \to A, \quad (a, b) \mapsto a$$
is then a surjective algebra homomorphism, and similarly for the projection map $\pi_B \colon A \times B \to B$.

   Note, however, that the inclusion map
$$\iota_A \colon A \to A \times B, \quad a \mapsto (a, 0)$$
is *not* an algebra homomorphism.

3.8 Lemma

Let A be an algebra with basis $\{e_i : i \in I\}$ and structure coefficients
$$e_i e_j = \sum_k c_{ij}^k e_k.$$
Then an algebra B is isomorphic to A if and only if B has a basis $\{f_i : i \in I\}$ with the same structure coefficients:
$$f_i f_j = \sum_k c_{ij}^k f_k.$$

Proof. If $\theta : A \to B$ is an algebra homomorphism, then defining $f_i = \theta(e_i)$ gives
$$f_i f_j = \theta(e_i)\theta(e_j) = \theta(e_i e_j) = \theta\big(\sum_k c_{ij}^k e_k\big) = \sum_k c_{ij}^k \theta(e_k) = \sum_k c_{ij}^k f_k.$$
Conversely, given basis elements $f_i \in B$ satisfying $f_i f_j = \sum_k c_{ij}^k f_k$, let $\theta : A \to B$ be the linear map sending e_i to f_i. Then
$$\theta(e_i)\theta(e_j) = f_i f_j = \sum_k c_{ij}^k f_k = \sum_k c_{ij}^k \theta(e_k) = \theta\big(\sum_k c_{ij}^k e_k\big) = \theta(e_i e_j),$$
so by bilinearity $\theta(a)\theta(a') = \theta(aa')$ for all $a, a' \in A$.

Now θ satisfies (a) and (b) and is bijective, so also satisfies (c'). Hence it is a bijective algebra homomorphism, so an isomorphism. □

3.9 Example

The algebra A with basis $\{e, f\}$ and multiplication

$$e^2 = e, \quad f^2 = f, \quad ef = fe = 0$$

is isomorphic to the algebra B with basis $\{1, u\}$ and multiplication $u^2 = u$.

For, A has unit $1 = e + f$, so has basis $\{1, e\}$ with $e^2 = e$.

Alternatively, B has basis

$$E := u, \quad F = 1 - u,$$

and these satisfy

$$E^2 = u^2 = u = E, \qquad EF = u(1-u) = u - u^2 = 0,$$
$$F^2 = (1-u)^2 = 1 - 2u + u^2 = 1 - u = F, \qquad FE = (1-u)u = 0.$$

3.10 Lemma

The vector space isomorphism $\Theta\colon \mathrm{End}_K(K^n) \xrightarrow{\sim} \mathbb{M}_n(K)$ sending a linear map to its matrix, is an algebra isomorphism.

Proof. Recall that the matrix $a_{ij})$ of $f \in \mathrm{End}_K(K^n)$ is determined by $f(e_j) = \sum_i a_{ij}e_i$. Clearly $\Theta(\mathrm{id}) = I$, so we just need to check that Θ respects the multiplication.

Suppose $\Theta(f) = a = (a_{ij})$ and $\Theta(g) = b = (b_{ij})$. Then

$$(fg)(e_j) = f(g(e_j) = f\big(\sum_p b_{pj}e_p\big) = \sum_p b_{pj}f(e_p)$$
$$= \sum_{i,p} b_{pj}a_{ip}e_i = \sum_i \big(\sum_p a_{ip}b_{pj}\big)e_i.$$

Hence $\Theta(fg)$ is the matrix $\big(\sum_p a_{ip}b_{pj}\big) = ab$, so $\Theta(fg) = \Theta(f)\Theta(g)$. □

3.11 Lemma

A vector space isomorphism $\theta\colon V \xrightarrow{\sim} W$ induces an algebra isomorphism

$$\Theta\colon \mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{End}_K(W), \quad \Theta(f) := \theta f \theta^{-1}.$$

Proof. We note that Θ is linear, since

$$\Theta(f + \lambda g) = \theta(f + \lambda g)\theta^{-1} = \theta f\theta^{-1} + \lambda\theta g\theta^{-1} = \Theta(f) + \lambda\Theta(g).$$

Moreover

$$\Theta(f)\Theta(g) = (\theta f\theta^{-1})(\theta g\theta^{-1}) = \theta fg\theta^{-1} = \Theta(fg)$$

and

$$\Theta(\mathrm{id}_V) = \theta\mathrm{id}_V\theta^{-1} = \theta\theta^{-1} = \mathrm{id}_W,$$

so that Θ respects the multiplication and preserves the unit. Hence Θ is an algebra homomorphism, and it is an isomorphism since it clearly has inverse

$$\Theta^{-1}\colon \mathrm{End}_K(W) \to \mathrm{End}_K(V), \quad h \mapsto \theta^{-1}h\theta. \qquad \square$$

As a special case, let V be a finite-dimensional vector space. Choosing a basis $\{e_1, \ldots, e_n\}$ for V is equivalent to choosing a vector space isomorphism $V \to K^n$, which then induces an algebra isomorphism $\mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{End}_K(K^n) \cong \mathbb{M}_n(K)$. This is just the map sending a linear map to its matrix with respect to the basis $\{e_1, \ldots, e_n\}$.

3.12 Intersections and generating sets

Let S and T be subalgebras of an algebra A. Then the vector space intersection $S \cap T$ is again a subalgebra of A.

Proof. We know that $S \cap T$ is a subspace of A, and clearly $1 \in S \cap T$. If $x, y \in S \cap T$, then $x, y \in S$ so $xy \in S$, and similarly $x, y \in T$ so $xy \in T$. Thus $xy \in S \cap T$ proving that $S \cap T$ is a subalgebra. $\square$

More generally, if S_j is a collection of subalgebras, then $\bigcap_j S_j$ is again a subalgebra. In particular, it is now possible to define the *smallest* subalgebra containing any subset $X \subset A$ — we just consider the intersection of all such subalgebras containing X. We call this the **subalgebra generated by** X. The elements of this subalgebra are all finite linear combinations of products of elements from X, so finite sums of things of the form

$$\lambda x_1 x_2 \cdots x_r \quad \text{with } \lambda \in K \text{ and } x_i \in X.$$

In particular, we say that X is a **generating set** for the algebra A provided that the only subalgebra containing X is A itself.

3.13 Examples

1. $\mathbb{C}$ is generated as an $\mathbb{R}$-algebra by i.
2. $\mathbb{H}$ is generated as an $\mathbb{R}$-algebra by i, j. For, $k = ij$.
3. K is generated as a K-algebra by the empty set.
4. $\mathbb{M}_2(K)$ is generated by E_{12}, E_{21}. For, $E_{11} = E_{12}E_{21}$ and $E_{22} = E_{21}E_{12}$.
5. The polynomial algebra $K[X_1, \ldots, X_n]$ is generated by $X_1, \ldots, X_n$.
6. The Temperley-Lieb algebra $TL_3(\delta)$ is generated by u_1 and u_2. For, it has basis $\{1, u_1, u_2, p, q\}$, and $p = u_1u_2$ and $q = u_2u_1$.

   In fact $TL_n(\delta)$ is generated by $u_1, \ldots, u_{n-1}$, though this is not obvious.
7. The algebra of upper-triangular matrices $U_n \leq \mathbb{M}_n(K)$ is generated by the elementary matrices E_{ii} and E_{ii+1} for $1 \leq i < n$.

3.14 Example

What is the subalgebra A of $\mathbb{M}_3(K)$ generated by

$$a := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}?$$

It is the subspace of $\mathbb{M}_3(K)$ spanned by $\{1, a, a^2, a^3, \ldots\}$. Setting $b = a - 1$ we see that A is also spanned by $\{1, b, b^2, \ldots\}$, so is generated by b. Now

$$1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad b^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad b^3 = 0.$$

Thus the subalgebra generated by a (or b) is

$$A = \left\{ \begin{pmatrix} x & y & z \\ 0 & x & y \\ 0 & 0 & x \end{pmatrix} : x, y, z \in K \right\}.$$

4 Ideals

Let $\theta\colon A \to B$ be a homomorphism of algebras. We have just seen that the image $\mathrm{Im}(\theta)$ is a subalgebra of B, but what about its kernel? Provided that B is not the zero algebra we have $\theta(1_A) = 1_B \neq 0$. Hence $1_A \notin \mathrm{Ker}(\theta)$ and so $\mathrm{Ker}(\theta)$ cannot be a subalgebra of A.

On the other hand, $\mathrm{Ker}(\theta)$ is closed under multiplication by *any* element of A. For, if $x \in \mathrm{Ker}(\theta)$ and $a \in A$, then

$$\theta(ax) = \theta(a)\theta(x) = 0 \quad \text{and} \quad \theta(xa) = \theta(x)\theta(a) = 0,$$

so $ax, xa \in \mathrm{Ker}(\theta)$.

4.1 Definition

A **(two-sided) ideal** I of an algebra A, denoted $I \lhd A$, is a subset I satisfying

(a) I is a vector subspace of A.

(b) $ax \in I$ for all $a \in A$ and $x \in I$.

(c) $xa \in I$ for all $a \in A$ and $x \in I$.

4.2 Remarks

1. $I = \{0\}$ (the zero ideal) and $I = A$ (the unit ideal) are always ideals of A.

2. There is also the notion of a **left ideal**, for which one only demands (a) and (b), and a **right ideal**, satisfying only (a) and (c). If A is commutative, then these are all the same.

3. If $\theta\colon A \to B$ is an algebra homomorphism, then $\mathrm{Ker}(\theta)$ is an ideal in A.

4.3 Examples

1. The set of polynomials having zero constant term forms an ideal of $K[X]$.

2. Let A and B be ideals, and consider their direct product $A \times B$. We saw earlier that the projection map $\pi_A\colon A \times B \to A$, $(a, b) \mapsto a$, is a surjective algebra homomorphism. Its kernel is $\{(0, b) : b \in B\}$, which is an ideal of $A \times B$.

3. More generally let $I \lhd A$ and $J \lhd B$ ideals. Then the set

$$I \times J = \{(x, y) : x \in I,\ y \in J\}$$

is an ideal of $A \times B$. For, it is easily seen to be a vector subspace, so we just need to check that it is closed under multiplication by elements of $A \times B$. Let $(a, b) \in A \times B$ and $(x, y) \in I \times J$. Since $ax, xa \in I$ and $by, yb \in J$, we deduce that $(a, b)(x, y) = (ax, by)$ and $(x, y)(a, b) = (xa, yb)$ are both in $I \times J$ as required.

We will see in the exercises that every ideal if $A \times B$ is of this form.

4. Let A be an algebra and $I \lhd A$ an ideal. Then the set

$$\mathbb{M}_n(I) = \{(x_{ij}) : x_{ij} \in I\}$$

is an ideal of $\mathbb{M}_n(A)$, and in fact every ideal of $\mathbb{M}_n(A)$ is of this form.

4.4 Example

Let $U = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\}$ be the algebra of upper-triangular matrices.

1. Is $I := \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \right\}$ an ideal?

   No, since $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \notin I$. (It is only a left ideal.)

2. Is $J := \left\{ \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \right\}$ an ideal?

   Yes. It is a subspace, satisfies (b) since $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ay \\ 0 & 0 \end{pmatrix} \in Y$, and similarly satisfies (c).

3. In fact, $0, J, U$ are the only ideals of U.

4.5 Lemma

If an ideal contains 1, or any invertible element, then it is the unit ideal. In particular, the only ideals in a division algebra are the zero ideal and the unit ideal.

Proof. If I contains an invertible element b, then it also contains $b^{-1}b = 1$, and hence also $a1 = a$ for any $a \in A$. □

4.6 Sums and intersections of ideals

Let I and J be ideals of an algebra A. Then the vector space constructions

$$I + J \quad \text{and} \quad I \cap J$$

are again ideals of A.

Proof. We know that $I + J$ and $I \cap J$ are both subspaces of A. Take $x \in I$, $y \in J$ and $a \in A$. Then

$$ax, xa \in I \quad \text{and} \quad ay, ya \in J,$$

so that

$$a(x + y) = ax + ay \in I + J \quad \text{and} \quad (x + y)a = xa + ya \in I + J.$$

Hence $I + J$ is an ideal.

Similarly, if $x \in I \cap J$ and $a \in A$, then

$$ax, xa \in I \quad \text{and} \quad ay, ya \in J, \quad \text{so} \quad ax, xa \in I \cap J.$$

Hence $I \cap J$ is an ideal. □

More generally, if I_j is a collection of ideals, then $\sum_j I_j$ and $\bigcap_j I_j$ are again ideals. In particular, it is now possible to define the *smallest* ideal containing any subset $X \subset A$ — we just consider the intersection of all such ideals containing X. We call this the **ideal generated by** X, and denote it by (X). The elements of (X) are all possible finite linear combinations of the form

$$a_1 x_1 b_1 + \cdots + a_n x_n b_n \quad \text{with} \quad a_i, b_i \in A \text{ and } x_i \in X.$$

As a special case we have the **principal ideal** (x).

We remark that these constructions also work for left (and right) ideals.

4.7 Examples

1. Let U be the algebra of upper-triangular 3×3 matrices. What is (E_{22}), the ideal generated by E_{22}?

Since U has basis E_{ij} for $i \leq j$, we see that (E_{22}) is spanned by the elements $E_{ij}E_{22}E_{pq} = \delta_{2j}\delta_{2p}E_{iq}$ for all $i \leq j$ and $p \leq q$. The only non-zero elements occur when $j = p = 2$, and hence $i \in \{1, 2\}$ and $q \in \{2, 3\}$. Thus (E_{22}) is spanned by the four elements $E_{12}, E_{13}, E_{22}, E_{23}$, so

$$(E_{22}) = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & d & e \\ 0 & 0 & 0 \end{pmatrix} : b, c, d, e \in K \right\}.$$

2. Let $A = \mathbb{M}_3(K)$. What is (E_{22})?

   This time A has basis E_{ij} for all i, j. Thus (E_{22}) contains $E_{i2}E_{22}E_{2j} = E_{ij}$, so it equals the whole of A.

   In fact, the zero ideal and the unit ideal are the only ideals of $\mathbb{M}_n(K)$.

3. It is an important fact that every ideal of $K[X]$ is principal. In fact, each non-zero ideal can be written uniquely as (f) for some monic polynomial f (so having leading coefficient 1).

4.8 Products of ideals

Let I and J be ideals of A. We define the ideal IJ to be the smallest ideal containing the set $\{xy : x \in I,\ y \in J\}$. Since $ax \in I$ for all $a \in A$ and $x \in I$, and similarly $yb \in J$ for all $b \in A$ and $y \in J$, we see that every element of IJ can be written as a finite sum of products xy for $x \in I$ and $y \in J$.

Clearly $IJ \subset I \cap J$, but in general this inclusion is strict.

We now observe that this product is associative. For, if I, J, L are ideals of A, then $(IJ)L$ is the smallest ideal containing all products $(xy)z$ for $x \in I$, $y \in J$ and $z \in L$. Since the multiplication in A is associative we have $(xy)z = x(yz)$, and hence $(IJ)L = I(JL)$.

More generally, given a finite set of ideals $I_1, \ldots, I_n$ of A, we can define their product inductively as $I_1 I_2 \cdots I_n = (I_1 \cdots I_{n-1})I_n$.

As special cases we observe that $AI = I = IA$ and $0I = 0 = I0$ for all ideals $I \lhd A$.

4.9 Lemma

Let I, J and L be ideals. Then $I(J + L) = IJ + IL$ and $(I + J)L = IL + JL$.

Proof. Since $J, L \subset J+L$ we must have $IJ, IL \subset I(J+L)$, and hence $IJ+IL \subset I(J + L)$. Conversely, $I(J + L)$ is the smallest ideal containing all elements of the form $x(y+z)$ for $x \in I$, $y \in J$ and $z \in L$. Since $x(y+z) = xy+xz \in IJ+IL$ we have $I(J + L) \subset IJ + IL$.

The proof for $(I + J)L = IL + JL$ is analogous. □

5 Quotient Algebras

Recall that if V is a vector space and $U \leq V$ a subspace, then we can form the quotient vector space V/U. This has elements the cosets $v + U$ for $v \in V$, so that $v + U = v' + U$ if and only if $v - v' \in U$. The addition and scalar multiplication are given by

$$(v+U)+(v'+U) = (v+v')+U \quad \text{and} \quad \lambda(v+U) = \lambda v+U \quad \text{for } v, v' \in V,\ \lambda \in K.$$

Moreover the natural map $\pi\colon V \to V/U$, $v \mapsto v + U$, is a surjective linear map with kernel U.

One important result is then the Factor Lemma, which states that if $f\colon V \to W$ is a linear map of vector spaces such that $U \subset \mathrm{Ker}(f)$, then there is a unique linear map $\bar{f}\colon V/U \to W$ such that $f = \bar{f}\pi$. In other words, the map f factors through the quotient space V/U.

In this section we show how these ideas can be extended to algebras and algebra homomorphisms.

5.1 Lemma

If I is an ideal in an algebra A, then the vector space quotient A/I becomes an algebra via the multiplication

$$(A/I) \times (A/I) \to A/I, \quad (a + I, b + I) \mapsto ab + I.$$

Clearly this has unit $1+I$. Moreover the natural map $\pi\colon A \to A/I$ is a surjective algebra homomorphism with kernel I.

In other words, ideals are the same as kernels of homomorphisms.

Proof. We first need to check that the multiplication is well-defined; that is, if $a + I = a' + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$. We can rewrite this as saying if $a - a', b - b' \in I$, then $ab - a'b' \in I$. This holds since

$$ab - a'b' = a(b - b') + (a - a')b \in AI + IA \subset I.$$

The product is clearly associative and bilinear (since it is induced from the product in A), and $1 + I$ is a unit. Thus A/I is an algebra. The natural map is easily seen to be an algebra homomorphism, since it is surjective and $\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$. □

5.2 Factor Lemma

Let $f\colon A \to B$ be a homomorphism of algebras, and $I \subset \mathrm{Ker}(f)$ an ideal of A. Then there is a unique algebra homomorphism $\bar{f}\colon A/I \to B$ such that $f = \bar{f}\pi$.

Proof. Using the Factor Lemma for vector spaces we know that there is a unique linear map $\bar{f}\colon A/I \to B$ such that $f = \bar{f}\pi$. We therefore only need to check that $\bar{f}$ is an algebra homomorphism.

Note that $\bar{f}(a+I) = \bar{f}\pi(a) = f(a)$, so

$$\bar{f}(a+I)\bar{f}(a'+I) = f(a)f(a') = f(aa') = \bar{f}(aa'+I),$$

and similarly $\bar{f}(1+I) = f(1) = 1$. □

5.3 Example

The quotient algebra $\mathbb{R}[X]/(X^2+1)$ is isomorphic to $\mathbb{C}$.

For, consider the evaluation map

$$\theta = \mathrm{ev}_i \colon \mathbb{R}[X] \to \mathbb{C}, \quad X \mapsto i.$$

This is clearly surjective, since $a+bX \mapsto a+bi$. Moreover $\theta(X^2+1) = i^2+1 = 0$, so $X^2+1 \in \mathrm{Ker}(\theta)$. Since $\mathrm{Ker}(\theta)$ is an ideal, we deduce that $(X^2+1) \subset \mathrm{Ker}(\theta)$. By the Factor Lemma we now have an induced algebra homomorphism $\bar{\theta} \colon \mathbb{R}[X]/(X^2+1) \to \mathbb{C}$, and this is still surjective.

The easiest way to complete the proof is to use a dimension argument. We know that $\mathbb{C}$ is a two-dimensional real vector space. Since $\bar{\theta}$ is surjective, we must have that $\mathbb{R}[X]/(X^2+1)$ is at least two dimensional. On the other hand, by the Division Algorithm, any polynomial $f(X) \in \mathbb{R}[X]$ can be written uniquely as $f(X) = (a+bX) + (X^2+1)q(X)$ for some $q(X) \in \mathbb{R}[X]$ and $a, b \in \mathbb{R}$. Thus $\mathbb{R}[X]/(X^2+1)$ is spanned by the images of 1 and X, so is at most two dimenisonal.

We deduce that $\mathbb{R}[X]/(X^2+1)$ is two dimensional, and hence that $\bar{\theta}$ is an isomorphism.

5.4 Example

Let U be the algebra of upper-triangular 3×3 matrices

$$\begin{pmatrix} x & u & w \\ 0 & y & v \\ 0 & 0 & z \end{pmatrix}$$

and let $I \lhd U$ be the ideal of matrices of shape

$$\begin{pmatrix} 0 & 0 & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now U has basis E_{ij} for $1 \le i \le j \le 3$ and I is spanned by E_{13}. Thus U/I has basis

$$f_1 := E_{11}+I,\ f_2 = E_{22}+I,\ f_3 = E_{33}+I,\ f_4 = E_{12}+I,\ f_5 = E_{23}+I,$$

and multiplication table

	f_1	f_2	f_3	f_4	f_5
f_1	f_1	0	0	f_4	0
f_2	0	f_2	0	0	f_5
f_3	0	0	f_3	0	0
f_4	0	f_4	0	0	0
f_5	0	0	f_5	0	0

For example,

$$f_4 f_5 = (E_{12} + I)(E_{23} + I) = E_{12}E_{23} + I = E_{13} + I = 0 + I,$$

since $E_{13} \in I$.

Note that $E_{11} + E_{22} + E_{33}$ is the unit in U, so $f_1 + f_2 + f_3$ is the unit in U/I.

5.5 Lemma

Let A be an algebra, $S \leq A$ a subalgebra and $I \lhd A$ an ideal. Suppose that $A = S \oplus I$ as vector spaces. Then $\pi\colon A \to A/I$ induces an isomorphism $S \cong A/I$.

Proof. Let $\theta\colon S \to A/I$ be the restriction of π to S. The kernel is $S \cap I = \{0\}$, so θ is injective. Also, since any $a \in A$ can be written as $s + x$ with $s \in S$ and $x \in I$, we have $a + I = (s + x) + I = s + I = \theta(s)$, so that θ is surjective. □

5.6 Examples

1. Let U be the algebra of upper-triangular 3×3 matrices. Let $J \lhd U$ be the ideal of matrices of shape

$$\begin{pmatrix} 0 & u & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

   Then U/J is isomorphic to the algebra S of matrices of shape

$$\begin{pmatrix} x & 0 & 0 \\ 0 & y & v \\ 0 & 0 & z \end{pmatrix}.$$

   One can check that S is a subalgebra of U and that $U = S \oplus J$.

2. You cannot do the same thing for the ideal I of matrices of shape

$$\begin{pmatrix} 0 & 0 & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

   For, if we could write $U = T \oplus I$ for some subalgebra T, then for some $\lambda, \mu \in K$ we have

$$s := \begin{pmatrix} 0 & 1 & \lambda \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad t := \begin{pmatrix} 0 & 0 & \mu \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{in } T.$$

   It follows that $E_{13} = st \in T \cap I$, a contradiction.

3. The **augmentation ideal** of the group algebra KG is the kernel I of the homomorphism

$$\epsilon\colon KG \to K, \quad e_g \mapsto 1 \text{ for all } g \in G.$$

The ideal I consists of all elements $\sum_g \lambda_g e_g$ such that $\sum_g \lambda_g = 0$, so has basis $e_g - 1$ for $g \in G \setminus \{1\}$. Observe that $KG = K \oplus I$ and $KG/I \cong K$.

5.7 First Isomorphism Theorem

Let $\theta\colon A \to B$ be a homomorphism of algebras. Then the induced algebra homomorphism

$$\bar{\theta}\colon A/\operatorname{Ker}(\theta) \to \operatorname{Im}(\theta)$$

is an isomorphism.

Proof. The map $\bar{\theta}$ exists by the Factor Lemma for algebras. On the other hand, we know it is an isomorphism of vector spaces, so it is an algebra isomorphism. □

5.8 Direct products

Let C be an algebra and suppose that I and J are ideals such that $C = I \oplus J$ (as a vector space). Define $A := C/J$ and $B := C/I$ to be the corresponding quotient algebras. Then there is an algebra isomorphism

$$C \xrightarrow{\sim} A \times B, \quad c \mapsto (c + J, c + I).$$

The only part which is not straightforward is to show that this map is surjective. We proceed as in the proof of the Chinese Remainder Theorem for integers, so write $1_C = e + f$ with $e \in I$ and $f \in J$. Then $e \mapsto (1_A, 0)$ and $f \mapsto (0, 1_B)$, so $c_1 e + c_2 f \mapsto (c_1 + J, c_2 + I)$, proving that the map is surjective.

6 Presentations of Algebras

So far we have defined algebras in terms of a basis and structure coefficients. Similarly, to define an algebra homomorphism, we need to give the images of the basis elements (so give a linear map) and then check that this preserves the unit and respects the multiplication. This is fine for small examples, but becomes very inefficient for larger algebras.

Compare with the situation for finite groups. You have probably only seen groups as subgroups of symmetric groups, or else via their multiplication tables. It is then quite laborious to check whether a given map defines a group homomorphism. Now imagine that you want to work with the Monster Group, having roughly 8×10^{53} elements.

The purpose of this section is to introduce a more compact way of exhibiting an algebra A. The basic idea is to write A as a quotient algebra B/I, where B is a larger algebra, but easier to understand, and $I \lhd B$ is some ideal.

Consider for example the quotient algebra given in Example 5.4. This algebra is quite awkward to work with, but if we regard it as the quotient U/I, then it becomes much easier to think about.

The type of algebra B one chooses may depend on the particular situation, but one choice which always works is when we take B to be a **free algebra**. In this case the description of A as a quotient of a free algebra is called a **presentation by generators and relations**. Such a description is particularly useful when constructing homomorphisms between algebras, since we only need to give the images of the generators and then check that the relations still hold. This is the content of the Proposition 6.11.

A word of warning: it is not always easy to transfer between these two descriptions, so it is often best to know both a basis for the algebra as well as a presentation in terms of generators and relations. Also, as for bases, generators are not unique.

6.1 Free Algebras

Let S be a set. We think of S as an 'alphabet', so a 'word' in S is a finite ordered list $X_1X_2\cdots X_r$ with $X_i \in S$, and the **length** of a word $X_1X_2\cdots X_r$ is r. We also include the 'empty word', of length 0 and denoted 1. Note that we can identify S with the set of words of length 1.

The **free algebra** $K\langle S\rangle$ is the vector space with basis all the words in the alphabet S and multiplication given by concatenation of words, so

$$X_1X_2\cdots X_r \cdot Y_1Y_2\cdots Y_s = X_1X_2\cdots X_rY_1Y_2\cdots Y_s.$$

This multiplication is clearly associative with unit the empty word 1. As usual, we often abbreviate XX by X^2, and XXX by X^3, and so on.

If $S = \{X_i : i \in I\}$, then we also write $K\langle X_i : i \in I\rangle$ for $K\langle S\rangle$.

6.2 Examples

1. If $S = \emptyset$, then there is only one possible word, so $K\langle\emptyset\rangle = K$.
2. If $S = \{X\}$, then $K\langle X\rangle$ has basis $1, X, X^2, X^3, \ldots$ and multiplication $X^m \cdot X^n = X^{m+n}$. Thus $K\langle S\rangle = K[X]$, the polynomial algebra.
3. If $S = \{X, Y\}$, then $K\langle X, Y\rangle$ has basis (in order of increasing length)

$$\begin{gathered} 1 \\ X,\ Y \\ X^2,\ XY,\ YX,\ Y^2 \\ X^3,\ X^2Y,\ XYX,\ YX^2,\ XY^2,\ YXY,\ Y^2X,\ Y^3 \\ \cdots \end{gathered}$$

and as an example of the multiplication we have

$$\begin{aligned}(2X + XY + 3Y^2X)&(4X - YX)\\ &= 2X(4X - YX) + XY(4X - YX) + 3Y^2X(4X - YX)\\ &= 8X^2 - 2XYX + 4XYX - XY^2X + 12Y^2X^2 - 3Y^2XYX\\ &= 8X^2 + 2XYX - XY^2X + 12Y^2X^2 - 3Y^2XYX.\end{aligned}$$

Note that $XY \neq YX$, so $K\langle X, Y\rangle$ is not isomorphic to the polynomial algebra $K[X, Y]$.

6.3 The Universal Property

Let S be a set and A an algebra. Given a map $f\colon S \to A$ there exists a unique algebra homomorphism $\theta\colon K\langle S\rangle \to A$ extending f, so $\theta(X) = f(X)$ for all $X \in S$.

In other words there is a bijection between algebra homomorphisms $K\langle S\rangle \to A$ and maps $S \to A$.

Proof. We define a linear map $\theta\colon K\langle S\rangle \to A$ via

$$\theta(X_1X_2\cdots X_n) := f(X_1)f(X_2)\cdots f(X_n) \quad \text{for all words } X_1X_2\cdots X_n.$$

Clearly $\theta(1) = 1$ and θ respects the multiplication, so does indeed define an algebra homomorphism. Moreover, $\theta(X) = f(X)$, so θ extends f.

To see that θ is unique, suppose that $\theta'\colon K\langle S\rangle \to A$ is another algebra homomorphism extending f. Then

$$\theta'(X_1\cdots X_n) = \theta'(X_1)\cdots\theta'(X_n) = f(X_1)\cdots f(X_n) = \theta(X_1\cdots X_n).$$

Hence θ and θ' agree on a basis, so they agree everywhere. □

6.4 Remark

Let A be an algebra and $S \subset A$ a subset. By the Universal Property there is a unique algebra homomorphism $\theta\colon K\langle S\rangle \to A$ which is the identity on S. We observe that its image is the smallest subalgebra containing S, so equals the subalgebra generated by S.

6.5 Relations

Let A be an algebra, and suppose A is generated by the subset $S \subset A$. We then have a surjective algebra homomorphism $\theta\colon K\langle S\rangle \to A$, and so by the First Isomorphism Theorem an induced isomorphism $A \cong K\langle S\rangle/\operatorname{Ker}(\theta)$.

The elements of $\operatorname{Ker}(\theta)$ are called the **relations** of A (with respect to the generating set S). If $\operatorname{Ker}(\theta) = (R)$ for some subset $R \subset K\langle S\rangle$, so is generated as an ideal by the set R, then we also say that A is **generated by S subject to the relations** R and call this a **presentation** of A.

Note that A has many choices for generators S, and for each choice of S, there may be many different choices for the set of relations R. Hence algebras have many different presentations, and different presentations may be easier or harder to work with in different situations.

We say that A is **finitely generated** if we can take S to be a finite set, and is **finitely presented** if we can take both S and R to be finite sets.

6.6 Remark

It is usually straightforward to find a set of generators for an algebra, and even to find some relations between them. The difficult part is to prove that we have found sufficiently many relations. One way of doing this is by computing dimensions. Another method which we shall look at in the next part is by looking at representations.

