Chapter 1

Linear algebra: key concepts

1.1 Vector spaces

Definition. A **vector space** V **over a field** $\mathbb{F}$ is a set V with two operations:

addition $V \times V \to V : (v, w) \mapsto v + w$ such that:

- $v + w = w + v$, for all $v, w \in V$;
- $u + (v + w) = (u + v) + w$, for all $u, v, w \in V$;
- there is a **zero element** $0 \in V$ for which $v + 0 = v = 0 + v$, for all $v \in V$;
- each element $v \in V$ has an **additive inverse** $-v \in V$ for which $v + (-v) = 0 = (-v) + v$.

In fancy language, V with addition is an **abelian group**.

scalar multiplication $\mathbb{F} \times V \to V : (\lambda, v) \mapsto \lambda v$ such that

- $(\lambda + \mu)v = \lambda v + \mu v$, for all $v \in V$, $\lambda, \mu \in \mathbb{F}$.
- $\lambda(v + w) = \lambda v + \lambda w$, for all $v, w \in V$, $\lambda \in \mathbb{F}$.
- $(\lambda\mu)v = \lambda(\mu v)$, for all $v \in V$, $\lambda, \mu \in \mathbb{F}$.
- $1v = v$, for all $v \in V$.

We call the elements of $\mathbb{F}$ **scalars** and those of V **vectors**.

1.2 Subspaces

Definition. A **vector** (or **linear**) **subspace** of a vector space V over $\mathbb{F}$ is a non-empty subset $U \subseteq V$ which is closed under addition and scalar multiplication: whenever $u, u_1, u_2 \in U$ and $\lambda \in \mathbb{F}$, then $u_1 + u_2 \in U$ and $\lambda u \in U$.

In this case, we write $U \leq V$.

Say that U is **trivial** if $U = \{0\}$ and **proper** if $U \neq V$.

1.3 Bases

Definitions. Let $v_1, \dots, v_n$ be a list of vectors in a vector space V.

(1) The **span** of $v_1, \dots, v_n$ is

$$\operatorname{span}\{v_1, \dots, v_n\} := \{\lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_i \in \mathbb{F}, 1 \leq i \leq n\} \leq V.$$

(2) $v_1, \dots, v_n$ **span** V (or **are a spanning list for** V) if $\operatorname{span}\{v_1, \dots, v_n\} = V$.

(3) $v_1, \dots, v_n$ are **linearly independent** if, whenever $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$, then each $\lambda_i = 0$, $1 \leq i \leq n$, and **linearly dependent** otherwise.

(4) $v_1, \dots, v_n$ is a **basis** for V if they are linearly independent and span V.

Definition. A vector space is **finite-dimensional** if it admits a finite list of vectors as basis and **infinite-dimensional** otherwise.

If V is finite-dimensional, the **dimension** of V, $\dim V$, is the number of vectors in a (any) basis of V.

1.3.1 Useful facts

Proposition 1.1 (Algebra 1B, Corollary 1.4.7)**.**
Any linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis.

Proposition 1.2 (Algebra 1B, Corollary 1.4.6)**.**
Let V be a finite-dimensional vector space and $U \leq V$. Then

$$\dim U \leq \dim V$$

with equality if and only if $U = V$.

1.4 Linear maps

Definitions. A map $\phi \colon V \to W$ of vector spaces over $\mathbb{F}$ is a **linear map** (or, in older books, **linear transformation**) if

$$\phi(v + w) = \phi(v) + \phi(w)$$
$$\phi(\lambda v) = \lambda \phi(v),$$

for all $v, w \in V$, $\lambda \in \mathbb{F}$.

The **kernel** of ϕ is $\ker\phi := \{v \in V \mid \phi(v) = 0\} \leq V$.

The **image** of ϕ is $\operatorname{im}\phi := \{\phi(v) \mid v \in V\} \leq W$.

Definition. A linear map $\phi : V \to W$ is a **(linear) isomorphism** if there is a linear map $\psi : W \to V$ such that

$$\psi \circ \phi = \mathrm{id}_V, \qquad \phi \circ \psi = \mathrm{id}_W.$$

If there is an isomorphism $V \to W$, say that V and W are isomorphic and write $V \cong W$.

Lemma 1.3 (Algebra 1B, lemma 1.2.3)**.**
$\phi : V \to W$ is an isomorphism if and only if ϕ is a linear bijection (and then $\psi = \phi^{-1}$).

Notation. For vector spaces V, W over $\mathbb{F}$, denote by $L_{\mathbb{F}}(V, W)$ (or simply $L(V, W)$) the set $\{\phi : V \to W \mid \phi \text{ is linear}\}$ of linear maps from V to W.

Theorem 1.4 (Linearity is a linear condition)**.**
$L(V, W)$ is a vector space under pointwise addition and scalar multiplication. Thus

$$(\phi + \psi)(v) := \phi(v) + \psi(v)$$
$$(\lambda\phi)(v) := \lambda\phi(v),$$

for all $\phi, \psi \in L(V, W)$, $v \in V$ and $\lambda \in \mathbb{F}$.

