ALTTITLE

Layout and typography by the author
Font: 11 pt Kp-fonts | `Inconsolata`
Typeset using PDFLaTeX and the *memoir* class

29th November 2023

Contents

⁜ Preface

These notes cover aspects of linear algebra that I have not found satisfactory expositions of elsewhere. We generally restrict ourselves to the finite-dimensional case, unless results can be generalised without significant effort. For instance, in the context of inner product spaces there is of course no loss in generality by restricting to the real or the complex numbers, and the elementary theory of Hilbert space adjoints is not simplified substantially by the assumption of finite dimension, so we make no such assumption. On the other hand, we only prove the spectral theorem for normal operators on finite-dimensional spaces.

Throughout we let $\mathbb{F}$ denote an arbitrary field, $\mathbb{K}$ a field that is either the real or the complex numbers, and R a commutative ring. Unless otherwise specified, vector spaces will be vector spaces over $\mathbb{F}$, and modules will be left modules over R. Furthermore, sesquilinear forms are linear in their *second* entry. This is rarely relevant, but it seems more natural both in the theory of duality of spaces equipped with sesquilinear forms (see **??**) and in the representation of sesquilinear forms with matrices (see **??**).

1 Linear Equations and Matrices

1.1 ⋄ Linear equations

Let m and n be positive integers. A ***linear equation in n unknowns*** is an equation on the form

$$l\colon a_1x_1 + \cdots + a_nx_n = b,$$

where $a_1, \dots, a_n, b \in \mathbb{F}$. A ***solution*** to l is an element $v = (v_1, \dots, v_n) \in \mathbb{F}^n$ such that

$$a_1v_1 + \cdots + a_nv_n = b.$$

A ***system of linear equations in n unknowns*** is a tuple $L = (l_1, \dots, l_m)$, where each l_i is a linear equation in n unknowns. An element $v \in \mathbb{F}^n$ is a ***solution*** to L if it is a solution to each linear equation $l_1, \dots, l_m$.

Let L and L' be systems of linear equations in n unknowns. We say that L and L' are ***solution equivalent*** if they have the same solutions. Furthermore, we say that they are ***combination equivalent*** if each equation in L' is a linear combination of the equations in L, and vice versa. Clearly, if L and L' are combination equivalent they are also solution equivalent, but the converse does not hold.

1.2 ⋄ Matrices

(a) For $m, n \in \mathbb{N}$ we denote by $\mathrm{M}_{m,n}(R)$ the set of $m \times n$ matrices over R. In the case where $R = \mathbb{F}$, it is well-known that a system of linear equations is equivalent to a matrix equation on the form $Ax = b$, where $A \in \mathrm{M}_{m,n}(\mathbb{F})$, $x \in \mathbb{F}^n$ and $b \in \mathbb{F}^m$. Recall the ***elementary row operations*** on A:

(1) multiplication of one row of A by a nonzero scalar,

(2) addition to one row of A a scalar multiple of another (different) row, and

(3) interchange of two rows of A.

If e is an elementary row operation, we write $e(A)$ for the matrix obtained when applying e to A. Clearly each elementary row operation e has an 'inverse', i.e. an elementary row operation e' such that $e'(e(A)) = e(e'(A)) = A$. Two matrices $A, B \in \mathrm{M}_{m,n}(\mathbb{F})$ are called ***row-equivalent*** if A is obtained by applying a finite sequence of elementary row operations to B (and vice versa, though this need not be assumed since each elementary row operation has an inverse).

Clearly, if $A, B \in \mathrm{M}_{m,n}(\mathbb{F})$ are row-equivalent, then the systems of equations $Ax = 0$ and $Bx = 0$ are combination equivalent, hence have the same solutions.

An ***elementary matrix*** is a matrix obtained by applying a single elementary row operation to the identity matrix I. It is easy to show that if e is an elementary row operation and $E = e(I) \in \mathrm{M}_m(\mathbb{F})$, then $e(A) = EA$ for $A \in \mathrm{M}_{m,n}(\mathbb{F})$. If also $B \in \mathrm{M}_{m,n}(\mathbb{F})$, then A and B are row-equivalent if and only if $A = PB$, where $P \in \mathrm{M}_m(\mathbb{F})$ is a product of elementary matrices.

(b) We now show that every matrix is row-equivalent to a matrix with a particularly simple form:

1.1 • Definition. A matrix $H \in \mathrm{M}_{m,n}(\mathbb{F})$ is called *row-reduced* if

(i) the first nonzero entry of each nonzero row in H is 1, and

(ii) each column of H containing the leading nonzero entry of some row has all its other entries equal 0.

If H is row-reduced, it is called a *row-reduced echelon matrix* if it also has the following properties:

(iii) Every row of H only containing zeroes occur below every row which has a nonzero entry, and

(iv) if rows $1, \dots, r$ are the nonzero rows of H, and if the leading nonzero entry of row i occurs in column k_i, then $k_1 < \cdots < k_r$.

1.2 • Proposition. *Every matrix in* $\mathrm{M}_{m,n}(\mathbb{F})$ *is row-equivalent to a unique row-reduced echelon matrix.*

Proof. The usual Gauss–Jordan elimination algorithm proves existence. If $H, K \in \mathrm{M}_{m,n}(R)$ are row-equivalent row-reduced echelon matrices, we claim that $H = K$. We prove this by induction in n. If $n = 1$ then this is obvious, so assume that $n > 1$. Let H_1 and K_1 be the matrices obtained by deleting the nth column in H and K respectively. Then H_1 and K_1 are also row-equivalent[1] and row-reduced echelon matrices, so by induction $H_1 = K_1$. Thus if H and K differ, they must differ in the nth column.

Let H_2 be the matrix obtained by deleting columns in H, only keeping those columns containing pivots, as well as keeping the nth column. Define K_2 similarly. Thus we have deleted the same columns in H and K, so H_2 and

[1] It should be obvious that deleting columns preserves row-equivalence, but we give a more precise argument: If $P \in \mathrm{M}_m(\mathbb{F})$ is a product of elementary matrices and $a_1, \dots, a_n \in \mathbb{F}^m$ are the columns in A, then the columns in PA are $Pa_1, \dots, Pa_m$. Thus elementary row operations are applied to each column independently of the other columns.

K_2 are also row-equivalent. Say that the number of columns in H_2 and K_2 is $r+1$, and write the matrices on the form

$$H_2 = \begin{pmatrix} I_r & h \\ 0 & h' \end{pmatrix} \quad \text{and} \quad K_2 = \begin{pmatrix} I_r & k \\ 0 & k' \end{pmatrix},$$

where $h, k \in \mathbb{F}^r$ and $h', k' \in \mathbb{F}^{m-r}$ are column vectors. Since H_2 and K_2 are row-equivalent, the systems $H_2 x = 0$ and $K_2 x = 0$ are solution equivalent. If $h' = 0$, then $H_2 x = 0$ has the solution $(-h, 1)$. But this is also a solution to $K_2 x = 0$, so $h = k$ and $k' = 0$. If $h' \neq 0$, then $H_2 x = 0$ only has the trivial solution. But then $K_2 x = 0$ also only has the trivial solution, and hence $k' \neq 0$. But that must be because both H_2 and K_2 has a pivot in the rightmost column, so also in this case $H_2 = K_2$. ■

(c) Next we study when square matrices are invertible. The main result says for a square matrix to be invertible, it suffices that it has either a left- or a right-inverse. Since (as we will see in **??**) square matrices are precisely the linear endomorphisms on finite-dimensional vector spaces, this shows that for such an endomorphism to be invertible, it suffices that it has either a left- or a right-inverse. This result is also a direct consequence of the rank–nullity theorem, see e.g. **romanlinalg**.

Notice that elementary matrices are invertible since elementary row operations are invertible.

1.3 • Lemma. *If $A \in \mathrm{M}_n(\mathbb{F})$, then the following are equivalent:*

(i) *A is invertible,*

(ii) *A is row-equivalent to I_n,*

(iii) *A is a product of elementary matrices, and*

(iv) *the system $Ax = 0$ has only the trivial solution $x = 0$.*

Proof. *??* $\Leftrightarrow$ *??* : Let $H \in \mathrm{M}_n(\mathbb{F})$ be a row-reduced echelon matrix that is row-equivalent to A. Then $H = PA$, where $P \in \mathrm{M}_n(\mathbb{F})$ is a product of elementary matrices. Then $A = P^{-1}H$, so A is invertible if and only if H is. But the only invertible row-reduced echelon matrix is the identity matrix, so ?? and ?? are equivalent.

?? $\Rightarrow$ *??* : As above, there exists a product P of elementary matrices such that $I_n = PA$, so $A = P^{-1}$.

?? $\Rightarrow$ *??* : This is obvious since elementary matrices are invertible.

?? $\Leftrightarrow$ *??* : If A and I_n are row-equivalent, then the systems $Ax = 0$ and $I_n x = 0$ have the same solutions. Conversely, assume that $Ax = 0$ only has

the trivial solution. If $H \in \mathrm{M}_{m,n}(\mathbb{F})$ is a row-reduced echelon matrix that is row-equivalent to A, then $Hx = 0$ has no nontrivial solution. Thus if r is the number of nonzero rows in H, then $r \geq n$. But then $r = n$, so H must be the identity matrix.

1.4 • **Proposition.** *Let $A \in \mathrm{M}_n(\mathbb{F})$. Then the following are equivalent:*

(i) *A is invertible,*

(ii) *A has a left inverse, and*

(iii) *A has a right inverse.*

Proof. If A has a left inverse, then $Ax = 0$ has no nontrivial solution, so A is invertible. If A has a right inverse $B \in \mathrm{M}_n(\mathbb{F})$, i.e. $AB = I$, then B has a left inverse and is thus invertible. But then A is the inverse of B and hence is itself invertible. ∎

2 Bases and Coordinates

2.1 ◇ Bases

(a) If $\mathcal{V}$ is a subset of V, the ***span*** of $\mathcal{V}$, denoted $\operatorname{span}\mathcal{V}$ or $\langle\mathcal{V}\rangle$, is the smallest subspace of V containing $\mathcal{V}$. Equivalently, it is the set of all linear combinations

$$\alpha_1 v_1 + \cdots + \alpha_n v_n,$$

where $\alpha_i \in \mathbb{F}$ and $v_i \in \mathcal{V}$. We say that $\mathcal{V}$ is ***linearly independent*** if any linear relation

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$$

among elements v_i in $\mathcal{V}$ can only be satisfied if $\alpha_1 = \cdots = \alpha_n = 0$. If $\mathcal{V}$ is both linearly independent and a spanning set, then we call it a ***basis*** for V. We have the folloing characterisation of bases:

2.1 • Proposition. *A subset $\mathcal{V} \subseteq V$ is a basis for V if and only if*

$$V = \bigoplus_{v \in \mathcal{V}} \langle v \rangle.$$

We next prove that bases always exist, but first we need a different characterisation of bases. An element $v \in V$ is an ***essentially unique*** linear combination of the elements in $\mathcal{V}$ if there is an up to ordering unique way to express v as a linear combination of elements in $\mathcal{V}$. It is easy to see that $\mathcal{V}$ is linearly independent if and only if every nonzero $v \in \langle\mathcal{V}\rangle$ is an essentially unique linear combination of the elements in $\mathcal{V}$.

2.2 • Proposition. *Let $\mathcal{V}$ be a subset of V. The following are equivalent:*

(i) *$\mathcal{V}$ is linearly independent and spans V.*

(ii) *Every nonzero $v \in V$ is an essentially unique linear combination of vectors in $\mathcal{V}$.*

(iii) *$\mathcal{V}$ is a minimal spanning set.*

(iv) *$\mathcal{V}$ is a maximal linearly independent set.*

Proof. *??* $\Leftrightarrow$ *??* : This follows easily as mentioned above.

?? $\Leftrightarrow$ *??* : If ?? holds and a proper subset $\mathcal{V}'$ of $\mathcal{V}$ spanned V, then any element of $\mathcal{V} \setminus \mathcal{V}'$ is a linear combination of elements in $\mathcal{V}'$, so $\mathcal{V}$ is not linearly independent. Conversely, if $\mathcal{V}$ is a minimal spanning set but is not linearly independent, then some $v \in \mathcal{V}$ is a linear combination of the other elements in $\mathcal{V}$, so $\mathcal{V} \setminus \{v\}$ is also a spanning set.

?? $\Leftrightarrow$ *??* : Again assuming ?? , if $\mathcal{V}$ were not maximal there would be some $v \in V \setminus \mathcal{V}$ such that $\mathcal{V} \cup \{v\}$ were linearly independent. But then v would not be a linear combination of elements in $\mathcal{V}$. Conversely, if $\mathcal{V}$ is a maximal linearly independent set that did not span V, then there would be some $v \in V \setminus \mathcal{V}$ that is not a linear combination of elements in $\mathcal{V}$. But then $\mathcal{V} \cup \{v\}$ is also linearly independent.

2.3 • **THEOREM.** *Let V be a vector space. If $\mathcal{I} \subseteq V$ is linearly independent, $\mathcal{S} \subseteq V$ is a spanning set, and $\mathcal{I} \subseteq \mathcal{S}$, then there is a basis $\mathcal{V}$ for V with $\mathcal{I} \subseteq \mathcal{V} \subseteq \mathcal{S}$.*

Proof. Let $\mathcal{A}$ be the collection of linearly independent subsets $\mathcal{J}$ of V with $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{S}$. If $\mathcal{C}$ is a chain in $\mathcal{A}$, then

$$\mathcal{U} = \bigcup_{\mathcal{J} \in \mathcal{C}} \mathcal{J}$$

is linearly independent and satisfies $\mathcal{I} \subseteq \mathcal{U} \subseteq \mathcal{S}$, so it lies in $\mathcal{A}$. Hence every chain in $\mathcal{A}$ has an upper bound, so it has a maximal element $\mathcal{V}$. This is linearly independent since it lies in $\mathcal{A}$, and it is also a spanning set by maximality, hence it is a basis. ■

2.4 • **COROLLARY.** *Every vector space has a basis.*

Proof. Let $\mathcal{I} = \emptyset$ and $\mathcal{S} = V$ in **??**. ■

(b) We next turn to the concept of the ***dimension*** of a vector space. Our presentation will focus on finite-dimensional vector spaces.

2.5 • **PROPOSITION.** *If the vectors $v_1, \dots, v_n$ in V are linearly independent, and the vectors $w_1, \dots, w_m$ span V, then $n \leq m$.*

Proof. List the vectors as follows:

$$w_1, \dots, w_m; v_1, \dots, v_n.$$

We transform this list such that the collection of vectors on the left-hand side of the semicolon always span V, and such that the vectors on the right-hand side are always linearly independent. Note that v_1 is a linear combination of the w_j, implying that we may add v_1 to the left-hand side and remove one of the w_j (which, by reindexing, we may assume is w_1) and still have a spanning set. We simultaneously remove v_1 from the right-hand side. That is, we obtain

$$v_1, w_2, \dots, w_m; v_2, \dots, v_n.$$

If $m < n$, then applying this process recursively will eventually exhaust the w_j, at which point we would have

$$v_1, \dots, v_m; v_{m+1}, \dots, v_n.$$

But this is not possible, since v_n does not lie in the span of $v_1, \dots, v_m$. Hence $n \leq m$. ■

2.6 • **Corollary.** *If V has a finite spanning set, then all bases for V have the same cardinality.* ■

This in fact holds for arbitrary vector spaces, though the proof is significantly more involved (cf. **romanlinalg**).

Since bases always exist and all bases have the same cardinality, the following definition makes sense:

2.7 • **Definition:** ***Dimension.***
The *dimension* of a vector space V, written $\dim V$, is the cardinality of any basis for V. ▲

(c) We now turn to a different characterisation of the dimension of finite-dimensional vector spaces. Below we write $\dim V = \infty$ if the dimension of the vector space V is infinite. A ***series*** of subspaces U_i of V is a finite or infinite decreasing sequence

$$V = U_0 \supsetneq U_1 \supsetneq U_2 \supsetneq \cdots.$$

If the sequence is finite, then the ***length*** of the series is the number of strict inclusions. If the sequence is infinite, then we say that the length of the series is ∞. The maximal length of a series of subspaces of V is denoted $l(V)$.

In the proposition below, we write $\dim V = \infty$ if the dimension of V is infinite.

2.8 • **Proposition.** *Let V be a vector space. Then* $\dim V = l(V)$.

Proof. First assume that V is finite-dimensional, and let $\mathcal{V} = (v_1, \dots, v_n)$ be a basis for V. Then there is a series

$$V = \langle v_1, \dots, v_n \rangle \supsetneq \langle v_1, \dots, v_{n-1} \rangle \supsetneq \cdots \supsetneq \langle v_1 \rangle \supsetneq 0$$

of subspaces of V, so $\dim V \leq l(V)$. Conversely, let

$$V = U_0 \supsetneq U_1 \supsetneq U_2 \supsetneq \cdots$$

be a series of subspaces of V. If the series ends with 0, remove it. Hence all subspaces in the series are nontrivial. Then choose for each i an element $v_i \in U_i \setminus U_{i+1}$, and collect them in a set $\mathcal{I}$. It is clear that $\mathcal{I}$ is linearly independent, hence finite. Thus the series is also finite with length $|\mathcal{I}| - 1$. Adding back 0 to the series we obtain a series that is at least as long as the original sequence, and that is of length $|\mathcal{I}| \leq \dim V$. Since the sequence was arbitrary, $l(V) \leq \dim V$.

Next assume that V is infinite-dimensional. Then V contains a sequence $(v_i)_{i \in \mathbb{N}}$ that is linearly independent, so the series

$$V \supseteq \langle v_i \mid i \in \mathbb{N} \rangle \supsetneq \langle v_i \mid i \geq 2 \rangle \supsetneq \langle v_i \mid i \geq 3 \rangle \supsetneq \cdots$$

is infinite, and $l(V) = \infty$. Conversely, assume that V has an infinite series. As above we construct a linearly independent set $\mathcal{I}$ whose size equals the length of the sequence. Thus V contains an infinite linearly independent set, so $\dim V = \infty$. ■

2.2 ⋄ Coordinate maps and matrices

(a) Every matrix $A \in \mathrm{M}_{m,n}(\mathbb{F})$ gives rise to a map $M_A \colon \mathbb{F}^n \to \mathbb{F}^m$ given by $M_A v = Av$. The next result shows that every linear map $\mathbb{F}^n \to \mathbb{F}^m$ arises in this way:

2.9 • Proposition. *Let $(e_1, \ldots, e_n)$ be the standard basis for $\mathbb{F}^n$. The map*

$$\begin{aligned} \mathcal{M} \colon \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m) &\to \mathrm{M}_{m,n}(\mathbb{F}), \\ T &\mapsto \bigl(Te_1 \mid \cdots \mid Te_n\bigr), \end{aligned}$$

is a linear isomorphism with inverse $A \mapsto M_A$. The matrix $\mathcal{M}(T)$ is called the ***standard matrix representation*** *of T. If $T \colon \mathbb{F}^n \to \mathbb{F}^m$ and $S \colon \mathbb{F}^m \to \mathbb{F}^l$ are linear maps, then*

(i) *$Tv = \mathcal{M}(T)v$ for all $v \in \mathbb{F}^n$.*

(ii) *$\mathcal{M}(\mathrm{id}_{\mathbb{F}^n}) = I$.*

(iii) *$\mathcal{M}(S \circ T) = \mathcal{M}(S)\mathcal{M}(T)$.*

(iv) *T is invertible if and only if $\mathcal{M}(T)$ is invertible, in which case $\mathcal{M}(T^{-1}) = \mathcal{M}(T)^{-1}$.*

Proof. The map $A \mapsto M_A$ is clearly linear, so to prove the first point it suffices to show that this is the inverse of $\mathcal{M}$. Let $T \in \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$. Then

$$M_{\mathcal{M}(T)} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \mathcal{M}(T) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \bigl(Te_1 \mid \cdots \mid Te_n\bigr) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \sum_{i=1}^n \alpha_i T e_i = T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

for $\alpha_1, \dots, \alpha_n \in \mathbb{F}$. Conversely, for $A \in \mathrm{M}_{m,n}(\mathbb{F})$ we have

$$\mathcal{M}(M_A) = \Big(M_A e_1 \mid \cdots \mid M_A e_n \Big) = \Big(A e_1 \mid \cdots \mid A e_n \Big) = A,$$

since Ae_i is the ith column of A. We prove the remaining claims:

?? : Simply notice that $Tv = M_{\mathcal{M}(T)} v = \mathcal{M}(T)v$.

?? : This is obvious from the definition of $\mathcal{M}$.

?? : Let $v \in \mathbb{F}^n$ and notice that

$$\mathcal{M}(S \circ T)v = (S \circ T)v = S(Tv) = S(\mathcal{M}(T)v) = \mathcal{M}(S)\mathcal{M}(T)v$$

by ?? . Since this holds for all v, the claim follows.

?? : This follows easily from ?? and ?? .

(b) Having characterised all linear maps between powers of the field $\mathbb{F}$, we now wish to characterise the linear maps between abstract finite-dimensional vector spaces. The first order of business is to establish a correspondence between such a vector space and an appropriate power of $\mathbb{F}$.

Let V be a finite-dimensional $\mathbb{F}$-vector space. If $\mathcal{V} = (v_1, \dots, v_n)$ is an ordered basis for V, then for every $v \in V$ there are unique $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that $v = \sum_{i=1}^n \alpha_i v_i$. Hence the map $\varphi_{\mathcal{V}} \colon V \to \mathbb{F}^n$ given by $\varphi_{\mathcal{V}}(v) = (\alpha_1, \dots, \alpha_n)$ is well-defined. Furthermore, it is clearly linear, and since $\mathcal{V}$ is a basis it is also bijective, hence a linear isomorphism. The map $\varphi_{\mathcal{V}}$ is called the ***coordinate map*** with respect to $\mathcal{V}$, and the vector $[v]_{\mathcal{V}} = \varphi_{\mathcal{V}}(v)$ is called the ***coordinate vector*** of v with respect to $\mathcal{V}$.

Now let $\mathcal{W}$ be another ordered basis for V. The composition $\varphi_{\mathcal{W},\mathcal{V}} = \varphi_{\mathcal{W}} \circ \varphi_{\mathcal{V}}^{-1}$ is called the ***change of basis operator*** from $\mathcal{V}$ to $\mathcal{W}$, and this makes the diagram

$$\begin{tikzcd}
& \mathbb{F}^n \arrow[dd, "\varphi_{\mathcal{W},\mathcal{V}}"] \\
V \arrow[ur, "\varphi_{\mathcal{V}}"] \arrow[dr, "\varphi_{\mathcal{W}}"'] & \\
& \mathbb{F}^n
\end{tikzcd} \tag{2.1}$$

commute. Its standard matrix is denoted ${}_{\mathcal{W}}[\square]_{\mathcal{V}}$. This has the expected properties:

2.10 • Proposition. *Let $\mathcal{V}$, $\mathcal{W}$ and $\mathcal{U}$ be ordered bases for a finite-dimensional $\mathbb{F}$-vector space V. Then*

(i) $[v]_{\mathcal{W}} = \varphi_{\mathcal{W},\mathcal{V}}([v]_{\mathcal{V}})$ *for all $v \in V$. In particular,* $[v]_{\mathcal{W}} = {}_{\mathcal{W}}[\square]_{\mathcal{V}} \cdot [v]_{\mathcal{V}}$.

(ii) $\varphi_{\mathcal{V},\mathcal{V}}$ *is the identity map. In particular,* ${}_{\mathcal{V}}[\square]_{\mathcal{V}}$ *is the identity matrix.*

(iii) *$\varphi_{\mathcal{U},\mathcal{W}} \circ \varphi_{\mathcal{W},\mathcal{V}} = \varphi_{\mathcal{U},\mathcal{V}}$. In particular, ${}_{\mathcal{U}}[\square]_{\mathcal{W}} \cdot {}_{\mathcal{W}}[\square]_{\mathcal{V}} = {}_{\mathcal{U}}[\square]_{\mathcal{V}}$.*

(iv) *$\varphi_{\mathcal{W},\mathcal{V}}$ (resp. ${}_{\mathcal{W}}[\square]_{\mathcal{V}}$) is invertible with inverse $\varphi_{\mathcal{V},\mathcal{W}}$ (resp. ${}_{\mathcal{V}}[\square]_{\mathcal{W}}$).*

Proof. All claims about change of basis matrices follow by **??** from the corresponding claims about change of basis operators.

The claim ?? follows by commutativity of the diagram **??**, i.e.

$$\varphi_{\mathcal{W},\mathcal{V}}([v]_{\mathcal{V}}) = (\varphi_{\mathcal{W}} \circ \varphi_{\mathcal{V}}^{-1}) \circ \varphi_{\mathcal{V}}(v) = \varphi_{\mathcal{W}}(v) = [v]_{\mathcal{W}}.$$

Claim ?? is an immediate consequence of the definition of $\varphi_{\mathcal{V},\mathcal{V}}$. The remaining claims are proved similarly to ?? . ■

(c) Next consider a linear map $T\colon V \to W$. If $\mathcal{V} \in V^n$ and $\mathcal{W} \in W^m$ are bases for V and W respectively, then the diagram

$$\begin{tikzcd}
V \arrow[r, "\varphi_{\mathcal{V}}"] \arrow[d, "T"'] & \mathbb{F}^n \arrow[d, "\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}"] \\
W \arrow[r, "\varphi_{\mathcal{W}}"'] & \mathbb{F}^m
\end{tikzcd}$$

commutes. The map $\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}$ is the ***basis representation*** of T with respect to the bases $\mathcal{V}$ and $\mathcal{W}$. This is a linear map $\mathbb{F}^n \to \mathbb{F}^m$, so it has a standard matrix which we denote ${}_{\mathcal{W}}[T]_{\mathcal{V}}$. This is called the ***matrix representation*** of T with respect to the bases $\mathcal{V}$ and $\mathcal{W}$.

2.11 • Proposition. *Let V and W be finite-dimensional $\mathbb{F}$-vector spaces with ordered bases $\mathcal{V} = (v_1, \dots, v_n) \in V^n$ and $\mathcal{W} \in W^m$, respectively. The map*

$$\begin{aligned} {}_{\mathcal{W}}[\,\cdot\,]_{\mathcal{V}}\colon \mathcal{L}(V,W) &\to \mathrm{M}_{m,n}(\mathbb{F}), \\ T &\mapsto {}_{\mathcal{W}}[T]_{\mathcal{V}}, \end{aligned}$$

is a linear isomorphism. Let $T\colon V \to W$ and $S\colon W \to U$ be linear maps, and let $\mathcal{U} \in U^l$ be an ordered basis for U. Then

(i) *${}_{\mathcal{W}}[T]_{\mathcal{V}} = \big([Tv_1]_{\mathcal{W}} \mid \cdots \mid [Tv_n]_{\mathcal{W}}\big)$.*

(ii) *$[Tv]_{\mathcal{W}} = {}_{\mathcal{W}}[T]_{\mathcal{V}} \cdot [v]_{\mathcal{V}}$ for all $v \in V$.*

(iii) *If $\mathcal{V}'$ is another basis for V, then ${}_{\mathcal{V}'}[\mathrm{id}_V]_{\mathcal{V}} = {}_{\mathcal{V}'}[\square]_{\mathcal{V}}$.*

(iv) *${}_{\mathcal{U}}[S \circ T]_{\mathcal{V}} = {}_{\mathcal{U}}[S]_{\mathcal{W}} \cdot {}_{\mathcal{W}}[T]_{\mathcal{V}}$.*

(v) *T is invertible if and only if ${}_{\mathcal{W}}[T]_{\mathcal{V}}$ is invertible, in which case ${}_{\mathcal{V}}[T^{-1}]_{\mathcal{W}} = {}_{\mathcal{W}}[T]_{\mathcal{V}}^{-1}$.*

Proof. For the first claim, notice that the map $T \mapsto \varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}$ is a linear isomorphism, since pre- and postcomposition with linear isomorphisms are themselves linear isomorphisms. Composing this map with $\mathcal{M}$ yields ${}_{\mathcal{W}}[\,\cdot\,]_{\mathcal{V}}$, so this is a linear isomorphism by **??**.

