Part IB — Linear Algebra
Theorems

Based on lectures by S. J. Wadsley
Notes taken by Dexter Chua

Michaelmas 2015

Definition of a vector space (over $\mathbb{R}$ or $\mathbb{C}$), subspaces, the space spanned by a subset. Linear independence, bases, dimension. Direct sums and complementary subspaces. [3]

Linear maps, isomorphisms. Relation between rank and nullity. The space of linear maps from U to V, representation by matrices. Change of basis. Row rank and column rank. [4]

Determinant and trace of a square matrix. Determinant of a product of two matrices and of the inverse matrix. Determinant of an endomorphism. The adjugate matrix. [3]

Eigenvalues and eigenvectors. Diagonal and triangular forms. Characteristic and minimal polynomials. Cayley-Hamilton Theorem over $\mathbb{C}$. Algebraic and geometric multiplicity of eigenvalues. Statement and illustration of Jordan normal form. [4]

Dual of a finite-dimensional vector space, dual bases and maps. Matrix representation, rank and determinant of dual map. [2]

Bilinear forms. Matrix representation, change of basis. Symmetric forms and their link with quadratic forms. Diagonalisation of quadratic forms. Law of inertia, classification by rank and signature. Complex Hermitian forms. [4]

Inner product spaces, orthonormal sets, orthogonal projection, $V = W \oplus W^{\perp}$. Gram-Schmidt orthogonalisation. Adjoints. Diagonalisation of Hermitian matrices. Orthogonality of eigenvectors and properties of eigenvalues. [4]

Contents

0 Introduction **3**

1 Vector spaces **4**
- 1.1 Definitions and examples . . . 4
- 1.2 Linear independence, bases and the Steinitz exchange lemma . . . 4
- 1.3 Direct sums . . . 5

2 Linear maps **6**
- 2.1 Definitions and examples . . . 6
- 2.2 Linear maps and matrices . . . 6
- 2.3 The first isomorphism theorem and the rank-nullity theorem . . . 6
- 2.4 Change of basis . . . 7
- 2.5 Elementary matrix operations . . . 8

3 Duality **9**
- 3.1 Dual space . . . 9
- 3.2 Dual maps . . . 9

4 Bilinear forms I **11**

5 Determinants of matrices **12**

6 Endomorphisms **14**
- 6.1 Invariants . . . 14
- 6.2 The minimal polynomial . . . 14
  - 6.2.1 Aside on polynomials . . . 14
  - 6.2.2 Minimal polynomial . . . 15
- 6.3 The Cayley-Hamilton theorem . . . 15
- 6.4 Multiplicities of eigenvalues and Jordan normal form . . . 16

7 Bilinear forms II **17**
- 7.1 Symmetric bilinear forms and quadratic forms . . . 17
- 7.2 Hermitian form . . . 18

8 Inner product spaces **19**
- 8.1 Definitions and basic properties . . . 19
- 8.2 Gram-Schmidt orthogonalization . . . 19
- 8.3 Adjoints, orthogonal and unitary maps . . . 20
- 8.4 Spectral theory . . . 20

0 Introduction

1 Vector spaces

1.1 Definitions and examples

Proposition. In any vector space V, $0\mathbf{v} = \mathbf{0}$ for all $\mathbf{v} \in V$, and $(-1)\mathbf{v} = -\mathbf{v}$, where $-\mathbf{v}$ is the additive inverse of $\mathbf{v}$.

Proposition. Let U, W be subspaces of V. Then $U + W$ and $U \cap W$ are subspaces.

1.2 Linear independence, bases and the Steinitz exchange lemma

Lemma. $S \subseteq V$ is linearly dependent if and only if there are distinct $\mathbf{s}_0, \cdots, \mathbf{s}_n \in S$ and $\lambda_1, \cdots, \lambda_n \in \mathbb{F}$ such that

$$\sum_{i=1}^{n} \lambda_i \mathbf{s}_i = \mathbf{s}_0.$$

Proposition. If $S = \{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ is a subset of V over $\mathbb{F}$, then it is a basis if and only if every $\mathbf{v} \in V$ can be written uniquely as a finite linear combination of elements in S, i.e. as

$$\mathbf{v} = \sum_{i=1}^{n} \lambda_i \mathbf{e}_i.$$

Theorem (Steinitz exchange lemma)**.** Let V be a vector space over $\mathbb{F}$, and $S = \{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ a finite linearly independent subset of V, and T a spanning subset of V. Then there is some $T' \subseteq T$ of order n such that $(T \setminus T') \cup S$ still spans V. In particular, $|T| \geq n$.

Corollary. Let $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ be a linearly independent subset of V, and suppose $\{\mathbf{f}_1, \cdots, \mathbf{f}_m\}$ spans V. Then there is a re-ordering of the $\{\mathbf{f}_i\}$ such that $\{\mathbf{e}_1, \cdots, \mathbf{e}_n, \mathbf{f}_{n+1}, \cdots, \mathbf{f}_m\}$ spans V.