6.7 Examples

1. As $\mathbb{R}$-algebras we have $\mathbb{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{C}$. Hence $\mathbb{C}$ is generated as an $\mathbb{R}$-algebra by i subject to the relation $i^2 = -1$.

2. The quaternion algebra $\mathbb{H}$ is generated by i and j subject to the relations
$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji.$$
For, we have a surjective algebra homomorphism
$$\theta\colon \mathbb{R}\langle X, Y\rangle \to \mathbb{H}, \quad X \mapsto i, \quad Y \mapsto j.$$
Clearly $I = (X^2+1, Y^2+1, XY+YX) \subset \mathrm{Ker}(\theta)$, so by the Factor Lemma we have an induced surjective algebra homomorphism
$$\bar{\theta}\colon A := \mathbb{R}\langle X, Y\rangle / I \to \mathbb{H}.$$
In particular, $\dim A \geq \dim \mathbb{H} = 4$.
Now, the set of words in X and Y span $\mathbb{R}\langle X, Y\rangle$, so the set of words in their images $x := X + I$ and $y := Y + I$ span the quotient algebra A. Using the relation $xy = -yx$ we can always swap x and y in any word, so the words $x^m y^n$ span A. Next, $x^2 = y^2 = -1$, so the words $1, x, y, xy$ span A. Thus $\dim A \leq 4$.
Hence $\dim A = 4$, $I = \mathrm{Ker}(\theta)$ and $\bar{\theta}$ is an isomorphism.

3. The polynomial algebra $K[X_1, \ldots, X_n]$ is generated by $X_1, \ldots, X_n$ subject to the relations $X_i X_j = X_j X_i$ for all i, j.
For, we know that the X_i generate the polynomial algebra, so set $A = K\langle X_1, \ldots, X_n\rangle / (\{X_i X_j - X_j X_i\})$. By the Factor Lemma there is a surjective algebra homomorphism $\theta\colon A \to K[X_1, \ldots, X_n]$, $X_i \mapsto X_i$.
Since $X_i X_j = X_j X_i$ in A, we can always swap X_i and X_j in any word. Thus A is spanned by the words $X_1^{m_1} \cdots X_n^{m_n}$ for $m_i \geq 0$. Since their images form a basis for the polynomial algebra $K[X_1, \ldots, X_n]$, we deduce that these words are linearly independent in A, and hence form a basis for A. It follows that θ is an isomorphism.

4. The matrix algebra $\mathbb{M}_2(K)$ is generated by $e = E_{12}$ and $f = E_{21}$ subject to the relations $e^2 = f^2 = 0$ and $ef + fe = 1$.

   For, let $A = K\langle X, Y\rangle/(X^2, Y^2, XY + YX - 1)$ and write x and y for the images of X and Y in A. We saw earlier that e, f generate $\mathbb{M}_2(K)$, and it is simple to check that the relations hold. Therefore we have a surjective algebra homomorphism $\theta\colon A \to \mathbb{M}_2(K)$, $x \mapsto e$, $y \mapsto f$. In particular, $\dim A \geq 4$.

   Now, A is spanned by all words in x, y, and using that $yx = 1 - xy$ we see that it is spanned by all words of the form $x^m y^n$. Since $x^2 = y^2 = 0$ we now see that A is spanned by $1, x, y, xy$, so $\dim A \leq 4$ and we are done.

5. The algebra $TL_3(\delta)$ is generated by u_1, u_2 subject to the relations

$$u_1^2 = \delta u_1, \quad u_2^2 = \delta u_2, \quad u_1 u_2 u_1 = u_1, \quad u_2 u_1 u_2 = u_2.$$

   For, consider the factor algebra $A = K\langle X_1, X_2\rangle/(X_i^2 - \delta X_i, X_i X_j X_i - X_i)$ and write x_i for the image of X_i in A. We have already seen that u_1, u_2 generate $TL_3(\delta)$, and it is easy to show that these relations hold in $TL_3(\delta)$. So there exists an epimorphism $\theta\colon A \to TL_3(\delta)$, $x_i \mapsto u_i$, whence $\dim A \geq 5$.

   Now A is spanned by all words in the x_i. We can use the relations $x_i^2 = \delta x_i$ to see that A is spanned by all 'alternating' words $x_i x_j x_i x_j \cdots$. Finally, we can use the relations $x_i x_j x_i = x_i$ to see that A is spanned by all alternating words of length at most two. Thus A is spanned by $\{1, x_1, x_2, x_1 x_2, x_2 x_1\}$ and $\dim A \leq 5$. Thus $\dim A = 5$ and θ is an isomorphism.

   More generally, the algebra $TL_n(\delta)$ is generated by u_i for $1 \leq i < n$ subject to the relations

$$u_i^2 = \delta u_i, \quad u_i u_{i\pm 1} u_i = u_i, \quad u_i u_j = u_j u_i \text{ for } |i - j| > 1.$$

   This is non-trivial to prove, and involves ideas from algebra and combinatorics, as well as manipulating diagrams.

6. The algebra of upper-triangular matrices $U_n \leq \mathbb{M}_n(K)$ is generated by $e_i = E_{ii}$ and $f_i = E_{ii+1}$ subject to the relations

$$e_i e_j = \delta_{ij} e_j, \quad e_i f_j e_k = \delta_{ij}\delta_{kj+1} f_j.$$

6.8 Characteristic

The **characteristic** of a field K is the smallest positive integer n such that $n \cdot 1 = 0 \in K$. If no such n exists, we define the characteristic to be zero.

[There is a unique ring homomorphism $\mathbb{Z} \to K$. The kernel of this is an ideal of $\mathbb{Z}$, hence of the form (n) for some $n \geq 0$. This n is precisely the characteristic of K.]

Examples.

1. The fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic zero.

2. If $p \in \mathbb{Z}$ is a prime, then $\mathbb{F}_p = \mathbb{Z}_p$ is a field of characteristic p.

3. The characteristic of a field is either zero or a prime number. For, if $\mathrm{char}(K) = n$ and $n = ab$ with $1 < a, b < n$, then $ab = n = 0 \in K$, whence either $a = 0 \in K$ or $b = 0 \in K$, contradicting the minimality of n.

6.9 Example

In $\mathrm{char}(K) \neq 2$ the matrix algebra $\mathbb{M}_2(K)$ is generated by $x = E_{11} - E_{22}$ and $y = E_{12} + E_{21}$ subject to the relations $x^2 = y^2 = 1$, $xy + yx = 0$.

For, $1 = E_{11} + E_{22}$ and $xy = E_{12} - E_{21}$, so

$$E_{11} = \tfrac{1}{2}(1 + x), \quad E_{22} = \tfrac{1}{2}(1 - x), \quad E_{12} = \tfrac{1}{2}(y + xy), \quad E_{21} = \tfrac{1}{2}(y - xy).$$

Hence x, y generate $\mathbb{M}_2(K)$.

Again it is easy to check that the relations hold so we have an epimorphism $\theta\colon A \to \mathbb{M}_2(K)$, where $A = K\langle X, Y\rangle/(X^2 - 1, Y^2 - 1, XY + YX)$, sending $X \mapsto x$ and $Y \mapsto y$. In particular $\dim A \geq 4$.

On the other hand, A is spanned by (the images of) the words in X and Y. Using that $YX = -XY$ in A we see that A is spanned by $X^m Y^n$, and using that $X^2 = Y^2 = 1$ we see that A is spanned by $1, X, Y, XY$. Thus $\dim A \leq 4$ and we are done.

6.10 Example

It is not always obvious when an algebra given in the form of generators and relations is zero.

For example, let A be the $\mathbb{R}$-algebra generated by X, Y subject to the relations $X^2 = 0$ and $XY - YX = 1$, so

$$A = \mathbb{R}\langle X, Y\rangle/(X^2, XY - YX - 1).$$

Write x and y for the images of X and Y in A. Then

$$x = x1 = x(xy - yx) = x^2 y - xyx = -xyx$$

and

$$x = 1x = (xy - yx)x = xyx - yx^2 = xyx.$$

Thus $2x = 0$, hence $x = 0$ in A. Thus $1 = xy - yx = 0$ in A, so A must be the zero algebra $\{0\}$.

6.11 Proposition

Suppose that A is given by generators and relations

$$A = K\langle\{X_i\}\rangle/(\{r_j\}).$$

Then algebra homomorphisms $\theta\colon A \to B$ are in bijection with maps $f\colon \{X_i\} \to B$ such that $f(r_j) = 0$ for all j.

Proof. By the Factor Lemma the algebra homomorphisms $\theta\colon A \to B$ are in bijection with the algebra homomorphisms $\hat{\theta}\colon K\langle\{X_i\}\rangle \to B$ such that the ideal $I := (\{r_j\})$ lies in the kernel of $\hat{\theta}$. By the Universal Property, the algebra homomorphisms $\hat{\theta}\colon K\langle\{X_i\}\rangle \to B$ are in bijection with maps $f\colon \{X_i\} \to B$, and then $I \subset \mathrm{Ker}(\hat{\theta})$ if and only if each r_j lies in the kernel, so $f(r_j) = 0$ in B for all j. □

6.12 Example

Since $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$, to give an $\mathbb{R}$-algebra homomorphism $\mathbb{C} \to A$ is the same as choosing an element $a \in A$ with $a^2 = -1$.

For example, the algebra homomorphisms $\mathbb{C} \to \mathbb{H}$ are in bijection with the pure quaternions of absolute value one.

To see this note that if $p \in \mathbb{H}$ is a pure quaternion of absolute value one, then $p^2 = -|p|^2 = -1$, so there is an algebra homomorphism $\mathbb{C} \to \mathbb{H}$, $i \mapsto p$. Conversely, if $\theta\colon \mathbb{C} \to \mathbb{H}$ is an algebra homomorphism, then $q = \theta(i) \in \mathbb{H}$ satisfies $q^2 = -1$. Write $q = a + p$ with $a \in \mathbb{R}$ and p a pure quaternion. Then

$$-1 = q^2 = a^2 + 2ap + p^2 = (a^2 - |p|^2) + 2ap.$$

Since ap is again a pure quaternion, we must have $ap = 0$. Then, since $\mathbb{H}$ is a division algebra, either $a = 0$ or $p = 0$. Finally, $-1 = a^2 - |p|^2$, so we must have $a = 0$ and $|p| = 1$, so that $q = p$ is a pure quaternion of absolute value 1.

6.13 Example

Since $\mathbb{H} \cong \mathbb{R}\langle X, Y\rangle/(X^2+1, Y^2+1, XY+YX)$, to give an algebra homomorphism $\mathbb{H} \to A$ is the same as choosing two elements $a, b \in A$ with $a^2 = b^2 = -1$ and $ab = -ba$.

For example, there is an algebra homomorphism

$$\theta\colon \mathbb{H} \to \mathbb{M}_2(\mathbb{C}), \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

To see this, we just need to check

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

and

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

In fact, this is a monomorphism. For, $\mathbb{H}$ is a division algebra, so the only ideals are 0 or $\mathbb{H}$ and hence $\mathrm{Ker}(\theta) = 0$.

Part II

Representations

7 Representations

Since algebras involve multiplication, they are 'non-linear' and hence can be difficult to study. Representations offer a way to 'linearise' the problem, with each representation yielding partial information ('local') about the algebra as a whole ('global'). One can view this as analogous to understanding functions via their derivatives (leading to the Taylor expansion), or more generally surfaces (or higher dimensional figures) via their tangent spaces.

7.1 Definition

If V is a vector space, then a **representation of A by endomorphisms of V** is an algebra homomorphism $A \to \mathrm{End}_K(V)$.

If $V = K^n$, then we can compose with the algebra isomorphism $\mathrm{End}_K(K^n) \cong \mathbb{M}_n(K)$ given in Lemma 3.10 to get an algebra homomorphism $A \to \mathbb{M}_n(K)$. Such an algebra homomorphism $A \to \mathbb{M}_n(K)$ is called a **matrix representation of A of degree n**.

7.2 Remarks

1. Suppose the algebra A has basis $\{e_1, \ldots, e_m\}$ and structure coefficients c_{ij}^k, so that
$$e_i e_j = \sum_{k=1}^{m} c_{ij}^k e_k.$$
Then to give a matrix representation of A is exactly the same as giving matrices $M_i \in \mathbb{M}_n(K)$ such that
$$M_i M_j = \sum_{k=1}^{m} c_{ij}^k M_k \quad \text{for all } i, j.$$
For, we just define ρ via $\rho(e_i) = M_i$. Note that the matrices $M_i = \rho(e_i)$ need not be linearly independent.
We often simplify matters by assuming $e_1 = 1_A$, and hence $\rho(e_1) = I_n$.

2. If instead A is given by generators and relations
$$A = K\langle X_1, \ldots, X_n \rangle / (r_1, \ldots, r_m),$$
then by Proposition 6.11 giving a matrix representation $A \to \mathbb{M}_n(K)$ is the same as giving matrices $M_i = \rho(x_i)$ satisfying each of the relations r_j.

7.3 Example

If we consider $\mathbb{C}$ as an $\mathbb{R}$-algebra, then we have a representation

$$\mathbb{C} \to \mathbb{M}_2(\mathbb{R}), \quad x + yi \mapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

In fact, since $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$, matrix representations $\rho\colon \mathbb{C} \to \mathbb{M}_n(\mathbb{R})$ are in bijection with matrices $M \in \mathbb{M}_n(\mathbb{R})$ such that $M^2 = -I_n$, the representation then being $\rho(x + yi) = xI_n + yM$.

The representation above corresponds to taking $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

7.4 Zero representation

The **zero representation** is the unique algebra homomorphism given by taking $V = \{0\}$. Then $\mathrm{End}_K(0) = \mathbb{M}_0(K) = \{0\}$ is the zero algebra.

7.5 Regular representation

If A is an algebra and $a \in A$, then we denote by $\hat{a}$ the map

$$\hat{a}\colon A \to A, \quad \hat{a}(x) := ax \quad (x \in A).$$

It is called the **homothety of left multiplication by** a.

The map

$$A \to \mathrm{End}_K(A), \quad a \mapsto \hat{a}$$

defines a representation of A by endomorphisms of A, called the **regular representation** of A.

7.6 Theorem

Every finite-dimensional algebra is isomorphic to a subalgebra of a matrix algebra.

Proof. Suppose $\dim A = n$. Then, after choosing a basis for A, the regular representation is of the form $A \to \mathbb{M}_n(K)$. This mapping is injective, for if $\hat{a} = 0$, then $0 = \hat{a}(1) = a1 = a$. Thus A is isomorphic to its image under this map, which is a subalgebra of $\mathbb{M}_n(K)$. □

7.7 Examples

1. Consider $\mathbb{C}$ as an $\mathbb{R}$-algebra, with basis $\{1, i\}$. The regular representation $\mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ sends $z = x + yi \in \mathbb{C}$ to the matrix of the homothety $\hat{z}$ with respect to this basis.

Now

$$\hat{z}(1) = (x+yi)1 = x+yi \quad \text{and} \quad \hat{z}(i) = (x+yi)i = -y+xi,$$

so the matrix of $\hat{z}$ is

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Thus $\mathbb{C}$ is isomorphic to the subalgebra of $\mathbb{M}_2(\mathbb{R})$ given by

$$\left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}.$$

2. An algebra can be isomorphic to a subalgebra of a matrix algebra in many different ways. For example, the algebra

$$A = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} : x, y, z \in K \right\}$$

is a subalgebra of $\mathbb{M}_2(K)$ by construction. On the other hand, since it is three dimensional, the theorem shows it is isomorphic to a subalgebra of $\mathbb{M}_3(K)$.

We can compute the latter subalgebra as follows: A has basis

$$b_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then for $a = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ we have

$$\hat{a}(b_1) = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = xb_1,$$

and similarly

$$\hat{a}(b_2) = xb_2, \quad \hat{a}(b_3) = yb_2 + zb_3.$$

Thus the matrix of $\hat{a}$ is

$$\begin{pmatrix} x & 0 & 0 \\ 0 & x & y \\ 0 & 0 & z \end{pmatrix},$$

so A is isomorphic to the subalgebra of $\mathbb{M}_3(K)$ given by

$$\left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & x & y \\ 0 & 0 & z \end{pmatrix} : x, y, z \in K \right\}.$$

3. Let G be a group. Then the regular representation of KG is induced from the action of G on itself by left multiplication, since $\widehat{e}_g(e_h) = e_{gh}$.

4. We have a matrix representation

$$\rho \colon TL_3(\delta) \to \mathbb{M}_2(K), \quad u_1 \mapsto \begin{pmatrix} \delta & 1 \\ 0 & 0 \end{pmatrix}, \quad u_2 \mapsto \begin{pmatrix} 0 & 0 \\ 1 & \delta \end{pmatrix}.$$

For, we know that $TL_3(\delta)$ is generated by u_1, u_2 subject to the relations $u_i^2 = u_i$ and $u_i u_j u_i = u_i$. So, by Proposition 6.11 we just need to check that the matrices also satisfy these relations. For example,

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

so $\rho(u_1)^2 = \delta\rho(u_1)$, and

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

so $\rho(u_1)\rho(u_2)\rho(u_1) = \rho(u_1)$. Similarly for the other two relations.

7.8 Restriction of scalars

Let $f\colon A \to B$ be an algebra homomorphism. Then composing with f gives a map from B-representations to A-representations, called **restriction of scalars**

$$\rho\colon B \to \mathrm{End}_K(V) \quad \text{is sent to} \quad \rho f\colon A \to \mathrm{End}_K(V).$$

In particular we can do this whenever A is a subalgebra of B.

7.9 Representations of quotient algebras

Let A be an algebra and $I \lhd A$ an ideal. Then restriction of scalars gives a bijection between representations of A/I and those representations ρ of A such that $I \leq \mathrm{Ker}(\rho)$.

Proof. This follows immediately from the Factor Lemma for algebras. □

7.10 Representations of group algebras

Let G be a group. Then representations of the group algebra $\rho\colon KG \to \mathbb{M}_n(K)$ are exactly the same thing as group homomorphisms $\theta\colon G \to \mathrm{GL}_n(K)$, the correspondence being given by $\theta(g) = \rho(e_g)$ for $g \in G$.

Proof. If ρ is any representation, then $\rho(e_g)$ is invertible for $g \in G$:

$$\rho(e_g)\rho(e_{g^{-1}}) = \rho(e_{gg^{-1}}) = \rho(e_1) = \rho(1_{KG}) = I.$$

We therefore have a map $\theta\colon G \to \mathrm{GL}_n(K)$, $g \mapsto \rho(e_g)$. It is now easy to check that this is group homomorphism. For, $\theta(1_G) = \rho(e_1) = \rho(1_{KG}) = I$ and

$$\theta(g)\theta(h) = \rho(e_g)\rho(e_h) = \rho(e_g e_h) = \rho(e_{gh}) = \theta(gh).$$

Conversely, given any group homomorphism $\theta\colon G \to \mathrm{GL}_n(K)$, the corresponding linear map $\rho\colon KG \to \mathbb{M}_n(K)$, $e_g \mapsto \theta(g)$ is indeed a representation (c.f. Exercise Sheet 2, Question 5). For, $\rho(1_{KG}) = \rho(e_1) = \theta(1_G) = I$ and

$$\rho(e_g)\rho(e_h) = \theta(g)\theta(h) = \theta(gh) = \rho(e_{gh}) = \rho(e_g e_h).$$

It then follows from linearity that $\rho(x)\rho(y) = \rho(xy)$ for all $x, y \in KG$, so that ρ preserves the multiplication. □

7.11 Example

If G is a group of rotations and reflections of $\mathbb{R}^n$, each fixing the origin, then $G \leq \mathrm{GL}_n(\mathbb{R})$. The corresponding representation $\rho\colon \mathbb{R}G \to \mathbb{M}_n(\mathbb{R})$ is called the **natural representation** of G (or $\mathbb{R}G$).

This holds, for example, for the dihedral group D_{2n} of order $2n$, since its elements are precisely those rotations and reflections of $\mathbb{R}^2$ fixing a regular n-gon (centred on the origin).

7.12 Equivalence

We say that two representations $\rho\colon A \to \mathrm{End}_K(V)$ and $\sigma\colon A \to \mathrm{End}_K(W)$ are **equivalent** provided there exists a vector space isomorphism $\theta\colon V \xrightarrow{\sim} W$ such that

$$\sigma(a) = \theta\rho(a)\theta^{-1} \quad \text{for all } a \in A.$$

Writing $\Theta\colon \mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{End}_K(W)$ for the induced algebra isomorphism as in Lemma 3.11, we can write this as $\sigma = \Theta\rho$.

Under the isomorphism $\mathrm{End}_K(K^n) \cong \mathbb{M}_n(K)$, vector space automorphisms of K^n correspond to invertible matrices. Therefore two matrix representations $\rho, \sigma\colon A \to \mathbb{M}_n(K)$ are equivalent provided there exists an invertible matrix $P \in \mathrm{GL}_n(K)$ such that

$$\sigma(a) = P\rho(a)P^{-1} \quad \text{for all } a \in A.$$

7.13 Example

If $\dim V = n$, then choosing a basis for V yields a vector space isomorphism $\theta\colon V \to K^n$, and hence an algebra isomorphism

$$\Theta\colon \mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{End}_K(K^n) \cong \mathbb{M}_n(K).$$

If now $\rho\colon A \to \mathrm{End}_K(V)$ is a representation, then composing with Θ gives a algebra homomorphism

$$\Theta\rho\colon A \to \mathrm{End}_K(V) \to \mathbb{M}_n(K), \quad a \mapsto \Theta(\rho(a)) = \theta\rho(a)\theta^{-1}.$$

Note that $\Theta\rho(a)$ is just the matrix of the linear map $\rho(a)$ with respect to the basis $\{e_1, \ldots, e_n\}$.

This shows that every representation $A \to \mathrm{End}_K(V)$ is equivalent to a matrix representation $A \to \mathbb{M}_n(K)$.

7.14 Example

By the Universal Property, giving a matrix representation $\rho\colon K[X] \to \mathbb{M}_n(K)$ is the same as just giving a single matrix $\rho(X)$. Then two matrix representations $\rho, \sigma\colon K[X] \to \mathbb{M}_n(K)$ are equivalent if and only there exists $P \in \mathrm{GL}_n(K)$ with $\sigma(X) = P\rho(X)P^{-1}$, or in other words if and only if $\rho(X)$ and $\sigma(X)$ are similar, or conjugate, matrices.

7.15 Direct product of representations

Let $\rho\colon A \to \mathbb{M}_m(K)$ and $\sigma\colon A \to \mathbb{M}_n(K)$ be two matrix representations. As in Example 3.6 we can view the algebra $\mathbb{M}_m(K) \times \mathbb{M}_n(K)$ as a subalgebra of $\mathbb{M}_{m+n}(K)$. We therefore define the **direct product** of ρ and σ to be the matrix representation

$$\rho \times \sigma\colon A \to \mathbb{M}_{m+n}(K), \quad (\rho \times \sigma)(a) := \begin{pmatrix} \rho(a) & 0 \\ 0 & \sigma(a) \end{pmatrix}.$$

More generally, we can regard the direct product $\mathrm{End}_K(V) \times \mathrm{End}_K(W)$ as a subalgebra of $\mathrm{End}_K(V \times W)$ via

$$(\theta, \phi)(v, w) := (\theta(v), \phi(w)) \quad \text{for } \theta \in \mathrm{End}_K(V),\ \phi \in \mathrm{End}_K(W),\ v \in V,\ w \in W.$$

Therefore, given representations $\rho\colon A \to \mathrm{End}_K(V)$ and $\sigma\colon A \to \mathrm{End}_K(W)$, we define their direct product to be the representation

$$\rho \times \sigma\colon A \to \mathrm{End}_K(V) \times \mathrm{End}_K(W) \leq \mathrm{End}_K(V \times W), \quad (\rho \times \sigma)(a) := (\rho(a), \sigma(a)).$$

A representation $A \to \mathrm{End}_K(U)$ is called **indecomposable** if it is not equivalent to a such a direct product $\rho \times \sigma$ with both ρ and σ non-zero, and is **decomposable** otherwise.

8 Modules

Modules are an alternative, and often more convenient, way of talking about representations. Their advantage is that we can now extend many of the results about vector spaces to modules.

8.1 Definition

Let A be an algebra. A **(left) A-module** consists of a vector space M together with an operation, called the **action**,

$$A \times M \to M, \quad (a, m) \mapsto am$$

satisfying the following properies for all $a, b \in A$, $m, n \in M$ and $\lambda \in K$:

Associative	$a(bm) = (ab)m$.
Unital	$1m = m$ for all $m \in M$.
Bilinear	$a(m + \lambda n) = am + \lambda(an)$ and $(a + \lambda b)m = am + \lambda(bm)$.

We sometimes write ${}_AM$ to indicate that M is a left A-module.

There is also the notion of a right A-module, using an action $M \times A \to M$, $(m, a) \mapsto ma$.

8.2 Examples

1. A K-module is exactly the same thing as a vector space over K.
2. For any algebra A we have the **zero module** $\{0\}$.
3. The **regular module** for A is the vector space A with the action given by multiplication in A. We usually denote this module as ${}_AA$.
4. If $A \leq \mathbb{M}_n(K)$ is given as a subalgebra of a matrix algebra, then the **natural module** for A is the vector space K^n with the action of A given by matrix multiplication

$$(ax)_i := \sum_j a_{ij}x_j, \quad \text{for } a \in A \leq \mathbb{M}_n(K) \text{ and } x \in K^n.$$

8.3 Proposition

Let A be an algebra and M a vector space. Then there is a bijection between A-module structures on M and representations $A \to \mathrm{End}_K(M)$.

As a special case it follows that there is a bijection between A-module structures on K^n and matrix representations $A \to \mathbb{M}_n(K)$.

Proof. Suppose we have an A-module structure on M, so an associative, unital, bilinear map $A \times M \to M$. Then for each $a \in A$ we obtain a linear map $\widehat{a}_M \in \mathrm{End}_K(M)$ via $\widehat{a}_M(m) := am$. This satisfies

$$\widehat{(ab)}_M = \widehat{a}_M\widehat{b}_M, \quad \widehat{1}_M = \mathrm{id}_M, \quad \widehat{(a+\lambda b)}_M = \widehat{a}_M + \lambda\widehat{b}_M,$$

and so the map

$$A \to \mathrm{End}_K(M), \quad a \mapsto \widehat{a}_M,$$

is an algebra homomorphism, so a representation of A.

Conversely, suppose we have a representation $\rho\colon A \to \mathrm{End}_K(M)$. Then we can define a map

$$A \times M \to M, \quad (a, m) \mapsto \rho(a)(m).$$

This is then associative, unital and bilinear, so defines an action of A on M.

Finally, it is easy to check that these constructions are mutually inverse. □

8.4 Example

Let A be the algebra with basis $\{1, i, j\}$ and multiplication given by $i^2 = j$ and $j^2 = ij = ji = 0$. The matrices

$$i' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad j' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

also satisfy these relations, so there is a homomorphism $\rho\colon A \to \mathbb{M}_3(K)$ sending i, j to these matrices. Thus

$$\rho(\alpha + \beta i + \gamma j) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & 0 & \alpha \end{pmatrix}$$

is a representation of A. The corresponding A-module is the vector space K^3 with the action

$$(\alpha + \beta i + \gamma j) \begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & 0 & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \alpha x \\ \alpha y + \beta z \\ \alpha z \end{pmatrix}.$$

8.5 Direct product of modules

If M and N are A-modules, then the vector space $M \times N$ is naturally a module via the action

$$A \times (M \times N) \to M \times N, \quad (a, (m, n)) \mapsto (am, an).$$

We call this the **direct product** of the modules.

Note that, under the bijection between module structures and representations, Proposition 8.3, the direct product of modules corresponds to the direct product of representations.

For, if ρ and σ respectively denote the representations corresponding to the modules M and N, then the representation τ corresponding to the direct product $M \times N$ is given by

$$\begin{aligned} \tau(a)(m, n) = a(m, n) = (am, an) &= \big(\rho(a)(m), \sigma(a)(n)\big) \\ &= \big(\rho(a) \times \sigma(a)\big)(m, n) = (\rho \times \sigma)(a)(m, n). \end{aligned}$$

Thus $\tau(a) = (\rho \times \sigma)(a)$ for all $a \in A$, so $\tau = \rho \times \sigma$.

8.6 Remark (non-examinable)

Recall that an action of a group G on a set X is given by a map

$$G \times X \to X, \quad (g, x) \mapsto gx$$

such that, for all $g, h \in G$ and $x \in X$,

$$g(hx) = (gh)x \quad \text{and} \quad 1x = x.$$

This is the same as giving a group homomorphism $G \to S_X$ from G to the symmetry group of X.

These two alternative ways of describing group actions are analogous to talking about either modules or representations.

To make this precise, recall that the vector space $K^{(X)}$ has basis e_x for $x \in X$. Then S_X acts linearly on $K^{(X)}$ by permuting the basis vectors, so $\sigma(e_x) =$

$e_{\sigma(x)}$, giving a group homomorphism $S_X \to \mathrm{Aut}_K\big(K^{(X)}\big)$, called the natural representation.

We now see that if G acts on X, then the map

$$KG \times K^{(X)} \to K^{(X)}, \quad (e_g, e_x) \mapsto e_{gx},$$

defines an action of the group algebra KG on $K^{(X)}$. Alternatively, the group homomorphism $G \to S_X$ induces an algebra homomorphism $KG \to KS_X$, which we can compose with the natural representation to get an algebra homomorphism $KG \to \mathrm{End}_K\big(K^{(X)}\big)$, so a representation of KG.

9 Homomorphisms and Submodules

Almost any notion or result about vector spaces generalizes to modules, provided that it doesn't use bases.

9.1 Homomorphisms

A map $f\colon M \to N$ between A-modules is an **(A-module) homomorphism** if

(a) f is a linear map.

(b) $f(am) = af(m)$ for all $a \in A$ and $m \in M$.

In other words, f is a linear map which **respects the A-action**. It follows that

$$f(m + am') = f(m) + af(m') \quad \text{for all } m, m' \in M \text{ and } a \in A,$$

and so we also say that f is an A-linear map.

In terms of representations we can also write this as

$$f\widehat{a}_M = \widehat{a}_N f \quad \text{for all } a \in A.$$

If $f\colon M \to N$ and $g\colon N \to P$ are homomorphisms, then so too is their composition $gf\colon M \to P$.

We call f an **isomorphism** provided there exists a homomorphism $g\colon N \to M$ with both $gf = \mathrm{id}_M$ and $fg = \mathrm{id}_N$. It is again a useful fact that f is an isomorphism if and only if it is a bijection.

If there is an isomorphism $M \to N$, we say that M and N are **isomorphic** and write $M \cong N$.