?? : If $(e_1,\dots,e_n)$ is the standard basis for $\mathbb{F}^n$, then the definition of the standard matrix representation yields that the ith column of ${}_{\mathcal{W}}[T]_{\mathcal{V}}$ is given by

$$ {}_{\mathcal{W}}[T]_{\mathcal{V}} \cdot e_i = \mathcal{M}(\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}) \cdot e_i = (\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1})e_i = \varphi_{\mathcal{W}}(Tv_i) = [Tv_i]_{\mathcal{W}}, $$

as claimed.

?? : Notice that

$$ \begin{aligned} [Tv]_{\mathcal{W}} &= (\varphi_{\mathcal{W}} \circ T)(v) \\ &= (\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}) \circ \varphi_{\mathcal{V}}(v) \\ &= (\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1})([v]_{\mathcal{V}}) \\ &= {}_{\mathcal{W}}[T]_{\mathcal{V}} \cdot [v]_{\mathcal{V}}. \end{aligned} $$

where the last equality follows from **??**.

?? : This is obvious from the definitions of ${}_{\mathcal{V}'}[\mathrm{id}_V]_{\mathcal{V}}$ and ${}_{\mathcal{V}'}[\square]_{\mathcal{V}}$.

?? : Notice that

$$ \varphi_{\mathcal{U}} \circ (S \circ T) \circ \varphi_{\mathcal{V}}^{-1} = (\varphi_{\mathcal{U}} \circ S \circ \varphi_{\mathcal{W}}^{-1}) \circ (\varphi_{\mathcal{W}} \circ T \circ \varphi_{\mathcal{V}}^{-1}) $$

The claim then follows from **??**.

?? : This is an immediate consequence of either ?? or of **??**.

2.12 • Proposition. *Let $\mathcal{V} = (v_1,\dots,v_n)$ be an ordered basis for an $\mathbb{F}$-vector space V, and let $T\colon V \to V$ be a linear isomorphism. Let $\mathcal{W} = (w_1,\dots,w_n)$ where $w_i = Tv_i$. Then $\mathcal{W}$ is an ordered basis for V and*

$$ \varphi_{\mathcal{W},\mathcal{V}} = \varphi_{\mathcal{V}} \circ T^{-1} \circ \varphi_{\mathcal{V}}^{-1}, \quad \textit{or} \quad {}_{\mathcal{W}}[\square]_{\mathcal{V}} = {}_{\mathcal{V}}[T^{-1}]_{\mathcal{V}}. $$

In particular, if $V = \mathbb{F}^n$ and $\mathcal{V}$ is the standard basis $\mathcal{E}$, then

$$ \varphi_{\mathcal{W},\mathcal{E}} = T^{-1}, \quad \textit{or} \quad {}_{\mathcal{W}}[\square]_{\mathcal{E}} = \mathcal{M}(T)^{-1}. $$

We think of this result as follows: If we change basis by applying an invertible linear transformation T, we obtain the coordinate vectors corresponding to the transformed basis by applying T^{-1} (in the old basis). This says that if we perform a *passive transformation*, i.e. a change of basis while keeping vectors themselves fixed, the coordinates change by the inverse of said transformation.

Proof. Let $v \in V$ and write $v = \sum_{i=1}^{n} \alpha_i v_i$. Then

$$Tv = \sum_{i=1}^{n} \alpha_i T v_i = \sum_{i=1}^{n} \alpha_i w_i = \varphi_{\mathcal{W}}^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \varphi_{\mathcal{W}}^{-1} \circ \varphi_{\mathcal{V}}(v),$$

implying that

$$\varphi_{\mathcal{W},\mathcal{V}} = \varphi_{\mathcal{W}} \circ \varphi_{\mathcal{V}}^{-1} = (T \circ \varphi_{\mathcal{V}}^{-1})^{-1} \circ \varphi_{\mathcal{V}}^{-1} = \varphi_{\mathcal{V}} \circ T^{-1} \circ \varphi_{\mathcal{V}}^{-1}$$

as claimed. ■

3 Structural Properties of Vector Spaces

3.1 ⋄ Projections I

(a) Let V be a vector space. A linear operator $P\colon V \to V$ is called a ***projection*** if it is idempotent, i.e. if $P^2 = P$.

3.1 • **Proposition.** *A linear map $P\colon V \to V$ is a projection if and only if there exist subspaces U and W of V such that $V = U \oplus W$, $P|_U = \iota_U$ and $P|_W = 0$. In this case $U = \operatorname{im} P$ and $W = \ker P$.*

We say that P is the projection onto U along W.

Proof. Assume that P is a projection, and let $v \in \operatorname{im} P$. Then $v = Pu$ for some $u \in V$, and

$$Pv = P^2 u = Pu = v.$$

If also $v \in \ker P$, then $v = 0$. Furthermore, for any $v \in V$ we have $v = Pv + (v - Pv) \in \operatorname{im} P \oplus \ker P$, so $\operatorname{im} P$ and $\ker P$ are indeed complements in V.

The converse is obvious, and so is the characterisation of U and W. ■

(b) We will return to projections in **??**.

3.2 ⋄ Quotient spaces and complements

(a) If U is a subspace of an $\mathbb{F}$-vector space V, then its underlying additive group is a subgroup of the underlying additive group of V. Since V considered as such is abelian, we may consider the quotient group V/U whose elements are cosets $v + U$ for $v \in V$. It is then trivial to check that the operation $\alpha(v + U) := \alpha v + U$ for $\alpha \in \mathbb{F}$ makes V/U into a vector space. We denote by π_U or simply by π the quotient map $\pi\colon V \to V/U$ given by $\pi(v) = v + U$.

3.2 • **Theorem.** *Let U be a subspace of V. If $T\colon V \to W$ satisfies $U \subseteq \ker T$, then there is a unique linear map $\tilde{T}\colon V/U \to W$ such that the diagram*

$$\begin{tikzcd}
 & W \\
V \arrow[ur, "T"] \arrow[dr, "\pi"'] & \\
 & V/U \arrow[uu, dashed, "\tilde{T}"']
\end{tikzcd}$$

commutes.

Proof. The corresponding result for groups yields a unique group homomorphism $\tilde{T}$. This is easily seen to also be a linear map. TODO do I also need for topological vector spaces? If not, put in preface that e.g. $\cong$ is only linear isomorphism, not anything topological. ■

This has the following immediate consequence:

3.3 • **COROLLARY:** ***Canonical decomposition.***
Every linear map $T\colon V \to W$ may be decomposed as follows:

$$\begin{tikzcd} V \arrow[r, two heads, "\pi"'] \arrow[rrr, bend left, "T"] & V/\ker T \arrow[r, "\sim", "\tilde{T}"'] & \operatorname{im} T \arrow[r, hook, "\iota_{\operatorname{im} T}"'] & U \end{tikzcd}$$

In particular we have the ***first isomorphism theorem****: $V/\ker T \cong \operatorname{im} T$.* ■

(b) If U is a subspace of V, then a subspace W of V with the property that $V = U \oplus W$ is called a ***complement*** of U. Complements are certainly not unique, but we have the following:

3.4 • **LEMMA.** *Assume that V has two direct sum compositions*

$$U \oplus W_1 = V = U \oplus W_2,$$

where $W_1 \subseteq W_2$. Then $W_1 = W_2$.

Proof. Assume that $v \in W_2$. Then there exist unique $u \in U$ and $w \in W_1$ such that $v = u + w$. But then w also lies in W_2, and uniqueness implies that $u = 0$ and $w = v$. But then $v \in W_1$ as desired. ■

Next we note the following characterisation of complements:

3.5 • **PROPOSITION.** *Let U be a subspace of V, and let W be a complement of U. The projection P onto W along U induces an isomorphism $V/U \cong W$.*

Proof. Note that $\ker P = U$ and $\operatorname{im} P = W$ by **??**, so **??** implies that $W \cong V/U$ as claimed. [TODO if I want to do TVS, when is this a homeomorphism?] ■

(c) So far in this section we have not made use of the fact that all vector spaces have bases. This fact enters the present discussion through the following result:

3.6 • Proposition. *Every subspace U of a vector space V has a complement.*

Proof. Choose a basis $\mathcal{U}$ for U and extend it to a basis $\mathcal{V}$ for V using **??**. Then we clearly have $V = U \oplus \langle \mathcal{V} \setminus \mathcal{U} \rangle$. ■

If U is a subspace of V, then the dimension of the quotient space V/U is called the ***codimension*** of U in V and is denoted $\operatorname{codim}_V U$ or simply $\operatorname{codim} U$. The results above then implies the following:

3.7 • Corollary. *If U is a subspace of V, then*

$$\dim V = \dim U + \operatorname{codim} U.$$

3.8 • Corollary: *The rank–nullity theorem.*
Let $T \in \mathcal{L}(V,W)$. Then $\operatorname{codim} \ker T = \dim \operatorname{im} T$, *and in particular*

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

3.3 ◇ Linear maps

(a) We begin by surveying the different kinds of ways two linear maps can be 'the same'. The most general way two maps can be the same is the following:

3.9 • Definition: *Equivalence of maps.*
The linear maps $T\colon V \to W$ and $S\colon X \to Y$ are *equivalent* if there exist linear isomorphisms $P\colon X \to V$ and $Q\colon Y \to W$ such that

$$S = Q^{-1} T P.$$

The matrices $A, B \in \mathrm{M}_{m,n}(\mathbb{F})$ are *equivalent* if there exist invertible matrices $P \in \mathrm{M}_n(\mathbb{F})$ and $Q \in \mathrm{M}_m(\mathbb{F})$ such that

$$B = Q^{-1} A P.$$

If isomorphic vector spaces are 'the same', then it makes sense that this notion of sameness should be inherited by linear maps between vector spaces. In **??** we saw that a map between finite-dimensional spaces is equivalent to its basis representation.

Next we have the following notion:

3.10 • DEFINITION: ***Similarity of maps.***
The linear maps $T\colon V \to V$ and $S\colon W \to W$ are *similar* if there exists a linear isomorphism $P\colon W \to V$ such that

$$S = P^{-1}TP.$$

The matrices $A, B \in \mathrm{M}_n(\mathbb{F})$ are *similar* if there exists an invertible matrix $P \in \mathrm{M}_n(\mathbb{F})$ such that

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

Notice that this only makes sense for endomorphisms, but the two maps in question can of course be defined on different spaces. As before, endomorphisms of finite-dimensional spaces are similar to their basis representation. We will also see in **??** that a map is so-called ***diagonalisable*** if and only if it is similar to a multiplication operator.

The third and final sameness notion is easy to state for matrices, but only makes sense for general linear transformations between spaces equipped with sesquilinear forms. We give the general definition here, but it will only make sense after reading **??**.

3.11 • DEFINITION: ***Congruency of maps.***
If V and W satisfy the assumptions in **??**, then the linear maps $T\colon V \to V$ and $S\colon W \to W$ are *congruent* if there exists a linear isomorphism $P\colon W \to V$ such that

$$S = P^{*}TP.$$

The matrices $A, B \in \mathrm{M}_n(\mathbb{F})$ are *congruent* if there exists an invertible matrix $P \in \mathrm{M}_n(\mathbb{F})$ such that

$$B = P^{\top}AP.$$

This notion will turn up in the matrix representation of sesquilinear forms, cf. **??**.

Note that all of these notions can be qualified by adverbs such as 'orthogonally' or 'isometrically' if the mediating maps (or matrices) P and Q above have the corresponding properties, here of being orthogonal and isometric. [TODO but what's the difference between orthogonal and isometric??]

(b) If a linear map $T\colon V \to W$ is bijective, then its inverse is easily seen to be linear. But if T is only injective (or surjective), does it have a linear left-inverse (or right-inverse)? The answer is affirmative:

3.12 • LEMMA. *If $T\colon V \to W$ is injective (surjective), then it has a linear left-inverse (right-inverse).*

Proof. First assume that T is injective and restrict its codomain to obtain an isomorphism $\tilde{T}\colon V \to \operatorname{im} T$. If U is a complement of $\operatorname{im} T$, writing $W = \operatorname{im} T \oplus U$ and letting $S = \tilde{T}^{-1} \oplus 0$ we get a linear left-inverse of T.

Next assume that T is surjective. Writing $V = \ker T \oplus U$, $T|_U\colon U \to W$ is an isomorphism. If $\iota_U\colon U \to V$ is the inclusion map, $S = \iota_U \circ T|_U^{-1}$ is a right-inverse of T. ■

Similarly, we can ask whether monomorphisms (epimorphisms) are necessarily injective (surjective):

3.13 • **Lemma.** *If $T\colon V \to W$ is a monomorphism (epimorphism), then it is injective (surjective).*

Proof. First assume that T is not injective, and assume that $v \neq v'$ satisfy $Tv = Tv'$. Let U be a nontrivial vector space, let $u \in U$ be nonzero, and consider linear maps $S, R\colon U \to V$ with $Su = v$ and $Ru = v'$, and that agree on a complement of $\langle u \rangle$. Then $TS = TR$ but $S \neq R$, so T is not a monomorphism.

Similarly, if T is not surjective then let $w \in W \setminus \operatorname{im} T$ and define maps $S, R\colon W \to U$ that agree on a complement of $\langle w \rangle$, and that satisfy $Sw \neq Rw$. Then $ST = RT$, but $S \neq R$. ■

These lemmas together imply the following:

3.14 • **Theorem.** *A linear map is injective (surjective) if and only if it is a monomorphism (epimorphism) if and only if it has a left-inverse (right-inverse).* ■

(c) Finally we note that between *finite-dimensional* spaces, **??** has the following fundamental corollary:

3.15 • **Corollary.** *If V and W are finite-dimensional, then $T\colon V \to W$ is injective if and only if it is surjective.* ■

3.4 ◇ Duality

(a) If V is an $\mathbb{F}$-vector space, then a ***linear functional*** is a linear map $V \to \mathbb{F}$. Since $\mathbb{F}$ itself is an $\mathbb{F}$-vector space, the set $\mathcal{L}(V, \mathbb{F})$ is also vector space. We denote this by V^* and call it the ***algebraic dual space*** of V.

We note that if $v \in V$ is nonzero, then there exists a $\varphi \in V^*$ with $\varphi(v) \neq 0$: For extend v to a basis for V, let $\varphi(v) = 1$ and let $\varphi = 0$ on any complement of $\langle v \rangle$.

The algebraic dual space is of little interest when the vector space in question is an infinite-dimensional topological $\mathbb{K}$-vector space. If V is such a space, we instead often let V^* denote the ***topological dual space***, the subspace of the algebraic dual space consisting of the *continuous* functionals. In the sequel, V^* will denote the algebraic dual space unless otherwise stated.

(b) We study how a basis for V gives rise to a basis for V^*. Let $\mathcal{V} = \{v_i \mid i \in I\}$, where I is some index set, be a basis for a vector space V. For $i \in I$ we then define $v_i^* \in V^*$ by $v_i^*(v_j) = \delta_{ij}$, and let $\mathcal{V}^* = \{v_i^* \mid i \in I\}$.

3.16 • **Proposition.** *If $\mathcal{V}$ is a basis for V, then the set $\mathcal{V}^*$ is linearly independent, and hence $\dim V \leq \dim V^*$. If V is finite-dimensional and $\mathcal{V} = (v_1, \dots, v_n)$, then $\mathcal{V}^*$ is a basis for V^* called the* ***dual basis*** *of $\mathcal{V}$, and*

$$\varphi = \sum_{i=1}^{n} \varphi(v_i) v_i^*$$

for all $\varphi \in V^*$. In particular, $V \cong V^*$.

Proof. Applying the functional

$$\alpha_{i_1} v_{i_1}^* + \cdots + \alpha_{i_n} v_{i_n}^* = 0$$

to the vector v_{i_k} we find that $\alpha_{i_k} = 0$. If V is finite-dimensional with $\dim V = n$ and $\varphi \in V^*$, then

$$\varphi(v_j) = \sum_{i=1}^{n} \varphi(v_i)\delta_{ij} = \sum_{i=1}^{n} \varphi(v_i) v_i^*(v_j),$$

so $\varphi = \sum_{i=1}^{n} \varphi(v_i) v_i^* \in \langle \mathcal{V}^* \rangle$. ■

The above in particular says that if $\varphi = \varphi_1 v_1^* + \cdots + \varphi_n v_n^*$, then $\varphi_i = \varphi(v_i)$.

So in the finite-dimensional case, V and V^* are isomorphic. In the infinite-dimensional case, one can show (cf. **romanlinalg**, which says that then $\dim V < \dim V^*$) that the algebraic dual space of V always has a strictly greater dimension than V, so these cannot be isomorphic. If instead V is a topological vector space, then we instead consider the continuous dual space V^*, and since this is generally smaller than the algebraic one, V again has a chance of being isomorphic to V^* (though note that the dual basis elements are not guaranteed to be continuous). We will return to this point below.

(c) If V is a vector space, we may consider its dual V^*. And if V is finite-dimensional, then so is V^*, and so we may consider *its* dual, V^{**}. On the other hand, if V is a topological vector space, then its topological dual V^* naturally carries the weak*-topology, in which case we may also consider *its* (topological) dual. In either case we call V^{**} the (algebraic or topological) ***double dual space*** of V. This will again denote the algebraic double dual space unless we state otherwise.

We construct a map from V into V^{**} as follows: For $v \in V$ define $\mathrm{ev}_v \colon V^* \to \mathbb{F}$ by evaluation at v, i.e. $\mathrm{ev}_v(\varphi) = \varphi(v)$. This induces a map $\mathrm{ev} \colon V \to V^{**}$ given by $v \mapsto \mathrm{ev}_v$. If $v \neq w$, then we may hope to find a $\varphi \in V^*$ such that $\varphi(v) \neq \varphi(w)$, which would implies that $\mathrm{ev}_v(\varphi) \neq \mathrm{ev}_w(\varphi)$, and so ev would be injective. If V is finite-dimensional, then this is clearly possible. However, if V is an infinite-dimensional topological vector space and V^* instead denotes the topological dual, then we can still performs the constructions above, but then there might not even be any nonzero continuous linear functionals on V. This is for instance the case for the Lebesgue space $\mathcal{L}^p([0,1])$ for $p \in (0,1)$ (cf. **rudinfunctional**). On the other hand, the Hahn–Banach theorem implies that we can in fact find such a functional φ in case V is locally convex.

Whether or not ev is injective, it may not be surjective, even if V is a Banach space. If V^* denotes the algebraic dual and ev is an isomorphism, then V is called ***reflexive***. If V^* instead denotes the topological dual, then we also call V reflexive if ev is an isomorphism, but we also require it to be a homeomorphism. Indeed, as mentioned above the algebraic dual of an infinite-dimensional vector space V is of strictly greater dimension than V itself, V cannot be isomorphic to its algebraic double dual. On the other hand, finite-dimensional vector spaces are always isomorphic to their double dual, so reflexivity is fairly trivial for vector spaces that are not topological. Hence the notion is usually only interesting for topological vector spaces. Whenever we below consider V^* the algebraic (topological) dual, the property of being reflexive will be in relation to the corresponding algebraic (topological) double dual space.

Finally, if $\mathcal{V} = (v_1, \ldots, v_n)$ is a basis for V, then the basis $\mathcal{V}^*$ itself has a dual basis $\mathcal{V}^{**}$. Applying an element v_i^{**} to the functional φ then yields

$$v_i^{**}(\varphi) = \varphi_i = \varphi(v_i).$$

That is, $v_i^{**} = \mathrm{ev}_{v_i}$.

(d) In the remainder of this section we do not consider topological vector spaces. We now introduce a new concept that is useful in characterising dual spaces:

3.17 • Definition. Let $M \subseteq V$. The *annihilator* of M is the set

$$M^0 = \{\varphi \in V^* \mid \varphi|_M = 0\}.$$

It is easy to see that M^0 is a subspace of V^* even when M is not. Furthermore, notice that $\emptyset^0 = V^*$. It is also obvious that if $M \subseteq N$ then $N^0 \subseteq M^0$.

Assume that we have a direct sum decomposition $V = U \oplus W$. If $\varphi \in U^*$ then we may extend φ to a functional $\overline{\varphi}$ on V by letting $\overline{\varphi}(w) = 0$ for all

$w \in W$. We say that $\overline{\varphi}$ is the ***extension by* 0** of φ. The map $\eta \colon U^* \to V^*$ given by $\eta(\varphi) = \overline{\varphi}$ has a left-inverse, namely the pullback[1]

$$\begin{aligned} \iota_U^\dagger \colon V^* &\to U^*, \\ \psi &\mapsto \psi \circ \iota_U, \end{aligned}$$

where $\iota_U \colon U \to V$ is the inclusion map: For notice that $(\iota_U^\dagger \circ \eta)(\varphi) = \overline{\varphi} \circ \iota_U = \varphi$. In particular, η is injective and $\iota_U^\dagger$ is surjective. Now notice that $\operatorname{im} \eta = W^0$, and that $\ker \iota_U^\dagger = U^0$. Hence we have proved:

3.18 • **Proposition.** *If $V = U \oplus W$, then the map $U^* \to W^0$ given by $\varphi \mapsto \overline{\varphi}$ is an isomorphism. If U is finite-dimensional, i.e. if W has finite codimension, then in particular* $\dim W^0 = \operatorname{codim} W$. ■

3.19 • **Proposition.** *If U is a subspace of V, then $V^*/U^0 \cong U^*$.* ■

3.20 • **Corollary.** *If U is a subspace of V, then $(V/U)^* \cong U^0$.*

Proof. If W is a complement of U, then $V/U \cong W$ by **??**, so $(V/U)^* \cong W^*$. But then **??** implies the claim. ■

Finally, we can also use annihilators to characterise the dual space of a direct sum:

3.21 • **Proposition.** $(U \oplus W)^* = U^0 \oplus W^0$.

Since $U^0 \cong W^*$ and $W^0 \cong U^*$, this gives an alternative proof of **??**. TODO find a place for dual-of-product

Proof. The sum of U^0 and W^0 is clearly direct, and the inclusion '$\supseteq$' is obvious. Now let $\varphi \in V^*$, and let P_U and P_W be the projections onto U and W along W and U, respectively. then $P_W + P_U = \mathrm{id}_V$, so

$$\varphi = \varphi \circ (P_W + P_U) = \varphi \circ P_W + \varphi \circ P_U \in U^0 \oplus W^0,$$

proving the other inclusion. ■

[1] In **??** we will meet this pullback again under the name *operator adjoint*.

3.5 ⋄ Operator adjoints

(a) Let $\mathcal{C}$ be a locally small category, and let $f: A \to B$ be an arrow in $\mathcal{C}$. For every object C, precomposition with f then induces an arrow

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(f,C)\colon \mathrm{Hom}_{\mathcal{C}}(B,C) &\to \mathrm{Hom}_{\mathcal{C}}(A,C), \\ g &\mapsto g \circ f. \end{aligned}$$

This gives rise to a contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-,C)\colon \mathcal{C} \to \mathbf{Set}$. Specialising to the case where $\mathcal{C}$ is the category $\mathbb{F}$-**Vect** and where C is the field $\mathbb{F}$ (considered as a vector space), we obtain the functor $(-)^*$ sending a vector space V to its (algebraic) dual V^*, and a linear map T to its pullback. Since we will use the notation T^* for the Hilbert space adjoint, we instead write $T^\dagger$ for the pullback of T, following **follandrealanalysis**. We also call this the *operator adjoint* of T:

3.22 • Definition: *Operator adjoints.*
Let V and W be $\mathbb{F}$-vector spaces, and let $T: V \to W$ be a linear map. The *(operator) adjoint* of T is the pullback

$$\begin{aligned} T^\dagger\colon W^* &\to V^*, \\ \varphi &\mapsto \varphi \circ T. \end{aligned}$$

This already satisfies $\mathrm{id}_V^\dagger = \mathrm{id}_{V^*}$ and $(ST)^\dagger = T^\dagger S^\dagger$ by functoriality, so that in particular $(T^{-1})^\dagger = (T^\dagger)^{-1}$ when T is invertible. Furthermore, it is easy to show that the map $T \mapsto T^\dagger$ is linear. As before, if W is either finite-dimensional or a locally convex space, if $Tv \neq Sv$ there is a $\varphi \in W^*$ with $\varphi(Tv) \neq \varphi(Sv)$, so in these cases $T \mapsto T^\dagger$ is injective.

3.23 • Proposition. *Let $T \in \mathcal{L}(V,W)$.*

(i) $\ker T^\dagger = (\operatorname{im} T)^0$.

(ii) $\operatorname{im} T^\dagger = (\ker T)^0$.

Proof. For part ?? , notice that

$$\begin{aligned} \ker T^\dagger &= \{\psi \in W^* \mid T^\dagger \psi = 0\} \\ &= \{\psi \in W^* \mid \psi \circ T = 0\} \\ &= \{\psi \in W^* \mid \psi(\operatorname{im} T) = \{0\}\} \\ &= (\operatorname{im} T)^0. \end{aligned}$$

For part ?? , if $\varphi \in \operatorname{im} T^\dagger$ then there is a $\psi \in W^*$ with $\varphi = T^\dagger \psi = \psi \circ T$. Hence $\ker T \subseteq \ker \varphi$, so $\varphi \in (\ker T)^0$. For the opposite inclusion, let $\varphi \in (\ker T)^0$. Let

U be a complement of $\ker T$ and let $S\colon W \to U$ be a linear left-inverse of $T|_U$. Letting $\psi = \varphi \circ S$ we thus get

$$T^\dagger \psi = \psi \circ T = \varphi \circ S \circ T.$$

This agrees with φ on U by definition of T, and it agrees with φ on $\ker T$ since φ lies in $(\ker T)^0$. Thus $\varphi \in \operatorname{im} T^\dagger$. ■

Since $T^\dagger$ is itself a linear map, we may of course consider *its* adjoint $T^{\dagger\dagger}\colon V^{**} \to W^{**}$. If V is not reflexive, then as far as I know there is little to say about $T^{\dagger\dagger}$, but if it is then we have the following:

3.24 • **Proposition.** *If V is reflexive and $T\colon V \to W$ is linear, then*

$$T^{\dagger\dagger} = \mathrm{ev} \circ T \circ \mathrm{ev}^{-1},$$

where the leftmost ev *is evaluation on W, and the rightmost* ev *is evaluation on V.*

Proof. If $v \in V$, then notice that $T^{\dagger\dagger}\mathrm{ev}_v = \mathrm{ev}_v \circ T^\dagger$. But if $\varphi \in W^*$, then notice that

$$(\mathrm{ev}_v \circ T^\dagger)(\varphi) = (T^\dagger \varphi)v = (\varphi \circ T)v = \mathrm{ev}_{Tv}(\varphi).$$

Hence $T^{\dagger\dagger}\mathrm{ev}_v = \mathrm{ev}_{Tv}$ for all $v \in V$, so $T^{\dagger\dagger} \circ \mathrm{ev} = \mathrm{ev} \circ T$. The claim follows since V is reflexive. ■

(b) We now consider the case where V and W are finite-dimensional in more detail.

3.25 • **Corollary.** *If $T \in \mathcal{L}(V,W)$ with V and W finite-dimensional, then* $\operatorname{rank} T^\dagger = \operatorname{rank} T$.