Corollary. Suppose V is a vector space over $\mathbb{F}$ with a basis of order n. Then

(i) Every basis of V has order n.

(ii) Any linearly independent set of order n is a basis.

(iii) Every spanning set of order n is a basis.

(iv) Every finite spanning set contains a basis.

(v) Every linearly independent subset of V can be extended to basis.

Lemma. If V is a finite dimensional vector space over $\mathbb{F}$, $U \subseteq V$ is a proper subspace, then U is finite dimensional and $\dim U < \dim V$.

Proposition. If U, W are subspaces of a finite dimensional vector space V, then

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

Proposition. If V is a finite dimensional vector space over $\mathbb{F}$ and $U \cup V$ is a subspace, then

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

1.3 Direct sums

2 Linear maps

2.1 Definitions and examples

Lemma. If U and V are vector spaces over $\mathbb{F}$ and $\alpha : U \to V$, then α is an isomorphism iff α is a bijective linear map.

Proposition. Let $\alpha : U \to V$ be an $\mathbb{F}$-linear map. Then

(i) If α is injective and $S \subseteq U$ is linearly independent, then $\alpha(S)$ is linearly independent in V.

(ii) If α is surjective and $S \subseteq U$ spans U, then $\alpha(S)$ spans V.

(iii) If α is an isomorphism and $S \subseteq U$ is a basis, then $\alpha(S)$ is a basis for V.

Corollary. If U and V are finite-dimensional vector spaces over $\mathbb{F}$ and $\alpha : U \to V$ is an isomorphism, then $\dim U = \dim V$.

Proposition. Suppose V is a $\mathbb{F}$-vector space of dimension $n < \infty$. Then writing $\mathbf{e}_1, \cdots, \mathbf{e}_n$ for the standard basis of $\mathbb{F}^n$, there is a bijection

$$\Phi : \{\text{isomorphisms } \mathbb{F}^n \to V\} \to \{\text{(ordered) basis}(\mathbf{v}_1, \cdots, \mathbf{v}_n) \text{ for } V\},$$

defined by

$$\alpha \mapsto (\alpha(\mathbf{e}_1), \cdots, \alpha(\mathbf{e}_n)).$$

2.2 Linear maps and matrices

Proposition. Suppose U, V are vector spaces over $\mathbb{F}$ and $S = \{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ is a basis for U. Then every function $f : S \to V$ extends uniquely to a linear map $U \to V$.

Corollary. If U and V are finite-dimensional vector spaces over $\mathbb{F}$ with bases $(\mathbf{e}_1, \cdots, \mathbf{e}_m)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ respectively, then there is a bijection

$$\mathrm{Mat}_{n,m}(\mathbb{F}) \to \mathcal{L}(U, V),$$

sending A to the unique linear map α such that $\alpha(\mathbf{e}_i) = \sum a_{ji}\mathbf{f}_j$.

Proposition. Suppose U, V, W are finite-dimensional vector spaces over $\mathbb{F}$ with bases $R = (\mathbf{u}_1, \cdots, \mathbf{u}_r)$, $S = (\mathbf{v}_1, .., \mathbf{v}_s)$ and $T = (\mathbf{w}_1, \cdots, \mathbf{w}_t)$ respectively.

If $\alpha : U \to V$ and $\beta : V \to W$ are linear maps represented by A and B respectively (with respect to R, S and T), then $\beta\alpha$ is linear and represented by BA with respect to R and T.

2.3 The first isomorphism theorem and the rank-nullity theorem

Theorem (First isomorphism theorem)**.** Let $\alpha : U \to V$ be a linear map. Then $\ker \alpha$ and $\operatorname{im} \alpha$ are subspaces of U and V respectively. Moreover, α induces an isomorphism

$$\begin{aligned} \bar{\alpha} : U/\ker \alpha &\to \operatorname{im} \alpha \\ (\mathbf{u} + \ker \alpha) &\mapsto \alpha(\mathbf{u}) \end{aligned}$$

Corollary (Rank-nullity theorem)**.** If $\alpha : U \to V$ is a linear map and U is finite-dimensional, then
$$r(\alpha) + n(\alpha) = \dim U.$$

Proposition. If $\alpha : U \to V$ is a linear map between finite-dimensional vector spaces over $\mathbb{F}$, then there are bases $(\mathbf{e}_1, \cdots, \mathbf{e}_m)$ for U and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ for V such that α is represented by the matrix
$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$
where $r = r(\alpha)$ and I_r is the $r \times r$ identity matrix.

In particular, $r(\alpha) + n(\alpha) = \dim U$.

Corollary. Suppose $\alpha : U \to V$ is a linear map between vector spaces over $\mathbb{F}$ both of dimension $n < \infty$. Then the following are equivalent

(i) α is injective;

(ii) α is surjective;

(iii) α is an isomorphism.