Proposition 1.5 (Extension by linearity)**.**
Let V, W be vector spaces over $\mathbb{F}$. Let $v_1, \ldots, v_n$ be a basis of V and $w_1, \ldots, w_n$ **any** vectors in W.

Then there is a **unique** $\phi \in L(V, W)$ such that

$$\phi(v_i) = w_i, \qquad 1 \leq i \leq n. \tag{1.1}$$

Theorem 1.6 (Rank-nullity)**.**
Let $\phi : V \to W$ be linear with V finite-dimensional. Then

$$\dim \operatorname{im}\phi + \dim \ker\phi = \dim V.$$

Proposition 1.7.
Let $\phi : V \to W$ be linear with V, W finite-dimensional vector spaces of the same dimension: $\dim V = \dim W$.

Then the following are equivalent:

(1) ϕ is injective.

(2) ϕ is surjective.

(3) ϕ is an isomorphism.

Chapter 2

Sums and quotients

Convention. In this chapter, all vector spaces are over the same field $\mathbb{F}$ unless we say otherwise.

2.1 Sums of subspaces

Definition. Let $V_1, \dots, V_k \leq V$. The **sum** $V_1 + \dots + V_k$ is the set

$$V_1 + \dots + V_k := \{v_1 + \dots + v_k \mid v_i \in V_i, 1 \leq i \leq k\}.$$

Proposition 2.1.
Let $V_1, \dots, V_k \leq V$. Then

(1) $V_1 + \dots + V_k \leq V$.

(2) If $W \leq V$ and $V_1, \dots, V_k \leq W$ then $V_1, \dots, V_k \leq V_1 + \dots + V_k \leq W$.

2.2 Direct sums

Definition. Let $V_1, \dots, V_k \leq V$. The sum $V_1 + \dots + V_k$ is **direct** if each $v \in V_1 + \dots + V_k$ can be written

$$v = v_1 + \dots + v_k$$

in only one way, that is, for unique $v_i \in V_i$, $1 \leq i \leq k$.

In this case, we write $V_1 \oplus \dots \oplus V_k$ instead of $V_1 + \dots + V_k$.

Proposition 2.2.

Let $V_1, \dots, V_k \leq V$. Then $V_1 + \cdots + V_k$ is direct if and only if whenever $v_1 + \cdots + v_k = 0$, with $v_i \in V_i$, $1 \leq i \leq k$, then $v_i = 0$, for all $1 \leq i \leq k$.

Proposition 2.3.
Let $V_1, V_2 \leq V$. Then $V_1 + V_2$ is direct if and only if $V_1 \cap V_2 = \{0\}$.

Definition. Let $V_1, V_2 \leq V$. V is the **(internal) direct sum of** V_1 **and** V_2 if $V = V_1 \oplus V_2$.

In this case, say that V_2 is a **complement** of V_1 (and V_1 is a complement of V_2).

Proposition 2.4.
Let $V_1, \dots, V_k \leq V$, $k \geq 2$. Then the sum $V_1 + \cdots + V_k$ is direct if and only if, for each $1 \leq i \leq k$, $V_i \cap (\sum_{j \neq i} V_j) = \{0\}$.

2.2.1 Induction from two summands

Lemma 2.5.
Let $V_1, \dots, V_k \leq V$. Then $V_1 + \cdots + V_k$ is direct if and only if $V_1 + \cdots + V_{k-1}$ is direct and $(V_1 + \cdots + V_{k-1}) + V_k$ (two summands) is direct.

2.2.2 Direct sums, bases and dimension

Proposition 2.6.
Let $V_1, V_2 \leq V$ be subspaces with bases $\mathcal{B}_1 \colon v_1, \dots, v_k$ and $\mathcal{B}_2 \colon w_1, \dots, w_l$. Then $V_1 + V_2$ is direct if and only if the **concatenation**[1] $\mathcal{B}_1\mathcal{B}_2 \colon v_1, \dots, v_k, w_1, \dots, w_l$ is a basis of $V_1 + V_2$.

Corollary 2.7.
Let $V_1, \dots, V_k \leq V$ be finite-dimensional subspaces with $\mathcal{B}_i$ a basis of V_i, $1 \leq i \leq k$. Then $V_1 + \cdots + V_k$ is direct if and only if the concatenation $\mathcal{B}_1 \dots \mathcal{B}_k$ is a basis for $V_1 + \cdots + V_k$.

Corollary 2.8.
Let $V_1, \dots, V_k \leq V$ be subspaces of a finite-dimensional vector space V with $V_1 + \cdots + V_k$ direct. Then

$$\dim V_1 \oplus \cdots \oplus V_k = \dim V_1 + \cdots + \dim V_k.$$

[1]The concatenation of two lists is simply the list obtained by adjoining all entries in the second list to the first.

2.2.3 Complements

Proposition 2.9 (Complements exist)**.**
Let $U \leq V$, a finite-dimensional vector space. Then there is a complement to U.

2.3 Quotients

Definition. Let $U \leq V$. Say that $v, w \in V$ are **congruent modulo** U if $v - w \in U$. In this case, we write $v \equiv w \mod U$.

Lemma 2.10.
Congruence modulo U is an equivalence relation.