Proof. Note that

$$\dim \operatorname{im} T^\dagger \overset{(1)}{=} \dim(\ker T)^0 \overset{(2)}{=} \operatorname{codim} \ker T \overset{(3)}{=} \dim \operatorname{im} T,$$

where (1) follows by **??**, (2) by **??**, and (3) by **??**. ■

3.26 • **Proposition.** *If $T \in \mathcal{L}(V,W)$ is a linear map between finite-dimensional vector spaces, and $\mathcal{V}$ and $\mathcal{W}$ are ordered bases for V and W respectively, then*

$${}_{\mathcal{V}^*}[T^\dagger]_{\mathcal{W}^*} = \bigl({}_{\mathcal{W}}[T]_{\mathcal{V}}\bigr)^\top.$$

Proof. Write $\mathcal{V} = (v_1, \dots, v_n)$ and $\mathcal{W} = (w_1, \dots, w_m)$. Then

$$\bigl({}_{\mathcal{W}}[T]_{\mathcal{V}}\bigr)_{ij} = \bigl([Tv_j]_{\mathcal{W}}\bigr)_i = w_i^*(Tv_j),$$

and

$$\bigl({}_{\mathcal{V}^*}[T^\dagger]_{\mathcal{W}^*}\bigr)_{ij} = \bigl([T^\dagger w_j^*]_{\mathcal{V}^*}\bigr)_i = v_i^{**}(T^\dagger w_j^*) = T^\dagger w_j^*(v_i) = w_j^*(Tv_i).$$

These expressions are the same, but with i and j switched. ■

From this we obtain the following result on the row and column rank of a matrix. This is often proved by showing that one can apply elementary row and column operations to the matrix in question, preserving the row and column rank, and obtain a diagonal matrix whose entries are either zero or one. The common row and column rank of the matrix is then simply the number of ones. Going through the abstract theory above we avoid these considerations.

3.27 • **Corollary.** *The row rank and the column rank of a matrix $A \in \mathrm{M}_{m,n}(\mathbb{F})$ are equal.*

Proof. The matrix representation of the multiplication operator M_A with respect to the standard bases on $\mathbb{F}^n$ and $\mathbb{F}^m$ is just A itself, and **??** then implies that the matrix representation of $(M_A)^\dagger$ with respect to the dual bases is $A^\top$. But the rank of an operator equals the rank of any matrix representation of that operator, so **??** implies that A and $A^\top$ have the same (column) rank. Finally, the column rank of $A^\top$ is the row rank of A, proving the claim. ■

(c) If V and W are instead *topological* vector spaces, of arbitrary dimension, and V^* and W^* denote their respective *continuous* dual spaces, then we may also consider the adjoint $T^\dagger$ of a *continuous* linear map $T\colon V \to W$. It then turns out that $T^\dagger$ is also continuous when V^* and W^* are equipped with the appropriate topologies.

3.28 • **Proposition.** *Let $T\colon V \to W$ be a continuous linear map, and let $T^\dagger\colon W^* \to V^*$ be its adjoint.*

(i) *$T^\dagger$ is continuous with respect to the weak*-topologies on W^* and V^*.*

(ii) *If V and W are normed vector spaces, then $T^\dagger$ is continuous with respect to the operator norms on W^* and V^*, and $\|T^\dagger\| = \|T\|$.*

Proof. Let $(\varphi_i)_{i\in I}$ be a net in W^* that converges to some $\varphi \in W^*$. That is, $\varphi_i(w) \to \varphi(w)$ for all $w \in W$, so in particular $\varphi_i(Tv) \to \varphi(Tv)$ for all $v \in V$. But then $T^\dagger\varphi_i = \varphi_i \circ T$ converges to $T^\dagger\varphi = \varphi \circ T$, so $T^\dagger$ is continuous as claimed.

If V and W are normed, then

$$\|T^\dagger\varphi\| = \|\varphi \circ T\| \leq \|\varphi\|\,\|T\|$$

for all $\varphi \in W^*$, implying that $T^\dagger$ is bounded with $\|T^\dagger\| \leq \|T\|$. If $T \neq 0$, then let $v \in V$ with $\|v\| = 1$ such that $Tv \neq 0$. The Hahn–Banach theorem then furnishes a $\varphi \in W^*$ with $\|\varphi\| = 1$ and $\varphi(Tv) = \|Tv\|$ (cf. **follandrealanalysis**). It follows that

$$\|T^\dagger\| \geq \|T^\dagger\varphi\| \geq |(T^\dagger\varphi)v| = |\varphi(Tv)| = \|Tv\|.$$

This inequality then holds for all $v \in V$ with $\|v\| = 1$, implying that $\|T^{\dagger}\| \geq \|T\|$. ■

3.6 ⋄ Resolutions of the identity

Let V be a vector space. Two projections $P, Q \in \mathcal{L}(V)$ are said to be ***orthogonal*** if $PQ = QP = 0$, in which case we write $P \perp Q$. A ***resolution of the identity*** on V is a decomposition

$$\mathrm{id}_V = P_1 + \cdots + P_k.$$

of the identity map on V, where $P_1, \ldots, P_k$ are pairwise orthogonal projections on V. If V is an inner product space and the P_i are themselves orthogonal projections, then we also say that the resolution of the identity is ***orthogonal***. [TODO move orthogonal to somewhere in chapter on sesquilinear]

3.29 • Proposition. *If* $\mathrm{id}_V = P_1 + \cdots + P_k$ *is a resolution of the identity, then*

$$V = \operatorname{im} P_1 \oplus \cdots \oplus \operatorname{im} P_k, \quad \textit{and} \quad \ker P_i = \bigoplus_{j \neq i} \operatorname{im} P_j$$

for all $i = 1, \ldots, k$. *Conversely, if*

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

and P_i *is the projection onto* U_i *along* $\bigoplus_{j \neq i} U_j$, *then* $\mathrm{id}_V = P_1 + \cdots + P_k$ *is a resolution of the identity.*

Proof. Clearly V is a (not necessarily direct) sum of the above images. To see that the sum is direct, if for $v_1, \ldots, v_k \in V$ we have

$$P_1 v_1 + \cdots P_k v_k = 0,$$

then applying P_i we get $P_i v_i = 0$. Furthermore, we clearly have $\bigoplus_{j \neq i} \operatorname{im} P_j \subseteq \ker P_i$ by orthogonality. For the opposite inclusion, notice that

$$\operatorname{im} P_i \oplus \ker P_i = V = \operatorname{im} P_i \oplus \left(\bigoplus_{j \neq i} \operatorname{im} P_j \right).$$

And since $\bigoplus_{j \neq i} \operatorname{im} P_j \subseteq \operatorname{im} P_i$ by orthogonality, the opposite inclusion follows from **??**.

For the converse, if $i \neq j$ then $\operatorname{im} P_i = U_i \subseteq \ker P_j$, so $P_i \perp P_j$. Furthermore, if $v = u_1 + \cdots + u_k$ with $u_i \in U_i$, then $P_i v = u_i$, so

$$v = u_1 + \cdots + u_k = P_1 v + \cdots + P_k v = (P_1 + \cdots + P_k) v,$$

as desired. ■

4 Determinants

4.1 ◇ Existence and uniqueness

(a) We begin by establishing some terminology and some basic properties of maps between modules. If $M_1,\dots,M_n,N$ are modules over a commutative ring R, a map

$$\varphi\colon M_1 \times \cdots \times M_n \to N$$

is called ***n-linear*** if, for all i, the maps $m_i \mapsto \varphi(m_1,\dots,m_n)$ are linear for all choices of $m_j \in M_j$ where $j \neq i$. Since there is a natural isomorphism $\mathrm{M}_{m,n}(R) \cong (R^n)^m$, a map $\varphi\colon \mathrm{M}_{m,n}(R) \to N$ that is linear in each row is also called n-linear.

In the case $M_1 = \cdots = M_n$, we call φ ***alternating*** if $\varphi(m_1,\dots,m_n) = 0$ whenever $m_i = m_j$ for some $i \neq j$. Furthermore, φ is called ***skew-symmetric*** if

$$\begin{aligned}\varphi(m_1,\dots,m_{i-1},m_i,m_{i+1},\dots,m_{j-1},m_j,m_{j+1},\dots,m_n)&\\ = -\varphi(m_1,\dots,m_{i-1},m_j,m_{i+1},\dots,m_{j-1},m_i,m_{j+1},\dots,m_n)&\end{aligned}$$

for all $i < j$.

With this terminology at hand, we can now define determinants:

4.1 • Definition: ***Determinant functions.***
If n be a positive integer, a *determinant function* is a map $\varphi\colon \mathrm{M}_n(R) \to R$ that is n-linear, alternating, and which satisfies $\varphi(I_n) = 1$. ▲

Before proceeding with proving the existence of determinants, we need the following lemma:

4.2 • Lemma. *Let M and N be R-modules, and let $\varphi\colon M^n \to N$ be an n-linear map.*

(i) *If φ is alternating, then φ is skew-symmetric. If* $\operatorname{char} R \neq 2$ *then the converse also holds.*

(ii) *If $\varphi(m_1,\dots,m_n) = 0$ whenever $m_i = m_{i+1}$ for some $i = 1,\dots,n-1$, then φ is alternating.*

We shall not use the converse direction of **??** but we include it for completeness.

Proof. *??* : Consider $m_1,\dots,m_n \in M$, and let $1 \leq i < j \leq n$. Define a map $\psi\colon M \times M \to N$ by

$$\psi(a,b) = \varphi(m_1,\dots,m_{i-1},a,m_{i+1},\dots,m_{j-1},b,m_{j+1},\dots,m_n),$$

and notice that it suffices to show that $\psi(m_i,m_j) = -\psi(m_j,m_i)$. But ψ is 2-linear and alternating, so for $a,b \in M$ we have

$$\psi(a+b,a+b) = \psi(a,a)+\psi(a,b)+\psi(b,a)+\psi(b,b) = \psi(a,b)+\psi(b,a).$$

Thus $\psi(m_i,m_j) = -\psi(m_j,m_i)$, so φ is skew-symmetric as claimed.

Conversely, if $\operatorname{char} R \neq 2$ and ψ is skew-symmetric, then since $\psi(a,b) = -\psi(b,a)$, letting $a = b$ we have $2\psi(a,a) = 0$, so $\psi(a,a) = 0$.

?? : The argument above shows that, in particular, if $A,B \in M^n$, and B is obtained from A by interchanging two adjacent elements, then $\varphi(B) = -\varphi(A)$. Assuming now that B is obtained from A by interchanging the ith and jth elements in A, with $i < j$, we claim that we may obtain B by successively interchanging adjacent elements of A. Writing $A = (m_1,\dots,m_n)$, we first perform $j-i$ such interchanges and arrive that the tuple

$$(m_1,\dots,m_{i-1},m_{i+1},\dots,m_{j-1},m_j,m_i,m_{j+1},\dots,m_n),$$

moving m_i to the right $j-i$ places. Next we perform another $j-i-1$ interchanges, moving m_j to the left until we reach

$$B = (m_1,\dots,m_{i-1},m_j,m_{i+1},\dots,m_{j-1},m_i,m_{j+1},\dots,m_n).$$

Since each interchange results in a sign change, we have

$$\varphi(B) = (-1)^{2(j-i)-1}\varphi(A) = -\varphi(A).$$

If $m_i = m_j$ for $i < j$, then we claim that $\varphi(A) = 0$. For let B be obtained from A by interchanging m_{i+1} and m_j. Then $\varphi(B) = 0$, so $\varphi(A) = -\varphi(B) = 0$ by the above argument, and hence φ is alternating as claimed.

(b) We now proceed with constructing determinants. If $A \in \mathrm{M}_n(R)$ with $n > 1$ and $1 \leq i,j \leq n$, denote by $M(A)_{i,j}$ the matrix in $\mathrm{M}_{n-1}(R)$ obtained by removing the the ith row and the jth column of A. This is called the ***(i, j)-th minor*** of A. If $\varphi\colon \mathrm{M}_{n-1}(R) \to R$ is an $(n-1)$-linear function and $A \in \mathrm{M}_n(R)$, then we write $\varphi_{i,j}(A) = \varphi(M(A)_{i,j})$. Then $\varphi_{i,j}\colon \mathrm{M}_n(R) \to R$ is clearly linear in all rows except row i, and is independent of row i.

We construct determinants recursively, using the Laplace expansion:

4.3 • Theorem: ***Construction of determinants.***
Let $n > 1$, and let $\varphi\colon \mathrm{M}_{n-1}(R) \to R$ be alternating and $(n-1)$-linear. For $j = 1,\dots,n$ define a map $\psi_j\colon \mathrm{M}_n(R) \to R$ by

$$\psi_j(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \varphi_{i,j}(A),$$

for $A = (a_{ij}) \in \mathrm{M}_n(R)$. Then ψ_j is alternating and n-linear. If φ is a determinant function, then so is ψ_j.

Proof. Let $A = (a_{ij}) \in \mathrm{M}_n(R)$. Then $A \mapsto a_{ij}$ is independent of all rows except row i, and $\varphi_{i,j}$ is linear in all rows except row i. Thus $A \mapsto a_{ij}\varphi_{i,j}(A)$ is linear in all rows except row i. Conversely, $A \mapsto a_{ij}$ is linear in row i, and $\varphi_{i,j}$ is independent of row i, so $A \mapsto a_{ij}\varphi_{i,j}(A)$ is also linear in row i. Since ψ_j is a linear combination of n-linear maps, is it itself n-linear.

Now assume that A has two equal adjacent rows, say $a_k, a_{k+1} \in R^n$. If $i \neq k$ and $i \neq k+1$, then $M(A)_{i,j}$ has two equal rows, so $\varphi_{i,j}(A) = 0$. Thus

$$\psi_j(A) = (-1)^{k+j} a_{kj} \varphi_{k,j}(A) + (-1)^{k+1+j} a_{(k+1)j} \varphi_{k+1,j}(A).$$

Since $a_k = a_{k+1}$ we also have $a_{kj} = a_{(k+1)j}$ and $M(A)_{k,j} = M(A)_{k+1,j}$. Thus $\psi_j(A) = 0$, so **??** implies that ψ_j is alternating.

Finally suppose that φ is a determinant function. Then $M(I_n)_{j,j} = I_{n-1}$ and we have

$$\psi_j(I_n) = (-1)^{j+j} \varphi_{j,j}(I_n) = \varphi(I_{n-1}) = 1,$$

so ψ_j is also a determinant function. ■

4.4 • Corollary: ***Existence of determinants.***
For every positive integer n, there exists a determinant function $\mathrm{M}_n(R) \to R$.

Proof. The identity map on $\mathrm{M}_1(R) \cong R$ is a determinant function for $n = 1$, and **??** allows us to recursively construct a determinant for each $n > 1$. ■

(c) We finally show that determinants are unique by showing that any determinant function must be given by the Leibniz formula:

4.5 • Theorem: ***Uniqueness of determinants.***
Let n be a positive integer. There is precisely one determinant function on $\mathrm{M}_n(R)$, namely the function $\det\colon \mathrm{M}_n(R) \to R$ given by

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

for $A = (a_{ij}) \in \mathrm{M}_n(R)$. If $\varphi\colon \mathrm{M}_n(R) \to R$ is any alternating n-linear function, then

$$\varphi(A) = (\det A)\varphi(I_n).$$

We use the notation det for the unique determinant on $\mathrm{M}_n(R)$ for all n.

Proof. Let $e_1,\dots,e_n$ denote the rows of I_n, and denote the rows of a matrix $A=(a_{ij})\in\mathrm{M}_n(R)$ by $a_1,\dots,a_n$. Then $a_i=\sum_{j=1}^n a_{ij}e_j$, so

$$\varphi(A)=\sum_{k_1,\dots,k_n} a_{1k_1}\cdots a_{nk_n}\varphi(e_{k_1},\dots,e_{k_n}),$$

where the sum is taken over all $k_i=1,\dots,n$. Since φ is alternating we have $\varphi(e_{k_1},\dots,e_{k_n})=0$ if two of the indices $k_1,\dots,k_n$ are equal. Thus it suffices to sum over those sequences $(k_1,\dots,k_n)$ that are permutations of $(1,\dots,n)$, and so

$$\varphi(A)=\sum_{\sigma\in S_n} a_{1\sigma(1)}\cdots a_{n\sigma(n)}\varphi(e_{\sigma(1)},\dots,e_{\sigma(n)}).$$

Next notice that, since φ is also skew-symmetric by **??**, we have $\varphi(e_{\sigma(1)},\dots,e_{\sigma(n)})=(-1)^m\varphi(e_1,\dots,e_n)$, where m is the number of transpositions of $(1,\dots,n)$ it takes to obtain the permutation $(\sigma(1),\dots,\sigma(n))$. But then $(-1)^m$ is just the sign of σ, so

$$\varphi(A)=\sum_{\sigma\in S_n}(\operatorname{sgn}\sigma)a_{1\sigma(1)}\cdots a_{n\sigma(n)}\varphi(I_n).$$

Finally, if φ is a determinant function, then $\varphi(I_n)=1$, so we must have $\varphi=\det$. The rest of the theorem follows directly from this. ■

4.2 ◇ Properties of determinants

(a) We begin with what is surely the most important property of determinants, which is also our first application of the uniqueness theorem for determinants:

4.6 • Theorem. *Let $A,B\in\mathrm{M}_n(R)$. Then*

$$\det AB=(\det A)(\det B).$$

In particular, $\det\colon \mathrm{GL}_n(R)\to R^*$ *is a group homomorphism.*

Proof. The map $\varphi\colon \mathrm{M}_n(R)\to R$ given by $\varphi(A)=\det AB$ is clearly n-linear and alternating. Hence $\varphi(A)=(\det A)\varphi(I)$, and $\varphi(I)=\det B$.

Furthermore, if A is invertible, then $1=\det I=(\det A)(\det A^{-1})$. Thus $\det A\in R^*$, so det is a group homomorphism as claimed. ■

4.7 • Corollary. *If $A,B\in\mathrm{M}_n(\mathbb{F})$ are similar matrices, then* $\det A=\det B$.

Proof. Let $P\in\mathrm{M}_n(\mathbb{F})$ be such that $B=P^{-1}AP$. **??** then implies that

$$\det B=(\det P^{-1})(\det A)(\det P)=(\det A)(\det P^{-1}P)=\det A.$$

?? allows us to define the determinant of a general linear operator $T\colon V \to V$ on a finite-dimensional $\mathbb{F}$-vector space. If $\mathcal{V}$ and $\mathcal{W}$ are bases for V, then the matrix representations ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ and ${}_{\mathcal{W}}[T]_{\mathcal{W}}$ are similar. This allows us to define the determinant $\det T$ of T as the matrix representation ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ for any basis $\mathcal{V}$.

Next the fairly obvious result that the determinant of a matrix equals the determinant of its transpose:

4.8 • PROPOSITION. *Let* $A \in \mathrm{M}_n(R)$. *Then* $\det A = \det A^\top$.

Proof. Writing $A = (a_{ij})$, first notice that

$$\det A^\top = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma^{-1}) a_{\sigma(1)1} \cdots a_{\sigma(n)n},$$

since $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$. Next notice that, if $j = \sigma(i)$, then $a_{\sigma(i)i} = a_{j\sigma^{-1}(j)}$. Since R is commutative, it follows that

$$\det A^\top = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma^{-1}) a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)},$$

and since $\sigma \mapsto \sigma^{-1}$ is a bijection on S_n, it follows that $\det A^\top = \det A$ as desired. ■

(b) Let $A \in \mathrm{M}_n(R)$. For $1 \leq i, j \leq n$, the ***(i, j)-th cofactor*** of A is the number $A_{i,j} = (-1)^{i+j} \det M(A)_{i,j}$, where we recall that $M(A)_{i,j}$ is the (i,j)-th minor of A. The ***cofactor matrix*** of A is the matrix $\operatorname{cof} A \in \mathrm{M}_n(R)$ whose (i,j)-th entry is the cofactor $A_{i,j}$. Note that

$$(A^\top)_{i,j} = (-1)^{i+j} \det M(A^\top)_{i,j} = (-1)^{j+i} \det M(A)_{j,i} = A_{j,i},$$

so $\operatorname{cof} A^\top = (\operatorname{cof} A)^\top$. Of greater importance than the cofactor matrix is the ***adjoint matrix*** of A, written $\operatorname{adj} A$, which is just the transpose of $\operatorname{cof} A$. That is, the (i,j)-th entry of $\operatorname{adj} A$ is the cofactor $A_{j,i}$. Similar to the cofactor matrix we have

$$\operatorname{adj} A^\top = (\operatorname{cof} A^\top)^\top = \operatorname{cof} A = (\operatorname{adj} A)^\top.$$

We then have the following:

4.9 • PROPOSITION. *Let* $A \in \mathrm{M}_n(R)$. *Then*

$$(\operatorname{adj} A)A = (\det A)I = A(\operatorname{adj} A).$$

Proof. Writing $A = (a_{ij})$ and fixing some $j \in \{1,\dots,n\}$, **??** implies that

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

which is just the (j,j)-th entry in the product $(\operatorname{adj} A)A$.

Next we claim that if $k \neq j$, then $\sum_{i=1}^{n} a_{ik} A_{i,j} = 0$. Let $B = (b_{ij}) \in \mathrm{M}_n(R)$ be the matrix obtained from A by replacing the jth column of A by its kth column. Then B has two equal columns, so $\det B = 0$. Also, $b_{ij} = a_{ik}$ and $M(B)_{i,j} = M(A)_{i,j}$, so it follows that

$$\begin{aligned} 0 = \det B &= \sum_{i=1}^{n} (-1)^{i+j} b_{ij} \det M(B)_{i,j} \\ &= \sum_{i=1}^{n} (-1)^{i+j} a_{ik} \det M(A)_{i,j} = \sum_{i=1}^{n} a_{ik} A_{i,j}. \end{aligned}$$

That is, the (j,k)-th entry of the product $(\operatorname{adj} A)A$ is zero, so the off-diagonal entries of $(\operatorname{adj} A)A$ are zero. In total we thus have $(\operatorname{adj} A)A = (\det A)I$.

Finally we prove the equality $A(\operatorname{adj} A) = (\det A)I$, Applying the first equality to $A^\top$ yields

$$(\operatorname{adj} A^\top)A^\top = (\det A^\top)I = (\det A)I,$$

and transposing we get

$$A(\operatorname{adj} A) = A(\operatorname{adj} A^\top)^\top = (\det A)I$$

as desired. ■

4.10 • **Corollary.** *Let $A \in \mathrm{M}_n(R)$. The following are equivalent:*

(i) *A is a (two-sided) unit in $\mathrm{M}_n(R)$.*

(ii) *A is a left- or right-unit in $\mathrm{M}_n(R)$.*

(iii) *$\det A$ is a unit in R.*

Proof. If A is e.g. a left-unit, then **??** implies that

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

so $\det A$ is a unit in R. Conversely, if $\det A$ is a unit then **??** implies that $(\det A)^{-1}(\operatorname{adj} A)$ is a two-sided inverse of A. ■

Notice that this gives us a second proof of the fact that a matrix is invertible just when it has either a left- or right-inverse. In fact, we see that this holds for matrices with entries in any commutative ring.

(c) We close this section by proving a result on the determinant of a block matrix:

4.11 • **Proposition.** *Let $A_{11},\dots,A_{nn}$ be square matrices with entries in R and consider the block matrix*

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

where the remaining A_{ij} are matrices of appropriate dimensions. Then $\det M = \prod_{i=1}^n \det A_{ii}$.

Proof. By induction it suffices to consider the case where M has the block form

$$M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix},$$

where $A \in \mathrm{M}_r(R)$, $B \in \mathrm{M}_s(R)$ and $C \in \mathrm{M}_{r,s}(R)$ for appropriate integers r,s. Notice that if we define the matrices

$$M_1 = \begin{pmatrix} I_r & 0 \\ 0 & B \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} A & C \\ 0 & I_s \end{pmatrix},$$

then $M = M_1 M_2$. But using **??** we easily see that $\det M_1 = \det B$ and $\det M_2 = \det A$, so it follows that

$$\det M = (\det M_1)(\det M_2) = (\det A)(\det B)$$

as desired. ■

4.3 ⋄ Cross products

(a) We now study rigorously the well-known

4.12 • **Definition:** ***Cross products.***
Let $v = (\alpha_1, \alpha_2, \alpha_3)$ and $w = (\beta_1, \beta_2, \beta_3)$ be vectors in $\mathbb{R}^3$. The *cross product* of v and w is the vector

$$v \times w = \begin{pmatrix} \alpha_2\beta_3 - \alpha_3\beta_2 \\ \alpha_3\beta_1 - \alpha_1\beta_3 \\ \alpha_1\beta_2 - \alpha_2\beta_1 \end{pmatrix}.$$

Denote the standard basis on $\mathbb{R}^3$ by $\mathcal{E} = (e_1, e_2, e_3)$. We easily see that $e_i \times e_j = e_k$ when (i,j,k) is a cyclic permutation of $(1,2,3)$. Perhaps surprisingly, there is an important connection between cross products and determinants which from which will follow most of the elementary properties of cross products:

4.13 • **Lemma.** *Let $v, w, u \in \mathbb{R}^3$. Then*

$$\langle u, v \times w \rangle = \det(u, v, w).$$

Proof. By multilinearity of the inner product and of determinants, it suffices to prove the lemma when u is a basis vector. But it is clear that

$$\langle e_i, v \times w \rangle = \det(e_i, v, w),$$

as desired. ■

The product $\langle u, v \times w \rangle$ is called the ***(scalar) triple product*** of u, v and w, and is denoted $[u, v, w]$. We call it the *scalar* triple product to distinguish it from the *vector* triple product $u \times (v \times w)$, whose properties we will examine in **??**. The scalar triple product has some very nice properties summarised in the following proposition:

4.14 • **Proposition.** *Let $u, v, w \in \mathbb{R}^3$.*

(i) *The cross product map $(v, w) \mapsto v \times w$ is bilinear.*

(ii) $v \times w = -w \times v$.

(iii) *The triple product $[u, v, w]$ is invariant under cyclic permutations, i.e.*

$$[u, v, w] = [v, w, u] = [w, u, v]$$

and invariant under interchange of inner product and cross product, i.e.

$$\langle u, v \times w \rangle = [u, v, w] = \langle u \times v, w \rangle.$$

(iv) $v \times w = 0$ *if and only if v and w are linearly dependent.*

(v) $v \times w$ *is orthogonal to both v and w.*

Proof. The first three claims follow from **??** since the determinant is multilinear and alternating (hence skew-symmetric).

For the fourth claim, if v and w are linearly dependent then $\det(u, v, w) = 0$ for all $u \in \mathbb{R}^3$, so $v \times w = 0$. Conversely, if v and w are linearly independent, then extending to a basis (u, v, w) for $\mathbb{R}^3$ we have $\det(u, v, w) \neq 0$, implying that $v \times w \neq 0$.

To prove the final claim, notice that

$$\langle v, v \times w \rangle = \det(v, v, w) = 0,$$

and similarly for w. ■

4.15 • Proposition. *Let $a,b,v,w \in \mathbb{R}^3$. Then*

$$\langle a\times b, v\times w\rangle = \det\begin{pmatrix} \langle a,v\rangle & \langle b,v\rangle \\ \langle a,w\rangle & \langle b,w\rangle \end{pmatrix}.$$

In particular,

$$\|v\times w\|^2 = \det\begin{pmatrix} \|v\|^2 & \langle v,w\rangle \\ \langle v,w\rangle & \|w\|^2 \end{pmatrix}. \tag{4.1}$$

Proof. By linearity it suffices to prove the identity when the four vectors are basis vectors. If $a = b$ or $v = w$ then both sides are zero, so we may assume that $a = e_i$, $b = e_j$, $v = e_k$ and $v = e_l$ with $i \neq j$ and $k \neq l$. By potentially swapping a and b and/or v and w we may assume that $e_i \times e_j = e_p$ and $e_k \times e_l = e_q$ for some $p,q \in \{1,2,3\}$.

