Advanced Vector Spaces

Henrik Schlichtkrull

2020

These are the lecture notes for the course Advanced Vector Spaces at the Department for Mathematical Sciences, University of Copenhagen. There are 14 chapters, each corresponding to approximately two hours of lecturing.

I am grateful to Stig Eilsøe-Madsen for typesetting an earlier version of the notes from my handwritten lecture notes.

Henrik Schlichtkrull, `schlicht@math.ku.dk`

Contents

1 Foundations 3

2 Linearity 11

3 Duality 21

4 Bilinear maps 29

5 Sums and products 39

6 Eigendecomposition 47

7 Generalized eigendecomposition 57

8 Orthogonality 65

9 Spectral theorems 75

10 Determinants 83

11 Jordan normal form 95

12 Bounded operators 101

13 Positivity 111

14 Factorization 119

Lecture 1. Foundations

Fields

In this lecture the fundamental concepts needed for describing a vector space will be developed. We consider vector spaces over an arbitrary field, and therefore we begin by recalling the definition of a field.

Definition 1.1. A *field* consists of a set $\mathcal{F}$, of which the elements are called *scalars*, and two binary maps $\mathcal{F} \times \mathcal{F} \to \mathcal{F}$, denoted $+$ and $\cdot$ (symbol often omitted), such that

(a) $\mathcal{F}$ with $+$ is an abelian group with identity element denoted 0,

(b) $\mathcal{F} \setminus \{0\}$ with $\cdot$ is an abelian group with identity element denoted 1,

(c) the *distributive* law $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ holds for all scalars α, β, γ.

In the language of (a) the statement in (c) is that multiplication by α is a homomorphism of the additive group. In particular (c) implies $\alpha \cdot 0 = 0$ for all α.

For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields with the standard definitions of sum and product. The ring $\mathbb{Z}/p\mathbb{Z}$ of integers mod p is a field when p is a prime.

Vector spaces

Definition 1.2. A *vector space* V over a field $\mathcal{F}$ consists of of set V, of which the elements are called *vectors*, equipped with a binary map $V \times V \to V$ denoted $+$, and a map $\mathcal{F} \times V \to V$ denoted $\cdot$ (*scalar multiplication*, symbol often omitted) such that the following rules hold:

(a) V with $+$ is an abelian group with identity element 0 (the *zero vector*),

(b) the *distributive* laws $\alpha(x + y) = \alpha x + \alpha y$ and $(\alpha + \beta)x = \alpha x + \beta x$ hold for all scalars α, β and all vectors x, y,

(c) $\alpha(\beta x) = (\alpha\beta)x$ and $1 \cdot x = x$ for all $\alpha, \beta \in \mathcal{F}$, $x \in V$.

The rule

$$\alpha = 0 \vee x = 0 \quad \Leftrightarrow \quad \alpha x = 0$$

follows from (b) and (c), for all $\alpha \in \mathcal{F}$, $x \in V$.

Examples 1.3.

1. $V = \mathcal{F}^n$ is a vector space over $\mathcal{F}$, for $n \in \mathbb{N}$ and $\mathcal{F}$ an arbitrary field.
2. $\{0\}$ is a vector space over any field, called the *trivial space.*
3. $\mathbb{C}$ is a vector space over $\mathbb{R}$, and $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Subspaces

Let V be a vector space over a field $\mathcal{F}$.

Definition 1.4. A subset U of V is a *subspace* if $0 \in U$ and if $x + y$ and αx are in U for all $x, y \in U$ and all scalars α.

A subspace of V is itself a vector space, when equipped with the sum and scalar product it inherits from V.

Linear combinations

Definition 1.5. A *linear combination* is a finite sum $\sum_{i=1}^{n} \alpha_i x_i \in V$ where $x_1, \dots, x_n \in V$ and $\alpha_1, \dots, \alpha_n \in \mathcal{F}$. The vector $x = \sum_{i=1}^{n} \alpha_i x_i$ is called the *sum* of the linear combination. If $S \subseteq V$ is a subset and $x_1, \dots, x_n \in S$, the linear combination is said to be *from* S.

In this definition we allow also $n = 0$, giving the *empty linear combination*. By definition its sum is the zero vector 0.

Remark 1.6. If $x_i \neq x_j$ for all $i \neq j$ we say the linear combination has *distinct vectors*. If this is not the case, we can make up for it by adding together terms with identical vectors. Clearly this will not affect sum of the linear combination.

Span

Definition 1.7. Let $S \subseteq V$ be a subset. The *span* of S is the set

$$\operatorname{Span} S := \{\text{linear combinations from } S\}$$

and if $\operatorname{Span} S = V$ we say that S *spans* V.

By the definition of the empty linear combination we see that the span of the empty set is $\operatorname{Span} \emptyset = \{0\}$ and that $0 \in \operatorname{Span} S$ for every S.

Lemma 1.8. *Let $S \subseteq V$ be a subset and $U \subseteq V$ a subspace.*

(a) $\operatorname{Span} S$ *is a subspace of* V.

(b) *If* $S \subseteq U$ *then* $\operatorname{Span} S \subseteq U$.

In particular $\operatorname{Span} S$ *is the smallest subspace of* V *which contains* S.

Proof. Both (a) and (b) are easily seen from the definitions, and the final statement follows. □

It follows from Lemma 1.8 that $\operatorname{Span} U = U$ for every subspace $U \subseteq V$, and hence in particular

$$\operatorname{Span}(\operatorname{Span} S) = \operatorname{Span} S \tag{1.1}$$

for every subset $S \subseteq V$.

Linear dependence

Let $L \subseteq V$ be a subset.

Definition 1.9. L is called *linearly dependent* if $x \in \operatorname{Span}(L \setminus \{x\})$ for some $x \in L$. Otherwise it is called *linearly independent.*

The definition implies that every set which contains the zero vector is linearly dependent. On the other hand, the empty set $L = \emptyset$ is linearly independent. It is also noteworthy that every subset of a linearly independent set is again linearly independent.

Lemma 1.10. *L is linearly dependent if and only if there exist distinct vectors $x_1, \dots, x_n$ in L, and scalars $\alpha_1, \dots, \alpha_n$ of which at least one is non-zero, such that*

$$\sum_{i=1}^{n} \alpha_i x_i = 0.$$

Proof. If $x \in \operatorname{Span}(L \setminus \{x\})$, then $x = \sum_j \beta_j x_j$ for some scalars β_j and some vectors $x_j \in L \setminus \{x\}$, which we may assume are distinct (see Remark 1.6). In the relation $x - \sum_j \beta_j x_j = 0$ all the vectors are distinct, and the coefficient 1 to x is not zero.

Conversely, if $\sum_i \alpha_i x_i = 0$ and $\alpha_i \neq 0$ for some i, then $x_i = -\sum_{j \neq i} \frac{\alpha_j}{\alpha_i} x_j$ and hence $x_i \in \operatorname{Span}(L \setminus \{x_i\})$ for this i. □

A useful lemma

Lemma 1.11. *Let $L \subseteq V$ be linearly independent, and let $x \notin L$. Then $L \cup \{x\}$ is linearly dependent if and only if $x \in \operatorname{Span} L$.*

Proof. If $L \cup \{x\}$ is linearly dependent then 0 is a linear combination from $L \cup \{x\}$ as in Lemma 1.10. That linear combination has to involve x with a non-zero coefficient α, because otherwise L would be linearly dependent. Thus $\sum_i \alpha_i x_i + \alpha x = 0$ with $x_i \in L$ and $\alpha \neq 0$. This implies that $x \in \operatorname{Span} L$. Conversely, if $x \in \operatorname{Span} L$ then $L \cup \{x\}$ is linearly dependent by definition. □

Basis and coordinates

Definition 1.12. A *basis* for a vector space V is a subset $B \subseteq V$ which

(a) spans V,

(b) is linearly independent.

Lemma 1.13. *A subset $B \subseteq V$ is a basis if and only if every vector $x \in V$ can be obtained in a unique way as a linear combination from B.*

The uniqueness needs to be clarified. That $x \in \operatorname{Span} B$ means

$$x = \sum_{v \in B'} \alpha_v \, v \tag{1.2}$$

for some finite subset $B' \subseteq B$. By saying that this expression is unique we mean that if

$$x = \sum_{v \in B'} \alpha_v \, v = \sum_{v \in B''} \beta_v \, v$$

then $\alpha_v = \beta_v$ for all $v \in B' \cap B''$, and all other coefficients α_v or β_v are zero.

Proof. We can assume that B spans V. The lemma asserts that B is linearly independent if and only if the expression (1.2) is unique for all $x \in V$.

Assume first that B is linearly independent, and that

$$\sum_{v \in B'} \alpha_v \, v = \sum_{v \in B''} \beta_v \, v.$$

By inserting extra terms with coefficient zero when necessary, we can assume that $B' = B''$. Then

$$\sum_{v \in B'} (\alpha_v - \beta_v) \, v = 0$$

and it follows from Lemma 1.10 that $\alpha_v = \beta_v$ for all v.

Conversely, if B is linearly dependent then Lemma 1.10 implies that the zero vector can be obtained as in (1.2) in a non-trivial way, which contradicts uniqueness of the expression. □

The main purpose of a basis B is to provide coordinates for the elements of V. We obtain that with Lemma 1.13.

Definition 1.14. Assuming B is a basis for V we call the scalars α_v in (1.2) the *coordinates* of x *with respect to* B.

In particular, if B is finite, say $B = \{x_1, \dots, x_n\}$, then this means that the map

$$x = \sum_{i=1}^{n} \alpha_i x_i \mapsto (\alpha_i)_{i=1,\dots,n} \tag{1.3}$$

is a bijection $V \to \mathcal{F}^n$.

Characterization by maximality

Let $L \subseteq S \subseteq V$ and assume that L is linearly independent and S spans V.

Lemma 1.15. *L is a basis for V if and only if it is maximal linearly independent in S, that is, if and only if*

$$\forall x \in S \setminus L : \quad L \cup \{x\} \text{ is linearly dependent.} \tag{1.4}$$

Proof. Since L is assumed to be linearly independent, it is a basis if and only if it spans V. Since S spans V, it follows from (1.1) that L spans V if and only if $S \subseteq \operatorname{Span} L$. Since $L \subseteq S$ this happens if and only if $S \setminus L \subseteq \operatorname{Span} L$. Finally by Lemma 1.11 this last condition is equivalent to (1.4). □

Existence of a basis

The following is the first main result of this lecture.

Theorem 1.16. *Let $L \subseteq S \subseteq V$ where S spans V and L is linearly independent. Assume S is finite. Then there exists a basis B for V such that*

$$L \subseteq B \subseteq S.$$

Proof. There are only finitely many sets between L and S, and at least one of them, L, is linearly independent. Hence among the linearly independent sets between L and S some set B must be maximal with respect to inclusion. By Lemma 1.15 this is a basis. □

Corollary 1.17. *If V is finitely spanned then it has a finite basis.*

Proof. Follows from Theorem 1.16 by taking $L = \emptyset$. □

Remark 1.18. The theorem holds without the assumption that S is finite. This can be seen with Zorn's lemma. As in the corollary we can then conclude that every vector space has a (not necessarily finite) basis.

Finite dimension

Definition 1.19. Let V be a vector space. We call V *finite-dimensional*, $\dim V < \infty$, if there exists a finite basis for it, and otherwise *infinite-dimensional*, $\dim V = \infty$. It is *n-dimensional* if there exists a finite basis with n elements.

By Corollary 1.17 finite-dimensional is equivalent with finitely spanned. We shall soon see that n is unique. Until then, a finite-dimensional space could potentially be n-dimensional for several integers n.

Exchange lemmas

Let S be a subset of V that spans V and let $k \in \mathbb{N}$.

Lemma 1.20. *If there exists in V a linearly independent subset with k elements, then there exists in S a linearly independent subset with k elements.*

The proof of this lemma is based on a second lemma. Let L and S be subsets of V such that L is linearly independent and S spans V.

Lemma 1.21. *For each $x \in L$ there exists $y \in S$ such that $y \notin L \setminus \{x\}$ and*

$$(L \setminus \{x\}) \cup \{y\}$$

is linearly independent.

Before giving the proof of this lemma, let us see how it is used to prove the first lemma.

Proof of Lemma 1.20. Lemma 1.21 says that we can exchange an element x in L, which is not already in S, by an element y from S, while maintaining both the linear independence and the number of elements. After at most k steps we reach a linearly independent subset of S. □

Proof of Lemma 1.21. Since L is linearly independent it follows from Lemma 1.10 that $x \notin \operatorname{Span}(L \setminus \{x\})$. In particular, $\operatorname{Span}(L \setminus \{x\})$ is a proper subspace of V. Since S spans V it follows (by (1.1)) that there must exist an element $y \in S$ outside of $\operatorname{Span}(L \setminus \{x\})$. Now Lemma 1.11 implies that $(L \setminus \{x\}) \cup \{y\}$ is linearly independent. □

Uniqueness of dimension

The following is the second main theorem. The important conclusion is that a finite-dimensional vector space has a unique dimension. This allows us to write $\dim V = n$ if V if is n-dimensional, and call it *the* dimension of V.

Theorem 1.22. *Let V be an n-dimensional vector space.*

(1) *Every linearly independent subset of V has at most n elements and is contained in a basis.*

(2) *Every spanning subset of V has at least n elements and contains a basis.*

(3) *Every basis has exactly n elements.*

Proof. By assumption V has a basis B with n elements.

(1) Let $L \subseteq V$ be linearly independent. It follows from Lemma 1.20 with $S = B$ that L has at most n elements, and from Theorem 1.16 with $S = L \cup B$ that L is contained in a basis.

(2) Let $S \subseteq V$ be spanning. It follows from Lemma 1.20 with $L = B$ that S contains a linearly independent set with n elements. By (1) this set is maximal linearly independent, and hence a basis by Lemma 1.15.

(3) This is immediate from (1) and (2). □

Verifying a basis

Here is a useful corollary. It shows that only one of the two conditions for a basis needs to be verified, if the number of elements is known to fit with the dimension of V. As before, V is finite-dimensional.

Corollary 1.23. *Let $X \subseteq V$ be a subset with exactly $n = \dim V$ elements. If X is linearly independent or spans V, then it is a basis.*

Proof. It follows from Theorem 1.22 that X is contained in, or contains, a basis, and that this basis has n elements. Hence this basis is equal to X. □

Infinite dimension

Lemma 1.24. *V is infinite-dimensional if and only if there exists an infinite linearly independent subset $L \subseteq V$.*

Proof. Assume $\dim V = \infty$. Since V is not finite-dimensional it follows from Lemma 1.15 that every finite linearly independent subset is contained in a linearly independent subset with one element more. Starting with $L_0 = \emptyset$ we obtain a sequence $L_0 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq V$ of linearly independent sets L_n with n elements. The union $\cup_n L_n$ is infinite and easily seen to be linearly independent.

The converse statement is clear from Theorem 1.22(1). □

Subspace dimension

Let V be finite-dimensional with $n = \dim V$.

Theorem 1.25. *Let $U \subseteq V$ be a subspace. Then U is finite-dimensional with $\dim U \leq n$. Moreover, every basis for U can be extended to a basis for V.*

Proof. Every linearly independent set in U has at most n vectors since it is also linearly independent in V. Hence $\dim U < \infty$ by Lemma 1.24, and a basis for it has at most n elements, that is $\dim U \leq n$. The final statement follows from Theorem 1.22(1). □

Lecture 2. Linearity

Linear maps

In this lecture we consider those maps between vector spaces, which preserve their algebraic structure. Let U, V be vector spaces over a common field $\mathcal{F}$.

Definition 2.1. A *linear map* (or *homomorphism*) from U to V is a map A for which

$$A(\alpha x + \beta y) = \alpha A(x) + \beta A(y)$$

for all $x, y \in U$ and all $\alpha, \beta \in \mathcal{F}$. In this case we say that $A(x)$ *depends linearly* on x. The set of linear maps from U to V is denoted by $\mathrm{Hom}(U, V)$.

In particular, we denote $\mathrm{Hom}(V, V) = \mathrm{End}(V)$ and call its elements *endomorphisms.*

The set $\mathrm{Hom}(U, V)$ is naturally organized into a vector space of its own:

Lemma 2.2. $\mathrm{Hom}(U, V)$ *is a vector space over* $\mathcal{F}$ *with operations defined by*

$$A + B : x \mapsto A(x) + B(x), \quad \alpha A : x \mapsto \alpha A(x)$$

for $x \in U$*, and with the zero map* $x \mapsto 0$ *as zero vector.*

Proof. It is straightforward to verify first that $A + B$ and αA belong to $\mathrm{Hom}(U, V)$ and next that with these definitions the axioms of a vector space are satisfied for $\mathrm{Hom}(U, V)$. □

Extension from a basis

The following lemma shows that a linear map from U to V is completely determined on a basis for U.

Lemma 2.3. *Let* B *be a basis for* U *and let* $f : B \to V$ *be a map. Then there exists a unique linear map* $A : U \to V$ *which extends* f*, that is, such that* $A(x) = f(x)$ *for all* $x \in B$*.*

Proof. Any linear map from U to V satisfies

$$A\big(\sum_i \alpha_i x_i\big) = \sum_i \alpha_i A(x_i) \tag{2.1}$$

for all linear combinations from B. Hence it is uniquely determined by its restriction to B. To ensure that the restriction is f, we define A by (2.1) with $A(x_i)$ replaced by $f(x_i)$ on the right hand side. It is easily seen from Lemma 1.13 that A is well-defined and linear. □

Null-space and range

Let U and V be vector spaces over $\mathcal{F}$.

Definition 2.4. Let $A \in \operatorname{Hom}(U, V)$.

(a) $N(A) := \{x \in U \mid Ax = 0\}$ is called the *null-space* (or *kernel*) of A.

(b) $R(A) := \{Ax \mid x \in U\}$ is called the *range* (or *image*) of A.

It is easily seen that $N(A) \subset U$ and $R(A) \subset V$ are subspaces. There is a simple relation of these subspaces to injectivity and surjectivity.

Lemma 2.5. *Let $A \in \operatorname{Hom}(U, V)$. Then*

(a) *A is injective if and only if $N(A) = \{0\}$.*

(b) *A is surjective if and only if $R(A) = V$.*

Proof. (a) follows easily from the simple observation that $Ax_1 = Ax_2$ if and only if $A(x_1 - x_2) = 0$. (b) is a tautology. □

Isomorphisms

Definition 2.6. A bijective linear map $U \to V$ is called a *linear isomorphism.* If such a map exists we say that U and V are *isomorphic.*

Lemma 2.7. *Let $A \in \operatorname{Hom}(U, V)$, and let $S, L, B \subseteq U$ be subsets which are, respectively, spanning, linearly independent, a basis. Then*

(1) *A is surjective $\Leftrightarrow$ $A(S)$ spans V.*

(2) *A is injective $\Rightarrow$ $A|_{\operatorname{Span} L}$ is injective $\Leftrightarrow$ $A|_L$ is injective and $A(L)$ is linearly independent.*

(3) *A is bijective $\Leftrightarrow$ $A|_B$ is injective and $A(B)$ is a basis for V.*

Proof. (1) This follows from the identity $A(\operatorname{Span} S) = \operatorname{Span} A(S)$, which is easily seen to hold for every subset $S \subset U$.

(2) The first implication is trivial. Assume $A|_{\operatorname{Span} L}$ is injective, and let $x \in L$. Then $x \notin \operatorname{Span}(L \backslash \{x\})$ since L is linearly independent. By injectivity

$$Ax \notin A(\operatorname{Span}(L \backslash \{x\})) = \operatorname{Span}(A(L \backslash \{x\})) = \operatorname{Span}(A(L) \backslash \{Ax\}).$$

Hence $A(L)$ is linearly independent.

For the converse it suffices (by Lemma 2.5(a)) to show that if $Ax = 0$ for some linear combination $x = \sum_i \alpha_i x_i$ from L, then $x = 0$. This follows by linearity of A and the linear independence of $A(L)$.

(3) This follows from (1) and (2). □

Dimension theorem

Corollary 2.8. *If U and V are finite-dimensional, then* $\dim U = \dim V$ *if and only if there exists an isomorphism from U to V.*

Proof. If there is an isomorphism, it maps a basis for U bijectively onto a basis for V, according to Lemma 2.7(3). Hence the dimensions agree.

Conversely, assume $\dim U = \dim V$. Let B and C be bases for U and V. Let $f : B \to C$ be an arbitrary bijective map. The linear map $A : U \to V$ of Lemma 2.3 is then an isomorphism by Lemma 2.7(3). □

The inverse

Let $A \in \mathrm{Hom}(U, V)$. It is easy to see that if A is bijective then the inverse map is also linear, that is, $A^{-1} \in \mathrm{Hom}(V, U)$.

The following lemma is essentially just a result of elementary set theory.

Lemma 2.9. *If $AT = I_V$ and $SA = I_U$ for some maps $S, T \in \mathrm{Hom}(V, U)$, then A is an isomorphism and $S = T$ is the inverse of A.*

Proof. It suffices to show $S = T$, and this follows from applying the associative rule to SAT. □

Theorem 2.10. *Assume that U and V both have the finite dimension n. If A is surjective or injective, then it is bijective.*

Proof. Let B be a basis for U, then B has n elements. By Lemma 2.7(3) it suffices to show that $A(B)$ has n elements and is a basis.

If A is surjective then $A(B)$ spans V by Lemma 2.7(1). Being the image of B it has at most n elements, hence exactly n by Theorem 1.22(2). By Corollary 1.23 it is a basis.

If A is injective then $A(B)$ has n elements and is linearly independent by Lemma 2.7(2). By the same corollary we conclude it is a basis. □

Hence we can improve Lemma 2.9 when the dimensions of U and V agree.

Corollary 2.11. *Suppose that* $\dim U = \dim V < \infty$*, and let* $T \in \mathrm{Hom}(V, U)$. *If $AT = 1_V$ or $TA = 1_U$, then A is an isomorphism, and $A^{-1} = T$.*

Proof. If $AT = 1_V$, then A is surjective, and if $TA = 1_U$, then it is injective. In both cases Theorem 2.10 implies A is bijective. Then $A^{-1} = T$ follows. □

In particular, if $U = V$ we call A *invertible* when it is an isomorphism, and we define

$$\mathrm{GL}(V) := \{\text{invertible maps } A \in \mathrm{End}(V)\}.$$

This is a subgroup of the group of all bijective maps $V \to V$ endowed with composition and with the identity map I_V of V as identity element. It is called the *general linear group* of V.

Quotient space

We start by recalling the following construction from group theory. Let G be a group and H a subgroup. We assume that G is abelian and denote its operation by $+$. Each element $x \in G$ determines a *coset* in G, which is denoted $x + H$ and defined by

$$x + H := \{x + h \mid h \in H\} \subseteq G.$$

The set $\{x + H \mid x \in G\}$ of all cosets is denoted G/H and called the *quotient* of G by H. It is organized as a group with addition defined by

$$(x + H) + (y + H) := (x + y) + H \tag{2.2}$$

and with identity element $0 + H$.

The standard example is that of modular arithmetic, where $G = \mathbb{Z}$ and $H = \mathbb{Z}n$ with a positive integer n. In this case the addition on G/H represents addition modulo n on $\mathbb{Z}$.

We apply the theory with $G = V$ a vector space V over an arbitrary field $\mathcal{F}$, and with $H = U$ a subspace. Together with the addition in (2.2) we equip the quotient V/U with a scalar multiplication, defined by

$$\alpha(x + U) := \alpha x + U.$$

It is now easy to verify the following.

Lemma 2.12. *Organized as above the quotient V/U is a vector space over $\mathcal{F}$. Moreover, the surjective map $\pi : V \to V/U$ defined by*

$$\pi(x) := x + U$$

is linear and has null-space $N(\pi) = U$.

Definition 2.13. V/U is called the *quotient space* of V by U, and the linear map $\pi : V \to V/U$ is called the *projection.*

Quotient space basis

Let V/U be as in Definition 2.13. We will determine a basis for it.

Theorem 2.14. *Let C be a basis for U and B a basis for V with $C \subseteq B$. Then the projection π maps the complement $B \setminus C$ bijectively onto a basis for V/U. In particular, if* $\dim V$ *is finite then* $\dim(V/U) = \dim V - \dim U$.

Proof. Let $D = B \setminus C$ and $W = \operatorname{Span}(D)$. Since π is surjective and B spans V, the image $\pi(B)$ spans V/U (see Lemma 2.7(1)). Since $\pi(C) = \{0\}$ we conclude that $\pi(D)$ spans V/U. Hence $\pi(W) = V/U$.

Besides, $U \cap W = \operatorname{Span}(C) \cap \operatorname{Span}(D) = \{0\}$ by Lemma 1.13. Since $N(\pi) = U$ this implies that $\pi|_W$ is injective. Hence this is a linear isomorphism and it maps the basis D for W bijectively onto a basis for V/U. □

Quotient maps

Let U and V be vector spaces over $\mathcal{F}$, and let $X \subseteq U$ and $Y \subseteq V$ be subspaces. Let $A \in \operatorname{Hom}(U, V)$ and assume that $A(X) \subseteq Y$.

By applying A we see that if $u_1 + X = u_2 + X$ for some $u_1, u_2 \in U$ then $Au_1 + Y = Au_2 + Y$. Hence the following is a valid definition.

Definition 2.15. The *quotient map* $\bar{A} : U/X \to V/Y$ is defined by

$$\bar{A}(u + X) = Au + Y$$

for $u \in U$.

It is easily seen that the quotient map $\bar{A}$ is linear. The following particular case is obtained when $U = V$ and $X = Y$.

Definition 2.16. If $A \in \operatorname{End}(V)$ is given, we say that a subspace $X \subseteq V$ is *invariant* (or A-*invariant*) if $A(X) \subseteq X$.

It follows that in this case $\bar{A} \in \operatorname{End}(V/X)$.

Nullity and rank

We now apply Definition 2.15 with $X = N(A)$ and $Y = \{0\}$ and obtain a quotient map $\bar{A} : U/N(A) \to V$ by setting

$$\bar{A}(u + N(A)) = Au$$

for all $u \in U$. The following is an analog of the *first isomorphism* for groups.

Theorem 2.17. *The map $\bar{A}$ provides an isomorphism of $U/N(A)$ onto $R(A)$.*

Proof. It is clear that $R(\bar{A}) = R(A)$. Moreover, if $\bar{A}(u + N(A)) = 0$ then $Au = 0$ by definition, and hence $u \in N(A)$. Thus $N(\bar{A}) = \{0\}$, the zero space of $U/N(A)$. Hence $\bar{A}$ is an isomorphism onto $R(A)$ by Lemma 2.5. □

Definition 2.18.

(a) $\operatorname{null}(A) := \dim N(A)$ is called the *nullity* of A

(b) $\operatorname{rank}(A) := \dim R(A)$ is called the *rank* of A.

Corollary 2.19 (Rank-nullity theorem)**.** *If* $\dim U$ *is finite then*

$$\operatorname{rank}(A) + \operatorname{null}(A) = \dim U.$$

Proof. It follows from Theorem 2.17 together with the dimension theorem, Corollary 2.8, that $\dim(U/N(A)) = \operatorname{rank}(A)$. On the other hand Theorem 2.14 shows that $\dim(U/N(A)) = \dim U - \operatorname{null}(A)$. The corollary follows. □

Basis for Hom

Assume $\dim U = m < \infty$ and $\dim V = n < \infty$. We can then determine a basis for $\operatorname{Hom}(U, V)$ as follows. Let $\{x_1, \dots, x_m\}$ and $\{y_1, \dots, y_n\}$ be bases for U and V. For each pair (i, j) of integers $i = 1, \dots, n$ and $j = 1, \dots, m$ we use Lemma 2.3 to define a linear map $E_{ij} \in \operatorname{Hom}(U, V)$ by extension of

$$E_{ij}(x_k) := \begin{cases} y_i & \text{if} \quad k = j \\ 0 & \text{else.} \end{cases}$$

Theorem 2.20. *The maps E_{ij} constitute a basis for* $\operatorname{Hom}(U, V)$. *In particular,*

$$\dim \operatorname{Hom}(U, V) = \dim(U)\dim(V) < \infty.$$

Proof. Given $A \in \operatorname{Hom}(U, V)$, we expand Ax_k for each k over the basis $\{y_i\}$ to obtain unique scalars α_{ik} such that

$$Ax_k = \sum_i \alpha_{ik} y_i, \quad k = 1, \dots, m. \tag{2.3}$$

The identity

$$A = \sum_{i,j} \alpha_{ij} E_{ij} \tag{2.4}$$

is then easily verified by applying both of its sides to x_k for each k. This proves that the E_{ij} span $\operatorname{Hom}(U, V)$.

If on the other hand we assume (2.4) for some scalars α_{ij}, then (2.3) follows, and as mentioned this determines the scalars uniquely. By Lemma 1.13 the set of the E_{ij} is then a basis for $\operatorname{Hom}(U, V)$. □

This construction of a basis for $\mathrm{Hom}(U, V)$ breaks down in general when U is infinite-dimensional.

Matrix representation

By definition an $n \times m$ matrix over $\mathcal{F}$ is an array with n rows and m columns

$$\mathbf{A} = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nm} \end{pmatrix}.$$

The scalars $\alpha_{ij} \in \mathcal{F}$ are called the *elements* of $\mathbf{A}$. We denote by $\mathrm{M}_{n,m}(\mathcal{F})$ the set of $n \times m$ matrices over $\mathcal{F}$.

Let U and V be finite-dimensional vector spaces, and let some bases $\{x_1, \dots, x_m\}$ and $\{y_1, \dots, y_n\}$ be given together with an ordering of the basis vectors as indicated. For a linear map $A \in \mathrm{Hom}(U, V)$, we then denote the $n \times m$ matrix with the elements α_{ij} from (2.4) by $[A]$.

Definition 2.21. We call $[A] \in \mathrm{M}_{n,m}(\mathcal{F})$ *the matrix of* A with respect to the given ordered bases.

Let us emphasize how $[A]$ is determined from A and the basis vectors.

Lemma 2.22. *The* k*-th column of* $[A]$ *holds the* y*-coordinates of* $Ax_k \in V$.

Proof. This was seen in (2.3). □

The set $M_{n,m}$ is an mn-dimensional vector space over $\mathcal{F}$, when equipped with entry wise addition and scalar multiplication, and it follows from the definition of $[A]$ that with $A \mapsto [A]$ we obtain a linear map into $M_{n,m}$.

Matrix multiplication

There is the following standard rule for the multiplication map

$$\mathrm{M}_{p,n}(\mathcal{F}) \times \mathrm{M}_{n,m}(\mathcal{F}) \to \mathrm{M}_{p,m}(\mathcal{F}).$$

If $\mathbf{B} \in \mathrm{M}_{p,n}$ has elements β_{ij}, and $\mathbf{A} \in \mathrm{M}_{n,m}$ has elements α_{jk}, then the product $\mathbf{BA} \in \mathrm{M}_{p,m}$ has elements γ_{ik} given by

$$\gamma_{ik} = \sum_{j=1}^{n} \beta_{ij} \alpha_{jk}.$$

The elements of $[A]$ are determined through Lemma 2.22. It follows that if $u \in U$ has coordinates $(\alpha_1, \ldots, \alpha_m)$ with respect to $\{x_1, \ldots, x_m\}$ then $Au \in V$ has coordinates $(\beta_1, \ldots, \beta_n)$ with respect to $\{y_1, \ldots, y_n\}$, where the coordinate vectors α and β, regarded as columns (that is, as $m \times 1$ and $n \times 1$ matrices) satisfy the following equation of matrix multiplication

$$\beta = [A]\alpha.$$

Products

Definition 2.23. Let U, V and W are vector spaces over the same field $\mathcal{F}$, and $A \in \mathrm{Hom}(U, V)$, $B \in \mathrm{Hom}(V, W)$. The composed map $B \circ A$, which is easily seen also to be linear, is called the *product* of B and A. It is denoted by $BA \in \mathrm{Hom}(U, W)$.

When the spaces are finite dimensional, and ordered bases are given for U, V, and W we can represent A and B by their matrices. Based on the equation (2.3) for Ax_k in terms of $[A]$ and the companion equation for By_i in terms of $[B]$, one shows by a straightforward calculation that $[BA] = [B][A]$ with the standard multiplication rule for matrices.

In particular, if $U = V = W$ we obtain with the product a map

$$\mathrm{End}(V) \times \mathrm{End}(V) \to \mathrm{End}(V)$$

which is *bilinear*, that is, both maps

$$A \mapsto AB \quad \text{and} \quad B \mapsto AB$$

are linear $\mathrm{End}(V) \to \mathrm{End}(V)$.

Definition 2.24. A vector space $\mathcal{A}$ over $\mathcal{F}$ equipped with a bilinear map $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ is called an *algebra* over $\mathcal{F}$.

Since composition of maps is associative we conclude that $\mathrm{End}(V)$ has the structure of an *associative algebra with unit.* The unit is the identity map $I_V \in \mathrm{End}(V)$. Given an ordered basis for V, the map $A \mapsto [A]$ is an isomorphism of algebras from $\mathrm{End}(V)$ to the matrix algebra $\mathrm{M}_{n,n}(\mathcal{F})$.

Change of basis

Sometimes it is convenient to change from one basis of a vector space to another. There are efficient formulas for this.

Assume $\{x_1, \dots, x_n\}$ and $\{x'_1, \dots, x'_n\}$ are two bases for an n-dimensional vector space V, and let $\mathbf{P}$ be the $n \times n$ matrix whose elements $p_{ij} \in \mathcal{F}$ are the coordinates in

$$x'_j = \sum_i p_{ij} x_i. \tag{2.5}$$

This matrix $\mathbf{P}$ is called the *transition matrix* or the *change of basis matrix.* It is invertible because a comparable matrix relation exists for the opposite change, and the product of the two matrices is then the identity matrix.

The following lemma tells how to change between the coordinates for the two bases.

Lemma 2.25. *If $x = \sum_{i=1}^n \alpha_i x_i = \sum_{j=1}^n \alpha'_j x'_j \in V$ then the column vectors of the coordinates $(\alpha_1, \dots, \alpha_n)$ and $(\alpha'_1, \dots, \alpha'_n)$ satisfy*

$$\alpha = \mathbf{P}\alpha'.$$

Proof. This follows from comparing coefficients to x_i in

$$\sum_{i=1}^n \alpha_i x_i = \sum_{j=1}^n \alpha'_j x'_j = \sum_{i,j=1}^n \alpha'_j p_{ij} x_i. \quad \square$$

The next lemma tells how to change between the matrices representing a given linear map A. We state it for endomorphisms, the generalization to maps between different spaces is obvious.