9.2 Endomorphism algebras of modules

We write $\mathrm{Hom}_A(M, N)$ for the set of A-module homomorphisms from M to N. Thus

$$\mathrm{Hom}_A(M, N) = \{f \in \mathrm{Hom}_K(M, N) : f\widehat{a}_M = \widehat{a}_N f \text{ for all } a \in A\}.$$

This is clearly a vector subspace of $\mathrm{Hom}_K(M,N)$.

In particular we write $\mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$ for the set of A-module endomorphisms of M. Then

$$\mathrm{End}_A(M) = \{f \in \mathrm{End}_K(M) : f\widehat{a}_M = \widehat{a}_M f \text{ for all } a \in A\}.$$

Observe that $\mathrm{End}_A(M)$ is the **centraliser** in $\mathrm{End}_K(M)$ of the set $\{\widehat{a}_M : a \in A\}$. By Exercise Sheet 2, Question 2, we conclude that $\mathrm{End}_A(M)$ is a subalgebra of $\mathrm{End}_K(M)$.

9.3 Example

Consider the algebra and module from Example 8.4, so A is the algebra with basis $\{1,i,j\}$ and multiplication given by $i^2 = j$ and $j^2 = ij = ji = 0$, and M is the module corresponding to the representation

$$i' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad j' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then, since every matrix commutes with 0 and I_n, we have

$$\begin{aligned} \mathrm{End}_A(M) &= \{f \in \mathbb{M}_3(K) : f\widehat{a}_M = \widehat{a}_M f \text{ for all } a \in A\} \\ &= \{f \in \mathbb{M}_3(K) : fi' = i'f\} \\ &= \left\{ \begin{pmatrix} p & 0 & q \\ r & s & t \\ 0 & 0 & s \end{pmatrix} : p,q,r,s,t \in K \right\}. \end{aligned}$$

9.4 Submodules

A **submodule** of an A-module M is a subspace N which is itself a module via the induced action. In other words

(a) N is a subspace of M.

(b) $an \in N$ for all $a \in A$ and $n \in N$.

We usually write $N \leq M$ to denote that N is a submodule of M.

9.5 Examples

1. If M is an A-module, then 0 and M are always submodules of M.
2. If A is the algebra of upper-triangular 2×2 matrices and $M = K^2$ is the natural module, then
   (a) $\left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in K \right\}$ is a submodule.

(b) $\left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} : y \in K \right\}$ is not a submodule.

In fact, (a) gives the only submodule of M other than 0 or M itself.

3. Submodules of the regular module ${}_AA$ are the same as left ideals in A. In particular any ideal of A is a submodule of ${}_AA$.

4. Suppose that $A = \mathbb{M}_n(K)$. For $1 \leq i \leq n$ let C_i be the set of matrices which are non-zero only in column i. Then C_i is a left ideal, so is a submodule of the regular module.

5. If M and N are submodules of a module L, then both the vector space sum $M + N$ and intersection $M \cap N$ are submodules of L. As usual, we say that the sum $M + N$ is **direct**, written $M \oplus N$, provided that $M \cap N = \{0\}$.

9.6 Lemma

If $f\colon N \to M$ is a homomorphism of modules, then $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ are submodules of N and M respectively. Conversely, if $N \leq M$ is a submodule, then the inclusion map $N \hookrightarrow M$ is a module homomorphism.

In other words, submodules are the same as images of module homomorphisms.

Proof. Exercise. □

Since f is *a priori* a linear map, we know it is injective if and only if $\mathrm{Ker}(f) = \{0\}$. We call f a **monomorphism** if it is injective, and an **epimorphism** if it is onto. Thus f is an isomorphism if and only if it is both a monomorphism and an epimorphism.

9.7 Lemma

Under the bijection between A-module structures on M and representations $A \to \mathrm{End}_K(M)$ given in Proposition 8.3, isomorphic modules correspond to equivalent representations.

Proof. Two A-modules M and N are isomorphic if and only if there exists a vector space isomorphism $\theta\colon M \xrightarrow{\sim} N$ such that $\theta\widehat{a}_M = \widehat{a}_N\theta$ for all $a \in A$. Since θ is an isomorphism, this is equivalent to saying that $\widehat{a}_N = \theta\widehat{a}_M\theta^{-1}$, and hence that the representations $a \mapsto \widehat{a}_M$ and $a \mapsto \widehat{a}_N$ are equivalent. □

It now follows that there is a bijection between finite-dimensional modules up to isomorphism and matrix representations up to equivalence, though to do this properly one should really use the language of category theory.

9.8 Submodules given via ideals

One important way of constructing submodules is by using ideals.

Let M be an A-module and $I \leq A$ a left ideal. Then

$$IM := \text{span}\{xm : x \in I, m \in M\}$$

is a submodule of M. For, it is clearly a vector subspace. Also, if $a \in A$, $x \in I$ and $m \in M$, then $ax \in I$ and so $a(xm) = (ax)m \in IM$. Since the A-action on M is bilinear we see that $am \in IM$ for all $m \in IM$.

Alternatively we could have defined IM to be the smallest submodule of M containing the set $\{xm : x \in I, m \in M\}$.

If $J \leq A$ is another left ideal, then

$$(I + J)M = IM + JM \quad \text{and} \quad I(JM) = (IJ)M.$$

For, both $(I+J)M$ and $IM+JM$ are spanned by elements of the form $xm+yn$ for $x \in I$, $y \in J$ and $m, n \in M$. Similarly, both $(IJ)M$ and $I(JM)$ are spanned by all elements of the form $(xy)m = x(ym)$ for $x \in I$, $y \in J$ and $m \in M$.

9.9 Warning

Since $I \cap J$ is contained in both I and J we clearly have $(I \cap J)M \subset (IM) \cap (JM)$. However, in general the two sides are different.

For example, let $A = K[x, y]$ and set $I := (x)$ and $J := (y)$, so that $I \cap J = (xy)$. Let M be the module with vector space K^2 and action

$$\rho \colon A \to \mathbb{M}_2(K), \quad x, y \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

We check that $\rho(xy) = \rho(yx) = 0$, so that ρ is indeed an algebra homomorphism.

Now, on one hand we have

$$IM = \text{span}\{xe_1, xe_2\} = \text{span}\{e_1\} \quad \text{and} \quad JM = \text{span}\{ye_1, ye_2\} = \text{span}\{e_1\}$$

so that $IM = JM = \text{span}\{e_1\}$. On the other hand

$$(I \cap J)M = \text{span}\{xye_1, xye_2\} = \{0\}.$$

9.10 Lemma

Let I, J be two-sided ideals of A. If $I + J = A$, then for all modules M we have

$$IM \cap JM = (I \cap J)M.$$

Proof. We begin by observing that $IJ, JI \subset I \cap J$. Now write $1 = x + y$ with $x \in I$ and $y \in J$. If $m \in IM$, then $ym \in J(IM) = (JI)M \subset (I \cap J)M$. Similarly, if $m \in JM$, then $xm \in (I \cap J)M$. Thus if $m \in (IM) \cap (JM)$, then $m = xm + ym \in (I \cap J)M$. □

We remark that this result is not true when I and J are just left ideals — see the exercises.

9.11 Restriction of scalars

If $f\colon A \to B$ is a homomorphism of algebras, then any B-module M becomes an A-module via $ax := f(a)x$. We denote this module by ${}_AM$ or ${}_fM$.

In particular, if $I \lhd A$ is an ideal, then restriction of scalars gives a bijection between A/I-modules and A-modules M with $IM = \{0\}$.

For, note that if $\rho\colon A \to \mathrm{End}_K(M)$ is the representation corresponding to the A-module M, then $IM = \{0\}$ if and only if $I \leq \mathrm{Ker}(\rho)$. The result now follows from Section 7.9.

10 Quotient Modules

10.1 Lemma

If N is a A-submodule of M, then the vector space quotient M/N becomes an A-module via the action

$$A \times (M/N) \to M/N, \quad (a, m+N) \mapsto am+N.$$

Moreover, the natural map $\pi\colon M \to M/N$ is a surjective module homomorphism with kernel N.

It follows that submodules are the same as kernels of module homomorphisms.

Proof. We first need to check that the action is well defined, so if $m+N = m'+N$ and $a \in A$, then $am+N = am'+N$. We can rewrite this as saying if $m-m' \in N$, then $am - am' \in N$. This is now clear, since $am - am' = a(m-m')$ and N is a submodule.

As the action on M/N is induced from the action on M it is immediately seen to be associtive, unital and bilinear, so does indeed define an A-module structure on M/N. Finally, we know that π is linear and surjective, and since $\pi(am) = am+N = a(m+N) = a\pi(m)$ it is also A-linear, so is a module homomorphism. □

10.2 Factor Lemma

Let $f\colon M \to L$ be a homomorphism of A-modules and $N \subset \mathrm{Ker}(f)$ a submodule of M. Then there is a unique module homomorphism $\bar{f}\colon M/N \to L$ such that $f = \bar{f}\pi$.

Proof. The existence and uniqueness of $\bar{f}$ as a linear map follow from the Factor Lemma for vector spaces. We therefore only need to check that $\bar{f}$ respects the action. Note that $\bar{f}(m+N) = \bar{f}\pi(m) = f(m)$, so

$$\bar{f}(a(m+N)) = \bar{f}(am+N) = f(am) = af(m) = a\bar{f}(m+N)$$

as required. □

10.3 Lemma

Suppose that $L = M \oplus N$. Then the natural map $L \to L/N$ induces an isomorphism $M \cong L/N$.

Proof. Let $\theta\colon M \to L/N$ be the restriction of the natural map to M. The kernel is $M \cap N = \{0\}$, so θ is injective. On the other hand, any $l \in L$ can be written as $l = m+n$ with $m \in M$ and $n \in N$, so $l-m = n \in N$, whence $l+N = m+N$. Therefore θ is also surjective. □

10.4 First Isomorphism Theorem

Let $f\colon M \to L$ be a module homomorphism. Then the induced module homomorphism

$$\bar{f}\colon M/\operatorname{Ker}(f) \to \operatorname{Im}(f)$$

is an isomorphism.

Proof. The Factor Lemma for modules tells us that $\bar{f}$ is a module homomorphism. On the other hand, we know it is an isomorphism of vector spaces, so it is a module isomorphism. □

10.5 Direct products again

Let M and N be A-modules, and consider their direct product $M \times N$. Then the natural maps

$$\iota_1\colon M \to M \times N, \quad m \mapsto (m,0), \quad \text{and} \quad \iota_2\colon N \to M \times N, \quad n \mapsto (0,n),$$

are monomorphisms, and

$$\pi_1\colon M \times N \to M, \quad (m,n) \mapsto m, \quad \text{and} \quad \pi_2\colon M \times N \to N, \quad (m,n) \mapsto n$$

are epimorphisms. Moreover,

$$\operatorname{Im}(\iota_1) = \operatorname{Ker}(\pi_2) = M' := \{(m,0) : m \in M\}$$
$$\operatorname{Im}(\iota_2) = \operatorname{Ker}(\pi_1) = N' := \{(0,n) : n \in N\},$$

inducing isomorphisms $M \cong M'$ and $N \cong N'$, and $M \times N = M' \oplus N'$. For this reason people often abuse notation and write $M \oplus N$ for the direct product $M \times N$.

10.6 Generating sets

If M is an A-module and $X \subset M$ a subset, then we can define the smallest submodule containing X, or the submodule **generated** by X, and this equals the intersection over all submodules containing X. In particular, we can talk about generating sets for M, and we say that M is **finitely generated** provided it has a finite generating set.

If $X = \{x_i : i \in I\}$, then we can define a module homomorphism

$$A^{(I)} \to M, \quad (a_i) \mapsto \sum_i a_i x_i.$$

Note that this makes sense, since almost all the a_i are zero, so the sum is actually finite.

The image of this module homomorphism clearly equals the submodule generated by X, which must therefore equal

$$\operatorname{span}\{ax : a \in A,\, x \in X\}.$$

Finally if X generates M, then the First Isomorphism Theorem gives an isomorphism $M \cong A^{(I)}/N$ for some submodule $N \leq A^{(I)}$.

11 More on homomorphism spaces

11.1 Lemma

The map

$$\Phi\colon \operatorname{Hom}_A(A, M) \to M, \quad f \mapsto f(1),$$

is an isomorphism of vector spaces.

Proof. We first check that Φ is linear. Let $f, g \in \operatorname{Hom}_A(A, M)$ and $\lambda \in K$. Then

$$\Phi(f + \lambda g) = (f + \lambda g)(1) = f(1) + \lambda g(1) = \Phi(f) + \lambda\Phi(g).$$

It is injective, since if $\Phi(f) = 0$, then $f(a) = f(a1) = af(1) = 0$ for all $a \in A$, so $f = 0$.

To see that Φ is surjective, let $m \in M$ and consider the map

$$r_m\colon A \to M, \quad a \mapsto am.$$

This is linear, since

$$r_m(a + \lambda b) = (a + \lambda b)m = am + \lambda bm = r_m(a) + \lambda r_m(b).$$

Moreover it respects the action, since

$$r_m(ab) = (ab)m = a(bm) = ar_m(b).$$

Hence $r_m \in \operatorname{Hom}_A(A, M)$ is a module homomorphism, and clearly

$$\Phi(r_m) = r_m(1) = 1m = m. \qquad \square$$

11.2 Opposite algebra

If A is an algebra, then the **opposite algebra** A^{op} is the algebra with the same vector space as A, but with new multiplication

$$A \times A \to A, \quad (a, b) \mapsto a \cdot b := ba.$$

This is clearly still associative, unital and bilinear, so A^{op} is indeed an algebra.

11.3 Lemma

The vector space isomorphism

$$\Phi\colon \mathrm{End}_A(A) \to A, \quad f \mapsto f(1),$$

induces an algebra isomorphism $\mathrm{End}_A(A) \cong A^{\mathrm{op}}$.

Proof. Suppose $\Phi(f) = a$ and $\Phi(g) = b$. Then

$$\Phi(fg) = (fg)(1) = f(g(1)) = f(b) = f(b1) = bf(1) = ba = \Phi(g)\Phi(f),$$

so $\Phi(fg) = \Phi(f)\cdot\Phi(g)$. Also, $\Phi(\mathrm{id}_A) = \mathrm{id}_A(1) = 1$. Thus Φ is indeed an algebra isomorphism. □

11.4 Homomorphisms between direct products

We now show that homomorphisms of direct products can be regarded as matrices, acting via matrix multiplication.

Let $M = M_1 \times M_2$ and $N_1 \times N_2$ be direct products. Given homomorphisms $f_{ij} \in \mathrm{Hom}_A(M_j, N_i)$, we can consider the 'matrix'

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix},$$

and this determines a homomorphism $f\colon M \to N$ via 'matrix multiplication'

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} f_{11}(m_1) + f_{12}(m_2) \\ f_{21}(m_1) + f_{22}(m_2) \end{pmatrix}.$$

11.5 Proposition

Let $M = M_1 \times M_2$ and $N = N_1 \times N_2$ be direct products. Then there is an isomorphism of vector spaces

$$\Theta\colon \mathrm{Hom}_A(M,N) \xrightarrow{\sim} \begin{pmatrix} \mathrm{Hom}_A(M_1,N_1) & \mathrm{Hom}_A(M_2,N_1) \\ \mathrm{Hom}_A(M_1,N_2) & \mathrm{Hom}_A(M_2,N_1) \end{pmatrix},$$

sending a homomorphism to its matrix.

Proof. Recall that M comes equipped with the natural homomorphisms

$$\iota_i\colon M_i \to M \quad \text{and} \quad \pi_i\colon M \to M_i$$

satisfying the formulae

$$\pi_i\iota_j = \delta_{ij}\mathrm{id}_{M_i} \quad \text{and} \quad \iota_1\pi_1 + \iota_2\pi_2 = \mathrm{id}_M.$$

Similarly $N = N_1 \times N_2$ comes equipeed with the homomorphisms $\bar{\iota}_i$ and $\bar{\pi}_i$.

Given $f\colon M \to N$, the entries of the matrix $\Theta(f) = (f_{ij})$ are given by the compositions

$$f_{ij} := \bar{\pi}_i\, f\, \iota_j.$$

Conversely, given a matrix (f_{ij}), the homomorphism f determined by matrix multiplication can be written as

$$f = \sum_{i,j} \bar{\iota}_i \, f_{ij} \, \pi_j.$$

Sums and compositions of module homomorphisms are again module homomorphisms, so these constructions really do give maps between $\mathrm{Hom}_A(M,N)$ and matrices $\big(\mathrm{Hom}_A(M_j,N_i)\big)$. Moreover, since composition of homomorphisms is bilinear, these constructions are actually linear maps.

We now check that these constructions are mutually inverse. Starting from f we first form $f_{ij} = \bar{\pi}_i \, f \, \iota_j$, and then take the sum

$$\sum_{i,j} \bar{\iota}_i \, f_{ij} \, \pi_j = \sum_{i,j} \bar{\iota}_i \bar{\pi}_i \, f \, \iota_j \pi_j = \Big(\sum_i \bar{\iota}_i \bar{\pi}_i \Big) \, f \, \Big(\sum_j \iota_j \pi_j \Big) = f.$$

Conversely, starting from f_{ij}, we form the sum $f = \sum_{p,q} \bar{\iota}_p \, f_{pq} \, \pi_q$, and then take the compositions

$$\bar{\pi}_i \, f \, \iota_j = \sum_{p,q} \bar{\pi}_i \bar{\iota}_p \, f \, \pi_q \iota_j = \sum_{p,q} \delta_{ip} \delta_{jq} f_{ij} = f_{ij}. \qquad \square$$

This construction generalises to arbitrary finite direct products $M = M_1 \times \cdots \times M_m$ and $N = N_1 \times \cdots \times N_n$.

11.6 Proposition

Let M be an A-module and set $E := \mathrm{End}_A(M)$. Then the vector space isomorphism

$$\Theta \colon \mathrm{End}_A(M^n) \xrightarrow{\sim} \mathbb{M}_n(E)$$

is in fact an algebra isomorphism.

Proof. Recall that $\Theta(f) = (f_{ij})$, where $f_{ij} = \pi_i \, f \, \iota_j$. We need to check that Θ respects the multiplication and preserves the unit.

We have

$$(fg)_{ij} = \pi_i \, fg \, \iota_j = \pi_i \, f \, \mathrm{id} \, g \, \iota_j = \sum_p \pi_i \, f \, \iota_p \pi_p \, g \, \iota_j = \sum_p f_{ip} g_{pj},$$

so Θ respects the multiplication. Also,

$$(\mathrm{id})_{ij} = \pi_i \, \mathrm{id} \, \iota_j = \pi_i \iota_j = \delta_{ij} \mathrm{id}_M,$$

so $\Theta(\mathrm{id})$ is the matrix having id_M on the diagonal and zero elsewhere, which is precisely the identity for $\mathbb{M}_n(E)$. Hence Θ is an algebra homomorphism. $\square$

Part III

Two Examples

12 Modules over the polynomial algebra

The idea of this section is to use representation theory, together with the fact that $K[X]$ is a principal ideal domain, to prove the standard results about square matrices up to conjugation.

A representation of $K[X]$ is an algebra homomorphism $\rho\colon K[X] \to \mathrm{End}_K(V)$ for some vector space V. By the Universal Property the map $\rho \mapsto \rho(X)$ gives a bijection between representations and elements of $\mathrm{End}_K(V)$. We can therefore think of a $K[X]$-module as a pair (V, ϕ) consisting of a vector space V and an endomorphism ϕ of V. In particular, if $f \in K[X]$ is a polynomial, then $\rho(f) = f(\phi) \in \mathrm{End}_K(V)$, so the action of $K[X]$ on V is given by $fv := f(\phi)(v)$.

A homomorphism $\theta\colon (V, \phi) \to (W, \psi)$ is given by a linear map $\theta\colon V \to W$ such that $\theta f(\phi) = f(\psi)\theta$ for all $f \in K[X]$. Since composition is associative and bilinear, this is the same as saying $\theta\phi = \psi\theta$. In particular, the two representations are equivalent if and only if θ is an isomorphism, which is if and only if ϕ and ψ are conjugate.

If $\dim V = n$ is finite, then we can choose a basis and hence view $\phi \in \mathbb{M}_n(K)$ as a matrix. It follows that studying finite-dimensional $K[X]$-modules up to isomorphism is the same as studying matrices up to conjugation.

12.1 Submodules

A submodule of (V, ϕ) is given by a subspace $U \leq V$ such that $f(\phi)(u) \in U$ for all $f \in K[X]$ and $u \in U$. Again, this is equivalent to saying that $\phi(u) \in U$ for all $u \in U$, so U is an **invariant subspace**. In particular, a one-dimensional submodule is given by $U = \mathrm{span}\{x\}$ for some $x \neq 0$ such that $\phi(x) \in U$. This is if and only if $\phi(x) = \lambda x$ for some $\lambda \in K$, so x is an eigenvector for ϕ.

Let $U \leq V$ be a vector subspace. Take a basis $\{e_1, \ldots, e_d\}$ for U and extend to a basis $\{e_1, \ldots, e_n\}$ for V, and let $\phi \in \mathbb{M}_n(K)$ be the matrix with respect to this basis. Then the first d columns of the matrix span the subspace $\phi(U)$, so U is a submodule if and only if these column vectors again lie in U, which is if and only if ϕ has an upper-triangular block shape, with zeros in the bottom left block.

In summary, finding submodules of (V, ϕ) is the same as finding a nice basis for V for which ϕ has an upper-triangular block shape.

Note further that the quotient space V/U has basis (the images of) the vectors $\{e_{d+1}, \ldots, e_n\}$. Thus if U is a submodule of V, then the module structure on the quotient space V/U is given by the bottom right block of ϕ.

12.2 Direct sums

Let (V, ϕ) be a module and suppose $V = U \oplus U'$ for some subspaces U, U'. If we take a basis for V given by the union of a basis for U and a basis for U', then U and U' are both submodules if and only if the matrix of ϕ has block-diagonal shape with respect to this basis, with upper left block $\phi|_U$ and bottom right block $\phi|_{U'}$.

In other words, finding a direct sum decomposition of (V, ϕ) is the same as finding a basis of V with respect to which ϕ has block-diagonal shape.

12.3 Generalised eigenspaces

Let $g \in K[X]$. Then $g(\phi) \in \mathrm{End}_K(V)$ can be viewed as a module endomorphism of (V, ϕ). For, we just need to check that $g(\phi)$ commutes with ϕ. Now, since $Xg(X) = g(X)X$ as polynomials, we can apply the algebra homomorphism ρ to get $\phi g(\phi) = g(\phi)\phi$ as endomorphisms of V.

It follows that $\mathrm{Ker}(g(\phi))$ and $\mathrm{Im}(g(\phi))$ are submodules of (V, ϕ). Note that if $I = (g)$ is the ideal generated by g, then $IV = \mathrm{Im}(g(\phi))$.

As a special case, if $g = X - \lambda$, then $\mathrm{Ker}(\phi - \lambda)$ is the eigenspace corresponding to the eigenvalue λ, and if $g = (X - \lambda)^n$ where $\dim V = n$, then $\mathrm{Ker}(\phi - \lambda)^n$ is the generalised eigenspace corresponding to λ.

12.4 The minimal polynomial

The **annihilator** of (V, ϕ) is the kernel of the representation $\rho\colon X \mapsto \phi$, so

$$\mathrm{ann}(V, \phi) = \mathrm{Ker}(\rho).$$

This is an ideal of $K[X]$, so is generated by a monic polynomial m, uniquely determined since it is monic. We call m the **minimal polynomial** of (V, ϕ).

We observe that (V, ϕ) is naturally a module for the quotient algebra $K[X]/(m)$. By unique factorisation we can write $m = f_1^{a_1} \cdots f_r^{a_r}$ for pairwise distinct, monic irreducible polynomials f_i and positive integers a_i. Set $I_i := (f_i^{a_i})$. Then the ideals I_i are pairwise coprime and their intersection is just (m). Thus, by the Chinese Remainder Theorem, we have an algebra isomorphism

$$K[X]/(m) \cong K[X]/I_1 \times \cdots \times K[X]/I_r.$$

The point is now that every module for a direct product of algebras can be thought of as a direct sum of modules for the individual algebras. Thus

$$V = V_1 \oplus \cdots \oplus V_r,$$

where V_i is a module for $K[X]/(f_i^{a_i})$. In general there is a little subtlety involved in making this precise, using the restriction of scalars map. Alternatively, setting $p_i := f_i^{a_i}$ and $q_i = m/p_i$, we can just define $V_i := \mathrm{Ker}(p_i(\phi))$, observe that this also equals $\mathrm{Im}(q_i(\phi))$, and then check that everything works.

If K is algebraically closed, then $f_i = X - \lambda_i$ for some λ_i and this decomposition is precisely the generalised eigenspace decomposition of V. We immediately see that eigenvectors having distinct eigenvalues are necessarily linearly independent. (In general we cannot assume that each f_i is linear, but we still get such a decomposition.)

In particular, we have shown that every matrix is conjugate to one having block-diagonal form, and such that each block has a single eigenvalue. Moreover, a large part of this result can be computed explicitly. We can find the minimal polynomial by solving a system of linear equations. Namely we want scalars μ_i such that $\sum_i \mu_i \phi(e_j) = 0$ for all basis elements e_j. If we can factorise m (the only non-algorithmic part), then we can compute $\mathrm{Im}(q_i(\phi)) = \mathrm{Ker}(p_i(\phi))$. Taking bases then yields the decomposition. We should observe that none of this *requires* the use of a determinant (so follows the philosophy of the book *Linear Algebra Done Right*).

13 The Weyl Algebra

The **Weyl algebra** W is defined to be the $\mathbb{C}$-algebra having generators x and d subject to the relation $dx - xd = 1$

$$W := \mathbb{C}\langle x, d\rangle / (dx - xd - 1).$$

We claim that W has basis the elements $x^m d^n$ for $m, n \geq 0$. In particular, we can write every element $w \in W$ uniquely in the form

$$w = f_n(x)d^n + \cdots + f_1(x)d + f_0(x) \quad \text{for polynomials } f_i(x) \in \mathbb{C}[x].$$

Proof. Using the relation $dx = 1 + xd$ we can write any element of W as a linear combination of elements $x^m d^n$ with $m, n \geq 0$. Thus these elements span W. We will now use representation theory to prove that these elements are linearly independent, and so form a basis for W.

Consider $\mathbb{C}[t]$, with basis $\{1, t, t^2, \ldots\}$. The action

$$x \cdot t^n := t^{n+1} \quad \text{and} \quad d \cdot t^n := nt^{n-1}$$

endows $\mathbb{C}[t]$ with the structure of a W-module. For, by Proposition 6.11, we just need to check that

$$d \cdot (x \cdot t^n) - x \cdot (d \cdot t^n) = 1 \cdot t^n = t^n.$$

Now,

$$d \cdot (x \cdot t^n) = d \cdot t^{n+1} = (n+1)t^n \quad \text{and} \quad x \cdot (d \cdot t^n) = x \cdot nt^{n-1} = nt^n,$$

so

$$d \cdot (x \cdot t^n) - x \cdot (d \cdot t^n) = (n+1)t^n - nt^n = t^n$$

as required.

Suppose that $\sum_{m,n} \lambda_{m,n} x^m d^n = 0$ with $\lambda_{m,n} \in \mathbb{C}$ almost all zero. Note that

$$d^n \cdot t^s = s(s-1)\cdots(s-n+1)t^{s-n} = \frac{s!}{(s-n)!}t^{s-n} = n!\binom{s}{n}t^{s-n}.$$

In particular, $d^n \cdot t^s = 0$ for $n > s$ and $d^s \cdot t^s = s!$.

Assume by induction that $\lambda_{m,n} = 0$ for all m, n with $n < s$. Then

$$0 = \big(\sum_{m,n} \lambda_{m,n} x^m d^n\big) \cdot t^s = \sum_m \lambda_{m,s} x^m d^s \cdot t^s = s! \sum_m \lambda_{m,s} x^m \cdot 1 = s! \sum_m \lambda_{m,s} t^m.$$

This is an equality in the polynomial algebra $\mathbb{C}[t]$, so $\lambda_{m,s} = 0$ for all m. By induction, $\lambda_{m,n} = 0$ for all m, n as required. □

In fact, this action of W is the motivating construction for W: we view W as the algebra of differential operators with polynomial coefficients, so $d = \partial_x$. Then for all $f \in \mathbb{C}[x]$ the Chain Rule implies

$$(dx) \cdot f = \partial_x(xf) = f + x\partial_x f = (1 + xd) \cdot f.$$

More generally one has the n-th Weyl algebra W_n, which is the algebra of differential operators with polynomial coefficients in n variables. This has generators x_i, d_i for $1 \le i \le n$ and relations

$$x_i x_j = x_j x_i, \quad d_i d_j = d_j d_i, \quad d_j x_i - x_i d_j = \delta_{ij}.$$

A similar argument shows that W_n has basis the elements $x_1^{a_1} \cdots x_n^{a_n} d_1^{b_1} \cdots d_n^{b_n}$ for $a_i, b_i \ge 0$.

Part IV

Semisimple Algebras

14 Semisimple Modules and Schur's Lemma

14.1 Semisimple modules

A module M is said to be **simple**, or **irreducible**, provided that

1. $M \neq \{0\}$.
2. M has no submodules other than $\{0\}$ and itself.

We shall call a module M **semisimple** if it can be written as a finite direct sum of simple modules $M = S_1 \oplus \cdots \oplus S_n$.

14.2 Examples

1. Every one-dimensional module is simple.
2. If K is algebraically closed, then every matrix $\phi \in \mathbb{M}_n(K)$ has an eigenvector, so all (finite-dimensional) simple $K[X]$-modules are one-dimensional.

   We can write a simple module as (K, λ), with action $fv = f(\lambda)v$. These modules are pairwise non-isomorphic, since $(K, \lambda) \cong (K, \mu)$ if and only if there exists $0 \neq \theta \in K$ such that $\mu = \theta\lambda\theta^{-1} = \lambda$. Thus, up to isomorphism, the simple modules are in bijection with the elements of K.
3. The two-dimensional $\mathbb{R}[X]$-module determined by the matrix $\phi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is simple. For, this matrix has no real eigenvalues, and hence there is no one-dimensional submodule.
4. More generally, recall that for $K[X]$, direct sums correspond to block-diagonal matrices. Thus, provided K is algebraically closed, the $K[X]$-module (K^n, ϕ) is semisimple if and only if ϕ is diagonalisable.

   In particular, the module $(K^2, J_2(\lambda))$ given by a Jordan block matrix is not semisimple.
5. The action of the Weyl agebra W on the space of polynomials $\mathbb{C}[t]$ describes a simple module. For, given a non-zero submodule $U \leq \mathbb{C}[t]$, take $f \in U$. If $\deg(f) = n$, say $f = f_n t^n + \cdots + f_1 t + f_0$ with $f_i \in \mathbb{C}$ and $f_n \neq 0$, then $d^n \cdot f = n! f_n \in U$, so $1 \in U$. Thus $t^m = x^m \cdot 1 \in U$ for all m, so $U = \mathbb{C}[t]$.