Lemma. Let $A \in M_{n,n}(\mathbb{F}) = M_n(\mathbb{F})$ be a square matrix. The following are equivalent

(i) There exists $B \in M_n(\mathbb{F})$ such that $BA = I_n$.

(ii) There exists $C \in M_n(\mathbb{F})$ such that $AC = I_n$.

If these hold, then $B = C$. We call A *invertible* or *non-singular*, and write $A^{-1} = B = C$.

2.4 Change of basis

Theorem. Suppose that $(\mathbf{e}_1, \cdots, \mathbf{e}_m)$ and $(\mathbf{u}_1, \cdots, \mathbf{u}_m)$ are basis for a finite-dimensional vector space U over $\mathbb{F}$, and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ and $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ are basis of a finite-dimensional vector space V over $\mathbb{F}$.

Let $\alpha : U \to V$ be a linear map represented by a matrix A with respect to $(\mathbf{e}_i)$ and $(\mathbf{f}_i)$ and by B with respect to $(\mathbf{u}_i)$ and $(\mathbf{v}_i)$. Then
$$B = Q^{-1}AP,$$
where P and Q are given by
$$\mathbf{u}_i = \sum_{k=1}^m P_{ki}\mathbf{e}_k, \quad \mathbf{v}_i = \sum_{k=1}^n Q_{ki}\mathbf{f}_k.$$

Corollary. If $A \in \mathrm{Mat}_{n,m}(\mathbb{F})$, then there exists invertible matrices $P \in \mathrm{GL}_m(\mathbb{F}), Q \in \mathrm{GL}_n(\mathbb{F})$ so that
$$Q^{-1}AP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$
for some $0 \leq r \leq \min(m, n)$.

Theorem. If $A \in \mathrm{Mat}_{n,m}(\mathbb{F})$, then $r(A) = r(A^T)$, i.e. the row rank is equivalent to the column rank.

2.5 Elementary matrix operations

Proposition. If $A \in \mathrm{Mat}_{n,m}(\mathbb{F})$, then there exists invertible matrices $P \in \mathrm{GL}_m(\mathbb{F}), Q \in \mathrm{GL}_n(\mathbb{F})$ so that

$$Q^{-1}AP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

for some $0 \leq r \leq \min(m, n)$.

3 Duality

3.1 Dual space

Lemma. If V is a finite-dimensional vector space over f with basis $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$, then there is a basis $(\varepsilon_1, \cdots, \varepsilon_n)$ for V^* (called the *dual basis* to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$) such that
$$\varepsilon_i(\mathbf{e}_j) = \delta_{ij}.$$

Corollary. If V is finite dimensional, then $\dim V = \dim V^*$.

Proposition. Let V be a finite-dimensional vector space over $\mathbb{F}$ with bases $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$, and that P is the change of basis matrix so that
$$\mathbf{f}_i = \sum_{k=1}^n P_{ki}\mathbf{e}_k.$$
Let $(\varepsilon_1, \cdots, \varepsilon_n)$ and $(\eta_1, \cdots, \eta_n)$ be the corresponding dual bases so that
$$\varepsilon_i(\mathbf{e}_j) = \delta_{ij} = \eta_i(\mathbf{f}_j).$$
Then the change of basis matrix from $(\varepsilon_1, \cdots, \varepsilon_n)$ to $(\eta_1, \cdots, \eta_n)$ is $(P^{-1})^T$, i.e.
$$\varepsilon_i = \sum_{\ell=1}^n P_{\ell i}^T \eta_\ell.$$

Proposition. Let V be a vector space over $\mathbb{F}$ and U a subspace. Then
$$\dim U + \dim U^0 = \dim V.$$

3.2 Dual maps

Proposition. Let $\alpha \in \mathcal{L}(V, W)$ be a linear map. Then $\alpha^* \in \mathcal{L}(W^*, V^*)$ is a linear map.

Proposition. Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ and $\alpha : V \to W$ be a linear map. Let $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ be a basis for V and $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$ be a basis for W; $(\varepsilon_1, \cdots, \varepsilon_n)$ and $(\eta_1, \cdots, \eta_m)$ the corresponding dual bases.

Suppose α is represented by A with respect to $(\mathbf{e}_i)$ and $(\mathbf{f}_i)$ for V and W. Then α^* is represented by A^T with respect to the corresponding dual bases.

Lemma. Let $\alpha \in \mathcal{L}(V, W)$ with V, W finite dimensional vector spaces over $\mathbb{F}$. Then

(i) $\ker \alpha^* = (\operatorname{im} \alpha)^0$.

(ii) $r(\alpha) = r(\alpha^*)$ (which is another proof that row rank is equal to column rank).

(iii) $\operatorname{im} \alpha^* = (\ker \alpha)^0$.

Lemma. Let V be a vector space over $\mathbb{F}$. Then there is a linear map $\mathrm{ev} : V \to (V^*)^*$ given by
$$\mathrm{ev}(\mathbf{v})(\theta) = \theta(\mathbf{v}).$$
We call this the *evaluation* map.