Lemma 2.26. *If $A \in \mathrm{End}(V)$ is represented by the matrix $[A]$ with respect to the first basis and $[A]'$ with respect to the second, then*

$$[A]' = \mathbf{P}^{-1}[A]\mathbf{P}.$$

Proof. It follows from Lemma 2.25 that coordinates of $x \in V$ are related by

$$\alpha = \mathbf{P}\alpha'$$

and likewise for the coordinates of $Ax \in V$

$$[A]\alpha = \mathbf{P}[A]'\alpha'.$$

Multiplying the first equation by $[A]$ and comparing with the second gives

$$[A]\mathbf{P}\alpha' = \mathbf{P}[A]'\alpha'.$$

Since α' is arbitrary the relation for the matrices follows. $\square$

Two square matrices $\mathbf{A}$ and $\mathbf{B}$ of the same size are called *similar* if

$$\mathbf{A} = \mathbf{P}\mathbf{B}\mathbf{P}^{-1}$$

for some invertible matrix $\mathbf{P}$. It follows that matrices which belong to the same map, but with respect to different bases are similar.

Lecture 3. Duality

Dual space

Let V be a vector space over $\mathcal{F}$. We begin by a definition.

Definition 3.1. The vector space

$$V' := \mathrm{Hom}(V, \mathcal{F}) = \{y : V \to \mathcal{F} \mid y \text{ is linear}\}$$

is called the *dual space* of V and its elements y are called *linear functionals* (or *linear forms*).

Coordinate functionals

Let $B = \{x_i \mid i \in I\}$ be a basis for V, parametrized by an index set I. Recall that every $x \in V$ admits a unique expression as a linear combination

$$x = \sum_{i \in I} \alpha_i x_i,$$

in which we call the scalars α_i the *coordinates* of x with respect to B.

Remark 3.2. As infinite sums are not defined in V, the sum over I needs clarification for the case that V is infinite dimensional. It is required that only finitely many scalars α_i are non-zero, and the sum is defined to extend only over the indices of those terms.

It is easily seen from the uniqueness that the α_i depend linearly on x.

Definition 3.3. Let $i \in I$. The linear functional

$$y_i : \sum_j \alpha_j x_j \mapsto \alpha_i, \qquad V \to \mathcal{F},$$

is called the i'th *coordinate functional.*

By definition we then have

$$x = \sum_{i \in I} y_i(x) x_i, \qquad (x \in V). \tag{3.1}$$

We also see that

$$y_i(x_j) = \delta_{ij} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else.} \end{cases} \tag{3.2}$$

Dual basis

Let $B' := \{y_i \mid i \in I\}$ be the set of coordinate functionals defined above.

Theorem 3.4. *The set B' is linearly independent. If* $\dim V < \infty$ *then*

$$y = \sum_{i \in I} y(x_i) y_i, \qquad (y \in V'), \tag{3.3}$$

and B' is a basis for the dual space V'.

When V is finite-dimensional we call B' the *dual basis* of B. Notice that without the assumption of finite dimension the sum in (3.3) might violate Remark 3.2, since the set of indices with $y(x_i) \neq 0$ can be infinite.

Proof. Assume $0 = \sum_{i \in I} \alpha_i y_i$ for some linear combination in V' (satisfying Remark 3.2 if I is infinite). Then

$$0 = \sum_{i \in I} \alpha_i y_i(x_j) = \sum_{i \in I} \alpha_i \delta_{ij} = \alpha_j$$

for all j. The linear independence follows.

We assume now that V is finite-dimensional, and let $y \in V'$ be given. Then by (3.1) and linearity we obtain

$$y(x) = y\Big(\sum_{i \in I} y_i(x) x_i\Big) = \sum_{i \in I} y_i(x) y(x_i) = \Big(\sum_{i \in I} y(x_i) y_i\Big)(x)$$

for all $x \in V$. This gives (3.3) and also that B' spans V'. □

Corollary 3.5. *If V is finite-dimensional then* $\dim V' = \dim V$. *Otherwise V and V' are both infinite-dimensional.*

Proof. If V is finite-dimensional the theorem shows the identity of dimensions. If V is infinite-dimensional then B' is infinite and linearly independent, and hence V' is also infinite-dimensional. □

Remark 3.6. The fact that B' is a basis for V' in the finite-dimensional case could also have been derived by applying Theorem 2.20 to $\mathrm{Hom}(V, \mathcal{F})$. In the notation used there, the basis vector y_j corresponds to $E_{1,j} \in \mathrm{Hom}(V, \mathcal{F})$.

Annihilator

Let $U \subseteq V$ be a subspace.

Definition 3.7. The subspace

$$U^\circ := \{y \in V' \mid \forall x \in U : y(x) = 0\}$$

of V' is called the *annihilator* of U.

It is easily seen that the annihilator is a subspace of V'. It is related to the quotient space V/U as follows. Let $\pi : V \to V/U$ be the quotient map.

Theorem 3.8. *The map $z \mapsto z \circ \pi$ is an isomorphism of $(V/U)'$ onto U°. In particular, if V is finite-dimensional then*

$$\dim U + \dim U^\circ = \dim V.$$

Proof. Let $A(z) = z \circ \pi$ for $z \in (V/U)'$. It is clear that A is a linear map of $(V/U)'$ into V', and it maps into U° since $z(\pi(x)) = 0$ for $x \in U$. Moreover, if $A(z) = 0$ then $z = 0$ because π is surjective. Hence A is injective.

For any $y \in U^\circ$ we can define a quotient map $\bar{y} : V/U \to \mathcal{F}$ by $\bar{y}(x+U) = y(x)$, since $y(u) = 0$ for $u \in U$. Then $y = A(\bar{y})$, and A is surjective.

It follows that $\dim U^\circ = \dim(V/U)' = \dim V/U$, and we obtain the last statement from Theorem 2.14. □

An extension theorem

Let $U \subseteq V$ be a subspace, and assume V is finite-dimensional. The following theorem allows us to extend a linear functional on U to a linear functional on all of V.

Theorem 3.9. *For each $z \in U'$ there exists $y \in V'$ such that $y(x) = z(x)$ for all $x \in U$.*

Proof. Let $J : V' \to U'$ denote the map of taking restrictions to U, that is, for $y \in V'$ we define

$$J(y)(x) := y(x), \qquad (x \in U). \tag{3.4}$$

This is a linear map. The assertion of the theorem is that it is surjective.

We see from (3.4) that the null-space of J is exactly the annihilator U°. The rank-nullity theorem therefore implies that

$$\dim R(J) + \dim U^\circ = \dim V'.$$

Since $\dim V' = \dim V$ and $\dim U' = \dim U$, it follows from Theorem 3.8 that $\dim R(J) = \dim U'$, and hence J is surjective. □

A similar result, valid for for infinite dimensional spaces with a norm, is called the Hahn-Banach theorem.

A separation theorem

Linear functionals can be used to distinguish elements in V that do not belong to a given subspace. We assume V is finite-dimensional.

Lemma 3.10. *Let $x \in V$ with $x \neq 0$. Then $y(x) \neq 0$ for some $y \in V'$.*

Proof. Let $U \subseteq V$ be the one-dimensional subspace spanned by x, and let $z \in U'$ be given by $z(\alpha x) = \alpha$ for $\alpha \in \mathcal{F}$. Then $y(x) = 1$ for the extension $y \in V'$ given by Theorem 3.9. □

Theorem 3.11. *Let $U \subseteq V$ be a subspace. For each $x \notin U$ there exists a linear form $y \in V'$ which annihilates U but not x. In other words*

$$U = \{x \in V \mid \forall y \in U^\circ : y(x) = 0\}. \tag{3.5}$$

Proof. Let $\pi : V \to V/U$ be the projection map. If $x \notin U$ then $\pi(x) \neq 0$. Hence it follows from Lemma 3.10 that $z(\pi(x)) \neq 0$ for some $z \in (V/U)'$. Let $y = z \circ \pi \in V'$. Then $y \in U^\circ$ and $y(x) \neq 0$.

The last equality is just a restatement of the first part of the theorem. □

Adjoint

Let U, V be vector spaces over $\mathcal{F}$, and let $A \in \mathrm{Hom}(U, V)$ be a linear map from U to V.

Definition 3.12. For $y \in V'$ let $A'y := y \circ A \in U'$, that is,

$$(A'y)(x) = y(Ax), \quad (x \in U).$$

The map $A' : V' \ni y \mapsto A'y \in U'$ is called the *adjoint* of A.

The following properties are straightforward from the definition.

Lemma 3.13. *The adjoint A' belongs to $\mathrm{Hom}(V', U')$ and satisfies*

(1) *$A \mapsto A'$ is linear $\mathrm{Hom}(U, V) \to \mathrm{Hom}(V', U')$,*

(2) *$(AB)' = B'A'$ for $B \in \mathrm{Hom}(U, V)$, $A \in \mathrm{Hom}(V, W)$,*

(3) *$(I_V)' = I_{V'} \in \mathrm{End}(V')$.*

Corollary 3.14. *If A is bijective then so is A', and $(A')^{-1} = (A^{-1})'$.*

Proof. It follows from the lemma that

$$(A^{-1})'A' = (AA^{-1})' = (I_V)' = I_{V'}$$

and

$$A'(A^{-1})' = (A^{-1}A)' = (I_U)' = I_{U'}.$$

The corollary follows. □

Transposed matrix

Assume $\dim U = m$ and $\dim V = n$, both finite, and let bases $\{u_1, \ldots, u_m\}$ for U and $\{x_1, \ldots, x_n\}$ for V be given. Moreover, let the corresponding dual bases be $\{z_1, \ldots, z_m\}$ for U' and $\{y_1, \ldots, y_n\}$ for V'.

Let $A \in \mathrm{Hom}(U, V)$. We will determine the matrix of $A' \in \mathrm{Hom}(V', U')$.

Lemma 3.15. *The matrix $[A']$ for A' with respect to the dual bases is the transpose $[A]^\top$ of $[A]$.*

Recall that the *transpose* of a matrix is defined by

$$\mathbf{A} = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nm} \end{pmatrix} \quad \Rightarrow \quad \mathbf{A}^\top := \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1m} & \ldots & \alpha_{nm} \end{pmatrix}$$

that is, the rows of $\mathbf{A}$ become columns in $\mathbf{A}^\top$.

Proof. The elements α_{ij} of $[A]$ are determined by the expansion

$$Au_j = \sum_{i=1}^{n} \alpha_{ij} x_i \in V, \tag{3.6}$$

and the elements β_{kl} of $[A']$ are determined similarly by

$$A' y_l = \sum_{k=1}^{m} \beta_{kl} z_k \in U'. \tag{3.7}$$

If we apply the linear form y_l to both sides of (3.6), and apply both sides of (3.7) to the vector u_j we obtain with (3.2) that

$$y_l(Au_j) = \sum_{i=1}^{n} \alpha_{ij} y_l(x_i) = \alpha_{lj},$$

and

$$(A' y_l)(u_j) = \sum_{k=1}^{m} \beta_{kl} z_k(u_j) = \beta_{jl}.$$

for all l and j. By definition of A' the left sides of these two identities are equal. Hence $\beta_{jl} = \alpha_{lj}$. □

Null-space of the adjoint

Let $A \in \operatorname{Hom}(U, V)$.

Lemma 3.16. *$N(A') = R(A)^\circ$.*

Proof. Let $y \in V'$. Then

$$A'y = 0 \Leftrightarrow \forall x \in U : (A'y)(x) = 0 \Leftrightarrow \forall x \in U : y(Ax) = 0$$

from which it follows that $y \in N(A') \Leftrightarrow y \in R(A)^\circ$. □

Rank of the adjoint

The following main theorem is now ready for proof. Let $A \in \operatorname{Hom}(U, V)$ and recall that we defined $\operatorname{rank}(A) = \dim R(A)$.

Theorem 3.17. *Assume $\dim V < \infty$. Then $\operatorname{rank}(A') = \operatorname{rank}(A)$.*

Proof. Let $n = \dim V$. Since V' is finite-dimensional the rank-nullity theorem applies to A'. It gives

$$n = \operatorname{rank}(A') + \operatorname{null}(A').$$

On the other hand it follows from Theorem 3.8 and Lemma 3.16 that

$$n = \dim R(A) + \dim R(A)^\circ = \operatorname{rank}(A) + \operatorname{null}(A').$$

The theorem follows. □

Column rank and row rank

Theorem 3.17 has an interesting interpretation in terms of matrices. For a matrix we define its *column rank* as the dimension of the span of its columns, and the *row rank* similarly for the rows. Then obviously the row rank of $\mathbf{A}$ equals the column rank of $\mathbf{A}^\top$.

Let $\mathbf{A}$ be an $n \times m$ matrix. It determines a linear map $A \in \operatorname{Hom}(\mathcal{F}^m, \mathcal{F}^n)$ by

$$A(x) = \mathbf{A}x, \quad (x \in \mathcal{F}^m),$$

where the right hand side is the matrix product with x regarded as an $m \times 1$ matrix. Then $[A] = \mathbf{A}$ with respect to the standard bases for $\mathcal{F}^m$ and $\mathcal{F}^n$.

With this definition we see that the range $R(A) \subseteq \mathcal{F}^n$ of A is exactly the span of the columns of $\mathbf{A}$. We can thus conclude that the column rank of $\mathbf{A}$ is equal to $\operatorname{rank}(A)$. With that we obtain the following corollary from Theorem 3.17 and Lemma 3.15.

Corollary 3.18. *The column rank and the row rank coincide for every matrix* $\mathbf{A}$ *over an arbitrary field* $\mathcal{F}$*.*

Because of this corollary, the column rank and the row rank are jointly dubbed the *rank* of $\mathbf{A}$.

Double dual

The last topic of this lecture concerns the dual space of the dual space of a vector space.

Definition 3.19. The vector space $V'' := (V')'$ is called the *double dual* of V.

There is an easy way to obtain elements in V'':

Lemma 3.20. *Let* $x \in V$*. The map* $y \mapsto y(x)$ *from* V' *to* $\mathcal{F}$ *belongs to* V''*.*

Proof. This just says that $y(x)$ depends linearly on y for every x. This is clear, since $(\alpha y + \beta z)(x) = \alpha y(x) + \beta z(x)$ by definition of the operations in V'. □

Natural correspondence

Definition 3.21. Let $T : V \to V''$ be the map which assigns to each $x \in V$ the linear form $y \mapsto y(x)$ of Lemma 3.20, that is,

$$T(x)(y) := y(x)$$

for $x \in V$ and $y \in V'$. Then T is called the *natural correspondence* from V to V''.

Lemma 3.22. *The natural correspondence* T *is a linear map from* V *to* V''*.*

Proof. This just says that $y(x)$ depends linearly on x for every y. This is evident since $y \in V'$. □

Theorem 3.23. *Assume that* V *is finite-dimensional. Then the natural correspondence* $T : V \to V''$ *is an isomorphism of vector spaces.*

Proof. It follows from Corollary 3.10 that if $x \in V$ is non-zero then $y(x) \neq 0$ for some $y \in V'$. Hence $T(x) \neq 0$. It follows that T is injective. By applying Corollary 3.5 twice we see that $\dim V'' = \dim V$. Hence the injectivity is sufficient to conclude that T is an isomorphism (see Theorem 2.10). □

For an infinite-dimensional space the natural correspondence is injective, but not necessarily surjective. However, if one adds structures of topology and continuity to V, V', and V'' then it is sometimes true. Then V is said to be *reflexive*.

The map T is called 'natural' because its definition does not require a choice of basis for V. If a basis $\{x_1, \ldots, x_n\}$ for V is given we can easily construct an isomorphism from V to V' by declaring that it shall map every basis vector x_i to the dual basis vector y_i with the same index. However, that map will not necessarily be the same if we use a different basis for V. It is only for the double dual that an isomorphism can be defined independently of the choice of a basis.

Double adjoint

The natural correspondence compares well with taking the adjoint. The proof of the following lemma is straightforward from the definitions.

Lemma 3.24. *Let U, V be vector spaces over the same field $\mathcal{F}$ and let $S : U \to U''$ and $T : V \to V''$ be the natural correspondences. Then*

$$A'' \circ S = T \circ A$$

for all $A \in \mathrm{Hom}(U, V)$.

Lecture 4. Bilinear maps

A *bilinear* map is a map of two variables which is linear in each of them separately. More precisely, the definition reads as follows.

Definition 4.1. Let X, Y, V be vector spaces over a common field $\mathcal{F}$. A map $B : X \times Y \to V$ is called *bilinear* if

(a) $x \mapsto B(x, y)$ is linear $X \to V$ for each $y \in Y$,

(b) $y \mapsto B(x, y)$ is linear $Y \to V$ for each $x \in X$.

For later reference we observe that the bilinearity implies

$$B\big(\sum_i \alpha_i x_i, \sum_j \beta_j y_j\big) = \sum_i \alpha_i B\big(x_i, \sum_j \beta_j y_j\big) = \sum_{ij} \alpha_i \beta_j B(x_i, y_j) \qquad (4.1)$$

for all linear combinations from X and Y.

Bilinear forms

A bilinear map into $\mathcal{F}$ is called a *bilinear form*. We denote

$$\mathrm{Bil}(X, Y) := \{\text{bilinear forms } X \times Y \to \mathcal{F}\}.$$

When $Y = X$ we write $\mathrm{Bil}(X) := \mathrm{Bil}(X, X)$.

Examples 4.2. (1) Let $u \in X'$ and $v \in Y'$. Then the product

$$uv : (x, y) \mapsto u(x)v(y)$$

is a bilinear form.

(2) Let $X = \mathcal{F}^m$ and $Y = \mathcal{F}^n$, and consider vectors in $x \in X$ and $y \in Y$ as columns. Let $\mathbf{B}$ be an $m \times n$ matrix with elements $b_{ij} \in \mathcal{F}$. Then

$$B(x, y) := x^t\, \mathbf{B}\, y = \sum_{i,j} \alpha_i b_{ij} \beta_j$$

defines a bilinear form on $X \times Y$. Here (α_i) and (β_j) are the coordinates of x and y.

(3) The form $B(x, y) = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ on $\mathcal{F}^n$ is bilinear.

Multilinearity

The notion of bilinearity admits an obvious generalization to several vector spaces. Let $V_1, \ldots, V_k$ and W be vector spaces over a common field $\mathcal{F}$.

Definition 4.3. A map $V_1 \times \cdots \times V_k \to W$ is *multilinear* if it is linear in each variable. When $W = \mathcal{F}$ it is called a *multilinear form.*

Vector space of bilinear forms

It is easy to see that $\mathrm{Bil}(X, Y)$ is a subspace of the vector space of all functions $X \times Y \to \mathcal{F}$, equipped with the standard addition and scalar multiplication for functions. We will now determine a basis for this vector space.

We assume X and Y are finite-dimensional, say with $\dim X = m$ and $\dim Y = n$. Moreover we fix an ordered basis $\{x_1, \ldots, x_m\}$ for X and an ordered basis $\{y_1, \ldots, y_n\}$ for Y, and we let $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$ be the dual bases for X' and Y'. Then the product

$$w_{i,j} := u_i v_j : (x, y) \mapsto u_i(x) v_j(y)$$

belongs to $\mathrm{Bil}(X, Y)$ for each pair of indices (i, j) (see Example 4.2(1)).

Theorem 4.4. *The set of all the products $w_{i,j}$ is a basis for $\mathrm{Bil}(X, Y)$, and the corresponding expansion of a form $B \in \mathrm{Bil}(X, Y)$ is*

$$B = \sum_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} B(x_i, y_j) w_{i,j}. \tag{4.2}$$

In particular, $\dim \mathrm{Bil}(X, Y) = mn$.

Proof. Let $x = \sum_i \alpha_i x_i \in X$ and $y = \sum_j \beta_j y_j \in Y$ be given. Then by definition

$$w_{i,j}(x, y) = \alpha_i \beta_j$$

and (4.2) follows from (4.1) for all $B \in \mathrm{Bil}(X, Y)$.

On the other hand the coefficients in (4.2) are unique, because

$$B = \sum_{i,j} b_{i,j} w_{i,j}$$

implies $B(x_l, y_k) = \sum_{i,j} b_{i,j} w_{i,j}(x_k, y_l) = b_{k,l}$ for each pair (k, l). □

We say that the matrix $\mathbf{B}$ with entries $B(x_i, y_j)$ *represents* B with respect to the given bases for X and Y. It follows that $B(x, y)$ is given by the formula in Example 4.2(2), when $x \in X$ and $y \in Y$ have coordinates $(\alpha_1, \ldots, \alpha_m)$ and $(\beta_1, \ldots, \beta_n)$ with respect to the bases.

Vector space of k-forms

We define a vector space

$$L^k(V) := \{\text{multilinear forms } \overbrace{V \times \cdots \times V}^{k \text{ times}} \to \mathcal{F}\},$$

which equals $\mathrm{Bil}(V)$ when $k = 2$. The elements of $L^k(V)$ are called *k-forms*.

If $y_1, \dots, y_k$ are linear forms on V we define a k-form $y_1 \cdots y_k \in L^k(V)$ by the product

$$y_1 \cdots y_k(v_1, \dots, v_k) = \Pi_{i=1}^k y_i(v_i) \tag{4.3}$$

for all $v_1, \dots, v_k \in V$. The following theorem is proved analogously to Theorem 4.4.

Theorem 4.5. *Assume V is finite-dimensional. Let $\{x_1, \dots, x_n\}$ be an ordered basis for V, and $\{y_1, \dots, y_n\}$ the dual basis for V'.*

The dimension of $L^k(V)$ is n^k and the set of all products $y_{i_1} \cdots y_{i_k}$ constitutes a basis. Here $i_j = 1, \dots, n$ for each j.

Symmetry and skew-symmetry

We make the following definitions.

Definition 4.6. A bilinear form $B \in \mathrm{Bil}(V)$ is called *symmetric* if

$$B(u, v) = B(v, u), \qquad \text{for all } u, v \in V$$

and *skew-symmetric* (or just *skew*) if

$$B(u, v) = -B(v, u), \qquad \text{for all } u, v \in V.$$

We denote by $\mathrm{Sym}(V)$ and $\mathrm{Skew}(V)$ the subspaces of $\mathrm{Bil}(V)$ consisting of the symmetric, respectively skew-symmetric, bilinear forms.

Characteristic two

For some of the following results we need to assume that the field $\mathcal{F}$ does not have characteristic 2. Let us recall that the *characteristic* of a field $\mathcal{F}$ is the smallest positive number p for which $p = 0$ in $\mathcal{F}$, that is,

$$\overbrace{1 + \cdots + 1}^{p \text{ times}} = 0$$

if such a number exists, and otherwise 0. It is denoted $p = \operatorname{char} \mathcal{F}$.

For the vector spaces $\mathrm{Sym}(V)$ and $\mathrm{Skew}(V)$ there is a spectacular contrast between the cases $p \neq 2$ and $p = 2$. If $p \neq 2$ then

$$\mathrm{Sym}(V) \cap \mathrm{Skew}(V) = \{0\} \tag{4.4}$$

since $B(u, v) = B(v, u) = -B(v, u)$ implies $B(u, v) = 0$, whereas if $p = 2$ then

$$\mathrm{Sym}(V) = \mathrm{Skew}(V)$$

since $-\alpha = \alpha$ for every scalar.

Alternating

Definition 4.7. A bilinear form $B \in \mathrm{Bil}(V)$ is called *alternating* if

$$B(v, v) = 0, \qquad \text{for all } v \in V.$$

We denote by $\mathrm{Alt}(V)$ the subspace of $\mathrm{Bil}(V)$ consisting of the alternating bilinear forms.

Lemma 4.8. $\mathrm{Alt}(V) \subseteq \mathrm{Skew}(V)$*, and if* $\mathrm{char}\,\mathcal{F} \neq 2$ *then* $\mathrm{Alt}(V) = \mathrm{Skew}(V)$.

Proof. Let $B \in \mathrm{Bil}(V)$. Then

$$B(u + v, u + v) - B(u, u) - B(v, v) = B(u, v) + B(v, u). \tag{4.5}$$

If $B \in \mathrm{Alt}(V)$ this implies $B(u, v) + B(v, u) = 0$ and hence B is skew.

Conversely, assume $\mathrm{char}\,\mathcal{F} \neq 2$ and let $B \in \mathrm{Skew}(V)$. The skew-symmetry implies $B(v, v) = -B(v, v)$, and hence $B(v, v) = 0$ for all $v \in V$. □

Quadratic forms

One important motivation for considering symmetric bilinear forms is their relation to quadratic forms. Quadratic forms on $\mathcal{F}^n$ are functions which are given by homogeneous polynomials of degree two in the coordinates. For a general vector space V over $\mathcal{F}$ the precise definition is as follows.

Definition 4.9. A *quadratic form* on a vector space V over $\mathcal{F}$ is a function $q : V \to \mathcal{F}$ for which there exists $B \in \mathrm{Bil}(V)$ such that

$$q(v) = B(v, v)$$

for all $v \in V$. The vector space of all quadratic forms on V is denoted $\mathrm{Quad}(V)$.

Lemma 4.10. *Assume* $\operatorname{char}\mathcal{F} \neq 2$. *The map* $Q : B \mapsto q$ *from* $\operatorname{Bil}(V)$ *to* $\operatorname{Quad}(V)$, *where* $q(v) = B(v, v)$, *restricts to an isomorphism of vector spaces*

$$\operatorname{Sym}(V) \xrightarrow{\sim} \operatorname{Quad}(V).$$

Proof. The map Q is clearly linear $\operatorname{Bil}(V) \to \operatorname{Quad}(V)$. It has null-space $N(Q) = \operatorname{Alt}(V)$. Since $\operatorname{Sym}(V) \cap \operatorname{Alt}(V) = \{0\}$ by (4.4) and Lemma 4.8, the restriction of Q is injective.

For $B \in \operatorname{Bil}(V)$ let $B^t(u, v) := B(v, u)$. Then

$$Q(B) = Q(B^t) = Q(\tfrac{1}{2}(B + B^t))$$

and hence the restriction is also surjective. □

In particular for $V = \mathcal{F}^n$ and $\operatorname{char}\mathcal{F} \neq 2$ all quadratic forms are given by $q(x) = x^t\mathbf{B}x$ where $\mathbf{B}$ is a symmetric matrix, which is uniquely determined by q (see Example 4.2(2)).

Orthogonal vectors

A common feature of symmetric and skew-symmetric forms is the property

$$B(u, v) = 0 \quad \Rightarrow \quad B(v, u) = 0, \qquad (\forall u, v \in V). \tag{4.6}$$

For the following definition we assume $B \in \operatorname{Bil}(V)$ satisfies (4.6).

Definition 4.11. Two vectors $u, v \in V$ are said to be *orthogonal* to each other if $B(u, v) = 0$. When this is the case we write $u \perp v$.

The term *perpendicular* is used for the same property, and for this reason the symbol $\perp$ is called *perp*. The assumption of (4.6) ensures that the relation of being orthogonal is symmetric. For any subset $M \subseteq V$ we define

$$M^{\perp} := \{v \in V \mid v \perp w,\ \forall w \in M\}.$$

This is a subspace of V.

Diagonability of symmetric forms

We assume that V is finite-dimensional and that $\operatorname{char}\mathcal{F} \neq 2$.

Theorem 4.12. *Let* $B \in \operatorname{Sym}(V)$. *There exists a basis for* V *which is orthogonal with respect to* B.

The matrix that represents B with respect to such a basis is diagonal.

Proof. The proof is by induction on $n = \dim V$. If $n = 0$ or if $B = 0$ there is nothing to prove. Assume $n \geq 1$ and $B \neq 0$. It follows from Lemma 4.10 that there exists a vector $x \in V$ with $B(x, x) \neq 0$.

Consider the linear form $v \mapsto B(x, v)$ on V. It is non-zero, and hence by rank-nullity its null-space $N := \{x\}^\perp$ has dimension $n - 1$. The restriction of B to $N \times N$ is symmetric, and hence by induction there is an orthogonal basis for N. Since $x \notin N$ the union of this basis with $\{x\}$ is an orthogonal basis for V. □

Symmetric forms over $\mathbb{C}$

If every element in $\mathcal{F}$ is a square, as it is for example the case for $\mathcal{F} = \mathbb{C}$, we can say more.

Corollary 4.13. *Assume $\alpha \mapsto \alpha^2$ is surjective $\mathcal{F} \to \mathcal{F}$. Then there exists a basis for V which is orthogonal with respect to B, and for which $B(x, x)$ is either* 0 *or* 1 *for every basis vector x.*

Proof. Let $\{x_1, \dots, x_n\}$ be an orthogonal basis. For every index i with $B(x_i, x_i) \neq 0$ we let α_i be a square root of $B(x_i, x_i)$ and normalize the basis vector by $\alpha_i^{-1} x_i$. □

In particular it follows that every quadratic form on V can be written as

$$q(x) = \alpha_1^2 + \cdots + \alpha_m^2 \tag{4.7}$$

with respect to some basis for V. Here $(\alpha_1, \dots, \alpha_n)$ are the coordinates of x for the basis, and $n - m = \dim V^\perp$.

Non-degenerate

Let $B \in \mathrm{Bil}(V)$ and assume (4.6). The subspace

$$V^\perp = \{v \in V \mid B(v, w) = 0, \, \forall w \in V\}$$

consists of the vectors which are orthogonal every vector in V.

Definition 4.14. B is called *non-degenerate* if $V^\perp = \{0\}$.

Symplectic vector spaces

Definition 4.15. A vector space V equipped with a non-degenerate alternating form B is said to be *symplectic.*

We assume that V is finite-dimensional and symplectic. The field $\mathcal{F}$ can be arbitrary.

Theorem 4.16. *There exists an ordered basis* $\{x_1, \dots, x_n, y_1, \dots, y_n\}$ *for* V *such that*

$$\begin{cases} B(x_i, x_j) = B(y_i, y_j) = 0 & \textit{for all } i, j \\ B(x_i, y_j) = 0 & \textit{for all } i \neq j \\ B(x_i, y_i) = 1 & \textit{for all } i. \end{cases} \tag{4.8}$$

In particular, V *is even dimensional.*

Thus, with respect to this basis, B is represented by the $2n \times 2n$ matrix with the following blocks of size $n \times n$

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

Proof. As in the proof of Theorem 4.12 we proceed by induction on V. If $V = \{0\}$ there is nothing to prove. Otherwise, since B is non-degenerate there exists a pair of vectors $x_1, y_1 \in V$ for which $B(x_1, y_1) \neq 0$, and by normalizing an arbitrary one of these vectors we can assume $B(x_1, y_1) = 1$.

Consider the linear map $v \mapsto (B(x_1, v), B(y_1, v))$ from V to $\mathcal{F}^2$. It is surjective since it maps x_1 to $(0, 1)$ and y_1 to $(1, 0)$. Hence by rank-nullity the null-space N has dimension $\dim V - 2$. The restriction of B to $N \times N$ is alternating. By induction there is a basis for N satisfying (4.8).

Together with this basis for N the vectors x_1 and y_1 clearly satisfy (4.8). We claim that they form a basis for V. As there are $\dim V$ vectors it suffices to prove $V = \mathrm{Span}(\{x_1, y_1\} \cup N)$.

Let $x \in V$. Then $z := x - B(x, y_1)x_1 + B(x, x_1)y_1$ belongs to N since

$$B(z, x_1) = B(x, x_1) - B(x, y_1)B(x_1, x_1) + B(x, x_1)B(y_1, x_1) = 0$$

and similarly $B(z, y_1) = 0$. Hence $x \in \mathrm{Span}(\{x_1, y_1\} \cup N)$. □

Symmetric forms over $\mathbb{R}$

Let $B \in \mathrm{Sym}(V)$ for a finite-dimensional vector space V over $\mathbb{R}$. We want to determine a version of Corollary 4.13, which is valid for this case.

Definition 4.17. B is called *positive definite* if $B(x, x) > 0$ for all $x \neq 0$, and *negative definite* if $B(x, x) < 0$ for all $x \neq 0$.

The following theorem is known as Sylvester's 'law of inertia'.

Theorem 4.18. *Let $n = \dim V$ and $n - m = V^{\perp}$. Then there exists a unique integer $0 \leq k \leq m$ and an ordered basis $\{x_1, \dots, x_n\}$ for V such that*

$$B(x_i, x_j) = \begin{cases} 1 & \textit{for } 1 \leq i = j \leq k \\ -1 & \textit{for } k < i = j \leq m \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. The existence follows as in the proof of Corollary 4.13 by normalizing x_i with the square root of $|B(x_i, x_i)|$ when it is non-zero.

Assume that $\{x_1, \dots, x_n\}$ is any ordered basis with the property of B mentioned in the theorem. We will prove that then k is the maximal dimension of any subspace on which the restriction of B is positive definite. This determines k uniquely.

Let $V_+ = \operatorname{Span}\{x_1, \dots, x_k\}$. The restriction of B to this k-dimensional subspace is positive definite. We need to prove that $\dim W \leq k$ for any other subspace W of V on which B restricts to a positive definite form.

Assume W is such a subspace, that is, $B(x, x) > 0$ for all non-zero $x \in W$. Let $U = \operatorname{Span}\{x_{k+1}, \dots, x_n\}$. Then $B(x, x) \leq 0$ for all $x \in U$ and hence only the zero vector belongs to $U \cap W$.

Consider the projection $\pi : V \to V/U$. It has null-space U, and hence its restriction to W is injective. It follows that

$$\dim W = \dim \pi(W) \leq \dim(V/U) = n - (n - k) = k,$$

as we wanted to prove. □

In analogy with (4.7) every quadratic form on V can then be written as

$$q(x) = \alpha_1^2 + \cdots + \alpha_k^2 - \alpha_{k+1}^2 - \cdots - \alpha_m^2 \tag{4.9}$$

with respect to some basis for V.