Definition. For $v \in V$, $U \leq V$, the set $v + U := \{v + u \mid u \in U\} \subseteq V$ is called a **coset of** U and v is called a **coset representative** of $v + U$.

Definition. Let $U \leq V$. The **quotient space** V/U **of** V **by** U is the set V/U, pronounced "V mod U", of cosets of U:

$$V/U := \{v + U \mid v \in V\}.$$

This is a subset of the **power set**[2] $\mathcal{P}(V)$ of V.

The **quotient map** $q : V \to V/U$ is defined by

$$q(v) = v + U.$$

Theorem 2.11.
Let $U \leq V$. Then, for $v, w \in V$, $\lambda \in \mathbb{F}$,

$$(v + U) + (w + U) := (v + w) + U$$
$$\lambda(v + U) := (\lambda v) + U$$

give well-defined operations of addition and scalar multiplication on V/U with respect to which V/U is a vector space and $q : V \to V/U$ is a linear map.

Moreover, $\ker q = U$ and $\operatorname{im} q = V/U$.

Corollary 2.12.
Let $U \leq V$. If V is finite-dimensional then so is V/U and

$$\dim V/U = \dim V - \dim U.$$

[2] Recall from Algebra 1A that the power set of a set A is the set of all subsets of A.

Theorem 2.13 (First Isomorphism Theorem)**.**
Let $\phi : V \to W$ be a linear map of vector spaces.

Then $V/\ker\phi \cong \operatorname{im}\phi$.

In fact, define $\bar{\phi} : V/\ker\phi \to \operatorname{im}\phi$ by

$$\bar{\phi}(q(v)) = \phi(v),$$

where $q : V \to V/\ker\phi$ is the quotient map.

Then $\bar{\phi}$ is a well-defined linear isomorphism.

Chapter 3

Polynomials, operators and matrices

3.1 Polynomials

Definitions. A **polynomial in a variable** x **with coefficients in a field** $\mathbb{F}$ is a formal expression

$$p = \sum_{k=0}^{\infty} a_k x^k$$

with **coefficients** $a_k \in \mathbb{F}$ such that only finitely many a_k are non-zero.

Two polynomials are equal if all their coefficients are equal.

The zero polynomial has all coefficients zero.

The **degree** of a polynomial p is $\deg p = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$. By convention, $\deg 0 = -\infty$.

The set of all polynomials in x with coefficients in $\mathbb{F}$ is denoted $\mathbb{F}[x]$.

Definition. A polynomial is **monic** if its leading coefficient is 1:

$$p = a_0 + \cdots + x^n.$$

Theorem 3.1 (Algebra 1A, Proposition 3.10)**.**
Let $p, q \in \mathbb{F}[x]$. Then there are unique $r, s \in \mathbb{F}[x]$ such that

$$p = sq + r$$

with $\deg r < \deg q$.

Theorem 3.2 (Fundamental Theorem of Algebra)**.**
Let $p \in \mathbb{C}[x]$ be a polynomial with $\deg p \geq 1$. Then p has a root. Thus there is $t \in \mathbb{C}$ with $p(t) = 0$.

Theorem 3.3.
Let $p \in \mathbb{C}[x]$ and $\lambda_1, \ldots, \lambda_k$ the distinct roots of p. Then

$$p = a \prod_{i=1}^{k} (x - \lambda_i)^{n_i},$$

for some $a \in \mathbb{C}$ and $n_i \in \mathbb{Z}_+$, $1 \leq i \leq k$.

n_i is called the **multiplicity** of the root λ_i.

3.2 Linear operators, matrices and polynomials

3.2.1 Linear operators and matrices

Definition. Let V be a vector space over $\mathbb{F}$. A **linear operator on** V is a linear map $\phi : V \to V$.

The vector space of linear operators on V is denoted $L(V)$ (instead of $L(V, V)$).

Notation. Write $M_n(\mathbb{F})$ for $M_{n\times n}(\mathbb{F})$.

Definition. Let V be a finite-dimensional vector space over $\mathbb{F}$ with basis $\mathcal{B} : v_1, \ldots, v_n$. Let $\phi \in L(V)$. The **matrix of** ϕ **with respect to** $\mathcal{B}$ is the matrix $A = (A_{ij}) \in M_n(\mathbb{F})$ defined by:

$$\phi(v_j) = \sum_{i=1}^{n} A_{ij} v_i, \tag{3.1}$$

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

3.2.2 Polynomials in linear operators and matrices

Notation. For $\phi, \psi \in L(V)$ write $\phi\psi$ for $\phi \circ \psi \in L(V)$.

Similarly, write ϕ^n for the n-fold composition of ϕ with itself:

$$\phi^n = \underbrace{\phi \circ \cdots \circ \phi}_{n \text{ times}}$$

and define $\phi^0 := \mathrm{id}_V$, $\phi^1 := \phi$.

Finally, for $A \in M_n(\mathbb{F})$, set $A^0 = I_n$, $A^1 = A$.