14.3 Remark

Clearly every simple module is semisimple, as is the zero module since it is the empty sum.

A (finite) direct product of semisimple modules is again semisimple. As a special case, we know that every finite-dimensional vector space is isomorphic to some K^n. Thus every finite-dimensional K-module is semisimple, and the simple modules are precisely the one-dimensional vector spaces.

14.4 Lemma

Every non-zero finite-dimensional module M has both a simple submodule and a simple quotient module.

Proof. Let $S \leq M$ be a non-zero submodule of minimal dimension. Then S must be simple. For, if $T \leq S$ is a non-zero submodule, then $T \leq M$ is non-zero and $\dim T \leq \dim S$. By the minimality of S we also have $\dim T \geq \dim S$, so that $\dim T = \dim S$ and hence $T = S$.

This proves that M has a simple submodule. The proof showing that M has a simple quotient module is entirely analogous; we take a proper submodule $N < M$ of maximal dimension and use the Third Isomorphism Theorem to see that M/N is simple. □

Note that this result is not true for infinite-dimensional modules.

14.5 Lemma

The natural module K^n for the matrix algebra $\mathbb{M}_n(K)$ is simple. More generally, if D is a division algebra, then the natural module D^n for $\mathbb{M}_n(D)$ is simple.

Proof. Let $N \neq \{0\}$ be a submodule of D^n and let $x = (x_1, \ldots, x_n) \in N$ be non-zero, say with $x_j \neq 0$. Then $e_i = (x_j^{-1}E_{ij})x \in N$, so for all $y = (y_1, \ldots, y_n)$ in D^n we have $y = \sum_i y_i e_i \in N$. Thus $N = D^n$ and D^n is simple. □

14.6 Schur's Lemma

Let $\theta\colon S \to T$ be a module homomorphism. If S is simple, then θ is either zero or injective. If T is simple, then θ is either zero or surjective. In particular, if S is simple, then $\mathrm{End}_A(S)$ is a division algebra.

Proof. Recall that $\mathrm{Ker}(\theta) \leq S$ and $\mathrm{Im}(\theta) \leq T$ are submodules. If S is simple, then either $\mathrm{Ker}(\theta) = S$, so θ is zero, or else $\mathrm{Ker}(\theta) = \{0\}$, so θ is injective. If T is simple, then either $\mathrm{Im}(\theta) = \{0\}$, so θ is zero, or else $\mathrm{Im}(\theta) = T$, so θ is surjective.

If S is simple and $\theta \in \mathrm{End}_A(S)$ is non-zero, then θ is must be a bijection, hence an isomorphism, so invertible. □

14.7 Theorem

The following are equivalent for a module M.

1. M is semisimple.
2. M can be written as a sum of simple submodules $M = S_1 + \cdots + S_n$.

Proof. 1. $\implies$ 2. Immediate.

2. $\implies$ 1. We prove this by induction on n. Set $N = S_1 + \cdots + S_{n-1}$, which is semisimple by induction, and observe that $M = N + S_n$. Since S_n is simple, either $N \cap S_n = 0$, so $M = N \oplus S_n$, or else $N \cap S_n = S_n$, so $M = N$. In either case we deduce that M is semisimple. □

14.8 Remark

It follows from the proof that if $M = S_1 + \cdots + S_n$ is a sum of simple modules, then there is a subset $I \subset \{1, \ldots, n\}$ such that $M = \bigoplus_{i \in I} S_i$.

14.9 Complements

Let M be a module and $N \leq M$ a submodule. We say that N has a **complement** in M if there there exists a submodule $C \leq M$ with $M = N \oplus C$.

In general, complements do not exist.

14.10 Theorem

Let M be semisimple. Then every submodule $N \leq M$ has a **complement**. Moreover, both N and M/N are semisimple.

Proof. Write $M = S_1 \oplus \cdots \oplus S_n$ with S_i simple. Let $\pi \colon M \to M/N$ be the canonical map. Then clearly $M/N = \pi(S_1) + \cdots + \pi(S_n)$, and by Schur's Lemma $\pi(S_i)$ is either zero or isomorphic to S_i, hence simple. Thus M/N is a sum of simple modules, so is semisimple by the previous theorem.

In particular, following the remark, we can find a subset $I \subset \{1, \ldots, n\}$ such that $\pi(S_i)$ is simple for all $i \in I$ and $M/N = \bigoplus_{i \in I} \pi(S_i)$. Set $C = \bigoplus_{i \in I} S_i$. We claim that $M = N \oplus C$, so that C is a complement for N.

By construction, π induces an isomorphism $\pi \colon C \xrightarrow{\sim} M/N$, and so $N \cap C = 0$. Now let $m \in M$. Since $\pi(m) \in M/N = \pi(C)$, we can find $c \in C$ such that $\pi(c) = \pi(m)$. Then $\pi(m - c) = 0$, so $m - c \in N$, whence $m = n + c \in N \oplus C$.

Finally, since $N \cong M/C$ as in Lemma 10.3, we see that N is also semisimple. □

14.11 Remarks

Let $M = S_1 + \cdots + S_n$ be a sum of simple modules, and $N \leq M$ a submodule.

Note that, in the proofs of Theorem 14.7 and Theorem 14.10, we *cannot* compare N with the sum $(N \cap S_1) + \cdots + (N \cap S_n)$. For, it will generally be the case that $N \cap S_i = \{0\}$ for all i.

The easiest such example just uses vector spaces. Consider $M = K^2$ with standard basis $\{e_1, e_2\}$. Then the co-ordinate axes $S_i = \text{span}\{e_i\}$ are simple K-modules and $M = S_1 \oplus S_2$. Now the subspace $N := \text{span}\{e_1 + e_2\}$ is simple, but $N \cap S_i = \{0\}$ for both $i = 1, 2$.

On the other hand, the proof of the preceeding theorem shows that one of S_1, S_2 must be a complement for N (in fact both are in this case).

15 Wedderburn's Structure Theorem

15.1 Semisimple algebras

An algebra A is called a **semisimple algebra** if the regular module ${}_AA$ is semisimple.

Wedderburn's Theorem completely describes the structure of semisimple algebras.

15.2 Lemma

If D is a division algebra, then $\mathbb{M}_n(D)$ is a semisimple algebra.

Proof. The set of all matrices which are non-zero only in column i forms a submodule (left ideal) C_i of the regular module for $\mathbb{M}_n(D)$. Moreover, C_i is isomorphic to the natural module D^n, so is simple by Lemma 14.5. Since $\mathbb{M}_n(D) = C_1 \oplus \cdots \oplus C_n$, we see that the regular module is semisimple. □

15.3 Proposition

Let A be a semisimple algebra. Then every finitely generated A-module is semisimple.

Proof. Since M is finitely generated we obtain an isomorphism $M \cong A^n/N$ for some n and some submodule $N \leq A^n$. Now, since the regular module is semisimple, so too is the direct product A^n, and hence also the quotient A^n/N by Theorem 14.10. Thus M is semisimple. □

15.4 Theorem

An algebra A is a semisimple algebra if and only if every submodule of the regular module (left ideal of A) has a complement.

Proof. Let A be a semisimple algebra, and $I \leq A$ a left ideal. Then by Theorem 14.10 I has a complement.

For simplicity we will only prove the converse when A is finite dimensional. The general case will be given as a sequence of exercises.

Let $I \leq A$ be a semisimple submodule of maximal dimension. If $I \neq A$, then I has a non-zero complement J, so $A = I \oplus J$. By Lemma 14.4 J has a simple submodule S, but then $I \oplus S$ is a semisimple module of greater dimension — a contradiction. Thus $A = I$ and the regular module is semisimple. □

15.5 Theorem

Let A and B be semisimple algebras, and $I \lhd A$ a two-sided ideal. Then both A/I and $A \times B$ are semisimple algebras.

Proof. By the previous proposition, it is enough to show that every left ideal of A/I or $A \times B$ has a complement.

Consider first the quotient algebra A/I. Write $\pi\colon A \to A/I$ for the canonical map and let $J \leq A/I$ be a left ideal. Then $\pi^{-1}(J) \leq A$ is a left ideal, so has a complement C. Set $J' := \pi(C)$. Then $J' \leq A/I$ is again a left ideal, and $A/I = J \oplus J'$. Thus J' is a complement for J.

Now consider the direct product $A \times B$. We know that every left ideal of $A \times B$ is of the form $I \times J$ for left ideals $I \leq A$ and $J \leq B$. Since A and B are semisimple algebras, I and J have complements I' and J' respectively, so $A = I \oplus I'$ and $B = J \oplus J'$. Then

$$A \times B = (I \oplus I') \times (J \oplus J') = (I \times J) \oplus (I' \times J'),$$

so the left ideal $I' \times J'$ is a complement for $I \times J$. □

15.6 Wedderburn's Structure Theorem

An algebra A is a semisimple algebra if and only if it is isomorphic to a direct product of matrix algebras over division algebras

$$A \cong \mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_r}(D_r).$$

Proof. Lemma 15.2 says that any matrix algebra over a division algebra is a semisimple algebra, and Theorem 15.5 together with induction implies that a finite product of semisimple algebras is again a semisimple algebra. Thus, if

$$A \cong \mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_r}(D_r)$$

is a direct product of matrix algebras over division algebras, then A is a semisimple algebra.

Conversely, let A be a semisimple algebra. We know that the regular module ${}_AA$ is semisimple, so we can write it as a direct sum of simple modules

$${}_AA = S_1 \oplus \cdots \oplus S_s.$$

Grouping together isomorphic simple modules we can write

$$ {}_AA \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r} $$

with the S_i pairwise non-isomorphic simple modules.

We now compute endomorphism algebras of both sides. On the left we have from Lemma 11.3 that $\mathrm{End}_A(A) \cong A^{\mathrm{op}}$, or equivalently that $A \cong \mathrm{End}_A(A)^{\mathrm{op}}$.

On the other hand, Proposition 11.5 tells us that $\mathrm{End}_A(S_1^{n_1} \oplus \cdots \oplus S_r^{n_r})$ can be thought of as 'matrices' whose (i,j)-th entry is in $\mathrm{Hom}_A(S_j^{n_j}, S_i^{n_i})$. Now, Schur's Lemma gives that $\mathrm{Hom}_A(S_i, S_j) = 0$ for $i \neq j$, whereas $E_i := \mathrm{End}_A(S_i)$ is a division algebra. Then Proposition 11.5 once more implies $\mathrm{Hom}_A(S_i^{n_i}, S_j^{n_j}) = 0$ for $i \neq j$, whereas $\mathrm{End}_A(S_i^{n_i}) \cong \mathbb{M}_{n_i}(E_i)$ by Proposition 11.6. Thus the algebra $\mathrm{End}_A(S_1^{n_1} \oplus \cdots \oplus S_r^{n_r})$ consists only of 'diagonal matrices', and hence

$$ \mathrm{End}_A(S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}) \cong \mathbb{M}_{n_1}(E_1) \times \cdots \times \mathbb{M}_{n_r}(E_r). $$

Putting this together yields

$$ A^{\mathrm{op}} \cong \mathbb{M}_{n_1}(E_1) \times \cdots \times \mathbb{M}_{n_r}(E_r). $$

Finally, take opposite algebras of both sides. Note that, for all algebras A_i,

$$ (A_1 \times A_2)^{\mathrm{op}} \cong A_1^{\mathrm{op}} \times A_2^{\mathrm{op}} \quad \text{and} \quad \mathbb{M}_n(A_1)^{\mathrm{op}} \cong \mathbb{M}_n(A_1^{\mathrm{op}}). $$

Thus, if $D_i = E_i^{\mathrm{op}}$, then D_i is again a division algebra and

$$ A \cong \mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_r}(D_r). $$ □

15.7 Remarks

Wedderburn's Theorem doesn't just give us that a semisimple algebra is isomorphic to a direct product of matrix algebras over division algebras; it also gives us a characterisation of which division algebras occur and how big the matrix algebras are.

More precisely, if A is a semisimple algebra, then we get a factor $\mathbb{M}_n(D)$ for each simple module S (up to isomorphism); the division algebra D is then the (opposite of the) endomorphism algebra $\mathrm{End}_A(S)$, and the size n of the matrix algebra is exactly the multiplicity of S as a direct summand of A.

Note also that if A is a semisimple algebra, then every simple module is isomorphic to a direct summand of ${}_AA$. (See Exercise Sheet 5, Question 4.)

It follows that if D is a division algebra, then $\mathbb{M}_n(D)$ has only one simple module, the natural module $S = D^n$. We know that this occurs n times in the regular module; on the other hand, we also get that $\dim S = n \dim D$.

Finally, we remark that our definition of a semisimple algebra depended on the *left* regular module ${}_AA$ being semisimple. We could instead have considered the *right* regular module A_A. It is easy to see, however, that if D is a division algebra, then $\mathbb{M}_n(D)$ is semisimple both on the left and on the right. Therefore Wedderburn's Theorem implies that left semisimple algebras are the same as right semisimple algebras.

15.8 Examples

1. We saw in the exercises that if $\delta^2 \neq 1$, then $TL_3(\delta) \cong K \times \mathbb{M}_2(K)$. On the other hand, by considering the left ideal I generated by u_1, u_2, we see that I does not have a complement when $\delta^2 = 1$.

   Thus $TL_3(\delta)$ is semisimple if and only if $\delta^2 \neq 1$.

2. More generally, assume we are working over the complex numbers and set $U_m := \{k\pi/m : 1 \leq k \leq 2m\}$. If $\delta \neq 2\cos\theta$ for any $\theta \in U_m$ and $1 \leq m \leq n$, then $TL_n(\delta)$ is semisimple.

3. Consider the ideal $I = (X) \lhd K[X]$. Then $K[X]/I \cong K$, so any complement J to I must be one dimensional, say with basis element f. Then $Xf \in I \cap J = 0$, so $f = 0$, a contradiction. Hence I does not have a complement, so $K[X]$ is not a semisimple algebra.

16 Maschke's Theorem

Maschke's Theorem gives a sufficient condition for the group algebra of a finite group to be semisimple. We will see later that it is also a necessary condition.

16.1 Maschke's Theorem

Let G be a finite group, and suppose that $|G|$ is invertible in the field K. Then the group algebra KG is semisimple.

Proof. We will prove that submodules of (finite-dimensional) KG-modules always have a complement. In particular we can apply this to the regular module, and hence deduce from Theorem 15.4 that KG is a semisimple algebra.

Let M be a (finite-dimensional) KG-module and $N \leq M$ a submodule. Since $N \leq M$ is a vector subspace, we can find a *vector space* complement C' of N in M. Thus $M = N \oplus C'$ and the projection $\theta' \colon M \to N$, $n + c' \mapsto n$, is a linear map. It has kernel C' and satisfies $\theta'(n) = n$ for all $n \in N$.

We will use θ' to construct a KG-module homomorphism $\theta \colon M \to N$ such that $\theta(n) = n$ for all $n \in N$, whence $M = N \oplus \mathrm{Ker}(\theta)$.

Define the **Reynolds operator**, or **averaging operator**, to θ', giving

$$\theta(m) := \frac{1}{|G|} \sum_{g \in G} e_{g^{-1}} \theta'(e_g m).$$

Clearly θ is linear, so to be a KG-module homomorphism, we just need to check that $\theta(e_h m) = e_h \theta(m)$ for all $h \in G$ and $m \in M$. For this we first note that

$\{gh : g \in G\} = Gh = G$ for any fixed $h \in G$. Thus

$$\theta(e_h m) = \frac{1}{|G|}\sum_{g\in G} e_{g^{-1}}\theta'(e_g e_h m) = \frac{1}{|G|}\sum_{g\in G} e_h e_{(gh)^{-1}}\theta'(e_{gh}m)$$
$$= e_h \frac{1}{|G|}\sum_{g\in G} e_{g^{-1}}\theta'(e_g m) = e_h\theta(m)$$

as required.

We next check that $\theta(n) = n$ for all $n \in N$. Since N is a KG-module we have $e_g n \in N$ for all $n \in N$ and $g \in G$, and so $\theta'(e_g n) = e_g n$. Hence

$$\theta(n) = \frac{1}{|G|}\sum_{g\in G} e_{g^{-1}}\theta'(e_g n) = \frac{1}{|G|}\sum_{g} e_{g^{-1}}e_g n = \frac{1}{|G|}\sum_{g\in G} n = n.$$

Finally, $C := \mathrm{Ker}(\theta)$ is a KG-submodule of M. As $\theta(n) = n$ for all $n \in N$, we have $N \cap C = \{0\}$, so the sum $N + C$ is direct. On the other hand, given $m \in M$, set $n := \theta(m) \in N$ and $c := m - n$. Then $c \in \mathrm{Ker}(\theta) = C$, so $m = n + c \in N \oplus C$. Thus C is a complement to N. □

16.2 Corollary

If G is a finite group and $\mathrm{char}(K) = 0$, then KG is a semisimple algebra.

Proof. Since K has characteristic zero, $|G|$ is invertible in K. □

16.3 Converse to Maschke's Theorem

If $\mathrm{char}(K) = p > 0$ and G is a finite group of order divisible by p, then the group algebra KG is not semisimple.

Proof. Consider the augmentation ideal $I = \{\sum_g \lambda_g e_g : \sum_g \lambda_g = 0\}$. This is a submodule of the regular module, so if we can show that I has no complement in the regular module, then KG cannot be semisimple.

Any complement C has dimension 1, since $KG/I \cong K$. Let $y = \sum_g \lambda_g e_g \in C$ be non-zero. Since C is a submodule of the regular module (left ideal of KG), we must have $e_h y \in C$ for all $h \in G$, so $e_h y = \mu_h y$ for some $\mu_h \in K$. Now,

$$e_h y = \sum_g \lambda_g e_h e_g = \sum_g \lambda_g e_{gh} = \sum_g \lambda_{h^{-1}g} g \quad \text{whereas} \quad \mu_h y = \sum_g \mu_h \lambda_g e_g.$$

Equating coefficients shows that $\lambda_{h^{-1}g} = \mu_h \lambda_g$ for all $g, h \in G$.

Consider $\alpha := \sum_g \lambda_g \in K$. We have

$$\mu_h \alpha = \sum_g \mu_h \lambda_g = \sum_g \lambda_{h^{-1}g} = \sum_g \lambda_g = \alpha.$$

Therefore $\alpha(\mu_h - 1) = 0$ for all $h \in G$.

If $\alpha \neq 0$, then $\mu_h = 1$ for all $h \in G$. Therefore $\lambda_{hg} = \lambda_g$ for all h, so that all the coefficients are equal, say to λ. Thus $\alpha = |G|\lambda = 0$, since $|G| = 0 \in K$, contradicting $\alpha \neq 0$. Hence $\alpha = 0$, so that $y \in I$, contradicting that $I \cap C = \{0\}$.

We deduce that the augmentation ideal I has no complement in the regular module KG, and hence that KG is not a semisimple algebra. □

16.4 Examples

1. Consider the group $\mathbb{Z}_2$ of order two. Then $\mathbb{Q}\mathbb{Z}_2 \cong \mathbb{Q} \times \mathbb{Q}$.
2. More generally, if p is a prime, then $\mathbb{C}\mathbb{Z}_p \cong \mathbb{C}^p$.

   If we work over $\mathbb{Q}$ instead, then $\mathbb{Q}\mathbb{Z}_p \cong \mathbb{Q} \times \mathbb{Q}(\zeta_p)$, where $\zeta_p \in \mathbb{C}$ is a primitive root of unity, and $\mathbb{Q}(\zeta_p) \subset \mathbb{C}$ is the subfield generated by ζ_p.
3. In fact, if G is abelian and $|G| = n$, then $\mathbb{C}G \cong \mathbb{C}^n$.
4. For the symmetric group S_3 we have $\mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{M}_2(\mathbb{Q})$.
5. Consider the group algebra $\mathbb{Q}G$ and the augmentation ideal I, with basis $\{e_g - 1 : g \neq 1\}$. By Maschke's Theorem, I must have a (one-dimensional) complement in the regular module. If you follow the construction of the proof, you will find that this complement is spanned by $\sum_g g$.
6. As an example of the converse to Maschke's Theorem, consider the finite field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ with two elements, and the cyclic group $\mathbb{Z}_2 = \{1, g\}$ also having two elements. Then $\mathbb{F}_2\mathbb{Z}_2$ has four elements, namely

   $$\mathbb{F}_2\mathbb{Z}_2 = \{0, 1, e_g, 1 + e_g\}.$$

   The augmentation ideal I equals $\{0, 1 + e_g\}$, so if C were a complement, then either $1 \in C$, so $e_g \cdot 1 = e_g \in C$, or $e_g \in C$, so $e_g \cdot e_g = 1 \in C$. Thus both $1, e_g \in C$, so $1 + e_g \in C \cap I$, a contradiction.

16.5 Remarks (non-examinable)

Let G be a finite group of order n, and K an algebraically-closed field of characteristic not dividing n, so the group algebra KG is semisimple.

Let $S_1, \ldots, S_r$ be all the simple KG-modules, up to isomorphism. We will see later in Theorem 20.3 that, since K is algebraically closed, $\mathrm{End}_{KG}(S_i) = K$. Thus Wedderburn's Theorem gives

$$KG \cong \mathbb{M}_{d_1}(K) \times \cdots \times \mathbb{M}_{d_r}(K)$$

and hence that

$$|G| = n = \dim KG = d_1^2 + \cdots + d_r^2.$$

Also, as in the remarks following Wedderburn's Theorem, we can also interpret d_i as the dimension of the simple S_i, so $d_i = \dim S_i$.

In other words, the order of the group is the sum of the squares of the dimensions of its simple modules.

(We can also interpret the number r of simple modules as the number of conjugacy classes in G, but that's another story.)

17 The Jacobson Radical

The definition of a semisimple algebra is in terms of the regular representation. We now wish to give an 'internal' description, in terms of the algebra structure. We will do this via the Jacobson radical of the algebra.

17.1 Definition

The **(Jacobson) radical** of an algebra A is the set of elements annihilating all simple modules

$$J(A) := \{a \in A : aS = 0 \text{ for all simple } A\text{-modules } S\}.$$

If we define the **annihilator** of a module M to be

$$\mathrm{Ann}(M) := \{a \in A : aM = 0\},$$

then

$$J(A) = \bigcap_{S \text{ simple}} \mathrm{Ann}(S).$$

17.2 Lemma

Each annihilator is an ideal in A, and hence $J(A)$ is an ideal in A.

Proof. Let M be a module and $\rho\colon A \to \mathrm{End}_K(M)$ the corresponding representation. Then $\mathrm{Ann}(M) = \mathrm{Ker}(\rho)$, so is an ideal. □

17.3 Theorem

A finite-dimensional algebra A is semisimple if and only if $J(A) = \{0\}$.

Proof. First suppose that A is semisimple. Then ${}_AA = S_1 \oplus \cdots \oplus S_n$ is a direct sum of simple modules. Write $1 = x_1 + \cdots + x_n$ with $x_i \in S_i$. If $a \in J(A)$, then $aS_i = \{0\}$ for all i, so $ax_i = 0$. Thus $a = a1 = ax_1 + \cdots + ax_n = 0$, so $J(A) = \{0\}$.

Suppose instead that $J(A) = \{0\}$. We will show that there exists a monomorphism from the regular module to a semisimple module. Since all submodules of semisimple modules are themselves semisimple, by Theorem 14.10, this will prove that the regular module is semisimple, and so A is a semisimple algebra.

Suppose we have a module homomorphism $\theta\colon {}_AA \to M$ with M semisimple. Let $I \leq A$ be its kernel (a left ideal). Suppose $0 \neq b \in I$. Since $J(A) = \{0\}$ we know that $b \notin J(A)$; that is, there exists some simple module S with $bS \neq \{0\}$, so $bx \neq 0$ for some $x \in S$. We now consider the semisimple module $M \times S$ and the module homomorphism

$$\phi\colon A \to M \times S, \quad a \mapsto (\theta(a), ax).$$

Now

$$\mathrm{Ker}(\phi) = \{a \in A : \theta(a) = 0,\ ax = 0\} = \{a \in I : ax = 0\} \leq I$$

and since $b \in I$ but $bx \neq 0$ we deduce that $\mathrm{Ker}(\phi)$ is strictly smaller than I.

Therefore, starting from the zero map ${}_AA \to \{0\}$, which has kernel A, and using that A is finite dimensional, we can construct the required monomorphism from A to a semisimple module. □

17.4 Nilpotent Ideals

Given ideals I and J of A, we can form their product $IJ = \mathrm{span}\{xy : x \in I, y \in J\}$ and this is again an ideal of A. In particular, given any ideal I we can define its n-th power I^n for $n > 0$. For convenience we set $I^0 = A$.

We say that an ideal I is **nilpotent** provided $I^n = \{0\}$ for some $n > 0$.

Note that $I^n = \mathrm{span}\{x_1 x_2 \cdots x_n : x_i \in I\}$. Thus $I^n = \{0\}$ if and only if $x_1 \ldots x_n = 0$ for all $x_i \in I$. In particular, if $I^n = \{0\}$, then $x^n = 0$ for all $x \in I$, but the converse does not hold in general.

17.5 Example

Let $A \leq \mathbb{M}_n(K)$ be the subalgebra of upper-triangular matrices and I the ideal of strictly upper-triangular matrices. Then I is a nilpotent ideal in A.

For, I has basis E_{ij} for $j - i \geq 1$. Therefore I^r is spanned by the products $E_{i_1 j_1} E_{i_2 j_2} \cdots E_{i_r j_r}$ such that $i_s < j_s$ for $1 \leq s \leq r$. This product is non-zero if and only if $i_s = j_{s-1}$ for all s, in which case it equals $E_{i_1 j_r}$ and $j_r - i_1 \geq r$. On the other hand, if $j - i \geq r$, then $E_{ij} = E_{ii+1} E_{i+1i+2} \cdots E_{i+r-1j}$ and so $E_{ij} \in I^r$.

This proves that I^r has basis E_{ij} for $j - i \geq r$, so consists of those matrices which are only non-zero above the 'r-th upper diagonal'. In particular, $I^n = 0$, so I is nilpotent.

17.6 Proposition

If I is a nilpotent ideal in A, then $I \leq J(A)$.

Proof. Let S be a simple module. Recall from Section 9.8 that $IS = \mathrm{span}\{xs : x \in I, s \in S\}$ is a submodule of S. Therefore either $IS = \{0\}$ or S. If $IS = S$, then by induction $I^r S = S$ for all $r \geq 1$. Since I is nilpotent, though, we have $I^n = \{0\}$ for some $n \geq 1$, so $S = I^n S = \{0\}$, a contradiction.

Thus $IS = \{0\}$, so $I \leq \mathrm{Ann}(S)$. This holds for all simples S, so $I \leq J(A)$. □

17.7 Lemma

Let $I \lhd A$ be an ideal, M an A-module, and $N \leq M$ a submodule. Then

$$I(M/N) = (IM + N)/N.$$

Proof. We have

$$I(M/N) = \text{span}\{x(m+N) = xm + N : x \in I, m \in M\},$$

so its preimage in M (under the canonical map $\pi\colon M \to M/N$) is the submodule $IM + N$. Thus $I(M/N) = (IM + N)/N$. □

17.8 Nakayama's Lemma

Let M be a finite-dimensional A-module. If $J(A)M = M$, then $M = \{0\}$.

Proof. Assume $M \neq \{0\}$, so M has a simple quotient module by Lemma 14.4, say M/N. Then, using the previous lemma, we have

$$0 = J(A)(M/N) = (J(A)M + N)/N = (M + N)/N = M/N,$$

contradicting that M/N is simple, so non-zero. □

17.9 Theorem

Let A be a finite-dimensional algebra. Then $J(A)$ is nilpotent, so is the unique largest nilpotent ideal of A. In particular, A is semisimple if and only if it has no non-zero nilpotent ideals.

Proof. Clearly $J(A)^{n+1} \leq J(A)^n$, so $\dim J(A)^{n+1} \leq \dim J(A)^n$. Since A is finite-dimensional, we can have only finitely many strict inequalities, so there exists $n \geq 1$ with $J(A)^{n+1} = J(A)^n$. Applying Nakayama's Lemma to the finite-dimensional A-module $J(A)^n$, we see that $J(A)^n = \{0\}$. □

17.10 Theorem

Let A be a finite-dimensional algebra and $I \lhd A$ an ideal. Then A/I is a semisimple algebra if and only if $J(A) \leq I$. In particular, $A/J(A)$ is a semisimple algebra, and is the largest semisimple quotient algebra of A.

Proof. For simplicity set $J := J(A)$.

Suppose first that A/I is a semisimple algebra and write $\pi\colon A \to A/I$ for the canonical map. We know that $J \lhd A$ is a nilpotent ideal, so $\pi(J) \lhd A/I$ is also a nilpotent ideal. Thus $\pi(J) = 0$ by the previous theorem, so $J \leq \text{Ker}(\pi) = I$.

Conversely, let $I \lhd A$ be an ideal containing J. By the Third Isomorphism Theorem we have $A/I \cong (A/J)/(I/J)$, so A/I is a quotient algebra of A/J and thus by Theorem 15.5 it is enough to prove that A/J is a semisimple algebra.

Write $\pi\colon A \to A/J$ for the canonical map. Let $L \lhd A/J$ be a nilpotent ideal and set $M := \pi^{-1}(L) \lhd A$. We have $M^r = \text{span}\{x_1 \cdots x_r : x_i \in M\}$, so $\pi(M^r) = L^r$. As L is nilpotent, $\pi(M^n) = 0$ for some n, so $M^n \leq \text{Ker}(\pi) = J$. Now J is also nilpotent by the previous theorem, so M^n is nilpotent, whence M itself is nilpotent. Thus $M \leq J$ by Proposition 17.6, so $L = \pi(M) = 0$.

Thus A/J has no non-zero nilpotent ideals, so is a semisimple algebra. □

17.11 Corollary

Let A be a finite-dimensional algebra and $I \lhd A$ an ideal. If I is nilpotent and A/I is a semisimple algebra, then $I = J(A)$.

Proof. As I is nilpotent we have $I \subset J(A)$ by Prop 17.6. On the other hand, as A/I is semisimple we have $J(A) \subset I$ by the theorem. Thus $I = J(A)$. □

17.12 Remark

In general there is no easy way to compute $J(A)$ directly, but it may be possible to find I satisfying the conditions of the corollary.

For example, if $A = S \oplus I$ with S a semisimple subalgebra and I a nilpotent ideal, then $I = J(A)$ and $A/J(A) \cong S$.