Quadrics and conics

Definition 4.19. A *quadric* in V is the solution set of a quadratic equation of the form

$$q(x) + y(x) = \text{ constant},$$

where q is a quadratic form and y a linear form. If $\dim V = 2$ quadrics are also called *conics.*

Two quadrics X_1 and X_2 are *equivalent* if $T(X_1) = X_2$ for some map $T : V \to V$ of the form $T(x) = Ax + b$ where $A \in \mathrm{GL}(V)$.

Here we consider the case of $V = \mathbb{R}^n$, and we want to determine the equivalence classes of quadrics. Note that the map T in the above definition corresponds to an affine change of coordinates, that is, a linear transformation together with a new choice of the origin (a translation).

First of all we choose basis vectors so that q takes the form (4.9). Next we eliminate for each $i = 1, \ldots, m$ the coordinate α_i from $y(x)$ by a translation of the coordinate which completes the square. For example, in

$$\alpha_1^2 + \beta\alpha_1 = (\alpha_1 + \beta/2)^2 - \beta^2/4$$

we can remove the linear term $\beta\alpha_1$ by translating the first coordinate by $-\beta/2$. This changes the constant on the right hand side by $\beta^2/4$. If there are no linear terms involving basis vectors x_i with $i > m$, we can scale q so the constant becomes 1, unless it is 0. The resulting form of q is (4.10) below.

On the other hand if there is still a linear term, in which case m must be less than n, we can combine all linear terms in one coordinate x_{m+1} by a linear change involving the last $n - m$ variables. Furthermore we can absorb the constant by a translation in that coordinate. The resulting form of q is (4.11) below.

We have sketched the proof of the following theorem.

Theorem 4.20. *Every real quadric is equivalent to one given by a quadratic equation of the form*

$$\alpha_1^2 + \cdots + \alpha_k^2 - \alpha_{k+1}^2 - \cdots - \alpha_m^2 = 1 \text{ or } 0, \tag{4.10}$$

with $0 \leq k \leq m \leq n$, or by an equation of the form

$$\alpha_1^2 + \cdots + \alpha_k^2 - \alpha_{k+1}^2 - \cdots - \alpha_m^2 = \alpha_{m+1} \tag{4.11}$$

where $0 \leq k \leq m < n$.

With this theorem one can now classify all quadrics. If we leave out all cases with $c = 0$ or $m < n$ in (4.10), or with $m + 1 < n$ in (4.11) (these cases are called *degenerate*), we obtain for dimension 2 the following curves.

Corollary 4.21. *Every non-degenerate real conic is equivalent to*

(1) *the circle $x^2 + y^2 = 1$,*

(2) *the hyperbola $x^2 - y^2 = 1$, or*

(3) *the parabola $x^2 = y$.*

Lecture 5. Sums and products

Sum of subspaces

Let V be a vector space and U, W two subspaces. We call

$$U + W := \operatorname{Span}(U \cup W) = \{u + w \in V \mid u \in U, w \in W\}$$

the *sum* of the subspaces U and W. It is easily seen to be a subspace of V.

Definition 5.1. We say that the sum is *direct*, if for each $v \in U + W$ the vectors $u \in U$, $w \in W$ such that $v = u + w$ are unique. In this case we write $U \oplus W$ for the sum.

We are mainly interested in the situation $V = U \oplus W$. It follows from the definition that this is the case if and only if the map $(u, w) \mapsto u + w$ is a bijection from $U \times W$ onto V.

Example 5.2. If B is a basis for V and $B = C \cup D$ a disjoint union, then V is the direct sum of its subspaces $\operatorname{Span} C$ and $\operatorname{Span} D$. This follows from the unique expansion in Lemma 1.13 of every vector as a linear combination of basis vectors.

Sum and intersection

Theorem 5.3. *The following conditions are equivalent:*

(1) $V = U + W$ *and* $U \cap W = \{0\}$.

(2) $V = U \oplus W$.

Proof. (1)⇒(2): Let $v \in V$. Existence of $v = u + w$ is clear from $V = U + W$. Uniqueness follows since $u + w = u' + w'$ implies $u - u' = w' - w \in U \cap W$.

(2)⇒(1): That $V = U + W$ is clear. Let $x \in U \cap W$. Then $0 = x + (-x)$ with $x \in U$ and $-x \in W$. Hence uniqueness implies $x = 0$. □

Dimensions

Theorem 5.4. *Assume* $V = U \oplus W$. *Then* U *and* W *are finite-dimensional if and only if* V *is finite-dimensional, and in this case*

$$\dim V = \dim U + \dim W. \tag{5.1}$$

Proof. If V is finite-dimensional, then so are its subspaces. Conversely, if U and W are finite-dimensional with bases C and D, respectively, then $C \cap D$ is empty since $U \cap W = \{0\}$. Furthermore, Definition 5.1 and Lemma 1.13 together imply that each $v \in V$ is obtainable as a unique linear combination of $B = C \cup D$. Hence B is a basis for V and (5.1) follows. □

Complement

Let U be a subspace of a vector space V.

Definition 5.5. A subspace W of V for which $V = U \oplus W$ is called a *complement* to U.

Lemma 5.6. *If* $\dim V < \infty$ *then every subspace* U *has a complement.*

Proof. Let C be a basis for U and extend it to a basis B for V. Then $W := \operatorname{Span}(B \setminus C)$ is a complement. □

In fact the lemma holds without the assumption on the dimension (with the same proof, together with a reference to Remark 1.18). On the other hand, a complement is never unique, unless U is $\{0\}$ or V.

Relation to quotient spaces

Here is another characterization of the property.

Theorem 5.7. *We have* $V = U \oplus W$ *if and only if the restriction* $\pi|_W$ *to* W *of the projection* $\pi : V \to V/U$ *is an isomorphism.*

Proof. The restriction of π is surjective if and only if for every coset $v + U$ there exists $w \in W$ such that $v + U = \pi(w)$, that is, every $v \in V$ belongs to the coset $w + U$ for some $w \in W$. This is equivalent to $V = U + W$.

The null-space of π is U and hence the null-space of $\pi|_W$ is $U \cap W$. It follows that $\pi|_W$ is injective if and only if $U \cap W = \{0\}$. □

External direct sum

The sums $U + W$ and $U \oplus W$ are sometimes called *internal* sums. This refers to U and W being subspaces of a common vector space V. The next definition has a different perspective.

Let X and Y be two vector spaces over the same field $\mathcal{F}$. Let

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$$

be the Cartesian product of the sets X and Y.

Lemma 5.8. *Let* $X \times Y$ *be equipped with entry-wise operations of addition and scalar multiplication. It is then a vector space over* $\mathcal{F}$.

Proof. By definition

$$(x, y) + (x', y') = (x + x', y + y'), \qquad \alpha(x, y) = (\alpha x, \alpha y),$$

and $(0, 0)$ is the zero vector. It is straightforward to verify all the axioms. □

Definition 5.9. The vector space of Lemma 5.8 is called the (external) *direct sum* of X and Y.

It follows from the definition that the projections

$$(x, y) \mapsto x \quad \text{and} \quad (x, y) \mapsto y$$

are linear. In particular $X \times \{0\}$ and $\{0\} \times Y$ are subspaces of $X \times Y$, which are canonically isomorphic to X and Y. Since every element $(x, y) \in X \times Y$ decomposes uniquely as

$$(x, y) = (x, 0) + (0, y) \in (X \times \{0\}) + (\{0\} \times Y)$$

it follows from Definition 5.1 that

$$X \times Y = (X \times \{0\}) \oplus (\{0\} \times Y).$$

This justifies the terminology in Definition 5.9, and from now on we shall write $X \oplus Y$ for the external direct sum $X \times Y$.

It follows from Theorem 5.4 that

$$\dim(X \oplus Y) = \dim X + \dim Y$$

if X and Y are finite dimensional.

Projections

Assume $V = U \oplus W$ where U, W are subspaces of V. It follows from Definition 5.1 that we can define a linear map $E \in \operatorname{End}(V)$ by $E(v) = u$ when $v = u + w \in V$ with $u \in U$ and $w \in W$.

Definition 5.10. The map E is called the *projection on U along W*.

There is a certain symmetry between two subspaces that are complementary to each other, and thus it makes sense also to form the projection on W along U. For that we make the elementary observation that if E is the projection on U along W then $I-E$ is the projection on W along U, because if $v = u + w$ with $u = Ev$ then $w = v - u = (I - E)v$.

The subspaces U and W can be detected from the projection as follows.

Lemma 5.11. *If E is the projection on U along W then*

(a) $U = R(E) = N(I - E)$

(b) $W = N(E) = R(I - E)$.

Proof. The statements for $I - E$ follow from those for E by interchanging the subspaces.

(a) By definition E maps into U. For $u \in U$ we have $u = Eu \in R(E)$. Hence $U = R(E)$.

(b) Let $v = u + w \in U + W$. Then $v \in W$ if and only if $u = 0$, that is, if and only if $Ev = 0$. Hence $W = N(E)$. □

Idempotent

Lemma 5.11 suggests that we can study direct sums through the corresponding projections. Motivated by that we want to determine when a linear map is a projection. The condition turns out to be purely algebraic.

Definition 5.12. A linear map $E \in \operatorname{End}(V)$ is called *idempotent* if $E^2 = E$.

Theorem 5.13. *Let V be a vector space and $E \in \operatorname{End}(V)$. Then E is idempotent if and only if it is the projection on U along W for some direct sum $V = U \oplus W$.*

Proof. If $V = U \oplus W$ and E is the projection on U along W then $Ev \in U$ for all $v \in V$ and hence $E(Ev) = Ev$. This shows that E is idempotent.

Conversely, assume $E^2 = E$. Inspired by Lemma 5.11 we let $U = R(E)$ and $W = R(I - E)$. Then $v = Ev + (I - E)v \in U + W$ for every $v \in V$, so that $V = U + W$.

It follows from $E^2 = E$ that $Eu = u$ for $u \in U$. It also follows that $E(I - E) = 0$ and hence $Ew = 0$ for $w \in W$. This shows $U \cap W = \{0\}$. □

Tensor product

Let X and Y be vector spaces over a common field $\mathcal{F}$. We want to define a vector space $X \otimes Y$ that can be regarded as a 'product' of X and Y. Specifically we want to be able to form the 'product' $x \otimes y \in X \otimes Y$ for every pair of a vector $x \in X$ and a vector $y \in Y$. Moreover, we want the distributive law

$$(\alpha_1 x_1 + \alpha_2 x_2) \otimes y = \alpha_1 (x_1 \otimes y) + \alpha_2 (x_2 \otimes y), \tag{5.2}$$

and likewise in the other variable, to be valid for this product.

The theory is simplest for finite-dimensional spaces X and Y, and we will focus mostly on this. In this case the definition is based on the space $\operatorname{Bil}(X, Y)$, but in order to define product vectors $x \otimes y$ in a natural way, we use the dual space $\operatorname{Bil}(X, Y)'$ rather than $\operatorname{Bil}(X, Y)$ itself.

Definition 5.14. Let X and Y be finite-dimensional vector spaces over $\mathcal{F}$. The space

$$X \otimes Y := \operatorname{Bil}(X, Y)'$$

is called the *tensor product* of X and Y, and its elements are called *tensors.*

If $x \in X$ and $y \in Y$ the linear form

$$w \mapsto w(x, y), \quad \operatorname{Bil}(X, Y) \to \mathcal{F}$$

is denoted $x \otimes y \in X \otimes Y$ and called a *pure* (or *elementary*) tensor.

The following lemma ensures the distributive rule for the product $x \otimes y$.

Lemma 5.15. *The map $(x, y) \mapsto x \otimes y$ is bilinear $X \times Y \to X \otimes Y$.*

Proof. Linearity of $x \otimes y$ with respect to x is expressed in (5.2), which is an equality in $\operatorname{Bil}(X, Y)'$. In order to verify this we must apply both sides to an arbitrary form $w \in \operatorname{Bil}(X, Y)$. By definition of $\operatorname{Bil}(X, Y)$ we have

$$w(\alpha_1 x_1 + \alpha_2 x_2, y) = \alpha_1 w(x_1, y) + \alpha_2 w(x_2, y).$$

This is exactly (5.2) applied to w. The proof for y is similar. □

A basis for $X \otimes Y$

As before X and Y are finite-dimensional. Let $m = \dim X$ and $n = \dim Y$, and let $\{x_1, \dots, x_m\}$ and $\{y_1, \dots, y_n\}$ be bases.

Theorem 5.16. *The dimension of $X \otimes Y$ is mn, and the tensors*

$$x_i \otimes y_j \in X \otimes Y, \quad i = 1, \dots, m; j = 1, \dots, n$$

form a basis for it.

Proof. In Theorem 4.4 we determined a basis $\{w_{i,j}\}$ for $\operatorname{Bil}(X, Y)$, for which the expansion of a form $w \in \operatorname{Bil}(X, Y)$ reads

$$w = \sum_{i,j} w(x_i, y_j) w_{ij}.$$

By definition the dual basis for $\operatorname{Bil}(X, Y)'$ consists of the corresponding coordinate functionals $w \mapsto w(x_i, y_j)$. By Definition 5.14 these are exactly the tensors $x_i \otimes y_j$. □

Since the basis vectors are pure tensors we conclude:

Corollary 5.17. *$X \otimes Y$ is spanned by the set of pure tensors.*

Not every tensor is pure. Tensors which are not of the form $x \otimes y$ for any pair $x \in X, y \in Y$ are said to be *entangled.*

Abstract definition

We now abandon the assumption that X and Y are finite-dimensional and describe a more abstract approach to $X \otimes Y$. It involves a so-called *universal property* (UP), which encodes a property we want the tensor product to have.

All vector spaces considered in what follows are over $\mathcal{F}$. Given three vector spaces U, V, W we let

$$\operatorname{Bil}(U, V; W) := \{\text{bilinear maps } U \times V \to W\}.$$

Definition 5.18. Let X and Y be vector spaces. A *tensor product* of X and Y is pair (T, B) of a vector space T and a bilinear map $B \in \operatorname{Bil}(X, Y; T)$ which has the following property:

(UP) For all vector spaces U is composition $\psi \mapsto \psi \circ B$ a bijection

$$\operatorname{Hom}(T, U) \to \operatorname{Bil}(X, Y; U).$$

The following diagram illustrates (UP) for the pair (T, B):

$$\begin{tikzcd} X \times Y \arrow[r, "B"] \arrow[dr, "a"'] & T \arrow[d, "\forall a \exists ! \psi"] \\ & U \end{tikzcd}$$

Here a denotes a bilinear map.

The main issue with this definition is whether such pairs (T, B) exist and are unique. This is addressed in the following theorem.

Theorem 5.19. (a) *There exists a tensor product (T, B) of X and Y.*

(b) *Let (T, B) and (S, A) be tensor products of X and Y. Then there exists a unique isomorphism $\Psi : T \to S$ such that $A = \Psi \circ B$.*

Proof. We first prove (a) for finite-dimensional spaces. More precisely we will prove that the pair consisting of the space $T = X \otimes Y$ and the bilinear map $B : (x, y) \mapsto x \otimes y$ as defined in Definition 5.14 satisfies (UP).

To see the injectivity of $\psi \mapsto \psi \circ B$ we assume $\psi \circ B = 0$. This means that $\psi(x \otimes y) = 0$ for all $(x, y) \in X \times Y$. Since the pure tensors span $X \otimes Y$ it follows that $\psi = 0$.

To show surjectivity let $a \in \operatorname{Bil}(X, Y; U)$ be given. Choose bases for X and Y as before. We define ψ on the basis vectors for $X \otimes Y$ by $\psi(x_i \otimes y_j) := a(x_i, y_j)$, and extend it to a linear map. Then $\psi \circ B$ and a agree on all pairs (x_i, y_j) of basis vectors. Because they are both bilinear this implies $\psi \circ B = a$.

The proof of (a) for general vector spaces is sketched below.

(b) By applying (UP) for (T, B) with $U = S$ we obtain a unique homomorphism $\Psi \in \text{Hom}(T, S)$ for which $\Psi \circ B = A$.

Likewise, by applying (UP) for (S, A) with $U = T$ we obtain a homomorphism $\Phi \in \text{Hom}(S, T)$ for which $\Phi \circ A = B$.

Now $\Psi \circ \Phi = I_T$ follows from (UP) for (T, B) with $U = T$, and $\Phi \circ \Psi = I_S$ follows from (UP) for (S, A) with $U = S$. Hence Ψ is an isomorphism with inverse Φ. □

It follows from the theorem that tensor products exist, and that they are all isomorphic. We then let $X \otimes Y := T$ and for $x \in X$ and $y \in Y$ we define $x \otimes y := B(x, y) \in T$. The proof of part (a) of the theorem shows that for finite-dimensional spaces this agrees with our previous construction.

Free vector space

In order to prove (a) in general we need the notion of the *free vector space over a set S*. By definition this is a subspace of the vector space of all functions $f : S \to \mathcal{F}$, and it consists of those functions f that have finite support, that is, $f(s) = 0$ for all but finitely many $s \in S$. Clearly this condition is stable for addition and scalar multiplication of functions. We denote this vector space $\text{Free}(S)$.

There is a natural map $s \mapsto \delta_s$ from S into $\text{Free}(S)$, given by $\delta_s(t) = \delta_{s,t}$. It is easily seen that the set of all these functions δ_s is a basis for $\text{Free}(S)$.

Existence

Given two vector spaces X and Y over $\mathcal{F}$ we now let $F = \text{Free}(X \times Y)$, and we define the subspace $R \subseteq F$ as the span of all elements of the following forms

$$\begin{aligned}
&\delta_{(x_1+x_2,y)} - \delta_{(x_1,y)} - \delta_{(x_1,y)} \\
&\delta_{(x,y_1+y_2)} - \delta_{(x,y_1)} - \delta_{(x,y_2)} \\
&\delta_{(\alpha x,y)} - \alpha\delta_{(x,y)} \\
&\delta_{(x,\alpha y)} - \alpha\delta_{(x,y)}.
\end{aligned}$$

Finally we let T be the quotient space $T = F/R$, and for $(x, y) \in X \times Y$ we define $B(x, y) \in T$ as the coset $B(x, y) = \delta_{(x,y)} + R$. The definition of R ensures exactly that B is a bilinear map.

The proof of the existence statement (a) now consists of establishing (UP) for the pair (T, B). We omit details.

Lecture 6. Eigendecomposition

In this lecture we define the notion of eigenvectors and eigenvalues for an endomorphism A. It is one of the most important concepts in linear algebra because it allows us a geometric understanding of the action of A.

Eigenvalues and eigenvectors

Definition 6.1. Let $A \in \operatorname{End}(V)$. For each $\lambda \in \mathcal{F}$ we call

$$V_\lambda := \{x \in V \mid Ax = \lambda x\}$$

the *eigenspace* corresponding to λ. If $V_\lambda \neq \{0\}$ we call λ an *eigenvalue* of A and the non-zero vectors $x \in V_\lambda$ *eigenvectors* for A.

The eigenspace is a subspace of V. In fact it is $V_\lambda = N(A - \lambda I)$. Since A acts on it by scalar multiplication it is obviously an invariant subspace.

Definition 6.2. When V is finite-dimensional we call the set

$$\sigma(A) := \{\lambda \in \mathcal{F} \mid \lambda \text{ is an eigenvalue of } A\}$$

the *spectrum* of A, and $\dim V_\lambda$ the *(geometric) multiplicity* of λ as eigenvalue.

Diagonalisation

An endomorphism $A \in \operatorname{End}(V)$ of a finite-dimensional vector space is called *diagonable* if V is spanned by eigenvectors, or equivalently, if there exists a basis for V consisting of eigenvectors. We see from the definition of the matrix $[A]$ that with respect to such a basis it is diagonal

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

with the eigenvalues of the basis vectors along the diagonal.

Polynomials

We are going to apply polynomials to endomorphisms. To prepare for that we recall the following definitions. Let $\mathcal{F}$ be a field.

Definition 6.3. A *polynomial over $\mathcal{F}$* is an expression of the form

$$p(X) = \sum_{i=0}^{n} \alpha_i X^i = \alpha_0 + \alpha_1 X + ... + \alpha_n X^n$$

where $n \geq 0$, $\alpha_0, \alpha_1, ..., \alpha_n \in \mathcal{F}$, and X is a symbol called the *indeterminate*. The set of all polynomials over $\mathcal{F}$ is denoted $\mathcal{F}[X]$.

The set $\mathcal{F}[X]$ is equipped with term-wise addition and scalar multiplication, by which it becomes an infinite-dimensional vector space over $\mathcal{F}$. Moreover a product can be defined within $\mathcal{F}[X]$ as follows.

If $p(X) = \sum_{i=0}^{n} \alpha_i X^i$ and $q(X) = \sum_{j=0}^{m} \beta_j X^j$ then

$$pq(X) := \sum_{k=0}^{n+m} \sum_{i+j=k} \big(\alpha_i \beta_j\big) X^k$$

With these definitions $\mathcal{F}[X]$ is a *commutative and associative algebra.*

Evaluation

There is a natural map from $\mathcal{F}[X]$ to functions on $\mathcal{F}$ given by *evaluation*: If $p(X) = \sum_{i=0}^{n} \alpha_i X^i$ we define a function $\mathcal{F} \to \mathcal{F}$, also denoted p, by

$$p(\gamma) = \sum_{i=0}^{n} \alpha_i \gamma^i, \quad (\gamma \in \mathcal{F}).$$

In particular, γ is called a *root* of p if $p(\gamma) = 0$.

The motivation for the definition of the product in $\mathcal{F}[X]$ is that the evaluation is multiplicative, that is, $(pq)(\gamma) = p(\gamma)q(\gamma)$ for all $\gamma \in \mathcal{F}$, as the following calculation shows

$$p(\gamma)q(\gamma) = \sum_i \alpha_i \gamma^i \sum_j \beta_j \gamma^j = \sum_k \sum_{i+j=k} \alpha_i \beta_j \gamma^k = (pq)(\gamma). \tag{6.1}$$

Applying a polynomial to an endomorphism

More generally we can also evaluate a polynomial in an endomorphism. This is defined as follows. Let V be a vector space over $\mathcal{F}$ and let $A \in \mathrm{End}(V)$.

Definition 6.4. For each polynomial $p(X) = \sum_{i=0}^{n} \alpha_i X^i \in \mathcal{F}[X]$ we define

$$p(A) = \sum_{i=0}^{n} \alpha_i A^i \in \mathrm{End}(V)$$

where $A^i = A \cdot \dots \cdot A$ is the product of A with itself i times (and $A^0 = I$, the identity map).

Lemma 6.5. *Let $A \in \operatorname{End}(V)$ be given. The map $p \mapsto p(A)$ is a homomorphism of algebras $\mathcal{F}[X] \to \operatorname{End}(V)$.*

Proof. Linearity is evident, and the main statement is then multiplicativity, that is, $(pq)(A) = p(A)q(A)$. This follows by replacing γ with A in the calculation of (6.1). □

For later reference we note that if $x \in V$ is an eigenvector for A with eigenvalue λ, then

$$p(A)x = p(\lambda)x \tag{6.2}$$

for every polynomial $p(X)$.

Algebraically closed field

A field $\mathcal{F}$ is said to be *algebraically closed* if every non-constant polynomial $p(X) \in \mathcal{F}[X]$ has at least one root, that is, if there exists $\lambda \in \mathcal{F}$ with $p(\lambda) = 0$. It is the content of the fundamental theorem of algebra that $\mathbb{C}$ is algebraically closed.

It is a consequence of the theorem of Euclidean division for polynomials that if λ is a root of $p(X)$, then there exists a unique polynomial $q(X)$ such that $p(X) = (X - \lambda)q(X)$. Obviously q has degree one less than p. Hence we see by induction on the degree, that if $\mathcal{F}$ is algebraically closed then every polynomial p of degree $k \geq 1$ can be factored as

$$p(X) = \alpha(X - \lambda_1) \cdots (X - \lambda_k).$$

Moreover, α and the list of scalars $\lambda_1, \dots, \lambda_k$ are unique (up to permutation of the indices).

The set $\{\lambda_1, \dots, \lambda_k\}$ is the set of roots of p. A scalar λ can occur more than once as a λ_j, and the number of times it occurs is called the *multiplicity* of λ as a root of p.

Minimal polynomial

Given an endomorphism $A \in \operatorname{End}(V)$ we are particularly interested in those polynomials which annihilate A, that is, for which $p(A) = 0$. This is because their roots are related to the spectrum of A.

If $p(X) \in \mathcal{F}[X]$ is a polynomial, let $R(p)$ denote the set of its roots.

Lemma 6.6. *$\sigma(A) \subseteq R(p)$ for every polynomial p with $p(A) = 0$.*

Proof. Let $\lambda \in \sigma(A)$ be an eigenvalue with eigenvector x. It follows from equation (6.2) that if $p(A) = 0$ then $p(\lambda)x = 0$. Hence $p(\lambda) = 0$. □

Definition 6.7. Let $\dim V = n < \infty$ and let $A \in \operatorname{End}(V)$. A *minimal polynomial* for A is a non-zero polynomial $p(X) \in \mathcal{F}[X]$ which annihilates A and has minimal degree among all such polynomials.

Note that for a constant polynomial $p(X) = \alpha$ we have $p(A) = \alpha I$. Hence a minimal polynomial is non-constant unless $V = 0$.

Lemma 6.8. *Let* $\dim V = n < \infty$ *and* $A \in \operatorname{End}(V)$. *There exists a minimal polynomial for A, and if p is a minimal polynomial then $\sigma(A) = R(p)$.*

Proof. For the existence it suffices to show that $p(A) = 0$ for some $p \neq 0$. Since $\dim \operatorname{End}(V) = n^2$ the vectors $A^0, A^1, \dots, A^{n^2}$ cannot be linearly independent. This means $\sum_{i=0}^{n^2} \alpha_i A^i = 0$ for some non-trivial linear combination. Hence $p(A) = 0$ for the polynomial $p(X) = \sum_{i=0}^{n^2} \alpha_i X^i$.

Let $p(X)$ be minimal for A and let $\lambda \in R(p)$. Then $p(X) = (X - \lambda)q(X)$ for some polynomial q of degree one less. By minimality of $\deg p$ we have $q(A) \neq 0$. Let $x \in V$ be a vector with $y := q(A)x \neq 0$. Then $(A - \lambda)y = p(A)x = 0$. Hence y is an eigenvector with eigenvalue λ and thus $\lambda \in \sigma(A)$. Hence $R(p) \subseteq \sigma(A)$. The opposite inclusion was shown in Lemma 6.6. □

Existence of eigenvectors

From Lemma 6.8 we derive the following main result of this lecture.

Theorem 6.9. *Assume that $\mathcal{F}$ is algebraically closed and* $0 < \dim V < \infty$. *Let* $A \in \operatorname{End}(V)$. *There exists an eigenvector $x \in V$ for A.*

Proof. Let $p(X)$ be a minimal polynomial for A. Then $\sigma(A) = R(p)$ and $R(p) \neq \emptyset$ since $\mathcal{F}$ is closed and p is non-constant. □

Flag

Definition 6.10. A *flag* in a finite-dimensional vector space V is a chain

$$\{0\} = U_0 \subset \cdots \subset U_i \subset \cdots \subset U_q = V$$

of subspaces inside each other. It is called *full* (or *complete*) if $\dim U_i = i$ for each i. It is called *invariant* for $A \in \operatorname{End}(V)$ if each U_i is A-invariant.

A full flag can easily be constructed by means of a basis for V. Given an ordered basis $\{x_1, \dots, x_n\}$ we let $U_j = \operatorname{Span}\{x_1, \dots, x_j\}$ for $j = 0, 1, \dots, n$. With that we obtain a full flag, which we will say *corresponds* to the basis.

Conversely, every full flag corresponds to some basis (although not a unique one). Namely, given a full flag we can choose the basis vectors consecutively such that $U_j = \operatorname{Span}\{x_1, \dots, x_j\}$ for each $j = 1, \dots, n$.

Triangular matrix

Definition 6.11. An $n \times n$ matrix $\mathbf{A} = (\alpha_{ij})$ is called *upper triangular* if $\alpha_{ij} = 0$ for all $i > j$,

$$\mathbf{A} = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ & \ddots & \vdots \\ 0 & & \alpha_{nn} \end{pmatrix}.$$

Lemma 6.12. *Let $A \in \operatorname{End}(V)$. The matrix $[A]$ with respect to an ordered basis is upper triangular if and only if the corresponding full flag is invariant.*

Proof. Recall that $Ax_j = \sum_i \alpha_{ij} x_i$. With $U_j = \operatorname{Span}\{x_1, \dots, x_j\}$ we can then observe that $Ax_j \in U_j$ if and only if $\alpha_{ij} = 0$ for $i > j$.

If the flag is invariant, then this observation immediately implies that $[A]$ is upper triangular. For the converse, assume that $[A]$ is upper triangular. Then $Ax_j \in U_j$ for each j. This implies $Ax_k \in U_k \subseteq U_j$ for every $k \leq j$. Hence

$$A(U_j) = \operatorname{Span}\{Ax_1, \dots, Ax_j\} \subseteq U_j. \quad \square$$

Existence of an invariant flag

The second main result of the lecture is as follows.

Theorem 6.13. *If $\mathcal{F}$ is algebraically closed then every $A \in \operatorname{End}(V)$ admits a full invariant flag and a basis such that $[A]$ is upper triangular.*

Proof. By Lemma 6.12 the existence of the basis follows from the existence of the flag. We will prove the latter by induction on n. If $n = 1$ the trivial flag $\{0\} \subset V$ is both full and invariant, so let us assume $n > 1$.

Let $A' \in \operatorname{End}(V')$ be the adjoint of A. According to Theorem 6.9 there exists an eigenvector $y \in V'$ for A'. Let $U_{n-1} := N(y) \subset V$ be its null-space. Since $y \neq 0$ its range as a linear map $V \to \mathcal{F}$ is $\mathcal{F}$ and hence $\dim U_{n-1} = n-1$ by rank-nullity.

The space U_{n-1} is invariant for A. This is seen as follows

$$y(x) = 0 \Rightarrow y(Ax) = (A'y)(x) = \lambda y(x) = 0$$

where λ is the eigenvalue of y. By induction there is then a full invariant flag in U_{n-1}, and together with $U_n = V$ this gives a full invariant flag in V. $\square$

The diagonal elements

Assume $\dim V = n$ and let $\{x_1, \ldots, x_n\}$ be a basis.

Theorem 6.14. *Let $A \in \operatorname{End}(V)$ and assume $[A]$ is upper triangular with diagonal elements $\lambda_1, \ldots, \lambda_n \in \mathcal{F}$. Then $\{\lambda_1, \ldots, \lambda_n\} = \sigma(A)$.*

Proof. As before let $U_j = \operatorname{Span}\{x_1, \ldots, x_j\}$ for $j = 0, \ldots, n$. Since U_{j-1} is invariant and $Ax_j = \lambda_j x_j + \sum_{i<j} \alpha_{ij} x_i$ we see that $A - \lambda_j$ maps U_j into U_{j-1}. Hence $A - \lambda_j$ restricts to an endomorphism of U_j which is not bijective. Its null-space consists of eigenvectors, and hence $\lambda_j \in \sigma(A)$.

Conversely let $\lambda \in \sigma(A)$, and let $x \in V_\lambda$ be an eigenvector. Let $j \geq 1$ be the largest index for which $x \notin U_{j-1}$. Then U_j is spanned by x and U_{j-1}, and since $(A - \lambda)x = 0$ we see that $A - \lambda$ also maps U_j into U_{j-1}. Then so does $(A - \lambda) - (A - \lambda_j) = \lambda_j - \lambda$, but this is impossible unless $\lambda_j = \lambda$. □

Invariant subspace reduction

Theorem 6.13 is important because it applies to every endomorphism of V, when $\mathcal{F}$ is algebraically closed. But it does not provide a diagonalisation. For those linear maps that are diagonable we have a much stronger result, called the 'spectral theorem'. The following definitions prepare for the statement of this theorem.

Recall that a subspace $U \subseteq V$ is called A-invariant if $A(U) \subseteq U$.

Definition 6.15. If both subspaces U and W in a direct sum $V = U \oplus W$ are A-invariant then the direct sum is said to *reduce A*.

Such a reduction may not exist, but when it does we can reduce the study of $A \in \operatorname{End}(V)$ to the study of its restrictions to U and W, which are endomorphisms of smaller spaces. If a basis for V is chosen such that the first vectors form a basis for U, and the remaining a basis for W, then the matrix of A is reduced to a matrix consisting of two diagonally placed blocks with zeroes everywhere else

$$[A] = \begin{pmatrix} [A|_U] & 0 \\ 0 & [A|_W] \end{pmatrix}.$$

The reducing projection

The reducing property of $V = U \oplus W$ can be expressed as a property of the corresponding projection on U along W. Recall that if two endomorphisms $A, B \in \operatorname{End}(V)$ satisfy $AB = BA$ we say that they *commute*.

Theorem 6.16. *Let $V = U \oplus W$ be a direct sum with projection E onto U. The following are equivalent for an endomorphism $A \in \operatorname{End}(V)$.*

(a) *$V = U \oplus W$ reduces A*

(b) *E commutes with A.*

Proof. Assume (a), and let $x \in V$ be arbitrary. We write $x = u+w$ according to the given decomposition. Then the invariance of U and W implies $Au \in U$ and $Aw \in W$. Hence $EAx = E(Au + Aw) = Au = AEx$, showing (b).

Assume (b), and note that then also $F := I - E$ commutes with A. Now for $u \in U$ we have $Au = AEu = EAu \in U$, and for $w \in W$ similarly $Aw = AFw = FAw \in W$. It follows that U and W are both invariant. □

Multiple direct sums

We need the notion of a direct sum for more than two subspaces. We extend Definition 5.1 as follows.

Definition 6.17. Let $U_1, \ldots, U_k$ be subspaces of V. We say that their sum

$$U_1 + \cdots + U_k := \operatorname{Span}(U_1 \cup \cdots \cup U_k)$$

is *direct*, and write $U_1 \oplus \cdots \oplus U_k$ for it, if for every $u \in U_1 + \cdots + U_k$ there exist unique vectors $u_i \in U_i$ such that $u = u_1 + \cdots + u_k$.

It follows from Corollary 5.4 by an easy inductive argument that

$$\dim(U_1 \oplus \cdots \oplus U_k) = \dim U_1 + \cdots + \dim U_k$$

if the dimensions are finite. When $U = U_1 \oplus \cdots \oplus U_k$ we define $E_i : U \to U_i$ by

$$E_i(v) = u_1 + \cdots + u_k \mapsto u_i.$$

Thus E_i is the projection to U_i along the sum of the other components.