Lemma. If V is finite-dimensional, then $\text{ev} : V \to V^{**}$ is an isomorphism.

Lemma. Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ after identifying (V and V^{**}) and (W and W^{**}) by the evaluation map. Then we have

(i) If $U \leq V$, then $U^{00} = U$.

(ii) If $\alpha \in \mathcal{L}(V, W)$, then $\alpha^{**} = \alpha$.

Proposition. Let V be a finite-dimensional vector space $\mathbb{F}$ and U_1, U_2 are subspaces of V. Then we have

(i) $(U_1 + U_2)^0 = U_1^0 \cap U_2^0$

(ii) $(U_1 \cap U_2)^0 = U_1^0 + U_2^0$

4 Bilinear forms I

Proposition. Suppose $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ are basis for V such that

$$\mathbf{v}_i = \sum P_{ki}\mathbf{e}_k \text{ for all } i = 1, \cdots, n;$$

and $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$ and $(\mathbf{w}_1, \cdots, \mathbf{w}_m)$ are bases for W such that

$$\mathbf{w}_i = \sum Q_{\ell j}\mathbf{f}_\ell \text{ for all } j = 1, \cdots, m.$$

Let $\psi : V \times W \to \mathbb{F}$ be a bilinear form represented by A with respect to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$, and by B with respect to the bases $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ and $(\mathbf{w}_1, \cdots, \mathbf{w}_m)$. Then

$$B = P^T AQ.$$

Lemma. Let $(\varepsilon_1, \cdots, \varepsilon_n)$ be a basis for V^* dual to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ of V; $(\eta_1, \cdots, \eta_n)$ be a basis for W^* dual to $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ of W.

If A represents ψ with respect to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$, then A also represents ψ_R with respect to $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$ and $(\varepsilon_1, \cdots, \varepsilon_n)$; and A^T represents ψ_L with respect to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\eta_1, \cdots, \eta_m)$.

Lemma. Let V and W be finite-dimensional vector spaces over $\mathbb{F}$ with bases $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_m)$ be their basis respectively.

Let $\psi : V \times W \to \mathbb{F}$ be a bilinear form represented by A with respect to these bases. Then ϕ is non-degenerate if and only if A is (square and) invertible. In particular, V and W have the same dimension.

5 Determinants of matrices

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

Lemma. If A is an upper triangular matrix, i.e.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

Then

$$\det A = \prod_{i=1}^n a_{ii}.$$

Lemma. $\det A$ is a volume form.

Lemma. Let d be a volume form on $\mathbb{F}^n$. Then swapping two entries changes the sign, i.e.

$$d(\mathbf{v}_1, \cdots, \mathbf{v}_i, \cdots, \mathbf{v}_j, \cdots, \mathbf{v}_n) = -d(\mathbf{v}_1, \cdots, \mathbf{v}_j, \cdots, \mathbf{v}_i, \cdots, \mathbf{v}_n).$$

Corollary. If $\sigma \in S_n$, then

$$d(\mathbf{v}_{\sigma(1)}, \cdots, \mathbf{v}_{\sigma(n)}) = \varepsilon(\sigma) d(\mathbf{v}_1, \cdots, \mathbf{v}_n)$$

for any $\mathbf{v}_i \in \mathbb{F}^n$.

Theorem. Let d be any volume form on $\mathbb{F}^n$, and let $A = (A^{(1)} \ \cdots \ A^{(n)}) \in \mathrm{Mat}_n(\mathbb{F})$. Then

$$d(A^{(1)}, \cdots, A^{(n)}) = (\det A) d(\mathbf{e}_1, \cdots, \mathbf{e}_n),$$

where $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ is the standard basis.

Theorem. Let $A, B \in \mathrm{Mat}_n(\mathbb{F})$. Then $\det(AB) = \det(A)\det(B)$.

Corollary. If $A \in \mathrm{Mat}_n(\mathbb{F})$ is invertible, then $\det A \neq 0$. In fact, when A is invertible, then $\det(A^{-1}) = (\det A)^{-1}$.

Theorem. Let $A \in \mathrm{Mat}_n(\mathbb{F})$. Then the following are equivalent:

(i) A is invertible.

(ii) $\det A \neq 0$.

(iii) $r(A) = n$.