Definition. Let $p \in \mathbb{F}[x]$, $p = a_0 + \cdots + a_n x^n$, $\phi \in L(V)$ and $A \in M_n(\mathbb{F})$. Then $p(\phi) \in L(V)$ and $p(A) \in M_n(\mathbb{F})$ are given by:

$$p(\phi) := a_0 \operatorname{id}_V + a_1\phi + \cdots + a_n\phi^n = \sum_{k\in\mathbb{N}} a_k\phi^k,$$
$$p(A) := a_0 I_n + a_1 A + \cdots + a_n A^n = \sum_{k\in\mathbb{N}} a_k A^k.$$

Proposition 3.4.
For $p, q \in \mathbb{F}[x]$, $\phi \in L(V)$ and $A \in M_n(\mathbb{F})$,

$$(p+q)(\phi) = p(\phi) + q(\phi) \qquad (p+q)(A) = p(A) + q(A) \tag{3.2}$$
$$(pq)(\phi) = p(\phi)q(\phi) = q(\phi)p(\phi) \qquad (pq)(A) = p(A)q(A) = q(A)p(A). \tag{3.3}$$

3.3 The minimum polynomial

Proposition 3.5.
Let $A \in M_n(\mathbb{F})$. Then there is a monic polynomial $p \in \mathbb{F}[x]$ such that $p(A) = 0$.

Similarly, if $\phi \in L(V)$ is a linear operator on a finite-dimensional vector space over $\mathbb{F}$ then there is a monic polynomial $p \in \mathbb{F}[x]$ with $p(\phi) = 0$.

Definition. A **minimum polynomial** for $\phi \in L(V)$, V a vector space over $\mathbb{F}$ is a monic polynomial $p \in \mathbb{F}[x]$ of minimum degree with $p(\phi) = 0$: thus, if $r \in \mathbb{F}[x]$ has $r(\phi) = 0$ and $\deg r < \deg p$, then $r = 0$.

Similarly, a minimum polynomial for $A \in M_n(\mathbb{F})$ is a monic polynomial p of least degree with $p(A) = 0$.

Theorem 3.6.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over a field $\mathbb{F}$. Then ϕ has a unique minimum polynomial.

Similarly, any $A \in M_n(\mathbb{F})$ has a unique minimum polynomial.

We denote these by m_ϕ and m_A respectively.

Proposition 3.7.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over $\mathbb{F}$ and $p \in \mathbb{F}[x]$.

Then $p(\phi) = 0$ if and only if m_ϕ divides p, that is, there is $s \in \mathbb{F}[x]$ such that $p = sm_\phi$.

3.4 Eigenvalues and the characteristic polynomial

Definitions. Let V be a vector space over $\mathbb{F}$ and $\phi \in L(V)$.

An **eigenvalue** of ϕ is a scalar $\lambda \in \mathbb{F}$ such that there is a **non-zero** $v \in V$ with

$$\phi(v) = \lambda v.$$

Such a vector v is called an **eigenvector of ϕ with eigenvalue λ**.

The **λ-eigenspace $E_\phi(\lambda)$ of ϕ** is given by

$$E_\phi(\lambda) := \ker(\phi - \lambda \,\mathrm{id}_V) \leq V.$$

Definition. Let V be a finite-dimensional vector space over $\mathbb{F}$ and $\phi \in L(V)$.

The **characteristic polynomial Δ_ϕ of ϕ** is given by

$$\Delta_\phi(\lambda) := \det(\phi - \lambda \,\mathrm{id}_V) = \det(A - \lambda \mathrm{I}),$$

where A is the matrix of ϕ with respect to some (any!) basis of V.

Thus $\deg \Delta_\phi = \dim V$.

Lemma 3.8.
A scalar $\lambda \in \mathbb{F}$ is an eigenvalue of ϕ if and only if λ is a root of Δ_ϕ.

Definitions. Let $\phi \in L(V)$ be in a linear operator on a finite-dimensional vector space V over $\mathbb{F}$ and λ an eigenvalue of ϕ. Then

(1) The **algebraic multiplicity** of λ, $\mathrm{am}(\lambda) \in \mathbb{Z}_+$, is the multiplicity of λ as a root of Δ_ϕ.
(2) The **geometric multiplicity** of λ, $\mathrm{gm}(\lambda) \in \mathbb{Z}_+$, is $\dim E_\phi(\lambda)$.

Theorem 3.9.
Let ϕ be a linear operator on a finite-dimensional vector space V over $\mathbb{C}$. Then ϕ has an eigenvalue.

Proposition 3.10.
Let $\phi \in L(V)$ be a linear operator on a vector space over a field $\mathbb{F}$ and let $v \in V$ be an eigenvector of ϕ with eigenvalue λ:

$$\phi(v) = \lambda v. \tag{3.4}$$

Let $p \in \mathbb{F}[x]$. Then

$$p(\phi)(v) = p(\lambda)v,$$

so that v is an eigenvector of $p(\phi)$ also with eigenvalue $p(\lambda)$.

Corollary 3.11.
Let ϕ be a linear operator on a finite-dimensional vector space V over $\mathbb{F}$. Then any eigenvalue of ϕ is a root of m_ϕ.

3.5 The Cayley–Hamilton theorem

Theorem 3.12 (Cayley–Hamilton[1] Theorem)**.**
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over a field $\mathbb{F}$.

Then $\Delta_\phi(\phi) = 0$.

Equivalently, for any $A \in M_n(\mathbb{F})$, $\Delta_A(A) = 0$.