If $p = q$ then $i = k$ and $j = l$, so both sides equal 1. If instead $p \neq q$, then the two cross products on the left-hand side are orthogonal, so the inner product is zero. Furthermore, either k or l equals p, so one of the rows in the right-hand side matrix is zero, and hence the determinant is zero. ■

The identity **??** is just Lagrange's identity in three dimensions. If θ is the angle between v and w, then $\langle v,w\rangle = \|v\|\|w\|\cos\theta$, so

$$\|v\times w\|^2 = \|v\|^2\|w\|^2 - \langle v,w\rangle^2 = \|v\|^2\|w\|^2(1-\cos^2\theta) = \|v\|^2\|w\|^2\sin^2\theta.$$

Hence $\|v\times w\| = \|v\|\|w\||\sin\theta|$, which is the area of the parallelogram spanned by v and w. If $u \in \mathbb{R}^3$ is another vector and φ is the angle between u and the normal of the plane spanned by v and w (e.g. $v\times w$), then

$$\big|[u,v,w]\big| = |\langle u, v\times w\rangle| = \|u\|\|v\times w\||\cos\varphi| = \|u\|\|v\|\|w\||\sin\theta\cos\varphi|.$$

But this is the volume of the parallelepiped spanned by u, v and w. This gives a geometric interpretation (or 'proof') of the invariance of the scalar triple product.

4.16 • Corollary. *Let $u,v,w \in \mathbb{R}^3$. Then*

$$u\times(v\times w) = v\langle u,w\rangle - w\langle u,v\rangle. \tag{4.2}$$

In particular, the cross product satisfies the ***Jacobi identity***

$$u\times(v\times w) + v\times(w\times u) + w\times(u\times v) = 0. \tag{4.3}$$

The identity **??** is sometimes called the 'bac-cab rule', a name that would have been self-explanatory had we used the names a, b and c instead of u, v and w. Note that to conform to this rule we need to write the vectors before the scalars.

Proof. For $x \in \mathbb{R}^3$ we have

$$\begin{aligned}\langle x, u \times (v \times w)\rangle &= [x, u, v \times w] \\ &= \langle x \times u, v \times w\rangle \\ &= \det\begin{pmatrix}\langle x, v\rangle & \langle u, v\rangle \\ \langle x, w\rangle & \langle u, w\rangle\end{pmatrix} \\ &= \langle x, v\rangle\langle u, w\rangle - \langle u, v\rangle\langle x, w\rangle \\ &= \Big\langle x, v\langle u, w\rangle - w\langle u, v\rangle\Big\rangle.\end{aligned}$$

The claim then follows since x was arbitrary. ■

(b) We now study how the cross product transforms under linear transformations. Since $\mathrm{M}_d(\mathbb{R})$ is a finite-dimensional vector space, it has a unique vector space topology. More concretely, all norms on $\mathrm{M}_d(\mathbb{R})$ are Lipschitz equivalent, so we may choose whatever norm we wish. We choose the Euclidean norm, identifying $\mathrm{M}_d(\mathbb{R})$ with $\mathbb{R}^{d^2}$. First a lemma:

4.17 • **Lemma.** $\mathrm{GL}_d(\mathbb{R})$ *is dense in* $\mathrm{M}_d(\mathbb{R})$.

Proof. Let $A \in \mathrm{M}_d(\mathbb{R})$, and let $t \in \mathbb{R} \setminus \{0\}$. Then $A - tI$ is invertible if and only if $\det(A - tI) = 0$, but $\det(A - tI)$ is a polynomial in t, so it has finitely many roots. Hence the nonzero roots of $\det(A - tI)$ are bounded away from zero, so since $A - tI \to A$ as $t \to 0$, the claim follows. ■

4.18 • **Proposition:** ***Transformation of cross products.***
Let $u, v, w \in \mathbb{R}^3$, and let $A \in \mathrm{M}_3(\mathbb{R})$. Then we have the following:

(i) $[Au, Av, Aw] = (\det A)[u, v, w]$.

(ii) $Av \times Aw = (\operatorname{cof} A)(v \times w) = (\operatorname{adj} A)^\top (v \times w)$.

(iii) *If A is orthogonal, then* $A(v \times w) = (\det A)(Av \times Aw)$.

Proof. *??* : Simply notice that

$$[Au, Av, Aw] = \det(Au, Av, Aw) = (\det A)\det(u, v, w) = (\det A)\langle u, v \times w\rangle,$$

where the second equality follows since $\det(Au, Av, Aw)$ is also the determinant of the matrix

$$\Big(Au \mid Av \mid Aw\Big) = A\Big(u \mid v \mid w\Big),$$

and the determinant is multiplicative.

?? : First assume that A is invertible. Then replacing u with $A^{-1}u$ in ?? we obtain

$$\begin{aligned}\langle u, Av \times Aw\rangle &= (\det A)\langle A^{-1}u, v \times w\rangle \\ &= (\det A)\langle u, (A^{-1})^\top (v \times w)\rangle \\ &= \langle u, (\operatorname{cof} A)(v \times w)\rangle,\end{aligned}$$

where the last equality follows from **??**. Hence we obtain the desired identity when A is invertible. Finally notice that both the maps $A \mapsto \operatorname{cof} A$ and $A \mapsto Av \times Aw$ are continuous. Hence the claim for general A follows from **??**.

?? : Notice that $A^{-1} = A^\top$, so this follows immediately from ?? .

This gives a geometric interpretation of the determinant. If $[u,v,w]$ is the signed volume of the parallelepiped spanned by u, v and w, and $[Au,Av,Aw]$ is the signed volume of the parallelepiped spanned by Au, Av and Aw, then $\det A$ is the factor by which this volume increasing when applying A to each of u, v and w. In particular, this explains why the determinant of A is zero if and only if A is singular: This means that A sends a basis of $\mathbb{R}^3$ to a linearly dependent set, and the parallelepiped spanned by such a set has zero volume.

(c) If A is a proper rotation, i.e. if A is orthogonal and $\det A = 1$, then **??** implies that $A(v \times w) = Av \times Aw$. This allows us to define a cross product on any three-dimensional inner product space, when this is equipped with an orientation.

First, if $\mathcal{V}$ and $\mathcal{W}$ are ordered bases for any finite-dimensional real vector space V, then we say that $\mathcal{V}$ and $\mathcal{W}$ have the ***same orientation*** if the change of basis operator $\varphi_{\mathcal{W},\mathcal{V}}$ has positive determinant. It follows that orientation partitions the set of ordered bases for V into two ***orientation classes***, each called an ***orientation*** of V. If V is equipped with an orientation $\mathcal{O}$, then we call this class the ***positive orientation*** of V, and the other class the ***negative orientation*** of V. An ordered basis for V is called ***positive*** if it lies in $\mathcal{O}$ and ***negative*** if it does not.

Returning to the case where V is three-dimensional and equipped with an orientation, let $\mathcal{V}$ and $\mathcal{W}$ be positive ordered orthonormal bases for V. For vectors $v, w \in V$ we can then consider the cross products of their coordinate vectors, i.e.

$$[v]_\mathcal{V} \times [w]_\mathcal{V} \quad \text{and} \quad [v]_\mathcal{W} \times [w]_\mathcal{W}.$$

Since ${}_\mathcal{W}[\square]_\mathcal{V}$ is orthogonal with determinant 1, we have

$${}_\mathcal{W}[\square]_\mathcal{V}([v]_\mathcal{V} \times [w]_\mathcal{V}) = {}_\mathcal{W}[\square]_\mathcal{V} \cdot [v]_\mathcal{V} \times {}_\mathcal{W}[\square]_\mathcal{V} \cdot [w]_\mathcal{V} = [v]_\mathcal{W} \times [w]_\mathcal{W}.$$

Hence we have

$$\varphi_\mathcal{V}^{-1}([v]_\mathcal{V} \times [w]_\mathcal{V}) = \varphi_\mathcal{W}^{-1}([v]_\mathcal{W} \times [w]_\mathcal{W}),$$

so we may define the cross product of v and w as $v \times w = \varphi_{\mathcal{V}}^{-1}([v]_{\mathcal{V}} \times [w]_{\mathcal{V}})$ where $\mathcal{V}$ is any positive ordered orthonormal basis for V. Notice that this means that $[v \times w]_{\mathcal{V}} = [v]_{\mathcal{V}} \times [w]_{\mathcal{V}}$.

This allows us to generalise most of the above results to abstract real vector spaces. For instance, using that the coordinate map $\varphi_{\mathcal{V}}$ is an isometry, the scalar triple product of $u, v, w \in V$ is given by

$$[u, v, w] = \langle u, v \times w \rangle = \langle [u]_{\mathcal{V}}, [v \times w]_{\mathcal{V}} \rangle = \langle [u]_{\mathcal{V}}, [v]_{\mathcal{V}} \times [w]_{\mathcal{V}} \rangle = \Big[[u]_{\mathcal{V}}, [v]_{\mathcal{V}}, [w]_{\mathcal{V}} \Big],$$

and hence it has all the properties of the scalar triple product on $\mathbb{R}^3$, such as invariance under cyclic permutations. Notice also that it is indeed a *scalar* quantity, in the sense that it is invariant under a change of basis. Similarly, the 'bac-cab rule' **??** becomes

$$\begin{aligned} [u \times (v \times w)]_{\mathcal{V}} &= [u]_{\mathcal{V}} \times [v \times w]_{\mathcal{V}} \\ &= [u]_{\mathcal{V}} \times ([v]_{\mathcal{V}} \times [w]_{\mathcal{V}}) \\ &= [v]_{\mathcal{V}} \langle [u]_{\mathcal{V}}, [w]_{\mathcal{V}} \rangle - [w]_{\mathcal{V}} \langle [u]_{\mathcal{V}}, [v]_{\mathcal{V}} \rangle \\ &= [v]_{\mathcal{V}} \langle u, w \rangle - [w]_{\mathcal{V}} \langle u, v \rangle \\ &= [v \langle u, w \rangle - w \langle u, v \rangle]_{\mathcal{V}}. \end{aligned}$$

Hence $u \times (v \times w) = v\langle u, w \rangle - w\langle u, v \rangle$ since $\varphi_{\mathcal{V}}$ is an isomorphism. In particular, the cross product on V also satisfies the Jacobi identity **??**, so V becomes a Lie algebra whose Lie bracket is given by the cross product, i.e. $[v, w] = v \times w$.

5 Eigenvalues and Eigenvectors

5.1 ⋄ Eigenvalues and spectra

(a) Let V be a vector space, and let $T \in \mathcal{L}(V)$. Recall that an ***eigenvalue*** of T is an element $\lambda \in \mathbb{F}$ such that there is a nonzero vector $v \in V$ with $Tv = \lambda v$. Then v is called an ***eigenvector*** of T associated with λ. The set of eigenvectors associated with an eigenvalue λ is called the ***eigenspace*** of λ and is denoted $E_T(\lambda)$. This is clearly a subspace of V, and its dimension is called the ***geometric multiplicity*** of λ and is denoted $\mathrm{Geo}_T(\lambda)$. The set of eigenvalues of T is called the ***spectrum*** of T and is denoted $\operatorname{Spec} T$. Clearly $\lambda \in \operatorname{Spec} T$ if and only if $\lambda I - T$ is not injective.

On finite-dimensional spaces being injective is the same as being invertible, but on infinite-dimensional vector spaces this is not the case, so the above definition of the spectrum is usually not sufficient. If V and W are Banach spaces over $\mathbb{K}$ and U is a subspace of V, then a (not necessarily bounded) linear map $T\colon U \to W$ is said to be ***boundedly invertible*** if there is a bounded operator $S\colon W \to V$ such that $TS = \mathrm{id}_W$ and $ST = \iota_U$. The ***resolvent set*** $\rho(T)$ of T is the set of $\lambda \in \mathbb{K}$ such that $\lambda I - T$ is boundedly invertible. The ***spectrum*** of T is then the set $\sigma(T) = \mathbb{K} \setminus \rho(T)$.

If T is in fact bounded and $U = V$, then another definition of the spectrum of T does not require that $\lambda I - T$ is not *boundedly* invertible, but that it is not invertible at all.[1] But the bounded inverse theorem (cf. e.g. **follandrealanalysis**) says that if T is a bounded and invertible linear map between Banach spaces, then its inverse is also bounded.

In this setting it is usual to collect the eigenvalues of T in a set $\sigma_{\mathrm{p}}(T)$ called the ***point spectrum*** of T. This thus agrees with the definition of $\operatorname{Spec} T$ above.

(b) Let V be a vector space, and let $T \in \mathcal{L}(V)$.

5.1 • Proposition. *If $\mathcal{V}$ be a collection of eigenvectors for T associated with distinct eigenvalues. Then $\mathcal{V}$ is linearly independent.*

Proof. Note that it suffices to show that any finite subset of $\mathcal{V}$ is linearly independent. Let $\mathcal{I} \subseteq \mathcal{V}$ be a finite subset with n elements. If $n = 1$, then since the sole element of $\mathcal{I}$ is an eigenvector, it is nonzero and hence $\mathcal{I}$ is linearly independent.

[1] This agrees with the definition of the spectrum of an element of a unital Banach algebra.

Assume now that $n > 1$ and that any $n-1$ element subset of $\mathcal{V}$ is linearly independent. Write $\mathcal{I} = \{v_1, \dots, v_n\}$ and consider a linear relation

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0. \tag{5.1}$$

Applying T to both sides yields

$$\alpha_1 \lambda_1 v_1 + \cdots + \alpha_n \lambda_n v_n = 0. \tag{5.2}$$

Multiplying **??** by λ_1 and subtracting it from **??** then gives

$$\alpha_2(\lambda_2 - \lambda_1)v_2 + \cdots + \alpha_n(\lambda_n - \lambda_1)v_n = 0.$$

But the set $\{v_2, \dots, v_n\}$ is linearly independent, so the coefficients above must all vanish. And since the eigenvalues are distinct, this implies that $\alpha_2 = \cdots \alpha_n = 0$. Hence $\alpha_1 v_1 = 0$, so also $\alpha_1 = 0$. ■

5.2 • **Corollary.** *The direct sum*

$$\bigoplus_{\lambda \in \operatorname{Spec} T} E_T(\lambda)$$

exists. ■

(c) We end this section with the following result on eigenvalues of matrix representations:

5.3 • **Lemma.** *Let V be a finite-dimensional vector space, let $T \in \mathcal{L}(V)$, and let $\mathcal{V}$ be an ordered basis for V. Then $v \in V$ is an eigenvector for T if and only if $[v]_{\mathcal{V}}$ is an eigenvector for ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ with the same eigenvalue.*

Proof. Let $\lambda \in \mathbb{F}$ be the eigenvalue of v. Then

$${}_{\mathcal{V}}[T]_{\mathcal{V}} \cdot [v]_{\mathcal{V}} = [Tv]_{\mathcal{V}} = [\lambda v]_{\mathcal{V}} = \lambda [v]_{\mathcal{V}}.$$

For the converse, a similar calculation shows that $[Tv]_{\mathcal{V}} = [\lambda v]_{\mathcal{V}}$. Since $\varphi_{\mathcal{V}}$ is an isomorphism, it follows that $Tv = \lambda v$ as desired. ■

5.2 ◇ The characteristic polynomial

(a) If V is finite-dimensional, then λ is an eigenvalue of T just when $\det(\lambda \operatorname{id}_V - T) = 0$. This motivates the definition of the ***characteristic polynomial*** $p_T(t) \in \mathbb{F}[t]$ of T, given by $p_T(t) = \det(t \operatorname{id}_V - T)$. The eigenvalues of T are then precisely the roots of $p_T(t)$.

It is also common to define the characteristic polynomial of T as the polynomial $\det(T - t \operatorname{id}_V)$ in t. Nothing substantial hangs on this choice, but our convention has the benefit that $p_T(t)$ becomes a monic polynomial, as the following result shows:

5.4 • **Proposition.** *Let $T \in \mathcal{L}(V)$.*

(i) *$p_T(t)$ is a monic polynomial of degree n.*

(ii) *The constant term of $p_T(t)$ equals $(-1)^n \det T$.*

(iii) *The coefficient of t^{n-1} in $p_T(t)$ equals $-\operatorname{tr} T$.*

Assume further that $p_T(t)$ splits over $\mathbb{F}$. Then:

(iv) *T has an eigenvalue.*

(v) $\det T$ *is the product of the eigenvalues of T.*

(vi) $\operatorname{tr} T$ *is the sum of the eigenvalues of T.*

The condition that $p_T(t)$ splits over $\mathbb{F}$ means that $p_T(t)$ decomposes into a product of linear factors on the form $t - a \in \mathbb{F}[t]$ (up to multiplication by a constant). This is in particular the case if $\mathbb{F}$ is algebraically closed.

Proof. *??* : Let $A = (a_{ij}) \in \mathrm{M}_n(\mathbb{F})$ be a matrix representation of T. The (i,j)-th entry of $tI - A$ is then $t\delta_{ij} - a_{ij}$, so

$$\det(t\,\mathrm{id}_V - T) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)(t\delta_{1\sigma(1)} - a_{1\sigma(1)}) \cdots (t\delta_{n\sigma(n)} - a_{n\sigma(n)}) \tag{5.3}$$

by **??**. Thus $p_T(t)$ is a polynomial in t. Furthermore, the only entries in $tI - A$ containing t are the diagonal entries, and the largest number of such entries occurring in a single term of **??** is n, so $\deg p_T(t) \leq n$. But notice that there is only one term in which t appears n times, namely the term corresponding to the identity permutation in S_n, giving the product of the diagonal entries in $tI - A$. This term equals

$$(t - a_{11})(t - a_{22}) \cdots (t - a_{nn}), \tag{5.4}$$

and multiplying out we see that the only resulting term containing t^n is t^n itself. Hence $p_T(t)$ is monic and of degree n. Thus we may write $p_T(t) = \sum_{i=0}^n c_i t^i$ for appropriate $c_0, \ldots, c_n \in \mathbb{F}$.

?? : Simply notice that

$$(-1)^n \det T = \det(-T) = p_T(0) = c_0$$

by n-linearity of det and the definition of $p_T(t)$.

?? : Consider a term in the sum **??**. The only way for this term to contain the factor t^{n-1} is for at least $n-1$ of the $t\delta_{i\sigma(i)} - a_{i\sigma(i)}$ to be a diagonal element. But in choosing $n-1$ elements along the diagonal we are forced to also choose the final diagonal element, since otherwise σ would not be a permutation.

Thus σ is forced to be the identity permutation, and in particular the only term in **??** that contains the factor t^{n-1} is the diagonal term **??**. Multiplying out the factors in this term, it is then clear that the coefficient of t^{n-1} is

$$c_{n-1} = -(a_{11} + \cdots + a_{nn}) = -\operatorname{tr} T$$

as claimed.

?? : Now assume that $p_T(t)$ splits over $\mathbb{F}$. Then some linear factor $t - \lambda \in \mathbb{F}[t]$ divides $p_T(t)$, which implies that $\lambda \in \mathbb{F}$ is an eigenvalue of T.

?? : Since $p_T(t)$ is monic we have

$$p_T(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_n)$$

for appropriate $\lambda_1, \dots, \lambda_n \in \mathbb{F}$. These are then the (not necessarily distinct) eigenvalues of T. Thus $p_T(0) = (-1)^n \lambda_1 \cdots \lambda_n$, and the claim follows from ?? .

?? : We similarly find that $c_{n-1} = -(\lambda_1 + \cdots + \lambda_n)$, so the final claim follows from ?? .

(b) Above we defined the geometric multiplicity of an eigenvalue. The characteristic polynomial gives rise to another kind of multiplicity: The ***algebraic multiplicity*** of λ is the multiplicity of λ as a root of the characteristic polynomial p_T. We denote this by $\operatorname{Alg}_T(\lambda)$.

5.5 • **Proposition.** *If λ is an eigenvalue of T, then* $\operatorname{Geo}_T(\lambda) \leq \operatorname{Alg}_T(\lambda)$.

Proof. Let $d = \operatorname{Geo}_T(\lambda)$. Choose any basis for the eigenspace $E_T(\lambda)$ and extend it to a basis $\mathcal{V}$ for V. The corresponding matrix representation of T then has the block form

$$_{\mathcal{V}}[T]_{\mathcal{V}} = \begin{pmatrix} \lambda I_d & A \\ 0 & B \end{pmatrix},$$

for appropriate matrices A and B. It follows from **??** that

$$\begin{aligned} p_T(t) &= \det(t \operatorname{id}_V - T) \\ &= \det(tI_d - \lambda I_d)\det(tI_{n-d} - B) \\ &= (t - \lambda)^d \det(tI_{n-d} - B). \end{aligned}$$

This proves the claim. ■

5.3 ⋄ Diagonalisability

(a) If V is finite-dimensional and $T \in \mathcal{L}(V)$, then we say that T is ***diagonalisable*** if there is a basis for V consisting of eigenvectors for T. That is, V has a basis $\mathcal{V} = (v_1, \ldots, v_n)$ such that $Tv_i = \lambda_i v_i$ for appropriate λ_i. It is then obvious that

5.6 • **Proposition.** *Let $T \in \mathcal{L}(V)$. The following are equivalent:*

(1) *T is diagonalisable.*

(2) *V has an ordered basis $\mathcal{V}$ such that ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ is diagonal.*

(3) *V has the form*

$$V = \bigoplus_{\lambda \in \operatorname{Spec} T} E_T(\lambda).$$

(4) *If* $\operatorname{Spec} T = \{\lambda_1, \ldots, \lambda_k\}$ *and P_i is projection onto $E_T(\lambda_i)$ along $\bigoplus_{j \neq i} E_T(\lambda_j)$, then* $\mathrm{id}_V = P_1 + \cdots + P_k$ *is a resolution of the identity.*

(5) *T is similar to a multiplication operator M_A, where $A \in \mathrm{M}_n(\mathbb{F})$ is a diagonal matrix whose diagonal contains the eigenvalues of T with multiplicity:*

$$T = \varphi_{\mathcal{V}}^{-1} \circ M_A \circ \varphi_{\mathcal{V}}.$$

Note that the last two properties are equivalent by **??**.

(b) There is a different way of characterising diagonalisability using resolutions of the identity. If $T \in \mathcal{L}(V)$, then a ***spectral resolution*** of T is a decomposition

$$T = \lambda_1 P_1 + \cdots + \lambda_k P_k,$$

where $\mathrm{id}_V = P_1 + \cdots + P_k$ is a resolution of the identity and $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$. Note that any resolution of the identity is itself a spectral resolution of id_V with all coefficients equal to 1. We then have the following result, which follows from **??** and **??**:

5.7 • **Proposition.** *A linear operator $T \in \mathcal{L}(V)$ is diagonalisable if and only if it has a spectral resolution*

$$T = \lambda_1 P_1 + \cdots + \lambda_k P_k.$$

In this case $\operatorname{Spec} T = \{\lambda_1, \ldots, \lambda_k\}$, *and*

$$\operatorname{im} P_i = E_T(\lambda_i), \quad \textit{and} \quad \ker P_i = \bigoplus_{j \neq i} E_T(\lambda_j).$$

5.4 ◇ Proofs without determinants

We now show how to obtain the results in **??** without using determinants. Since we do not have access to the characteristic polynomial, we must assume that V is a (finite-dimensional) vector space over an algebraically closed field $\mathbb{F}$. Consider $T \in \mathcal{L}(V)$.

(a) We begin by showing that T has an eigenvalue. For $d \in \mathbb{N}$, let $\mathbb{F}[t]_d$ denote the vector space of polynomials in $\mathbb{F}[t]$ with degree strictly less than d, such that $\dim \mathbb{F}[t]_d = d$. Consider the linear map $\mathrm{ev}_T \colon \mathbb{F}[t]_{n^2+1} \to \mathcal{L}(V)$ given by $\mathrm{ev}_T(p) = p(T)$. This cannot be injective, so there is some nonzero $p(t) \in \mathbb{F}[t]_{n^2+1}$ such that $p(T) = 0$. Note that $p(t)$ cannot be constant.

Since $\mathbb{F}$ is algebraically closed, there exist $c, \lambda_1, \dots, \lambda_m \in \mathbb{F}$ such that $p(t) = c\prod_{i=1}^m (t - \lambda_i)$. But then

$$0 = p(T) = c\prod_{i=1}^{m}(T - \lambda_i I),$$

so at least one $T - \lambda_i I$ is not injective. Hence λ_i is an eigenvalue of T.

(b) And for the remaining of the promised results:

5.8 • **Corollary.** *Let $\mathbb{F}$ be algebraically closed, and let $T \in \mathcal{L}(V)$. Then the sum of the eigenvalues of T is $\operatorname{tr} T$, and the product of the eigenvalues of T is $\det T$.*

Proof. Let $A \in \mathrm{M}_n(\mathbb{F})$ be an upper triangular matrix for T. As we will see in **??**, such a matrix always exists. The diagonal elements of A are then the eigenvalues, and the trace of T is of course the sum of these elements.

For the second claim, simply notice that if A is upper triangular then the Leibniz formula for $\det A$ only contains a single term, namely the one corresponding to the identity permutation. ∎

6 Complexification

(a) If W is a complex vector space, then we may restrict the scalar multiplication $\mathbb{C} \times W \to W$ to a map $\mathbb{R} \times W \to W$. When we equip W with this restricted scalar multiplication instead of the original one, we call the resulting space the ***real version*** of W and denote it by $W_{\mathbb{R}}$.

Conversely, if V is a real vector space then we define the ***complexification*** of V as the vector space $V^{\mathbb{C}}$ whose underlying set is $V \times V$, and which is equipped with componentwise addition and the complex scalar multiplication

$$(\alpha + \mathrm{i}\beta)(v,u) = (\alpha v - \beta u, \alpha u + \beta v),$$

for $\alpha, \beta \in \mathbb{R}$ and $v, u \in V$. Notice that the map $v \mapsto (v, 0)$ is injective (and real linear), that $(v,0)+(w,0) = (v+w,0)$, and that $\alpha(v,0) = (\alpha v, 0)$ for $\alpha \in \mathbb{R}$, so $V^{\mathbb{C}}$ contains an isomorphic copy of V, and we may identify elements $v \in V$ with elements $(v,0) \in V^{\mathbb{C}}$. Furthermore, notice that $(v,u) = (v,0) + \mathrm{i}(u,0)$, so by the above identification we may write $(v,u) = v + \mathrm{i}u$.

(b) We briefly study the relationship between a real vector space and its complexification.

6.1 • Proposition. *If $\mathcal{B}$ is a basis for V, then $\mathcal{B}^{\mathbb{C}} = \{b + \mathrm{i}0 \mid b \in \mathcal{B}\}$ is a basis for $V^{\mathbb{C}}$. In particular,* $\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V^{\mathbb{C}}$.

Proof. Let $v + \mathrm{i}u \in V^{\mathbb{C}}$. Then there are real numbers α_b and β_b (finitely many nonzero) such that $v = \sum_{b\in\mathcal{B}} \alpha_b b$ and $u = \sum_{b\in\mathcal{B}} \beta_b b$. But then

$$v + \mathrm{i}u = \sum_{b\in\mathcal{B}} \alpha_b b + \mathrm{i}\sum_{b\in\mathcal{B}} \beta_b b = \sum_{b\in\mathcal{B}} (\alpha_b + \mathrm{i}\beta_b) b = \sum_{b\in\mathcal{B}} (\alpha_b + \mathrm{i}\beta_b)(b + \mathrm{i}0),$$

so $\mathcal{B}^{\mathbb{C}}$ spans $V^{\mathbb{C}}$. Furthermore, if $v + \mathrm{i}u = 0$, then the previous computation shows that $\sum_{b\in\mathcal{B}} \alpha_b b = 0 = \sum_{b\in\mathcal{B}} \beta_b b$. Linear independence of $\mathcal{B}$ then implies that $\alpha_b = \beta_b = 0$ for all $b \in \mathcal{B}$. ∎

6.2 • Example. Notice that $(\mathbb{R}^n)^{\mathbb{C}} \cong \mathbb{C}^n$. The above proposition then implies that the standard basis for $\mathbb{R}^n$ gives rise to a basis for $\mathbb{C}^n$, and we notice that this is precisely the standard basis. ⌟

(c) We now show how to extend linear maps defined between real vector spaces to the complexifications of those spaces. If $T\colon V \to W$ is a linear map between real vector spaces, then we define the complexification of T by

$$\begin{aligned} T^{\mathbb{C}}\colon V^{\mathbb{C}} &\to W^{\mathbb{C}}, \\ v + \mathrm{i}u &\mapsto Tv + \mathrm{i}Tu. \end{aligned}$$

That is, $T^{\mathbb{C}}$ is just the product map $T \times T$. This is easily seen to be complex-linear.