Lemma. Let $A \in \mathrm{Mat}_n(\mathbb{F})$. Then

(i) We can expand $\det A$ along the jth column by

$$\det A = \sum_{i=1}^n (-1)^{i+j} A_{ij} \det \hat{A}_{ij}.$$

(ii) We can expand $\det A$ along the ith row by

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} A_{ij} \det \hat{A}_{ij}.$$

Theorem. If $A \in \mathrm{Mat}_n(\mathbb{F})$, then $A(\operatorname{adj} A) = (\det A)I_n = (\operatorname{adj} A)A$. In particular, if $\det A \neq 0$, then

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A.$$

Lemma. Let A, B be square matrices. Then for any C, we have

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = (\det A)(\det B).$$

Corollary.

$$\det \begin{pmatrix} A_1 & & & \text{stuff} \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_n \end{pmatrix} = \prod_{i=1}^{n} \det A_i$$

6 Endomorphisms

6.1 Invariants

Lemma. Suppose $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ are bases for V and $\alpha \in \mathrm{End}(V)$. If A represents α with respect to $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and B represents α with respect to $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$, then

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

where P is given by

$$\mathbf{f}_i = \sum_{j=1}^n P_{ji}\mathbf{e}_j.$$

Lemma.

(i) If $A \in \mathrm{Mat}_{m,n}(\mathbb{F})$ and $B \in \mathrm{Mat}_{n,m}(\mathbb{F})$, then

$$\operatorname{tr} AB = \operatorname{tr} BA.$$

(ii) If $A, B \in \mathrm{Mat}_n(\mathbb{F})$ are similar, then $\operatorname{tr} A = \operatorname{tr} B$.

(iii) If $A, B \in \mathrm{Mat}_n(\mathbb{F})$ are similar, then $\det A = \det B$.

Lemma. If A and B are similar, then they have the same characteristic polynomial.

Lemma. Let $\alpha \in \mathrm{End}(V)$ and $\lambda_1, \cdots, \lambda_k$ distinct eigenvalues of α. Then

$$E(\lambda_1) + \cdots + E(\lambda_k) = \bigoplus_{i=1}^k E(\lambda_i)$$

is a direct sum.

Theorem. Let $\alpha \in \mathrm{End}(V)$ and $\lambda_1, \cdots, \lambda_k$ be distinct eigenvalues of α. Write E_i for $E(\lambda_i)$. Then the following are equivalent:

(i) α is diagonalizable.

(ii) V has a basis of eigenvectors for α.

(iii) $V = \bigoplus_{i=1}^k E_i$.

(iv) $\dim V = \sum_{i=1}^k \dim E_i$.

6.2 The minimal polynomial

6.2.1 Aside on polynomials

Lemma (Polynomial division)**.** If $f, g \in \mathbb{F}[t]$ (and $g \neq 0$), then there exists $q, r \in \mathbb{F}[t]$ with $\deg r < \deg g$ such that

$$f = qg + r.$$

Lemma. If $\lambda \in \mathbb{F}$ is a root of f, i.e. $f(\lambda) = 0$, then there is some g such that

$$f(t) = (t - \lambda)g(t).$$

Lemma. A non-zero polynomial $f \in \mathbb{F}[t]$ has at most $\deg f$ roots, counted with multiplicity.

Corollary. Let $f, g \in \mathbb{F}[t]$ have degree $< n$. If there are $\lambda_1, \cdots, \lambda_n$ distinct such that $f(\lambda_i) = g(\lambda_i)$ for all i, then $f = g$.

Corollary. If $\mathbb{F}$ is infinite, then f and g are equal if and only if they agree on all points.

Theorem (The fundamental theorem of algebra)**.** Every non-constant polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$.

6.2.2 Minimal polynomial

Theorem (Diagonalizability theorem)**.** Suppose $\alpha \in \mathrm{End}(V)$. Then α is diagonalizable if and only if there exists non-zero $p(t) \in \mathbb{F}[t]$ such that $p(\alpha) = 0$, and $p(t)$ can be factored as a product of *distinct* linear factors.

Lemma. Let $\alpha \in \mathrm{End}(V)$, and $p \in \mathbb{F}[t]$. Then $p(\alpha) = 0$ if and only if $M_\alpha(t)$ is a factor of $p(t)$. In particular, M_α is unique.

Theorem (Diagonalizability theorem 2.0)**.** Let $\alpha \in \mathrm{End}(V)$. Then α is diagonalizable if and only if $M_\alpha(t)$ is a product of its distinct linear factors.

Theorem. Let $\alpha, \beta \in \mathrm{End}(V)$ be both diagonalizable. Then α and β are simultaneously diagonalizable (i.e. there exists a basis with respect to which both are diagonal) if and only if $\alpha\beta = \beta\alpha$.

6.3 The Cayley-Hamilton theorem

Theorem (Cayley-Hamilton theorem)**.** Let V be a finite-dimensional vector space and $\alpha \in \mathrm{End}(V)$. Then $\chi_\alpha(\alpha) = 0$, i.e. $M_\alpha(t) \mid \chi_\alpha(t)$. In particular, $\deg M_\alpha \leq n$.

Lemma. An endomorphism α is triangulable if and only if $\chi_\alpha(t)$ can be written as a product of linear factors, not necessarily distinct. In particular, if $\mathbb{F} = \mathbb{C}$ (or any algebraically closed field), then every endomorphism is triangulable.