17.13 Examples

1. Let A be the algebra of upper-triangular 3×3-matrices

$$A = \left\{ \begin{pmatrix} a & d & f \\ 0 & b & e \\ 0 & 0 & c \end{pmatrix} : a, \ldots, f \in K \right\}.$$

   Then $J(A)$ consists of all strictly upper-triangular matrices, and the quotient is isomorphic to K^3. For, consider

$$I := \left\{ \begin{pmatrix} 0 & d & f \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} \right\} \quad \text{and} \quad S := \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \right\}.$$

   Then $A = S \oplus I$, I is a nilpotent ideal, and $S \cong K^3$ is a semisimple subalgebra. Thus $I = J(A)$ and $A/J(A) \cong K^3$.

2. Let

$$A := \left\{ \begin{pmatrix} a & b & x \\ c & d & y \\ 0 & 0 & e \end{pmatrix} : a, \ldots, e, x, y \in K \right\}$$

   and consider

$$I := \left\{ \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \right\} \quad \text{and} \quad S := \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e \end{pmatrix} \right\}.$$

   Then $A = S \oplus I$, I is nilpotent (since it consists of strictly upper-triangular matrices), and $S \cong \mathbb{M}_2(K) \times K$ is a semisimple subalgebra. Thus $I = J(A)$ and $A/J(A) \cong \mathbb{M}_2(K) \times K$.

3. There is no general description of the Jacobson radical of the group algebra KG when $\mathrm{char}(K)$ divides $|G|$.

18 Clifford Algebras

18.1 Definition

Given $\lambda_1, \ldots, \lambda_n \in K$, the **Clifford algebra** $C_K(\lambda_1, \ldots, \lambda_n)$ is the K-algebra generated by elements $c_1, \ldots, c_n$ subject to relations

$$c_i^2 = \lambda_i \text{ for each } i \qquad \text{and} \qquad c_i c_j = -c_j c_i \text{ for all } i \neq j.$$

18.2 Theorem

The Clifford algebra $C := C_K(\lambda_1, \ldots, \lambda_n)$ has basis

$$\{c_{i_1} \cdots c_{i_r} : 1 \leq i_1 < \cdots < i_r \leq n\}.$$

In particular, $\dim C = 2^n$.

Proof. By definition, the set of words in the c_i span C. Using the relations $c_i c_j = -c_j c_i$ we see that C is spanned by all words $c_{i_1}^{m_1} \cdots c_{i_r}^{m_r}$ with $i_1 < \cdots < i_r$. Then, using that $c_i^2 = \lambda_i$, we see that C is spanned by the elements $c_{i_1} \cdots c_{i_r}$ with $i_1 < \cdots < i_r$.

For convience write $[n] = \{1, \ldots, n\}$. Given $I \subset [n]$, say $I = \{i_1, \ldots, i_r\}$ with $i_1 < \cdots < i_r$, set

$$c_I := c_{i_1} \cdots c_{i_r}.$$

We have therefore shown that the c_I for $I \subset [n]$ span C.

We now use representation theory to prove that the c_I are linearly independent. Let V be the K-vector space with basis v_I indexed by the subsets of $[n]$, so $\dim V = 2^n$. Given such a subset I we set

$$d_i(I) := |\{k \in I : k < i\}|.$$

We make V into a C-module via

$$c_i \cdot v_I := \begin{cases} (-1)^{d_i(I)} \lambda_i v_{I \setminus \{i\}} & \text{if } i \in I; \\ (-1)^{d_i(I)} v_{I \cup \{i\}} & \text{if } i \notin I. \end{cases}$$

To see that this does indeed define a C-action on V, we just need to check (using Proposition 6.11) that

$$c_i \cdot (c_i \cdot v_I) = \lambda_i v_I \quad \text{and} \quad c_i \cdot (c_j \cdot v_I) = -c_j \cdot (c_i \cdot v_I).$$

If $i \in I$, then

$$c_i \cdot (c_i \cdot v_I) = (-1)^{d_i(I)} \lambda_i c_i \cdot v_{I \setminus \{i\}} = (-1)^{2d_i(I)} \lambda_i v_I = \lambda_i v_I.$$

Similarly if $i \notin I$. Thus $c_i \cdot (c_i \cdot v_I) = \lambda_i v_I$ for all i and I.

Assume now that $i < j$. There are four possible cases, depending on whether i or j lie in the subset I. We can simplify this by assuming that $i, j \notin I$, and setting

$$I_i = I \cup \{i\}, \quad I_j = I \cup \{j\}, \quad I_{ij} = I \cup \{i, j\}.$$

Set $d := d_i(I)$ and $e := d_j(I)$. Then

$$d_i(I_i) = d_i(I_j) = d_i(I_{ij}) = d_i(I) = d$$

whereas

$$d_j(I_j) = d_j(I) = e, \quad \text{and} \quad d_j(I_i) = d_j(I_{ij}) = d_j(I) + 1 = e + 1.$$

Thus

$$\begin{aligned} c_i \cdot v_I &= (-1)^d v_{I_i}, & c_i \cdot v_{I_i} &= (-1)^d \lambda_i v_I, \\ c_i \cdot v_{I_j} &= (-1)^d v_{I_{ij}}, & c_i \cdot v_{I_{ij}} &= (-1)^d \lambda_i v_{I_j}, \end{aligned}$$

and similarly

$$\begin{aligned} c_j \cdot v_I &= (-1)^e v_{I_j}, & c_j \cdot v_{I_i} &= -(-1)^e v_{I_{ij}}, \\ c_j \cdot v_{I_j} &= (-1)^e \lambda_j v_I, & c_j \cdot v_{I_{ij}} &= -(-1)^e \lambda_j v_{I_i}. \end{aligned}$$

Therefore

$$\begin{aligned} c_i \cdot (c_j \cdot v_I) &= (-1)^{d+e} v_{I_{ij}}, & c_i \cdot (c_j \cdot v_{I_i}) &= -(-1)^{d+e} \lambda_i v_{I_j}, \\ c_i \cdot (c_j \cdot v_{I_j}) &= (-1)^{d+e} \lambda_j v_{I_i}, & c_i \cdot (c_j \cdot v_{I_{ij}}) &= -(-1)^{d+e} \lambda_i \lambda_j v_I, \end{aligned}$$

and similarly

$$\begin{aligned} c_j \cdot (c_i \cdot v_I) &= -(-1)^{d+e} v_{I_{ij}}, & c_j \cdot (c_i \cdot v_{I_i}) &= (-1)^{d+e} \lambda_i v_{I_j}, \\ c_j \cdot (c_i \cdot v_{I_j}) &= -(-1)^{d+e} \lambda_j v_{I_i}, & c_j \cdot (c_i \cdot v_{I_{ij}}) &= (-1)^{d+e} \lambda_i \lambda_j v_I. \end{aligned}$$

In all cases $J \in \{I, I_i, I_j, I_{ij}\}$ we see that $c_i \cdot (c_j \cdot v_J) = -c_j \cdot (c_i \cdot v_J)$. It follows that V is indeed a $C_K(\lambda_1, \ldots, \lambda_n)$-module.

We can now prove that the c_I are linearly independent. For, suppose that

$$\sum_I \mu_I c_I = 0$$

and apply this element to the vector $v_\emptyset \in V$. By induction on $|I|$ it is easy to see that $c_I \cdot v_\emptyset = v_I$. Therefore

$$0 = \big(\sum_I \mu_I c_I\big) \cdot v_\emptyset = \sum_I \mu_I c_I \cdot v_\emptyset = \sum_I \mu_I v_I.$$

Since the v_I are linearly independent in V, we deduce that $\mu_I = 0$ for all I. Hence the c_I are linearly independent in the Clifford algebra. □

18.3 Remark

In fact, we have actually just constructed the regular representation.

18.4 Examples

The following examples can all be proved in the following manner. We know the dimensions on both sides, so it is enough to prove that the map given is a surjective algebra homomorphism. We can use our knowledge of the algebra on the right hand side to show that the images of the c_i generate the whole algebra, and Proposition 6.11 to check that the map is an algebra homomorphism.

1. $C_{\mathbb{R}}(1) \cong \mathbb{R} \times \mathbb{R}$ via $c_1 \mapsto (1, -1)$.
2. $C_{\mathbb{R}}(-1) \cong \mathbb{C}$ via $c_1 \mapsto i$.
3. $C_{\mathbb{R}}(-1, -1) \cong \mathbb{H}$ via $c_1 \mapsto i$, $c_2 \mapsto j$.

   For, we have already seen that $\mathbb{H}$ is generated by i and j subject to the relations $i^2 = j^2 = -1$ and $ij = -ji$.
4. $C_{\mathbb{R}}(1, 1) \cong \mathbb{M}_2(\mathbb{R})$ via

$$c_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad c_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

5. We also have $C_{\mathbb{R}}(1, -1) \cong \mathbb{M}_2(\mathbb{R})$ via

$$c_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad c_2 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

6. $C_{\mathbb{R}}(1, 1, 1) \cong \mathbb{M}_2(\mathbb{C})$ via $c_i \mapsto \sigma_i$, where

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   are the Pauli spin matrices.

   For, it is easy to check that $\sigma_i^2 = I$ and $\sigma_i \sigma_j = -\sigma_j \sigma_i$ for $i \neq j$, so the map is an algebra homomorphism.

   Now, using 1 and σ_3 we see that E_{11} and E_{22} are in the image. Then, using σ_1 and σ_2 we get that E_{12}, E_{21}, iE_{12} and iE_{21} are all in the image. Finally $iE_{11} = iE_{12} \cdot E_{21}$ and $iE_{22} = iE_{21} \cdot E_{21}$ are in the image, so the map is onto.

18.5 Theorem

Suppose $\mathrm{char}(K) \neq 2$ and $\lambda_i \neq 0$ for all i. Then the Clifford algebra $C := C_K(\lambda_1, \ldots, \lambda_n)$ is semisimple.

Proof. The proof is similar in flavour to Maschke's Theorem, though the details are somewhat more involved. The idea there was to construct an averaging operator, turning any vector space complement into a module complement. The main ingredient for this construction was having a basis B of invertible elements such that $bb' \in B$ for all $b, b' \in B$.

We do the same thing for the Clifford algebra using the basis $\{c_I : I \subset [n]\}$, where if $I = \{i_1 < \cdots < i_r\}$, then $c_I = c_{i_1} \cdots c_{i_r}$. There is one minor change — each product $c_I c_J$ is a non-zero scalar multiple of another basis element.

Set $\lambda_I := \lambda_{i_1} \cdots \lambda_{i_r}$. Then

$$c_{i_r} \cdots c_{i_1} c_I = \lambda_I \quad \text{and} \quad c_{i_r} \cdots c_{i_1} = (-1)^{\binom{|I|}{2}} c_I,$$

so each c_I is invertible, with inverse $c_I^{-1} = (-1)^{\binom{|I|}{2}} \frac{1}{\lambda_I} c_I$. Moreover, since

$$c_I c_i = \begin{cases} (-1)^{e_i(I)} \lambda_i c_{I \setminus \{i\}} & \text{if } i \in I \\ (-1)^{e_i(I)} c_{I \cup \{i\}} & \text{if } i \notin I \end{cases} \qquad \text{where } \; e_i(I) := |\{k \in I : k > i\}|$$

we see that multiplying on the right by c_i just permutes and rescales the basis elements c_I. In other words, fixing i, there exist non-zero scalars μ_I such that $\{c_I c_i : I \subset [n]\} = \{\mu_I c_I : I \subset [n]\}$.

We can now construct an averaging operator exactly as in the proof of Maschke's Theorem. Let M be a (finite-dimensional) C-module, and $U \leq M$ a submodule. Choose a vector space complement V', so that $M = U \oplus V'$. Let $\theta' \colon M \to U$ be the corresponding projection map, sending $m = u + v' \mapsto u$. We now apply the averaging trick to θ' to get

$$\theta \colon M \to U, \quad \theta(m) := \frac{1}{2^n} \sum_I c_I^{-1} \theta'(c_I m).$$

We wish to show that θ is a C-module homomorphism and that $\theta(u) = u$ for all $u \in U$.

We have

$$\begin{aligned} \theta(c_i m) &= \frac{1}{2^n} \sum_I c_I^{-1} \theta'(c_I c_i m) = \frac{1}{2^n} \sum_I c_i (c_I c_i)^{-1} \theta'(c_I c_i m) \\ &= c_i \cdot \frac{1}{2^n} \sum_I (\mu_I c_I)^{-1} \theta'(\mu_I c_I m) = c_i \cdot \frac{1}{2^n} \sum_I c_I^{-1} \theta'(c_I m) \\ &= c_i \theta(c_i m), \end{aligned}$$

so θ is a C-module homomorphism. Also, since U is a submodule, if $u \in U$, then $c_I u \in U$ for all I and so $\theta'(c_I u) = c_I u$. Thus

$$\theta(u) = \frac{1}{2^n} \sum_I c_I^{-1} \theta'(c_I u) = \frac{1}{2^n} \sum_I c_I^{-1} c_I u = u.$$

It follows exactly as before that the kernel $V := \mathrm{Ker}(\theta)$ is a submodule of M and that $M = U \oplus V$. Thus V is a complement to U.

In particular every submodule of the regular module (left ideal of C) has a complement, so C is a semisimple algebra by Theorem 15.4. □

18.6 Remark

The converse of this theorem also holds; that if $\lambda_i = 0$ for some i, then the Clifford algebra is not semisimple. We will now prove this in the case when $\lambda_i = 0$ for all i, the so-called exterior algebra. The general case is very similar and will be discussed in the exercises.

18.7 Exterior Algebra

The **exterior algebra**, or **Grassmann algebra**, is $\Lambda := C_K(0,\dots,0)$. This is generated by $c_1,\dots,c_n$ subject to the relations

$$c_i^2 = 0 \quad \text{for all } i \quad \text{and} \quad c_i c_j = -c_j c_i \quad \text{for } i \neq j.$$

The exterior algebras are useful when dealing with multilinear alternating forms, for example the determinant.

18.8 Lemma

Given a matrix $A \in \mathbb{M}_n(K)$ there exists an algebra endomorphism

$$\theta\colon \Lambda \to \Lambda, \quad c_i \mapsto \sum_p a_{pi} c_p.$$

This satisfies

$$\theta(c_1 c_2 \cdots c_n) = \det(A) c_1 c_2 \cdots c_n.$$

Proof. By Proposition 6.11 we just need to check that

$$\theta(c_i)\theta(c_j) = -\theta(c_j)\theta(c_i) \quad \text{and} \quad \theta(c_i)^2 = 0.$$

We have

$$\theta(c_i)\theta(c_j) = \sum_{p,q} a_{pi} a_{qj} c_p c_q.$$

Using that $c_p c_q = -c_q c_p$ and $c_p^2 = 0$, we can rewrite this as

$$\theta(c_i)\theta(c_j) = \sum_{p<q} \big(a_{pi}a_{qj} - a_{qi}a_{pj}\big) c_p c_q.$$

It is now clear that this equals $-\theta(c_j)\theta(c_i)$, and equals 0 if $i = j$.

Since θ is an algebra endomorphism, we have

$$\theta(c_1 c_2 \cdots c_n) = \theta(c_1)\theta(c_2)\cdots\theta(c_n) = \sum_{p_1,p_2,\dots,p_n} a_{p_1 1} a_{p_2 2} \cdots a_{p_n n} c_{p_1} c_{p_2} \cdots c_{p_n}.$$

Since $c_p^2 = 0$, the only non-zero terms are when $p_1, p_2, \dots, p_n$ are all distinct. This happens if and only if $\sigma\colon i \mapsto p_i$ is a permutation of $\{1,\dots,n\}$. In this case we can use the characterisation

$$\operatorname{sgn}(\sigma) = |\{i < j : \sigma(i) > \sigma(j)\}|$$

to deduce that

$$c_{\sigma(1)} \cdots c_{\sigma(n)} = \operatorname{sgn}(\sigma) c_1 \cdots c_n.$$

Thus

$$\begin{aligned}\theta(c_1 \cdots c_n) &= \sum_\sigma a_{\sigma(1)1} \cdots a_{\sigma(n)n} c_{\sigma(1)} \cdots c_{\sigma(n)} \\ &= \sum_\sigma \operatorname{sgn}(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} c_1 \cdots c_n = \det(A) c_1 \cdots c_n,\end{aligned}$$

using the Leibniz Formula for $\det(A)$. □

18.9 Proposition

Recall that the exterior algebra $\Lambda := C_K(0,0,\ldots,0)$ has basis $\{c_I\}$ indexed by the subsets $I \subset \{1,\ldots,n\}$. The Jacobson radical of Λ is

$$J := \operatorname{span}\{c_I : I \neq \emptyset\} = \operatorname{span}\{c_I : |I| \geq 1\}.$$

Proof. Note that J is an ideal, since

$$c_i c_I = \begin{cases} \pm c_{I\cup\{i\}} & \text{if } i \notin I \\ 0 & \text{if } i \in I \end{cases} \qquad \text{and} \qquad c_I c_i = \begin{cases} \pm c_{I\cup\{i\}} & \text{if } i \notin I \\ 0 & \text{if } i \in I \end{cases}$$

In fact, this shows that $J^2 = \operatorname{span}\{c_I : |I| \geq 2\}$. An easy induction now gives $J^r = \operatorname{span}\{c_I : |I| \geq r\}$. Since there are no subsets of $\{1,\ldots,n\}$ with more than n elements, we must have $J^{n+1} = \{0\}$, and hence J is nilpotent.

Finally, $\Lambda/J = K$ is semisimple, so $J(\Lambda) = J$. Note that K is a subalgebra of Λ via the structure map (sending $\lambda \mapsto \lambda 1$), and $\Lambda = K \oplus J$. □

18.10 Remark (non-examinable)

The cross-product of vectors in $\mathbb{R}^3$ is an example of a bilinear alternating map, so is also related to the exterior algebra Λ. More precisely we have two linear maps

$$f\colon \mathbb{R}^3 \to \Lambda, \quad (x,y,z) \mapsto xc_1 + yc_2 + zc_3,$$
$$g\colon \mathbb{R}^3 \to \Lambda, \quad (x,y,z) \mapsto xc_2c_3 + yc_3c_1 + zc_1c_2$$

and the multiplication in the exterior algebra is related to the cross- and scalar-products of vectors via

$$f(u)f(v) = g(u \times v) \quad \text{and} \quad f(u)g(v) = (u \cdot v)c_1c_2c_3.$$

In particular, we recover Lemma 18.8, since if $A = (u|v|w) \in \mathbb{M}_3(\mathbb{R})$ and θ is the corresponding endomorphism of the exterior algebra, then

$$\theta(c_1c_2c_3) = f(u)f(v)f(w) = f(u)g(v \times w) = (u \cdot v \times w)c_1c_2c_3 = \det(A)c_1c_2c_3.$$

18.11 Symmetric Bilinear Forms (non-examinable)

In fact, the remainder of this section is non-examinable.

A **symmetric bilinear form** on a vector space V is a bilinear form

$$\beta\colon V \times V \to K, \quad (x,y) \mapsto \beta(x,y),$$

which is symmetric, so $\beta(x,y) = \beta(y,x)$. Let $e_1,\ldots,e_n$ be a basis for V. Then symmetric bilinear forms correspond to symmetric matrices $B = (b_{ij})$ via $b_{ij} = \beta(e_i,e_j)$.

Given a vector space V together with a symmetric bilinear form β, there is an associated Clifford algebra $C(V,\beta)$. This has generators the vectors in V and

relations $vw + wv = \beta(v, w)$ for all $v, w \in V$. If V has basis $e_1, \ldots, e_n$ and β corresponds to the matrix $B = (b_{ij})$, then we can define $C(V, \beta)$ to be the algebra with basis $c_1, \ldots, c_n$ and relations $c_i c_j + c_j c_i = b_{ij}$.

In particular, when $\mathrm{char}(K) \neq 2$, we recover our original definition of the Clifford algebra by taking the matrix (b_{ij}) with $b_{ij} = \frac{1}{2}\delta_{ij}\lambda_i$.

18.12 Definition

Let β be a symmetric bilinear form on V. We say that an endomorphism $\theta \in \mathrm{End}_K(V)$ **preserves** the form β provided $\beta(\theta(v), \theta(w)) = \beta(v, w)$ for all $v, w \in V$. In terms of matrices, if θ is represented by $A = (a_{ij})$, then θ preserves β if and only if $A^{\mathrm{tr}} B A = B$.

18.13 Examples

1. If B is the identity matrix, then A preserves the form if and only if A is an orthogonal matrix, so $A^{\mathrm{tr}} A = I$.

2. If B is the zero matrix, then every matrix A preserves the form.

18.14 Lemma

This lemma generalises Lemma 18.8.

Let (V, β) be a vector space equipped with a symmetric bilinear form. Suppose that the endomorphism $\theta \in \mathrm{End}_K(V)$ preserves the bilinear form β. Then θ extends to an algebra endomorphism

$$\theta \colon C(V, \beta) \to C(V, \beta), \quad v \mapsto \theta(v) \text{ for all } v \in V.$$

Proof. By Proposition 6.11 we just need to check that

$$\theta(v)\theta(w) + \theta(w)\theta(v) = \beta(v, w).$$

This is clear, since the left-hand side equals $\beta(\theta(v), \theta(w))$ and θ preserves the bilinear form β. □

As a special case we can consider the exterior algebra. Then $V = K^n$ and $\beta = 0$, so every endomorphism preserves β.

18.15 Discussion

Three-dimensional Euclidean space consists of the vector space $\mathbb{R}^3$ together with the symmetric bilinear form $\beta(x, y) = x_1 y_1 + x_2 y_2 + x_3 y_3$. The corresponding Clifford algebra is therefore $C = C_{\mathbb{R}}(1, 1, 1) \cong \mathbb{M}_2(\mathbb{C})$, by Example 18.4 (6).

Each rotation θ preserves β, so induces an automorphism of C.

Why does $\mathbb{H}$ appear when studying rotations? It is isomorphic to the subalgebra of C spanned by words of even length via

$$i \mapsto c_2c_3, \quad j \mapsto c_1c_3, \quad k \mapsto c_1c_2.$$

Note that this agrees with the embedding $\mathbb{H} \to \mathbb{M}_2(\mathbb{C})$ given in Exercise Sheet 3, Question 10.

Now, θ restricts to an automorphism of $\mathbb{H}$, and identifying the set of pure quaternions P with $\mathbb{R}^3$, we see that θ acts on P as a^{-1}. Moreover, the Skolem-Noether Theorem says that every automorphism is given by conjugation, so there exists a non-zero quaternion $q \in \mathbb{H}$ such that $\theta(x) = qxq^{-1}$ for all $x \in \mathbb{H}$, just as we saw in Theorem 1.8.

In special relativity one studies $\mathbb{R}^4$ with the quadratic form $x_1^2 - x_2^2 - x_3^2 - x_4^2$, and hence the corresponding Clifford algebra $C_{\mathbb{R}}(1, -1, -1, -1)$. See John Snygg, Clifford algebras: a computational tool for physicists.

19 The Jordan-Hölder Theorem

The Jordan-Hölder Theorem can be thought of as a generalisation of the fact that, over an algebraically-closed field K, every matrix ϕ is conjugate to one in upper-triangular form and the diagonal entries depend only on ϕ, not on the choice of basis (they are the roots of the characteristic polynomial of ϕ).

19.1 Composition series

A **composition series** for a module M is a finite chain of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = \{0\}$$

such that M_i/M_{i+1} is simple for $0 \leq i < n$.

The **length** of the chain is $\ell(M) = n$, and the simple modules M_i/M_{i+1} are called the **composition factors**.

Note: not every module has a composition series, and even when they exist, they are not unique.

19.2 Lemma

Every finite-dimensional module has a composition series.

Proof. If $M = \{0\}$, then the result is trivial, so assume M is non-zero. By Lemma 14.4 M has a simple submodule S, and $\dim M/S < \dim M$. By induction on dimension, M/S has a composition series

$$M/S = \overline{M}_0 \supset \overline{M}_1 \supset \cdots \supset \overline{M}_n = \{0\}.$$

Let $\pi\colon M \to M/S$ be the natural map and set $M_i := \pi^{-1}(\overline{M}_i)$. We claim that

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = S \supset M_{n+1} = \{0\}$$

is a composition series for M.

For $i = n$ we have $M_n/M_{n+1} \cong S$, whereas for $0 \leq i < n$ we can apply the Third Isomorphism Theorem to get

$$M_i/M_{i+1} \cong (M_i/S)/(M_{i+1}/S) = \overline{M}_i/\overline{M}_{i+1}.$$

Thus all successive quotient modules are simple. □

19.3 Proposition

Let M be a module and $N \leq M$ a submodule. Then M has a composition series if and only if both N and M/N do.

Proof. Let $\pi\colon M \to M/N$ be the canonical map. Suppose first that we are given composition series for N and M/N, say

$$N = F_0 \supset \cdots \supset F_r = \{0\} \quad \text{and} \quad M/N = G_0 \supset \cdots \supset G_s = \{0\}.$$

Set $M_i := \pi^{-1}(G_i)$ for $0 \leq i \leq s$ and $M_i := F_{i-s}$ for $s \leq i \leq r+s$. We claim that

$$M = M_0 \supset \cdots \supset M_s = N \supset \cdots \supset M_{r+s} = \{0\}$$

is a composition series for M.

Note first that $M_0 = \pi^{-1}(G_0) = M$ and $M_{r+s} = F_r = \{0\}$. Also, $\pi^{-1}(G_s) = N = F_0$, so that M_s is well-defined. Now, if $0 \leq i < s$, then $G_i = M_i/N$, so that $M_i/M_{i+1} \cong (M_i/N)/(M_{i+1}/N) = G_i/G_{i+1}$ by the Third Isomorphism Theorem. In particular, M_i/M_{i+1} is simple. Similarly, if $s \leq i < r+s$, then $M_i = F_{i-s}$, so that $M_i/M_{i+1} = F_{i-s}/F_{i-s+1}$ is also simple. Thus all successive quotient modules are simple.

We remark for later that the composition factors for M are just the composition factors of N and M/N combined.

Conversely, let

$$M = M_0 \supset \cdots \supset M_n = \{0\}$$

be a composition series for M. Set $F_i := M_i \cap N$ and consider the composition

$$F_i = M_i \cap N \to M_i \to M_i/M_{i+1}.$$

This has kernel $F_{i+1} = M_{i+1} \cap N$, so by the Factor Lemma we have a monomorphism $F_i/F_{i+1} \to M_i/M_{i+1}$. Since M_i/M_{i+1} is simple we deduce that either F_i/F_{i+1} is simple, or else it is zero and $F_i = F_{i+1}$. Therefore, upon removing repeated submodules, we obtain a composition series for N

$$N = F_0 \supset F_{i_1} \supset \cdots \supset F_{i_{r-1}} \supset F_n = \{0\},$$

where $i_0 < i_1 < \cdots < i_r$ is some subsequence of $1 < 2 < \cdots < n$.

Similarly, set $G_i := \pi(M_i) = (M_i + N)/N$. This time, consider the composition

$$M_i \to G_i \to G_i/G_{i+1}.$$

By the Second Isomorphism Theorem $G_i \cong M_i/(M_i \cap N)$, so $M_i \to G_i/G_{i+1}$ is onto. Clearly M_{i+1} is contained in the kernel, so by the Factor Lemma we have an epimorphism $M_i/M_{i+1} \to G_i/G_{i+1}$. Since M_i/M_{i+1} is simple we again deduce that G_i/G_{i+1} is either simple, or else it is zero and $G_i = G_{i+1}$. Removing repeated modules we obtain a composition series for M/N. □

19.4 Jordan-Hölder Theorem

Suppose M has a composition series. Then any two composition series of M have the same length and, after reordering, isomorphic composition factors.

Proof. Let

$$M_\bullet := \big(M = M_0 \supset \cdots \supset M_m = \{0\}\big)$$

be a composition series for M. We will prove the theorem by induction on m. Observe that if $m = 0$, then $M = \{0\}$ and the result holds.

Now suppose that $m \geq 1$. Note that the set of simple submodules of M is non-empty, since it contains M_1. Let $S \leq M$ be any simple submodule. By the previous proposition we obtain a composition series for the quotient $\overline{M} := M/S$ by setting $\overline{M}_i := (M_i + S)/S$ and removing repeated modules.

Since $M_i \cap S \leq S$ and S is simple, this submodule is either zero or S. Since $M_0 \cap S = S$ and $M_m \cap S = 0$ we can take j maximal such that $M_j \cap S = S$.

Now, $\overline{M}_i = M_i/S$ for all $i \leq j$ and the Third Isomorphism Theorem gives $\overline{M}_i/\overline{M}_{i+1} \cong M_i/M_{i+1}$ for all $i < j$.

On the other hand, $M_i \cap S = \{0\}$ for all $i > j$ and $\overline{M}_i \cong M_i/(M_i \cap S) \cong M_i$ by the Second Isomorphism Theorem, so $\overline{M}_i/\overline{M}_{i+1} \cong M_i/M_{i+1}$ for all $i > j$.

Finally, $M_{j+1} \oplus S$ is a submodule of M_j, so there is a monomorphism $S \to M_j \to M_j/M_{j+1}$. The right hand side is simple, so this is an isomorphism by Schur's Lemma. Thus $M_j = M_{j+1} \oplus S$ and $M_j/M_{j+1} \cong S$.

It follows that $\overline{M}_j = \overline{M}_{j+1}$, giving the following composition series for $\overline{M} := M/S$

$$\overline{M}_\bullet := \big(\overline{M} = \overline{M}_0 \supset \cdots \supset \overline{M}_j = \overline{M}_{j+1} \supset \cdots \supset \overline{M}_m = \{0\}\big).$$

Moreover, the composition factors for $M_\bullet$ are precisely the composition factors for $\overline{M}_\bullet$, together with S.

Observe that $\overline{M}$ has a composition series of length $m-1$, so by induction the theorem holds for $\overline{M}$. Therefore, if

$$M'_\bullet := \big(M = M'_0 \supset \cdots \supset M'_n = \{0\}\big)$$

is another composition series for M, then applying the same construction yields, for some k, the composition series

$$\overline{M}'_\bullet := \big(\overline{M} = \overline{M}'_0 \supset \cdots \supset \overline{M}_k = \overline{M}'_{k+1} \supset \cdots \supset \overline{M}'_n = \{0\}\big)$$

for $\overline{M}$. We deduce that $m-1 = n-1$ and that, up to reordering, the composition factors for $\overline{M}_\bullet$ and $\overline{M}'_\bullet$ are isomorphic. It follows that $m = n$ and that, up to reordering, the composition factors for $M_\bullet$ and $M'_\bullet$ are isomorphic. □

19.5 Corollary

Let M be a module, and $N \leq M$ a submodule. If M has a composition series, then $\ell(M) = \ell(N) + \ell(M/N)$ and the composition factors of M are just the composition factors of N and M/N combined.