Corollary 3.13.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over a field $\mathbb{F}$.

(1) m_ϕ divides Δ_ϕ. Equivalently, m_A divides Δ_A, for any $A \in M_n(\mathbb{F})$.
(2) The roots of m_ϕ are exactly the eigenvalues of ϕ.

[1] Arthur Cayley, 1821–1895; William Rowan Hamilton, 1805–1865.

Chapter 4

The structure of linear operators

4.1 On normal forms

Definition. Matrices $A, B \in M_n(\mathbb{F})$ are **similar** if there is an invertible matrix $P \in M_n(\mathbb{F})$ such that

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

4.2 Invariant subspaces

Definition. Let ϕ be a linear operator on a vector space V. A subspace $U \subseteq V$ is ϕ-invariant if and only if $\phi(u) \in U$, for all $u \in U$.

Lemma 4.1.
Let $\phi, \psi \in L(V)$ be linear operators and suppose that $\phi\psi = \psi\phi$ (say that ϕ and ψ **commute**).

Then $\ker\psi$ and $\operatorname{im}\psi$ are ϕ-invariant.

Definition. Let $V_1, \ldots, V_k \leq V$ with $V = V_1 \oplus \cdots \oplus V_k$ and let $\phi_i \in L(V_i)$, for $1 \leq i \leq k$.

Define $\phi : V \to V$ by

$$\phi(v) = \phi_1(v_1) + \cdots + \phi_k(v_k),$$

where $v = v_1 + \cdots + v_k$ with $v_i \in V_i$, for $1 \leq i \leq k$.

Call ϕ the **direct sum of the** ϕ_i and write $\phi = \phi_1 \oplus \cdots \oplus \phi_k$.

Definition. Let $A_1, \ldots, A_k$ be square matrices with $A_i \in M_{n_i}(\mathbb{F})$. The **direct sum of the** A_i is

$$A_1 \oplus \cdots \oplus A_k := \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_k \end{pmatrix} \in M_n(\mathbb{F}),$$

where $n = n_1 + \cdots + n_k$.

A matrix of this type is said to be **block diagonal**.

Proposition 4.2.
Let $V_1, \ldots, V_k \leq V$ with $V = V_1 \oplus \cdots \oplus V_k$ and let $\phi_i \in L(V_i)$, for $1 \leq i \leq k$. Let $\phi = \phi_1 \oplus \cdots \oplus \phi_k$. Then

(1) ϕ is linear so that $\phi \in L(V)$.
(2) Each V_i is ϕ-invariant and $\phi_{|V_i} = \phi_i$, $1 \leq i \leq k$.
(3) Let $\mathcal{B}_i$ be a basis of V_i and ϕ_i have matrix A_i with respect to $\mathcal{B}_i$, $1 \leq i \leq k$. Then ϕ has matrix $A_1 \oplus \cdots \oplus A_k$ with respect to the concatenated basis $\mathcal{B} = \mathcal{B}_1 \ldots \mathcal{B}_k$.

Proposition 4.3.
Let $V_1, \ldots, V_k \leq V$ with $V = V_1 \oplus \cdots \oplus V_k$ and let $\phi \in L(V)$. Suppose that each V_i is ϕ-invariant.

Then $\phi = \phi_1 \oplus \cdots \oplus \phi_k$ where $\phi_i := \phi_{|V_i} \in L(V_i)$.

Proposition 4.4.
Let $V_1, \ldots, V_k \leq V$ with $V = V_1 \oplus \cdots \oplus V_k$, $\phi_i \in L(V_i)$, $1 \leq i \leq k$ and $\phi = \phi_1 \oplus \cdots \oplus \phi_k$.

Then:

(1) $\ker \phi = \ker \phi_1 \oplus \cdots \oplus \ker \phi_k$.
(2) $\operatorname{im} \phi = \operatorname{im} \phi_1 \oplus \cdots \oplus \operatorname{im} \phi_k$.
(3) $p(\phi) = p(\phi_1) \oplus \cdots \oplus p(\phi_k)$, for any $p \in \mathbb{F}[x]$.
(4) $\Delta_\phi = \prod_{i=1}^k \Delta_{\phi_i}$.

Proposition 4.5.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over a field $\mathbb{F}$ and let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of ϕ.

Then ϕ is diagonalisable if and only if

$$V = \bigoplus_{i=1}^k E_\phi(\lambda_i). \tag{4.1}$$

4.3 Jordan decomposition

4.3.1 Powers of operators and Fitting's Lemma

Proposition 4.6 (Increasing kernels, decreasing images)**.**
Let V be a vector space over a field $\mathbb{F}$ and $\phi \in L(V)$. Then

(1) $\ker \phi^k \leq \ker \phi^{k+1}$, for all $k \in \mathbb{N}$. That is,

$$\{0\} = \ker \phi^0 \leq \ker \phi \leq \ker \phi^2 \leq \dots.$$

If $\ker \phi^k = \ker \phi^{k+1}$ then $\ker \phi^k = \ker \phi^{k+n}$, for all $n \in \mathbb{N}$.