Theorem (Cayley-Hamilton theorem)**.** Let V be a finite-dimensional vector space and $\alpha \in \mathrm{End}(V)$. Then $\chi_\alpha(\alpha) = 0$, i.e. $M_\alpha(t) \mid \chi_\alpha(t)$. In particular, $\deg M_\alpha \leq n$.

Lemma. Let $\alpha \in \mathrm{End}(V), \lambda \in \mathbb{F}$. Then the following are equivalent:

(i) λ is an eigenvalue of α.

(ii) λ is a root of $\chi_\alpha(t)$.

(iii) λ is a root of $M_\alpha(t)$.

6.4 Multiplicities of eigenvalues and Jordan normal form

Lemma. If λ is an eigenvalue of α, then

(i) $1 \leq g_\lambda \leq a_\lambda$

(ii) $1 \leq c_\lambda \leq a_\lambda$.

Lemma. Suppose $\mathbb{F} = \mathbb{C}$ and $\alpha \in \mathrm{End}(V)$. Then the following are equivalent:

(i) α is diagonalizable.

(ii) $g_\lambda = a_\lambda$ for all eigenvalues of α.

(iii) $c_\lambda = 1$ for all λ.

Theorem (Jordan normal form theorem)**.** Every matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ is similar to a matrix in Jordan normal form. Moreover, this Jordan normal form matrix is unique up to permutation of the blocks.

Theorem. Let $\alpha \in \mathrm{End}(V)$, and A in Jordan normal form representing α. Then the number of Jordan blocks $J_n(\lambda)$ in A with $n \geq r$ is

$$n((\alpha - \lambda\iota)^r) - n((\alpha - \lambda\iota)^{r-1}).$$

Theorem (Generalized eigenspace decomposition)**.** Let V be a finite-dimensional vector space $\mathbb{C}$ such that $\alpha \in \mathrm{End}(V)$. Suppose that

$$M_\alpha(t) = \prod_{i=1}^k (t - \lambda_i)^{c_i},$$

with $\lambda_1, \cdots, \lambda_k \in \mathbb{C}$ distinct. Then

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

where $V_i = \ker((\alpha - \lambda_i\iota)^{c_i})$ is the *generalized eigenspace*.

7 Bilinear forms II

7.1 Symmetric bilinear forms and quadratic forms

Lemma. Let V be a finite-dimensional vector space over $\mathbb{F}$, and $\phi : V \times V \to \mathbb{F}$ is a symmetric bilinear form. Let $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ be a basis for V, and let M be the matrix representing ϕ with respect to this basis, i.e. $M_{ij} = \phi(\mathbf{e}_i, \mathbf{e}_j)$. Then ϕ is symmetric if and only if M is symmetric.

Lemma. Let V is a finite-dimensional vector space, and $\phi : V \times V \to \mathbb{F}$ a bilinear form. Let $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{f}_1, \cdots, \mathbf{f}_n)$ be bases of V such that

$$\mathbf{f}_i = \sum_{k=1}^n P_{ki}\mathbf{e}_k.$$

If A represents ϕ with respect to $(\mathbf{e}_i)$ and B represents ϕ with respect to $(\mathbf{f}_i)$, then

$$B = P^T AP.$$

Proposition (Polarization identity)**.** Suppose that $\operatorname{char}\mathbb{F} \neq 2$, i.e. $1 + 1 \neq 0$ on $\mathbb{F}$ (e.g. if $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$). If $q : V \to \mathbb{F}$ is a quadratic form, then there exists a *unique* symmetric bilinear form $\phi : V \times V \to \mathbb{F}$ such that

$$q(\mathbf{v}) = \phi(\mathbf{v}, \mathbf{v}).$$

Theorem. Let V be a finite-dimensional vector space over $\mathbb{F}$, and $\phi : V \times V \to \mathbb{F}$ a symmetric bilinear form. Then there exists a basis $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ for V such that ϕ is represented by a diagonal matrix with respect to this basis.

Theorem. Let ϕ be a symmetric bilinear form over a complex vector space V. Then there exists a basis $(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ for V such that ϕ is represented by

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

with respect to this basis, where $r = r(\phi)$.

Corollary. Every symmetric $A \in \operatorname{Mat}_n(\mathbb{C})$ is congruent to a unique matrix of the form

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

Theorem. Let ϕ be a symmetric bilinear form of a finite-dimensional vector space over $\mathbb{R}$. Then there exists a basis $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ for V such that ϕ is represented

$$\begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0 \end{pmatrix},$$

with $p + q = r(\phi)$, $p, q \geq 0$. Equivalently, the corresponding quadratic forms is given by

$$q\left(\sum_{i=1}^n a_i \mathbf{v}_i\right) = \sum_{i=1}^p a_i^2 - \sum_{j=p+1}^{p+q} a_j^2.$$

Theorem (Sylvester's law of inertia)**.** Let ϕ be a symmetric bilinear form on a finite-dimensional real vector space V. Then there exists unique non-negative integers p, q such that ϕ is represented by

$$\begin{pmatrix} I_p & 0 & 0\\ 0 & -I_q & 0\\ 0 & 0 & 0 \end{pmatrix}$$

with respect to some basis.