Proof. We know from Proposition 19.3 that M has a composition series if and only if both N and M/N do. Moreover, we remarked in the proof of that result that, given composition series for N and M/N, we can construct a composition series for M having composition factors those of N and M/N combined. Finally, the Jordan-Hölder Theorem tells us that these composition factors are independent of the choice of composition series. □

19.6 Example

Let $M = S_1 \oplus \cdots \oplus S_n$ be semisimple. Then $\ell(M) = n$ and M has composition factors $S_1, \ldots, S_n$.

19.7 Remark

Over a field K, a module is the same as a vector space, and the length as a module equals the dimension as a vector space, provided this is finite.

In general, the length is a more appropriate measure for modules than dimension, with the simple modules playing a role similar to that of one-dimensional vector spaces. One can think of the simple modules as the 'building blocks' for modules; the composition factors tell you which blocks are needed to make that module (but not how they are 'glued together'); the length just tells you how many blocks are needed in total.

However, the analogy with vector spaces only goes so far. Every vector space has a basis, which implies that every module over K is semisimple, but this does not happen for general algebras. We will study when this happens in the next section.

19.8 Example

Let K be algebraically closed. Recall that $K[X]$-modules correspond to pairs (V, ϕ) and submodules correspond to invariant subspaces, so subspaces $U \leq V$ with $\phi(U) \subset U$. Thus one-dimensional submodules of V are spanned by eigenvectors, and since every matrix has an eigenvalue, all (finite-dimensional) simple modules are one dimensional. It follows that the length of a module equals its dimension.

Next recall that finding a submodule is the same as finding a basis for V for which ϕ has upper-triangular block shape. In particular, if $U \leq V$ is a submodule, then with respect to an appropriate basis, ϕ has upper left block $\phi|_U$, bottom left block zero and bottom right block $\phi|_{V/U}$.

Suppose now that we have a composition series for (V, ϕ), say

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = \{0\}.$$

The successive quotients are simple, so $V_{n-i}/V_{n-i+1} \cong (K, \lambda_i)$ for some $\lambda_i \in K$.

Consider the submodule $V_1 \leq V$. Then with respect to an appropriate basis we have ϕ in upper-triangular block form with the block $\phi|_{V/V_1}$ in the bottom right corner. Now $V/V_1 \cong (K, \lambda_n)$, so $\phi|_{V/V_1} = \lambda_n$. This shows that the bottom row of the matrix of ϕ is a string of zeros followed by λ_n.

We can now repeat this construction for V_1. By induction we deduce that, with respect to an appropriate basis, the matrix of ϕ is upper triangular with diagonal entries $\lambda_1, \ldots, \lambda_n$

$$\begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}.$$

Note that the basis we are using is $\{e_1, \ldots, e_n\}$, found inductively so that $\{e_1, \ldots, e_{n-i}\}$ is a basis for V_i.

In conclusion, the Jordan-Hölder Theorem implies that every matrix is conjugate to an upper-triangular matrix, and the diagonal entries (with multiplicities) depend only on the linear map. Moreover, since the determinant depends only on the linear map, and not on the choice of matrix representation, we can compute the characteristic polynomial using this upper-triangular form, giving $\chi_\phi(t) = (t - \lambda_1) \cdots (t - \lambda_n)$. We therefore see that the diagonal entries are precisely the roots of the characteristic polynomial, each one repeated according to its algebraic multiplicity.

It is a small step from here to get one proof of the Cayley-Hamilton Theorem, that every matrix satisfies its own characteristic polynomial. For, the matrix of $\phi - \lambda_i$ is again upper-triangular, with diagonal entries $\lambda_1 - \lambda_i, \ldots, \lambda_n - \lambda_i$. In particular, this has a zero in position (i, i). By induction the product $(\phi - \lambda_i) \cdots (\phi - \lambda_n)$ is zero in rows $i, \ldots, n$, so $(\phi - \lambda_1) \cdots (\phi - \lambda_n) = 0$.

19.9 Grothendieck Group (non-examinable)

The **Grothendieck group** of finite-dimensional modules is the free abelian group generated by the isomorphism classes of finite-dimensional simple modules $[S_i]$. For each finite-dimensional module M we write $\theta(M) := \sum_i m_i[S_i]$, where m_i is the number of times S_i occurs as a composition factor of M. The Jordan-Hölder Theorem tells us that this is well-defined, since it does not depend on the choice of composition series. Moreover, Corollary 19.5 shows that if $N \leq M$ is a submodule, then $\theta(M) = \theta(N) + \theta(M/N)$.

20 Division algebras and Frobenius's Theorem

Having seen how important division algebras are in studying semisimple algebras, we now study them in more detail.

Recall that a division algebra is a non-zero algebra in which every non-zero element is invertible. Thus a commutative division algebra is just a field. The quaternions $\mathbb{H}$ are an example of a non-commutative division algebra over $\mathbb{R}$.

20.1 Lemma

Let A be a finite-dimensional algebra. Then for each $a \in A$ there exists a monic polynomial (so having leading coefficient 1)

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in K[x]$$

with

$$f(a) = a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0 \in A.$$

Proof. Suppose $\dim A = r$. Then the $r+1$ elements $1, a, a^2, \ldots, a^r$ cannot be linearly independent. If $c_n a^n + \cdots + c_0 = 0$ with $c_i \in K$ and $c_n \neq 0$, then take $f = c_n^{-1} \sum_i c_i X^i$.

Alternatively, set $B := \mathrm{span}\{1, a, a^2, \ldots\}$, the subalgebra of A generated by a. Then B becomes a finite-dimensional $K[x]$-module by letting x act as multiplication by a, and so we can take $f(x)$ to be the minimal polynomial, or the characteristic polynomial. □

20.2 Definition

A field K is said to be **algebraically closed** if every non-constant polynomial $f \in K[X]$ has a root in K. It follows that f can be written as a product of linear factors over K

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n).$$

By the Fundamental Theorem of Algebra, $\mathbb{C}$ is algebraically closed.

For a polynomial $f \in \mathbb{R}[X]$, the roots of f in $\mathbb{C}$ are either real, or come in complex-conjugate pairs. For, if $\alpha \in \mathbb{C}$ is a root of f, then $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$, so $\bar{\alpha}$ is also a root of f. Thus we can factor f in $\mathbb{R}[X]$ as a product of linear and quadratic factors, since

$$(X - \alpha)(X - \overline{\alpha}) = (X - \lambda)^2 + \mu^2, \quad \alpha = \lambda + \mu i, \quad \mu \neq 0.$$

20.3 Theorem

If K is algebraically closed, then the only finite-dimensional division algebra over K is K itself.

Proof. Let A be a finite-dimensional division algebra over K, and let $a \in A$. By the lemma we have $f(a) = 0$ for some monic polynomial $f \in K[x]$. Since K is algebraically closed we can factorise f as

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_n), \quad \alpha_i \in K,$$

whence $(a-\alpha_1)\cdots(a-\alpha_n)=0\in A$. Since A is a division algebra, we must have $a-\alpha_i=0$ for some i. Hence $a=\alpha_i\in K$. □

20.4 Lemma

If A is a finite-dimensional division algebra over $\mathbb{R}$ and $a\in A\setminus\mathbb{R}$, then there exists $i\in\operatorname{span}\{1,a\}$ with $i^2=-1$. In particular, $a=\lambda+\mu i$ for some $\lambda,\mu\in\mathbb{R}$ with $\mu\neq 0$.

Proof. Since A is finite-dimensional there exists a monic polynomial $f\in\mathbb{R}[x]$ with $f(a)=0$. We can factorise $f(x)=f_1(x)\cdots f_n(x)$ with each $f_r\in\mathbb{R}[x]$ monic and either linear or quadratic (with non-real roots). Now, $0=f(a)=f_1(a)\cdots f_n(a)$, so A a division algebra implies $f_r(a)=0$ for some r.

If $f_r(x)=x-\alpha$ is linear, then $a=\alpha\in\mathbb{R}$, a contradiction. Thus $f_r(x)$ is quadratic, say $f_r(x)=(x-\lambda)^2+\mu^2$ with $\mu\neq 0$. Define $i:=(a-\lambda)/\mu\in A$. Then $a=\lambda+\mu i$ and $i^2=(a-\lambda)^2/\mu^2=\big(f_r(a)-\mu^2\big)/\mu^2=-1$. □

Note that the subalgebra $\operatorname{span}\{1,a\}=\operatorname{span}\{1,i\}$ is isomorphic to $\mathbb{C}$.

20.5 Lemma

Let A be a finite-dimensional division algebra over $\mathbb{R}$, and let $i\in A$ satisfy $i^2=-1$. Then $a\in A$ commutes with i if and only if $a\in\operatorname{span}\{1,i\}$.

Proof. Clearly every element in $\operatorname{span}\{1,i\}$ commutes with i. Now suppose that $a\in A\setminus\mathbb{R}$ commutes with i. By the previous lemma we can write $a=\lambda+\mu j$ for some $\lambda,\mu\in\mathbb{R}$ with $\mu\neq 0$, and some $j\in A$ with $j^2=-1$. Then

$$0=ai-ia=\mu(ji-ij),$$

so $ij=ji$. Since

$$(i-j)(i+j)=i^2-j^2+ij-ji=0,$$

we deduce that $j=\pm i$, and hence $a\in\operatorname{span}\{1,i\}$. □

20.6 Frobenius's Theorem

The only finite-dimensional division algebras over $\mathbb{R}$ are, up to isomorphism, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.

Proof. Let A be a finite-dimensional division algebra over $\mathbb{R}$. If $A=\mathbb{R}$, then we are done. Otherwise, by Lemma 20.4 there exists $i\in A$ with $i^2=-1$. Now $\operatorname{span}\{1,i\}$ is a subalgebra of A, isomorphic to $\mathbb{C}$. So if $A=\operatorname{span}\{1,i\}$, then $A\cong\mathbb{C}$.

Otherwise we have an element in $\bar{a}\in A\setminus\operatorname{span}\{1,i\}$ and we can apply Lemma 20.4 again to get $a\in\operatorname{span}\{1,\bar{a}\}$ with $a^2=-1$. Observe that $ia+ai$ commutes with both i and a: for example,

$$i(ia+ai)=-a+iai=(ia+ai)i.$$

Therefore by Lemma 20.5 we have $ia+ai \in \operatorname{span}\{1,i\}$ and $ia+ai \in \operatorname{span}\{1,a\}$. Since $1,i,a$ are linearly independent, we deduce that $x := \frac{1}{2}(ia+ai) \in \mathbb{R}$.

We claim that $x^2 < 1$. For, $(i+a)^2 = i^2 + a^2 + ia + ai = 2(x-1) \in \mathbb{R}$. If $2(x-1) \geq 0$, then there exists $y \in \mathbb{R}$ such that $y^2 = 2(x-1)$. Thus

$$(i+a+y)(i+a-y) = (i+a)^2 - y^2 = 0,$$

so that $i + a = \pm y \in \mathbb{R}$, a contradiction. Thus $x < 1$. Similarly $(i-a)^2 = -2(x+1) \in \mathbb{R}$, so $x > -1$. Hence $x^2 < 1$ as claimed.

Set

$$j := \frac{1}{\sqrt{1-x^2}}(xi + a).$$

Then

$$j^2 = \frac{1}{1-x^2}\big(x^2 i^2 + a^2 + x(ia+ai)\big) = \frac{-x^2 - 1 + 2x^2}{1-x^2} = \frac{x^2-1}{1-x^2} = -1$$

and

$$ij + ji = \frac{1}{\sqrt{1-x^2}}(2xi^2 + ia + ai) = \frac{1}{\sqrt{1-x^2}}(-2x + 2x) = 0.$$

We have therefore found linearly independent elements $1, i, j \in A$ such that $i^2 = j^2 = -1$ and $ij = -ji$. Set $k := ij$. Then $\operatorname{span}\{1,i,j,k\}$ is a subalgebra of A, isomorphic to $\mathbb{H}$. So, if $A = \operatorname{span}\{1,i,j,k\}$, then $A \cong \mathbb{H}$.

Otherwise we can apply Lemma 20.4 once more to get $b \in A \setminus \operatorname{span}\{1,i,j,k\}$ with $b^2 = -1$. As above, we must have

$$ib + bi = 2s, \quad jb + bj = 2t, \quad kb + bk = 2u, \quad \text{for some } s,t,u \in \mathbb{R}.$$

Then

$$2sj = (ib+bi)j = bk + i(2t - jb) = 2ti + bk - kb = 2ti + 2bk - 2u,$$

so that

$$bk = u - ti + sj.$$

Therefore

$$b = -(bk)k = -(u - ti + sj)k = -(si + tj + uk) \in \operatorname{span}\{1,i,j,k\},$$

a contradiction.

Thus the only finite-dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. □

20.7 Corollary

Let K be an algebraically-closed field, A a K-algebra, and S a finite-dimensional simple A-module. Then $\operatorname{End}_A(S) = K$.

For, by Schur's Lemma, it is a finite-dimensional division algebra over K, and we can apply Theorem 20.3.

It follows that any finite-dimensional semisimple K-algebra is isomorphic to a direct product $\mathbb{M}_{n_1}(K) \times \cdots \times \mathbb{M}_{n_r}(K)$. For example, up to isomorphism, the nine-dimensional semisimple K-algebras are

$$K^9, \quad K^5 \times \mathbb{M}_2(K), \quad K \times \mathbb{M}_2(K) \times \mathbb{M}_2(K), \quad \mathbb{M}_3(K).$$

Similarly, we can use Frobenius's Theorem to describe all semisimple $\mathbb{R}$-algebras. For example, the four-dimensional, semisimple $\mathbb{R}$-algebras are

$$\mathbb{R}^4, \quad \mathbb{R}^2 \times \mathbb{C}, \quad \mathbb{C}^2, \quad \mathbb{H}, \quad \mathbb{M}_2(\mathbb{R}).$$

20.8 Wedderburn's Little Theorem (non-examinable)

Let D be a finite division algebra (so D is finite as a set). Then D is a field.

Proof. Set $K := Z(D)$. Then K is commutative and a division algebra, hence a field. So K is a finite field, say $|K| = q$. We can view D as a vector space over K, so $|D| = q^n$ where $\dim_K D = n$.

We now consider the set $D^\times$ of non-zero elements of D. Since D is a divison algebra, every non-zero element has an inverse, so $D^\times$ is a group under multiplication. The group $D^\times$ acts on itself by conjugation: for $x \in D^\times$, we have the group action $\hat{x}\colon D^\times \to D^\times$, $y \mapsto xyx^{-1}$. As usual, we can partition $D^\times$ into orbits, and use the **Orbit-Stabiliser Theorem** to count the size of each orbit. This yields the **class formula**

$$q^n - 1 = |D^\times| = \sum_\Gamma \frac{|D^\times|}{|\mathrm{Stab}(\Gamma)|},$$

where the sum is over the distinct orbits. Recall also that $|\mathrm{Stab}(\Gamma)| = |\mathrm{Stab}(y)|$ for any $y \in \Gamma$.

Suppose $y \in D^\times$. The subalgebra $K(y)$ generated by y is a commutative division algebra, so a field, and the stabiliser is the set of $x \in D^\times$ such that $xyx^{-1} = y$. Thus $\mathrm{Stab}(y) = C(K(y))^\times$, where $C(K(y))$ is the commutator of $K(y)$.

Now, $C(K(y)) = D$ if and only if $y \in Z(D) = K$. Thus there are precisely $q-1$ elements $y \in K^\times$ such that $|C(K(y))^\times| = |D^\times|$.

For any other y we have $K < K(y) \leq C(K(y)) < D$, a chain of inclusions with the first and last inclusions being strict. For each y we can view $C(K(y))$ as a vector space over K, so we set $n(y) := \dim_K C(K(y))$. The class formula now reads

$$q^n - 1 = q - 1 + \sum_y \frac{q^n - 1}{q^{n(y)} - 1},$$

where the sum is over representatives y for the obits $\Gamma \not\subset K$.

Finally, we observe that $C(K(y))$ is a division subalgebra of D, and we can view D as a left module for $C(K(y))$ via left multiplication. Since a division algebra is semisimple, we must have $D \cong C(K(y))^{r(y)}$ for some r, and hence $n = n(y)r(y)$. In particular, $n(y)$ divides n for all y.

The trick is now to use the **cyclotomic polynomials** $\phi_n(t) \in \mathbb{Q}[t]$. These are defined inductively using

$$t^n - 1 = \prod_{d|n} \phi_d(t).$$

It follows from **Gauss's Lemma** that $\phi_n(t) \in \mathbb{Z}[t]$ for all n. Also, over $\mathbb{C}$ we have the factorisation

$$\phi_n(t) = \prod_{\zeta} (t - \zeta),$$

where the product is taken over all **primitive n-th roots of unity**; that is, $\zeta^n = 1$ and $\zeta^r \neq 1$ for all $1 \leq r < n$. Alternatively, $\zeta = \exp(2m\pi i/n)$ for $1 \leq m < n$ with $\gcd(m, n) = 1$.

Substituting in $t \mapsto q$ now gives $0 < \phi_n(q) \in \mathbb{Z}$ and $q^n - 1 = \prod_{d|n} \phi_n(q)$ as a product of positive integers. In particular, $\phi_n(q)$ divides $(q^n - 1)/(q^d - 1)$ for all $d < n$. then, since

$$q - 1 = q^n - 1 - \sum_y \frac{q^n - 1}{q^{n(y)} - 1},$$

we deduce that $\phi_n(q)$ divides $q - 1$.

On the other hand, if ζ is a primitive n-th root of unity and $n > 1$, then $\zeta \neq 1$ but $|\zeta| = 1$, so $|q - \zeta| > |q - 1|$. Thus $|\phi_n(q)| > |q - 1|$, contradicting the fact that $\phi_n(q)$ divides $q - 1$. Hence $n = 1$ and $D = K$ is commutative, hence a field. □

Part V

Some More Examples

21 $K[x]/(x^2)$-modules

Consider the **algebra of dual numbers** $K[\epsilon] \cong K[x]/(x^2)$. This has a basis $\{1, \epsilon\}$ and multiplication $\epsilon^2 = 0$. [Alternatively it has one generator ϵ and one relation $\epsilon^2 = 0$.]

A module for $K[\epsilon]$ is give by a vector space together with an action of ϵ. Thus we can consider a module as a pair (V, ϕ) such that V is a vector space and $\phi \in \mathrm{End}_K(V)$ satisfies $\phi^2 = 0$. The action is then given by

$$(a + b\epsilon) \cdot v := av + b\phi(v).$$

This fits together nicely with our earlier description of $K[x]$-modules, using the restriction of scalars $K[x] \to K[\epsilon]$.

A submodule is an invariant subspace, so a subspace $U \leq V$ satisfying $\phi(U) \leq U$. In this case, we have the submodule $(U, \phi|_U) \leq (V, \phi)$. In particular, we have the submodule $(\mathrm{Ker}(\phi), 0) \leq (V, \phi)$.

We now observe that $\mathrm{Ker}(\phi) = 0$ if and only if $V = 0$. (Why?) More generally, if $U \leq \mathrm{Ker}(\phi)$ is any subspace, then $(U, 0) \leq (V, \phi)$. So, if (V, ϕ) is simple, then $(V, \phi) = (U, 0)$ for any one-dimensional subspace $U \leq \mathrm{Ker}(\phi)$. Hence $\dim V = 1$ and $\phi = 0$, so $(V, \phi) \cong (K, 0)$. Thus there is a unique simple module (up to isomorphism).

More generally, a module is semisimple if and only if it is a direct sum of simple modules. So a $K[\epsilon]$-module (V, ϕ) is semisimple if and only if it is isomorphic to $(K, 0)^n = (K^n, 0)$. This happens if and only if $\phi = 0$.

In summary, $K[\epsilon]$-modules correspond to pairs (V, ϕ) with $\phi^2 = 0$. A module is simple if and only if $\dim V = 1$ (so necessarily $\phi = 0$ and $(V, \phi) \cong (K, 0)$), and a module is semisimple if and only if $\phi = 0$.

Now consider the regular module. This has basis $\{1, \epsilon\}$ and the action is

$$\epsilon \cdot 1 = \epsilon, \quad \epsilon \cdot \epsilon = \epsilon^2 = 0.$$

Thus ϵ acts via the matrix $\phi = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (satisfying $\phi^2 = 0$), so the regular module is (K^2, ϕ).

We observe that the regular module is not semisimple, since the matrix ϕ is non-zero. The Jordan-Hölder Theorem tells us that the regular module has a composition series. To find a simple submodule, we can again consider $(\mathrm{Ker}(\phi), 0)$, which is the submodule $(K\epsilon, 0)$. The quotient is then also simple (since it is one-dimensional). Explicitly the quotient has basis $1 + K\epsilon$ and action

$$\epsilon \cdot (1 + K\epsilon) = \epsilon + K\epsilon = 0 + K\epsilon.$$

We therefore have the composition series

$$(K^2, \phi) \supset (K\epsilon, 0) \supset 0$$

and the regular module has length two.

In fact, this is the only composition series of $K[\epsilon]$ — but this phenomenon is very rare. Also, the two modules (K^2, ϕ) and $(K, 0)$ are the only indecomposable modules for $K[\epsilon]$ — in the sense that every finite-dimensional module is isomorphic to a direct sum of copies of these two modules. Again, in general algebras will have many non-isomorphic simple modules, and even more ways of 'gluing' them together.

22 Symmetric Groups (non-examinable)

Let S_n be the symmetric group on n letters. Using the generators $s_i := (i\, i+1)$ for $1 \leq i < n$ this has the presentation

$$S_n = \langle s_i : s_i^2 = 1,\ s_i s_j s_i = s_j s_i s_j \text{ for } |i-j| = 1,\ s_i s_j = s_j s_i \text{ for } |i-j| > 1 \rangle.$$

We want to construct some interesting representations of S_n, the so-called Specht modules. To do this, we first observe that S_n acts on the polynomial algebra $K[x_1, \ldots, x_n]$ via

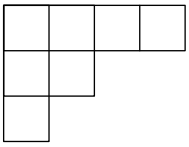
$$w \cdot x_i x_j \cdots x_k := x_{w(i)} x_{w(j)} \cdots x_{w(k)}.$$

The Specht modules will be certain submodules of the polynomial algebra $K[x_1, \ldots, x_n]$ indexed by partitions of n.

A **partition** of n is a decreasing sequence of positive integers

$$\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r)$$

such that $|\lambda| := \lambda_1 + \lambda_2 + \cdots + \lambda_r$ equals n. We write this as $\lambda \vdash n$. It is usual to visualise a partition as a diagram with λ_i boxes in row i, for example



$(4, 2, 1)$

Such a diagram is called a **Young diagram**.

Given $\lambda \vdash n$, a **λ-tableau** is a way of filling the boxes with the numbers $\{1, \ldots, n\}$, each number occurring exactly once. For example, the following are tableaux of shape $(4, 2, 1)$

1	3	4	5
2	7		
6			

T_1

and

3	6	2	5
2	1		
7			

T_2

A tableau is called **standard** if the numbers increase along rows and down columns. In the above example, the first tableau is standard, the second not.

We let S_n act on λ-tableaux by letting it act on each of the entries. This defines a group action on the set of λ-tableaux (or on the vector space with basis the λ-tableaux).

Given a tableau T, we define an element $\alpha(T) \in \mathbb{N}_0^n$ by setting $\alpha(T)_i$ to be $r-1$ provided the number i occurs in T in row r. We then define the monomial $m_T \in K[x_1, \ldots, x_n]$ via

$$m_T := x^{\alpha(T)} = \prod_i x_i^{\alpha(T)_i}.$$

Thus, for the two tableaux above, we have the monomials $m_{T_1} = x_2 x_6^2 x_7$ and $m_{T_2} = x_1 x_2 x_7^2$.

Note that $m_{w \cdot T} = w \cdot m_T$. It follows that the subspace

$$M^\lambda := \operatorname{span}\{m_T : T \text{ a } \lambda\text{-tableau}\}$$

is a submodule of $K[x_1, \ldots, x_n]$, called the **Young module**, or **permutation module**. Unfortunately it is a bit too big to be useful, and so we now define a submodule of M^λ.

Given a tableau T, let $f_T \in K[x_1, \ldots, x_n]$ be the polynomial having a factor $x_i - x_j$ whenever i and j appear in the same column of T, and i lies below j. Thus for the two tableaux above we have the polynomials

$$f_{T_1} = (x_2 - x_1)(x_6 - x_1)(x_6 - x_2)(x_7 - x_3)$$

and

$$f_{T_2} = (x_2 - x_3)(x_7 - x_3)(x_7 - x_2)(x_1 - x_6).$$

Note that, expanding all the brackets in f_T, the monomial m_T occurs with coefficient 1. Moreover, each polynomial f_T actually lies in M^λ, and $w \cdot f_T = f_{w \cdot T}$.

We define the **Specht module** S^λ to be the submodule of M^λ given by

$$S^\lambda := \operatorname{span}\{f_T : T \text{ a } \lambda\text{-tableau}\}.$$

The Specht modules are very important in the representation theory of S_n.

If the characteristic of the field K does not divide $|S_n| = n!$, for example if $K = \mathbb{C}$, then the regular module decomposes as

$$KS_n \cong \bigoplus_{\lambda \vdash n} (S^\lambda)^{f^\lambda},$$

where $f^\lambda = \dim S^\lambda$; in other words, each S^λ occurs with multiplicity f^λ, and every simple module is isomorphic to a Specht modules. Moreover, $\operatorname{End}(S^\lambda) = K$, so Wedderburn's Theorem gives an algebra isomorphism

$$KS_n \cong \prod_{\lambda \vdash n} \mathbb{M}_{f^\lambda}(K).$$

In general, KS_n is not semisimple, and the Specht modules S^λ are not simple. However, over a field of characteristic $p > 0$, we can always take a subset of the partitions of n (called p-regular partitions) such that the corresponding Specht modules are indecomposable and have a unique quotient module D^λ which is simple. Moreover, each simple module is isomorphic to one of these D^λ.

Clearly

$$\dim M^\lambda = \frac{n!}{\prod_i \lambda_i!} =: \binom{n}{\lambda}.$$

For, we need to choose λ_2 of the x_i to occur with exponent 1, then λ_3 of the remaining x_i to occur with exponent 2, and so on.

There is also a formula for the dimensions of the Specht modules $f^\lambda = \dim S^\lambda$, called the hook length formula. It is still an open problem to give a general formula for the dimensions of the simple modules D^λ when the characteristic of the field divides $n!$.

For the Specht module S^λ, the polynomials f_T for T a standard tableau form a basis. We will just show here that they are linearly independent.

Let us order the monomials in M^λ lexicographically; that is, we say $x_1^{d_1} \cdots x_n^{d_n} \leq x_1^{e_1} \cdots x_n^{e_n}$ provided that there exists an r with $d_i = e_i$ for $i < r$ and $d_r < e_r$. (This is the analogous to the ordering used in dictionaries, hence the name.) Then it is not hard to see that if T is standard, then $f_T = m_T + \text{smaller terms}$. Since the monomials m_T are distinct for distinct standard tableaux, we conclude that the f_T for T standard are linearly independent.

We stated above that the f_T for T standard form a basis for the Specht module. In fact, more is true. Every other f_T can be written as a linear combination of the these basis elements with *integer* coefficients. It is this property that allows us to define the Specht modules over any field, or even over any ring.

Let us consider some examples. For the partition $\lambda = (n)$ we have that $m_T = 1$ for all tableaux T, and hence $S^\lambda = M^\lambda = K$. Moreover, each element $w \in S_n$ acts as the identity, so that M^λ is just the trivial module.

At the other extreme, let $\lambda = (1, 1, \ldots, 1)$, so that $\dim M^\lambda = n!$. In fact, M^λ is isomorphic to the regular module, via the linear map $\mathbb{C}S_n \to M^\lambda$ sending $w \in S_n$ to the monomial $x_{w(2)} x_{w(3)}^2 \cdots x_{w(n)}^{n-1}$. This induces a bijection between tableaux and permutations, where w is sent to the tableau having entry $w(i)$ in row i, and then $f_w = \prod_{i<j}(x_{w(i)} - x_{w(j)})$. We see that there is a unique standard tableau, corresponding to the identity element, and $f_1 = \Delta = \prod_{i<j}(x_i - x_j)$. It is not hard to check (using one of the characterisations of the sign of a permutation) that $f_w = w\Delta = \operatorname{sgn}(w)\Delta$. Thus the Specht module S^λ is one dimensional, and each permutation w acts as multiplication by $\operatorname{sgn}(w)$. Thus S^λ is called the **sign module**.

Another easy example is when $\lambda = (n-1, 1)$. Then M^λ has dimension n, and for a tableau T we have $m_T = x_j$ where j is the entry in the second row of T. We note that M^λ is the **natural module**, or **permutation module**, of S_n, since we just have $w \cdot x_j = x_{w(j)}$, so the action corresponds directly to the action of S_n on the set $\{1, \ldots, n\}$. In fact, if $P(w) \in GL_n(K)$ is the matrix representing the action of w with respect to the basis x_j, then $P(w) = \sum_j E_{w(j)j}$, so has one 1 in each row and each column, and zeros elsewhere. In particular, the columns

of $P(w)$ form an orthonormal basis with respect to the usual scalar product on K^n, so $P(w)^{-1} = P(w)^t$ and $P(w) \in O_n(K)$ is an orthogonal matrix. It follows that $\det(P(w)) = \pm 1$, and in fact it is not hard to see that $\det(P(w)) = \mathrm{sgn}(w)$.

Now, if i is the entry in T in the top left corner, then $f_T = x_i - x_j$. We therefore see that S^λ has basis given by the polynomials $x_1 - x_j$, and that these correspond bijectively to the standard tableaux. Thus S^λ has dimension $n-1$. A vector space complement to S^λ is given by taking the span of $x_1 + x_2 + \cdots + x_n$. We see that this is again a submodule of M^λ, and that each $w \in S_n$ acts as the identity. Thus this submodule is isomorphic to the trivial module, and so

$$M^{(n-1,1)} \cong S^{(n-1,1)} \oplus S^{(n)}.$$

Furthermore, if $P'(w) \in \mathrm{GL}_{n-1}(K)$ is the matrix representing the action of w on $S^{(n-1,1)}$, then we can represent the action of w on $M^{(n-1,1)}$ by the block diagonal matrix $P'(w) \oplus (1)$. It follows that $\det(P'(w)) = \det(P(w)) = \mathrm{sgn}(w)$ as well.

Part VI

Appendix

A Review of Some Linear Algebra

Much of this you should already know, and feel confident about. In this module, all algebras and all representations will be vector spaces (with additional structure), and we will often use ideas from linear algebra, for example by choosing a basis, or representing a linear map as a matrix (once we have chosen a basis). I would therefore recommend that you read through this appendix, and revise any topics you are less sure about.