Direct sum of eigenspaces

The following result shows that eigenvectors for different eigenvalues are linearly independent.

Lemma 6.18. *Let $\lambda_1, \ldots, \lambda_k$ be a finite set of distinct eigenvalues. Then the sum of the eigenspaces*

$$V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k}$$

is a direct sum. Furthermore, for each i the projection

$$E_i : V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k} \to V_{\lambda_i}$$

can be obtained as a polynomial of A, restricted to $V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_k}$.

Proof. We need to show that when $x = \sum_{i=1}^{k} x_i$ is a sum of eigenvectors $x_i \in V_{\lambda_i}$, then each x_i is uniquely determined by x.

We fix an index i and consider the polynomial $p(X) := \prod_{j \neq i}(X - \lambda_j)$. Note that $p(\lambda_j) = 0$ for all $j \neq i$, whereas $p(\lambda_i) \neq 0$ since the eigenvalues are assumed to be distinct. Now (6.2) implies $p(A)x = \sum_j p(A)x_j = p(\lambda_i)x_i$ which shows that x_i is uniquely determined.

It also follows that E_i is the restriction of $p(\lambda_i)^{-1}p(A)$. □

Corollary 6.19. *For every* $A \in \operatorname{End}(V)$ *we have* $\sum_{\lambda \in \sigma(A)} \dim V_\lambda \leq \dim V$. *In particular,* $\sigma(A)$ *has at most* $\dim V$ *many elements.*

Proof. This is immediate from the lemma. □

Decomposition by projections

Lemma 6.20. *Let* $E_1, \dots, E_k \in \operatorname{End}(V)$ *be projections, and let* $U_i = R(E_i)$. *Then*

$$V = U_1 \oplus \cdots \oplus U_k$$

if and only if

$$E_iE_j = 0 \textit{ if } i \neq j, \quad E_1 + \cdots + E_k = I.$$

In this case E_i *is the projection to* U_i *along the sum of the other components.*

Proof. We need to prove that every $v \in V$ admits a unique expansion

$$v = u_1 + \cdots + u_k \tag{6.3}$$

with $u_i \in U_i$ for each i.

For the uniqueness we assume (6.3) for some vectors $u_i \in U_i$. It follows from the equality $E_iE_j = 0$ that $E_iu_j = 0$ for $i \neq j$. Hence by applying E_i to (6.3) we find $E_iv = u_i$, and the uniqueness is shown.

For the existence we just let $u_i = E_iv \in U_i$ for each i and note that (6.3) follows from $E_1 + \cdots + E_k = I$. □

The spectral theorem

Assume V is finite-dimensional. The following theorem summarizes the properties we have shown for a diagonable map.

Theorem 6.21. *Let* $A \in \operatorname{End}(V)$ *and let* $\sigma(A)$ *be its spectrum. Then* A *is diagonable if and only if*

$$V = \oplus_{\lambda \in \sigma(A)} V_\lambda. \tag{6.4}$$

If this is the case, and E_λ *denotes the associated projection map to* V_λ, *then*

(1) $E_\lambda E_\mu = 0$ *for all* $\lambda \neq \mu$

(2) $\sum_{\lambda\in\sigma(A)} E_\lambda = I$

(3) $A = \sum_{\lambda\in\sigma(A)} \lambda E_\lambda$

(4) $p(A) = \sum_{\lambda\in\sigma(A)} p(\lambda)E_\lambda$ *for every polynomial* p

(5) $E_\lambda = p_\lambda(A)$ *for some polynomial* p_λ*, for each* λ

(6) *Let* $B \in \operatorname{End}(V)$*. Then* $BA{=}AB$ *if and only if* $BE_\lambda{=}E_\lambda B$ *for all* λ*.*

Proof. The equivalence with (6.4) follows from Lemma 6.18. (1)-(2) were seen in Lemma 6.20. (3) follows from (2) since $AE_\lambda = \lambda E_\lambda$. (4) was seen in (6.2). (5) was seen in Lemma 6.18. (6) follows from (3) and (5). □

The projections E_λ are called the *spectral projections* of A, and the expansion (3) of A in terms of these is called the *spectral resolution* of A.

The inverse as a polynomial

To prove the existence of eigenvalues in Theorem 6.9 we used Lemma 6.8. Here is another remarkable consequence of that lemma. We assume that V is finite-dimensional over an arbitrary field $\mathcal{F}$.

Theorem 6.22. *Let* $A \in \mathrm{GL}(V)$*. There exists a polynomial* $p \in \mathcal{F}[X]$ *for which* $p(A) = A^{-1}$*.*

Proof. Let $p(X) = \sum_{i=0}^m \alpha_i X^i$ be a minimal polynomial. Since A is invertible, zero is not an eigenvalue and hence not a root of p. It follows that $\alpha_0 \neq 0$. Let us normalize p such that

$$p(X) = 1 + \sum_{i=1}^m \alpha_i X^i.$$

Then $p(A) = 0$ implies

$$I = -\sum_{i=1}^m \alpha_i A^i = A\left(-\sum_{i=1}^m \alpha_i A^{i-1}\right),$$

and hence $A^{-1} = -\sum_{i=1}^m \alpha_i A^{i-1}$. □

Lecture 7. Generalized eigendecomposition

Since not every endomorphism is diagonable we need to generalize the notions of the preceding lecture.

Generalized eigenspaces

Definition 7.1. Let $A \in \mathrm{End}(V)$. For each $\lambda \in \mathcal{F}$ we call

$$M_\lambda := \{x \in V \mid \exists k > 0 : (A - \lambda I)^k x = 0\}$$

the *generalized eigenspace* corresponding to λ, and non-zero vectors in M_λ *generalized eigenvectors* for A.

Note that every eigenvector is a generalized eigenvector, that is $V_\lambda \subseteq M_\lambda$. Moreover, if M_λ is non-zero, then $A - \lambda I$ is not injective because that would imply $(A - \lambda I)^k$ is injective for all $k > 0$. Hence V_λ is non-zero. Thus λ has to be an eigenvalue for generalized eigenvectors to exist, and there is no need to define a notion of 'generalized eigenvalues'.

The generalized eigenspace is an invariant subspace for $A - \lambda I$, and hence also for A. This follows from the fact that by definition

$$M_\lambda = \cup_{k>0} N((A - \lambda I)^k), \tag{7.1}$$

the union of the ascending chain of $(A - \lambda I)$-invariant subspaces

$$N(A - \lambda I) \subseteq \cdots \subseteq N((A - \lambda I)^k) \subseteq \cdots \subseteq V.$$

Definition 7.2. We call $\dim M_\lambda$ the *algebraic multiplicity* of λ.

The restriction of $A - \lambda I$ to $N((A - \lambda I)^k)$ has the property that its k-th power is zero. We are going to study this property of a linear map further.

Nilpotence

Definition 7.3. $A \in \mathrm{End}(V)$ is called *nilpotent* if $A^k = 0$ for some $k > 0$. In this case the least such value of k is the *index of nilpotency* of A.

It follows from the definition that if A is nilpotent, then A is not injective, and hence 0 is an eigenvalue of A (unless $V = \{0\}$). In fact, it is the only eigenvalue, since $Ax = \lambda x$ implies $0 = A^k x = \lambda^k x$, and hence $\lambda = 0$ if $x \neq 0$.

For example, if $\dim V = 3$ and for some basis

$$[A] = \begin{pmatrix} 0 & \alpha & \gamma \\ 0 & 0 & \beta \\ 0 & 0 & 0 \end{pmatrix}$$

then $A^3 = 0$. The next theorem shows that this example is typical.

Strictly triangular

From now on, and for the rest of this lecture we assume $n = \dim V$ is finite. An upper triangular matrix is said to be *strictly upper triangular* if all the diagonal elements are zero.

Theorem 7.4. *Let $A \in \mathrm{End}(V)$. The following are equivalent.*

(a) *A is nilpotent.*

(b) *There exists a full flag*

$$V = U_n \supset U_{n-1} \supset \cdots \supset U_0 = \{0\}$$

with descending action of A, that is, $A(U_j) \subseteq U_{j-1}$ for $j = n, \ldots, 1$.

(c) *There exists a basis for V with respect to which the matrix $[A]$ is strictly upper triangular.*

In particular, if A is nilpotent its index is at most $n = \dim V$.

Proof. Assume (a). We will prove (b) by induction on n. The case $n = 0$ is trivial, so we assume $n > 0$. Since A is not injective, it is not surjective either. Hence $R(A) \subset V$ is a proper subspace. Let $U_{n-1} \subset V$ be an arbitrary codimension one subspace containing $R(A)$. Then U_{n-1} is invariant, and by induction there exists a full flag $U_{n-1} \supset \cdots \supset U_0 = \{0\}$ with descending action. Together with $U_n = V$ this gives (b). Conversely, it is clear that (b) implies $A^n = 0$.

It is easily seen that a full flag has a descending action of A if and only if the vectors of a corresponding basis satisfy $Ax_j \in \mathrm{Span}\{x_1, \ldots, x_{j-1}\}$ for all j. This happens exactly when $[A]$ is strictly upper triangular. Hence (b) and (c) are equivalent. □

Nilpotent-invertible reduction

The following theorem shows for finite-dimensional spaces that being nilpotent is in some sense complementary to being invertible.

Theorem 7.5. *Assume V is finite-dimensional and let $A \in \operatorname{End}(V)$.*

(a) *There exists a unique reduction $V = N \oplus R$, for which $A|_N \in \operatorname{End}(N)$ is nilpotent and $A|_R \in \operatorname{End}(R)$ is invertible.*

(b) *Every invariant subspace $M \subseteq V$, for which $A|_M \in \operatorname{End}(M)$ is nilpotent, is contained in N.*

(c) *Every invariant subspace $S \subseteq V$, for which $A|_S \in \operatorname{End}(S)$ is invertible, is contained in R.*

Proof. (a) For each $k \geq 0$ let $N_k = N(A^k)$ and $R_k = R(A^k)$. These are invariant subspaces and they form an ascending and a descending chain,

$$\{0\} = N_0 \subseteq \dots \subseteq N_k \subseteq \dots$$

and

$$V = R_0 \supseteq \dots \supseteq R_k \supseteq \dots .$$

Let N be the union and R the intersection, respectively, of these chains. Since $\dim V = n < \infty$ there are at most n strict inclusions in each chain, and the chains must eventually stabilize. Hence there exists $q \geq 0$ such that

$$N := \cup_k N_k = N_q \qquad \text{and} \qquad R := \cap_k R_k = R_q.$$

It is clear that $(A|_N)^q = 0$, so that $A|_N$ is nilpotent. It is also clear that $A|_R$ is surjective, since $A(R_q) = R_{q+1}$ and $R_{q+1} = R_q$. Since the dimension is finite this implies that $A|_R$ is invertible.

Let $x \in N \cap R$. Then $A^q x = 0$. Since $A|_R$ is injective it follows that $x = 0$. Hence $N \cap R = \{0\}$. To show $N + R = V$ it now suffices to observe that $\dim N + \dim R = n$ by rank-nullity applied to A^q. Hence $V = N \oplus R$.

Uniqueness of N and R follows from (b) and (c), once they are proved.

(b) If $A|_M$ is nilpotent, then $A^k(M) = \{0\}$ for some k, and $M \subseteq N_k \subseteq N$.

(c) If $A|_S$ is invertible, then $S = A^k(S) \subseteq R_k$ for all k, and $S \subseteq R$. □

Polynomial expression for the projection

Lemma 7.6. *Let $V = N \oplus R$ be the reduction in Theorem 7.5. There exists a polynomial $p \in \mathcal{F}[X]$ such that the projection E on N along R is $E = p(A)$.*

Proof. In Theorem 6.22 we have seen that if an endomorphism is invertible, then the inverse can be obtained by applying a polynomial to the endomorphism. It follows that $(A|_R)^{-1} = q(A|_R)$ for some $q \in \mathcal{F}[X]$.

On the other hand, $(A|_N)^k = 0$ for some $k \geq 0$. Let $p(X) = q(X)^k X^k$. Then

$$p(A)x = q(A)^k A^k x = \begin{cases} 0 & \text{if } x \in N \\ (A|_R)^{-k} A^k x = x & \text{if } x \in R. \end{cases}$$

Hence $p(A) = I - E$ and $E = (1 - p)(A)$. □

Decomposition with remainder

Theorem 7.7. *Assume $E_1, \dots, E_k \in \operatorname{End}(V)$ are projections and that*

$$E_i E_j = 0$$

for all $i \neq j$. Let $U_i = R(E_i)$ and $W_i = N(E_i)$ for each i. Then

$$V = U_1 \oplus \cdots \oplus U_k \oplus (W_1 \cap \cdots \cap W_k)$$

with projections $E_1, \dots, E_k$ and $I - (E_1 + \cdots + E_k)$.

Proof. Let $E = E_1 + \cdots + E_k$. It follows from $E_i^2 = E_i$ and $E_i E_j = 0$ that

$$E^2 = \sum_i E_i^2 + \sum_{i \neq j} E_i E_j = \sum_i E_i = E.$$

Hence E is a projection. Moreover

$$E_i(I - E) = E_i(I - \sum_j E_j) = E_i - E_i^2 = 0.$$

Hence we can apply Lemma 6.20 to $E_1, \dots, E_k$ and $I - E$.

It only remains to show that $R(I - E) = W_1 \cap \cdots \cap W_k$. The inclusion $R(I - E) \subseteq W_1 \cap \cdots \cap W_k$ follows from $E_i(I - E) = 0$. For the opposite inclusion we notice that $R(I - E) = N(E)$ and that $N(E_1) \cap \cdots \cap N(E_k) \subseteq N(E)$ is clear from $E = E_1 + \cdots + E_k$. □

Jordan decomposition

We return to our study of the generalized eigenspaces

$$M_\lambda = \{x \in V \mid \exists k > 0 : (A - \lambda I)^k x = 0\}$$

where $\lambda \in \mathcal{F}$ is an eigenvalue of A. We assume $\dim V < \infty$.

Theorem 7.8. *Let $\lambda_1, \dots, \lambda_m$ be the eigenvalues of A. There exists a unique invariant subspace R such that*

$$V = M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_m} \oplus R. \tag{7.2}$$

Moreover, $A|_R$ has no eigenvectors, and for each $i = 1, \dots, m$ there exists a polynomial $p_i \in \mathcal{F}[X]$ such that $p_i(A)$ is the projection to M_{λ_i} along the other components.

Proof. Observe that $M_i = M_{\lambda_i}$ is exactly the space N of Theorem 7.5 for the map $A - \lambda_i I$. Hence there exists for each i a unique invariant complement R_i to M_i for which $(A - \lambda I)|_{R_i}$ is invertible.

Consider two eigenvalues $\lambda_i \neq \lambda_j$. We claim that $(A - \lambda_i I)|_{M_j}$ is invertible. If this were not the case, then we would have $(A - \lambda_i I)x = 0$ for some non-zero $x \in M_j$. This is impossible, since $Ax = \lambda_i x$ and $x \in M_j$ imply

$$0 = (A - \lambda_j)^k x = (\lambda_i - \lambda_j)^k x.$$

Hence $M_j \subseteq R_i$ by Theorem 7.5(c).

Let $E_i \in \mathrm{End}(V)$ denote the projection to M_i along R_i. Then the inclusion just shown gives $E_i E_j = 0$ for all $j \neq i$. Hence by Theorem 7.7 we have

$$V = M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_m} \oplus (R_1 \cap \cdots \cap R_m).$$

This shows the existence of R in (7.2). Moreover it follows from Lemma 7.6 that $E_i = p_i(A)$ for some polynomial.

Since every eigenvector for A belongs to one of the generalized eigenspaces, there can be no eigenvectors in any complementary space R as in (7.2). This implies for every eigenvalue λ_i that $(A - \lambda_i I)|_R$ is invertible, and hence $R \subseteq R_i$. Hence $R \subseteq R_1 \cap \cdots \cap R_m$, and the uniqueness of R follows by dimension. □

Corollary 7.9. *If $\mathcal{F}$ is algebraically closed then*

$$V = M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_m}.$$

Proof. It was shown in Theorem 6.9 that when the field is algebraically closed, every endomorphism has an eigenvector unless $V = \{0\}$. Hence $R = \{0\}$ in Theorem 7.8. □

Diagonability of restrictions

Before we can proceed with our study of the Jordan decomposition we need some results about diagonable maps.

Lemma 7.10. *Let $A \in \operatorname{End}(V)$ be diagonable, and let $U \subseteq V$ be an invariant subspace. The restriction $A|_U \in \operatorname{End}(U)$ is diagonable.*

Proof. Let $x \in U$, and let $x = \sum_{\lambda \in \sigma(A)} x_\lambda$ be its decomposition as a sum of eigenvectors for A. It suffices to show that $x_\lambda \in U$ for each λ. Recall from Lemma 6.18 that in the eigenspace decomposition $V = \oplus_{\lambda \in \sigma(A)} V_\lambda$ each projection map E_λ can be attained as a polynomial applied to A. It follows that E_λ leaves U invariant. Hence $x_\lambda = E_\lambda x \in U$. □

Simultaneous diagonalisation

Theorem 7.11. *Let $A, B \in \operatorname{End}(V)$ be diagonable and assume that A and B commute. Then there exists a basis for V consisting of vectors which are eigenvectors for both A and B.*

Proof. Let $V = \oplus_{\lambda \in \sigma(A)} V_\lambda$ be the eigenspace decomposition of V for A. We have seen in Theorem 6.21 that the commutation of A and B implies that the spectral projections E_λ of A also commute with B, or equivalently (see Theorem 6.16) that all the A-eigenspaces V_λ are B-invariant. It then follows from Lemma 7.10 that for each λ there exists in V_λ a basis of B-eigenvectors. These vectors are then eigenvectors for both A and B, and by combined over all λ they comprise a basis for V. □

Corollary 7.12. *The sum $A + B$ and the product AB of two commuting diagonable maps A and B is again diagonable.*

Proof. They will both be diagonalized by the basis from Theorem 7.11. □

Commuting nilpotent maps

In analogy with Corollary 7.12 nilpotent maps have the following property.

Lemma 7.13. *The sum $A+B$ and the product AB of two commuting nilpotent maps A and B is again nilpotent.*

Proof. Assume $A^k = 0$ and $B^l = 0$, say with $k \geq l$. Then $(AB)^l = A^l B^l = 0$, which shows that AB is nilpotent. To calculate the powers of $A + B$ we use the binomial formula, which is applicable because A and B commute. Then

$$(A + B)^{k+l} = \sum_{0 \leq j \leq k+l} \binom{k+l}{j} A^j B^{k+l-j} = 0$$

since either $j \geq k$ or $k + l - j \geq l$ for each summand. □

Additive Jordan decomposition

We return to the Jordan decomposition. Here is a more qualitative version. As in Corollary 7.9 we assume $\mathcal{F}$ is algebraically closed.

Theorem 7.14. *Let $A \in \operatorname{End}(V)$.*

(i) *There exists a unique pair of commuting maps $A_d, A_n \in \operatorname{End}(V)$ such that A_d is diagonable, A_n is nilpotent, and*

$$A = A_d + A_n.$$

(ii) *There exist polynomials $p_d, p_n \in \mathcal{F}[X]$ such that $p_d(A) = A_d$ and $p_n(A) = A_n$.*

Proof. Let

$$V = M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_m}$$

be the decomposition in generalized eigenspaces from Corollary 7.9, and let E_i denote the corresponding projection to M_{λ_i}. Recall that each E_i commutes with A and that $E_iE_j = 0$ for $i \neq j$. Let

$$A_d := \sum_i \lambda_i E_i, \qquad A_n := \sum_i (A - \lambda_i I)E_i.$$

Then A_d is diagonable by construction, and A_n is nilpotent because the restriction of $(A - \lambda_i I)$ to $M_{\lambda_i} = R(E_i)$ is nilpotent for each i. Moreover A_d and A_n commute with each other, and $A_d + A_n = A$ because $\sum_i E_i = I$. This proves the existence in (i).

Next we note that (ii) is valid for the pair A_d, A_n just constructed. In fact, since each E_i can be obtained as a polynomial p_i of A we find the desired expressions with $p_d := \sum_i \lambda_i p_i$ and $p_n := 1 - p_d$.

Finally we show the uniqueness. Assume we have $A = A'_d + A'_n$ for another pair as in (i), besides the one constructed above. Since A'_d and A'_n commute with each other they commute also with their sum A. It follows from (ii) that then they also commute with A_d and A_n. Now $A = A_d + A_n = A'_d + A'_n$ implies that

$$A_d - A'_d = A'_n - A_n.$$

It follows from Corollary 7.12 that $A_d - A'_d$ is diagonable, and from Lemma 7.13 that $A'_n - A_n$ is nilpotent. However, a nilpotent map has only the eigenvalue 0, so if it is diagonable it is the zero map. Hence $A'_d = A_d$ and $A'_n = A_n$. □

The preceding theorem can be generalized to certain other fields, including $\mathbb{R}$ (called perfect fields), with appropriate reformulation of the asserted diagonability of A_d. It is then called the *Jordan-Chevalley theorem.* Its proof consists of a reduction to Theorem 7.14 by means of Galois theory.

Lecture 8. Orthogonality

So far we have mostly been concerned with the linear properties of a vector space. We will now add a structure which is essentially geometric, because it relates to angles between vectors.

In this lecture the field $\mathcal{F}$ is always $\mathbb{R}$ or $\mathbb{C}$ unless otherwise noted. We denote the complex conjugation of $\mathbb{C}$ by $\alpha \mapsto \bar{\alpha}$ (and let $\bar{\alpha} = \alpha$ for $\alpha \in \mathbb{R}$).

Inner products

Let V be a vector space over $\mathcal{F}$.

Definition 8.1. A map $\langle \cdot\,, \cdot \rangle : V \times V \to \mathcal{F}$ is an *inner product on* V if

(a) $x \mapsto \langle x, y \rangle$ is linear $V \to \mathcal{F}$ for all $y \in V$

(b) $\langle y, x \rangle = \overline{\langle x, y \rangle}$ for all $x, y \in V$

(c) $\langle x, x \rangle > 0$ for all $x \neq 0$.

A vector space with an inner product is called an *inner product space.*

When $\mathcal{F} = \mathbb{R}$ the conjunction of axioms (a) and (b) is equivalent to $\langle \cdot\,, \cdot \rangle$ being a symmetric bilinear form. On the other hand, when $\mathcal{F} = \mathbb{C}$ an inner product is not bilinear, as it follows from the axioms that it is anti-linear in the second variable, that is,

$$\langle x, \alpha_1 y_1 + \alpha_2 y_2 \rangle = \bar{\alpha}_1 \langle x, y_1 \rangle + \bar{\alpha}_2 \langle x, y_2 \rangle.$$

For $V = \mathcal{F}^n$ the standard dot product $\sum_{i=1}^n \alpha_i \bar{\beta}_i$ is an inner product. The geometric content is that for two unit vectors, the inner product is the cosine of their angle.

Length and orthogonality

Definition 8.2. Let V be an inner product space.

(a) The *length* of a vector $x \in V$ is $\|x\| := \sqrt{\langle x, x \rangle}$.

(b) Two vectors $x, y \in V$ are *orthogonal* if $\langle x, y \rangle = 0$. We write $x \perp y$.

(c) For a subset $X \subseteq V$ we define $X^\perp = \{y \in V \mid \forall x \in X : x \perp y\}$.

Note that the length is positive-homogeneous

$$\|\alpha x\| = |\alpha| \, \|x\|, \qquad \alpha \in \mathcal{F}, x \in V,$$

and that orthogonality is symmetric:

$$x \perp y \Leftrightarrow y \perp x.$$

Pythagoras identity

Lemma 8.3. *If $x \perp y$ then $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.*

Proof. For all $x, y \in V$ we find

$$\|x+y\|^2 = \langle x+y, x+y\rangle = \|x\|^2 + \langle x,y\rangle + \langle y,x\rangle + \|y\|^2. \tag{8.1}$$

Assuming $x \perp y$ the Pythagoras identity follows. □

From (8.1) and its companion

$$\|x-y\|^2 = \langle x-y, x-y\rangle = \|x\|^2 - \langle x,y\rangle - \langle y,x\rangle + \|y\|^2 \tag{8.2}$$

we obtain the following *parallelogram identity* for all $x, y \in V$

$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2). \tag{8.3}$$

Cauchy-Schwarz inequality

Theorem 8.4. *Let $x, y \in V$. Then $|\langle x,y\rangle| \leq \|x\|\,\|y\|$.*

Proof. It suffices to show $|\langle x,y\rangle| \leq 1$ for all unit vectors x and y. In addition we can scale x by a complex scalar of modulus 1 so that $\langle x,y\rangle \in \mathbb{R}$. Then

$$0 \leq \|x \pm y\|^2 = \|x\|^2 + \|y\|^2 \pm 2\langle x,y\rangle = 2(1 \pm \langle x,y\rangle)$$

by (8.1)-(8.2), and hence $|\langle x,y\rangle| \leq 1$. □

The proof shows also that if $|\langle x,y\rangle| = \|x\|\,\|y\|$ then x and y are proportional (and the scaled vectors are equal up to a sign).

Triangle inequality

From the Cauchy-Schwarz inequality we derive another important inequality.

Theorem 8.5. *Let $x, y \in V$. Then $\|x+y\| \leq \|x\| + \|y\|$.*

Proof. It follows from (8.1) and Cauchy-Schwarz that

$$\|x+y\|^2 \leq \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2. \quad \square$$

Orthonormal sets

A subset $X \subseteq V$ is called *orthonormal* if all its vectors are orthogonal to each other and have length one.

Lemma 8.6. *Let X be orthonormal.*

(i) *If $z = \sum_{i=1}^{n} \alpha_i x_i$ with distinct vectors x_i from X then*

$$\alpha_j = \langle z, x_j \rangle, \quad j = 1, \dots, n.$$

(ii) *X is linearly independent.*

(iii) *If X is finite then $y - \sum_{x \in X} \langle y, x \rangle x \in X^{\perp}$ for all $y \in V$.*

Proof. (i) Since $\langle x_i, x_j \rangle = \delta_{ij}$ we find

$$\langle z, x_j \rangle = \langle \sum_{i=1}^{n} \alpha_i x_i, x_j \rangle = \sum_{i=1}^{n} \alpha_i \langle x_i, x_j \rangle = \alpha_j.$$

(ii) If $z = 0$ in (i) then $\alpha_j = 0$ for all j.

(iii) Let $y \in V$ and put $z := \sum_{x \in X} \langle y, x \rangle x$. Then (i) implies $\langle y, x \rangle = \langle z, x \rangle$ for each $x \in X$. Hence $y - z \in X^{\perp}$. □

Note that if X consists of a single unit vector x, the content of (iii) is well-known from plane geometry: The vector $z = \langle y, x \rangle x$ is the projection of y on the line determined by x, and the decomposition

$$y = z + (y - z) \tag{8.4}$$

gives the components of y along the line and orthogonal to the line.

Gram-Schmidt process

Gram-Schmidt orthonormalisation is a procedure to obtain from a set of linearly independent vectors $y_1, \dots, y_n$ an orthonormal set of vectors $x_1, \dots, x_n$ with the property $\operatorname{Span}\{x_1, \dots, x_k\} = \operatorname{Span}\{y_1, \dots, y_k\}$ for each k.

The procedure is recursive. We first normalize y_1 to a unit vector x_1. Then $\operatorname{Span}\{x_1\} = \operatorname{Span}\{y_1\}$. Suppose next that orthonormal vectors $x_1, \dots, x_k$ have been found such that $\operatorname{Span}\{x_1, \dots, x_k\} = \operatorname{Span}\{y_1, \dots, y_k\}$. Then

$$x := y_{k+1} - \sum_{i=1}^{k} \langle y_{k+1}, x_i \rangle x_i \in \{x_1, \dots, x_k\}^{\perp}$$

by (iii). Moreover, this vector is non-zero because

$$y_{k+1} \notin \operatorname{Span}\{y_1, \dots, y_k\} = \operatorname{Span}\{x_1, \dots, x_k\}.$$

Hence we can normalize x and extend our list of vectors x_i by it. We thus obtain orthonormal vectors $x_1, \dots, x_{k+1}$ with the same span as $y_1, \dots, y_{k+1}$.

Orthonormal basis

We are particularly interested in bases which are orthonormal, because the property (i) of Lemma 8.6 makes it easy to determine coordinates of vectors.

Theorem 8.7. *Every finite-dimensional inner product space V contains an orthonormal basis.*

Proof. This follows by applying Gram-Schmidt to any basis for V. □

Orthogonal direct sum

Definition 8.8. An *orthogonal direct sum* in an inner product space V is a direct sum $U \oplus W$ of subspaces for which

$$U \perp W,$$

that is, $u \perp w$ for all $u \in U$, $w \in W$. When $V = U \oplus W$ is orthogonal, we say W is an *orthogonal complement* to U, or *orthocomplement* for short.

Note that $U \perp W$ implies $U \cap W = \{0\}$. Hence a subspace W is an orthogonal complement to U if and only if $V = U + W$ and $U \perp W$. As a matter of fact, $U^\perp$ is the only subspace that can be an orthogonal complement:

Lemma 8.9. *Let $V = U \oplus W$ be an orthogonal direct sum. Then $W = U^\perp$.*

Proof. By assumption $W \subseteq U^\perp$. Let $y \in U^\perp$, and write $y = u + w \in U + W$. Since $w \in U^\perp$ we find $u = y - w \in U \cap U^\perp$. Hence $u = 0$ and $y \in W$. □

However, in general it is not always the case that $U + U^\perp = V$.

Orthogonal projection

Definition 8.10. An *orthogonal projection*, or *orthoprojection* for short, is a projection $E \in \mathrm{End}(V)$ for which

$$R(E) \perp N(E),$$

or equivalently, for which $V = R(E) \oplus N(E)$ is an orthogonal direct sum.

When E is an orthogonal projection it follows from Lemma 8.9 that $N(E) = R(E)^\perp$. Thus there is no need to mention the space along which we project, and we say just that E is the *orthogonal projection onto* $R(E)$.

Best approximation

Let $U \subseteq V$ be a subspace and let $v \in V$. The following theorem gives a significant interpretation of the orthogonal decomposition $v = u + w$ (if it exists), where $u \in U$ and $w \in U^\perp$. It says $u \in U$ provides the best approximation from U to v, with respect to the distance $\|v - u\|$.

Theorem 8.11. *Let $v \in V$ and $u \in U$. Then $v - u \perp U$ if and only if*

Øvelse F2020

$$\|v - u\| = \min_{x \in U} \|v - x\|. \tag{8.5}$$

Proof. Assume $v - u \in U^\perp$ and let $x \in U$. Then $v - u \perp u - x$, and hence

$$\|v - x\|^2 = \|v - u\|^2 + \|u - x\|^2 \geq \|v - u\|^2$$

by Pythagoras.

Conversely, assume the minimality of $\|v - u\|$. To show $v - u \perp U$ it suffices to show $\langle v - u, x\rangle = 0$ for all unit vectors $x \in U$. We apply (8.4) to the vector $y = v - u$. It follows that for $z := \langle v - u, x\rangle x$ we obtain with

$$v - u = z + (v - u - z)$$

an orthogonal decomposition of $v - u$. Hence $\|v - u\|^2 = \|z\|^2 + \|v - u - z\|^2$. Since $u + z \in U$ the minimality (8.5) implies $z = 0$, that is, $\langle v - u, x\rangle = 0$. □

Finite dimensional projections

As mentioned an orthocomplement need not exist. However, for finite dimensions it does exist:

Theorem 8.12. *Assume U is a finite-dimensional subspace of V. Then*

$$V = U \oplus U^\perp.$$

Proof. Clearly U, equipped with the restriction of the inner product, is again an inner product space. Hence by Theorem 8.7 it has an orthonormal basis, say with elements $x_1, \ldots, x_r \in U$. Given $y \in V$ we let

$$u = \sum_{i=1}^{r} \langle y, x_i\rangle x_i. \tag{8.6}$$

Then $u \in U$ and $y - u \in U^\perp$ by Lemma 8.6(iii). Hence $y \in U + U^\perp$. This shows $V = U + U^\perp$ and since $U \cap U^\perp = \{0\}$ the theorem follows. □

It follows from the proof that the orthogonal projection is given by $Ey = u$ in (8.6).

Duality

Let V be a vector space with inner product. The presence of the inner product allows us to view the dual vector space V' in a different light. For each $v \in V$ we define a linear form $\Phi(v) \in V'$ by

$$\Phi(v)(x) := \langle x, v \rangle, \quad (x \in V).$$

With that we obtain a map $\Phi : V \to V'$. It is an anti-linear map (which is the same as linear if $\mathcal{F} = \mathbb{R}$), because the inner product is anti-linear in the second variable.

Theorem 8.13. *Let $z \in V'$.*

(a) *There exists at most one $v \in V$ with $z(x) = \langle x, v \rangle$ for all $x \in V$.*

(b) *If $\dim V < \infty$ then such a vector v exists.*

Proof. If two vectors both satisfy (a) then their difference is orthogonal to all $x \in V$, and hence they are equal.

For (b) we can assume $z \neq 0$. Let $U \subset V$ be the null-space of z. Then $V = U \oplus U^\perp$ by Theorem 8.12, and hence $U^\perp \simeq V/U$ is one-dimensional. Let $v \in U^\perp \setminus \{0\}$. By scaling v appropriately we can arrange that $z(v) = \|v\|^2$. Now $z(x) = \langle x, v \rangle$ holds both for $x \in U$ and for $x = v$, hence for all $x \in V$. □

Corollary 8.14. *Φ is injective. When V is finite-dimensional it is bijective.*

Proof. This is just a restatement of the theorem. □

Adjoint

Recall that for two vector spaces U and V the adjoint of a linear map $A \in \mathrm{Hom}(U, V)$ was defined to be a map $A' \in \mathrm{Hom}(V', U')$ between the dual spaces. In the light of the (anti-linear) isomorphism from Corollary 8.14 an alternative definition of an adjoint can be given for inner product spaces, at least when the dimension is finite. To distinguish it we denote it by A^* instead of A', although essentially it is the same object (except that $A \mapsto A^*$ is now an anti-linear map).