6.3 • Proposition. *Let V be a real vector space, and let $T \in \mathcal{L}(V)$. If $\lambda \in \mathbb{R}$ is an eigenvalue of the complexification $T^{\mathbb{C}}$ of T, then λ is also an eigenvalue of T. Furthermore, if $v + \mathrm{i}u \in E_{T^{\mathbb{C}}}(\lambda)$ then $v, u \in E_T(\lambda)$.*

Note that this does not mean that v and u are eigenvectors of T since they might be zero. But if $v + \mathrm{i}u$ is an eigenvector of $T^{\mathbb{C}}$, then at least one of v and u is nonzero and hence an eigenvector of T.

Proof. Let $v + \mathrm{i}u \in V^{\mathbb{C}}$ be an eigenvector of $T^{\mathbb{C}}$ corresponding to λ. Then

$$Tv + \mathrm{i}Tu = T^{\mathbb{C}}(v + \mathrm{i}u) = \lambda(v + \mathrm{i}u) = \lambda v + \mathrm{i}\lambda u.$$

It follows that $Tv = \lambda v$ and $Tu = \lambda u$ as desired. ■

If V is finite-dimensional and $\mathcal{V}$ is an ordered basis for V, then $\mathcal{V}^{\mathbb{C}}$ carries the obvious ordering. Since V and $V^{\mathbb{C}}$ have the same dimension, the following result is not surprising:

6.4 • Proposition. *Let V and W be a finite-dimensional real vector spaces, and consider $T\colon V \to W$. If $\mathcal{V} = (v_1, \dots, v_n)$ and $\mathcal{W}$ are ordered bases of V and W respectively, then*

$${}_{\mathcal{W}^{\mathbb{C}}}[T^{\mathbb{C}}]_{\mathcal{V}^{\mathbb{C}}} = {}_{\mathcal{W}}[T]_{\mathcal{V}}.$$

Proof. By **??**, the ith column of ${}_{\mathcal{W}^{\mathbb{C}}}[T^{\mathbb{C}}]_{\mathcal{V}^{\mathbb{C}}}$ is given by

$$[T^{\mathbb{C}}(v_i + \mathrm{i}0)]_{\mathcal{W}^{\mathbb{C}}} = [Tv_i + \mathrm{i}0]_{\mathcal{W}^{\mathbb{C}}} = [Tv_i]_{\mathcal{W}},$$

that is, the ith column of ${}_{\mathcal{W}}[T]_{\mathcal{V}}$, which proves the claim. ■

(d) Finally, if V is a real normed space, then we define a norm on $V^{\mathbb{C}}$ by the equation

$$\|v + \mathrm{i}u\|^2 = \|v\|^2 + \|u\|^2. \tag{6.1}$$

Furthermore, if V is an inner product space, then we define an inner product on $V^{\mathbb{C}}$ by

$$\langle v + \mathrm{i}u, x + \mathrm{i}y \rangle = \langle v, x \rangle + \langle u, y \rangle + \mathrm{i}(\langle v, y \rangle - \langle u, x \rangle). \tag{6.2}$$

The norm induced by this inner product agrees with the norm defined by **??**. Notice that the identity **??** holds in any *complex* inner product space, where the notation $v + \mathrm{i}u$ instead means the sum of v and the scalar product of i and u (recalling that our sesquilinear forms are linear in the *second* entry).

7 Triangularisation

Recall that a matrix $A = (a_{ij}) \in \mathrm{M}_n(R)$ is called *upper triangular* if $a_{ij} = 0$ whenever $i > j$. If V is an n-dimensional $\mathbb{F}$-vector space and $\mathcal{V}$ is an ordered basis for V, then we say that the operator $T \in \mathcal{L}(V)$ is *upper triangular with respect to* $\mathcal{V}$ if the matrix representation ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ is upper triangular.

A subspace U of a vector space V is said to be *invariant under* $T \in \mathcal{L}(T)$ if $T(U) \subseteq U$.

7.1 • Proposition. *Let V be an $\mathbb{F}$-vector space with $n = \dim V < \infty$, and let $\mathcal{V} = (v_1, \dots, v_n)$ be an ordered basis for V. An operator $T \in \mathcal{L}(V)$ is upper triangular with respect to $\mathcal{V}$ if and only if* $\operatorname{span}(v_1, \dots, v_i)$ *is invariant under T for all $i \in \{1, \dots, n\}$.*

Proof. This is obvious. ■

7.2 • Lemma. *Let V be an $\mathbb{F}$-vector space, and let $T \in \mathcal{L}(V)$ be an isomorphism. If U is a finite-dimensional subspace of V that is invariant under T, then U is also invariant under T^{-1}.*

Proof. Since U is finite-dimensional and $T|_U : U \to U$ is injective, applying the rank–nullity theorem implies that $T|_U$ is also surjective. Hence if $u \in U$, then there exists a $v \in U$ such that $Tv = u$. It follows that

$$T^{-1}u = T^{-1}Tv = v \in U,$$

so U is invariant under T^{-1}. ■

7.3 • Proposition. *Let V be a finite-dimensional $\mathbb{F}$-vector space, and let $\mathcal{V}$ be an ordered basis for V. If $T \in \mathcal{L}(V)$ is an isomorphism that is upper triangular with respect to $\mathcal{V}$, then T^{-1} is also upper triangular with respect to $\mathcal{V}$.*

In particular, the subset of $\mathrm{GL}_n(\mathbb{F})$ *consisting of upper triangular matrices is a subgroup.*

Proof. This is an obvious consequence of the above two results. ■

7.4 • Lemma. *Let $A \in \mathrm{M}_n(\mathbb{F})$ be upper triangular. Then A is invertible if and only if all its diagonal elements are nonzero.*

Proof. Denote the diagonal elements of A by $\lambda_1,\dots,\lambda_n$, and let $(e_1,\dots,e_n)$ be the standard basis of $\mathbb{F}^n$. First assume that the diagonal elements are nonzero. Then notice that $e_1 \in R(A)$, and that

$$Ae_i = a_1e_1 + \cdots + a_{i-1}e_{i-1} + \lambda_i e_i$$

for appropriate $a_1,\dots,a_{i-1} \in \mathbb{F}$. By induction we then have $e_i \in R(A)$. Since $(e_1,\dots,e_n)$ is a basis, this implies that $R(A) = \mathbb{F}^n$.

Conversely, assume that some diagonal element λ_i is zero. Then

$$A\operatorname{span}(e_1,\dots,e_i) \subseteq \operatorname{span}(e_1,\dots,e_{i-1}),$$

so the null-space of A is nontrivial, and hence A is singular. ■

7.5 • **Lemma.** *Let $A \in \mathrm{M}_n(\mathbb{F})$ be upper triangular. Then the eigenvalues of A are its diagonal elements.*

Proof. Let $\lambda \in \mathbb{F}$, and denote the diagonal elements of A by $\lambda_1,\dots,\lambda_n$. By **??**, the matrix $\lambda I - A$ is singular if and only if $\lambda - \lambda_i = 0$ for some i, and hence $\lambda_1,\dots,\lambda_n$ are the eigenvalues of A. ■

7.6 • **Proposition.** *Let $\mathbb{F}$ be algebraically closed, and let V be a finite-dimensional $\mathbb{F}$-vector space. If $T \in \mathcal{L}(V)$, then V has an ordered basis with respect to which T is upper triangular.*

Proof. This is obvious if $\dim V = 1$, so assume that $n = \dim V > 1$, and assume that the claim is true for $\mathbb{F}$-vector spaces of dimension $n-1$. Since $\mathbb{F}$ is algebraically closed, T has an eigenvector $v_1 \in V$. Then $U = \operatorname{span}(v_1)$ is invariant under T, so we may define a linear operator[1] $\tilde{T} \in \mathcal{L}(V/U)$ by $\tilde{T}(v+U) = Tv+U$. Since $\dim V/U = n-1$, by induction there is a basis $v_2+U,\dots,v_n+U$ of V/U with respect to which the matrix of $\tilde{T}$ is upper triangular. It is easy to show that the collection $v_1,\dots,v_n$ is linearly independent, hence a basis for V.

Now notice that

$$Tv_i + U = \tilde{T}(v_i + U) \in \operatorname{span}(v_2 + U,\dots,v_i + U)$$

for $i \in \{2,\dots,n\}$. That is, there exist $a_2,\dots,a_i \in \mathbb{F}$ such that

$$Tv_i + U = (a_2v_2 + \cdots + a_iv_i) + U.$$

But then $Tv_i \in \operatorname{span}(v_1,\dots,v_i)$ for all $i \in \{2,\dots,n\}$, and since U is invariant under T this also holds for $i = 1$. Hence T is upper triangular with respect to the basis $v_1,\dots,v_n$ of V. ■

[1] The operator $\tilde{T}$ may arise as follows: Let $\pi\colon V \to V/U$ be the quotient map. Then $U \subseteq \ker(\pi \circ T)$ since U is invariant under T, so $\pi \circ T$ descends to a linear map $\tilde{T}\colon V/U \to V/U$.

7.7 • Theorem: ***Schur's Theorem.***
Let V be a finite-dimensional complex inner product space. If $T \in \mathcal{L}(V)$, then V has an ordered orthonormal basis with respect to which T is upper triangular.

Proof. By **??** V has an ordered basis $\mathcal{V} = (v_1, \ldots, v_n)$ with respect to which ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ is upper triangular. Now apply the Gram–Schmidt procedure to $\mathcal{V}$ and obtain an orthonormal basis $\mathcal{U} = (u_1, \ldots, u_n)$ for V such that

$$\operatorname{span}(u_1, \ldots, u_i) = \operatorname{span}(v_1, \ldots, v_i)$$

for all $i \in \{1, \ldots, n\}$. Then **??** shows that ${}_{\mathcal{U}}[T]_{\mathcal{U}}$ is also upper triangular, proving the claim. ■

8 Sesquilinear Forms

8.1 ⋄ Definitions

(a) If V is a complex vector space, recall that a map $\varphi\colon V \times V \to \mathbb{C}$ is called ***sesquilinear*** if it is linear in one entry and conjugate-linear in the other. Opinions differ as to in which entry φ should be linear, but our sesquilinear forms will be linear in the *second* entry. Similarly, if V is a vector space over an arbitrary field $\mathbb{F}$, recall that $\varphi\colon V \times V \to \mathbb{F}$ is ***bilinear*** if it is linear in each entry (i.e., if it is 2-linear in the terminology of **??**).

In order to collect these two properties under one concept, we first note explicitly the difference between linearity

$$T(\alpha u + v) = \alpha Tu + Tv$$

of a map $T\colon V \to W$ between $\mathbb{F}$-vector spaces, and conjugate linearity

$$T(\alpha u + v) = \overline{\alpha} Tu + Tv$$

in the case where $\mathbb{F} = \mathbb{C}$. We notice that both of the right-hand side expressions are on the form

$$T(\alpha u + v) = \sigma(\alpha) Tu + Tv,$$

where in the first case σ is just the identity function on $\mathbb{F}$, and in the latter case it is complex conjugation. Both of these maps are field automorphisms, and in fact they are involutions, in the sense that $\sigma^2 = \mathrm{id}$. We denote the automorphisms on $\mathbb{F}$ by $\mathrm{Aut}(\mathbb{F})$.

If $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $T\colon V \to W$ is a map between $\mathbb{F}$-vector spaces, then we will say that T is ***σ-linear*** if

$$T(\alpha u + v) = \sigma(\alpha) Tu + Tv$$

for all $u, v \in V$ and $\alpha \in \mathbb{F}$. We note that if T is σ-linear and bijective, then its inverse is σ^{-1}-linear: For if $w, z \in W$ with $w = Tu$ and $z = Tv$, then

$$\alpha w + z = \alpha Tu + Tv = T(\sigma^{-1}(\alpha) u + v),$$

and applying T^{-1} to both sides we find that $T^{-1}(\alpha w + z) = \sigma^{-1}(\alpha) Tw + Tz$. If T is σ-linear and bijective, we will call T a ***σ-isomorphism***, though this is really most useful when σ is an involution, since then T^{-1} is then also a σ-isomorphism and not just a σ^{-1}-isomorphism. Furthermore, if $S\colon V \to W$ is also σ-linear, then it is easy to see that $T + S$ is σ-linear, and that αT is σ-linear for all $\alpha \in \mathbb{F}$. Hence the set of σ-linear maps $V \to W$ is a vector space. Finally, if $R\colon W \to U$ is ρ-linear for an automorphism ρ, then $R \circ T$ is $\rho \circ \sigma$-linear.

(b) We wish to study forms whose first entry respect such an automorphism σ. However, it is not ideal to consider the automorphism σ as part of the underlying structure on which we define the form, say as a pair (V, σ). Notice for instance that if we did so, then we could not define a sesquilinear and a bilinear form on the same complex vector space V, since in the former case σ is complex conjugation and in the latter it is the identity. But notice also that since we wish to consider sesquilinear forms in general, and not just sesquilinear forms that respect a particular automorphism, we also do not wish to consider σ as part of the form itself. Hence we arrive at the following definition:

8.1 • Definition: ***Sesquilinear form.***
Let V be an $\mathbb{F}$-vector space. A map $\varphi\colon V \times V \to \mathbb{F}$ is called a *sesquilinear form* on V if there exists a $\sigma \in \operatorname{Aut}(\mathbb{F})$ such that $\varphi(\cdot, v)$ is σ-linear and $\varphi(v, \cdot)$ is linear for all $v \in V$. If σ is such an automorphism, then we also call φ a *σ-sesquilinear form.* ▲

The usual notion of sesquilinear forms on complex vector spaces is recovered if σ is complex conjugation. Notice also that a bilinear form is just a id_V-sesquilinear form. We should also note that there is a generalisation of this concept to modules over a division ring, but we shall not need this.

(c) We next describe the different kinds of sesquilinear forms that are of interest to us.

TODO sigma epsilon hermitian without being sigma sesquilinear????

8.2 • Definition. The sesquilinear form φ on V is said to be

(i) *nontrivial* if $\varphi(u, v) \neq 0$ for some $u, v \in V$.

(ii) *reflexive* if $\varphi(u, v) = 0$ implies $\varphi(v, u) = 0$ for all $u, v \in V$.

(iii) *(σ, ε)-Hermitian* if there is a $\sigma \in \operatorname{Aut}(\mathbb{F})$ and an $\varepsilon \in \mathbb{F}$ such that φ is σ-sesquilinear, and such that $\varphi(u, v) = \varepsilon\sigma(\varphi(v, u))$ for all $u, v \in V$. Furthermore, φ is called

σ-Hermitian	if it is	$(\sigma, 1)$-
σ-anti-Hermitian		$(\sigma, -1)$-
symmetric		$(\mathrm{id}_{\mathbb{F}}, 1)$-
skew-symmetric		$(\mathrm{id}_{\mathbb{F}}, -1)$-

Hermitian. If φ is (σ, ε)-Hermitian for some σ and ε, then it is simply called *Hermitian*.

(iv) *alternating* if $\varphi(v, v) = 0$ for all $v \in V$.

More concretely, φ is symmetric if $\varphi(u,v) = \varphi(v,u)$ for all $u,v \in V$, and skew-symmetric if $\varphi(u,v) = -\varphi(v,u)$ for all $u,v \in V$. Usually the element ε above will be nonzero; indeed it is most often ± 1. Furthermore, as mentioned in **??** the case where σ is an involution is particularly nice, since then a bijective map T is a σ-isomorphism just when its inverse T^{-1} is a σ-isomorphism. On the other hand, Hermitian forms are also of great interest, not least because they generalise the many important cases mentioned above. But it also turns out that there is a connection between Hermitian forms and involutions:

8.3 • Lemma. *If φ is a nontrivial (σ,ε)-Hermitian form, then σ is an involution.*

Proof. There exist $u,v \in V$ such that $\varphi(u,v) \neq 0$. If $\alpha \in \mathbb{F}$, then

$$\begin{aligned} \alpha\varphi(u,v) &= \varphi(\sigma(\alpha)u,v) \\ &= \varepsilon\sigma\big(\varphi(v,\sigma(\alpha)u)\big) \\ &= \varepsilon\sigma^2(\alpha)\sigma\big(\varphi(v,u)\big) \\ &= \sigma^2(\alpha)\varphi(u,v). \end{aligned}$$

Dividing through by $\varphi(u,v)$ yields $\sigma^2(\alpha) = \alpha$, so σ is an involution. ■

Now note the following relationships between the properties in **??**:

8.4 • Lemma. (i) *If* $\operatorname{char}\mathbb{F} = 2$, *then*

$$\textit{alternating} \Rightarrow \textit{symmetric} \Leftrightarrow \textit{skew-symmetric.}$$

(ii) *If* $\operatorname{char}\mathbb{F} \neq 2$, *then*

$$\textit{alternating} \Leftrightarrow \textit{skew-symmetric.}$$

(iii) *For all* $\sigma \in \operatorname{Aut}(\mathbb{F})$ *and* $\varepsilon \in \mathbb{F}$,

$$(\sigma,\varepsilon)\textit{-Hermitian} \Rightarrow \textit{reflexive.}$$

It turns out that every reflexive σ-sesquilinear form is also (σ,ε)-Hermitian for some $\varepsilon \in \mathbb{F}$, so the implication in ?? is actually an equivalence. [TODO reference to proof]

Proof. Note that if φ is alternating then it is skew-symmetric: For

$$0 = \varphi(u+v,u+v) = \varphi(u,v) + \varphi(v,u),$$

implying that φ is skew-symmetric. If $\operatorname{char}\mathbb{F} = 2$ then $1 = -1$, and so symmetry and skew-symmetry are clearly equivalent. If instead $\operatorname{char}\mathbb{F} \neq 2$ and φ

is skew-symmetric, then $\varphi(v,v) = -\varphi(v,v)$, so $2\varphi(v,v) = 0$ which implies that $\varphi(v,v) = 0$.

For the final claim, assume that φ is (σ,ε)-Hermitian, and let $u,v \in V$ satisfy $\varphi(u,v) = 0$. It follows that

$$\varphi(v,u) = \varepsilon\sigma(\varphi(u,v)) = \varepsilon\sigma(0) = 0,$$

since σ is a field homomorphism. ■

In particular, a skew-symmetric form is either symmetric or alternating, and we thus do not need to explicitly study skew-symmetric forms.

(d) If φ is a sesquilinear form on V, then the ***associated quadratic form*** is the map $Q\colon V \to \mathbb{F}$ given by $Q(v) = \varphi(v,v)$. If φ is σ-sesquilinear, then it follows that $Q(\alpha v) = \alpha\sigma(\alpha)Q(v)$. In particular, if φ is bilinear then $Q(\alpha v) = \alpha^2 Q(v)$.

It is well-known that the real and complex inner products can be recovered from their quadratic forms, and we will return to these in TODO ref. For now we assume that φ is bilinear and that $\operatorname{char}\mathbb{F} \neq 2$, and we let

$$\varphi_s(u,v) = \tfrac{1}{2}\bigl(\varphi(u,v) + \varphi(v,u)\bigr) \quad\text{and}\quad \varphi_a(u,v) = \tfrac{1}{2}\bigl(\varphi(u,v) - \varphi(v,u)\bigr),$$

so that $\varphi = \varphi_s + \varphi_a$. Then both φ_s and φ_a are bilinear, φ_s is symmetric and φ_a anti-symmetric [TODO decide between anti and skew], hence alternating. If Q_s is the quadratic form associated with φ_s, then

$$Q(v) = \varphi(v,v) = \varphi_s(v,v) + \varphi_a(v,v) = \varphi_s(v,v) = Q_s(v)$$

for all $v \in V$. That is, the quadratic form associated with a bilinear form can only determine its 'symmetric part'. Indeed, we could replace φ_a with any anti-symmetric bilinear form and we would still have $Q = Q_s$. Hence we cannot hope to find a polarisation identity for arbitrary bilinear forms, a fortiori for sesquilinear forms. But if φ is already symmetric, then we have the following:

8.5 • PROPOSITION. *Assume that φ is bilinear and symmetric, and that* $\operatorname{char}\mathbb{F} \neq 2$. *Then*

$$\varphi(u,v) = \tfrac{1}{2}\bigl(Q(u+v) - Q(u) - Q(v)\bigr) = \tfrac{1}{4}\bigl(Q(u+v) - Q(u-v)\bigr)$$

for all $u,v \in V$. ■

The proof is simply a case of inserting the definition of Q.

The real case is thus taken care of. There is of course also a polarisation identity for inner products on complex vector spaces, but since this is not bilinear it takes a slightly different form. We will return to this in TODO ref.

(e) We make the following conventions:

> **ASSUMPTION.** For the remainder of this chapter, let V be an $\mathbb{F}$-vector space V equipped with a sesquilinear form denoted $\langle \cdot, \cdot \rangle$. Assume that $\langle \cdot, \cdot \rangle$ is σ-sesquilinear for some $\sigma \in \mathrm{Aut}(\mathbb{F})$. We denote the associated quadratic form by Q. We also write $\langle \cdot, \cdot \rangle_V$ for the form on V and Q_V for the associated quadratic form for clarity, to distinguish this from forms on other vector spaces.
>
> If V is a topological vector space, we further assume that the form on V is continuous in each entry separately. ❈

8.2 ⋄ Properties of sesquilinear forms

(a) We begin with a concept familiar from the theory of inner product spaces:

8.6 • DEFINITION: *Orthogonality.*
Let $M, N \subseteq V$ be subsets. If $\langle u, v \rangle = 0$ for all $u \in M$ and $v \in N$, then we say that M is *orthogonal* to N, written $M \perp N$. The *orthogonal complement* of M is the set $M^{\perp} = \{v \in V \mid v \perp M\}$. ▲

If either M or N (or both) is a singleton, then we write e.g. $u \perp N$ for $\{u\} \perp N$, and we say that u is orthogonal to N. Note that if $M \subseteq N$, then $N^{\perp} \subseteq M^{\perp}$.

We usually only study orthogonality in the context of reflexive forms, since these are precisely the forms for which the orthogonality relation is symmetric. Hence:

> **ASSUMPTION.** For the remainder of this section, the form on V is reflexive. ❈

8.7 • LEMMA. *If $M \subseteq V$, then $M^{\perp}$ is a subspace of V.*

Proof. If $u, v \in M^{\perp}$ and $\alpha \in \mathbb{F}$, then for all $w \in M$ we have

$$\langle w, \alpha u + v \rangle = \alpha \langle w, u \rangle + \langle w, v \rangle = 0,$$

so $\alpha u + v \in M^{\perp}$. ∎

(b) In an inner product space, only the zero vector is orthogonal to itself. However, in the context of general sesquilinear forms this is not so, and it is in fact possible for a nonzero vector to be orthogonal to *every* vector in the space.

First of all, a vector $v \in V$ is ***isotropic*** if $v \perp v$, and ***nonisotropic*** otherwise. If V contains at least one isotropic vector, then V itself is called isotropic, and otherwise nonisotropic. In case every vector in V is isotropic, then V is said to be ***totally isotropic***.

On the other hand, v is ***degenerate*** if $v \perp V$. The set of all degenerate vectors in V is called the ***radical*** of V and is denoted $\sqrt{V}$. (Note that $\sqrt{V}$ is simply the orthogonal complement $V^{\perp}$, so in particular it is a subspace of V.) If $\sqrt{V} = 0$ then V is called ***nonsingular/nondegenerate***, if $\sqrt{V} \neq 0$ it is ***singular/degenerate***, and if $\sqrt{V} = V$ it is ***totally singular/degenerate***.

That is, a degenerate vector is isotropic, so a nonisotropic space is nonsingular. On pseudo inner product spaces, the converse is also the case due to the Cauchy–Schwarz inequality, but this is not so for general sesquilinear forms. Notice that a subspace of a nonisotropic space is also nonisotropic, while a subspace of a nondegenerate space might still be degenerate. Notice also that the form on V is alternating if and only if V is totally isotropic.

Note that if U is a subspace of V, then the notation $U^{\perp}$ is ambiguous. It might refer to the subset of U of vectors orthogonal to U, or the subset of V of vectors orthogonal to U. However, the notation $\sqrt{U}$ always refers to the former. In either interpretation of $U^{\perp}$, note that $\sqrt{U} = U \cap U^{\perp}$.

To better understand the significance of singularity, we note the following result:

8.8 • Lemma. *Assume that V is nonsingular and let $u, v \in V$. If $\langle u, w\rangle = \langle v, w\rangle$ for all $w \in V$, then $u = v$.*

In particular, if X is a set and the functions $f, g\colon X \to V$ satisfy $\langle f(x), w\rangle = \langle g(x), w\rangle$ for all $x \in X$ and $w \in V$, then $f = g$.

Proof. If the assumption holds, then $\langle u - v, w\rangle$ for all $w \in V$, i.e., $u - v$ is degenerate. But then we must have $u - v = 0$ since V is nonsingular. ■

(c) Every subspace of a vector space has a complement. However, in the present context we can wish for something more:

8.9 • Definition: *Orthogonal direct sum.*
The space V is the *orthogonal direct sum* of the subspaces U and W, written

$$V = U \odot W,$$

if $V = U \oplus W$ and $U \perp W$. ▲

We recall that we have assumed that the form on V is reflexive, so $U \odot W = W \odot U$.

8.10 • Proposition. *If U is a complement of $\sqrt{V}$, then U is nonsingular and $V = \sqrt{V} \odot U$.*

Proof. Clearly $\sqrt{V} \perp U$. Now notice that if $v \in \sqrt{U}$, then $v \perp U$, and we obviously also have $v \perp \sqrt{V}$. Hence $v \perp \sqrt{V} \oplus U = V$, so $\sqrt{U} \subseteq \sqrt{V}$. And since also $\sqrt{U} \subseteq U$, we must have $\sqrt{U} = 0$, so U is nonsingular. ■

This result shows that we can find a subspace of V that is nonsingular, and every element of V almost lies in U: we just have to add a degenerate vector to it. And if degenerate vectors are somehow insignificant, then a restriction to nonsingular spaces is not very severe. And of course, we can always obtain a complement U of $\sqrt{V}$ as the quotient $V/\sqrt{V}$ by **??**.

If $V = U \odot W$, then we regrettably cannot call U an 'orthogonal complement' of W, since we have already used this term for the set $U^\perp$, as is standard, and while U and $U^\perp$ are certainly orthogonal, it is not generally the case that $V = U \oplus U^\perp$.

(d) If $u \in V$, define a map[1] $\varphi_u \colon V \to \mathbb{F}$ by $\varphi_u(v) = \langle u, v \rangle$. If V is a topological vector space, recall that V^* denotes its topological dual, and that $\langle \cdot, \cdot \rangle$ is assumed to be continuous in each entry, so φ_u is continuous. Hence this gives rise to the σ-linear ***Riesz map*** $\Phi_V \colon V \to V^*$ given by $\Phi_V(u) = \varphi_u$. If a functional $\varphi \in V^*$ is on the form φ_u for some $u \in V$, then u is called a ***Riesz vector*** for φ. If Φ_V is bijective, then the unique Riesz vector for φ is denoted r_φ, and the map $\varphi \mapsto r_\varphi$ is of course the inverse of Φ_V, so it is σ^{-1}-linear. Hence $r_{\varphi_u} = u$ and $\varphi_{r_\psi} = \psi$ for $u \in V$ and $\psi \in V^*$.