(2) $\operatorname{im} \phi^k \geq \operatorname{im} \phi^{k+1}$, for all $k \in \mathbb{N}$. That is,

$$V = \operatorname{im} \phi^0 \geq \operatorname{im} \phi \geq \operatorname{im} \phi^2 \geq \dots.$$

If $\operatorname{im} \phi^k = \operatorname{im} \phi^{k+1}$ then $\operatorname{im} \phi^k = \operatorname{im} \phi^{k+n}$, for all $n \in \mathbb{N}$.

Corollary 4.7.
Let V be finite-dimensional with $\dim V = n$ and $\phi \in L(V)$. Then, for all $k \in \mathbb{N}$,

$$\ker \phi^n = \ker \phi^{n+k}$$
$$\operatorname{im} \phi^n = \operatorname{im} \phi^{n+k}.$$

Theorem 4.8 (Fitting[1]'s Lemma)**.**
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over a field $\mathbb{F}$. Then, with $n = \dim V$, we have

$$V = \ker \phi^n \oplus \operatorname{im} \phi^n.$$

4.3.2 Generalised eigenspaces

Definition. Let $\phi \in L(V)$ be a linear operator on an n-dimensional vector space over a field $\mathbb{F}$. A **generalised eigenvector of** ϕ **with eigenvalue** λ is a non-zero $v \in V$ such that

$$(\phi - \lambda \operatorname{id})^n (v) = 0. \tag{4.2}$$

The set of all such along with 0 is called the **generalised eigenspace of** ϕ **with eigenvalue** λ and denoted $G_\phi(\lambda)$. Thus

$$G_\phi(\lambda) = \ker(\phi - \lambda \operatorname{id}_V)^n \leq V.$$

Lemma 4.9.
$E_\phi(\lambda) \leq G_\phi(\lambda) \leq V$ and $G_\phi(\lambda)$ is ϕ-invariant.

[1]Hans Fitting, 1906–1938.

Lemma 4.10.
Let $\phi \in L(V)$ be a linear operator on an n-dimensional vector space over $\mathbb{F}$ and $\lambda_1, \lambda_2 \in \mathbb{F}$ distinct eigenvalues of ϕ. Then $G_\phi(\lambda_1) \cap G_\phi(\lambda_2) = \{0\}$.

Theorem 4.11 (Jordan[2] decomposition)**.**
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over $\mathbb{C}$ with distinct eigenvalues $\lambda_1, \dots, \lambda_k$. Then

$$V = \bigoplus_{i=1}^{k} G_\phi(\lambda_i).$$

Definition. A linear operator ϕ on a vector space V is **nilpotent** if $\phi^k = 0$, for some $k \in \mathbb{N}$. or, equivalently, if $\ker \phi^k = V$.

Proposition 4.12.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space V over $\mathbb{F}$.

Then ϕ is nilpotent if and only if there is a basis with respect to which ϕ has a strictly upper triangular matrix A (thus $A_{ij} = 0$ whenever $i \geq j$):

$$A = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}.$$

Proposition 4.13.
Let $\lambda \in \mathbb{C}$ be an eigenvalue of a linear operator ϕ on a complex finite-dimensional vector space. Then

$$\operatorname{am}(\lambda) = \dim G_\phi(\lambda).$$

Proposition 4.14.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space over $\mathbb{C}$ with distinct eigenvalues $\lambda_1, \dots, \lambda_k$. Set $\phi_i = \phi_{|G_\phi(\lambda_i)}$. Then

(1) Each $m_{\phi_i} = (x - \lambda_i)^{s_i}$, for some $s_i \leq \dim G_\phi(\lambda_i)$.
(2) $m_\phi = \prod_{i=1}^{k} m_{\phi_i} = \prod_{i=1}^{k} (x - \lambda_i)^{s_i}$.

Corollary 4.15.
Let $\phi \in L(V)$ be a linear operator with minimum polynomial $\prod_{i=1}^{k} (x - \lambda_i)^{s_i}$. Then

$$G_\phi(\lambda_i) = \ker(\phi - \lambda_i \operatorname{id}_V)^{s_i}.$$

[2] Camille Jordan, 1838–1922.

4.4 Jordan normal form

4.4.1 Jordan blocks

Definition. The **Jordan block of size** $n \in \mathbb{Z}_+$ **and eigenvalue** $\lambda \in \mathbb{F}$ is $J(\lambda, n) \in M_n(\mathbb{F})$ with λ's on the diagonal, 1's on the super-diagonal and zeros elsewhere. Thus

$$J(\lambda, n) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}$$

Notation. Set $J_n := J(0, n)$ so that $J(\lambda, n) = \lambda I_n + J_n$.

Lemma 4.16.
Let $v_1, \dots, v_n$ be a basis for a vector space V and $\phi \in L(V)$.

Then the following are equivalent:

(1) ϕ has matrix J_n with respect to $v_1, \dots, v_n$.
(2) $\phi(v_1) = 0$ and $\phi(v_i) = v_{i-1}$, for $2 \leq i \leq n$.
(3) $v_i = \phi^{n-i}(v_n)$, $0 \leq i \leq n-1$ and $\phi^n(v_n) = 0$.