At the end I have also included a discussion about Zorn's Lemma, and bases and dimension for arbitrary vector spaces. You do not need to worry about this material; you only really need to be familiar with the finite-dimensional situation. I have included it for the sake of completeness, and because it is something you should at least know about.

For a slick textbook treatment see P. M. Cohn, *Classic Algebra*.

A.1 Vector spaces

We fix a field K, and all vector spaces and linear maps will be over K.

A **vector space** V over K is a set together two operations

$$\begin{array}{rll} \textbf{vector addition} & V \times V \to V, & (u, v) \mapsto u + v \\ \textbf{scalar multiplication} & K \times V \to V, & (\lambda, v) \mapsto \lambda v \end{array}$$

satisfying the following axioms:

1. V is an **abelian group under vector addition**; that is
   (a) addition is **associative**,
   $$(x + y) + z = x + (y + z) \quad \text{for all } x, y, z \in V.$$
   (b) there exists $0 \in V$, the **zero vector**, such that
   $$0 + x = x = x + 0 \quad \text{for all } x \in V.$$
   (c) every vector x has an additive **inverse** $-x$, so
   $$x + (-x) = 0 = (-x) + x \quad \text{for all } x \in V.$$
   (d) addition is **commutative**, so
   $$x + y = y + x \quad \text{for all } x, y \in V.$$

2. **compatibility** of scalar multiplication with the field operations

$$(\lambda+\mu)x = \lambda x + \mu x, \quad (\lambda\mu)x = \lambda(\mu x), \quad 1x = x \quad \text{for all } \lambda, \mu \in K,\ x \in V.$$

3. **distributivity** of scalar multiplication over vector addition

$$\lambda(x+y) = \lambda x + \lambda y \quad \text{for all } \lambda \in K,\ x, y \in V.$$

It follows that $-x = (-1)x$ and $0x = 0$.

A.1.1 Matrices

The set of matrices

$$\mathbb{M}_{n\times m}(K) = \{(a_{ij}) : a_{ij} \in K,\ 1 \le i \le n,\ 1 \le j \le m\}$$

is a vector space via component-wise vector addition and scalar multiplication

$$(a_{ij}) + \lambda(b_{ij}) = (a_{ij} + \lambda b_{ij}).$$

As special cases we have the vector spaces of column vectors $\mathbb{M}_{n\times 1}(K)$ and row vectors $\mathbb{M}_{1\times n}(K)$. We often just write K^n for either of these, so

$$K^n = \{(a_1, \ldots, a_n) : a_i \in K\}.$$

More generally, let I be a set. Then we can consider the set of I-tuples of scalars

$$K^I := \{(a_i : a \in I) : a_i \in K\}.$$

This is again a vector space via component-wise vector addition and scalar multiplication

$$(a_i) + \lambda(b_i) := (a_i + \lambda b_i).$$

We also have the subset

$$K^{(I)} := \{(a_i) : a_i \in K \text{ almost all zero}\}$$

meaning that only finitely many of the components a_i are non-zero. This is also a vector space with the same rules for vector addition and scalar multiplication.

Note that, if $I = \{1, \ldots, n\}$ is finite, then $K^I = K^{(I)} = K^n$. Otherwise, if I is infinite, then $K^{(I)}$ is a proper subset of K^I.

A.1.2 Linear Combinations

Let V be a vector space. A **linear combination** of vectors $x_1, \ldots, x_n \in V$ is a sum of the form

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \in V \quad \text{for scalars } \lambda_i \in K.$$

Given a (possibly infinite) set of vectors $\{x_i : i \in I\} \subset V$, a linear combination of the x_i is a linear combination of a *finite* subset of the x_i. We can write this as $\sum_{i\in I} \lambda_i x_i$, where almost all the scalars $\lambda_i \in K$ are zero; that is, only finitely many are non-zero.

A.1.3 Example

Given any set X, we have the vector space K^X of all functions $f\colon X \to K$, where vector addition and scalar multiplication are given by

$$(f + \lambda g)(x) := f(x) + \lambda g(x) \quad \text{for } f, g \in K^X,\ \lambda \in K,\ x \in X.$$

We define the **support** of $f \in K^X$ to be

$$\operatorname{supp}(f) := \{x \in X : f(x) \neq 0\},$$

and hence have the subset

$$K^{(X)} = \{f \in K^X : \operatorname{supp}(f) \text{ is finite}\}.$$

This is again a vector space, with the same rules for vector addition and scalar multiplication.

Note that if we index the elements of $X = \{x_i : i \in I\}$, then we can identify these sets with I-tuples of scalars

$$K^X \to K^I \quad \text{and} \quad K^{(X)} \to K^{(I)}$$

via

$$f \mapsto (a_i) \text{ such that } f(x_i) = a_i.$$

A.1.4 Subspaces

Let V be a vector space. A subset $U \subset V$ is called a **subspace**, written $U \leq V$, provided that it contains 0 and is closed under vector addition and scalar multiplication

1. $0 \in U$.
2. $x + \lambda y \in U$ for all $x, y \in U$ and $\lambda \in K$.

It follows that U is itself a vector space.

As an example, $K^{(I)}$ is always a subspace of K^I.

A.1.5 Sums and Intersections

Let $U, U' \leq V$ be subspaces. Then the **sum**

$$U + U' := \{u + u' \in V : u \in U,\ u' \in U'\}$$

and the **intersection**

$$U \cap U' := \{v \in V : v \in U \text{ and } v \in U'\}$$

are again subspaces of V.

More generally, if we have subspaces U_i for $i \in I$, then we can form the sum

$$\sum_{i\in I} U_i := \{v \in V : v = u_1 + \cdots u_n \text{ for some } u_r \in U_{i_r}\}$$

and intersection

$$\bigcap_{i\in I} U_i := \{v \in V : v \in U_i \text{ for all } i\},$$

and these are again subspaces of V.

Note that the vectors in $\sum_i U_i$ are precisely the possible linear combinations of vectors in $\bigcup_i U_i$. This is because we only allow *finite* linear combinations.

A.1.6 Definition

One useful consequence of being able to form arbitrary intersections is that we can now define the *smallest* subspace of V containing a given subset S — we just take the intersection over all subspaces containing S. This is called the **subspace generated by** S, or the **subspace spanned by** S, and denoted $\text{span}(S)$. It follows that the vectors in $\text{span}(S)$ are all possible linear combinations of elements of S.

For example, given subspaces $U_i \leq V$ for $i \in I$, then the sum $\sum_{i\in I} U_i$ is the span of the subset $\bigcup_{i\in I} U_i$.

A.1.7 Direct Sums

We say that the sum $U + U'$ is **direct**, written $U \oplus U'$, if every $v \in U + U'$ can be written uniquely as $v = u + u'$ with $u \in U$ and $u' \in U'$. This is equivalent to saying that $U \cap U' = \{0\}$.

If $U \oplus U' = V$, then we call U' a **complement** to U (in V).

More generally we say that the sum $\sum_{i\in I} U_i$ is direct provided that every element $v \in \sum_{i\in I} U_i$ can be written uniquely as $v = \sum_i u_i$ with $u_i \in U_i$ and almost all u_i zero. This is equivalent to saying that

$$U_i \cap \big(\sum_{j\neq i} U_j\big) = \{0\} \quad \text{for all } i \in I.$$

A.1.8 Direct Products

Let U and V be vector spaces. We endow the Cartesian product $U \times V$ with the structure of a vector space by taking component-wise vector addition and scalar multiplication

$$(u, v) + \lambda(u', v') := (u + \lambda u', v + \lambda v').$$

We call this the **direct product**, or **external direct sum**.

Observe that K^n is the direct product of n copies of K.

A.1.9 Quotient Spaces

Let $U \leq V$ be a subspace. We can define an equivalence relation on V by setting

$$x \sim y \quad \text{if} \quad x - y \in U.$$

This means that the relation is

reflexive	$x \sim x$
symmetric	$x \sim y$ implies $y \sim x$
transitive	$x \sim y$ and $y \sim z$ imply $x \sim z$

We denote the equivalence class of x by $x + U$, and write V/U for the set of all equivalence classes. Thus $x + U = y + U$ if and only if $x - y \in U$.

The set V/U becomes a vector space by defining vector addition and scalar multiplication to be

$$(x + U) + \lambda(y + U) := (x + \lambda y) + U.$$

These operations are well-defined; that is, if $x + U = x' + U$ and $y + U = y' + U$, and $\lambda \in K$, then

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

In other words, if $x - x', y - y' \in U$ and $\lambda \in K$, then $(x + \lambda y) - (x' + \lambda y') \in U$.

It is now easy to check that the vector space axioms are fulfilled.

We call V/U the **quotient space** of V by U.

A.2 Linear Maps

Let U and V be vector spaces. A map $f\colon U \to V$ is called **linear**, or a **homomorphism**, provided that it respects the vector space structures of U and V. In other words, we have

$$f(x + \lambda y) = f(x) + \lambda f(y) \quad \text{for all } x, y \in U \text{ and } \lambda \in K.$$

In the special case when $U = V$ we also call f an **endomorphism** of V. Note that the identity map $\mathrm{id}_V\colon x \mapsto x$ is an endomorphism of V.

If $f\colon U \to V$ and $g\colon V \to W$ are both linear, then so too is their composition

$$gf\colon U \to W, \quad u \mapsto g(f(u)).$$

A.2.1 Lemma

If $f\colon U \to V$ is a linear map, then we have subspaces

$$\mathrm{Im}(f) = \{f(u) : u \in I\} \leq V \quad \text{and} \quad \mathrm{Ker}(f) = \{u \in U : f(u) = 0\} \leq U.$$

If $U \leq V$ is a subspace, then both the inclusion map

$$\iota\colon U \hookrightarrow V, \quad u \mapsto u,$$

and the natural map

$$\pi\colon V \twoheadrightarrow V/U, \quad v \mapsto v + U,$$

are linear. Moreover $\mathrm{Im}(\iota) = U = \mathrm{Ker}(\pi)$.

It follows that subspaces can be characterised as either images of linear maps, or as kernels of linear maps.

A.2.2 Definition

A linear map $f\colon U \to V$ is called a **monomorphism** provided that $\mathrm{Ker}(f) = 0$, and an **epimorphism** provided that $\mathrm{Im}(f) = V$.

We call f an **isomorphism** provided there exists a linear map $g\colon V \to U$ with both $gf = \mathrm{id}_U$ and $fg = \mathrm{id}_V$. In the special case when $U = V$ we also call f an **automorphism**.

Clearly f is onto if and only if it is a epimorphism. More interestingly, it is injective if and only if it is a monomorphism, and it is an isomorphism if and only if it is a bijection.

A.2.3 Lemma

Let V be a vector space and $S = \{x_i : i \in I\}$ a subset of V. Then there exists a linear map $f\colon K^{(I)} \to V$ such that $f(\lambda_i) = \sum_{i\in I} \lambda_i x_i$. Moreover, $\mathrm{Im}(f) = \mathrm{span}(S)$.

Proof. Note first that since $(\lambda_i) \in K^{(I)}$, almost all λ_i are zero and hence the sum $\sum_{i\in I} \lambda_i x_i$ has only finitely many non-zero terms. Therefore this sum makes sense inside V. Now,

$$\begin{aligned} f\big((\lambda_i) + \alpha(\mu_i)\big) = f(\lambda_i + \alpha\mu_i) &= \sum_i (\lambda_i + \alpha\mu_i)x_i \\ &= \sum_i \lambda_i x_i + \alpha \sum_i \mu_i x_i = f(\lambda_i) + \alpha f(\mu_i). \end{aligned}$$

Therefore f is linear. The image of f is all possible linear combinations of vectors in S, which is precisely $\mathrm{span}(S)$. □

A.2.4 Lemma

We denote the set of all homomorphisms $U \to V$ by $\mathrm{Hom}(U, V)$. This set becomes a vector space by defining

$$(f + \lambda g)(u) := f(u) + \lambda g(u).$$

The zero is the homomorphism $u \mapsto 0$ for all $u \in U$.

In the special case when $U = V$ we write $\mathrm{End}(V) := \mathrm{Hom}(V, V)$.

A.2.5 Factor Lemma

Let $f\colon V \to W$ be linear, and let $U \leq \operatorname{Ker}(f)$. Then there is a linear map

$$\bar{f}\colon V/U \to W, \quad v + U \mapsto f(v).$$

Moreover, this is the unique linear map with $f = \bar{f}\pi$, where $\pi\colon V \to V/U$ is the natural map.

Proof. To check that $\bar{f}$ is well-defined, suppose $v+U = v'+U$, so that $v-v' \in U$. Since $U \leq \operatorname{Ker}(f)$ we have $f(v - v') = 0$, and hence $f(v) = f(v')$.

It is now immediate that $f = \bar{f}\pi$, since

$$\bar{f}\pi(v) = \bar{f}(v + U) = f(v).$$

To see that $\bar{f}$ is linear we observe that

$$\begin{aligned}\bar{f}\big((v + U) + \lambda(v' + U)\big) &= \bar{f}\big((v + \lambda v') + U\big) = f(v + \lambda v') \\ &= f(v) + \lambda f(v') = \bar{f}(v + U) + \lambda\bar{f}(v' + U).\end{aligned}$$

Finally, suppose $g\colon V/U \to W$ also satisfies $f = g\pi$. Then

$$g(v + U) = g\pi(v) = f(v) = \bar{f}(v + U).$$

Thus $g = \bar{f}$. □

A.2.6 First Isomorphism Theorem

Let $f\colon V \to W$ be linear. Then the induced map $\bar{f}\colon V/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ is an isomorphism.

Proof. The map $\bar{f}\colon V/\operatorname{Ker}(f) \to W$ exists by the Factor Lemma. It is a monomorphism, so injective, since if $\bar{f}(v + \operatorname{Ker}(f)) = 0$, then $f(v) = 0$, so that $v \in \operatorname{Ker}(f)$. Thus $v + \operatorname{Ker}(f) = 0 + \operatorname{Ker}(f)$. Finally, since $\operatorname{Im}(f) = \operatorname{Im}(\bar{f})$, the induced map $\bar{f}\colon V/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ is onto. Therefore $\bar{f}$ is a bijection, so an isomorphism. □

A.2.7 Example

Let U and V be vector spaces, and consider the direct product $U \times V$. Then the natural maps

$$\iota_1\colon U \to U \times V, \quad u \mapsto (u, 0), \quad \text{and} \quad \iota_2\colon V \to U \times V, \quad v \mapsto (0, v),$$

are monomorphisms, and the natural maps

$$\pi_1\colon U \times V \to U, \quad (u, v) \mapsto u, \quad \text{and} \quad \pi_2\colon U \times V \to V, \quad (u, v) \mapsto v,$$

are epimorphisms.

Moreover,

$$\mathrm{Im}(\iota_1) = \mathrm{Ker}(\pi_2) = U' = \{(u, 0) : u \in U\}$$

and

$$\mathrm{Im}(\iota_2) = \mathrm{Ker}(\pi_1) = V' = \{(0, v) : v \in V\}.$$

Finally $U \times V = U' \oplus V'$.

Note that we have natural isomorphisms $U \cong U'$ and $V \cong V'$, and it is for this reason people often abuse notation and write $U \oplus V$ for the direct product $U \times V$.

Observe that the homomorphisms ι_i and π_i satisfy

$$\pi_1\iota_1 = \mathrm{id}_U, \quad \pi_2\iota_2 = \mathrm{id}_V, \quad \iota_1\pi_1 + \iota_2\pi_2 = \mathrm{id}_{U\times V}.$$

A.3 Bases

A.3.1 Linear Independence

Let V be a vector space and $S \subset V$ a subset.

We say that S is **linearly independent** provided that we cannot write 0 as a non-trivial linear combination of elements of S. In other words, if $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ with $\lambda_i \in K$ and $x_i \in S$, then necessarily $\lambda_i = 0$ for all i.

We say that S is a **basis** for V provided that it is linearly independent and spans V.

It is easy to show that S is a basis for V if and only if *every* element $v \in V$ can be written *uniquely* in the form $v = \lambda_1 x_1 + \cdots + \lambda_n x_n$ for some $\lambda_i \in K$ and $x_i \in S$.

Note that if S is linearly independent, then it is necessarily a basis for the subspace $\mathrm{span}(S)$.

A.3.2 Example

We usually write $e_i \in K^{(I)}$ for the element having a 1 in position i and zero elsewhere. These elements are clearly linearly independent. Moreover, if $v = (a_i) \in K^{(I)}$, then almost all $a_i \in K$ are zero, so the sum $\sum_{i\in I} a_i e_i$ makes sense and equals v. This proves that the e_i form a basis for $K^{(I)}$, called the **standard basis vectors**.

Note that the analogous statement for K^I is *not* true. For, we only allow *finite* sums of vectors, so it is not true in general that $(a_i) = \sum_i a_i e_i$. This holds if and only if almost all $a_i \in K$ are zero, or equivalently $(a_i) \in K^{(I)}$.

A.3.3 Example

The set of matrices $\mathbb{M}_{n\times m}(K)$ has a basis given by the **elementary matrices** E_{ij}, which have a 1 in position (i, j) and are zero elsewhere.

A.3.4 Matrices as Linear Maps

Let $e_1, \ldots, e_m \in K^m$ be the standard basis vectors for K^m, and $e'_1, \ldots, e'_n \in K^n$ the standard basis vectors for K^n.

If $f\colon K^m \to K^n$ is a linear map, then we can write $f(e_j) = \sum_i a_{ij} e'_i$ with $a_{ij} \in K$, and hence form the matrix $A = (a_{ij}) \in \mathbb{M}_{n\times m}(K)$. This construction gives an isomorphism

$$\Theta\colon \operatorname{Hom}(K^m, K^n) \xrightarrow{\sim} \mathbb{M}_{n\times m}(K).$$

Proof. We check that Θ is linear. Suppose that $\Theta(f) = A$ and $\Theta(g) = B$. Then for $\lambda \in K$ we have

$$(f + \lambda g)(e_j) = f(e_j) + \lambda g(e_j) = \sum_i a_{ij} e'_i + \lambda \sum_i b_{ij} e'_i = \sum_i (a_{ij} + \lambda b_{ij}) e'_i.$$

Thus

$$\Theta(f + \lambda g) = (a_{ij} + \lambda b_{ij}) = (a_{ij}) + \lambda (b_{ij}) = \Theta(f) + \lambda \Theta(g).$$

We now check that Θ is an isomorphism. Suppose that $\Theta(f) = 0$. Then $f(e_j) = 0$ for all j, so $f = 0$. Hence Θ is injective. Conversely let (a_{ij}) be a matrix and define $f\colon K^m \to K^n$ via

$$(x_1, x_2, \ldots, x_m) \mapsto \big(\sum_j a_{1j} x_j, \sum_j a_{2j} x_j, \ldots, \sum_j a_{nj} x_j\big).$$

Then it is again easy to check that f is linear, and since

$$f(e_j) = (a_{1j}, a_{2j}, \ldots, a_{nj}) = \sum_i a_{ij} e'_i,$$

we have $\Theta(f) = (a_{ij})$, so Θ is surjective. Hence Θ is an isomorphism. □

A.3.5 Lemma

Let V be a vector space and $S = \{x_i : i \in I\} \subset V$ a subset. Recall that we have a linear map $f\colon K^{(I)} \to V$, $(\lambda_i) \mapsto \sum_{i\in I} \lambda_i x_i$, whose image is precisely $\operatorname{span}(S)$.

Then S is linearly independent if and only if f is a monomorphism, and S is a basis if and only if f is an isomorphism. In other words, picking a basis $\{x_i : i \in I\}$ for V is equivalent to picking an isomorphism $V \cong K^{(I)}$.

Proof. We observe that S is linearly dependent if and only if we can write $0 = \sum_{i\in I} \lambda_i x_i$ as a finite sum with $\lambda_i \in K$ not all zero. This is equivalent to saying that $(\lambda_i) \in K^{(I)}$ is non-zero and lies in the kernel of f, or in other words that f is not a monomorphism.

Now, S is a basis if and only if it is both a spanning set and linearly independent, which is if and only if f is both an epimorphism and a monomorphism, so an isomorphism. □

A.3.6 Theorem

The following are equivalent for a subset S of a vector space V.

1. S is a basis for V.
2. S is a maximal linearly independent set.
3. S is a minimal spanning set.

Proof. $1 \Rightarrow 2, 3$. Let S be a basis for V. Then S is linearly independent and spans V.

To see that S is maximal linearly independent, take $v \in V \setminus S$. Since S is a basis we can write $v = \lambda_1 x_1 + \cdots + \lambda_n x_n$ for $\lambda_i \in K$ and $x_i \in S$. Rearranging gives $\lambda_1 x_1 + \cdots + \lambda_n x_n - v = 0$ and the coefficient of v is 1. Hence $S \cup \{v\}$ is not linearly independent.

To see that S is minimal spanning, take $v \in S$ and set $S' = S \setminus \{v\}$. If $\text{span}(S') = V$, then we can write $v = \lambda_1 x_1 + \cdots + \lambda_n x_n$ with $\lambda_i \in K$ and $x_i \in S'$. Rearranging gives $\lambda_1 x_1 + \cdots + \lambda_n x_n - v = 0$, contradicting the linear independence of S.

$2 \Rightarrow 1$. Let S be a linearly independent set and suppose $v \in V \setminus \text{span}(S)$. We claim that $S \cup \{v\}$ is linearly independent. For, suppose $0 = \lambda_1 x_1 + \cdots + \lambda_n x_n + \mu v$ with $\lambda_i, \mu \in K$ and $x_i \in S$. If $\mu = 0$, then since S is linearly independent we know that each $\lambda_i = 0$. If instead $\mu \neq 0$, then rearranging gives $v = -\mu^{-1}(\lambda_1 x_1 + \cdots + \lambda_n x_n)$, so $v \in \text{span}(S)$, a contradiction.

It follows that if S is maximal linearly independent, then it is also a spanning set and hence a basis.

$3 \Rightarrow 1$. Let S be a spanning set and suppose that S is not linearly independent. Therefore we can write $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ for some $x_i \in S$ and $\lambda_i \in K$ with $\lambda_1 \neq 0$. Rearranging gives $x_1 = -\lambda_1^{-1}(\lambda_2 x_2 + \cdots + \lambda_n x_n)$, and so $x_1 \in \text{span}(S')$ where $S' = S \setminus \{x_1\}$. If $v \in \text{span}(S)$, then we can write $v = \mu_1 x_1 + \mu_2 y_2 + \cdots + \mu_m y_m$ with $\mu_i \in K$ and $y_i \in S'$. Substituting in for x_1 then gives

$$v = -\lambda_1^{-1}(\lambda_2 x_2 + \cdots + \lambda_n x_n) + \mu_2 y_2 + \cdots + \mu_m y_m,$$

so $v \in \text{span}(S')$. Thus $\text{span}(S') = \text{span}(S)$.

It follows that if S is a minimal spanning set, then it is also linearly independent and hence a basis. □

A.4 Dimension

A.4.1 Proposition

We have $K^m \cong K^n$ if and only if $m = n$.

More generally if $m > n$, then no linear map $K^m \to K^n$ is injective, and no linear map $K^n \to K^m$ is surjective.

Proof. Let $e_1, \ldots, e_m \in K^m$ and $e'_1, \ldots, e'_n \in K^n$ be the standard basis vectors.

Let $m > n$. Suppose $f\colon K^m \to K^n$ is linear. Write $f(e_j) = \sum_i a_{ij} e'_i$ with $a_{ij} \in K$. Then we can form the matrix $(a_{ij}) \in \mathbb{M}_{n\times m}(K)$. By applying the Gauss Algorithm we can find $\lambda_j \in K$ not all zero such that $\sum_j a_{ij}\lambda_j = 0$ for each i. Thus $x = \sum_j \lambda_j e_j \in K^m$ is non-zero and

$$\begin{aligned} f(x) &= f\big(\sum_j \lambda_j e_j\big) = \sum_j \lambda_j f(e_j) \\ &= \sum_j \lambda_j \big(\sum_i a_{ij} e'_i\big) = \sum_i \big(\sum_j a_{ij}\lambda_j\big) e'_i = 0. \end{aligned}$$

Thus $\operatorname{Ker}(f) \neq 0$, so f is not injective.

Now suppose that $g\colon K^n \to K^m$ is linear. Write $g(e'_j) = \sum_i b_{ij} e_i$, so $(b_{ij}) \in \mathbb{M}_{m\times n}(K)$. By applying the Gauss Algorithm to the transpose of this matrix we can find $\mu_i \in K$ not all zero such that $\sum_i \mu_i b_{ij} = 0$. We claim that if $v = (v_1, \ldots, v_m) \in \operatorname{Im}(g)$, then $\sum_i \mu_i v_i = 0$. Since $\mu_l \neq 0$ for some l it follows that $e_l \notin \operatorname{Im}(g)$, and hence g is not surjective.

To prove the claim note that, if $v = g(x)$ with $x = (x_1, \ldots, x_n)$, then

$$\sum_i v_i e_i = g\big(\sum_j x_j e'_j\big) = \sum_i \big(\sum_j b_{ij} x_j\big) e_i,$$

so $v_i = \sum_j b_{ij} x_j$. Thus

$$\sum_i \mu_i v_i = \sum_i \mu_i \big(\sum_j b_{ij} x_j\big) = \sum_j \big(\sum_i \mu_i b_{ij}\big) x_j = 0.$$

If $h\colon K^m \xrightarrow{\sim} K^n$ is an isomorphism, then it must be a bijection, so $m = n$. □

A.4.2 Finite-Dimensional Vector Spaces

A vector space is called **finite dimensional** if it is isomorphic to some K^n. If this is the case, then by the proposition above the integer n is unique, so we say that V has dimension n and write $\dim V = n$.

If $\dim V = n$, then every basis has size n. For, let $g\colon V \xrightarrow{\sim} K^n$ be an isomorphism. Given a basis $S = \{x_1, \ldots, x_m\} \subset V$ we obtain by Lemma A.3.5 an isomorphism $f\colon K^m \xrightarrow{\sim} V$, and hence an isomorphism $gf\colon K^m \xrightarrow{\sim} K^n$. Thus $m = n$ by the previous proposition.

Note that V is finite dimensional if and only if it has a finite spanning set. For, given a finite spanning set, we can successively remove vectors until we have a minimal spanning set, which is then a basis by Theorem A.3.6.

A.4.3 Rank-Nullity Theorem

Let V be a finite-dimensional vector space and $U \leq V$ a subspace. Then both U and V/U are finite-dimensional, and $\dim V = \dim U + \dim V/U$.

More generally, let $f\colon V \to W$ be linear. Then $\dim V = \dim \operatorname{Ker}(f) + \dim \operatorname{Im}(f)$.

Proof. Suppose $\dim V = d$ and let $\{e_1, \ldots, e_d\}$ be a basis for V. Then their images $e_i + U$ span V/U. For, let $v + U \in V/U$. Since the e_i form a basis for V we can write $v = \lambda_1 e_1 + \cdots + \lambda_d e_d$, and so

$$v + U = (\lambda_1 e_1 + \cdots + \lambda_d e_d) + U = \lambda_1(e_1 + U) + \cdots + \lambda_d(e_d + U).$$

Thus V/U is spanned by the $e_i + U$ as claimed.

Since V/U has a finite spanning set, it is finite dimensional by the previous remarks. In fact, by successively removing superfluous vectors we can find a minimal spanning set, which must then be a basis. Thus, renumbering if necessary, we may assume that for some $n \leq d$ the set $\{e_1 + U, \ldots, e_n + U\}$ is a basis for V/U.

Set $U' = \operatorname{span}\{e_1, \ldots, e_n\}$. We claim that $V = U \oplus U'$. For, we first note that the restriction map $U' \to V/U$ is an isomorphism. Since the kernel is $U \cap U'$ we deduce that $U \cap U' = \{0\}$. On the other hand, given $v \in V$ we can write $v + U = u' + U$ for some $u' \in U'$. Thus $v - u' = u \in U$, so $v = u + u'$, so $V = U + U'$. Hence $V = U \oplus U'$ as claimed.

Exchanging the roles of U and U' we immediately get that the map $U \to V/U'$ is an isomorphism, and hence as above that U is finite dimensional, say $\dim U = m$. We now have isomorphisms $f\colon K^m \xrightarrow{\sim} U$ and $g\colon K^n \xrightarrow{\sim} U'$. Putting these together we obtain an isomorphism

$$(f, g)\colon K^m \times K^n \xrightarrow{\sim} U \oplus U' = V, \quad (x, y) \mapsto f(x) + g(y).$$

Finally it is easy to see that $K^m \times K^n \cong K^{m+n}$. Thus we have an isomorphism $V \cong K^{m+n}$, so $\dim V = m + n = \dim U + \dim V/U$.

The more general statement follows from the First Isomorphism Theorem. For, $\operatorname{Im}(f) \cong V/\operatorname{Ker}(f)$, and so $\dim \operatorname{Im}(f) = \dim V/\operatorname{Ker}(f) = \dim V - \dim \operatorname{Ker}(f)$. □

A.4.4 Corollary

Let U and V be finite-dimensional subspaces of a vector space W. Then

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

Proof. We first observe that $U + V$ is finite dimensional. For, if $\{x_i\}$ and $\{y_j\}$ are bases for U and V respectively, then their union $\{x_i, y_j\}$ is a finite spanning set for $U + V$.

Consider the canonical map $U + V \to (U + V)/U$. We know that this is an epimorphism with kernel U, so by the Rank-Nullity Theorem we have

$$\dim(U + V) = \dim U + \dim(U + V)/U.$$

Now consider the restriction $V \to (U + V)/U$. This has kernel $U \cap V$. On the other hand it is still an epimorphism. For, every element in $(U + V)/U$ is of the form $(u + v) + U$ for some $u \in U$ and $v \in V$. Since $(u + v) - v \in U$ we have $(u + v) + U = v + U$. By the Rank-Nullity Theorem we get

$$\dim V = \dim(U \cap V) + \dim(U + V)/U.$$

Putting these together we get that

$$\dim V = \dim(U \cap V) + \dim(U + V) - \dim U$$

as required. □

A.5 Infinite-Dimensional Vector Spaces

In this section we show that every vector space V has a basis and that any two bases of V have the same cardinality. We thus define $\dim V$ to be the cardinality of a basis of V. We will need Zorn's Lemma to prove that bases exist, and Hall's Marriage Theorem together with the Cantor-Bernstein-Schröder Theorem to prove that any two bases have the same cardinality.

A.5.1 Partial Orders

A **partially ordered set**, or **poset**, is a set X together with a **partial order** $\leq$ on the elements of X. This is a relation which is

reflexive	$x \leq x$.
antisymmetric	$x \leq y$ and $y \leq x$ imply $x = y$.
transitive	$x \leq y$ and $y \leq z$ imply $x \leq z$.