Corollary. Every real symmetric matrix is congruent to precisely one matrix of the form

$$\begin{pmatrix} I_p & 0 & 0\\ 0 & -I_q & 0\\ 0 & 0 & 0 \end{pmatrix}.$$

7.2 Hermitian form

Lemma. Let $\phi : V \times V \to \mathbb{C}$ be a sesquilinear form on a finite-dimensional vector space over $\mathbb{C}$, and $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ a basis for V. Then ϕ is Hermitian if and only if the matrix A representing ϕ is Hermitian (i.e. $A = A^\dagger$).

Proposition (Change of basis)**.** Let ϕ be a Hermitian form on a finite dimensional vector space V; $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ and $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ are bases for V such that

$$\mathbf{v}_i = \sum_{k=1}^n P_{ki}\mathbf{e}_k;$$

and A, B represent ϕ with respect to $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ and $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ respectively. Then

$$B = P^\dagger AP.$$

Lemma (Polarization identity (again))**.** A Hermitian form ϕ on V is determined by the function $\psi : \mathbf{v} \mapsto \phi(\mathbf{v}, \mathbf{v})$.

Theorem (Hermitian form of Sylvester's law of inertia)**.** Let V be a finite-dimensional complex vector space and ϕ a hermitian form on V. Then there exists unique non-negative integers p and q such that ϕ is represented by

$$\begin{pmatrix} I_p & 0 & 0\\ 0 & -I_q & 0\\ 0 & 0 & 0 \end{pmatrix}$$

with respect to some basis.

8 Inner product spaces

8.1 Definitions and basic properties

Theorem (Cauchy-Schwarz inequality)**.** Let V be an inner product space and $\mathbf{v}, \mathbf{w} \in V$. Then

$$|(\mathbf{v}, \mathbf{w})| \leq \|\mathbf{v}\|\|\mathbf{w}\|.$$

Corollary (Triangle inequality)**.** Let V be an inner product space and $\mathbf{v}, \mathbf{w} \in V$. Then

$$\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|.$$

Lemma (Parseval's identity)**.** Let V be a finite-dimensional inner product space with an orthonormal basis $\mathbf{v}_1, \cdots, \mathbf{v}_n$, and $\mathbf{v}, \mathbf{w} \in V$. Then

$$(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^n \overline{(\mathbf{v}_i, \mathbf{v})}(\mathbf{v}_i, \mathbf{w}).$$

In particular,

$$\|\mathbf{v}\|^2 = \sum_{i=1}^n |(\mathbf{v}_i, \mathbf{v})|^2.$$

8.2 Gram-Schmidt orthogonalization

Theorem (Gram-Schmidt process)**.** Let V be an inner product space and $\mathbf{e}_1, \mathbf{e}_2, \cdots$ a linearly independent set. Then we can construct an orthonormal set $\mathbf{v}_1, \mathbf{v}_2, \cdots$ with the property that

$$\langle \mathbf{v}_1, \cdots, \mathbf{v}_k \rangle = \langle \mathbf{e}_1, \cdots, \mathbf{e}_k \rangle$$

for every k.

Corollary. If V is a finite-dimensional inner product space, then any orthonormal set can be extended to an orthonormal basis.

Proposition. Let V be a finite-dimensional inner product space, and $W \leq V$. Then

$$V = W \perp W^\perp.$$

Proposition. Let V be a finite-dimensional inner product space and $W \leq V$. Let $(\mathbf{e}_1, \cdots, \mathbf{e}_k)$ be an orthonormal basis of W. Let π be the orthonormal projection of V onto W, i.e. $\pi : V \to W$ is a function that satisfies $\ker \pi = W^\perp$, $\pi|_W = \mathrm{id}$. Then

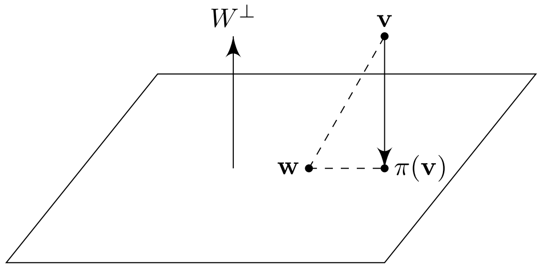
(i) π is given by the formula

$$\pi(\mathbf{v}) = \sum_{i=1}^k (\mathbf{e}_i, \mathbf{v})\mathbf{e}_i.$$

(ii) For all $\mathbf{v} \in V, \mathbf{w} \in W$, we have

$$\|\mathbf{v} - \pi(\mathbf{v})\| \leq \|\mathbf{v} - \mathbf{w}\|,$$

with equality if and only if $\pi(\mathbf{v}) = \mathbf{w}$. This says $\pi(\mathbf{v})$ is the point on W that is closest to $\mathbf{v}$.