Theorem 4.17.
Let $\phi \in L(V)$ be a nilpotent operator on a finite-dimensional vector space over $\mathbb{F}$. Then there are $v_1, \dots, v_k \in V$ and $n_1, \dots, n_k \in \mathbb{Z}_+$ such that

$$\phi^{n_1 - 1}(v_1), \dots, \phi(v_1), v_1, \dots, \phi^{n_k - 1}(v_k), \dots, \phi(v_k), v_k$$

is a basis of V and $\phi^{n_i}(v_i) = 0$, for $1 \leq i \leq k$.

Corollary 4.18.
Let $\phi \in L(V)$ be a nilpotent operator on a finite-dimensional vector space over $\mathbb{F}$. Then there is a basis for which ϕ has matrix $J_{n_1} \oplus \cdots \oplus J_{n_k}$.

Proposition 4.19.
Let $\phi \in L(V)$ be nilpotent with matrix $J_{n_1} \oplus \cdots \oplus J_{n_k}$ for some basis of V. Then $n_1, \dots, n_k$ are unique up to order. Indeed,

$$\#\{i \mid n_i \geq s\} = \dim \ker \phi^s - \dim \ker \phi^{s-1},$$

for each $s \geq 1$.

Proposition 4.20.
In the situation of Proposition 4.19, we have

$$m_\phi = x^s,$$

where $s = \max\{n_1, \ldots, n_k\}$.

4.4.2 Jordan normal form

Theorem 4.21.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space V over $\mathbb{C}$. Then there is a basis of V for which ϕ has as matrix a direct sum of Jordan blocks which are unique up to order.

Such a basis is called a **Jordan basis** and the direct sum of Jordan blocks is called the **Jordan normal form (JNF) of** ϕ.

Corollary 4.22.
Let $\phi \in L(V)$ be a linear operator on a finite-dimensional vector space V over $\mathbb{C}$ with distinct eigenvalues $\lambda_1, \ldots, \lambda_k$. Then

$$m_\phi = \prod_{i=1}^{k} (x - \lambda_i)^{s_i}$$

where s_i is the size of the largest Jordan block of ϕ with eigenvalue λ_i.

Corollary 4.23.
Any $A \in M_n(\mathbb{C})$ is similar to a direct sum of Jordan blocks, that is, there is an invertible matrix $P \in M_n(\mathbb{C})$ such that

$$P^{-1}AP = A_1 \oplus \cdots \oplus A_r,$$

with each A_i a Jordan block.

$A_1 \oplus \cdots \oplus A_r$ is called the **Jordan normal form (JNF) of** A and is unique up to the order of the A_i.

Theorem 4.24.
Matrices $A, B \in M_n(\mathbb{C})$ are similar if and only if they have the same Jordan normal form, up to reordering the Jordan blocks.

Chapter 5

Symmetric bilinear forms and quadratic forms

5.1 Bilinear forms and matrices

Definition. Let V be a vector space over a field $\mathbb{F}$. A map $B : V \times V \to \mathbb{F}$ is **bilinear** if it is linear in each slot separately:

$$B(\lambda v_1 + v_2, v) = \lambda B(v_1, v) + B(v_2, v)$$
$$B(v, \lambda v_1 + v_2) = \lambda B(v, v_1) + B(v, v_2),$$

for all $v, v_1, v_2 \in V$, $v, v_1, v_2 \in V$ and $\lambda \in \mathbb{F}$.

A bilinear map $V \times V \to \mathbb{F}$ is called a **bilinear form on** V.

Definition. Let V be a vector space over $\mathbb{F}$ with basis $\mathcal{B} = v_1, \ldots, v_n$ and let $B : V \times V \to \mathbb{F}$ be a bilinear form. The **matrix of** B **with respect to** $\mathcal{B}$ is $A \in M_n(\mathbb{F})$ given by

$$A_{ij} = B(v_i, v_j),$$

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

Proposition 5.1.
Let $B : V \times V \to \mathbb{F}$ be a bilinear form with matrix A with respect to $\mathcal{B} = v_1, \ldots, v_n$. Then B is completely determined by A: if $v = \sum_{i=1}^{n} x_i v_i$ and $w = \sum_{j=1}^{n} y_j v_j$ then

$$B(v, w) = \sum_{i,j=1}^{n} x_i y_j A_{ij} = \mathbf{x}^T A \mathbf{y}.$$

Proposition 5.2.
Let $B : V \times V \to \mathbb{F}$ be a bilinear form with matrices A and A' with respect to bases

$\mathcal{B} : v_1, \dots, v_n$ and $\mathcal{B}' : v'_1, \dots, v'_n$ of V. Then

$$A' = P^T AP$$

where P is the change of basis matrix[1] from $\mathcal{B}$ to $\mathcal{B}'$: thus $v'_j = \sum_{i=1}^n P_{ij} v_i$, for $1 \leq j \leq n$.

Definition. We say that matrices $A, B \in M_n(\mathbb{F})$ are **congruent** if there is $P \in \mathrm{GL}(n, \mathbb{F})$ such that

$$B = P^T AP.$$

5.2 Symmetric bilinear forms

Definition. A bilinear form $B : V \times V \to \mathbb{F}$ is **symmetric** if, for all $v, w \in V$,

$$B(v, w) = B(w, v)$$

5.2.1 Rank and radical

Definitions. Let $B : V \times V \to \mathbb{F}$ be a symmetric bilinear form.