It is a *partial* order, since for any two elements $x, y \in X$, it could be that neither $x \leq y$ nor $y \leq x$ is true. We say x and y are **incomparable** if this happens.

A **chain** in X is a subset $C \subset X$ such that every two elements $x, y \in C$ are comparable; that is, either $x \leq y$ or $y \leq x$. Thus $(C, \leq)$ is **totally ordered**.

An **upper bound** for a subset $Y \subset X$ is an element $x \in X$ such that $y \leq x$ for all $y \in Y$. We do *not* require that $x \in Y$. A **maximal element** of X is an element $x \in X$ such that $x \leq x'$ implies $x = x'$; thus no element is strictly larger than x.

A.5.2 Zorn's Lemma

If $(X, \leq)$ is a non-empty poset in which every chain has an upper bound, then X has a maximal element.

Zorn's Lemma is frequently used in algebra to deal with cases where one might otherwise use induction. See for example the discussion by Tim Gowers.

A.5.3 Hall's Marriage Theorem

Let X and Y be two sets. Suppose $S \subset X \times Y$ has the property that for each finite subset $X' \subset X$ the set of neighbours

$$N(X') = \{y \in Y : (x, y) \in S \text{ for some } x \in X'\}$$

is finite of size at least that of X', so $|X'| \leq |N(X')| < \infty$. Then Hall's Marriage Theorem states that there exists an injective map $f \colon X \to Y$ with $(x, f(x)) \in S$ for all $x \in X$.

Note that if X and Y are both finite, then giving a subset $S \subset X \times Y$ is the same as giving a bipartite graph with vertices $X \cup Y$ and edges S.

A.5.4 Cantor-Bernstein-Schröder Theorem

Let X and Y be two sets. If there exist injective maps $X \to Y$ and $Y \to X$, then there exists a bijection $X \cong Y$.

Follow the link for a proof of the Cantor-Bernstein-Schröder Theorem. One of the strengths of this proof is that it does not assume the Axiom of Choice.

Recall that two sets X and Y have the same cardinality provided there exists a bijection between them. One can think of this as saying that bijective maps induce an equivalence relation on sets (but one should be careful since the 'set of all sets' does not exist). In a similar manner, the Cantor-Bernstein-Schröder Theorem says that the relation

$$|X| \leq |Y| \text{ provided there exists an injective map } X \to Y$$

is antisymmetric, and so injective maps induce a partial order on cardinalities (but again there is no 'set of all cardinalities'). If we assume the Axiom of Choice, then we even get a total order.

A.5.5 Every Vector Space has a Basis

Let V be a vector space. We want to apply Zorn's Lemma to the set $\mathcal{S}$ of linearly independent subsets of V.

We begin by noting that $\mathcal{S}$ is a poset via the usual inclusion relation on subsets. We therefore need to check that $\mathcal{S}$ is non-empty and that every chain in $\mathcal{S}$ has an upper bound.

The first is easy, since $\mathcal{S}$ contains the empty set. Alternatively, if $0 \neq v \in V$ then $\{v\}$ is linearly independent.

For the second, let $\{S_i : i \in I\}$ be a chain in $\mathcal{S}$. Therefore S_i is linearly independent for all $i \in I$, and if $i, j \in I$, then either $S_i \subset S_j$ or $S_j \subset S_i$. We claim that their union $S := \bigcup_i S_i$ is an upper bound for the chain $\{S_i : i \in I\}$.

Clearly $S_i \subset S$ for all i, so we just need to check that $S \in \mathcal{S}$; i.e. that S is linearly independent. Suppose $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ with $\lambda_r \in K$ and $x_r \in S$. Then each x_r lies in some S_{i_r}, and by assumption, for each p, r we have either $S_{i_p} \subset S_{i_r}$ or $S_{i_r} \subset S_{i_p}$. We may therefore take q such that $S_{i_r} \subset S_{i_q}$ for all r. Hence $x_r \in S_{i_q}$ for all r, and since S_{i_q} is linearly independent we deduce that $\lambda_r = 0$ for all r. This proves that S is linearly independent.

We can therefore apply Zorn's Lemma to obtain a maximal element $S \in \mathcal{S}$. In other words S is a maximal linearly independent set, so by Theorem A.3.6 it is a basis.

A.5.6 Dimension

Let V be a vector space. Then any two bases of V have the same cardinality. We may therefore define the **dimension** of V, denoted $\dim V$, to be the cardinality of any basis of V.

Proof. Let V be a vector space, and $X = \{x_j\}$ and $Y = \{y_i\}$ two bases of V. We will use Hall's Marriage Theorem to show that there is an injection $X \to Y$. Swapping X and Y then gives an injection $Y \to X$, and so $|X| = |Y|$ by the Cantor-Bernstein-Schroöder Theorem.

For each $x_j \in X$ we can write it uniquely as $x_j = \sum_i a_{ij} y_i$ with almost all a_{ij} zero. Setting

$$S = \{(x_j, y_i) : a_{ij} \neq 0\} \subset X \times Y$$

we therefore see that $N(x_j)$ is finite for all $x_j \in X$, and hence $N(X')$ is finite for all finite subsets $X' \subset X$.

Let $X' = \{x_1, \ldots, x_m\} \subset X$ be a finite subset, and let $N(X') = \{y_1, \ldots, y_n\} \subset Y$. We need to check that $|X'| \leq |N(X')|$. Using the scalars a_{ij} for $1 \leq i \leq n$ and $1 \leq j \leq m$ we may form the matrix $A = (a_{ij}) \in \mathbb{M}_{n \times m}(K)$. If $|X'| > |N(X')|$, then $m > n$, so by the Gauss Algorithm we can find scalars $\lambda_j \in K$ not all zero such that $\sum_j a_{ij} \lambda_j = 0$ for all i. It follows that

$$\sum_j \lambda_j x_j = \sum_j \lambda_j \big(\sum_i a_{ij} y_i \big) = \sum_i \big(\sum_j a_{ij} \lambda_j \big) y_i = 0,$$

contradicting the linear independence of X. Thus $m \leq n$ as required.

We can therefore apply Hall's Marriage Theorem to obtain an injection $X \to Y$, finishing the proof. □

B Rotations

We review the basic properties of rotations in **Euclidean space** $\mathbb{R}^n$. Recall that this is an n-dimensional real vector space equipped with the **scalar product**

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = x_1 y_1 + \cdots + x_n y_n.$$

Note that this scalar product is

positive definite	$x \cdot x \geq 0$ with equality if and only if $x = 0$.
symmetric	$x \cdot y = y \cdot x$.
bilinear	$(x + \lambda y) \cdot z = (x \cdot z) + \lambda(y \cdot z)$ and $x \cdot (y + \lambda z) = (x \cdot y) + \lambda(x \cdot z)$.

It follows that the scalar product is also **non-degenerate**, so $x \cdot y = 0$ for all y implies $x = 0$.

We define the **length** of a vector x to be

$$|x| = \sqrt{x \cdot x}.$$

If $x \cdot y = 0$, then we say that x and y are **orthogonal**.

B.1 Orthogonal Matrices

We define the group of **orthogonal matrices** to be

$$O_n(\mathbb{R}) = \{M \in \mathbb{M}_n(\mathbb{R}) : MM^t = I\},$$

where M^t is the **transpose** of M. Inside this we have the subgroup of **special orthogonal matrices**

$$SO_n(\mathbb{R}) = \{M \in O_n(\mathbb{R}) : \det(M) = 1\}.$$

Since $\det(M^t) = \det(M)$ we have for all $M \in O_n(\mathbb{R})$ that $\det(M)^2 = 1$, so $\det(M) = \pm 1$. Thus $SO_n(\mathbb{R})$ is the kernel of the group homomorphism $\det\colon O_n(\mathbb{R}) \to \{\pm 1\}$. Much more information can be found on Wikipedia.

Note that the scalar product can be viewed in terms of matrix multiplication: taking vectors in $\mathbb{R}^n$ to be column vectors we have $x \cdot y = x^t y$. Using this we see that if M is a matrix with columns $x_1, \ldots, x_n$, then $M^t M$ is the matrix $(x_i \cdot x_j)$.

An **orthogonal basis** of $\mathbb{R}^n$ is a basis $\{e_1, \ldots, e_n\}$ of orthogonal vectors, so $e_i \cdot e_j = 0$ for $i \neq j$. An **orthonormal basis** is an orthogonal basis $\{e_i\}$ such that each e_i has length 1, so $e_i \cdot e_j = \delta_{ij}$. It follows that a matrix M is orthogonal if and only if its columns form an orthonormal basis.

B.1.1 Lemma

The importance of the orthogonal matrices is that they preserve the scalar product, and hence also the length of vectors.

For, M preserves the scalar product if and only if $(Mx) \cdot (My) = x \cdot y$ for all x and y. Now,

$$x \cdot (My) = x^t My = (M^t x)^t y = (M^t x) \cdot y,$$

so $(Mx) \cdot (My) = (M^t M)x \cdot y$. Since the scalar product is blinear it follows that M preserves the scalar product if and only if $((M^t M)x - x) \cdot y = 0$ for all x and y. Using that the scalar product is non-degenerate, this is equivalent to $(M^t M)x = x$ for all x, and hence to $M^t M = I$. Thus M preserves the scalar product if and only if $M \in O_n(\mathbb{R})$.

B.1.2 Orientations

Let $\{e_1, \ldots, e_n\}$ be an orthonormal basis, and let N be the orthogonal matrix with columns $e_1, \ldots, e_n$. We say that the *ordered* basis $(e_1, \ldots, e_n)$ is **positive** (or **right handed**) provided $\det(N) = 1$, and **negative** (or **left handed**) if $\det(N) = -1$.

Using that the scalar product is bilinear we can reinterpret the previous lemma as showing that a matrix M is orthogonal if and only if $\{Me_1, \ldots, Me_n\}$ is again orthonormal. In this setting M is special orthogonal if and only if it preserves the orientation; that is, $(e_1, \ldots, e_n)$ is a positive basis if and only if $(Me_1, \ldots, Me_n)$ is positive.

For, the matrix with columns $Me_1, \ldots, Me_n$ is just MN and $\det(MN) = \det(M)\det(N)$. Hence M preserves the orientation if and only if $\det(MN) = \det(N)$, which is if and only if $\det(M) = 1$.

B.2 Rotations in 2-Space

The rotation through angle θ in $\mathbb{R}^2$ is the matrix (or rather the corresponding linear map)

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

Note that $R_0 = I$ is the identity, and rotating through angle θ and then through angle ϕ is the same as rotating through angle $\theta + \phi$. In terms of matrices, $R_\phi R_\theta = R_{\theta+\phi}$, which is just the double angle formulae:

$$\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{pmatrix}.$$

We claim that the group of rotations is $SO_2(\mathbb{R})$. Clearly $R_\theta^t = R_{-\theta}$, so $R_\theta R_\theta^t = R_0 = I_2$, and $\det(R_\theta) = (\cos\theta)^2 + (\sin\theta)^2 = 1$, so $R_\theta \in SO_2(\mathbb{R})$. Conversely suppose that

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO(2, \mathbb{R}).$$

Then the conditions on M translate into three conditions on a, b, c, d:

$$a^2 + b^2 = 1, \quad c^2 + d^2 = 1, \quad ac + bd = 0, \quad ad - bc = 1.$$

Using the first two equations we see that there are unique angles $\theta, \phi \in [0, 2\pi)$ satisfying

$$(a, b) = (\cos\theta, -\sin\theta) \quad \text{and} \quad (c, d) = (\sin\phi, \cos\phi).$$

The third and fourth equations can now be rewritten as

$$\sin(\theta - \phi) = 0 \quad \text{and} \quad \cos(\theta - \phi) = 1.$$

Since $\theta - \phi \in (-2\pi, 2\pi)$, we deduce that $\theta = \phi$, whence $M = R_\theta$.

B.3 Rotations in 3-space

To describe a rotation in 3-space we take an axis n (which we may assume has length 1) and an angle θ, and consider the rotation about n through angle θ. To avoid ambiguity we take this to mean that we rotate anticlockwise by θ when looking back along the axis n.

In terms of a basis, let (n, u, v) be a right-handed orthonormal basis. Then the rotation about n through angle θ is the linear map $R_{n,\theta}$ given by

$$n \mapsto n, \quad u \mapsto \cos(\theta)u + \sin(\theta)v, \quad v \mapsto -\sin(\theta)u + \cos(\theta)v.$$

Note that if u is any unit vector orthogonal to n, then there is a unique right-handed orthonormal basis (n, u, v) given by $v = n \times u$, the **vector product** or **cross product** of n by u.

B.3.1 Theorem

An endomorphism of $\mathbb{R}^3$ is a rotation if and only if its matrix is special orthogonal.

The following proof is due to B. Palais and R. Palais in 2007 (pdf), although the result is originally due to Euler in 1775.

Proof. Let (n, u, v) be a right-handed orthonormal basis, and let $R = R_{n,\theta}$ be the (matrix of the) rotation about n through angle θ, so

$$n \mapsto n, \quad u \mapsto \cos(\theta)u + \sin(\theta)v, \quad v \mapsto -\sin(\theta)u + \cos(\theta)v.$$

A quick check shows that (Rn, Ru, Rv) is again an orthonormal basis. Moreover, since $v = n \times u$, we have $n \times v = -u$ and so

$$\begin{aligned}(Rn) \times (Ru) &= n \times \big(\cos(\theta)u + \sin(\theta)v\big) = \cos(\theta)n \times u + \sin(\theta)n \times v \\ &= \cos(\theta)v - \sin(\theta)u = Rv.\end{aligned}$$

Thus (Rn, Ru, Rv) is again right handed, and hence $R \in SO_3(\mathbb{R})$.

Conversely let $M \in SO_3(\mathbb{R})$. We will show that M has an axis: that is, that there exists a unit vector n such that $Mn = n$.

We first show that M respects the vector product, so $(Mf) \times (Mg) = M(f \times g)$ for all $f, g \in \mathbb{R}^3$. Consider the standard basis $\{e_1, e_2, e_3\}$. Then (e_i, e_j, e_k) is

right-handed for all cyclic permutations (ijk) of (123) (that is, $(ijk) = (123)$, (231) or (312)), since $e_i \times e_j = e_k$. As M is special orthogonal we have $(Me_i) \times (Me_j) = Me_k = M(e_i \times e_j)$ for all cyclic permutations (ijk) of (123), and hence that $(Me_i) \times (Me_j) = M(e_i \times e_j)$ for all i, j. Finally, since the vector product is bilinear, we have $(Mf) \times (Mg) = M(f \times g)$ for all $f, g \in \mathbb{R}^3$ as required.

Now consider the matrix $A = \frac{1}{2}(M - M^t)$. Then $A^t = -A$, so there exist numbers $a, b, c \in \mathbb{R}$ such that

$$A = \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix}.$$

Set $n := (a, b, c)$ and observe that for any vector $f = (x, y, z)$ we have

$$Af = \begin{pmatrix} bz - cy \\ cx - az \\ ay - bx \end{pmatrix} = n \times f.$$

Using the observation above we have

$$(MAM^t)f = M(A(M^t f)) = M(n \times (M^t f)) = (Mn) \times (MM^t f) = (Mn) \times f.$$

On the other hand,

$$MAM^t = \tfrac{1}{2}M(M - M^t)M^t = \tfrac{1}{2}(MMM^t - MM^tM^t) = \tfrac{1}{2}(M - M^t) = A.$$

Thus $n \times f = (Mn) \times f$ for all f. We conclude that $Mn = n$.

So, provided that $n \neq 0$, we can rescale to make n a unit vector and we are done.

Otherwise $n = 0$, so $A = 0$, and hence $M = M^t$. Therefore $M^2 = MM^t = I$. In this case consider the matrix $B = I + M$. Since $\det M = 1$ we know that $M \neq -I$ and so $B \neq 0$. Also,

$$MB = M(I + M) = M + M^2 = M + I = B.$$

This shows that M fixes each of the columns of B, and since one of these is non-zero we obtain our axis n.

Now let (n, u, v) be a right-handed orthonormal basis. Then (Mn, Mu, Mv) is again a right-handed orthonormal basis and $Mn = n$. Thus Mu and Mv are linear combinations of u and v, say

$$Mu = au + cv \quad \text{and} \quad Mv = bu + dv.$$

Finally let V be the matrix with columns n, u, v, so $V \in SO_3(\mathbb{R})$. Then

$$V^tMV = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

and also $V^tMV \in SO_3(\mathbb{R})$ since this is a group. It follows that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2(\mathbb{R}),$$

so by the previous result $a = d = \cos\theta$ and $-b = c = \sin\theta$ for some $\theta \in [0, 2\pi)$. Thus $M = R_{n,\theta}$ is the rotation about n through angle θ. □

B.4 Rotations in n-space

Analogously to what happens in 2-space and 3-space, if $(e_1, \ldots, e_n)$ is a right-handed orthonormal basis and $\theta \in [0, 2\pi)$, then we should call the linear map

$$e_1 \mapsto (\cos\theta)e_1 + (\sin\theta)e_2, \quad e_2 \mapsto -(\sin\theta)e_1 + (\cos\theta)e_2, \quad e_i \mapsto e_i \text{ for } i \geq 3$$

a rotation. Also, we should allow compositions of rotations to again be rotations.

With this definition one can show that the group of rotations in n-space is precisely the special orthogonal group $SO_n(\mathbb{R})$. Note however that rotations may not have axes. For example, in $\mathbb{R}^4$ we have the rotation

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

C Presentations of Groups (non-examinable)

In this appendix we show how the same ideas used for algebras can be used to give presentations of groups. The main difference is that it is harder to construct the free group on a set than it is to construct the free algebra on a set, the reason being that we now have to have inverses of elements. In fact, a better analogy would be between algebras and monoids, and between groups and division algebras.

C.1 Free Monoids

A **monoid** is like a group, except that it may not have inverses. More precisely it is a set with an associative multiplication and having a unit. As usual, we can define monoid homomorphisms and submonoids, and if $\theta\colon M \to N$ is a monoid homomorphism, then the image $\mathrm{Im}(\theta)$ is a submonoid of N.

Kernels of monoid homomorphisms correspond to congruence relations. A **congruence relation** $\sim$ on a monoid M is an equivalence relation which is compatible with the multiplication: if $x \sim x'$ and $y \sim y'$, then $xy \sim x'y'$. Given a congruence relation $\sim$ on M, the set of equivalence classes has a natural structure of a monoid via $[x][y] := [xy]$, and the canonical map $M \to M/\sim$, $x \mapsto [x]$, is then a monoid homomorphism.

Given a set X, we can now define the **free monoid** $\mathcal{M}(X)$. As a set this has as elements all the words $x_1x_2\cdots x_n$ with $x_i \in X$, and multiplication is given by concatenation of words. This is clearly associative, with unit the empty word 1. The map $X \to \mathcal{M}(X)$ sending an element x to the word x is obviously injective.

Free monoids satisfy the relevant universal property, that monoid homomorphisms $\theta\colon \mathcal{M}(X) \to N$ are in bijection with maps $X \to N$.

For, suppose that N is a monoid and $f\colon X \to N$ is a map. Define $\theta\colon \mathcal{M}(X) \to N$ via

$$\theta(x_1x_2\cdots x_n) := f(x_1)f(x_2)\cdots f(x_n),$$

and observe that this is a monoid homomorphism, and is the unique monid homomorphism extending f.

Again, completely analogously to the situation with algebras, the monoid $\mathcal{M}(X)$ is unique up to isomorphism.

As an example, note that the free monoid $\mathcal{M}(x)$ on a single element x is isomorphic to the monoid of non-negative integers under addition.

C.2 Free Groups

We can now use free monoids to construct free groups, since a group is a monoid for which every element has an inverse.

So, let X be a set. We introduce another set $X^{-1} := \{x^{-1} : x \in X\}$, whose elements are in bijection with X, and form the free monoid $\mathcal{M}(X \cup X^{-1})$. We next take $\sim$ to be the smallest congruence relation on $\mathcal{M}(X \cup X^{-1})$ containing

the relations

$$xx^{-1} \sim 1 \quad \text{and} \quad x^{-1}x \sim 1 \quad \text{for all } x \in X.$$

Finally, we set $\mathcal{F}(X) := \mathcal{M}(X \cup X^{-1})/\sim$, and call this the **free group** on the set X.

We first check that $\mathcal{F}(X)$ is a group. We know that it is a monoid, so we just need to check that every element has an inverse. This is clear, since the word

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}, \quad x_i \in X, \quad \varepsilon_i \in \{\pm 1\}$$

has inverse

$$w^{-1} = x_n^{-\varepsilon_n} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1}.$$

We next check that the map $\iota\colon X \to \mathcal{F}(X)$ sending x to the (equivalence class of the) word x is injective. To do this, fix $x \in X$ and consider the monoid homomorphism

$$\mathcal{M}(X \cup X^{-1}) \to \mathbb{Z}_2 = \{\pm 1\}, \quad y^{\pm 1} \mapsto \begin{cases} 1 & \text{if } y \neq x \\ -1 & \text{if } y = x \end{cases}$$

Clearly yy^{-1} and $y^{-1}y$ are in the kernel of this homomorphism, so it factors through the quotient $\mathcal{F}(X)$. It follows that $\iota(x) \neq 1$ and $\iota(x) \neq \iota(y)$ for all $y \neq x$. Doing this for each $x \in X$ shows that $\iota\colon X \to \mathcal{F}(X)$ is injective.

As an example, the free group $\mathcal{F}(x)$ on a single element x is isomorphic to the integers under addition.

Similarly, $\mathcal{F}(x, y)$ has elements

$$\begin{gathered} 1 \\ x, x^{-1}, y, y^{-1}, \\ x^2, xy, xy^{-1}, x^{-2}, x^{-1}y, x^{-1}y^{-1}, y^2, yx, yx^{-1}, y^{-2}, y^{-1}x, y^{-1}x^{-1} \\ \cdots \end{gathered}$$

C.3 Universal Property

Let G be a group and $f\colon X \to G$ a map. Then there exists a unique group homomorphism $\theta\colon \mathcal{F}(X) \to G$ extending f.

In other words there is a bijection between group homomorphisms $\mathcal{F}(X) \to G$ and maps $X \to G$.

Proof. Suppose we have $f\colon X \to G$. Then we can extend this to $\hat{f}\colon X \cup X^{-1} \to G$ via $\hat{f}(x^{-1}) := f(x)^{-1}$. By the universal property for $\mathcal{M}(X \cup X^{-1})$, there exists a unique *monoid* homomorphism $\hat{\theta}\colon \mathcal{M}(X \cup X^{-1}) \to G$ extending $\hat{f}$. This is given by

$$\hat{\theta}\big(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}\big) := f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \cdots f(x_n)^{\varepsilon_n}.$$

Since G is a group and $\hat{\theta}(x^{-1}) = \hat{\theta}(x)^{-1}$, we see that $\hat{\theta}$ factors through the quotient $\mathcal{F}(X)$. It follows that the induced map $\theta\colon \mathcal{F}(X) \to G$ is a *group* homomorphism extending f.

To see that θ is unique, suppose that $\theta' \colon \mathcal{F}(X) \to G$ is another group homomorphism extending f. Then

$$1 = \theta'(1) = \theta'(x^{-1}x) = \theta'(x^{-1})\theta'(x) = \theta'(x^{-1})f(x),$$

so $\theta'(x^{-1}) = f(x)^{-1} = \hat{f}(x^{-1})$. Composing with the canonical homomorphism $\mathcal{M}(X \cup X^{-1}) \to \mathcal{F}(X)$ now yields two monoid homomorphisms $\hat{\theta}$ and $\hat{\theta}'$ both extending $\hat{f}$. By the uniqueness property for the free monoid we deduce that $\hat{\theta} = \hat{\theta}'$, and hence that $\theta = \theta'$. □

As usual, we can now prove that the free group $\mathcal{F}(X)$ is unique up to isomorphism.

C.4 Generators

Let G be a group and $\{g_i\}$ a subset of G. The **subgroup generated by the** g_i, denoted $\langle\{g_i\}\rangle$, is the smallest subgroup of G containing each of the g_i. It follows that every element in $\langle\{g_i\}\rangle$ can be written (non-uniquely) as a product of the $g_i^{\pm 1}$.

We say that the g_i generate G provided that $G = \langle\{g_i\}\rangle$.

C.5 Examples

1. Everyone knows that the transpositions generate the symmetric group S_n, and that there are $\binom{n}{2}$ such. In fact, we can improve on this, since the symmetric group is generated by the transpositions $(1\,i)$ for $2 \leq i < n$, or else by the $s_i := (i\,i+1)$. In both cases, we need only $n-1$ generators.

2. Similarly the alternating group A_n is generated by the 3-cycles, of which there are $2\binom{n}{3}$. Again, we can improve on this, since the alternating group is generated by the 3-cycles of the form $(12i)$ for $3 \leq i \leq n$. Hence we need only $n-2$ generators.

3. Cyclic groups are those needing only one generator, $G = \langle g \rangle$. Note that if $|G| = n$ is finite, then $g^{-1} = g^{n-1}$, so every element of G is a positive multiple of g; if G is infinite, though, then $G \cong (\mathbb{Z}, +)$ and g^{-1} is not a positive multiple of g.

C.6 Presentations

Suppose $\{g_i\}$ generates G and let $X = \{x_i\}$ be a set. Then the group homomorphism $\theta \colon \mathcal{F}(X) \to G$, $x_i \mapsto g_i$, must be surjective. By the First Isomorphism Theorem we have $G \cong \mathcal{F}(X)/\operatorname{Ker}(\theta)$.

The **relations** are the elements of $\operatorname{Ker}(\theta)$. Let $\operatorname{Ker}(\theta)$ be generated *as a normal subgroup* by elements r_j; that is, $\operatorname{Ker}(\theta)$ is the smallest normal subgroup containing the r_j. Then we say that G is generated by the x_i subject to the relations $r_j = 1$.

We often write

$$G = \langle x_i : r_j = 1 \rangle$$

and call this a **presentation** of G.

Note that, as for algebras, groups usually have many presentations.

C.7 Examples

1. Consider the cyclic group $G = \langle g \rangle$. If $|G| = n$ is finite, then G is generated by g subject to the relation $g^n = 1$. If G is infinite, then $G \cong \mathcal{F}(g)$ is free, and isomorphic to $(\mathbb{Z}, +)$.

2. The symmetric group S_n is generated by the $s_i := (i\, i+1)$ subject to the relations

$$s_i^2 = 1, \quad (s_i s_{i+1})^3 = 1, \quad (s_i s_j)^2 = 1 \text{ for } j > i+1.$$

   In particular, we have

$$S_3 = \langle s_1, s_2 : s_1^2 = s_2^2 = (s_1 s_2)^3 = 1 \rangle$$

   which we can also write as

$$S_3 = \langle s_1, s_2 : s_1^2 = s_2^2 = 1,\ s_1 s_2 s_1 = s_2 s_1 s_2 \rangle.$$

3. For the dihedral groups we have

$$D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = (\sigma\tau)^2 = 1 \rangle = \langle \sigma, \tau : \sigma^n = \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1} \rangle.$$

   For, we let σ be any generator for the subgroup of rotations, so $\sigma^n = 1$. Let τ be any reflection, so $\tau^2 = 1$. It is easily checked that $\tau\sigma\tau = \sigma^{-1}$, so all the relations do lie in the kernel. Also, it is not hard to check that every element in D_n can be written uniquely in the form σ^r or $\sigma^r\tau$ with $0 \le r < n$. Hence σ, τ generate D_n, so we have a surjective group homomorphism

$$G := \mathcal{F}(s,t)/(s^n, t^2, (st)^2) \to D_n, \quad s \mapsto \sigma, \quad t \mapsto \tau.$$

   In particular, $|G| \ge |D_n| = 2n$.

   Conversely, let $N := (s^n, t^2, (st)^2)$ be the normal subgroup of $\mathcal{F}(s,t)$ generated by s^n, t^2 and $(st)^2$. Then every word in $\mathcal{F}(s,t)$ is equivalent to one of the form s^r or $s^r t$ modulo N. For, suppose we have a coset represented by a word in $s^{\pm 1}, t^{\pm 1}$. Since $s^n, t^2 \in N$, we may assume that only powers s^a for $0 \le a < n$ and t^b for $0 \le b < 2$ are used. Also, since $tsts = t(stst)t^{-1} \in tNt^{-1} = N$, we have the equality of cosets $tsN = s^{-1}t^{-1}N = s^{n-1}tN$. So, we can replace any occurrence of ts by $s^{n-1}t$. This shows that every coset has a representative of the form s^a or $s^a t$ with $0 \le a < n$. Hence there are at most $2n$ cosets, so $|G| \le 2n$.

   Putting this together we deduce that $|G| = 2n$ and that $G \cong D_n$.

4. The Quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ has the presentation

$$Q = \langle i, j : i^2 = j^2 = (ij)^2, i^4 = 1 \rangle.$$

As above, we can use the Factor Lemma to deduce that there is a surjective group homomorphism

$$G := \mathcal{F}(x, y)/(x^2y^2, x^3yxy, x^4) \to Q, \quad x \mapsto i, \quad y \mapsto j.$$

Note that we have replace $i^2 = j^2$ by $i^2j^2 = i^4 = 1$, and similarly $i^2 = (ij)^2$ by $i^3jij = 1$.

It is enough to show that $|G| \leq 8$. We claim that every element in G can be written in the form x^r or x^ry with $0 \leq r < 4$. For, we can use the relations $x^4 = 1$ to replace x^{-1} by x^3, and $x^2y^2 = 1$ to replace both y^{-1} by x^2y and y^2 by $x^{-2} = x^2$. Thus every word in $x^{\pm 1}, y^{\pm 1}$ is equivalent to a word using only x^a for $0 \leq a < 4$ and y^b for $0 \leq y < 2$. Finally, we can use $x^3yxy = 1$ to replace yx by $x^{-3}y^{-1} = x^3y$. Thus every word is equivalent to one of the form x^ay^b with $0 \leq a < 4$ and $0 \leq b < 2$. Thus $|G| \leq 8$ as required.

C.8 Proposition

Let $G = \langle g_i : r_j = 1 \rangle$. Then group homomorphisms $G \to H$ are in bijection with maps $f\colon \{g_i\} \to H$ such that $f(r_j) = 1$ for all j.

Proof. By the Factor Lemma, group homomorphisms $\theta\colon G \to H$ are in bijection with group homomorphisms $\hat{\theta}\colon \mathcal{F}(\{g_i\}) \to H$ such that the normal subgroup $N := (\{r_j\})$ lies in the kernel of $\hat{\theta}$. By the Universal Property, group homomorphisms $\hat{\theta}\colon \mathcal{F}(\{g_i\}) \to H$ are in bijection with maps $f\colon \{g_i\} \to H$, and then $N \subset \mathrm{Ker}(\hat{\theta})$ if and only if each r_j lies in the kernel, so $f(r_j) = 1$ for all j. $\square$