Definition 8.15. Let U, V be inner product spaces over the same field $\mathbb{R}$ or $\mathbb{C}$, and let $A \in \mathrm{Hom}(U, V)$. We say that A *has an adjoint* if there exists $A^* \in \mathrm{Hom}(V, U)$ such that

$$\langle Ax, y \rangle = \langle x, A^* y \rangle, \qquad \forall x \in U, \forall y \in V.$$

When that is the case we call A^* the *adjoint* of A.

Lemma 8.16. *If an adjoint exists, then it is unique. When* $\dim U < \infty$ *then every* $A \in \operatorname{Hom}(U, V)$ *has an adjoint.*

Proof. Let $y \in V$. It follows from Theorem 8.13(a) with $z \in U'$ given by $z(x) = \langle Ax, y\rangle$, that the vector $u = A^*y \in U$ is unique if it exists, and from (b) that it always exists when U is finite-dimensional. □

Properties

The following rules are easily seen from Definition 8.15:

$$(A + B)^* = A^* + B^*, \quad (\alpha A)^* = \bar{\alpha} A^*, \quad (AB)^* = B^* A^*, \quad A^{**} = A.$$

Lemma 8.17. $N(A^*) = R(A)^{\perp}$.

Proof. $A^*y = 0 \Leftrightarrow \forall x : \langle x, A^*y\rangle = 0 \Leftrightarrow \forall x : \langle Ax, y\rangle = 0 \Leftrightarrow R(A) \perp y.$ □

Self-adjoint

From now on we take $U = V$ and $A \in \operatorname{End}(V)$.

Definition 8.18. A map $A \in \operatorname{End}(V)$ is called *self-adjoint* if

$$\langle x, Ay\rangle = \langle Ax, y\rangle, \qquad \forall x, y \in V,$$

or in other words, if it is the adjoint of itself.

If $\mathcal{F} = \mathbb{R}$ the term *symmetric* is often used instead of self-adjoint, and if $\mathcal{F} = \mathbb{C}$ the term *Hermitean* is used.

The matrix of the adjoint

Lemma 8.19. *Let* $A \in \operatorname{End}(V)$ *and let* $[A]$ *be the matrix of* A *with respect to an orthonormal basis for* V*. With respect to that same basis,* $[A^*]$ *is the conjugate transpose of* $[A]$*.*

Proof. Let $x_1, \ldots, x_n$ denote the basis vectors. The i, j entry of of $[A]$ is the i-th coordinate of Ax_j, which by (i) of Lemma 8.6 is $\langle Ax_j, x_i\rangle$. The adjoint then similarly has $\langle A^*x_j, x_i\rangle$ in this entry of $[A^*]$. By definition of A^* this is the conjugate of $\langle Ax_i, x_j\rangle$. □

Characterization of orthogonal projections

Recall from Lecture 5 that the projections are characterized as the idempotent elements of $\mathrm{End}(V)$. The following theorem gives a necessary and sufficient condition for E also to be orthogonal.

Theorem 8.20. *Let $E \in \mathrm{End}(V)$ be a projection. The following conditions are equivalent*

(1) *E is an orthogonal projection,*

(2) *E is self-adjoint.*

Proof. It follows from $E^2 = E$ that $(E^*)^2 = E^*$. Hence E^* is a projection. Assume (1). Then $N(E) = R(E)^\perp = N(E^*)$ by Lemma 8.17. The same argument applied to $I - E$ shows that $R(E) = R(E^*)$. Hence $E^* = E$.

The converse implication is immediate from Lemma 8.17. □

Mutually orthogonal projections

Definition 8.21. Two orthogonal projections $E_1, E_2 \in \mathrm{End}(V)$ are called *mutually orthogonal* if $R(E_1) \perp R(E_2)$. In this case we write $E_1 \perp E_2$.

Note that if E_1 and E_2 are mutually orthogonal then $E_1E_2 = 0$, because the assumption $R(E_1) \perp R(E_2)$ implies $R(E_2) \subseteq R(E_1)^\perp = N(E_1)$.

Theorem 8.22. *Assume $E_1, \ldots, E_k \in \mathrm{End}(V)$ are orthoprojections and that*

$$E_i \perp E_j$$

for all $i \neq j$. Let $E = E_1 + \cdots + E_k$. Then E is an orthoprojection with

$$R(E) = R(E_1) \oplus \cdots \oplus R(E_k)$$

and

$$N(E) = N(E_1) \cap \cdots \cap N(E_k).$$

Proof. This follows from Theorem 7.7 since $E_iE_j = 0$ for all $i \neq j$, as observed before the theorem. □

Inner product preservation

Let U and V be inner product spaces. We are interested in the structure preserving maps from U to V. A linear map $A \in \mathrm{Hom}(U, V)$ is said to *preserve inner products* if $\langle Ax, Ay\rangle = \langle x, y\rangle$ for all $x, y \in U$. A linear isomorphism which preserves inner products is called a *unitary isomorphism.*

Lemma 8.23. *Assume* $\dim U = \dim V < \infty$. *The following are equivalent*

(i) *A preserves inner products*

(ii) *A carries orthonormal bases to orthonormal bases*

(iii) $A^*A = I$

(iv) *A is a unitary isomorphism.*

Proof. This is easy. □

Unitary maps

Definition 8.24. A linear map $A \in \mathrm{End}(V)$ is called *unitary* if it is a unitary isomorphism. When $\mathcal{F} = \mathbb{R}$ the term *orthogonal* is also used.

When $\mathcal{F} = \mathbb{C}$ the set of unitary maps in $\mathrm{End}(V)$ is denoted $\mathrm{U}(V)$ and called the *unitary group* of V. When $\mathcal{F} = \mathbb{R}$ it is denoted $\mathrm{O}(V)$, and called the *orthogonal group* of V (these are easily seen to be subgroups of $\mathrm{GL}(V)$).

For a square matrix over $\mathcal{F}$ the same terms as in Definition 8.24 are used when it satisfies one and hence both of the identities

$$\mathbf{A}^*\mathbf{A} = \mathbf{I} \quad \text{and} \quad \mathbf{A}\mathbf{A}^* = \mathbf{I}$$

The first identity expresses that columns are orthonormal with respect to the standard dot product on $\mathcal{F}^n$. The second expresses the same for the rows.

Trace

There is a convenient way to equip the space of maps between two inner product spaces with an inner product. The definition involves the trace of a map, and we shall introduce that first. We begin by defining it for matrices.

Definition 8.25. Let $\mathbf{A} = (\alpha_{ij})$ be an $n \times n$ matrix with entries from an arbitrary field $\mathcal{F}$. The sum of the diagonal elements

$$\mathrm{tr}(\mathbf{A}) := \sum_{i=1}^{n} \alpha_{ii}$$

is called the *trace* of $\mathbf{A}$.

The map $\mathbf{A} \mapsto \mathrm{tr}(\mathbf{A})$ is clearly linear from the vector space of $n \times n$ matrices into $\mathcal{F}$. The main property of the trace is the following.

Lemma 8.26. *Let* $\mathbf{A}$ *be* $m \times n$ *and* $\mathbf{B}$ *be* $n \times m$. *Then* $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA})$.

Proof. Let $\mathbf{A} = (\alpha_{ij})$ and $\mathbf{B} = (\beta_{kl})$, then the i-th diagonal element of $\mathbf{AB}$ is $\sum_{j=1}^{n} \alpha_{ij}\beta_{ji}$, and hence

$$\operatorname{tr}(\mathbf{AB}) = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}\beta_{ji}.$$

Similarly

$$\operatorname{tr}(\mathbf{BA}) = \sum_{k=1}^{n}\sum_{l=1}^{m} \beta_{kl}\alpha_{lk}.$$

The two formulas clearly have the same sum. □

Corollary 8.27. *Similar matrices share the same trace, that is, if* $\mathbf{P}$ *is invertible then* $\operatorname{tr}(\mathbf{P}^{-1}\mathbf{AP}) = \operatorname{tr}(\mathbf{A})$.

We can now define the trace of a linear map.

Definition 8.28. Let V be a finite-dimensional vector space, and let $A \in \operatorname{End}(V)$. We define $\operatorname{tr}(A) = \operatorname{tr}([A])$, where the matrix $[A]$ is determined with an arbitrary basis.

It follows from the corollary that the trace is independent of the choice of basis. With an orthonormal basis and Lemma 8.19 we obtain

$$\operatorname{tr}(A^*) = \overline{\operatorname{tr}(A)},$$

since $[A^*]$ has the same diagonal elements, but conjugated.

Inner product on Hom

Theorem 8.29. *Let* U, V *be finite-dimensional inner product spaces over* $\mathbb{R}$ *or* $\mathbb{C}$. *By defining*

$$\langle A, B\rangle = \operatorname{tr}(AB^*)$$

for $A, B \in \operatorname{Hom}(U, V)$ *we obtain an inner product on* $\operatorname{Hom}(U, V)$.

The inner product is called the *Frobenius inner product.*

Proof. It is straightforward to verify the first two axioms of Definition 8.1. For the last axiom we need to show that $\operatorname{tr}(AA^*) > 0$ for $A \neq 0$. We choose orthonormal bases for U and V, and let α_{ij} denote the elements of $[A]$. Then $[A^*]$ has the conjugate transposed elements and hence

$$\operatorname{tr}(AA^*) = \sum_{i,j} \alpha_{ij}\bar{\alpha}_{ij} = \sum_{i,j} |\alpha_{ij}|^2$$

which is > 0 unless all entries are zero. □

Lecture 9. Spectral theorems

Orthogonal diagonability

In this lecture we will derive a main theorem for finite dimensional inner product spaces, the spectral theorem for self-adjoint linear maps.

With the extra structure provided by the inner product, it is reasonable to request of the direct sums, used to reduce A, that they are orthogonal. This is expressed in the following definition.

Definition 9.1. An endomorphism $A \in \operatorname{End}(V)$ of a finite-dimensional inner product space is called *orthogonally diagonable* if there exists an orthonormal basis consisting of eigenvectors, or equivalently, if

$$V = \oplus_{\lambda \in \sigma(A)} V_\lambda$$

is an orthogonal decomposition.

In particular, we obtain the following from Lemma 8.23(ii).

Lemma 9.2. *Let V be a finite-dimensional inner product space for which an orthonormal basis is given. Then $A \in \operatorname{End}(V)$ is orthogonally diagonable if and only if there exists a unitary matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}[A]\mathbf{P}$ is diagonal.*

Each column of $\mathbf{P}$ consists of the coordinates of an eigenvector in the given basis, and the matrix is unitary because these columns are orthonormal.

Orthogonality of eigenspaces

The following lemma is valid both for $\mathcal{F} = \mathbb{R}$ and $\mathcal{F} = \mathbb{C}$, although the first conclusion is empty in the real case.

Lemma 9.3. *Let $A \in \operatorname{End}(V)$ be self-adjoint. Then $\sigma(A) \subseteq \mathbb{R}$ and the eigenspaces of A are orthogonal to each other.*

Proof. Let $x, y \in V$ be eigenvectors with eigenvalues λ and μ, respectively. Then

$$\lambda\langle x, y\rangle = \langle Ax, y\rangle = \langle x, Ay\rangle = \bar{\mu}\langle x, y\rangle.$$

Taking $y = x$ and $\mu = \lambda$ we derive that $\lambda = \bar{\lambda}$, since $\langle x, x\rangle \neq 0$. Having obtained that, we consider $\lambda \neq \mu$ and derive that $\langle x, y\rangle = 0$, since $\lambda \neq \bar{\mu}$. □

Invariance of $W^\perp$

Lemma 9.4. *If a subspace $W \subseteq V$ is A-invariant then $W^\perp$ is A^*-invariant.*

Proof. Let $y \in W^\perp$. Then for each $x \in W$ we find $\langle x, A^*y\rangle = \langle Ax, y\rangle = 0$ since $Ax \in W$. Hence $A^*y \in W^\perp$. □

Spectral theorem for Hermitean maps

Let $\mathcal{F} = \mathbb{C}$ and let V be a finite-dimensional inner product space. Recall that $A \in \operatorname{End}(V)$ is called Hermitean when it is self-adjoint. The following is then the spectral theorem for self-adjoint maps over $\mathbb{C}$.

Theorem 9.5. *Every Hermitean map $A \in \operatorname{End}(V)$ is orthogonally diagonable.*

Proof. Let $W = \oplus_{\sigma(A)} V_\lambda$ be the sum of the eigenspaces. This is an invariant subspace, and by Lemma 9.4 also $W^\perp$ is invariant. The restriction of A to $W^\perp$ has no eigenvectors as they all belong to some V_λ. By Theorem 6.9 this is not possible unless $W^\perp = \{0\}$. □

Normal maps

A complex diagonal matrix is self-adjoint only when its diagonal elements are real. In the complex case self-adjointness is therefore not necessary for orthogonal diagonability, and we would like to determine what is then a necessary and sufficient condition.

A necessary condition can be obtained by observing that all diagonal matrices commute with each other, and in particularly with their conjugate transposes. It follows that every linear map $A \in \operatorname{End}(V)$, which is orthogonally diagonable, will commute with its adjoint. We shall see that when $\mathcal{F} = \mathbb{C}$ (but not when $\mathcal{F} = \mathbb{R}$) this necessary condition is also sufficient for orthogonal diagonalization.

Definition 9.6. A linear map $A \in \operatorname{End}(V)$ is called *normal* if $AA^* = A^*A$.

All self-adjoint maps are normal, but the converse is not true. For example if $A^* = -A$, then A is normal but not self-adjoint (unless it is zero).

Properties

Lemma 9.7. *Let $A \in \operatorname{End}(V)$ be normal.*

(1) $\|Ax\| = \|A^*x\|$ *for all* $x \in V$.

(2) *$N(A) = N(A^*)$.*

(3) *The λ-eigenspace of A equals the $\bar{\lambda}$-eigenspace of A^*, for each $\lambda \in \mathcal{F}$.*

(4) *All eigenspaces of A are orthogonal to each other.*

Proof. (1) Follows from $\langle Ax, Ax\rangle = \langle x, A^*Ax\rangle = \langle x, AA^*\rangle = \langle A^*x, A^*x\rangle$.

(2) Follows from (1).

(3) Follows from (2) because $(A - \lambda)^* = A^* - \bar{\lambda}$.

(4) Let $x \in V_\mu$ and $y \in V_\lambda$ with $\lambda \neq \mu$. Then $\langle x, y\rangle = 0$ because it follows from (3) that $\lambda\langle x, y\rangle = \langle x, \bar{\lambda}y\rangle = \langle x, A^*y\rangle = \langle Ax, y\rangle = \mu\langle x, y\rangle$. □

In particular, (2) has the following consequence.

Lemma 9.8. *Let $A \in \operatorname{End} V$ be nilpotent and normal. Then $A = 0$.*

Proof. Let k be the index of A, and let $x \in V$ with $A^{k-1}x \neq 0$. If $k > 1$ then $A^{k-1}x \in N(A) \cap R(A)$. Since $N(A^*) \perp R(A)$ by Lemma 8.17, it follows from (2) that $N(A) \cap R(A) = \{0\}$. Hence $k = 1$ and $A = 0$. □

Spectral theorem for normal maps

We can now conclude the spectral theorem for normal maps.

Theorem 9.9. *Let $\mathcal{F} = \mathbb{C}$. Every normal map $A \in \operatorname{End}(V)$ is orthogonally diagonable.*

Proof. Recall that V is the direct sum of the generalized eigenspaces M_λ. Since every linear map which commutes with A leaves M_λ invariant, it follows that M_λ is A^*-invariant. This implies that the restriction of A to M_λ is also normal. Therefore the restriction of $A - \lambda$ to M_λ is both nilpotent and normal, hence zero by Lemma 9.8. Thus $M_\lambda = V_\lambda$ for every λ, and A is diagonable. By Lemma 9.7 it is also orthogonally diagonable. □

The theorem is not valid over $\mathbb{R}$. For example, the 2×2 matrix

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

has no eigenvectors, but it commutes with the adjoint which is $-\mathbf{A}$.

Spectral theorem for symmetric maps

Let $\mathcal{F} = \mathbb{R}$ and let V be a finite-dimensional inner product space. Recall that $A \in \mathrm{End}(V)$ is called symmetric when it is self-adjoint. The proof of the spectral theorem for self-adjoint maps over $\mathbb{C}$ was based on the fundamental theorem of algebra, which is not available for the reals. Nevertheless we shall see that the spectral theorem is valid for symmetric maps.

The following simple lemma will be crucial.

Lemma 9.10. *Let A be symmetric. Then $\sigma(A^2) \subseteq [0, \infty[$.*

Proof. Assume $A^2 x = \lambda x$ and $x \neq 0$. Then $0 \leq \lambda$ since

$$0 \leq \langle Ax, Ax \rangle = \langle A^2 x, x \rangle = \lambda \langle x, x \rangle. \quad \square$$

Lemma 9.11. *Let $V \neq \{0\}$ and $A \in \mathrm{End}(V)$ symmetric. Then there exists an eigenvector.*

Proof. We have seen in Lemma 6.8 that $p(A) = 0$ for some non-zero polynomial $p \in \mathbb{R}[X]$, and that when p is of minimal degree with this property then its set of roots is $\sigma(A)$.

Recall that a polynomial with real coefficients is divisible by

$$(X - \alpha)^2 + \beta^2 = (X - \lambda)(X - \bar{\lambda})$$

if $\lambda = \alpha + i\beta \in \mathbb{C}$ is a root with $\beta \neq 0$.

It follows from Lemma 9.10 that $(A - \alpha I)^2 + \beta^2 I$ is injective, since otherwise $-\beta^2$ would be an eigenvalue for the square of the symmetric map $A - \alpha I$. Hence such a factor $(X - \alpha)^2 + \beta^2$ can be removed from $p(X)$ without disturbing the validity of $p(A) = 0$. By the minimality of p we conclude that all its $\mathbb{C}$-roots belong to $\mathbb{R}$, and hence $\sigma(A) \subseteq \mathbb{R}$. □

Theorem 9.12. *Every symmetric map $A \in \mathrm{End}(V)$ is orthogonally diagonable.*

Proof. It follows from Lemma 9.4 that the orthocomplement of every invariant subspace is invariant. In particular this is then the case for the orthocomplement W of the sum of all eigenspaces. Note that W is itself an inner product space. Moreover, because W is invariant the restriction of A to it is again symmetric.

It now follows from Lemma 9.11 that $W = \{0\}$. Hence A is diagonable, and by Lemma 9.3 then also orthogonally diagonable. □

The orthogonal spectral theorem

We summarize our results about the spectral decomposition in the following theorem.

Theorem 9.13. *Let $\mathcal{F} = \mathbb{R}$ or $\mathbb{C}$ and let $A \in \mathrm{End}(V)$ be self-adjoint, or let $\mathcal{F} = \mathbb{C}$ and A normal. Then*

$$V = \oplus_{\lambda \in \sigma(A)} V_\lambda \tag{9.1}$$

and the associated projection maps E_λ satisfy

(0) *E_λ is self-adjoint for each λ*

(1) *$E_\lambda E_\mu = 0$ for all $\lambda \neq \mu$*

(2) *$\sum_{\lambda \in \sigma(A)} E_\lambda = I$*

(3) *$A = \sum_{\lambda \in \sigma(A)} \lambda E_\lambda$*

(4) *$p(A) = \sum_{\lambda \in \sigma(A)} p(\lambda) E_\lambda$ for every polynomial p*

(5) *$E_\lambda = p_\lambda(A)$ for some polynomial p_λ, for each λ*

(6) *Let $B \in \mathrm{End}(V)$. Then $BA{=}AB$ if and only if $BE_\lambda{=}E_\lambda B$ for all λ.*

Proof. Equation (9.1) was already seen, and (0) is equivalent to the orthogonality of the sum. The rest is taken from Theorem 6.21. □

Functions of maps

Let V be a finite-dimensional inner product space, and let $A \in \mathrm{End}(V)$ be self-adjoint, or normal if $\mathcal{F} = \mathbb{C}$, so that the spectral theorem applies to A. With the following definition we can apply a function to A. It is motivated by property (4) from the spectral theorem, which describes how to apply a polynomial to A.

Definition 9.14. Let $\Omega \subseteq \mathcal{F}$ and let $f : \Omega \to \mathcal{F}$ be any function. When $\sigma(A) \subseteq \Omega$ we define

$$f(A) := \sum_{\lambda \in \sigma(A)} f(\lambda) E_\lambda \in \mathrm{End}(V)$$

where E_λ denotes the spectral projection for the eigenvalue λ.

Here are some properties, which easily follow from the definition

(i) $(f + g)(A) = f(A) + g(A)$.

(ii) $f(A)g(A) = (fg)(A)$.

(iii) If $AB = BA$ then $f(A)B = Bf(A)$.

(iv) $f(A)^* = f^*(A)$ where f^* is defined by $f^*(\alpha) := \overline{f(\alpha)}$.

(v) If A is normal, then so is $f(A)$.

(vi) If $f(\mathbb{R}) \subseteq \mathbb{R}$ and A is self-adjoint then so is $f(A)$.

Square root

Let $A \in \operatorname{End}(V)$ be self-adjoint with non-negative spectrum $\sigma(A) \subset [0, \infty[$.

Theorem 9.15. *There exists a unique $C \in \operatorname{End}(V)$ which is self-adjoint with non-negative spectrum such that $A = C^2$. Moreover, C commutes with every endomorphism which commutes with A.*

Proof. Let $\Omega = [0, \infty[$ and $f(\lambda) = \sqrt{\lambda}$. Then $C = f(A)$ has the mentioned properties. It is unique, because if B is another self-adjoint operator with square A, then B commutes with A and hence with C. The pair of B and C then allows a simultaneous diagonalization. With $\sigma(B) \geq 0$ and $\sigma(C) \geq 0$ it follows from $B^2 = C^2$ that $Bx = Cx$ for every joint eigenvector x. □

The convex hull of the spectrum

Let V be a finite-dimensional inner product space, and let $A \in \operatorname{End}(V)$ be orthogonally diagonable. By using the spectral theorem we can describe the convex hull of $\sigma(A)$. Recall that for a subset S of $\mathcal{F}$ we define the *convex hull* as the set of all convex combinations of S, that is,

$$\operatorname{conv} S := \{\sum_{i=1}^{r} t_i \lambda_i \mid \lambda_i \in S,\, t_i \geq 0,\, t_1 + \cdots + t_r = 1\}.$$

Lemma 9.16. *The convex hull of the spectrum is given by*

$$\operatorname{conv} \sigma(A) = \{\langle Ax, x\rangle \mid \|x\| = 1\}.$$

Proof. Let $A = \sum_{\lambda \in \sigma(A)} \lambda E_\lambda$ be the spectral resolution of A. Then

$$\langle Ax, x\rangle = \sum_{\lambda \in \sigma(A)} \lambda \langle E_\lambda x, x\rangle. \tag{9.2}$$

Since E_λ is a self-adjoint projection we have $\langle E_\lambda x, x\rangle = \|E_\lambda x\|^2 \geq 0$ and $\sum_{\lambda \in \sigma(A)} \langle E_\lambda x, x\rangle = \|x\|^2 = 1$. Hence $\langle Ax, x\rangle \in \operatorname{conv} \sigma(A)$.

Conversely every convex combination $\alpha = \sum_i t_i \lambda_i$ of eigenvalues occurs for some x. Specifically, let x_i be an eigenvector of eigenvalue λ_i and unit length. Then $\alpha = \langle Ax, x\rangle$ for $x = \sum_i \sqrt{t_i} x_i$. □

Rayleigh-Ritz theorem

Assume now that A is self-adjoint. Then $\langle Ax, x\rangle$ is real for every x, and the eigenvalues are real. The expression $\frac{\langle Ax,x\rangle}{\langle x,x\rangle}$, or $\langle Ax, x\rangle$ for a unit vector, is called a *Rayleigh quotient.*

Theorem 9.17. *The smallest and largest eigenvalues are given by*

$$\lambda_{\min} = \min\{\langle Ax, x\rangle \mid \|x\| = 1\}, \quad \lambda_{\max} = \max\{\langle Ax, x\rangle \mid \|x\| = 1\}.$$

Moreover every unit vector x, for which the minimum or maximum occurs, is a corresponding eigenvector.

Proof. The first statement follows from Lemma 9.16 according to which

$$[\lambda_{\min}, \lambda_{\max}] = \{\langle Ax, x\rangle \mid \|x\| = 1\}.$$

The second follows from (9.2). If a weighted average $\sum_{\lambda\in\sigma(A)}\langle E_\lambda x, x\rangle\lambda$ gives an extremal eigenvalue, then all coefficients $\langle E_\lambda x, x\rangle = \|E_\lambda x\|^2$ must be zero except the one in front of the extremal eigenvalue. This implies x belongs to that eigenspace. □

The min-max principle

Not only the extreme eigenvalues but the entire spectrum can be determined by means of the numerical values $\{\langle Ax, x\rangle \mid \|x\| = 1\}$ if one uses more delicate information on how they are distributed over subspaces of V.

Theorem 9.18. *Let V be a finite-dimensional inner product space, and $A \in$ End(V) self-adjoint. For every subspace $W \subseteq V$ let*

$$\mu(W) := \max\{\langle Ax, x\rangle \mid x \in W, \|x\| = 1\}.$$

Number the eigenvalues of A so that $\lambda_1 \leq \cdots \leq \lambda_n$, each repeated according to multiplicity. Then

$$\lambda_k = \min\{\mu(W) \mid \dim W = k\} \tag{9.3}$$

for $k = 1, \dots, n$.

Note that the maximum exists, since it is taken over a compact set. The existence of the minimum is part of the theorem.

Proof. Choose an orthonormal basis of eigenvectors x_i with $Ax_i = \lambda_i x_i$. Let

$$W_k := \operatorname{Span}\{x_1, \dots, x_k\}, \quad U_k := \operatorname{Span}\{x_k, \dots, x_n\}.$$

These are invariant subspaces of dimension k and $n-k+1$, respectively, and with spectra

$$\sigma(A|_{W_k}) = \{\lambda_1, \dots, \lambda_k\}, \quad \sigma(A|_{U_k}) = \{\lambda_k, \dots, \lambda_n\}.$$

First we show that $\mu(W) \geq \lambda_k$ for every subspace W with dimension k. Let W be such a subspace. Then $U_k \cap W \neq \{0\}$ because $\dim U_k + \dim W > n$. Theorem 9.17 applied to $A|_{U_k}$ implies $\langle Ax, x\rangle \geq \lambda_k$ for all $x \in U_k$ with unit length. In particular, this is the case when $x \in U_k \cap W$. We conclude that $\mu(W) \geq \lambda_k$.

Next we show that $\mu(W) = \lambda_k$ for some subspace W with dimension k. Specifically Theorem 9.17 applied to $A|_{W_k}$ gives $\mu(W_k) = \lambda_k$. Hence this is the minimal value of the $\mu(W)$. □

By applying (9.3) to $-A$ a max-min principle is derived. For that the numbering of the eigenvalues is assumed to be the opposite of before, that is, $\lambda_1 \geq \dots \geq \lambda_n$ (so that the eigenvalues of $-A$ are $-\lambda_1 \leq \dots \leq -\lambda_n$). Then

$$\lambda_k = \max\{\nu(W) \mid \dim W = k\}, \tag{9.4}$$

where

$$\nu(W) := \min\{\langle Ax, x\rangle \mid x \in W, \|x\| = 1\}.$$

Lecture 10. Determinants

In this lecture we will associate to every endomorphism of a finite dimensional vector space a scalar called its *determinant*. In order to do that we first need to develop theory of alternating forms.

Alternating forms

Let V be a finite-dimensional vector space with a basis $\{x_1, \ldots, x_n\}$. Recall from Theorem 4.5 that the space $L^k(V)$ of k-linear forms has dimension n^k, and that a basis is given by the set of all products $y_{i_1} \cdots y_{i_k}$ of linear forms from the dual basis.

Definition 10.1. A k-form $w \in L^k(V)$ is called *alternating* if $w(v_1, \ldots, v_k) = 0$ whenever $v_i = v_j$ for some pair of indices $i \neq j$. The vector space of these k-forms is denoted $A^k(V)$.

Here is a convenient characterization. It implies for a finite-dimensional space V that $A^k(V) = \{0\}$ when $k > \dim V$.

Lemma 10.2. *A k-form w is alternating if and only if $w(v_1, \ldots, v_k) = 0$ for all linearly dependent tuples $(v_1, \ldots, v_k) \in V^k$.*

Proof. A tuple $(v_1, \ldots, v_k)$ is linearly dependent if and only if one v_j is a linear combination of the others. In particular, any tuple with a repetition is linearly dependent. Hence the if-statement. For the converse we assume $v_j = \sum_{i \neq j} \alpha_i v_i$ and derive

$$w(v_1, \ldots, v_j, \ldots, v_k) = \sum_{i \neq j} \alpha_i w(v_1, \ldots, v_i, \ldots, v_n) = 0$$

where the v_i is in slot j and thus repeats the v_i in slot i. □

The symmetric group

We want to generalize from bilinear forms the property of being skew. For that we need to recall some basic facts about permutations.

Definition 10.3. Let I be a finite set with k elements. A *permutation* of I is a bijective map $I \to I$, and the group of all permutations, equipped with composition $\sigma \cdot \tau := \sigma \circ \tau$, is called the *symmetric group* of I. It only depends on k, up to isomorphism, and is denoted S_k. A *transposition* is a permutation which interchanges two elements from I and leaves the other unchanged.

The basic properties we need are:

- Every permutation can be obtained as a product of transpositions.
- There is a unique group homomorphism sgn : $S_k \to \{\pm 1\}$ which maps every transposition to -1.

Action on $L^k(V)$

We first define what is an action. Let G be a group and X a set.

Definition 10.4. A (left) *action* of G on X is a map

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

which satisfies $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ and $e \cdot x = x$ for the identity element e.

If in addition X is a vector space and $x \mapsto g \cdot x$ is linear for every $g \in G$, then we speak of a *linear action*.

We apply this with $G = S_k$, considered as the group of permutations of $I = \{1, \dots, k\}$, and with $X = L^k(V)$.

Definition 10.5. For $\sigma \in S_k$ and $w \in L^k(V)$ we define a k-form $\sigma \cdot w$ by

$$\sigma \cdot w(v_1, \dots, v_k) = w(v_{\sigma(1)}, \dots, v_{\sigma(k)}).$$

Lemma 10.6. *The map $(\sigma, w) \mapsto \sigma \cdot w$ is a linear action of S_k on $L^k(V)$*

Proof. It is easy to see that $w \to \sigma \cdot w$ is linear for each $\sigma \in S_k$. We need to verify for each $\tau, \sigma \in S_k$ and $w \in L^k(V)$ that $(\tau\sigma) \cdot w = \tau \cdot (\sigma \cdot w)$.

It is convenient to regard $V^k = V \times \dots \times V$ as the set of maps $I \to V$, that is, we write $v(j)$ instead of v_j, if $v = (v_1, \dots, v_k)$ is a k-tuple from V. Then by definition $(\sigma \cdot w)(v) = w(v \circ \sigma)$ for $v \in V^k$, and hence

$$((\tau\sigma) \cdot w)(v) = w(v \circ \tau\sigma) = (\sigma \cdot w)(v \circ \tau) = (\tau \cdot (\sigma \cdot w))(v). \quad \square$$

Skew forms

We can now define what it means for a k-form to be skew.

Definition 10.7. $w \in L^k(V)$ is called *skew* if $\sigma \cdot w = \operatorname{sgn}(\sigma) w$ for all $\sigma \in S_k$.

Here is then the result that we want.

Theorem 10.8. *Every alternating k-form is skew, and if* $\operatorname{char} \mathcal{F} \neq 2$ *then every skew k-form is alternating.*

Proof. Since S_k acts on $L^k(V)$ and since S_k is generated by transpositions, it follows from the fact that sgn is a homomorphism that w is skew if and only if $\sigma \cdot w = -w$ for all transpositions. Essentially this reduces the proof to the case $k = 2$, which was considered in Lemma 4.8. □

Wedge product

Recall that in (4.3) we defined the multilinear product $y_1 \cdots y_k \in L^k(V)$ of a tuple of linear forms $y_i \in V'$. We want to have also an alternating product.

Definition 10.9. The *wedge product* of $y_1, \ldots, y_k \in V'$ is

$$y_1 \wedge \cdots \wedge y_k := \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\, \sigma \cdot (y_1 \cdots y_k) \in L^k(V).$$

In other words for all k-tuples v from V^k we define

$$(y_1 \wedge \cdots \wedge y_k)(v_1, \ldots, v_k) = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{i=1}^{k} y_i(v_{\sigma(i)}).$$

That $y_1 \wedge \cdots \wedge y_k \in L^k(V)$ is by definition. In fact we have the following.

Lemma 10.10. $y_1 \wedge \cdots \wedge y_k \in A^k(V)$

Proof. For simplicity we assume $\operatorname{char} \mathcal{F} \neq 2$, although the statement is valid also in characteristic 2. Then it suffices to show $y_1 \wedge \cdots \wedge y_k$ is skew.

Let $\tau \in S_k$. Then by definition of the wedges and linearity of the action

$$\tau \cdot (y_1 \wedge \cdots \wedge y_k) = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \tau \cdot (\sigma \cdot (y_1 \cdots y_k)).$$

We substitute $\rho = \tau\sigma$ in the sum over σ and obtain

$$\tau \cdot (y_1 \wedge \cdots \wedge y_k) = \sum_{\rho \in S_k} \operatorname{sgn}(\tau^{-1}\rho) \rho \cdot (y_1 \cdots y_k).$$

Since sgn is a homomorphism and $\operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\tau)$ this implies

$$\tau \cdot (y_1 \wedge \cdots \wedge y_k) = \operatorname{sgn}(\tau) y_1 \wedge \cdots \wedge y_k. \quad \square$$

Basis for $A^k(V)$

We assume V is finite-dimensional and let $\{x_1, \ldots, x_n\}$ be an ordered basis, with dual basis $\{y_1, \ldots, y_n\}$ for V'.

Definition 10.11. For each k-element set $I \subseteq \{1, \ldots, n\}$ we order its elements increasingly and write $I = \{i_1, \ldots, i_k\}$ with $1 \leq i_1 < \cdots < i_k \leq n$. We then define

$$y_I := y_{i_1} \wedge \cdots \wedge y_{i_k} \in A^k(V).$$

Here is the main result about $A^k(V)$.