The **radical** $\mathrm{rad}\, B$ **of** B is given by

$$\mathrm{rad}\, B := \{v \in V \mid B(v, w) = 0, \text{ for all } w \in V\}.$$

We shall shortly see that $\mathrm{rad}\, B \leq V$.

We say that B is **non-degenerate** if $\mathrm{rad}\, B = \{0\}$.

If V is finite-dimensional, the **rank** of B is $\dim V - \dim \mathrm{rad}\, B$ (so that B is non-degenerate if and only if $\mathrm{rank}\, B = \dim V$).

Lemma 5.3.
Let $B : V \times V \to \mathbb{F}$ be a symmetric bilinear form with matrix A with respect to a basis $v_1, \dots, v_n$. Then $v = \sum_{i=1}^n x_i v_i \in \mathrm{rad}\, B$ if and only if $A\mathbf{x} = 0$ if and only if $\mathbf{x}^T A = 0$.

Corollary 5.4.
Let $B : V \times V \to \mathbb{F}$ be a symmetric bilinear form on a finite-dimensional vector space V with matrix A with respect to some basis of V. Then

$$\mathrm{rank}\, B = \mathrm{rank}\, A.$$

In particular, B is non-degenerate if and only if $\det A \neq 0$.

[1] Algebra 1B, Definition 1.6.1.

5.2.2 Classification of symmetric bilinear forms

Convention. In this section, we work with a field $\mathbb{F}$ where $1+1 \neq 0$ so that $\frac{1}{2} = (1+1)^{-1}$ makes sense. This excludes, for example, the 2-element field $\mathbb{Z}_2$.

Lemma 5.5.
Let $B : V \times V \to \mathbb{F}$ be a symmetric bilinear form such that $B(v, v) = 0$, for all $v \in V$. Then $B \equiv 0$.

Theorem 5.6 (Diagonalisation Theorem)**.**
Let B be a symmetric bilinear form on a finite-dimensional vector space over $\mathbb{F}$. Then there is a basis $v_1, \dots, v_n$ of V with respect to which the matrix of B is diagonal:

$$B(v_i, v_j) = 0,$$

for all $1 \leq i \neq j \leq n$. We call $v_1, \dots, v_n$ a **diagonalising basis** for B.

Corollary 5.7.
Let $A \in M_{n \times n}(\mathbb{F})$ be symmetric. Then there is an invertible matrix $P \in \mathrm{GL}(n, \mathbb{F})$ such that $P^T AP$ is diagonal.

5.2.3 Sylvester's Theorem

Definitions. Let B be a symmetric bilinear form on a **real** vector space V.

Say that B is **positive definite** if $B(v, v) > 0$, for all $v \in V \setminus \{0\}$.

Say that B is **negative definite** if $-B$ is positive definite.

If V is finite-dimensional, the **signature** of B is the pair (p, q) where

$$p = \max\{\dim U \mid U \leq V \text{ with } B_{|U \times U} \text{ positive definite}\}$$
$$q = \max\{\dim W \mid W \leq V \text{ with } B_{|W \times W} \text{ negative definite}\}.$$

Theorem 5.8 (Sylvester's Law of Inertia)**.**
Let B be a symmetric bilinear form of signature (p, q) on a finite-dimensional real vector space Then:

- $p + q = \operatorname{rank} B$;
- any **diagonal** matrix representing B has p positive entries and q negative entries (necessarily on the diagonal!).

5.3 Application: Quadratic forms

Convention. We continue working with a field $\mathbb{F}$ where $1+1 \neq 0$.

Definition. A **quadratic form** on a vector space V over $\mathbb{F}$ is a function $Q : V \to \mathbb{F}$ of the form

$$Q(v) = B(v, v),$$

for all $v \in V$, where $B : V \times V \to \mathbb{F}$ is a symmetric bilinear form.

Lemma 5.9.
Let $Q : V \to \mathbb{F}$ be a quadratic form with $Q(v) = B(v, v)$ for a symmetric bilinear form B. Then

$$B(v, w) = \tfrac{1}{2}\big(Q(v+w) - Q(v) - Q(w)\big),$$

for all $v, w \in V$.

B is called the **polarisation of** Q.

Definitions. Let Q be a quadratic form on a finite-dimensional vector space V over $\mathbb{F}$.

The **rank** of Q is the rank of its polarisation.

If $\mathbb{F} = \mathbb{R}$, the **signature** of Q is the signature of its polarisation.

Theorem 5.10.
Let Q be a quadratic form with rank r polarisation on a finite-dimensional vector space over $\mathbb{F}$.

(1) When $\mathbb{F} = \mathbb{C}$, there is a basis $v_1, \dots, v_n$ of V such that

$$Q(\sum_{i=1}^{n} x_i v_i) = x_1^2 + \cdots + x_r^2.$$

(2) When $\mathbb{F} = \mathbb{R}$ and Q has signature (p, q), there is a basis $v_1, \dots, v_n$ of V such that

$$Q(\sum_{i=1}^{n} x_i v_i) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2.$$