It is sometimes the case that if there is a $\sigma \in \mathrm{Aut}(\mathbb{F})$ such that Φ_V is a σ-isomorphism, then V is in fact reflexive. This is for instance the case for Hilbert spaces. We cannot pursue the theory of duality for general topological spaces here in any detail.

(e) We now make the further assumption that V is finite-dimensional. In this case we have the following fundamental theorem:

8.11 • THEOREM: *The Riesz representation theorem.*
The Riesz map Φ_V is injective if and only if V is nonsingular. In particular, if V is finite-dimensional and nonsingular, then Φ_V is a σ-isomorphism.

Proof. Notice that $\varphi_u(v) = 0$ for all $v \in V$ just when $u \perp V$, i.e. when u is degenerate. This is the case if and only if $u \in \sqrt{V}$, so $\ker \Phi_V = \sqrt{V}$. ∎

While the Riesz representation theorem only applies to nonsingular spaces, there is also a version for singular subspaces of nonsingular spaces which is sometimes useful. If U is a subspace of V, define a map $\Psi_U^V \colon V \to U^*$ by $\Psi_U^V(v) = \varphi_v|_U$. Note that $\Psi_U^V = \iota_U^\dagger \circ \Phi_V$, so Ψ_U^V is σ-linear. We then have the following:

8.12 • COROLLARY. *Let V be finite-dimensional, and let U be a subspace of V. Then $\ker \Psi_U^V = U^\perp$, and if either V or U is nonsingular, then Ψ_U^V is surjective.*

[1] We begin to see why it is useful that sesquilinear forms are linear in the *second* entry. In this way, the vectors u and v appear in the same order in the expressions $\varphi_u(v)$ and $\langle u, v \rangle$. Notice that this is simply a consequence of the fact that functions are written to the left of their arguments.

Proof. Notice that $\varphi_v|_U$ is zero just when $\langle v,u\rangle = 0$ for all $u \in U$. But this says that $v \perp U$, i.e. $v \in U^\perp$. Hence $\ker \Psi_U^V = U^\perp$ as claimed.

Next assume that V is nonsingular. Let $\varphi \in U^*$ and extend this by 0 to a linear functional $\overline{\varphi}$ on V. **??** then furnishes a vector $v \in V$ such that $\overline{\varphi} = \varphi_v$. But then $\varphi = \varphi_v|_U$ as desired. If instead U is nonsingular, then we can simply apply **??** to U directly. ■

As an example of an application of this corollary, we have the following result, which itself has an important corollary:

8.13 • **Proposition.** *Let V be finite-dimensional, and let U be a subspace of V. If either V or U is nonsingular, then*

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

Hence the following are equivalent:

(i) $V = U + U^\perp$.

(ii) $V = U \odot U^\perp$.

(iii) *U is nonsingular, i.e., $U \cap U^\perp = \{0\}$.*

Proof. By **??**, the map Ψ_U^V is surjective onto U with kernel $U^\perp$. Hence **??** implies that

$$\dim V = \dim U^* + \dim U^\perp.$$

But since U is finite-dimensional, it follows that $\dim U = \dim U^*$ by **??**, so the claim follows. ■

8.14 • **Corollary.** *Let V be finite-dimensional and nonisotropic. Then V has an orthogonal basis.*

Proof. Every subspace of V is also nonisotropic, in particular nondegenerate, so **??** applies. We prove the claim by induction on $n = \dim V$. If $n = 0$, then the claim is obvious, so assume that $n > 0$ and that the claim holds for $n-1$. Choose some nonzero $v \in V$ and let $U = \operatorname{span}(v)$. Then $\dim U^\perp = n-1$, so $U^\perp$ has an orthogonal basis $\mathcal{U}$ by induction. Then $\mathcal{U} \cup \{v\}$ is clearly an orthogonal basis for V. ■

(f) We next study maps that respect sesquilinear forms.

8.15 • **Definition:** ***Isometry.***
Let V and W be equipped with sesquilinear forms. A linear map $T\colon V \to W$ is an *isometry* if

$$\langle Tu, Tv\rangle_W = \langle u,v\rangle_V$$

for all $u,v \in V$. If T is also bijective, we say that it is *unitary* and say that V and W are *isometric*. ▲

Clearly the composition of two isometries is an isometry, and the inverse of a unitary map is also unitary. In particular, the set of unitary maps on V is a group under composition.

If T is an isometry, then notice that it also respects the associated quadratic forms, i.e. that $Q_W(Tv) = Q_V(v)$ for all $v \in V$. [TODO converse when quadratic form determines sesquilinear form.] Furthermore, we are used to isometries being injective, and the analogous result for sesquilinear forms is the following:

8.16 • Lemma. *If V is nonisotropic and $T\colon V \to W$ is an isometry, then T is injective.*

Proof. Let $u, v \in V$ and assume that $Tu = Tv$. Then

$$0 = Q_W(Tu - Tv) = Q_W\big(T(u-v)\big) = Q_V(u-v),$$

and since V is nonisotropic, this is only possible when $u = v$. ■

8.3 ⋄ Hilbert space adjoints

(a) In **??** we defined one notion of adjoint of a linear map $T\colon V \to W$, namely the pullback $T^\dagger\colon W^* \to V^*$. We now define a different kind of adjoint, denoted T^*, that only makes sense for linear maps between spaces equipped with sesquilinear forms. For T^* to be linear we need V and W to both be equipped with a σ-sesquilinear form for the same $\sigma \in \mathrm{Aut}(\mathbb{F})$, so we make this assumption from the onset. We also assume that V and W are nonsingular; this is not strictly necessary to define T^*, but we lose fundamental properties of adjoints if this is not the case (cf. **??**).[2] Later we will also need to assume that V and W are nonisotropic (cf. **??**).

It will also turn out to be useful to assume that the forms on V and W are (σ,ε)-Hermitian for possibly different ε. In V and W are nontrivial, then since they are assumed nonsingular, we must have $\varepsilon \neq 0$. Under the same assumptions the forms must be nontrivial, so **??** implies that σ is an involution. The case where V and W is trivial is – of course – trivial, so to avoid having to deal this special case, we simply assume that σ is always an involution, and that $\varepsilon \neq 0$.

Finally, we require that the Riesz maps Φ_V and Φ_W (cf. **??**) are σ-isomorphisms. It is not strictly necessary for this to be true of Φ_W to define T^*, but we again lose important properties without this assumption. For later use we also let U denote another vector space with the same properties. In total:

[2] Also strictly speaking, it is only necessary that one of V and W is nonsingular, but we assume that both are for simplicity.

Assumption. In this section, V, W, U are $\mathbb{F}$-vector spaces that are

(1) equipped with (σ, ε)-Hermitian forms for the same $\sigma \in \mathrm{Aut}(\mathbb{F})$ but possibly different $\varepsilon \in \mathbb{F}$, and

(2) nonsingular,

such that

(3) σ is an involution,

(4) $\varepsilon \neq 0$, and

(5) the Riesz maps Φ_V, Φ_W and Φ_U are σ-isomorphisms.

(b) We are now ready for the main definition in this section:

8.17 • Definition: *Hilbert space adjoints.*
Let $T \in \mathcal{L}(V, W)$. TODO notation, bounded vs. general linear The *(Hilbert space) adjoint* of T is the operator $T^* \colon W \to V$ given by

$$T^* = \Phi_V^{-1} \circ T^\dagger \circ \Phi_W.$$

Properties of the operator adjoint $T^\dagger$ are often inherited by the Hilbert space adjoint: Since Φ_V and Φ_W are both σ-linear and $T^\dagger$ is linear, it follows that T^* is linear. Furthermore, if $S \in \mathcal{L}(W, U)$ then

$$\begin{aligned}
(ST)^* &= \Phi_V^{-1} \circ (ST)^\dagger \circ \Phi_U \\
&= \Phi_V^{-1} \circ T^\dagger \circ S^\dagger \circ \Phi_U \\
&= (\Phi_V^{-1} \circ T^\dagger \circ \Phi_W) \circ (\Phi_W^{-1} \circ S^\dagger \circ \Phi_U) \\
&= T^* S^*.
\end{aligned}$$

8.18 • Proposition. *Let $T \in \mathcal{L}(V, W)$. For all $w \in W$ we have $T^\dagger \varphi_w = \varphi_{T^* w}$. In particular, T^* is the unique linear operator $W \to V$ with the property that*

$$\langle T^* w, v \rangle_V = \langle w, Tv \rangle_W,$$

or equivalently

$$\langle v, T^* w \rangle_V = \langle Tv, w \rangle_W,$$

for all $v \in V$ and $w \in W$. Furthermore, $T^{**} = T$, i.e., the map $T \mapsto T^*$ is an involution.

Note that we cannot (at least prima facie) prove that $T^{**} = T$ just by using the definition, since V^* and W^* are not equipped with sesquilinear forms.

Proof. First notice that T^* indeed has this property. For $w \in W$ we have

$$\varphi_{T^*w} = \Phi_V(T^*w) = (T^\dagger \circ \Phi_W)(w) = T^\dagger \varphi_w,$$

so for $v \in V$ it thus follows that

$$\langle T^*w, v\rangle_V = \varphi_{T^*w}(v) = T^\dagger \varphi_w(v) = \varphi_w(Tv) = \langle w, Tv\rangle_W,$$

as desired. The other identity follows since the forms are Hermitian. Furthermore, if $S\colon W \to V$ is another such operator, then $\langle Sw, v\rangle_V = \langle T^*w, v\rangle_V$ for all v and w, so $S = T^*$ by **??** since V is nonsingular. The final claim that $T^{**} = T$ follows by uniqueness, by replacing T with T^* in the identities above. ∎

(c) In **??** we defined what it means for a linear map to be an isometry or to be unitary. In the present context we can also characterise isometries using adjoints. Furthermore, recall from **??** that an isometry between *nonisotropic* spaces is automatically injective. We have not (yet, see **??**) assumed that the spaces in question are nonisotropic, only that they are nonsingular, but in the current setting we still get injectivity:

8.19 • LEMMA. *A linear map $T\colon V \to W$ is an isometry if and only if $T^*T = \mathrm{id}_V$. In particular, isometries are injective, and T is unitary if and only if T is bijective with $T^{-1} = T^*$.*

Proof. If T is an isometry, then

$$\langle T^*Tv, u\rangle_V = \langle Tv, Tu\rangle_W = \langle v, u\rangle_V,$$

implying that $T^*T = \mathrm{id}_V$ by **??**. The converse is obvious.

For the final claims, notice that the above says that T^* is a left-inverse of T, so T is injective. Furthermore, if T is unitary it is bijective, so T^* is also a right-inverse of T. Conversely, if $TT^* = \mathrm{id}_W$ then T is surjective and hence unitary. ∎

An operator $TT^* = \mathrm{id}_W$ with the property is called a ***coisometry***.

In the case $W = V$ we say that T is ***normal*** if $TT^* = T^*T$, and that T is ***self-adjoint*** if $T^* = T$. Clearly both self-adjoint and unitary operators (with $V = W$) are normal.

(d) Properties of adjoints TODO text

8.20 • PROPOSITION. *Let V be a finite-dimensional inner product space, and let $T \in \mathcal{L}(V)$ and $\lambda \in \mathbb{F}$. Then $\lambda \mathrm{id}_V - T$ is invertible if and only if $\sigma(\lambda)\mathrm{id}_V - T^*$ is invertible. In other words, λ is an eigenvalue of T if and only if $\sigma(\lambda)$ is an eigenvalue of T^*.*

TODO what about infinite dimension? Boundedly invertible? Also need σ to be an involution for the iff.

Proof. Since the maps $T \mapsto T^*$ and σ are involutions it suffices to prove one implication, so assume that $\lambda \operatorname{id}_V - T$ is invertible. Then there exists an $S \in \mathcal{L}(V)$ such that

$$S(\lambda \operatorname{id}_V - T) = (\lambda \operatorname{id}_V - T)S = \operatorname{id}_V,$$

and taking adjoints we find that

$$(\sigma(\lambda)\operatorname{id}_V - T^*)S^* = S^*(\sigma(\lambda)\operatorname{id}_V - T^*) = \operatorname{id}_V.$$

That is, $\sigma(\lambda)\operatorname{id}_V - T^*$ is invertible as claimed. ∎

8.21 • Remark. Note that this does *not* say that $v \in V$ is an eigenvector of T^* if it is an eigenvector of T. A counterexample is given by the matrix

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

which has the eigenvector $(1,0)$ with eigenvalue 1. However, while 1 is also an eigenvalue of the transpose $A^\top$ (with eigenvector $(1,1)$), $(1,0)$ is not an eigenvector of $A^\top$.

While this does not hold in general, recall that in **??** we saw that it holds for *normal* operators. ⌟

8.22 • Proposition. *Let $T \in \mathcal{L}(V)$ be a normal operator.*

(i) *$Q(Tv) = Q(T^*v)$ for all $v \in V$.*

(ii) *Assume that V is nonisotropic. Then $E_T(\lambda) = E_{T^*}(\sigma(\lambda))$ for all $\lambda \in \mathbb{F}$.*

(iii) *Assume that V is nonisotropic. If $\lambda, \mu \in \mathbb{F}$ are distinct eigenvalues of T, then $E_T(\lambda)$ and $E_T(\mu)$ are orthogonal.*

Proof. *??* : Notice that

$$Q(Tv) = \langle Tv, Tv \rangle = \langle T^*Tv, v \rangle = \langle TT^*v, v \rangle = \langle T^*v, T^*v \rangle = Q(T^*v).$$

?? : If T is normal then so is $\lambda \operatorname{id}_V - T$, so ?? implies that

$$Q\big((\lambda \operatorname{id}_V - T)v\big) = Q\big((\sigma(\lambda)\operatorname{id}_V - T^*)v\big),$$

and since V is assumed nonisotropic, this implies that $(\lambda \operatorname{id}_V - T)v = 0$ if and only if $(\sigma(\lambda)\operatorname{id}_V - T^*)v = 0$. Hence v is an eigenvector for T with eigenvalue λ if and only if v is an eigenvector for T^* with eigenvalue $\sigma(\lambda)$.

?? : Let $v \in E_T(\lambda)$ and $u \in E_T(\mu)$. Since v is also an eigenvector for T^* with eigenvalue $\sigma(\lambda)$ by ?? , we have

$$\mu\langle v,u\rangle = \langle v,Tu\rangle = \langle T^*v,u\rangle = \langle \sigma(\lambda)v,u\rangle = \lambda\langle v,u\rangle.$$

Since $\lambda \neq \mu$ we must have $\langle v,u\rangle = 0$ as claimed.

In the proof of **??** we will need to restrict normal operators to subspaces of V. In the discussion above we have assumed that V is nonsingular, but since this is not a hereditary property, we need to assume that relevant subspaces of V are also nonsingular. In **??** we will assume that V is nonisotropic, in which case this is automatically satisfied.

If U is a subspace of V and $T \in \mathcal{L}(V)$, then we say that U is ***invariant*** under T. In this case we define an operator $T_U \in \mathcal{L}(U)$ by $T_U u = Tu$ for $u \in U$. We then have the following results:

8.23 • Lemma. *Let $T \in \mathcal{L}(V)$. If a subspace U of V is invariant under T, then $U^\perp$ is invariant under T^*.*

Proof. Let $v \in U^\perp$. For $u \in U$ we have $Tu \in U$, so

$$\langle T^*v,u\rangle = \langle v,Tu\rangle = 0.$$

Since this holds for all $u \in U$, it follows that $T^*v \in U^\perp$ as desired. ■

8.24 • Lemma. *If $T \in \mathcal{L}(V)$ is normal and the subspace $U \subseteq V$ is nonsingular and invariant under both T and T^*, then $T_U \in \mathcal{L}(U)$ is also normal. To wit, $(T_U)^* = (T^*)_U$.*

Proof. This is obvious from **??**. ■

8.4 ◇ Orthogonal diagonalisation

(a) If V is a vector space equipped with a sesquilinear form, then a basis $\mathcal{V}$ for V is ***orthogonal*** if for $u,v \in \mathcal{V}$, $\langle u,v\rangle = 0$ when $u \neq v$. Furthermore, $\mathcal{V}$ is called ***orthonormal*** if also $Q(v) = 1$ for all $v \in \mathcal{V}$. In real or complex vector spaces any orthogonal basis can be modified to obtain an orthonormal basis, by dividing each basis vector by its norm. But for general σ-sesquilinear forms this is not possible, since even if $\sigma = \mathrm{id}_V$ we would need to divide v by a square root of $Q(v)$, and this might not exist; indeed $Q(v)$ might not even be nonzero.

To state the spectral theorem we need a definition. Recall that we in **??** defined what it means for an operator T to be diagonalisable. In the context of sesquilinear forms we have the following stronger properties: If V is finite-dimensional and equipped with a sesquilinear form, then an operator $T \in \mathcal{L}(V)$

is ***orthogonally diagonalisable*** if there is an orthogonal basis for V consisting of eigenvectors for T. If there is an *orthonormal* basis for V of eigenvectors, then T is ***orthonormally diagonalisable***. Clearly the latter is the stronger of the two properties.

Furthermore, if $\mathrm{id}_V = P_1 + \cdots + P_k$ is a resolution of the identity, then we say that it is ***orthogonal*** if each P_i is an orthogonal projection. We then have the following analogue of **??**:

8.25 • Proposition. *Let $T \in \mathcal{L}(V)$. The following are equivalent:*

(1) *T is orthogonally diagonalisable.*

(2) *V has an ordered orthogonal basis $\mathcal{V}$ such that ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ is diagonal.*

(3) *V has the form*
$$V = \bigodot_{\lambda \in \operatorname{Spec} T} E_T(\lambda).$$

(4) *If* $\operatorname{Spec} T = \{\lambda_1, \dots, \lambda_k\}$ *and P_i is projection onto $E_T(\lambda_i)$ along $\bigoplus_{j \neq i} E_T(\lambda_j)$, then* $\mathrm{id}_V = P_1 + \cdots + P_k$ *is an orthogonal resolution of the identity.*

(5) *T is orthogonally similar*[3] *to a multiplication operator M_A, where $A \in \mathrm{M}_n(\mathbb{F})$ is a diagonal matrix whose diagonal contains the eigenvalues of T with multiplicity:*
$$T = \varphi_{\mathcal{V}}^{-1} \circ M_A \circ \varphi_{\mathcal{V}}.$$

(b) We now arrive at the main theorem in this chapter, the spectral theorem. This is usually proved for normal operators on complex vector spaces, but as we show in this section, we can get away with assuming somewhat less. Apart from the assumptions we made in **??**, we will need the vector space V to be nonisotropic in order to access the results in **??**. We also need V to be finite-dimensional, partly since our proof of the spectral theorem will be by induction in the dimension of V, and partly since we will also need every (normal) operator on V to have an eigenvalue. For the latter reason we also assume that $\mathbb{F}$ is algebraically closed. In total:

> **Assumption.** For the remainder of this section, V denotes an $\mathbb{F}$-vector space that is
>
> (1) finite-dimensional,
>
> (2) equipped with a (σ, ε)-Hermitian form, and
>
> (3) nonisotropic,
>
> such that

[3] Cf. **??**.

(4) $\mathbb{F}$ is algebraically closed,
(5) σ is an involution, and
(6) $\varepsilon \neq 0$.

Note that since V is finite-dimensional, we do not need to assume that the Riesz map Φ_V is a σ-isomorphism.

8.26 • Theorem: ***The spectral theorem.***
An operator $T \in \mathcal{L}(V)$ is normal if and only if it is orthogonally diagonalisable.

Proof. First assume that T is normal. We prove by induction in $n = \dim V$ that T is orthogonally diagonalisable. If $n = 1$ then this follows since T has an eigenvalue, so assume that the claim is proved for operators on spaces of dimension strictly less than n.

Let $\lambda \in \operatorname{Spec} T$, and consider the corresponding eigenspace $E_T(\lambda)$. If $d := \dim E_T(\lambda) = n$, then any orthogonal basis of $E_T(\lambda)$ will suffice (and such a basis exists by **??**). Assume therefore that $0 < d < n$.

The space $E_T(\lambda) = E_{T^*}(\sigma(\lambda))$ is clearly invariant under both T and T^*. It follows from **??** that $E_T(\lambda)^\perp$ is also invariant under both T and T^*. We furthermore have $\dim E_T(\lambda)^\perp = n - d$ and $0 < n - d < n$ by **??**. Let $T_\parallel \in \mathcal{L}(E_T(\lambda))$ and $T_\perp \in \mathcal{L}(E_T(\lambda)^\perp)$ denote the restrictions of T to $E_T(\lambda)$ and $E_T(\lambda)^\perp$ respectively. Both $T_\parallel$ and $T_\perp$ are also normal by **??**, so the induction hypothesis furnishes orthogonal bases $\mathcal{U}$ and $\mathcal{W}$ for $E_T(\lambda)$ and $E_T(\lambda)^\perp$ consisting of eigenvectors of T. But then $\mathcal{V} = \mathcal{U} \cup \mathcal{W}$ is an orthogonal basis for V as desired.

Conversely, let $\mathcal{V}$ be an orthogonal basis for V consisting of eigenvectors for T, so that the matrix representation ${}_{\mathcal{V}}[T]_{\mathcal{V}}$ is diagonal. Hence this commutes with ${}_{\mathcal{V}}[T^*]_{\mathcal{V}}$, so T and T^* also commute. ■

8.5 ⋄ Coordinate representations

(a) In the sequel we fix a finite-dimensional $\mathbb{F}$-vector space, and we also fix a σ-sesquilinear form $\langle \cdot, \cdot \rangle$ on V. If $A = (a_{ij}) \in \mathrm{M}_{m,n}(\mathbb{F})$ is a matrix, we denote by A^σ the $n \times m$ matrix whose (i,j)th element is $\sigma(a_{ji})$ and call this the ***σ-conjugate*** of A. That is, A^σ is obtained from A by transposition and entrywise application of σ. If $B \in \mathrm{M}_{n,k}(\mathbb{F})$ is another matrix, notice that $(AB)^\sigma = B^\sigma A^\sigma$.

In the case where $\sigma = \mathrm{id}_V$, we recover the transpose $A^\top$, and when $\mathbb{F} = \mathbb{C}$ and σ is complex conjugation, A^σ is the conjugate transpose.

(b) Consider an ordered basis $\mathcal{V} = (v_1, \dots, v_n)$ for V, and let $u = \sum_{i=1}^n \alpha_i v_i$ and $v = \sum_{i=1}^n \beta_i v_i$ be vectors in V. Notice that

$$\langle u, v \rangle = \sum_{i=1}^n \sum_{j=1}^n \sigma(\alpha_i) \langle v_i, v_j \rangle \beta_j.$$

Hence if we define the matrix $\Sigma = (\langle v_i, v_j \rangle)_{i,j} \in \mathrm{M}_n(\mathbb{F})$, then[4]

$$\langle u, v \rangle = \begin{pmatrix} \sigma(\alpha_1) & \cdots & \sigma(\alpha_n) \end{pmatrix} \begin{pmatrix} \langle v_1, v_1 \rangle & \cdots & \langle v_1, v_n \rangle \\ \vdots & \ddots & \vdots \\ \langle v_n, v_1 \rangle & \cdots & \langle v_n, v_n \rangle \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = [v]_{\mathcal{V}}^{\sigma} \Sigma [w]_{\mathcal{V}}. \quad (8.1)$$

We call Σ the ***matrix representation*** of the form $\langle \cdot, \cdot \rangle$ with respect to the basis $\mathcal{V}$. [TODO Σ singular iff V singular, right?]

Conversely, notice that after fixing a basis $\mathcal{V}$, any square matrix Σ gives rise to a sesquilinear form by the identity **??**. Furthermore, such a matrix is uniquely determined (once a basis has been chosen), so there is a one-to-one correspondence between sesquilinear forms and square matrices, given a choice of basis. [TODO is there? Just double check.]

(c) Next we study how a matrix representation of transforms under a change of basis. If $\mathcal{W}$ is another basis for V then the results in [TODO ref] show that e.g. $[v]_{\mathcal{W}} = {}_{\mathcal{W}}[\square]_{\mathcal{V}} [v]_{\mathcal{V}}$. If Σ and Γ are the matrix representation of φ with respect to $\mathcal{V}$ and $\mathcal{W}$, respectively, then

$$\langle u, v \rangle = [u]_{\mathcal{W}}^{\sigma} \Gamma [v]_{\mathcal{W}} = [u]_{\mathcal{V}}^{\sigma} {}_{\mathcal{W}}[\square]_{\mathcal{V}}^{\sigma} \Gamma {}_{\mathcal{W}}[\square]_{\mathcal{V}} [v]_{\mathcal{V}},$$

so $\Sigma = {}_{\mathcal{W}}[\square]_{\mathcal{V}}^{\sigma} \Gamma {}_{\mathcal{W}}[\square]_{\mathcal{V}}$ by uniqueness. Two matrices $A, B \in \mathrm{M}_n(\mathbb{F})$ are said to be ***σ-congruent*** if there is an invertible matrix P such that $A = P^{\sigma} B P$. We have thus shown that matrix representations of a form with respect to different bases are σ-congruent. [TODO converse, there exists a basis for which...]

(d) Now let V and W be finite-dimensional inner product spaces, and let $\Sigma \in \mathrm{M}_n(\mathbb{K})$ and $\Gamma \in \mathrm{M}_m(\mathbb{K})$ be the matrices of the inner products of V and W with respect to ordered bases $\mathcal{V}$ and $\mathcal{W}$, respectively. We then have the following characterisation of adjoints of linear maps $V \to M$.

8.27 • Proposition. *Let $T\colon V \to W$ be a linear map. Its adjoint $T^*\colon W \to V$ is the unique linear map satisfying*

$$\Sigma {}_{\mathcal{V}}[T^*]_{\mathcal{W}} = ({}_{\mathcal{W}}[T]_{\mathcal{V}})^* \Gamma.$$

Proof. **??** implies that

$$[v]_{\mathcal{V}}^* \Sigma {}_{\mathcal{V}}[T^*]_{\mathcal{W}} [w]_{\mathcal{W}} = \langle v, T^* w \rangle_V = \langle Tv, w \rangle_W = [v]_{\mathcal{V}}^* ({}_{\mathcal{W}}[T]_{\mathcal{V}})^* \Gamma [w]_{\mathcal{W}},$$

for all $v \in V$ and $w \in W$, and T^* is clearly unique with this property. ■

[4] Again we see the usefulness of sesquilinear forms being linear in the second entry: For then we simply σ-transpose the coordinate vector of the left argument and leave the coordinate vector of the right argument untouched.

This result has various important consequences in the case where $\mathcal{V}$ and $\mathcal{W}$ are orthonormal:

8.28 • COROLLARY. *If $\mathcal{V}$ and $\mathcal{W}$ are orthonormal, then*

$$_{\mathcal{V}}[T^*]_{\mathcal{W}} = (_{\mathcal{W}}[T]_{\mathcal{V}})^{\sigma}.$$

8.29 • COROLLARY. *If $V = W$, and if $\mathcal{V}$ is orthogonal and consists of nonisotropic vectors, then*

$$_{\mathcal{V}}[T^*]_{\mathcal{V}} = (_{\mathcal{V}}[T]_{\mathcal{V}})^{\sigma}.$$

Proof. In this case $\Sigma = \Gamma$ is diagonal, so it commutes with $(_{\mathcal{V}}[T]_{\mathcal{V}})^{\sigma}$. Its diagonal elements are also nonzero, so it is invertible, and hence

$$_{\mathcal{V}}[T^*]_{\mathcal{V}} = \Sigma^{-1}(_{\mathcal{V}}[T]_{\mathcal{V}})^{\sigma}\Sigma = \Sigma^{-1}\Sigma(_{\mathcal{V}}[T]_{\mathcal{V}})^{\sigma} = (_{\mathcal{V}}[T]_{\mathcal{V}})^{\sigma},$$

as claimed. ■

8.30 • COROLLARY. *If $T\colon \mathbb{K}^n \to \mathbb{K}^m$, then*

$$\mathcal{M}(T^*) = \mathcal{M}(T)^*.$$

8.31 • COROLLARY. *If $A \in \mathrm{M}_{m,n}(\mathbb{K})$, then*

$$M_{A^*} = (M_A)^*.$$

8.6 ◇ Projections II

(a) If V is equipped with a sesquilinear form, then a projection $P\colon V \to V$ is ***orthogonal*** if $\operatorname{im} P$ and $\ker P$ are orthogonal subspaces of V.