Theorem 10.12. *Let $0 \leq k \leq n$. The dimension of $A^k(V)$ is $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and the set of all k-forms y_I as above is a basis.*

Proof. It will be convenient to denote by x_I the k-tuple $(x_{i_1}, \ldots, x_{i_k}) \in V^k$ of basis vectors, where again we require increasing order of the indices.

We will first show that for two k-element sets $I, J \subseteq \{1, \ldots, n\}$ we have

$$y_I(x_J) = \delta_{I,J}, \tag{10.1}$$

that is, $y_I(x_J) = 1$ if $I = J$ and 0 otherwise. To see this let $I = \{i_1, \ldots, i_k\}$ and $J = \{j_1, \ldots, j_k\}$ as before. Then $I = J$ if and only if $i_l = j_l$ for all l. Now

$$y_I(x_J) = (y_{i_1} \wedge \cdots \wedge y_{i_k})(x_{j_1}, \ldots, x_{j_k}) = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{l=1}^{k} y_{i_l}(x_{j_{\sigma(l)}})$$

and $y_{i_l}(x_{j_{\sigma(l)}}) = \delta_{i_l, j_{\sigma(l)}}$. Hence the product $\prod_{l=1}^{k} y_{i_l}(x_{j_{\sigma(l)}})$ is non-zero only if $j_{\sigma(l)} = i_l$ for all l. For this we clearly need $J = I$ as sets, but because of the increasing order of the indices also that σ is the trivial permutation. It follows that (10.1) holds as claimed.

We now claim that for every $w \in A^k(V)$ we have $w = \sum_I \alpha_I y_I$ where the sum extends over all k-element sets $I \subseteq \{1, \ldots, n\}$, if and only if $\alpha_I = w(x_I)$ for all I. Clearly this implies that the y_I constitute a basis.

Let $w \in A^k(V)$. For the only-if we just apply $w = \sum_I \alpha_I y_I$ to the tuple x_J and use (10.1). The if-claim amounts to

$$w = \sum_I w(x_I) y_I. \tag{10.2}$$

Since both sides of this identity are multilinear it suffices to establish

$$w(x_{j_1}, \ldots, x_{j_k}) = \sum_I w(x_I) y_I(x_{j_1}, \ldots, x_{j_k})$$

for all k-tuples of basis vectors, and since both sides are also alternating we can assume that the elements $j_1, \ldots, j_k$ of J are distinct. Finally, since both sides are skew we can permute the j's to increasing order. Thus we have reduced the proof of (10.2) to the identity

$$w(x_J) = \sum_I w(x_I) y_I(x_J)$$

which follows from (10.1). □

For later reference we emphasize the following special case of (10.1)

$$(y_1 \wedge \cdots \wedge y_n)(x_1, \ldots, x_n) = 1. \tag{10.3}$$

Top degree

Let $n = \dim V$ as before, and recall that $A^k(V) = \{0\}$ for $k > n$. The alternating forms of the top degree n are particularly interesting.

Corollary 10.13. $\dim A^n(V) = 1$

Proof. Immediate from Theorem 10.12. □

Corollary 10.14. *Let $w \in A^n(V)$ be non-zero, and let $v_1, \dots, v_n \in V$. The tuple $(v_1, \dots, v_n)$ is linearly independent if and only if $w(v_1, \dots, v_n) \neq 0$.*

Proof. Lemma 10.2 shows that $w(v_1, \dots, v_n) \neq 0$ implies linear independence. For the converse we assume $(v_1, \dots, v_n)$ is linear independent. Its vectors then comprise a basis for V, which we can use as the basis $\{x_1, \dots, x_n\}$ applied in Theorem 10.12. As in that theorem we denote the dual basis by $\{y_1, \dots, y_n\}$. Since w is non-zero, Corollary 10.13 implies $w = \alpha\, y_1 \wedge \cdots \wedge y_n$ for some scalar $\alpha \neq 0$. Now (10.3) implies

$$w(v_1, \dots, v_n) = \alpha \neq 0. \quad \square$$

The determinant

The following theorem lists two properties of the determinant which are sufficient to show it is unique.

Theorem 10.15. *There exists for every finite dimensional vector space V a non-trivial map $\det : \mathrm{End}(V) \to \mathcal{F}$ such that the following holds:*

(i) $\det(AB) = \det(A)\det(B)$ *for all $A, B \in \mathrm{End}(V)$.*

(ii) *If $W \subseteq V$ is an A-invariant subspace of codimension one, and α is the scalar by which the quotient map $\bar{A}$ acts on V/W, then*

$$\det(A) = \alpha \det(A|_W).$$

These properties determine the collection of maps $\det\colon \mathrm{End}(V) \to \mathcal{F}$ uniquely.

The existence of the map det is established in Theorem 10.19. Uniqueness will be shown in a later lecture (from Theorem 14.5).

First we will derive from (i) and (ii) some further important properties. Since the map is required to be non-trivial on $\mathrm{End}(V)$, there exists an endomorphism $A \in \mathrm{End}(V)$ with $\det(A) \neq 0$. Then (i) implies for the identity map

$$\det(I) = 1. \tag{10.4}$$

Criterion for invertibility

A main motivation for the determinant is that it detects invertibility.

Theorem 10.16. *A is invertible if and only if* $\det(A) \neq 0$. *Then*

$$\det(A^{-1}) = \det(A)^{-1}.$$

Proof. If A is invertible then (i) and (10.4) imply $\det(A^{-1})\det(A) = 1$. It follows that $\det(A) \neq 0$ and $\det(A^{-1}) = \det(A)^{-1}$.

Assume conversely that A is not invertible. Then $R(A)$ is a proper subspace of V and hence contained in a subspace W of codimension one. It follows from $R(A) \subseteq W$ that W is invariant and also that the quotient map $\bar{A} \in \operatorname{End}(V/W)$ is trivial. Therefore (ii) implies $\det(A) = 0$. □

Further properties

Theorem 10.17. *Let* $A \in \operatorname{End}(V)$.

(a) *If the matrix of A with respect to some basis for V is triangular, then* $\det A$ *is the product of the diagonal elements of that matrix.*

(b) *If $V = U_1 \oplus U_2$ reduces A then* $\det(A) = \det(A|_{U_1})\det(A|_{U_2})$.

Proof. (a). By applying (ii) inductively we obtain

$$\det(A) = \alpha_1 \cdots \alpha_k \det(A|_{W_k}). \tag{10.5}$$

if $\{0\} \subseteq W_k \subset \cdots \subset W_1 \subset W_0 = V$ is an invariant flag, for which the quotients W_j/W_{j-1} are one-dimensional and $\alpha_1, \ldots, \alpha_k$ are the scalars by which A act on them. The result follows after $k = \dim V$ steps.

(b). Let $A_1, A_2 \in \operatorname{End}(V)$ be defined by

$$A_1(u_1 + u_2) = Au_1 + u_2, \qquad A_2(u_1 + u_2) = u_1 + Au_2$$

for $u_i \in U_i$. Then $A = A_1A_2$, and it suffices to show $\det(A_i) = \det(A|_{U_i})$. This results immediately from the following claim:

If $W \subseteq V$ is invariant and $\bar{A} = I$ on V/W, then $\det(A) = \det(A|_W)$.

We use (10.5) with $W_k = W$ and an arbitrary increasing chain of subspaces $W \subset W_{k-1} \subset \cdots \subset W_1 \subset W_0 = V$ with $\dim W_j/W_{j-1} = 1$. Here $\alpha_j = 1$ for each j, since A acts by the identity modulo W, and $W \subseteq W_{j-1}$. □

Existence of the determinant

For $A \in \operatorname{End}(V)$ and $w \in A^k(V)$ we define

$$(\tilde{A}w)(v_1, \ldots, v_k) := w(Av_1, \ldots, Av_k).$$

It is easily seen that $\tilde{A}w$ is alternating and depends linearly on w. Thus we have defined a map $\tilde{A} \in \operatorname{End}(A^k(V))$. In particular, for $k = n = \dim V$ it follows from Corollary 10.13 that $\tilde{A}$ is multiplication by a scalar.

Definition 10.18. The *determinant* $\det(A)$ of A is this scalar. That is

$$w(Av_1, \ldots, Av_n) = \det(A) w(v_1, \ldots, v_n) \tag{10.6}$$

for all $w \in A^n(V)$ and all $v_1, \ldots, v_n$.

Theorem 10.19. *The function* det *satisfies all conditions in Theorem 10.15.*

Proof. It is clear from (10.6) that $\det(I) = 1$, so that det is non-trivial. Also

$$\det(AB) = \det(A)\det(B), \qquad A, B \in \operatorname{End}(V) \tag{10.7}$$

follows immediately from (10.6). This is property (i) of Theorem 10.15.

Let $W \subset V$ be invariant with dimension $n-1$. If we fix v_n we can consider $w(v_1, \ldots, v_n)$ as an alternating form in the variables $v_1, \ldots, v_{n-1}$. By restricting these variables to W, we obtain an element of $A^{n-1}(W)$. By (10.6) for $A|_W$ we then have

$$w(Av_1, \ldots, Av_{n-1}, v_n) = \det(A|_W) w(v_1, \ldots, v_n)$$

for all $v_n \in V$ and $v_1, \ldots, v_{n-1} \in W$.

Let $\{x_1, \ldots, x_n\}$ be a basis for V with $W = \operatorname{Span}\{x_1, \ldots, x_{n-1}\}$. Then

$$w(Ax_1, \ldots, Ax_n) = \det(A|_W)\, w(x_1, \ldots, x_{n-1}, Ax_n). \tag{10.8}$$

Define $\alpha \in \mathcal{F}$ by $Ax_n = \alpha x_n$ modulo W. Then $Ax_n - \alpha x_n$ is spanned by $x_1, \ldots, x_{n-1}$, and $w(x_1, \ldots, x_{n-1}, Ax_n - \alpha x_n) = 0$ by Lemma 10.2. Thus

$$w(x_1, \ldots, x_{n-1}, Ax_n) = \alpha\, w(x_1, \ldots, x_n). \tag{10.9}$$

Since $w(x_1, \ldots, x_n) \neq 0$ it finally follows by combining (10.6), (10.8) and (10.9) that $\det(A) = \alpha \det(A|_W)$. □

The determinant of a matrix

Let $\mathbf{A}$ be a square matrix of size n with entries from $\mathcal{F}$.

Definition 10.20. The *determinant* $\det \mathbf{A}$ is the determinant of the endomorhism of $\mathcal{F}^n$ given by multiplication of $\mathbf{A}$ on column vectors.

It is then immediate from (10.7) that the product rule

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$$

holds also for $n \times n$ matrices.

Theorem 10.21. *Let $\alpha_{i,j}$ be the elements of $\mathbf{A}$. Then*

$$\det \mathbf{A} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \alpha_{i,\sigma(i)}. \tag{10.10}$$

Moreover, let $A \in \operatorname{End}(V)$. Then

$$\det A = \det[A] \tag{10.11}$$

for the matrix of A with respect to any basis for V.

The equation (10.10) is called the *Leibniz determinant formula.*

Proof. The two equations will be proved simultaneously by showing

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \alpha_{i,\sigma(i)}, \tag{10.12}$$

where α_{ij} are the elements of $[A]$. When applied to $V = \mathcal{F}^n$ this produces (10.10). Knowing (10.10) for every $\mathbf{A}$ we obtain (10.11) from (10.12).

We have $\alpha_{ij} = y_i(Ax_j)$ for the given basis $\{x_1, \dots, x_n\}$ and its dual basis $\{y_1, \dots, y_n\}$. Let $w = y_1 \wedge \cdots \wedge y_n$. Then

$$w(Ax_1, \dots, Ax_n) = \det(A)$$

by (10.6) and (10.3), and on the other hand

$$w(Ax_1, \dots, Ax_n) = (y_1 \wedge \cdots \wedge y_n)(Ax_1, \dots, Ax_n).$$

By definition of the wedge product this gives (10.10). □

Polynomials over infinite fields

The rest of this lecture contains some results which we will only prove for infinite fields although they are valid for all fields. By excluding the finite fields we can use the following lemma to simplify the exposition.

Recall that a polynomial over $\mathcal{F}$ is an expression $p(X) = \sum_{i=0}^{n} \alpha_i X^i$ with coefficients $\alpha_i \in \mathcal{F}$, and that the associated scalar function $\lambda \mapsto p(\lambda)$ is obtained by substituting $\lambda \in \mathcal{F}$ for X in the expression.

Lemma 10.22. *If $\mathcal{F}$ is infinite then every polynomial $p(X)$ is uniquely determined by its associated function $\lambda \mapsto p(\lambda)$.*

Proof. If $p_1(\lambda) = p_2(\lambda)$ for all $\lambda \in \mathcal{F}$ then $p_1 - p_2$ is a polynomial with infinitely many roots. This implies $p_1 - p_2 = 0$ since a non-zero polynomial of degree k has at most k roots. □

The assertion of the lemma fails for every finite field. For example, when $\mathcal{F}$ is finite, a non-zero polynomial is defined by

$$p(X) = \prod_{\alpha \in \mathcal{F}} (\alpha - X),$$

but the associated function is zero. Incidentally $p(X)$ can also be used to show that a finite field is not algebraically closed, since $p(X)+1$ has no roots.

Characteristic polynomial

By means of the determinant we can associate an important polynomial to every endomeorphism of V. We first define it for a matrix.

Definition 10.23. Let $\mathbf{A}$ be an $n \times n$ matrix. The *characteristic polynomial* $\chi_{\mathbf{A}}(X)$ of $\mathbf{A}$ is the polynomial obtained from (10.10) by replacing each occurrence of a diagonal element α_{ii} by $\alpha_{ii} - X$.

The characteristic polynomial is a polynomial of degree n. The top degree X^n occurs only in the term $\prod_{i=1}^{n}(\alpha_{ii} - X)$ for $\sigma = e$, and hence it has coefficient $(-1)^n$.

Let V be a vector space with $\dim V = n < \infty$, and let $A \in \mathrm{End}(V)$. As before we denote the map $A - \lambda I \in \mathrm{End}(V)$ just by $A - \lambda$.

Lemma 10.24. *The characteristic polynomial $\chi_{[A]}(X)$ is the same for all matrices $[A]$ which represent A with respect to some basis for V. The associated scalar function is given by*

$$\chi_{[A]}(\lambda) = \det(A - \lambda), \quad (\lambda \in \mathcal{F}). \tag{10.13}$$

Proof. We first prove (10.13). The elements of the matrix $[A-\lambda]=[A]-\lambda[I]$ are the same as those of $[A]$, except on the diagonal, where λ is subtracted. Hence $\chi_{[A]}(\lambda)=\det([A-\lambda])$ by the definition of $\chi_{[A]}(X)$, and (10.13) follows.

For the first statement in the lemma we assume for simplicity that $\mathcal{F}$ is infinite. Then the statement follows from (10.13) and Lemma 10.22. □

Definition 10.25. The polynomial $\chi_A(X)=\chi_{[A]}(X)$ in the above lemma is called the *characteristic polynomial* of A.

Characteristic roots and eigenvalues

A main motivation for the characteristic polynomial is that it can be used to determine the eigenvalues of a linear map.

Theorem 10.26. *Let $A\in\operatorname{End}(V)$. The set of roots $\lambda\in\mathcal{F}$ of the characteristic polynomial χ_A coincides with the spectrum $\sigma(A)$.*

Proof. Let $\lambda\in\mathcal{F}$. Then λ is an eigenvalue for A if and only if $A-\lambda$ is not bijective. Hence the theorem follows from (10.13) and Theorem 10.16. □

Cayley-Hamilton theorem

Theorem 10.27. $\chi_A(A)=0$ *for all* $A\in\operatorname{End}(V)$.

Proof. Assume first that $\mathcal{F}$ algebraically closed, and hence also infinite. From Corollary 7.9 we know that V admits the Jordan decomposition

$$V=M_1\oplus\cdots\oplus M_s$$

where $\mu_1,\dots,\mu_s\in\mathcal{F}$ are the eigenvalues, and $M_1,\dots,M_s$ the generalized eigenspaces $M_i=M_{\mu_i}$. Therefore V admits a basis with respect to which $[A]$ is a triangular matrix with the eigenvalues in the diagonal, each occurring according to its algebraic multiplicity $m_i=\dim(M_i)$. Moreover, $(A-\mu_i)^{m_i}|_{M_i}=0$ by the last statement in Theorem 7.4.

It now follows from Theorem 10.17 that $\det(A-\lambda)=\prod_{i=1}^{s}(\mu_i-\lambda)^{m_i}$. Then

$$\chi_A(X)=(\mu_1-X)^{m_1}\cdots(\mu_s-X)^{m_s} \tag{10.14}$$

by (10.13) and Lemma 10.22. Hence

$$\chi_A(A)=(\mu_1-A)^{m_1}\cdots(\mu_s-A)^{m_s}$$

is zero on M_i for each i, and it follows that $\chi_A(A)=0$.

Next we prove $\chi_{\mathbf{A}}(\mathbf{A})=0$ for matrices over an arbitrary field. This is true over an algebraically closed field, because we just saw it for the corresponding endomorphism of $\mathcal{F}^n$. We observe that Definition 10.23 produces the same polynomial $\chi_{\mathbf{A}}(X)$ for every extension of $\mathcal{F}$. As the equation $\chi_{\mathbf{A}}(\mathbf{A}) = 0$ holds true if we regard $\mathbf{A}$ as a matrix with elements from the algebraic closure, it also holds in the original field.

Finally we obtain Theorem 10.27 by reducing it to the corresponding statement for matrices, using Definition 10.25. □

Algebraic multiplicities

The following theorem shows the algebraic multiplicities are the root multiplicities in the characteristic polynomial.

Theorem 10.28. *Let $A \in \operatorname{End}(V)$ with eigenvalues $\mu_1, \ldots, \mu_s \in \mathcal{F}$, and let*

$$V = M_{\mu_1} \oplus \cdots \oplus M_{\mu_s} \oplus R$$

be its Jordan decomposition. Let $m_i = \dim M_{\mu_i}$. Then

$$\chi_A(X) = (\mu_1 - X)^{m_1} \cdots (\mu_s - X)^{m_s}\, q(X), \tag{10.15}$$

where $q(X) = \chi_{A|_R}(X) \in \mathcal{F}[X]$ has no roots.

Proof. For simplicity we assume $\mathcal{F}$ is infinite. The proof of (10.15) is essentially the same as given above for (10.14) in the algebraically closed case. The extra factor $q(X) = \chi_{A|_R}(X) \in \mathcal{F}[X]$ has no roots because $A|_R$ has no eigenvalues. □

Lecture 11. Jordan normal form

In a previous lecture we saw that when $\mathcal{F}$ is algebraically closed there is a unique decomposition of every map into a commuting pair of a diagonable map and a nilpotent map. Diagonable maps are easy to understand, by their nature. In this lecture we will study the nilpotent maps closer.

Recall from Theorem 7.4 that for every nilpotent map $A \in \operatorname{End}(V)$ there exists a basis for V such that $[A]$ is strictly upper triangular. The aim is to improve this result.

Cyclic vectors

Let V be a vector space over an arbitrary field.

Definition 11.1. Let $A \in \operatorname{End}(V)$. A subspace $H \subseteq V$ is called *cyclic* if there exists $x \in H$ such that $H = \operatorname{Span}\{A^j x \mid j \geq 0\}$. Then x is called a *cyclic* or *generating* vector for H.

Cyclic basis

For the current purpose of studying nilpotent maps we are particularly interested in the case where $A^k x = 0$ for some $k > 0$.

Lemma 11.2. *Let x be cyclic for H and assume $A^k x = 0$ but $A^{k-1}x \neq 0$ for some $k > 0$. Then $\dim H = k$ and $S := \{x, Ax, \dots, A^{k-1}x\}$ is a basis.*

Proof. It follows from $A^k x = 0$ that $A^j x = 0$ for all $j \geq k$. Hence $H = \operatorname{Span} S$ and $\dim H \leq k$. Moreover, $A|_H$ is nilpotent of index k. By Theorem 7.4 we have $\dim H \geq k$. Hence the dimension is k and S is a basis □

It is customary to order the basis in the lemma reversely, that is, with $x_j = A^{k-j}x$ for $j = 1, \dots, k$ so that

$$(x_1, \dots, x_k) = (A^{k-1}x, \dots, Ax, x). \tag{11.1}$$

By using that ordering, the restriction of A to H obtains the strictly upper triangular matrix

$$[A|_H] = \begin{pmatrix} 0 & 1 & & \dots & 0 \\ & 0 & 1 & & \vdots \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} \tag{11.2}$$

with 1's on the super-diagonal and 0's everywhere else.

Rank and nullity

Let $H = \operatorname{Span}\{x, Ax, \dots, A^{k-1}x\}$ with $A^{k-1}x \neq 0$ and $A^k x = 0$ as before.

Lemma 11.3. *The range and null-space of $A|_H$ are*

$$R(A|_H) = \operatorname{Span}\{Ax, \dots, A^{k-1}x\}, \quad \textit{and} \quad N(A|_H) = \operatorname{Span}\{A^{k-1}x\}$$

with rank $k-1$ and nullity 1.

Proof. The inclusion $\supseteq$ is clear in both cases. Hence $\operatorname{rank}(A|_H) \geq k-1$ and $\operatorname{null}(A|_H) \geq 1$. Since $\operatorname{rank}(A|_H) + \operatorname{null}(A|_H) = k$, equality follows. □

Annihilators

For our continued study of nilpotent maps we need some simple results about annihilators in a finite-dimensional vector space V and its dual space V'.

Recall that for a subspace $U \subseteq V$ we defined its annihilator by

$$U^\circ = \{y \in V' \mid \forall x \in U : y(x) = 0\} \subseteq V'.$$

For a subspace $W \subseteq V'$ the annihilator W° then belongs in the double dual

$$W^\circ = \{z \in V'' \mid \forall y \in W : z(y) = 0\} \subseteq V''.$$

However, the following is also a natural definition of an annihilator

$$^\circ W = \{x \in V \mid \forall y \in W : y(x) = 0\} \subseteq V.$$

The two spaces are in fact closely related, as it is evident from the definition of the natural correspondence $T : V \to V''$ that $T(^\circ W) = W^\circ$. Hence the two spaces are isomorphic and have the same dimension

$$\dim {}^\circ W = \dim W^\circ = \dim V - \dim W$$

by Theorem 3.8.

Invariance of annihilators

Lemma 11.4. *Let $A \in \operatorname{End}(V)$ with adjoint $A' \in \operatorname{End}(V')$.*

(1) *If $U \subseteq V$ is A-invariant then U° is A'-invariant*

(2) *If $W \subseteq V'$ is A'-invariant then $^\circ W$ is A-invariant.*

Proof. (1) Assume U is invariant. Then $y \in U^\circ$ implies $(A'y)(x) = y(Ax) = 0$ for all $x \in U$, and hence $A'y \in U^\circ$. Hence U° is invariant.

(2) Assume W is invariant. Then $x \in {}^\circ W$ implies $y(Ax) = (A'y)(x) = 0$ for all $y \in W$, and hence $Ax \in {}^\circ W$. Hence $^\circ W$ is invariant. □

Cyclic reduction

The following is a main result of this lecture. Assume $\dim V = n < \infty$.

Theorem 11.5. *Let $A \in \operatorname{End}(V)$ be nilpotent. There exists a decomposition*

$$V = H_1 \oplus \cdots \oplus H_r$$

with cyclic invariant subspaces H_i.

Proof. By induction on n. The case of $n = 0$ is clear, so let us assume $n > 0$. Let k be the index of A and let $x \in V$ with $A^{k-1}x \neq 0$ but $A^k x = 0$. Then by Lemma 11.2 the cyclic subspace

$$H := \operatorname{Span}\{x, Ax, \dots, A^{k-1}x\} \subseteq V$$

has dimension k.

We want to find an invariant complement to H, and for that we invoke the adjoint $A' \in \operatorname{End}(V')$ of A. Note first that $(A')^j = (A^j)'$ for all $j \geq 0$. Hence A' is nilpotent of index k as well.

Let $y \in V'$ be a linear form with $y(A^{k-1}x) \neq 0$. Then $(A')^{k-1}y \neq 0$ and hence by the same lemma as before

$$L := \operatorname{Span}\{y, A'y, \dots, (A')^{k-1}y\} \subseteq V'$$

is a cyclic subspace of V' also of dimension k.

Let

$$K := {}^{\circ}L = \{v \in V \mid \forall w \in L : w(v) = 0\} \subseteq V$$

be the annihilator of L in V. Then $\dim K = n - k$, and by Lemma 11.4 it follows from the A'-invariance of L that K is A-invariant. Note that $A^{k-1}x \notin K$ since $y(A^{k-1}x) \neq 0$.

It now follows from Lemma 11.3 that $N(A|_H) \cap K = \{0\}$. Hence $A|_{H\cap K}$ is injective, which is absurd unless $H \cap K = \{0\}$, since A is nilpotent. Since the dimensions of H and K add to n we finally conclude that

$$V = H \oplus K.$$

By induction the restriction $A|_K$ admits a cyclic decomposition, and together with H we thus obtain a cyclic decomposition for A. □

Uniqueness in the cyclic decomposition

We keep the assumptions of the previous section. The cyclic decomposition of Theorem 11.5 is in general not uniquely determined by A, but some of its properties are.

Lemma 11.6. *Assume*

$$V = H_1 \oplus \cdots \oplus H_r$$

with cyclic A-invariant subspaces H_i. Then the number r is the nullity of A. The dimensions $\dim H_i$ are also uniquely determined (up to permutation).

Proof. Since each H_i is invariant, the null-space of A decomposes directly as

$$N(A) = N(A|_{H_1}) \oplus \cdots \oplus N(A|_{H_r}).$$

By Lemma 11.3 each component has dimension one. Hence $\dim N(A) = r$.

The uniqueness of the dimensions of the H_i is shown by induction on $n = \dim V$. The range of A also decomposes directly,

$$R(A) = R(A|_{H_1}) \oplus \cdots \oplus R(A|_{H_r}),$$

and by Lemma 11.3 each component has dimension exactly one less than $\dim H_i$. By induction the numbers $\dim R(A|_{H_i})$ are uniquely determined by $A|_{R(A)}$, hence by A. It follows that so are the dimensions of the H_i. □

Canonical form

The following is a more explicit version of the cyclic reduction. It follows immediately from Theorem 11.5 and Lemma 11.6, from which we keep the assumptions.

Corollary 11.7. *There exist unique integers $r \geq 0$ and $q_1 \geq \cdots \geq q_r > 0$, and there exist vectors $x_1, \dots, x_r \in V$ such that*

(1) *The vectors $A^j x_i$ for all $0 \leq j < q_i$, $i = 1, \dots, r$ form a basis for V,*

(2) *$A^{q_i} x_i = 0$ for $i = 1, \dots, r$.*

The matrix of A with respect to this basis then has the following form, called the *canonical form.* It consists of r square blocks of sizes $q_1, \dots, q_r$ along the diagonal

$$[A] = \begin{pmatrix} [q_1 \times q_1] & & 0 \\ & \ddots & \\ 0 & & [q_r \times q_r] \end{pmatrix} \tag{11.3}$$

With appropriate reverse ordering of the basis vectors as in (11.1), each of the blocks is a strictly upper triangular matrix as (11.2), with 1's on the super-diagonal and 0 everywhere else.

Classification of nilpotent maps

The cyclic reduction attaches numbers r and $q_1, \ldots, q_r$ uniquely to every nilpotent map A. The following theorem shows that conversely, these numbers determine A uniquely up to isomorphism.

Let $A \in \mathrm{End}(V)$ and $B \in \mathrm{End}(W)$ be nilpotent endomorphisms of some finite-dimensional vector spaces V and W.

Theorem 11.8. *The same integers r and $q_1, \ldots, q_r$ are attached to A and B if and only if there exists an isomorphism $T \in \mathrm{Hom}(V, W)$ such that $BT = TA$.*

Proof. If the same integers are attached to A and B then $\dim V = \dim W = q_1 + \cdots + q_r$, and we can define an isomorphism $T \in \mathrm{Hom}(V, W)$ by mapping each basis vector $A^j x_i$ for V to the corresponding basis vector $B^j y_i$ for W. Then

$$TA(A^j x_i) = T(A^{j+1} x_i) = B^{j+1} y_i = BT(A^j x_i)$$

for all i and j, so that $TA = BT$.

Conversely, if

$$V = H_1 \oplus \cdots \oplus H_r$$

is a cyclic decomposition for A, and $T \in \mathrm{Hom}(V, W)$ is an isomorphism such that $TA = BT$, then

$$W = T(H_1) \oplus \cdots \oplus T(H_r)$$

is a cyclic decomposition for B with the same numbers attached. □

Jordan normal form

By combining the preceding result about nilpotent maps with the Jordan decomposition from Theorem 7.9 we obtain the following theorem, which essentially amounts to a classification of all endomorphisms of V, provided $\mathcal{F}$ is algebraically closed.

Theorem 11.9 (Jordan normal form)**.** *Let A be an endomorphism of a finite-dimensional vector space over an algebraically closed field, and let*

$$V = M_1 \oplus \cdots \oplus M_s$$

be the canonical decomposition of V in generalized eigenspaces for A.

There exists for each $i = 1, \ldots, s$ a basis for M_i such that with respect to the combined basis for V

$$[A] = \begin{pmatrix} [A|_{M_1}] & & 0 \\ & \ddots & \\ 0 & & [A|_{M_s}] \end{pmatrix}, \tag{11.4}$$

where each of the block matrices $[A|_{M_i}]$ has the form

$$\lambda_i \mathbf{I} + \textit{canonical form of } [(A - \lambda_i I)|_{M_i}].$$

The number s, the eigenvalues $\lambda_1, \ldots, \lambda_s$, the corresponding dimensions $\dim M_1, \ldots, \dim M_s$*, and the numbers r_i and $q_1, \ldots, q_{r_i}$ attached to the canonical form of $(A - \lambda_i I)|_{M_i}$ for each $i = 1, \ldots, s$ determine A uniquely up to an isomorphism of V.*

Notice that there are two layers of block matrices with this description. The i'th block of (11.4) is a matrix of the form (11.3) which consists of blocks of the form (11.2), but with λ_i on the diagonal instead of 0. For example

$$[A] = \begin{pmatrix} \lambda_1 & 1 & & & & & \\ & \lambda_1 & & & & & \\ & & \lambda_2 & 1 & & & \\ & & & \lambda_2 & 1 & & \\ & & & & \lambda_2 & & \\ & & & & & \lambda_2 & 1 \\ & & & & & & \lambda_2 \end{pmatrix}$$

with $s = 2$ appears in (11.4) as the block-block-matrix

$$[A] = \begin{pmatrix} \begin{pmatrix} \lambda_1 & 1 \\ & \lambda_1 \end{pmatrix} & \\ & \begin{pmatrix} \begin{pmatrix} \lambda_2 & 1 & \\ & \lambda_2 & 1 \\ & & \lambda_2 \end{pmatrix} & \\ & \begin{pmatrix} \lambda_2 & 1 \\ & \lambda_2 \end{pmatrix} \end{pmatrix} \end{pmatrix}.$$

Lecture 12. Bounded operators

Normed vector space

In this lecture the field $\mathcal{F}$ is $\mathbb{R}$ or $\mathbb{C}$. Let V be a vector space over $\mathcal{F}$.

Definition 12.1. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}$ such that

(a) $\|\alpha x\| = |\alpha|\,\|x\|$ for all $\alpha \in \mathcal{F}$, $x \in V$

(b) $\|x + y\| \leq \|x\| + \|y\|$ (triangle inequality) for all $x, y \in V$

(c) $\|x\| > 0$ for all $x \neq 0$ and $\|0\| = 0$.

A vector space with a norm is called a *normed vector space.*

Example 12.2. If V has an inner product then $\|x\| = \sqrt{\langle x, x\rangle}$ is a norm. Not every normed space is obtained like that, for example $V = \mathcal{F}^n$ with the *max-norm*

$$\|x\|_\infty = \|(\alpha_1, \dots, \alpha_n)\|_\infty := \max |\alpha_i|.$$

It is easy to see that this is a norm, and that the parallelogram identity (8.3) fails for it when $n \geq 2$.

Bounded operators

In this lecture we want to investigate some general properties of normed spaces. These are mainly related to the topology, which is obtained as follows.

It is immediate from the axioms above that with $d(x, y) := \|x - y\|$ as the distance function, one obtains a metric space and hence a topological structure on V. The closed metric ball of radius $r > 0$ around the origin is then $\{x \in V \mid \|x\| \leq r\}$, and it is called the *unit ball* when $r = 1$. It is a general property of a metric that $x \mapsto d(x, 0) = \|x\|$ is continuous- In particular, the closed balls are closed.

Definition 12.3. A linear map $A \in \operatorname{Hom}(V, U)$ between normed vector spaces is said to be *bounded* or a *bounded operator* if the image of the unit ball is bounded, that is, if there exists $K \geq 0$ such that $\|Ax\| \leq K$ for all x in the unit ball of V.

Since the norm is homogeneous under scalar multiplication

$$\|Ax\| \leq K\|x\|, \qquad x \in V,$$

is an equivalent condition.

Continuity

Lemma 12.4. *A linear map A is bounded if and only if it is continuous.*

Proof. Since A is linear it is continuous at every $v \in V$ if and only if it is continuous at $v = 0$, that is, if and only if

$$\forall \epsilon > 0 \, \exists \delta > 0 : \, \|x\| \leq \delta \Rightarrow \|Ax\| \leq \epsilon. \tag{12.1}$$

If $\|Ax\| \leq K\|x\|$ for all x we immediately obtain (12.1) by taking $\delta = \epsilon/K$.

Conversely, with (12.1) we can find δ such that $\|Ax\| \leq 1$ when $\|x\| \leq \delta$. Then $\|Ax\| \leq 1/\delta$ when $\|x\| \leq 1$. □

Corollary 12.5. *Every linear map of $V = \mathcal{F}^n$ with max-norm into any normed vector space U is continuous.*

Proof. Let $A \in \mathrm{Hom}(V, U)$. Let $e_1, \ldots, e_n$ be the standard basis for $\mathcal{F}^n$. Then for every $x = \sum \alpha_i e_i$ with $\|x\|_\infty \leq 1$ we find

$$\|Ax\| = \|\sum_i \alpha_i A e_i\| \leq \sum_i |\alpha_i| \|Ae_i\| \leq \sum_i \|Ae_i\|,$$

which makes A bounded with $K = \sum_i \|Ae_i\|$. □

Local compactness

Definition 12.6. A metric space is *locally compact* if every bounded sequence contains a converging subsequence.