8.3 Adjoints, orthogonal and unitary maps

Lemma. Let V and W be finite-dimensional inner product spaces and $\alpha : V \to W$ is a linear map. Then there exists a unique linear map $\alpha^* : W \to V$ such that

$$(\alpha\mathbf{v}, \mathbf{w}) = (\mathbf{v}, \alpha^*\mathbf{w}) \tag{$*$}$$

for all $\mathbf{v} \in V$, $\mathbf{w} \in W$.

Lemma. Let V be a finite-dimensional space and $\alpha \in \mathrm{End}(V)$. Then α is orthogonal if and only if $\alpha^{-1} = \alpha^*$.

Corollary. $\alpha \in \mathrm{End}(V)$ is orthogonal if and only if α is represented by an orthogonal matrix, i.e. a matrix A such that $A^TA = AA^T = I$, with respect to any orthonormal basis.

Proposition. Let V be a finite-dimensional real inner product space and $(\mathbf{e}_1, \cdots, \mathbf{e}_n)$ is an orthonormal basis of V. Then there is a bijection

$$\begin{aligned} \mathrm{O}(V) &\to \{\text{orthonormal basis for } V\} \\ \alpha &\mapsto (\alpha(\mathbf{e}_1, \cdots, \mathbf{e}_n)). \end{aligned}$$

Lemma. Let V be a finite dimensional complex inner product space and $\alpha \in \mathrm{End}(V)$. Then α is unitary if and only if α is invertible and $\alpha^* = \alpha^{-1}$.

Corollary. $\alpha \in \mathrm{End}(V)$ is unitary if and only if α is represented by a unitary matrix A with respect to any orthonormal basis, i.e. $A^{-1} = A^\dagger$.

Proposition. Let V be a finite-dimensional complex inner product space. Then there is a bijection

$$\begin{aligned} U(V) &\to \{\text{orthonormal basis of } V\} \\ \alpha &\mapsto \{\alpha(\mathbf{e}_1), \cdots, \alpha(\mathbf{e}_n)\}. \end{aligned}$$

8.4 Spectral theory

Lemma. Let V be a finite-dimensional inner product space, and $\alpha \in \mathrm{End}(V)$ self-adjoint. Then

(i) α has a real eigenvalue, and all eigenvalues of α are real.

(ii) Eigenvectors of α with distinct eigenvalues are orthogonal.

Theorem. Let V be a finite-dimensional inner product space, and $\alpha \in \mathrm{End}(V)$ self-adjoint. Then V has an orthonormal basis of eigenvectors of α.

Corollary. Let V be a finite-dimensional vector space and α self-adjoint. Then V is the orthogonal (internal) direct sum of its α-eigenspaces.

Corollary. Let $A \in \mathrm{Mat}_n(\mathbb{R})$ be symmetric. Then there exists an orthogonal matrix P such that $P^T AP = P^{-1}AP$ is diagonal.

Corollary. Let V be a finite-dimensional real inner product space and $\psi : V \times V \to \mathbb{R}$ a symmetric bilinear form. Then there exists an orthonormal basis $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ for V with respect to which ψ is represented by a diagonal matrix.

Corollary. Let V be a finite-dimensional real vector space and ϕ, ψ symmetric bilinear forms on V such that ϕ is positive-definite. Then we can find a basis $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ for V such that both ϕ and ψ are represented by diagonal matrices with respect to this basis.

Corollary. If $A, B \in \mathrm{Mat}_n(\mathbb{R})$ are symmetric and A is positive definitive (i.e. $\mathbf{v}^T A\mathbf{v} > 0$ for all $\mathbf{v} \in \mathbb{R}^n \setminus \{0\}$). Then there exists an invertible matrix Q such that $Q^T AQ$ and $Q^T BQ$ are both diagonal.

Proposition.

(i) If $A \in \mathrm{Mat}_n(\mathbb{C})$ is Hermitian, then there exists a unitary matrix $U \in \mathrm{Mat}_n(\mathbb{C})$ such that
$$U^{-1}AU = U^\dagger AU$$
is diagonal.

(ii) If ψ is a Hermitian form on a finite-dimensional complex inner product space V, then there is an orthonormal basis for V diagonalizing ψ.

(iii) If ϕ, ψ are Hermitian forms on a finite-dimensional complex vector space and ϕ is positive definite, then there exists a basis for which ϕ and ψ are diagonalized.

(iv) Let $A, B \in \mathrm{Mat}_n(\mathbb{C})$ be Hermitian, and A positive definitive (i.e. $\mathbf{v}^\dagger A\mathbf{v} > 0$ for $\mathbf{v} \in V \setminus \{0\}$). Then there exists some invertible Q such that $Q^\dagger AQ$ and $Q^\dagger BQ$ are diagonal.

Theorem. Let V be a finite-dimensional complex vector space and $\alpha \in U(V)$ be unitary. Then V has an orthonormal basis of α eigenvectors.