In this section we make the same further assumptions as in **??**. In particular, operators on V have Hilbert space adjoints.

8.32 • PROPOSITION. *A projection $P\colon V \to V$ is orthogonal if and only if P is self-adjoint.*

Proof. Assume that P is orthogonal so that $\operatorname{im} P \perp \ker P$ and let $u, v \in V$. Since then $Pu \in \operatorname{im} P$ and $u - Pu \in \ker P$, and similarly for v, we get

$$\langle u - Pu, Pv\rangle = 0 = \langle Pu, v - Pv\rangle.$$

This implies that

$$\langle u, Pv\rangle = \langle Pu, Pv\rangle = \langle Pu, v\rangle = \langle u, P^* v\rangle,$$

which shows that $P = P^*$.

Conversely assume that P is self-adjoint. For $u \in \operatorname{im} P$ and $v \in \ker P$ we then have

$$\langle u, v\rangle = \langle Pu, v\rangle = \langle u, Pv\rangle = \langle u, 0\rangle = 0,$$

so $\operatorname{im} P$ and $\ker P$ are orthogonal. ∎

(b) TODO Next we consider finite-dimensional inner product spaces V and W. If U is a subspace of V, then the inclusion map $\iota_U \colon U \to V$ is injective and its image is $\operatorname{im} \iota_U$. Hence the following gives a formula for orthogonal projection operators onto any subspace:

8.33 • **Proposition.** *Let $T \colon W \to V$ be an injective linear operator, and let P be the orthogonal projection onto* $\operatorname{im} T$. *Then $P = T(T^*T)^{-1}T^*$.*

Proof. First note that T^*T is indeed injective (hence invertible) since T is. This follows from the identity $\ker T^* = (\operatorname{im} T)^{\perp}$. TODO prove this

Next notice that the rank of P is $\dim \operatorname{im} T$. But T^* is surjective since T is injective, so the rank of $T(T^*T)^{-1}T^*$ is also $\dim \operatorname{im} T$. It thus suffices to show that P and $T(T^*T)^{-1}T^*$ agree on $\operatorname{im} T$, and writing $v = Tw$ we have

$$T(T^*T)^{-1}T^*v = T(T^*T)^{-1}(T^*T)w = Tw = v,$$

as desired. ∎

Note that the proof does not go through in the infinite-dimensional case, for then we cannot simply use dimension arguments.

We specialise to the case where $V = \mathbb{R}^n$, and the inner product on $\mathbb{R}^n$ has the matrix representation Σ with respect to the standard basis.[5] In this case we may also assume that $W = \mathbb{R}^k$ where $k = \dim U$: Simply precompose ι_U with any isomorphism $\mathbb{R}^k \to U$.

Furthermore, let $A \in \mathrm{M}_{n,k}(\mathbb{R})$ be the standard matrix representation of $T \colon \mathbb{R}^k \to \mathbb{R}^n$. In this case, U is of course the column space of A, and A is of full rank. We then have the following result:

8.34 • **Proposition.** *The orthogonal projection P onto $R(A)$ is given by*

$$\mathcal{M}(P) = A(A^\top \Sigma A)^{-1} A^\top \Sigma.$$

Proof. Equip $\mathbb{R}^k$ with the standard inner product. Its matrix representation with respect to the standard basis is then just the identity matrix, so **??** implies that

$$\mathcal{M}(T^*) = \mathcal{M}(T)^\top \Sigma = A^\top \Sigma.$$

[5] Note that the standard basis is not necessarily orthonormal with respect to the given inner product.

Applying this to **??** we thus obtain

$$\begin{aligned}\mathcal{M}(P) &= A\Big(\mathcal{M}(T^*)A\Big)^{-1}\mathcal{M}(T^*)\\ &= A(A^\top \Sigma A)^{-1}A^\top \Sigma,\end{aligned}$$

as claimed. ■

8.7 ⋄ Real and complex sesquilinear forms

The spectral theorem in the form stated in TODO ref applies directly to inner products on complex vector spaces, but there is of course also a version of the spectral theorem for real vector spaces. In order to formulate it in the desired generality, we first study how to extend the constructions developed in this chapter from real to complex vector spaces.

(a) We first consider how to extend a field automorphism on $\mathbb{R}$ to an automorphism on $\mathbb{C}$. Note that since an endomorphism on $\mathbb{R}$ is in particular an $\mathbb{R}$-linear map, it is either surjective or the zero map. But the latter is impossible since it must send 1 to 1, so every field endomorphism is automatically an automorphism.

8.35 • Lemma. *Let $\sigma \in \operatorname{Aut}(\mathbb{R})$. Then the maps $\sigma_\pm^{\mathbb{C}} \colon \mathbb{C} \to \mathbb{C}$ given by*

$$\sigma_\pm^{\mathbb{C}}(\alpha + \mathrm{i}\beta) = \sigma(\alpha) \pm \mathrm{i}\sigma(\beta)$$

for $\alpha, \beta \in \mathbb{R}$ are the only endomorphisms on $\mathbb{C}$ that extend σ, and they are also automorphisms. Furthermore, σ is an involution if and only if the $\sigma_\pm^{\mathbb{C}}$ are.

Proof. It is easy to see that they are in fact field homomorphisms, hence $\mathbb{C}$-linear and thus bijective. To prove uniqueness, let $\tau \colon \mathbb{C} \to \mathbb{C}$ be a field homomorphism extending σ. For $\alpha, \beta \in \mathbb{R}$ we then have

$$\tau(\alpha + \mathrm{i}\beta) = \tau(\alpha) + \tau(\mathrm{i})\tau(\beta) = \sigma(\alpha) + \tau(\mathrm{i})\sigma(\beta).$$

But since $\mathrm{i}^2 = -1$, we have

$$\tau(\mathrm{i})^2 = \tau(\mathrm{i}^2) = \tau(-1) = -1,$$

so $\tau(\mathrm{i}) \in \{\pm \mathrm{i}\}$. The final claim is obvious. ■

We will see shortly which of $\sigma_+^{\mathbb{C}}$ and $\sigma_-^{\mathbb{C}}$ is the right choice.

Next we must consider how to extend sesquilinear forms from a real vector space V to its complexification $V^{\mathbb{C}}$. There is of course a canonical way of extending inner products as mentioned in TODO ref, so we extend general sesquilinear forms to be consistent with that procedure: Namely, if φ is a sesquilinear form on V, then we define $\varphi^{\mathbb{C}} \colon V^{\mathbb{C}} \times V^{\mathbb{C}} \to \mathbb{C}$ by

$$\varphi^{\mathbb{C}}(u + \mathrm{i}v, x + \mathrm{i}y) = \varphi(u,x) + \varphi(v,y) + \mathrm{i}\big(\varphi(u,y) - \varphi(v,x)\big),$$

for $u,v,x,y \in V$. It is easy to see that this is bi-additive and $\mathbb{C}$-linear in its second entry, and that it agrees with φ on $V \times V$. But assume that φ is a σ-sesquilinear form. Then we might hope that $\varphi^{\mathbb{C}}$ is either a $\sigma_+^{\mathbb{C}}$- or a $\sigma_-^{\mathbb{C}}$-sesquilinear form. But a short calculation shows that it is indeed $\sigma_-^{\mathbb{C}}$-sesquilinear. This we might have expected, since the canonical automorphism on $\mathbb{C}$ is complex conjugation which precisely sends i to −i.

8.36 • PROPOSITION. (i) *φ is nontrivial if and only if $\varphi^{\mathbb{C}}$ is nontrivial.*

(ii) *φ is (σ, ε)-Hermitian if and only if $\varphi^{\mathbb{C}}$ is $(\sigma_-^{\mathbb{C}}, \varepsilon)$-Hermitian.*

Proof. TODO ■

8.37 • PROPOSITION. *TODO Isotropic?*

(b) The trick is to take the complexification $T^{\mathbb{C}}$ of a self-adjoint operator T on a real vector space. We first show that $T^{\mathbb{C}}$ is then also self-adjoint:

8.38 • PROPOSITION. *Let V and W be real Hilbert spaces, and let $T \in \mathcal{B}(V,W)$. Then we have*

$$(T^{\mathbb{C}})^* = (T^*)^{\mathbb{C}},$$

i.e., the adjoint of the complexification of T is the complexification of the adjoint of T. In particular

(i) *T is normal if and only if $T^{\mathbb{C}}$ is normal, and*

(ii) *T is self-adjoint if and only if $T^{\mathbb{C}}$ is self-adjoint.*

Proof. For $v,u,x,y \in V$ we have

$$\begin{aligned}
\langle (T^*)^{\mathbb{C}}(x + \mathrm{i}y), v + \mathrm{i}u \rangle &= \langle T^*x + \mathrm{i}T^*y, v + \mathrm{i}u \rangle \\
&= \langle T^*x, v \rangle + \langle T^*y, u \rangle + \mathrm{i}(\langle T^*x, u \rangle - \langle T^*y, v \rangle) \\
&= \langle x, Tv \rangle + \langle y, Tu \rangle + \mathrm{i}(\langle x, Tu \rangle - \langle y, Tv \rangle) \\
&= \langle x + \mathrm{i}y, Tv + \mathrm{i}Tu \rangle \\
&= \langle x + \mathrm{i}y, T^{\mathbb{C}}(v + \mathrm{i}u) \rangle.
\end{aligned}$$

Uniqueness of adjoints thus yields the claim.

Assume that T is normal. Then

$$T^{\mathbb{C}}(T^{\mathbb{C}})^* = T^{\mathbb{C}}(T^*)^{\mathbb{C}} = (TT^*)^{\mathbb{C}} = (T^*T)^{\mathbb{C}} = (T^*)^{\mathbb{C}}T^{\mathbb{C}} = (T^{\mathbb{C}})^*T^{\mathbb{C}},$$

so $T^{\mathbb{C}}$ is normal. The converse follows similarly. If T is self-adjoint, then

$$(T^{\mathbb{C}})^* = (T^*)^{\mathbb{C}} = T^{\mathbb{C}},$$

and similarly if $T^{\mathbb{C}}$ is self-adjoint. ∎

(c) As promised we prove a polarisation identity for certain sesquilinear forms on complex vector spaces. Let V be a complex vector space, and denote complex conjugation by $\alpha \mapsto \alpha^*$. Then a *-sesquilinear form is just a form that is conjugate-linear in its first entry. Its quadratic form Q then satisfies $Q(\alpha v) = |\alpha|^2 Q(v)$ for all $v \in V$ and $\alpha \in \mathbb{C}$.

8.39 • Proposition. *Let φ be a *-sesquilinear form on V with quadratic form Q. Then*

$$\varphi(u,v) = \frac{1}{4}\sum_{k=0}^{3} \mathrm{i}^k Q(\mathrm{i}^k u + v)$$

for all $u,v \in V$. ∎

As in the proof of TODO ref, this follows simply by inserting the definition of Q.

The usual complex inner product is in fact also $(^*,1)$-Hermitian, and this property allows us to give a different proof of TODO ref which illustrates the connection between the polarisation identity for bilinear forms and the one for *-sesquilinear forms. The first step is to notice that whether or not a form is $(^*,1)$-Hermitian is determined by its quadratic form:

8.40 • Lemma. *Let φ be a *-sesquilinear form on V with quadratic form Q. Then φ is $(^*,1)$-Hermitian if and only if $Q(v) \in \mathbb{R}$ for all $v \in V$.*

Proof. If φ is $(^*,1)$-Hermitian, then

$$\overline{Q(v)} = \overline{\varphi(v,v)} = \varphi(v,v) = Q(v).$$

Conversely, if Q is real-valued then

$$0 = \operatorname{Im} Q(u+v) = \operatorname{Im}\varphi(u,v) + \operatorname{Im}\varphi(v,u)$$

and

$$0 = \operatorname{Im} Q(u+\mathrm{i}v) = -\operatorname{Re}\varphi(u,v) + \operatorname{Re}\varphi(v,u)$$

for all $u,v \in V$, implying that φ is $(^*,1)$-Hermitian. ∎

Now notice that if φ is *-sesquilinear and $(^*, 1)$-Hermitian, then the quadratic forms corresponding to φ and $\operatorname{Re}\varphi$ coincide since they are real-valued. It thus follows from TODO ref that

$$\operatorname{Re}\varphi(u,v) = \frac{1}{4}\big(Q(u+v) - Q(u-v)\big)$$

for all $u,v \in V$. Further notice that for $u \in V$ the map $v \mapsto \varphi(u,v)$ is a linear functional, and hence on the form [TODO ref]

$$\begin{aligned}
\varphi(u,v) &= \operatorname{Re}\varphi(u,v) - \mathrm{i}\operatorname{Re}\varphi(u,\mathrm{i}v) \\
&= \operatorname{Re}\varphi(u,v) + \mathrm{i}\operatorname{Re}\varphi(\mathrm{i}u,v) \\
&= \frac{1}{4}\big(Q(u+v) - Q(u-v) + \mathrm{i}Q(\mathrm{i}u+v) - \mathrm{i}Q(\mathrm{i}u-v)\big) \\
&= \frac{1}{4}\big(Q(u+v) - Q(-u+v) + \mathrm{i}Q(\mathrm{i}u+v) - \mathrm{i}Q(-\mathrm{i}u+v)\big),
\end{aligned}$$

where we have used that $Q(-w) = Q(w)$. And this is precisely TODO ref.

9 TODO Lambda Calculus

9.1 ◇ Syntax

(a) Let *Vars* denote a countable collection of variables. Along with these variables, the alphabet Σ also contains the lambda symbol 'λ', the full stop '.', and the left and right parentheses '(' and ')'. If x and y are words over Σ, then we write $x \equiv y$ to denote that x and y contain the same symbols, i.e. that they are ***syntactically equal***. The notation $M :\equiv N$ means that we define M to be syntactically equal to N. We will define different types of equality between terms of the lambda calculus below, hence the perhaps strange disuse of the equals sign.

9.1 • Definition: *λ-terms*.
The collection Λ of λ-*terms* is the smallest collection of words over Σ satisfying the following:

(i) If $x \in \mathit{Vars}$, then $x \in \Lambda$.

(ii) If $M, N \in \Lambda$, then $(MN) \in \Lambda$.

(iii) If $x \in \mathit{Vars}$ and $M \in \Lambda$, then $(\lambda x.M) \in \Lambda$.

Here we fall into the usual abuse of notation of mixing object and meta language symbols. Being precise for a moment, if 'x' is a variable (that is, the symbol itself is a variable), then '$\lambda x.xx$' is a λ-term. If the metavariable 'M' denotes the term 'xx', then we we will usually write '$\lambda x.M$' for '$\lambda x.xx$'. That is, the λ-term beginning with '$\lambda x.$', followed by M.

We also omit parentheses whenever it does not lead to confusion. Furthermore, application is left-associative, and we define $MNL :\equiv (MN)L$. Similarly, abstraction is right-associative, and we use the shorthand

$$\lambda x_1 x_2 \cdots x_n.M :\equiv (\lambda x_1(\lambda x_2(\cdots(\lambda x_n.M)))).$$

(b) The collection of ***free variables*** in a λ-term is defined by

$$\begin{aligned} FV(x) &= \{x\}, \\ FV(MN) &= FV(M) \cup FV(N), \\ FV(\lambda x.M) &= FV(M) \setminus \{x\}. \end{aligned}$$

Strictly speaking, for this definition to make sense we would need to show that λ-terms satisfy ***unique parsing***, i.e. that a λ-term can be on exactly one of the forms x, (MN) or $(\lambda x.M)$. Furthermore, the value of FV on some term M is defined in terms of the value that FV takes on terms that contain strictly fewer symbols than M. Similarly, the collection of ***bound variables*** is defined by

$$\begin{aligned} BV(x) &= \emptyset, \\ BV(MN) &= BV(M) \cup BV(N), \\ BV(\lambda x.M) &= BV(M) \cup \{x\}. \end{aligned}$$

Notice that $FV(M)$ and $BV(M)$ are not necessarily disjoint. The collection of all variables occurring in a λ-term M is clearly given by $FV(M) \cup BV(M)$ and is denoted $V(M)$.

(c) Finally, we define the set of ***subterms*** of a λ-term:

$$\begin{aligned} \mathrm{Sub}(x) &= \{x\}, \\ \mathrm{Sub}(MN) &= \mathrm{Sub}(M) \cup \mathrm{Sub}(N) \cup \{(MN)\}, \\ \mathrm{Sub}(\lambda x.M) &= \mathrm{Sub}(M) \cup \{(\lambda x.M)\}. \end{aligned}$$

9.2 ⋄ Reduction and equivalence of λ-terms

(a) We first review the basics of binary relations. If X and Y are sets, then a ***(binary) relation*** from X to Y is a subset $R \subseteq X \times Y$. If $(x,y) \in R$ then we also write xRy. We will later need the ***domain of definition*** of R, defined as the set

$$\operatorname{dom} R = \{x \in X \mid \exists y \in Y : (x,y) \in R\}.$$

The ***converse relation*** of R is the relation $R^\top \subseteq Y \times X$ with the property that $yR^\top x$ just when xRy. Given relations $R_i \subseteq X \times Y$ for i in some index set I, it is easy to see that $(\bigcup_{i\in I} R_i)^\top = \bigcup_{i \in I} R_i^\top$. We also write R_1R_2 for the union $R_1 \cup R_2$.

If $S \subseteq Y \times Z$ is another relation, then the composition of R with S is given by

$$S \circ R = \{(x,z) \in X \times Z \mid \exists y \in Y : xRy \text{ and } ySz\}.$$

We see that $(S \circ R)^\top = R^\top \circ S^\top$. The ***diagonal relation*** on X is given by $\Delta_X = \{(x,x) \mid x \in X\}$. Notice that Δ_X is just equality, so it is in particular an equivalence relation. If $Y = X$, then we define $R^0 = \Delta_X$ and $R^n = R^{n-1} \circ R$ for $n \in \mathbb{N}$. Finally we let[1] $R^+ = \bigcup_{n\in\mathbb{N}} R^n$.

If $R \in X \times X$, then the ***reflexive closure*** of R is the smallest relation on X that is reflexive and contains R. We define the symmetric and transitive closures similarly. It is then easy to see that

$$R_r = R \cup \Delta_X, \quad R_s = R \cup R^\top, \quad \text{and} \quad R_t = R^+,$$

[1] Note that $0 \notin \mathbb{N}$.

are the reflexive, symmetric and transitive closures of R, respectively. From these definitions it is easy to show that $(R_r)_s = (R_s)_r$, and that R_t is reflexive/symmetric if R is reflexive/symmetric.

(b) If R is a binary relation on Λ, there is another desirable property R may have:

9.2 • DEFINITION: ***Compatibility.***
The relation R is *compatible* if for $M,N,L \in \Lambda$ and $x \in \mathit{Vars}$, $(M,N) \in R$ implies that

(i) $(ML,NL) \in R$,

(ii) $(LM,LN) \in R$, and

(iii) $(\lambda x.M, \lambda x.N) \in R$.

If R is compatible, reflexive and transitive, then we call it a *reduction*. ▲

TODO weak extensionality.

The ***compatible closure*** of a relation R is the smallest compatible relation containing R, denoted R_λ. This clearly exists since the intersection of a collection of compatible relations is itself compatible. We may also give an explicit characterisation of R_λ: First let $S_0 = R$ and recursively define

$$S_n = S_{n-1} \cup \{(ML,NL),(LM,LN),(\lambda x.M,\lambda x.N) \mid (M,N) \in S_{n-1}\}$$

for $n \in \mathbb{N}$. It is then easy to see that $R_\lambda = \bigcup_{n\in\mathbb{N}} S_n$.

(c) If R is any binary relation on Λ that we think of as providing a way of 'reducing' terms, then we call R a ***notion of reduction***. The compatible closure R_λ is then called ***one-step R-reduction*** and is denoted $\rightarrow_R$. The reflexive and transitive closure of $\rightarrow_R$ is simply called ***R-reduction*** and is denoted $\twoheadrightarrow_R$. Instead taking the equivalence closure of $\rightarrow_R$ yields a relation $=_R$ called ***R-equivalence***. Notice that if we instead take the symmetric closure of $\twoheadrightarrow_R$, then the resulting relation is not necessarily transitive. Afterwards taking the transitive closure we again obtain the relation $=_R$.

9.3 • LEMMA. *If R is compatible, then so are $\rightarrow_R$, $\twoheadrightarrow_R$ and $=_R$.*

Proof. It suffices to show that the closures R_r, R_s and R_t are also compatible. For the reflexive closure R_r, this is obvious. For the symmetric closure R_s, let $(M,N) \in R_s = R \cup R^\top$. If $(M,N) \in R$ then we clearly have e.g. $(ML,NL) \in R$. If instead $(M,N) \in R^\top$, then $(N,M) \in R$ which implies that $(NL,ML) \in R \subseteq R_s$. The other properties are proved similarly.

For the transitive closure R_t, simply notice that R^n is compatible (which is easily shown by induction). ■

9.4 • **Definition.** Let R be a notion of reduction. An element of $\operatorname{dom} R$ is called an *R-redex*. If $M \in \Lambda$ and no subterm of M is an R-redex, then M is an *R-normal form*. If also $N \in \Lambda$ and $M =_R N$, then we say that M is an R-normal form of N. ▲

The following lemma is intuitively very obvious, but it is relatively difficult to prove rigorously, so we omit the proof:

9.5 • **Lemma.** *Let M be an R-normal form. Then $M \twoheadrightarrow_R N$ implies that $M \equiv N$. In other words, there is no N such that $M \rightarrow_R N$.* ■

9.6 • **Definition: *The diamond property.***
A binary relation $\rhd$ on Λ is said to satisfy the *diamond property* if $M \rhd N_1$ and $M \rhd N_2$ implies the existence of an L such that $N_1 \rhd L$ and $N_2 \rhd L$. ▲

Put diagrammatically, if we represent the relationship $M \rhd N$ with an arrow $M \rightarrow N$:

$$\begin{tikzcd}
& N_1 \arrow[dr] & \\
M \arrow[ur] \arrow[dr] & & L \\
& N_2 \arrow[ur] &
\end{tikzcd}$$

9.7 • **Definition: *Church–Rosser.***
A notion of reduction R is said to be *Church–Rosser* if $\twoheadrightarrow_R$ has the diamond property. ▲

9.8 • **Theorem: *The Church–Rosser theorem.***
If R is Church–Rosser and $M =_R N$, then there exists an $L \in \Lambda$ such that

$$M \twoheadrightarrow_R L \quad \textit{and} \quad N \twoheadrightarrow_R L$$

Proof. This follows easily by structural induction on the second definition of $=_R$ as the symmetric and transitive closure of $\twoheadrightarrow_R$. ■

9.9 • **Corollary.** *If R is Church–Rosser and N is an R-normal form of M, then $M \twoheadrightarrow_R N$.*

Proof. By **??** there is an L such that $M \twoheadrightarrow_R L$ and $N \twoheadrightarrow_R L$. But since N is an R-normal form, **??** implies that $N \equiv L$. ■

9.10 • **Corollary.** *If R is Church–Rosser, then a term can have at most one R-normal form.*

Proof. If N_1 and N_2 are both R-normal forms of M, then $N_1 =_R M =_R N_2$. **??** then yields an L to which both normal forms reduce, but then $N_1 \equiv L \equiv N_2$ by **??**. ■

9.3 ◇ α-equivalence and substitution

9.11 • Definition: ***Renaming.***
Let $M, N \in \Lambda$ and $x, y, z \in \mathit{Vars}$. Define the *renaming* operation $M \mapsto M^{x\to y}$ on Λ by

$$\begin{aligned} x^{x\to y} &:\equiv y, \\ z^{x\to y} &:\equiv z && \text{if } z \not\equiv x, \\ (MN)^{x\to y} &:\equiv M^{x\to y}N^{x\to y}, \\ (\lambda x.M)^{x\to y} &:\equiv \lambda x.M, \\ (\lambda z.M)^{x\to y} &:\equiv \lambda z.(M^{x\to y}) && \text{if } z \not\equiv x. \end{aligned}$$

The renaming operation replaces all 'free occurrences' of x with y. This allows us to define the following: Let

$$\alpha = \{(\lambda x.M, \lambda y.M^{x\to y}) \mid M \in \Lambda, x \in \mathit{Vars}, y \in \mathit{Vars} \setminus V(M)\}.$$

The corresponding equivalence relation $=_\alpha$ is of course called ***α-equivalence***. This is supposed to capture changes of bound variables, since the particular choice of bound variables is immaterial. When performing such a change, we require that the new variable y does not already occur in the body M of the term. If it occurred in M as a free variable, then the new binding λy would inadvertently bind these free occurrences. On the other hand, if Y occurred in M as a bound variable, then renaming a free x to y would also inadvertently bind the renamed variable.

With α-equivalence at our disposal, we can now define general substitution of terms in place of variables:

9.12 • Definition: ***Substitution.***
Let $M, M_1, M_2, N \in \Lambda$ and $x, y, z \in \mathit{Vars}$. We define the *substitution* operation $M \mapsto M[x := N]$ on Λ by

$$\begin{aligned} x[x := N] &:\equiv N, \\ z[x := N] &:\equiv z \quad \text{if } z \not\equiv x, \\ (M_1M_2)[x := N] &:\equiv M_1[x := N]M_2[x := N], \end{aligned}$$

and we further define

$$(\lambda y.M)[x := N] :\equiv \lambda z.(M^{y\to z}[x := N]),$$

if $\lambda z.M^{y\to z} =_\alpha \lambda y.M$ and $z \notin FV(N)$. ▲

Note that the last definition is not strictly speaking well-defined, since different choices of z lead to different expressions. This is of course no problem in practice (not least because we only consider terms up to α-equivalence), but if we really wanted to, we could e.g. index the variables with the natural numbers (since there are countably many variables) and require that z be the variable not occurring in either $\lambda y.M$ or N with the lowest index. Notice also that these terms contain finitely many variables, so there is in fact such a z.

9.4 ⋄ β-reduction

Until now the interpretation of λ-terms as functions has not been used to apply functions to arguments. To include this interpretation in the theory, we need some way of identifying the application of a function to an argument with the result of this application. We do this using the notion of reduction

$$\beta = \Big\{\big((\lambda x.M)N, M[x := N]\big) \,\Big|\, x \in \mathit{Vars} \text{ and } M, N \in \Lambda\Big\}.$$

That is, the one-step reduction $\rightarrow_\beta$ replaces every free occurrence of x in M with the argument N. Notice that by definition of substitution, it may happen that we rename bound variables in M when applying $\lambda x.M$ to N. Hence it makes little sense to consider β-equivalence without also identifying terms that are α-equivalent. We thus arrive at the usual notion of equivalence between λ-terms, namely $\alpha\beta$-equivalence (recalling that we write $\alpha\beta = \alpha \cup \beta$). Instead of '$=_{\alpha\beta}$' for the resulting equivalence relation, we simply write '$=$'.

Not only is β-reduction a natural notion of reduction, it is also very well-behaved. The following theorem is fairly nontrivial, so we omit the proof:

9.13 • Theorem. *β is Church–Rosser.* ■

(a) If we consider α-equivalence as a way of identifying different terms, then this induces a notion of equality on terms that is ***intensional***. That is, two terms are α-equivalent if they somehow mean the same. This is intuitive enough, since all α-equivalence does is allow us to rename bound variables.