In a normed vector space translations and scalar multiplications by non-zero numbers are homeomorphisms. It follows that local compactness is equivalent with compactness of the unit ball.

It is known from the Heine-Borel theorem that $\mathbb{R}$ is locally compact, and this implies easily that $(\mathcal{F}^n, \| \cdot \|_\infty)$ is locally compact in both cases $\mathcal{F} = \mathbb{R}$ and $\mathbb{C}$.

Equivalent norms

Two norms $\| \cdot \|_1$ and $\| \cdot \|_2$ on V, which define the same topology, are said to be *equivalent*. This happens if and only if the identity map is continuous both ways between the two norms. By Lemma 12.4 it is an equivalent condition that there exist two positive constants c, C such that

$$c\|x\|_1 \leq \|x\|_2 \leq C\|x\|_1$$

for all $x \in V$.

Lemma 12.7. *Any two norms on $V = \mathcal{F}^n$ are equivalent.*

Proof. It suffices to prove that every norm $\|\cdot\|$ is equivalent to the max-norm. It follows from Corollary 12.5 that the identity map is continuous from $\|\cdot\|_\infty$ to $\|\cdot\|$, that is,

$$\|x\| \leq C\|x\|_\infty \tag{12.2}$$

for some $C > 0$.

Consider the unit sphere $S = \{x \in V \mid \|x\|_\infty = 1\}$. It is a closed subset of the unit ball and hence max-norm-compact since $\mathcal{F}^n$ is locally compact with this topology. Let $c \geq 0$ be the infimum $c := \inf_{x\in S} \|x\|$. Then

$$c\|x\|_\infty \leq \|x\|$$

for all $x \in V$. All we have to show is that $c > 0$.

Note that $\|x\| > 0$ for all $x \in S$ since $0 \notin S$. As we have seen with (12.2) that the function $x \mapsto \|x\|$ is max-norm-continuous, we conclude from the compactness that $c > 0$. □

Corollary 12.8. *Let U be a normed vector space and let A be an injective linear map $\mathcal{F}^n \to U$. Then A is a homeomorphism to its image in U.*

Proof. One verifies easily that the function $x \mapsto \|Ax\|$ is a norm on $\mathcal{F}^n$. Hence

$$c\|x\|_\infty \leq \|Ax\| \leq C\|x\|_\infty.$$

This implies A is a homeomorphism. □

Finite-dimensional normed spaces

We now obtain for a general finite-dimensional normed space the same topological properties as we saw for $\mathcal{F}^n$.

Theorem 12.9. *Let V be a finite-dimensional normed vector space.*

(1) *All $A \in \operatorname{Hom}(V, U)$ are continuous for all normed vector spaces U.*

(2) *V is locally compact.*

Proof. Since V is finite-dimensional there is a linear isomorphism $\mathcal{F}^n \to V$ for some n. By Corollary 12.8 this is also a topological isomorphism. Hence these properties follow from what we have already seen for $\mathcal{F}^n$. □

Operator norm

Let V and U be normed vector spaces.

Definition 12.10. For a bounded operator $A \in \operatorname{Hom}(V, U)$ we call

$$\|A\| := \sup\{\|Ax\| \mid x \in V, \|x\| = 1\} = \sup\left\{\frac{\|Ax\|}{\|x\|}\,\middle|\, x \in V, x \neq 0\right\}$$

the *operator norm* of A.

The identity between the two supremums is easily seen from the homogeneity of the norms. It follows from the second expression and the definition of the supremum as the least upper bound, that $\|A\|$ is the least constant K for which $\|Ax\| \leq K\|x\|$ for all x.

Let $B(V, U) := \{A \in \operatorname{Hom}(V, U) \mid A \text{ is bounded}\}$ and equip it with the operator norm. If $U = V$ we write just $B(V)$.

Lemma 12.11. *$B(V, U)$ is a normed vector space.*

Proof. It is easy to see that αA and $A + B$ belong to $B(V, U)$ for all $A, B \in B(V, U)$ and $\alpha \in \mathcal{F}$, and that

$$\|\alpha A\| = |\alpha|\, \|A\| \quad \text{and} \quad \|A + B\| \leq \|A\| + \|B\|.$$

Hence $B(V, U)$ is a vector space, and since $\|A\| = 0$ only when $A = 0$, it is also normed. □

The inequality

$$\|AB\| \leq \|A\|\, \|B\| \tag{12.3}$$

is also easy. Here $A \in B(V, U)$ and $B \in B(W, V)$ with normed spaces U, V and W.

Spectral radius

Let $A \in \operatorname{End}(V)$ where V is a finite-dimensional normed space. We want to investigate the relation between the spectrum of A and its operator norm.

Definition 12.12. The *spectral radius* of A is

$$\rho(A) := \max\{|\lambda| \mid \lambda \in \sigma(A)\}$$

(if the spectrum is empty we put $\rho(A) = -\infty$).

Lemma 12.13. $\rho(A) \leq \|A\|$.

Proof. Let $x \in V$ be an eigenvector with eigenvalue λ. Then

$$\|Ax\| = |\lambda|\, \|x\|.$$

Hence $\|A\| \geq |\lambda|$ by the definition of the operator norm. □

Application of the spectral theorem

In the following theorem we assume that an inner product is given on V. Recall that if A is self-adjoint or if $\mathcal{F} = \mathbb{C}$ and A is normal, then A is orthogonally diagonable (and vice versa). In these cases the relation between operator norm and spectral radius is simple.

Theorem 12.14. *Let V be a finite-dimensional inner product space and assume $A \in \mathrm{End}(V)$ is orthogonally diagonable. Then $\rho(A) = \|A\|$.*

Proof. Because of Lemma 12.13 it suffices to show $\|A\| \le \rho(A)$. Let

$$A = \sum_{\lambda \in \sigma(A)} \lambda E_\lambda$$

be the spectral resolution of A, and note that by assumption $E_\lambda \perp E_\mu$ when $\lambda \neq \mu$. Then by Pythagoras

$$\|Ax\|^2 = \sum_{\lambda \in \sigma(A)} |\lambda|^2 \|E_\lambda x\|^2 \le \rho(A)^2 \sum_{\lambda \in \sigma(A)} \|E_\lambda x\|^2 = \rho(A)^2 \|x\|^2$$

for all x, and hence $\|A\| \le \rho(A)$. □

A norm independent limit

The operator norm of a linear map $A \in \mathrm{End}(V)$ depends on which norm is used on V, and equivalent norms do not necessarily determine the same operator norm of A. In Theorem 12.14 it is crucial that the norm used for V is the one associated with the inner product. We would like to replace the statement of the theorem by a statement which is invariant under norm equivalence. The following lemma prepares the way for this.

Lemma 12.15. *Let V be finite-dimensional and let $\|\cdot\|_1$ and $\|\cdot\|_2$ be equivalent norms on V. Let $A \in \mathrm{End}(V)$ and let $\|A\|_1$ and $\|A\|_2$ denote the operator norm of A with respect to these norms. Then*

$$\lim_{k\to\infty} \|A^k\|_1^{\frac{1}{k}} = \lim_{k\to\infty} \|A^k\|_2^{\frac{1}{k}}$$

in the sense that if one of the limits exists then they both exist and are equal.

Proof. The assumption is that for some positive constants C_1, C_2 we have

$$\|x\|_1 \le C_1 \|x\|_2 \quad \text{and} \quad \|x\|_2 \le C_2 \|x\|_1$$

for all x. From this we derive that

$$\|Ax\|_1 \leq C_1\|Ax\|_2 \leq C_1\|A\|_2\|x\|_2 \leq C_1C_2\|A\|_2\|x\|_1$$

and hence $\|A\|_1 \leq C_1C_2\|A\|_2$. Similarly $\|A\|_2 \leq C_1C_2\|A\|_1$. Then

$$(C_1C_2)^{-1/k}\|A^k\|_1^{1/k} \leq \|A^k\|_2^{1/k} \leq (C_1C_2)^{1/k}\|A^k\|_1^{1/k}.$$

Since $(C_1C_2)^{\pm 1/k} \to 1$ for $k \to \infty$ we can conclude with the sandwich lemma that if $\lim \|A^k\|_1^{1/k}$ exists, then so does $\lim \|A^k\|_2^{1/k}$ with the same value. □

The following observation will be used in what follows.

Lemma 12.16. *$\rho(A) \leq \|A^k\|^{\frac{1}{k}} \leq \|A\|$ for all k.*

Proof. It is convenient to rewrite the claim as

$$\rho(A)^k \leq \|A^k\| \leq \|A\|^k. \tag{12.4}$$

When λ is an eigenvalue for A then λ^k is eigenvalue for A^k of the same eigenvector. It follows that $\rho(A)^k \leq \rho(A^k)$. The first inequality in (12.4) then follows from Lemma 12.13. The second inequality comes from (12.3). □

Gelfand's limit formula, diagonable operators

Theorem 12.17. *Let $A \in \operatorname{End}(V)$ for a finite-dimensional normed space V. If A is diagonable then $\rho(A) = \lim_{k\to\infty} \|A^k\|^{\frac{1}{k}}$.*

Proof. Lemma 12.15 allows us to pick any norm on V. Let $e_1, \ldots, e_n$ be a basis for V consisting of eigenvectors, and define an inner product on V by

$$\langle \sum_i \alpha_i e_i, \sum_i \beta_i e_i \rangle = \sum_i \alpha_i \bar{\beta}_i,$$

that is, via the chosen basis it corresponds to the standard inner product on $\mathcal{F}^n$. With this inner product A is orthogonally diagonable, and hence $\rho(A) = \|A\|$ by Theorem 12.14. Then Lemma 12.16 implies that $\rho(A) = \|A^k\|^{\frac{1}{k}}$ for all k. In particular $\rho(A) = \lim_{k\to\infty} \|A^k\|^{\frac{1}{k}}$. □

General operators

We now assume $\mathcal{F} = \mathbb{C}$. Then we can generalize the preceding theorem to operators that are not necessarily diagonable.

Theorem 12.18. *Let $A \in \operatorname{End}(V)$ for a finite-dimensional normed space V. Then $\rho(A) = \lim_{k\to\infty} \|A^k\|^{\frac{1}{k}}$.*

Proof. We use the additive Jordan decomposition $A = A_d + A_n$ of Theorem 7.14, where A_d is diagonable, A_n nilpotent, and $A_d A_n = A_n A_d$.

Let m be the nilpotency index of A_n. Because A_d and A_n commute we can calculate A^k with the binomial formula. Since $A_n^j = 0$ for $j \geq m$ we obtain for $k \geq m$

$$A^k = (A_d + A_n)^k = \sum_{j=0}^{m-1} \binom{k}{j} A_d^{k-j} A_n^j.$$

We estimate each binomial coefficient by $\leq k^m$, write $A_d^{k-j} = A_d^{k-m} A_d^{m-j}$, and obtain

$$\|A^k\| \leq k^m \|A_d^{k-m}\| \sum_{j=0}^{m-1} \|A_d^{m-j} A_n^j\| = C k^m \|A_d^{k-m}\|$$

where C does not depend on k.

With Lemma 12.16 we then find

$$\rho(A) \leq \|A^k\|^{\frac{1}{k}} \leq (Ck^m)^{\frac{1}{k}} \|A_d^{k-m}\|^{\frac{1}{k}}$$

for $k \geq m$. Now $(Ck^m)^{\frac{1}{k}} \to 1$ for $k \to \infty$, and

$$\|A_d^k\|^{\frac{1}{k}} \to \rho(A_d) = \rho(A)$$

by Theorem 12.17 and the fact that A and A_d have the same spectrum.

It is easy to see for any sequence $x_k > 0$ that $x_k^{\frac{1}{k}}$ and $x_{k-m}^{\frac{1}{k}} = (x_{k-m}^{\frac{1}{k-m}})^{1-\frac{m}{k}}$ have the same limits. Hence $\|A_d^{k-m}\|^{\frac{1}{k}} \to \rho(A)$, and the theorem follows. □

Hilbert spaces

Recall that a metric space in which every Cauchy sequence converges is said to be *complete*.

Definition 12.19. A *Hilbert space* is an inner product space V for which the metric given by the corresponding norm is complete.

In particular, every finite dimensional inner product space is a Hilbert space, because it is isomorphic to $\mathbb{R}^n$ or $\mathbb{C}^n$, which are complete metric spaces.

Example 12.20. The space ℓ^2 of all sequences $x = (x_1, x_2, \dots)$ from $\mathcal{F}$, for which $\sum_k |x_k|^2 < \infty$, is a Hilbert space when equipped with the inner product $\langle x, y\rangle = \sum_k x_k \overline{y_k}$.

More generally, if μ is a positive measure on a set X, then $L^2(X, \mu)$ is a Hilbert space with the inner product $\langle f, g\rangle = \int_X f\bar{g}\, d\mu$. This is the content of the Riesz-Fischer theorem.

Projection theorem

Theorem 12.21. *Let $U \subseteq V$ be a closed subspace of a Hilbert space. Then*

$$V = U \oplus U^\perp.$$

Proof. By Theorem 8.11 it suffices to show for every $y \in V$ that there exists a vector $u \in U$ which is closest to y, that is, $\|y - u\| = \min_{x\in U} \|y - x\|$.

Let $c = \inf_{x\in U} \|y - x\|$, and let x_n be a sequence in U for which

$$\lim_{n\to\infty} \|y - x_n\| = c.$$

The theorem will be proved if we show convergence of the sequence x_n, since its limit x will belong to the closed subspace U and satisfy $\|y - x\| = c$.

Since V is complete it suffices to show the Cauchy property for x_n. By the identity (8.3) we have

$$\|v - w\|^2 = 2(\|v\|^2 + \|w\|^2) - \|v + w\|^2$$

for all $v, w \in V$. For the vectors $v = y - x_n$ and $w = y - x_m$ this yields

$$\|x_m - x_n\|^2 = 2(\|y - x_n\|^2 + \|y - x_m\|^2) - 4\|y - \tfrac{1}{2}(x_n + x_m)\|^2,$$

and since $\frac{1}{2}(x_n + x_m) \in U$ we have $\|y - \frac{1}{2}(x_n + x_m)\| \geq c$ and

$$0 \leq \|x_m - x_n\|^2 \leq 2(\|y - x_n\|^2 + \|y - x_m\|^2) - 4c^2.$$

Since $\|y - x_n\|$ and $\|y - x_m\|$ both tend to c, this implies the property. □

Riesz-Fréchet representation theorem

It follows from the Cauchy-Schwartz inequality that for each $y \in V$ the linear form $x \mapsto \langle x, y\rangle$ on V is continuous. On a Hilbert space we have the following important converse, which is a generalization of Theorem 8.13.

Theorem 12.22. *Let V be a Hilbert space and $z \in V'$ a continuous linear form. Then there exists a unique $y \in V$ such that $z(x) = \langle x, y\rangle$ for all $x \in V$.*

Proof. The continuity of z implies that its null-space $U \subseteq V$ is closed. Hence $V = U \oplus U^\perp$. With that we can repeat the proof of Theorem 8.13. □

Corollary 12.23. *Every bounded linear map $A \in \mathrm{Hom}(U, V)$ between two Hilbert spaces has an adjoint $A^* \in \mathrm{Hom}(V, U)$, which is bounded with operator norm equal to that of A.*

Proof. Let $y \in V$. Since A is bounded, $x \mapsto \langle Ax, y\rangle$ is a continuous linear form on U, hence equal to $\langle x, u\rangle$ for some $u \in U$. Then by definition $A^*y = u$.

It follows from Cauchy-Schwartz that

$$\|A^*y\|^2 = \langle A^*y, A^*y\rangle = \langle AA^*y, y\rangle \leq \|A\| \, \|A^*y\| \, \|y\|$$

and hence

$$\|A^*y\| \leq \|A\| \, \|y\|.$$

This shows A^* is bounded with $\|A^*\| \leq \|A\|$. The opposite inequality then follows from $A^{**} = A$. □

Maximal orthonormal

An orthonormal set X in an inner product space V is *maximal* if it is not properly contained in any other orthonormal set.

Lemma 12.24. *Let V be a Hilbert space and $X \subset V$ an orthonormal set. Then X is maximal if and only if* $\mathrm{Span}(X)$ *is dense in V.*

Proof. Maximality of X is evidently equivalent to $X^\perp = \{0\}$. On the other hand, let U be the closure of $\mathrm{Span}(X)$, then $V = U \oplus U^\perp$ by Theorem 12.21. Hence $\mathrm{Span}(X)$ is dense if and only if $U^\perp = \{0\}$.

We now prove $X^\perp = \{0\} \Leftrightarrow U^\perp = \{0\}$. Since $X \subseteq U$, it is clear that $X^\perp = \{0\}$ implies $U^\perp = \{0\}$. Conversely assume $U^\perp = \{0\}$, and let $y \in X^\perp$. Then $y \perp \mathrm{Span}(X)$ by linearity of the inner product, and then $y \perp U$ by continuity of the inner product. Hence $y = 0$, and thus $X^\perp = \{0\}$. □

Recall that a metric space is called *separable* if it contains a countable dense subset.

Theorem 12.25. *Every separable Hilbert space contains a countable maximal orthonormal set.*

Proof. Let $S = \{x_n\}$ be a countable dense subset of V. By discarding from S every element x_n which belongs to the span of the preceding elements x_j, we obtain a linearly independent countable set X with the same span as S. Hence $\mathrm{Span}(X)$ is dense. Applying also Gram-Schmidt we obtain then an orthonormal set for which the span is dense. □

Orthonormal expansion

Let $X = \{x_n \mid n \in \mathbb{N}\}$ be a countable orthonormal set in a Hilbert space V.

Lemma 12.26. *Let $\alpha_k \in \mathcal{F}$ be a sequence with $\sum_{k=1}^{\infty} |\alpha_k|^2 < \infty$. The limit*

$$y = \sum_{k=1}^{\infty} \alpha_k x_k$$

exists in V. It satisfies $\|y\|^2 = \sum_{k=1}^{\infty} |\alpha_k|^2 < \infty$ and $\langle y, x_k\rangle = \alpha_k$ for all k.

Proof. Let $y_n = \sum_{k=1}^{n} \alpha_k x_k$, and $\eta_n = \|y_n\|^2 = \sum_{k=1}^{n} |\alpha_k|^2$. It follows from the assumption on α_k that η_n is a Cauchy sequence in $\mathcal{F}$. Since by Pythagoras

$$\|y_n - y_m\|^2 = \sum_{k=m+1}^{n} |\alpha_k|^2 = \eta_n - \eta_m$$

for $n > m$, this implies that y_n is a Cauchy sequence in V. Hence $y_n \to y$ for some vector $y \in V$. Moreover $\|y\|^2 = \lim \|y_n\|^2 = \sum_{k=1}^{\infty} |\alpha_k|^2 < \infty$ and

$$\langle y, x_k\rangle = \lim_{n\to\infty} \langle y_n, x_k\rangle = \alpha_k$$

by continuity of the norm and inner product. □

Theorem 12.27. *Assume in addition that X is maximal. Then every $x \in V$ is expressed by a convergent sum*

$$x = \sum_{n=1}^{\infty} \langle x, x_n\rangle x_n, \tag{12.5}$$

and its norm is given by

$$\|x\|^2 = \sum_{n=1}^{\infty} |\langle x, x_n\rangle|^2. \tag{12.6}$$

Proof. Let $y_n = \sum_{k=1}^{n} \langle x, x_k\rangle x_k$. Then $x - y_n \perp y_n$ by Lemma 8.6, and hence by Pythagoras

$$\|y_n\|^2 = \|x\|^2 - \|x - y_n\|^2 \leq \|x\|^2 < \infty$$

for all n. Since $\|y_n\|^2 = \sum_{k=1}^{n} |\langle x, x_k\rangle|^2$, also by Pythagoras, this implies

$$\sum_{k=1}^{\infty} |\langle x, x_k\rangle|^2 \leq \|x\|^2 < \infty.$$

Hence the limit $y = \sum_{k=1}^{\infty} \langle x, x_k\rangle x_k$ exists by Lemma 12.26, and it satisfies

$$\langle y, x_k\rangle = \langle x, x_k\rangle$$

for all k. Hence $x - y \perp X$, and then $y = x$ by the maximality of X. □

Lecture 13. Positivity

In this lecture several notions of positivity will be introduced, for linear maps, matrices and vectors. Unless otherwise specified $\mathcal{F}$ can be $\mathbb{R}$ or $\mathbb{C}$, and V is an inner product space over $\mathcal{F}$.

Positive operators

Definition 13.1. A *positive operator* is a self-adjoint linear map $A \in \operatorname{End}(V)$ for which $\langle Ax, x\rangle \geq 0$ for all $x \in V$. If in addition $\langle Ax, x\rangle = 0$ only for $x = 0$ we call it *strictly positive.* We write $A \succeq 0$ and $A \succ 0$ in these cases.

Positive spectrum and square root

Let V be finite-dimensional and $A \in \operatorname{End}(V)$.

Theorem 13.2. *The following are equivalent*

(1) $A \succeq 0$

(2) $A = A^*$ *and* $\sigma(A) \subset [0, \infty[$

(3) $A = B^2$ *for some self-adjoint* $B \in \operatorname{End}(V)$.

Proof. (3)⇒(1) $\langle Ax, x\rangle = \langle B^2x, x\rangle = \langle Bx, Bx\rangle = \|Bx\|^2 \geq 0$ for all $x \in V$.
(1)⇒(2) Let $\lambda \in \sigma(A)$ and $Ax = \lambda x$ with $\|x\| = 1$. Then $\lambda = \langle Ax, x\rangle \geq 0$.
(2)⇒(3) This was seen in Theorem 9.15. □

Since an endomorphism of a finite-dimensional space is invertible if and only if 0 is not an eigenvalue, we obtain also the following equivalences.

Theorem 13.3. *The following are equivalent*

(1) $A \succ 0$

(2) $A = A^*$ *and* $\sigma(A) \subset]0, \infty[$

(3) $A = B^2$ *for some self-adjoint* $B \in \operatorname{GL}(V)$.

Corollary 13.4. *If* $A \succeq 0$*, respectively* $\succ 0$*, then the determinant and trace of* A *are* ≥ 0*, respectively* > 0.

Proof. This follows from (2) since the determinant is a product of eigenvalues and the trace is a sum. □

Positive definite matrices

Let $\mathbf{A} = (\alpha_{ij})$ be an $n \times n$ matrix with elements from $\mathcal{F}$. We denote by $A \in \mathrm{End}(\mathcal{F}^n)$ the corresponding linear map given by matrix multiplication with vectors of $\mathcal{F}^n$ seen as columns, and we use for $\mathcal{F}^n$ the standard inner product (dot product).

Definition 13.5. $\mathbf{A}$ is *positive semi-definite* if $A \succeq 0$ and *positive definite* if $A \succ 0$. Equivalently, these terms apply to $\mathbf{A}$ when it is self-adjoint and satisfies $\sum_{i,j} \alpha_{ij}\xi_i\bar{\xi}_j \geq 0$, respectively > 0, for all non-zero $\xi \in \mathcal{F}^n$.

The spectrum of a real symmetric matrix is unchanged when the matrix is regarded as over $\mathbb{C}$. Hence Theorems 13.2(2) and 13.3(2) imply that for such a matrix the properties in Definition 13.5 do not change either, if $\mathcal{F} = \mathbb{R}$ is replaced by $\mathbb{C}$.

Principal minors

By (2) one can determine from the eigenvalues of a given Hermitian matrix whether is positive definite. It is useful to be able to decide this also when the eigenvalues are unknown. This is the purpose of the next theorem.

Let $\mathbf{A}_k$ denote the $k \times k$ matrix in the upper left corner of $\mathbf{A}$,

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_k & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

In other words all rows and columns with indices $> k$ are deleted.

Definition 13.6. The determinants $\det \mathbf{A}_k$ for $k = 1, \ldots, n$ are called the *leading principal minors* of $\mathbf{A}$.

More generally a *principal minor* is the determinant of a submatrix $\mathbf{A}_J$ obtained from $\mathbf{A}$ by deleting all rows and columns except those with indices in some given subset $J \subseteq \{1, \ldots, n\}$.

Sylvester's criterion

Theorem 13.7. *A Hermitian matrix* $\mathbf{A}$ *is positive definite if and only if all leading principal minors are positive, that is,* $\det \mathbf{A}_k > 0$ *for* $k = 1, \ldots, n$.

Proof. If $\mathbf{A}$ is positive definite then so is every submatrix $\mathbf{A}_J$, since for all non-zero $\eta \in \mathbb{C}^J$

$$\sum_{i\in J, j\in J} \alpha_{ij}\eta_i\bar{\eta}_j = \sum_{i,j} \alpha_{ij}\xi_i\bar{\xi}_j > 0$$

when $\xi_i = \eta_i$ for $i \in J$ and $\xi_i = 0$ otherwise. Hence $\det \mathbf{A}_J > 0$ by Corollary 13.4, and in particular $\det \mathbf{A}_k > 0$ for $k = 1, \dots, n$.

For the converse implication an obvious inductive argument reduces to showing that if $\mathbf{A}_{n-1}$ is positive definite and $\det \mathbf{A} > 0$, then $\mathbf{A}$ is positive definite.

Assume that $\mathbf{A}_{n-1}$ is positive definite, and let us express this in terms of the linear map A. Let $e_1, \dots, e_n$ be the standard basis vectors for $\mathbb{C}^n$, and let $U = \operatorname{Span}\{e_1, \dots, e_{n-1}\}$. Then the assumption on $\mathbf{A}_{n-1}$ amounts to $\langle Ax, x\rangle > 0$ for all non-zero $x \in U$.

We will apply the min-max principle in the form (9.4). Let the function ν be defined on subspaces of V by

$$\nu(W) = \min\{\langle Ax, x\rangle \mid x \in W, \|x\| = 1\}, \tag{13.1}$$

and let $\lambda_1 \geq \cdots \geq \lambda_n$ be the eigenvalues of A. Then

$$\lambda_k = \max\{\nu(W) \mid \dim W = k\}. \tag{13.2}$$

Since $\langle Ax, x\rangle > 0$ for all non-zero $x \in U$ we find with (13.1) that $\nu(U) > 0$, from which we conclude with (13.2) that $\lambda_{n-1} > 0$. Hence all eigenvalues of A are positive except possibly the smallest one. The additional assumption of $\det \mathbf{A} > 0$ implies that the number of negative eigenvalues is even. Hence the smallest eigenvalue must be positive too, and thus $\sigma(A) \subset]0, \infty[$. □

This theorem does not generalize to positive semidefinite matrices. For example, the leading principal minors of

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

are both zero, but A is not $\succeq 0$. However, the first part of the proof above shows that if $\mathbf{A}$ is positive semidefinite then *all* the principal minors are ≥ 0. The converse of this is true, but the proof will not be given here.

Positive vectors

Let V be a real inner product space with a fixed orthonormal basis $e_1, \dots, e_n$ (for example $\mathbb{R}^n$ with standard basis).

Definition 13.8. For $x = \sum_i \xi_i e_i \in V$ we write

$$\begin{aligned} &x \geq 0 \quad \text{if } \xi_i \geq 0 \text{ for all } i \\ &x \gneq 0 \quad \text{if } \xi_i \geq 0 \text{ for all } i \text{ and } \xi_k > 0 \text{ for some } k \\ &x > 0 \quad \text{if } \xi_i > 0 \text{ for all } i \end{aligned}$$

We say that x is a *non-negative vector* when $x \geq 0$, and a *positive vector* when $x > 0$.

These inequalities are also used between arbitrary pairs of vectors, so that for example $x \geq y$ means $x - y \geq 0$. We note that

$$x \geq y \geq 0 \quad \Rightarrow \quad \|x\| \geq \|y\|,$$

since if $x \geq y \geq 0$ then all coordinates of both x and y are ≥ 0, and those of x are larger or equal than those of y.

Positive maps

Let $A \in \mathrm{End}(V)$ with V as above.

Definition 13.9. We call A a *positive map* and write $A > 0$ if for $x \in V$

$$x \gneq 0 \quad \Rightarrow \quad Ax > 0. \tag{13.3}$$

Lemma 13.10. *$A > 0$ if and only if $Ae_i > 0$ for all i.*

Proof. If $A > 0$ then $Ae_i > 0$ because $e_i \gneq 0$. Conversely if $Ae_i > 0$ for all i, and $x = \sum_i \xi_i e_i \gneq 0$ then $Ax = \sum_i \xi_i Ae_i$ is a sum of non-negative vectors at least one of which is positive. Hence $Ax > 0$ □

Positive matrices

Definition 13.11. A real $n \times n$-matrix $\mathbf{A}$ with all entries > 0 is called *positive*. We write $\mathbf{A} > 0$ in this case.

Lemma 13.12. *Let $\mathbf{A}$ be the matrix of $A \in \mathrm{End}(V)$ for the basis $e_1, \dots, e_n$. Then $A > 0$ if and only if $\mathbf{A} > 0$.*

Proof. This follows from Lemma 13.10 because the entries of $\mathbf{A}$ are exactly the coordinates of the vectors Ae_i. □

Perron-Frobenius theorem

Let V be a real inner product space with a fixed orthonormal basis $e_1, \dots, e_n$, and let $A \in \mathrm{End}(V)$ with associated matrix $\mathbf{A}$. In what follows we want to consider the complex spectrum of A, by which we mean all eigenvalues of $\mathbf{A}$ considered as a complex matrix, or equivalently all complex roots of the characteristic polynomial. These will be referred to as *complex eigenvalues*.

In particular we now define the spectral radius of A by

$$\rho_{\mathbb{C}}(A) = \max\{|\lambda| \mid \lambda \text{ a complex eigenvalue of } A\}.$$

We note that if A is positive then so is its adjoint A^*, since it has the same matrix entries, just transposed. Moreover, it has the same spectrum and spectral radius, since the characteristic polynomial is the same.

Theorem 13.13. *Let $A \in \operatorname{End}(V)$ be positive, and let $\rho = \rho_{\mathbb{C}}(A)$ be its spectral radius. Then $\rho > 0$ and*

(1) *The ρ-eigenspace has dimension 1 and contains an eigenvector $v > 0$.*

(2) *There are no other complex eigenvalues λ with $|\lambda| = \rho$.*

(3) *The generalized eigenspace for ρ is equal to the eigenspace.*

(4) *The following limit holds for all $x \in V$*

$$\rho^{-k} A^k x \to \frac{\langle x, w\rangle}{\langle v, w\rangle} v, \qquad (k \to \infty).$$

Here w is a positive eigenvector for A^*, also with eigenvalue ρ.

The proof of Theorem 13.13 will be given after some preparatory lemmas.

Spectral radius formula A

We would like to use the spectral radius formula

$$\rho = \lim_{k\to\infty} \|A^k\|^{\frac{1}{k}} \tag{13.4}$$

for the positive map A. We need the version from Theorem 12.18, which requires a complex vector space. Hence some preparation is necessary.

As we already fixed an orthonormal basis for V it is no loss of generality to consider instead of A its matrix $\mathbf{A}$. This matrix we consider as a complex matrix, and as such it acts on $\mathbb{C}^n$. Then $\mathbf{A}(x+iy) = \mathbf{A}x + i\mathbf{A}y$ for $x, y \in \mathbb{R}^n$. Since

$$\|\mathbf{A}(x+iy)\|^2 = \|\mathbf{A}x\|^2 + \|\mathbf{A}y\|^2$$

we see that viewing $\mathbf{A}$ as complex does not alter its operator norm.

We now apply Theorem 12.18 to $\mathbf{A}$ and conclude that (13.4) is valid, provided the spectral radius is defined as $\rho = \rho_{\mathbb{C}}(A)$.

Applications of the limit formula for $\rho(A)$

The following lemma will be used to provide the eigenvector v in Theorem 13.13.

Lemma 13.14. *Assume $A > 0$. If a vector $x \in V$ satisfies $Ax \geq \rho x \geq 0$ then $Ax = \rho x$.*

Proof. Let $y := Ax$ and assume $y \neq \rho x$ in order to reach a contradiction. Then $y \gneq \rho x$ and since $A > 0$ we obtain $Ay > A(\rho x) = \rho y$ from (13.3). Hence $y \neq 0$ and $Ay \geq \delta y \geq 0$ for some $\delta > \rho$. By repeated applications of the positive map A we obtain $A^k y \geq \delta^k y \geq 0$. Hence $\|A^k y\| \geq \|\delta^k y\|$ and $\|A^k\| \geq \delta^k$. With (13.4) we reach the contradiction that $\rho \geq \delta$. □

Lemma 13.15. *Let $A \in \operatorname{End}(V)$ (not necessarily positive). If $\tau > \rho(A)$ then*

$$\tau^{-k} A^k x \to 0$$

for $k \to \infty$, for all $x \in V$.

Proof. Choose $\delta \in \mathbb{R}$ such that $\tau > \delta > \rho(A)$. It follows from (13.4) that $\|A^k\|^{\frac{1}{k}} \leq \delta$ for all k sufficiently large. Then

$$\tau^{-k}\|A^k\| \leq \left(\frac{\delta}{\tau}\right)^k$$

and hence $\tau^{-k}\|A^k\| \to 0$ for $k \to \infty$. The lemma follows. □

Modulus vector

We associate with each vector $z = (\zeta_1, \dots, \zeta_n) \in \mathbb{C}^n$ the *modulus vector*

$$|z| = (|\zeta_1|, \dots, |\zeta_n|) \in \mathbb{R}^n$$

which is non-negative. It should not be confused with the norm $\|z\|$ of z.

Lemma 13.16. *Assume $A > 0$. Then*

$$|Az| \leq A|z|$$

for all $z \in \mathbb{C}^n$. Moreover $|Az| < A|z|$ unless $z = \gamma|z|$ for some $\gamma \in \mathbb{C}$.

Proof. Let $z = (\zeta_1, \dots, \zeta_n)$ and let $\alpha_{ij} > 0$ denote the entries of $\mathbf{A}$. Then

$$|\sum_j \alpha_{ij}\zeta_j| \leq \sum_j \alpha_{ij}|\zeta_j| \tag{13.5}$$

for each i, and hence $|Az| \leq A|z|$.

It is a general property of the complex plane that if $\beta_1, \dots, \beta_n$ are complex numbers for which $|\beta_1 + \cdots + \beta_n| = |\beta_1| + \cdots + |\beta_n|$ then the numbers $\beta_1, \dots, \beta_n$ all belong to a common half-line in the complex plane, that is, there exists a complex number γ such that $\beta_j = |\beta_j|\gamma$ for all j.

If there is equality in (13.5) for some value i we obtain $\alpha_{ij}\zeta_j = |\alpha_{ij}\zeta_j|\gamma$ for this i and all j. Hence also $\zeta_j = |\zeta_j|\gamma$ for all j, that is, $z = \gamma|z|$. □

Proof of Theorem 13.13

(1) By definition of ρ there exists an eigenvector $z \in \mathbb{C}^n$ with an eigenvalue $\lambda \in \mathbb{C}$ of modulus $|\lambda| = \rho$. Then by Lemma 13.16

$$0 \leq \rho|z| = |\lambda z| = |Az| \leq A|z|. \tag{13.6}$$

Hence

$$A|z| = \rho|z| \tag{13.7}$$

by Lemma 13.14. Moreover, since $A > 0$ and $|z| \gneq 0$ we have $\rho|z| = A|z| > 0$, and hence $|z| > 0$. We have shown that there is a positive eigenvector with eigenvalue ρ.

We have also seen that $|z| > 0$ for every eigenvector z with eigenvalue ρ. Hence all coordinates of z are non-zero, and in particular the first. Since the subspace of all vectors in $\mathbb{C}^n$ with first coordinate 0 has dimension $n-1$ it would necessarily intersect non-trivially with the ρ-eigenspace if that had dimension greater than one.

(2) Let $z \in \mathbb{C}^n$ be an eigenvector with eigenvalue $\lambda \in \mathbb{C}$ where $|\lambda| = \rho$. Then (13.6) and (13.7) are valid and imply $|Az| = A|z| = \rho|z|$. Hence $z = \gamma|z|$ for some $\gamma \in \mathbb{C}$ by the last statement of Lemma 13.16, and hence $\lambda = \rho$.

(3) The adjoint A^* is positive, and it has the same spectrum as A. By (1) there exists a positive eigenvector w for it with eigenvalue ρ. Since v and w are both positive, they are not orthogonal to each other.

Let $U = \{w\}^\perp$. Then U is an A-invariant subspace of V of dimension $n-1$. If the generalized eigenspace for ρ were larger than the eigenspace, it would intersect non-trivially with U. That intersection would contain an eigenvector, in contradiction to the one-dimensionality of the eigenspace.

(4) It follows from (1)-(2) that the restriction of A to U has spectral radius strictly smaller than ρ. It then follows from Lemma 13.15 that $\rho^{-k}A^k x \to 0$ for all $x \in U$.

Let $x \in V$ be arbitrary. Then

$$x - \frac{\langle x, w\rangle}{\langle v, w\rangle}\, v \in U$$

and hence

$$\rho^{-k}A^k\Big(x - \frac{\langle x, w\rangle}{\langle v, w\rangle}\, v\Big) \to 0.$$

Since $A^k v = \rho^k v$ this implies

$$\rho^{-k}A^k x \to \frac{\langle x, w\rangle}{\langle v, w\rangle}\, v$$

and the theorem is proved. □

Non-negative maps

The theorem of Perron-Frobenius does not generalize in its full extent to maps which are not positive but just non-negative. However, the first part of it carries over.

Definition 13.17. We call $A \in \mathrm{End}(V)$ a *non-negative map* if for $x \in V$

$$x \geq 0 \quad \Rightarrow \quad Ax \geq 0. \tag{13.8}$$

or equivalently, if all entries of $\mathbf{A} = [A]$ are ≥ 0.

Theorem 13.18. *Let $A \in \mathrm{End}(V)$ be non-negative, and let $\rho = \rho_{\mathbb{C}}(A)$ be its spectral radius. There exists an eigenvector $v \geq 0$ for A of eigenvalue ρ.*

The proof, a limit argument, will not be given here.

Lecture 14. Factorization

A factorization of a linear map consists of writing it as a product of linear maps of some particular types. Factorizations are important tools for efficient algorithms, and they are usually formulated directly in terms of matrices.

QR-factorization

The Gram-Schmidt orthonormalization procedure gives rise to a useful factorization. It applies to matrices over $\mathcal{F} = \mathbb{R}$ or $\mathbb{C}$ and reads as follows.

Theorem 14.1. *Every $n \times m$ matrix $\mathbf{A}$ with independent columns admits a unique factorization*

$$\mathbf{A} = \mathbf{QR} \tag{14.1}$$

with an $n \times m$ matrix $\mathbf{Q}$ with orthonormal columns and an upper triangular $m \times m$ matrix $\mathbf{R}$ with positive diagonal elements.

A similar factorization exists without the assumption of independent columns, but then uniqueness fails.

Motivation

Before proving the theorem we give some motivation. Orthonormality of the columns of $\mathbf{Q}$ is equivalent to $\mathbf{Q}^*\mathbf{Q} = \mathbf{I}$. With (14.1) it follows that

$$\mathbf{A}x = b \quad \Leftrightarrow \quad \mathbf{R}x = \mathbf{Q}^*b$$

for $x \in \mathcal{F}^m$ and $b \in \mathcal{F}^n$. When $\mathbf{R}$ is upper triangular we can easily determine x from $\mathbf{R}x$ by backwards substitution - find first x_n, then x_{n-1} etc. Thus the factorization provides an efficient method to solve linear equations.

Existence

Recall first the Gram-Schmidt procedure. Let V be an n-dimensional vector space with inner product. Given some linearly independent vectors $y_1, \dots, y_m$ the procedure constructs orthonormal vectors $x_1, \dots, x_m$ such that

$$\operatorname{Span}\{x_1, \dots, x_k\} = \operatorname{Span}\{y_1, \dots, y_k\}$$

for all $k = 1, \dots, m$. The main recursive step consists of defining the unit vector x_k by

$$x_k = \frac{1}{c_k}\big(y_k - \sum_{i<k} \langle y_k, x_i \rangle \, x_i\big)$$

where $c_k > 0$ is the norm of the vector in parenthesis. Hence

$$y_k = c_k x_k + \sum_{i<k} \langle y_k, x_i \rangle \, x_i. \tag{14.2}$$

We apply this procedure for $V = \mathcal{F}^n$ with standard inner product, and with $y_1, \dots, y_m$ as the columns of $\mathbf{A}$. Let $\mathbf{Q}$ be the matrix with the resulting vectors $x_1, \dots, x_m$ as columns, and let $\mathbf{R}$ be the transition matrix with elements r_{ik} such that

$$y_k = \sum_{i=1}^{m} r_{ik} x_i, \qquad (k = 1, \dots, m), \tag{14.3}$$

that is, the k-th column of $\mathbf{R}$ holds the x-coordinates of y_k. Then (14.3) says that $\mathbf{A} = \mathbf{QR}$.

The matrix $\mathbf{Q}$ has orthonormal columns by construction, and by comparing (14.2) and (14.3) we see that $r_{ik} = 0$ if $i > k$, that is, $\mathbf{R}$ is upper triangular. Moreover, the diagonal elements r_{kk} are the positive numbers c_k.

This proves the existence of the decomposition. The uniqueness will be shown after a couple of lemmas.

The inverse of an upper triangular matrix

If an invertible linear map A leaves a flag

$$\{0\} = W_0 \subset W_1 \subset \cdots \subset W_n = V$$

invariant, then its restriction $W_j \to W_j$ is injective and hence also surjective for each j. This implies that A^{-1} also leaves the flag invariant. It follows from this that the inverse of an invertible upper triangular matrix is again upper triangular:

$$\begin{pmatrix} \alpha_1 & & * \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}^{-1} = \begin{pmatrix} \alpha_1^{-1} & & * \\ & \ddots & \\ 0 & & \alpha_n^{-1} \end{pmatrix}. \tag{14.4}$$

Lemma 14.2. *The set*

$$\mathrm{P}(n) = \{\textit{upper triangular with positive diagonal elements}\}$$

is a subgroup of $\mathrm{GL}(n, \mathcal{F})$.

Proof. It is easily seen that the set is stable under multiplication, and (14.4) implies stability for taking inverses. □

Lemma 14.3. $\mathrm{U}(n) \cap \mathrm{P}(n) = \{\mathbf{I}\}$.

Proof. Let $\mathbf{U} \in \mathrm{U}(n) \cap \mathrm{P}(n)$. Then $\mathbf{U} = (\mathbf{U}^{-1})^*$, and $\mathbf{U}^{-1}$ is upper triangular according to Lemma 14.2. Therefore $\mathbf{U} = (\mathbf{U}^{-1})^*$ is an equality between an upper and a lower triangular matrix. Hence $\mathbf{U}$ is diagonal. The diagonal elements have modulus 1, and since they are also positive we can conclude that $\mathbf{U} = \mathbf{I}$. □

Uniqueness

Proof of Theorem 14.1. The existence was seen. Since $\mathbf{Q} = \mathbf{A}\mathbf{R}^{-1}$ it suffices to show uniqueness of $\mathbf{R}$.

Assume $\mathbf{A} = \mathbf{Q}_1\mathbf{R}_1 = \mathbf{Q}_2\mathbf{R}_2$ are two decompositions as in the theorem. Consider $\mathbf{R}_1\mathbf{R}_2^{-1} \in \mathrm{GL}(m, \mathcal{F})$. By Lemma 14.2 it belongs to $\mathrm{P}(m)$. On the other hand, it follows from $\mathbf{Q}^*\mathbf{Q} = \mathbf{I}$ that $\mathbf{A}^*\mathbf{A} = \mathbf{R}_1^*\mathbf{R}_1 = \mathbf{R}_2^*\mathbf{R}_2$. Hence

$$(\mathbf{R}_1\mathbf{R}_2^{-1})^*\mathbf{R}_1\mathbf{R}_2^{-1} = \mathbf{R}_2^{-1*}\mathbf{R}_1^*\mathbf{R}_1\mathbf{R}_2^{-1} = \mathbf{R}_2^{-1*}\mathbf{R}_2^*\mathbf{R}_2\mathbf{P}^{-1} = \mathbf{I},$$

which shows that $\mathbf{R}_1\mathbf{R}_2^{-1} \in \mathrm{U}(m)$. Then $\mathbf{R}_1\mathbf{R}_2^{-1} = \mathbf{I}$ by Lemma 14.3, and $\mathbf{R}_1 = \mathbf{R}_2$. □

Permutation matrices

Let V be a vector space and $v_1, \ldots, v_n$ an ordered basis for it. For each permutation $\sigma \in S_n$ we define $T_\sigma \in \mathrm{GL}(V)$ by $T_\sigma(v_j) = v_{\sigma(j)}$. Then $\sigma \mapsto T_\sigma$ is a homomorphism of the group S_n into $\mathrm{GL}(V)$.

In particular, it follows from Theorem 10.15 that

$$\det(T_\sigma) = \mathrm{sgn}(\sigma) \tag{14.5}$$

for all $\sigma \in S_n$. By the first axiom in that theorem we can reduce to transpositions, and for a transposition the determinant -1. For example if σ interchanges 1 and 2 then T_σ is diagonalized by the eigenvectors

$$v_1 - v_2, v_1 + v_2, v_3, \ldots, v_n$$

with eigenvalue -1 for the first and 1 for all the others. Hence $\det(T_\sigma) = -1$.

Specializing to $V = \mathcal{F}^n$ with canonical basis vectors we define $\mathbf{T}_\sigma = [T_\sigma]$, the matrix for which the entries are $t_{ij} = \delta_{i,\sigma(j)}$.

Definition 14.4. A *permutation matrix* is a square matrix in which all entries are 0 except one entry of 1 in each row and each column.

We conclude that $\sigma \mapsto \mathbf{T}_\sigma$ is an isomorphism of S_n onto the subgroup of $\mathrm{GL}(n, \mathcal{F})$ of permutation matrices and that $\det(\mathbf{T}_\sigma) = \mathrm{sgn}(\sigma)$ for all $\sigma \in S_n$.

LUP-factorization

The following so-called LUP-decomposition is valid over any field $\mathcal{F}$. Essentially it expresses the result of the Gaussian elimination by elementary row reductions.

Theorem 14.5. *Let* $\mathbf{A} \in \mathrm{GL}(n, \mathcal{F})$. *There exist a permutation matrix* $\mathbf{T}$ *and invertible lower and upper triangular matrices* $\mathbf{L}$ *and* $\mathbf{N}$ *such that*

$$\mathbf{A} = \mathbf{TLN}. \tag{14.6}$$

In particular, if all the leading principal minors of $\mathbf{A}$ *are non-zero this can be attained with* $\mathbf{T} = \mathbf{I}$ *and all diagonal elements of* $\mathbf{N}$ *equal to* 1. *When all this is required,* $\mathbf{L}$ *and* $\mathbf{N}$ *are unique.*

Proof. We first show that the assumption about the leading principal minors is valid for every $\mathbf{A} \in \mathrm{GL}(n, \mathcal{F})$ after a suitable permutation of its rows. We proceed by induction on n. Since $\mathbf{A}$ is invertible, its first $n-1$ columns are linearly independent. This implies that the matrix comprised by these columns contains $n-1$ linearly independent rows, and by a permutation of the rows of $\mathbf{A}$ we can assume these are the first rows. Then the $(n-1)\times(n-1)$ matrix in the upper left corner of $\mathbf{A}$ is invertible. We apply the induction hypothesis to it, and readily obtain the assumption for $\mathbf{A}$.

Note that any permutation of the rows of $\mathbf{A}$ can be obtained from multiplying $\mathbf{A}$ on the left by the corresponding permutation matrix. With that the proof is reduced to the case where $\mathbf{A}$ satisfies the hypothesis on the leading principal minors. We assume this from now on.

Let $V = \mathcal{F}^n$ with the canonical basis vectors $e_1, \dots, e_n$. With

$$V_k = \mathrm{Span}\{e_1, \dots, e_k\}, \qquad W_k = \mathrm{Span}\{e_{k+1}, \dots, e_n\}.$$

we obtain two complementary complete flags

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V \tag{14.7}$$

and

$$V = W_0 \supset W_1 \supset \cdots \supset W_n = \{0\}. \tag{14.8}$$

In Lemma 6.12 we saw that a linear map $N \in \mathrm{End}(V)$ leaves the ascending flag (14.7) invariant if and only if its matrix $\mathbf{N}$ with respect to $e_1, \dots, e_n$ is upper triangular. Similarly, a linear map $L \in \mathrm{End}(V)$ leaves the descending flag (14.8) invariant if and only if its matrix $\mathbf{L}$ is lower triangular.

Let $Ax = \mathbf{A}x$ for $x \in V$. The hypothesis on $\mathbf{A}$ implies that $E_k A|_{V_k}$ is an isomorphism of V_k, where E_k is the projection on V_k along W_k. This in turn implies that

$$V = A(V_k) \oplus W_k$$

for each k.

It follows that $\dim(A(V_k)\cap W_{k-1}) = 1$ for $k = 1, \dots, n$. Choose a non-zero vector $x_k \in V_k$ for which $y_k := Ax_k \in W_{k-1}$. Since $A(V_{k-1}) \cap W_{k-1} = \{0\}$ we have $x_k \notin V_{k-1}$ for all k. This implies that x_k is linearly independent from $x_1, \dots, x_{k-1}$. It follows that the vectors $x_1, \dots, x_n$ are linearly independent, and their A-images $y_1, \dots, y_n$ likewise.

Let $N, L \in \mathrm{GL}(V)$ be the invertible linear maps given by $Ne_k = x_k$ and $Le_k = y_k$ for each k. Since $x_k \in V_k$ and $y_k \in W_{k-1}$ for each k, the flags (14.7) and (14.8) are invariant for N and L, respectively. Hence their matrices $\mathbf{N}$ and $\mathbf{L}$ with respect to $e_1, \dots, e_n$ are upper and lower triangular, respectively. Moreover, by a suitable normalization of the x_k we can arrange that $\mathbf{N}$ has diagonal elements 1. Since $L = AN$ it finally follows from Lemma 14.2 that $\mathbf{A} = \mathbf{L}\mathbf{N}^{-1}$ has the desired form.

The uniqueness is seen as follows. If $\mathbf{L}_1\mathbf{N}_1 = \mathbf{L}_2\mathbf{N}_2$ then $\mathbf{L}_2^{-1}\mathbf{L}_1 = \mathbf{N}_2\mathbf{N}_1^{-1}$ is an equality between a lower triangular matrix and an upper triangular matrix with 1 in the diagonal. Hence it is the identity matrix. □

Uniqueness of the determinant

We can now finish the proof of Theorem 10.15. We claim that if two functions from $\mathrm{End}(V)$ to $\mathcal{F}$ both satisfy the axioms in that theorem, then they agree on all $A \in \mathrm{End}(V)$. By Theorem 10.16 we can assume that A is invertible. We choose an arbitrary basis for V and conclude from Theorem 14.5 that $A = TLN$ for an endomorphism T which permutes the basis vectors, and two endomorphisms $L, N \in \mathrm{End}(V)$ for which the corresponding matrices are lower and upper triangular, respectively. It then follows from (14.5) and Theorem 10.17(a) that our two determinant functions agree on T, L and N, and hence also on their product by the first axiom in Theorem 10.15.

Polar decomposition

Let V and W be finite-dimensional inner product spaces over $\mathcal{F} = \mathbb{R}$ or $\mathbb{C}$, and assume $\dim V \leq \dim W$.

Theorem 14.6. *Let $A \in \mathrm{Hom}(V, W)$. There exist a unique positive operator $P \in \mathrm{End}(V)$ and an isometry $U \in \mathrm{Hom}(V, W)$ such that*

$$A = UP. \tag{14.9}$$

If A is injective then in addition P is strictly positive and U is unique.

Recall that U is an isometry if $U^*U = I$. If $\dim V = \dim W$ this implies that U is a unitary isomorphism.

The identity $A = UP$ is called the *polar decomposition* of A, because it generalizes the polar decomposition of complex numbers:

For every $z \in \mathbb{C}$ there exist a unique $p \geq 0$ and a complex number u with $|u| = 1$ such that $z = up$. If $z \neq 0$ then in addition $p > 0$ and u is unique.

The proof of Theorem 14.6 will be given in the course of the next sections.

Uniqueness

Notice that A^*A is a positive operator since $\langle A^*Ax, x\rangle = \|Ax\|^2 \geq 0$. It is strictly positive if A is injective, since then $\|Ax\| > 0$ for $x \neq 0$.

Now if $A = UP$ and $U^*U = I$ then $A^*A = PU^*UP = P^2$, and hence P is the unique positive square root of A^*A, see Theorem 9.15. If A is injective then so is P. Then P is invertible and $U = AP^{-1}$ is unique.

Existence when A is injective

Assume A is injective. Then the polar decomposition is easily proved as follows. Let P be the strictly positive square root of A^*A and let $U = AP^{-1}$. Then $A = UP$ and U is an isometry:

$$U^*U = (AP^{-1})^*(AP^{-1}) = P^{-1}A^*AP^{-1} = P^{-1}P^2P^{-1} = I.$$

Range and null-space of A^*A

The following lemma prepares for the rest of the proof. It will be used again later in this lecture. Let V and W be arbitrary finite-dimensional inner product spaces and let $A \in \operatorname{Hom}(V, W)$.

Lemma 14.7. *V admits the orthogonal decomposition*

$$V = R(A^*) \oplus N(A). \tag{14.10}$$

Moreover, $R(A^*A) = R(A^*)$ and $N(A^*A) = N(A)$. In particular,

$$\operatorname{rank}(A) = \operatorname{rank}(A^*) = \operatorname{rank}(A^*A).$$

Proof. The orthogonal decomposition is equivalent to $R(A^*)^\perp = N(A)$, and this follows from Lemma 8.17, applied to A^*.

It is clear that $N(A) \subseteq N(A^*A)$. On the other hand if $x \in N(A^*A)$ then $\|Ax\|^2 = \langle A^*Ax, x\rangle = 0$ and thus $x \in N(A)$. Hence $N(A) = N(A^*A)$. Finally, by taking orthocomplements we obtain $R(A^*) = R(A^*A)$.

I follows from (14.10) and rank-nullity that $R(A)$ and $R(A^*)$ have the same dimensions. The statement about ranks follows. □

Note that by interchanging A and A^* we obtain an orthogonal decomposition of W,

$$W = R(A) \oplus N(A^*). \tag{14.11}$$

Existence

Proof of Theorem 14.6. It follows from (14.10) that A restricts to an isomorphism

$$A|_{R(A^*)} : R(A^*) \xrightarrow{\sim} R(A). \tag{14.12}$$

By the previously shown case then $A|_{R(A^*)} = U_1 P_1$ for a positive operator $P_1 \in \mathrm{GL}(R(A^*))$ and an isometry $U_1 \in \mathrm{Hom}(R(A^*), R(A))$.

Since $\dim R(A) = \dim R(A^*)$ it follows from $\dim V \leq \dim W$ and rank-nullity that $\dim N(A) \leq \dim N(A^*)$. Hence there exists an isometry $U_2 \in \mathrm{Hom}(N(A), N(A^*))$ (we just select an arbitrary one).

We now extend $P_1 \in \mathrm{End}(R(A^*))$ to a positive operator $P \in \mathrm{End}(V)$ by making it zero on the orthocomplement,

$$P := P_1 \oplus 0 : R(A^*) \oplus N(A) \to R(A^*) \oplus N(A).$$

Furthermore, using the orthogonal decompositions (14.10) and (14.11) we combine the isometries U_1 and U_2 to an isometry $V \to W$

$$U := U_1 \oplus U_2 : R(A^*) \oplus N(A) \to R(A) \oplus N(A^*).$$

It is easily seen that $Ax = UPx$ both for $x \in R(A^*)$ and for $x \in N(A)$, hence for all x. This shows the asserted existence, and completes the proof. □

Singular values and singular vectors

We now come to the final factorization theorem of the lecture, called *singular value decomposition.* Again V and W are finite-dimensional inner product spaces and $A \in \mathrm{Hom}(V, W)$.

Lemma 14.8. *Let $\sigma \in \mathbb{R} \setminus \{0\}$. The following conditions are equivalent.*

(1) *There exists a pair of non-zero vectors $x \in V$, $y \in W$, such that*

$$Ax = \sigma y, \quad \textit{and} \quad A^* y = \sigma x.$$

(2) *σ^2 is an eigenvalue for A^*A.*

Proof. If $Ax = \sigma y$ and $Ay = \sigma x$ then $A^*Ax = \sigma^2 x$. Conversely, if $A^*Ax = \sigma^2 x$ then $Ax = \sigma y$ and $A^*y = \sigma x$ for $y = \sigma^{-1}Ax$. □

Definition 14.9. A positive number σ satisfying (1)-(2) is called a *singular value* of A, and a pair of vectors as in (1) is called a *pair of singular vectors* for σ. The *multiplicity* of σ is the eigenvalue multiplicity of σ^2 for A^*A

The definition is extended to $m \times n$ matrices by regarding them as linear maps from $V = \mathcal{F}^n$ to $W = \mathcal{F}^m$ in the standard way.

Singular value decomposition

The following theorem provides an analogue of the orthogonal diagonalization of self-adjoint endomorphisms. However, now we consider separate source and target spaces V and W. Let $n = \dim V$ and $m = \dim W$.

Let $A \in \operatorname{Hom}(V, W)$ and let $k \leq \min\{m, n\}$ be its rank.

Theorem 14.10. *There exist scalars $\sigma_1, \dots, \sigma_k > 0$, and orthonormal bases $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_m\}$ for V and W such that*

$$Ax_i = \begin{cases} \sigma_i y_i, & i = 1, \dots, k \\ 0, & i = k+1, \dots, n. \end{cases} \tag{14.13}$$

Then for $i = 1, \dots, k$ the pairs of vectors (x_i, y_i) are singular, and $\sigma_1, \dots, \sigma_k$ are the corresponding singular values, each repeated according to multiplicity.

The following lemma paves the way for the proof.

Lemma 14.11. *Let $x_1, \dots, x_n$ be an orthonormal basis for V consisting of eigenvectors for A^*A with eigenvalues $\lambda_1, \dots \lambda_n$. Then $Ax_i \perp Ax_j$ for $i \neq j$ and $\|Ax_i\|^2 = \lambda_i$.*

Proof. The basis exists because A^*A is self-adjoint and positive. Orthogonality and length are both seen from

$$\langle Ax_i, Ax_j \rangle = \langle A^*Ax_i, x_j \rangle = \lambda_i \langle x_i, x_j \rangle. \quad \square$$

Proof of Theorem 14.10. Let $x_1, \dots, x_n$ and $\lambda_1, \dots, \lambda_n$ be as in Lemma 14.11. It follows from Lemma 14.7 that $\operatorname{rank}(A^*A) = \operatorname{rank}(A) = k$. Hence we can order the basis so that $\lambda_1, \dots, \lambda_k > 0$ and the remaining eigenvalues are 0. It follows that $Ax_i = 0$ for $i > k$.

Let $\sigma_i = \sqrt{\lambda_i}$. Then $\sigma_i = \|Ax_i\| > 0$ for $i = 1, \dots, k$ and $\sigma_i = 0$ else. For $i = 1, \dots, k$ we normalize the vectors Ax_i and define $y_i = \frac{1}{\sigma_i} Ax_i$. Then (14.13) holds. By Lemma 14.11 the vectors $y_1, \dots, y_k \in W$ are orthonormal, hence they can be supplemented to an orthonormal basis for W.

It follows from (14.13) that $\langle y_j, Ax_i \rangle = \sigma_i \delta_{ji}$ for all $j \leq m$, $i \leq n$. Since $\langle A^*y_j, x_i \rangle = \langle y_j, Ax_i \rangle$, and since the x_i form an orthonormal basis, we conclude that $A^*y_j = \sigma_j x_j$ if $j \leq k$ and $A^*y_j = 0$ otherwise. The final statement of the theorem follows. $\square$

SVD for matrices

Theorem 14.12. *Every $m \times n$ matrix $\mathbf{A}$ over $\mathcal{F}$ can be factorized as*

$$\mathbf{A} = \mathbf{U}_2 \mathbf{D} \mathbf{U}_1^* \tag{14.14}$$

where, with $k = \operatorname{rank}(A)$

1) *$\mathbf{U}_1$ is $n \times k$ and has orthonormal columns*
2) *$\mathbf{U}_2$ is $m \times k$ and has orthonormal columns*
3) *$\mathbf{D}$ is $k \times k$ diagonal with the singular values of $\mathbf{A}$ in the diagonal.*

The columns of $\mathbf{U}_1$ and $\mathbf{U}_2$ consist of pairs of singular vectors.

Proof. Let $V = \mathcal{F}^n$ and $W = \mathcal{F}^m$, and equip each of these spaces with its standard basis. Let $A \in \operatorname{Hom}(V, W)$ be the linear map for which $[A] = \mathbf{A}$ with respect to these bases.

From Theorem 14.10 we obtain two other orthonormal bases $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ for V and W. It follows from (14.13) that the matrix of A with respect to these bases is an $m \times n$ matrix of the form

$$\mathbf{D}' = \begin{pmatrix} \mathbf{D} & 0 \\ 0 & 0 \end{pmatrix}$$

with a diagonal $k \times k$ matrix $\mathbf{D}$ with the singular values on the diagonal.

Let $\mathbf{U}_1'$ and $\mathbf{U}_2'$ be the unitary matrices having $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$, respectively, as columns. These are the transition matrices for changing from the standard coordinates, and it follows that

$$\mathbf{A} = \mathbf{U}_2' \mathbf{D}' {\mathbf{U}_1'}^*$$

Since all entries are zero in all rows and columns of $\mathbf{D}'$ with indices $> k$, we obtain (14.14) when $\mathbf{U}_1$ and $\mathbf{U}_2$ are obtained from $\mathbf{U}_1'$ and $\mathbf{U}_2'$ by removing all columns with indices $> k$. □

Low rank approximation

In the proof above we removed the columns of $\mathbf{U}_1'$ and $\mathbf{U}_2'$ which correspond to diagonal value 0 of $\mathbf{D}'$. More drastically one could remove also the smallest singular values, if one considers them to be insignificant. If only the r largest singular values remain, where $r < k$, then one obtains the best approximation to $\mathbf{A}$ by a matrix of rank $\leq r$. This is the content of the following theorem of Eckart-Young, which is important for example in machine learning.

Let $\mathbf{A} = \mathbf{U}_2\mathbf{D}\mathbf{U}_1^*$ be a factorization of an $m \times n$ matrix over $\mathcal{F}$ with rank k, as in (14.14). Let the singular values in the diagonal of $\mathbf{D}$ be ordered such that $\sigma_1 \geq \cdots \geq \sigma_k > 0$.

Both the operator norm and the norm associated to the Frobenius inner product (see Theorem 8.29) are easy to express in terms of the singular values. Since $\langle \mathbf{A}^*\mathbf{A}x, x\rangle = \|\mathbf{A}x\|^2$ it follows from Theorem 9.17 applied to $\mathbf{A}^*\mathbf{A}$ that

$$\sigma_1^2 = \max\{\|\mathbf{A}x\|^2 \mid \|x\| = 1\}$$

and hence the operator norm is

$$\|\mathbf{A}\|_{\text{op}} = \sigma_1.$$

On the other hand we obtain for the Frobenius norm

$$\|\mathbf{A}\|_{\text{Frob}}^2 = \text{tr}(\mathbf{A}^*\mathbf{A}) = \sum_{i=1}^{k} \sigma_i^2$$

since the trace is the sum of the eigenvalues.

Theorem 14.13. *Let $0 \leq r \leq k$, and let $\mathbf{D}_r$ be the $k \times k$ diagonal matrix with diagonal elements $\sigma_1, \ldots, \sigma_r, 0 \ldots, 0$. Let $\mathbf{A}_r = \mathbf{U}_2\mathbf{D}_r\mathbf{U}_1^*$. Then*

$$\|\mathbf{A} - \mathbf{A}_r\| \leq \|\mathbf{A} - \mathbf{B}\|$$

for every $k \times k$ matrix $\mathbf{B}$ of rank $\leq r$.

Here the norm $\|\cdot\|$ on $m \times n$ matrices can be either $\|\cdot\|_{\text{op}}$ or $\|\cdot\|_{\text{Frob}}$.

Proof. The singular values of $\mathbf{A} - \mathbf{A}_r$ are $\sigma_{r+1}, \ldots \sigma_k$. Let $\tau_1, \tau_2, \ldots$ be the singular values of $\mathbf{A} - \mathbf{B}$. We claim that

$$\sigma_{r+i} \leq \tau_i \tag{14.15}$$

whenever $1 \leq i \leq k - r$. This implies the theorem for both of the norms.

We apply the max-min principle of (9.4) to $\mathbf{A}^*\mathbf{A}$ and obtain a subspace W of dimension $r + i$ such that

$$\sigma_{r+i}^2 = \nu(W) = \min\{\langle \mathbf{A}^*\mathbf{A}x, x\rangle \mid x \in W, \|x\| = 1\}.$$

Since the null-space $N = N(\mathbf{B})$ has dimension at least $n - r$, the intersection $W \cap N$ has dimension at least i. Let W_0 be an arbitrary subspace of $W \cap N$ with $\dim W_0 = i$. Then $\mathbf{A} = \mathbf{A} - \mathbf{B}$ on W_0, and hence

$$\sigma_{r+i}^2 \leq \langle \mathbf{A}^*\mathbf{A}x, x\rangle = \langle (\mathbf{A} - \mathbf{B})^*(\mathbf{A} - \mathbf{B})x, x\rangle$$

for every $x \in W_0$ with $\|x\| = 1$. By the max-min principle for $(\mathbf{A}-\mathbf{B})^*(\mathbf{A}-\mathbf{B})$ this implies (14.15). □

Index

additive Jordan decomposition, 63
adjoint, 24, 70
algebra over a field, 18
algebraic multiplicity, 57
algebraically closed, 49
alternating form, 32

basis, 6
bilinear, 29
bounded operator, 101

canonical form, 98
coordinates, 6
cyclic subspace, 95

determinant, 83, 89
diagonable, 47
dimension, 7
direct sum, 39
double dual, 27
dual space, 21

eigenspace, 47
eigenvalue, 47
eigenvector, 47
endomorphism, 11
entangled, 43
equivalent norms, 102

field, 3
finite-dimensional, 7
flag, 50
free vector space, 45
Frobenius inner product, 74

general linear group, 14
generalized eigenspace, 57
geometric multiplicity, 47
Gram-Schmidt, 67
group action, 84

Hilbert space, 107

idempotent, 42
infinite-dimensional, 7
inner product, 65
invariant subspace, 15
isomorphism, 12

Jordan decomposition, 61
Jordan normal form, 99

leading principal minor, 112
linear combination, 4
linear dependence, 5
linear map, 11
LUP-decomposition, 122

matrix, 17
max-min principle, 82
min-max principle, 81
minimal polynomial, 50
multilinear, 30
multilinear form, 30

natural correspondence, 27
nilpotent, 57
norm, 101
normal map, 76
null-space, 12
nullity, 16

operator norm, 104
orthocomplement, 68
orthogonal, 65
orthogonal group, 73
orthogonal map, 73
orthogonal projection, 68

orthogonally diagonable, 75
orthonormal, 67
orthonormal basis, 68

permutation matrix, 121
Perron-Frobenius theorem, 115
polar decomposition, 124
polynomial, 48
positive definite, 112
positive matrix, 114
positive operator, 111
positive semi-definite, 112
principal minor, 112
projection, 41
pure tensor, 43

QR-factorization, 119
quadratic form, 32
quotient space, 14

range, 12
rank, 16
Rayleigh quotient, 81
reduction, 52
root of a polynomial, 48

self-adjoint, 71
similar, 19
singular value, 126
singular value decomposition, 126
singular vector, 126
skew-symmetric, 31
span, 4
spectral radius, 104
spectrum, 47
subspace, 4
symmetric form, 31
symmetric group, 83
symplectic, 34

tensor product, 43
trace, 73
transition matrix, 19

unitary group, 73
unitary map, 73
universal property, 44
upper triangular, 51

vector space, 3