But notice that there are terms that are not α-equivalent, but that we usually would identify anyway. If the variable x is not free in the term M, then we would usually identify $\lambda x.Mx$ and M: For the former is just the function that applies M to its argument. Despite this, since we cannot obtain one by renaming bound variables in the other, they are not α-equivalent. If we wish to identify terms not solely by their intension but also by their ***extension***, i.e. the values that they take on different arguments, then we add the relation

$$\eta = \{(\lambda x.Mx, M) \mid M \in \Lambda, x \in \mathit{Vars} \setminus FV(M)\}$$

and consider instead $\alpha\beta\eta$-equivalence. But this is not usually done.

2 Foundations

2.1 ⋄ Absolute Values on a Field

Problem 31. Let $\mathbb{K}$ be a finite field. Show that the only absolute value on $\mathbb{K}$ is the trivial absolute value

Solution. Let $x \in \mathbb{K} \setminus \{0,1\}$. Then $x^n = 1$ for some $n \in \mathbb{Z}$, so $1 = |x^n| = |x|^n$. But then $|x| = 1$. ■

Problem 36. Let A be an integral domain, and let K be its field of fractions. Let $v\colon A \setminus \{0\} \to \mathbb{R}$ be a valuation on A. Extend v to $K \setminus \{0\}$ by setting $v(a/b) = v(a) - v(b)$. Show that the function $|\cdot|_v\colon K \to \mathbb{R}^+$ defined by

$$|x|_v = \mathrm{e}^{-v(x)} \quad \text{for } x \neq 0$$

and $|0|_v = 0$ is a non-archimedean absolute value on K. Conversely, show that if $|\cdot|$ is a non-archimedean absolute value, then $-\log|\cdot|$ is a valuation.

Solution. Most of this is obvious. We show that the extension of v to $K \setminus \{0\}$ is well-defined. If $a/b = c/d$ then $ad = bc$, and so

$$v(a) + v(d) = v(ad) = v(bc) = v(b) + v(c),$$

which implies that $v(a) - v(b) = v(c) - v(d)$. ■

Problem 37. Let $v\colon \mathbb{K}^* \to \mathbb{R}$ be a valuation. Show that the image of v is an additive subgroup of $\mathbb{R}$. This is sometimes called the ***value group*** of the valuation v. What is the value group of the p-adic valuation?

Solution. Since $v(xy) = v(x) + v(y)$ for all $x, y \in \mathbb{K}^*$, v is a group homomorphism from the multiplicative group $\mathbb{K}^*$ to the additive group $(\mathbb{R}, +)$. Hence its image is an additive subgroup of $\mathbb{R}$.

For the p-adic valuation v_p, $v_p(\mathbb{Z} \setminus \{0\}) = \mathbb{N}_0$, so $v_p(\mathbb{Q}^*) = \mathbb{Z}$. ■

Problem 49. Show that if $C = \sup\{|n| \mid n \in \mathbb{Z}\} < \infty$, then $|\cdot|$ is non-archimedean, and $C = 1$.

Solution. We have $|1| = 1$, so $C \geq 1$. If there is some $n \in \mathbb{Z}$ with $|n| > 1$, then the powers of n are unbounded. Hence we must have $|n| \leq 1$. That $|\cdot|$ is non-archimedean follows from Theorem 2.2.4. ■

2.3 ◇ Topology

Problem 56. Describe the closed ball of radius 1 around the point $x = 0$ in $\mathbb{Q}$ with respect to the p-adic absolute value. Describe the open ball of radius 1 around $x = 3$; which integers belong to this ball?

Solution. We have $y \in \overline{B}(0,1)$ if and only if $p^{-v_p(y)} = |y|_p \leq 1$. This is the case just when $v_p(y) \geq 0$, i.e. when $y = m/n$ (with m and n coprime) and $p \nmid n$. For instance, $\overline{B}(0,1)$ contains all the integers.

Similarly, we have $y \in B(3,1)$ if and only if $v_p(y-3) > 1$, i.e. when $y-3 = m/n$ (with m and n coprime) and $p \mid m$ and $p \nmid n$. For instance, an integer k lies in $B(3,1)$ just when $p \mid k-3$, i.e. when $k \equiv_p 3$. ■

Problem 57. Let $\mathbb{K} = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Show that the closed ball $\overline{B}(0,1)$ can be written as a disjoint union of open balls

$$\overline{B}(0,1) = B(0,1) \cup B(1,1) \cup \cdots \cup B(p-1,1).$$

Solution. To show that the open balls are disjoint, it suffices by Proposition 2.3.7 to show that each ball has points not contained in the others. So let $k' \in \{0,1,\ldots,p-1\}$. Then $k' \in B(k,1)$ just when $p \mid k-k'$. But then we must have $k = k'$.

As in Problem 56, $\overline{B}(0,1)$ is the set of rationals m/n with $p \nmid n$. The numbers $0, n, 2n, \ldots, (p-1)n$ lie in distinct p-residue classes, so there exists a $k \in \{0,1,\ldots,p-1\}$ such that $p \mid m-kn$. It follows that $m/n - k = (m-kn)/n \in B(0,1)$, so $m/n \in B(k,1)$. ■

Problem 62. Show that in a field with a (non-trivial) non-archimedean absolute value every closed ball with radius $r > 0$ is disconnected. Is the same true for open balls?

Solution. First a lemma:

> *If $|\cdot|$ is a nontrivial absolute value on $\mathbb{K}$, then for every $\varepsilon > 0$ there is an $x \in \mathbb{K}$ such that $|x| < \varepsilon$.*

Let $y \in \mathbb{K}$ be such that $|y| < 1$ (if $|y| > 1$, then replace y with $1/y$). Then $|y^n| = |y|^n \to 0$ as $n \to \infty$, proving the claim.

Next, since the metric on $\mathbb{K}$ is invariant, this implies that for every $y \in \mathbb{K}$ there is an $x \in \mathbb{K} \setminus \{y\}$ with $|x-y| < \varepsilon$. In particular, every open ball contains infinitely many points.

Now let B be a (closed or open) ball with radius $r > 0$, centered at x, and let $y \in B \setminus \{x\}$. Let $s = |x-y| \leq r$, and consider the open ball $B(x,s)$. This is both open and closed by Proposition 2.3.7(iii) (here we use that the absolute value is non-archimedean), and it is a proper subset of B. Then $B(x,s)$ and $B(x,s)^c$ disconnect B. ■

Problem 63. Show that if a set in a field with a non-archimedean absolute value contains two distinct points then it is disconnected.

Solution. Let the set A contain distinct points x and y, and let $r = |x-y| > 0$. The open ball $B(x,r)$ contains x but not y, and it is both open and closed by Proposition 2.3.7(iii). Hence it and $B(x,r)^c$ disconnect A. ■

2.4 ⋄ Algebra

Problem 67. Prove that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$.

Solution. Consider the composition $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)} \twoheadrightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, and notice that its kernel is $\mathbb{Z} \cap p\mathbb{Z}_{(p)} = p\mathbb{Z}$. The first isomorphism theorem thus implies the claim. ■

Problem 69. Consider $\mathbb{Q}$ with a p-adic absolute value, and let $a \in \mathbb{Z}$. Describe the open ball $B(a,1)$ in terms of the algebraic structure. Use your description to interpret algebraically the fact (Problem 57) that the closed ball $\bar{B}(0,1)$ is the disjoint union of finitely many open balls of radius 1.

Solution. Recall that $\bar{B}(0,1) = \mathbb{Z}_{(p)}$, and that $B(0,1) = p\mathbb{Z}_{(p)}$. Next notice that since the metric in $\mathbb{Q}$ is invariant, we have $B(x,1) = x + B(0,1)$ for all $x \in \mathbb{Q}$. And the additive group $\mathbb{Z}_{(p)}$ is a union of its $p\mathbb{Z}_{(p)}$-cosets, which by Problem 67 are represented by the integers $0, 1, \dots, p-1$. Hence

$$\mathbb{Z}_{(p)} = \bigcup_{k=0}^{p-1} \left(k + p\mathbb{Z}_{(p)}\right).$$

Rewriting this in terms of balls we get the statement in Problem 57. ■

Problem 71. Let $\mathbb{K}$ be a field, and let $|\cdot|$ be a non-archimedean absolute value on $\mathbb{K}$. Define a valuation v on $\mathbb{K}$ by $v(x) = -\log|x|$ for $x \neq 0$ and $v(0) = \infty$.

(1) If $|\cdot|$ is the p-adic absolute value, how does v relate to the p-adic valuation v_p? What is the image of v in this case?

(2) Show that the valuation ideal of $|\cdot|$ is a principal ideal if and only if the image of v is a discrete additive subgroup of $\mathbb{R}$.

(3) Show that if the image of v is a discrete subgroup of $\mathbb{R}$ then the valuation ring $\mathcal{O}$ is a principal ideal domain whose only prime ideals are 0 and $\mathfrak{P}$. (For example, check that this happens for the p-adic absolute values.)

Solution. (i) We have

$$v(x) = -\log|x|_p = -\log p^{-v_p(x)} = v_p(x)\log p.$$

In particular, $v(\mathbb{Q}^*) = v_p(\mathbb{Q}^*)\log p = \mathbb{Z}\log p$.

(ii) Assume that $\mathfrak{P}$ is principal, e.g. generated by x. Then $x \in \mathfrak{P}$, so $|x| < 1$. Since every element in $\mathfrak{P}$ is on the form xy for some $y \in \mathcal{O}$, we have $|xy| = |x||y| \leq |x|$. Hence there do not exist elements in $\mathfrak{P}$ whose absolute value come arbitrarily close to 1. This implies that there do not exist elements in $\mathfrak{P}$ whose valuation come arbitrarily close to 0. In other words, $v(\mathfrak{P})$ does not have 0 as a limit point. Next notice that $\mathbb{K} \setminus \mathcal{O}$ also does not contain elements whose absolute value come arbitrarily close to 1, since then $\mathfrak{P}$ would also contain such elements (by taking the reciprocal). Of course, elements in $\mathcal{O} \setminus \mathfrak{P}$ are mapped by v to 0. This shows that $\operatorname{im} v$ is discrete.

Conversely, assume that the value group is discrete, and let $x \in \mathfrak{P}$ be an element such that $v(x)$ is minimal and positive. Then $|x|$ is maximal among elements in $\mathfrak{P}$. Thus if $y \in \mathfrak{P}$, then $|y/x| \leq 1$, and so $y/x \in \mathcal{O}$. But $x(y/x) = y$, so x generates $\mathfrak{P}$.

(iii) TODO ■

3 The p-Adic Numbers

3.1 ⋄ Absolute Values on $\mathbb{Q}$

Problem 76. Show that if p and q are two different primes, the p-adic and the q-adic absolute values are not equivalent.

Solution. Notice that $|p|_p = 1/p$ and $|q|_q = 1/q$, but $|q|_p = |p|_q = 1$. So there is no number α as in Proposition 3.1.3(iv). ∎

Problem 77. Show that in general a non-archimedean absolute value cannot be equivalent to an archimedean absolute value.

Solution. Let $|\cdot|_1$ be non-archimedean, and let $|\cdot|_2$ be equivalent to $|\cdot|_1$. Let α be as in Proposition 3.1.3(iv). For any x, y we then have

$$|x+y|_2^\alpha = |x+y|_1 \leq |x|_1 \vee |y|_1 = |x|_2^\alpha \vee |y|_2^\alpha = \big(|x|_2 \vee |y|_2\big)^\alpha.$$

Taking the αth root shows that $|\cdot|_2$ is also non-archimedean. ∎

3.2 ⋄ Completions

Step 1: Embedding a metric space as a dense subset of a complete pseudometric space.

Let (S,ρ) be a metric space. We first consider the set $\mathcal{C}_S$ of Cauchy sequences in S. For $x = (x_n)$ and $y = (y_n)$ in $\mathcal{C}_S$ we define

$$\rho_\mathcal{C}(x,y) = \lim_{n\to\infty} \rho(x_n, y_n).$$

This limit exists since $(\rho(x_n,y_n))$ is a Cauchy sequence and $\mathbb{R}$ is complete.[1] One easily show that $\rho_\mathcal{C}$ is a pseudometric on $\mathcal{C}_S$.

For completeness, let $(x^n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathcal{C}_S$, and write $x^n = (x^n_k)_{k\in\mathbb{N}}$. Now let $N_1 = 1$, and assume that we have chosen a sequence of strictly increasing integers $N_1, \dots, N_{k-1}$ such that for all $i \in \{1, \dots, k-1\}$ and for $m, n \geq N_i$ we have $\rho(x^i_m, x^i_n) < 1/i$. Since x^k is a Cauchy sequence in S, there is

[1] Notice that since we assume completeness of $\mathbb{R}$, we cannot use this procedure to construct $\mathbb{R}$. But this is not an issue, since we wouldn't even be able to *define* either absolute values or metrics without the existence of $\mathbb{R}$. And from the existence of $\mathbb{R}$ we of course also get completeness.

a $N_k \in \mathbb{N}$ such that $\rho(x^k_m, x^k_n) < 1/k$ when $m,n \geq N_k$. Choose this integer such that furthermore $N_k > N_{k-1}$. This yields a sequence $(N_k)_{k\in\mathbb{N}}$ with the above property.

Now define a sequence $y = (y_n)_{n\in\mathbb{N}}$ by $y_n = x^n_{N_n}$. We claim that this is a Cauchy sequence in S, such that it lies in $\mathcal{C}_S$. Notice that for any $k \in \mathbb{N}$ we have

$$\rho(y_m, y_n) = \rho(x^m_{N_m}, x^n_{N_n}) \leq \rho(x^m_{N_m}, x^m_k) + \rho(x^m_k, x^n_k) + \rho(x^m_k, x^n_{N_n}).$$

Let $\varepsilon > 0$. Since (x^n) is a Cauchy sequence, for large enough m and n we have $\rho_{\mathcal{C}}(x^m, x_n) < \varepsilon$. In particular, the middle term above eventually becomes less than ε as $k \to \infty$. Taking the lim sup as $k \to \infty$ we thus get

$$\rho(y_m, y_n) \leq \tfrac{1}{m} + \varepsilon + \tfrac{1}{n}.$$

Given any ε we can find large enough m and n such that this holds, so y is a Cauchy sequence.

We next show that $x^n \to y$ in $\mathcal{C}_S$. Let $\varepsilon > 0$ and notice that

$$\rho_{\mathcal{C}}(x^n, y) = \lim_{k\to\infty} \rho(x^n_k, y_k) \leq \limsup_{k\to\infty} \rho(x^n_k, x^n_{N_n}) + \limsup_{k\to\infty} \rho(y_n, y_k),$$

since $y_n = x^n_{N_n}$. Since y is a Cauchy sequence, there exists a $N \in \mathbb{N}$ such that $\rho(y_m, y_n) < \varepsilon$ when $m,n \geq N$. Also choose N such that $1/N < \varepsilon$. By definition of N_n, we get for $n \geq N$ that

$$\rho_{\mathcal{C}}(x^n, y) \leq \tfrac{1}{n} + \varepsilon \leq \tfrac{1}{N} + \varepsilon \leq 2\varepsilon.$$

Hence $x^n \to y$.

Finally notice that the map $\iota\colon S \to \mathcal{C}_S$ that sends an element $x \in S$ to the constant sequence $(x, x, \ldots)$ is an isometry, hence is injective. We claim that $\iota(S)$ is dense in $\mathcal{C}_S$. If $y = (y_k)_{k\in\mathbb{N}}$ is an element of $\mathcal{C}_S$, i.e. a Cauchy sequence in S, then we have

$$\rho_{\mathcal{C}}(\iota(y_n), y) = \lim_{k\to\infty} \rho(y_n, y_k).$$

Since y is a Cauchy sequence, choosing n large enough the above can become arbitrarily small. Hence $\iota(y_n) \to y$.

Step 2: The metric identification of a complete space is complete.

Next let (S, ρ) be a complete pseudometric space. We quotient out by the ***metric identification*** $\sim$, i.e. the equivalence relation on S given by $x \sim y$ if $\rho(x,y) = 0$. Then define a metric $\tilde{\rho}$ on $\tilde{S} = S/$ by $\tilde{\rho}([x],[y]) = \rho(x,y)$. It is easy to show that this is well-defined. Hence the quotient map $q\colon S \to \tilde{S}$ given by $x \mapsto [x]$ is an isometry. Now let $(\tilde{x}_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\tilde{S}$, and choose for each equivalence class $\tilde{x}_n$ a representative x_n. Then (x_n) is a Cauchy sequence in S and hence converges to some $x \in S$. It follows that

$$\tilde{\rho}(\tilde{x}_n, [x]) = \rho(x_n, x) \to 0,$$

as $n \to \infty$. Hence $\tilde{S}$ is also complete.

We note for future reference that the metric identification coincides with the T_0-identification, which in particular implies that the quotient map q is closed.

Step 3: Dense embedding of metric space in completion.

Let (S,ρ) be a metric space, let $\mathcal{C}_S$ be its space of Cauchy sequences, and denote by $(\overline{S},\overline{\rho})$ the metric identification of $\mathcal{C}_S$. Step 1 shows that the image $\iota(S)$ is dense in $\mathcal{C}_S$. And since the quotient map q is continuous and closed, we have

$$\overline{S} = q(\mathcal{C}_S) = q\Big(\overline{\iota(S)}\Big) = \overline{(q \circ \iota)(S)}.$$

Next, it is clear that $q \circ \iota$ is injective, since q only identifies elements if the distance between them is 0, and S is a metric space. Hence $q \circ \iota$ embeds S as a dense subset of a complete metric space.

Step 4: Completion of fields.

Let $\mathbb{K}$ be a field equipped with an absolute value $|\cdot|$. Notice that the space $\mathcal{C}_{\mathbb{K}}$ of Cauchy sequences has a natural ring structure, where addition and multiplication are defined elementwise. This makes $\mathcal{C}_{\mathbb{K}}$ into a commutative ring with identity, and the subring $\iota(\mathbb{K})$ is a field. Furthermore, notice that since the metric $\rho(x,y) = |x-y|$ on $\mathbb{K}$ is invariant, so is the metric $\rho_{\mathcal{C}}$.

The absolute value on $\mathbb{K}$ of course induces an absolute value on $\iota(\mathbb{K})$, and we may extend this to a map on $\mathcal{C}_{\mathbb{K}}$ as follows: If $x = (x_n)$ is an element of $\mathcal{C}_{\mathbb{F}}$, define

$$|x| = \lim_{n\to\infty} |x_n|.$$

This is well-defined since $(|x_n|)$ is a Cauchy sequence in $\mathbb{R}$ (by the inverse triangle inequality), hence is convergent. Notice that we also have

$$\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} \rho(x_n, 0) = \rho_{\mathcal{C}}(x, \iota(0)),$$

so $|x| = \rho_{\mathcal{C}}(x,\iota(0))$, and in particular

$$\rho_{\mathcal{C}}(x,y) = \rho_{\mathcal{C}}(x-y,\iota(0)) = |x-y|,$$

for $y \in \mathcal{C}_{\mathbb{K}}$. Next, the map $|\cdot|$ on $\mathcal{C}_{\mathbb{K}}$ inherits many of the properties of the absolute value on $\mathbb{K}$. For instance,

$$|xy| = \lim_{n\to\infty} |x_n y_n| = \lim_{n\to\infty} |x_n||y_n| = \lim_{n\to\infty} |x_n| \lim_{n\to\infty} |y_n| = |x||y|.$$

We also get the triangle inequality by a similar calculation. If the absolute value on $\mathbb{K}$ is non-archimedean, we also get

$$|x+y| = \lim_{n\to\infty} |x_n + y_n| \leq \limsup_{n\to\infty} \Big(|x_n| \vee |y_n|\Big) \leq \limsup_{n\to\infty} |x_n| \vee \limsup_{n\to\infty} |y_n| = |x| \vee |y|.$$

In particular, the ring operations are continuous. Hence the additive group $(\mathcal{C}_{\mathbb{K}}, +)$ is in particular a topological group.

Now recall that the metric identification which constructs $\overline{\mathbb{F}}$ from $\mathcal{C}_{\mathbb{K}}$ coincides with the T_0-identification. Furthermore, the T_0-identification on a topological group is also given by its quotient by the normal subgroup $\overline{\{e\}}$, where e is the identity. Let $\mathcal{N}$ denote the corresponding subgroup of $\mathcal{C}_{\mathbb{K}}$ so that $\overline{\mathbb{F}} = \mathcal{C}_{\mathbb{F}}/\mathcal{N}$, which makes $\overline{\mathbb{F}}$ into a group. In fact it is a ring, since $\mathcal{N}$ is an ideal: Notice that $\mathcal{N}$ is precisely the set of elements x with $|x| = 0$. Hence if $y \in \mathcal{C}_{\mathbb{K}}$, then

$$|xy| = |x||y| = 0,$$

so $xy \in \mathcal{N}$. Thus $\overline{\mathbb{F}}$ is a ring. Furthermore, the map $|\cdot|$ on $\mathcal{C}_{\mathbb{K}}$ descends to $\overline{\mathbb{K}}$ by letting $|[x]| = |x|$. The triangle inequality on $\mathcal{C}_{\mathbb{K}}$ implies that this is well-defined. Thus the map $|\cdot|$ on $\overline{\mathbb{K}}$ inherits all the relevant properties of the same map on $\mathcal{C}_{\mathbb{K}}$. Furthermore, we have

$$\overline{\rho}([x],[y]) = \rho(x,y) = |x-y| = \big|[x]-[y]\big|,$$

as expected. It follows that the ring operations on $\overline{\mathbb{F}}$ are continuous.

Finally we may show that $\mathcal{N}$ is a maximal ideal, making $\overline{\mathbb{F}}$ into a field: Let $x = (x_n) \in \mathcal{C}_{\mathbb{K}} \setminus \mathcal{N}$ so that $|x| > 0$, and denote by $\mathcal{I}$ the ideal generated by x and $\mathcal{N}$. There exist $R > 0$ and $N \in \mathbb{N}$ such that $|x_n| \geq R > 0$ when $n \geq N$. Now define a sequence $y = (y_n)$ by

$$y_n = \begin{cases} 0, & n < N, \\ \frac{1}{x_n}, & n \geq N. \end{cases}$$

For $m, n \geq N$ we thus have

$$|y_m - y_n| = \left|\frac{1}{x_m} - \frac{1}{x_n}\right| = \frac{|x_m - x_n|}{|x_m x_n|} \leq \frac{|x_m - x_n|}{R^2}.$$

Hence y is a Cauchy sequence since x is. Now notice that xy is eventually constant and equal to 1. But then $\iota(1) - xy \in \mathcal{N}$, so $\iota(1) \in \mathcal{I}$, and it follows that $\mathcal{I} = \mathcal{C}_{\mathbb{K}}$. Thus $\mathcal{N}$ is maximal.

4 Exploring $\mathbb{Q}_p$

4.2 ⋄ p-adic Integers

Problem 100. Show that the sets $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}$ form a fundamental system of neighborhoods of $0 \in \mathbb{Q}_p$ which covers all of $\mathbb{Q}_p$.

Solution. Recall that $\mathbb{Z}_p = \overline{B}(0,1)$ is open, so that $p^n\mathbb{Z}_p = \overline{B}(0,p^{-n})$ is also open. This is clearly a neighbourhood basis at 0 (since p^{-n} can become arbitrarily small), and it clearly covers $\mathbb{Q}_p$ (since p^{-n} can become arbitrarily large). For the last point we could also have used the first part of Corollary 4.2.4, but this is not necessary. ■

TODO 102

Problem 103. For any $n \geq 1$, show that there is a homomorphism $\varphi_n \colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ such that the sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_p \arrow[r, "p^n"] & \mathbb{Z}_p \arrow[r, "\varphi_n"] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

of abelian groups is exact, and that the maps are continuous when $\mathbb{Z}/p^n\mathbb{Z}$ is equipped with the discrete topology.

Solution. Note that this must be a sequence of groups and not of rings, since the map $x \mapsto p^n x$ is not a ring homomorphism.

We construct the map φ_n as follows: Given $x \in \mathbb{Z}_p$, Proposition 4.2.2(ii) furnishes a unique $\alpha \in \mathbb{Z}$ such that $0 \leq \alpha < p^n$ and $|x-\alpha|_p \leq p^{-n}$. We let $\varphi_n(x) = [\alpha]$, which is well-defined by uniqueness of α. We next show that this is a group homomorphism. If $y \in \mathbb{Z}_p$ and $\beta \in \mathbb{Z}$ with $0 \leq \beta < p^n$ and $\varphi_n(y) = [\beta]$, then choose $\gamma \in \mathbb{Z}$ with $0 \leq \gamma < p^n$ and $\gamma \equiv_{p^n} \alpha + \beta$. Then we have

$$\begin{aligned} |x+y-\gamma|_p &\leq |x+y-(\alpha+\beta)|_p \vee |\alpha+\beta-\gamma|_p \\ &\leq |x-\alpha|_p \vee |y-\beta| \vee |\alpha+\beta-\gamma|_p \\ &\leq p^{-n}. \end{aligned}$$

Here we have used the definitions of α and β, and the fact that $|\alpha+\beta-\gamma|_p \leq p^{-n}$ since $\gamma \equiv_{p^n} \alpha+\beta$. By the uniqueness part of Proposition 4.2.2(ii) we have

$$\varphi_n(x+y) = [\gamma] = [\alpha+\beta] = [\alpha]+[\beta] = \varphi_n(x)+\varphi_n(y),$$

so φ_n is a group homomorphism.

Furthermore, $x \in \ker\varphi_n$ if and only if $\alpha = 0$, which is the case just when $|x|_p \leq p^{-n}$. But $\overline{B}(0, p^{-n}) = p^n\mathbb{Z}_p$, so $\ker\varphi_n = p^n\mathbb{Z}_p$. This is clearly also the image of the map $x \mapsto p^n x$. Next, $x \mapsto p^n x$ is clearly injective (since its codomain lies in a field where we can perform division), and φ_n is clearly surjective, so the sequence is exact.

Finally, to show that φ_n is continuous, notice that the preimage under φ_n of $[\alpha]$ with $0 \leq \alpha < p^n$ are all the $x \in \mathbb{Z}_p$ with $|x - \alpha|_p \leq p^{-n}$. That is, the preimage is the closed ball $\overline{B}(\alpha, p^{-n})$, which is an open set.

The first isomorphism theorem then implies that $\mathbb{Z}_p/p^n\mathbb{Z}_p$ and $\mathbb{Z}/p^n\mathbb{Z}$ are isomorphic as groups. However, they are in fact isomorphic as rings, since φ_n is a ring homomorphism: Clearly $\varphi_n(1) = [1]$. Next, define γ as above, except that $\gamma \equiv_{p^n} \alpha\beta$, and show that $|xy - \gamma|_p \leq p^{-n}$. In this calculation we use that

$$\begin{aligned} |xy - \alpha\beta|_p &= |(xy - x\beta) + (x\beta - \alpha\beta)|_p \\ &\leq |x|_p\,|y - \beta|_p \vee |x - \alpha|_p\,|\beta|_p \\ &\leq p^{-n}. \end{aligned}$$

Here we use the fact that $x, \beta \in \mathbb{Z}_p$, so $|x|_p, |\beta|_p \leq 1$. This shows that $\varphi_n(xy) = [\gamma] = [\alpha][\beta] = \varphi_n(x)\varphi_n(y)$. ■

PROBLEM 106. If $\mathbb{K}$ is a field with an absolute value, show that $\mathbb{K}$ is locally compact if and only if there exists a neighborhood of zero that is compact.

Solution. This is obvious since the topology on $\mathbb{K}$ is homogeneous. ■

PROBLEM 108. Let $\mathbb{K}$ be a field, $|\cdot|$ a non-archimedean absolute value on $\mathbb{K}$, $\mathcal{O} \subseteq \mathbb{K}$ the valuation ring, and $\mathfrak{P}$ the valuation ideal. Suppose that $\mathbb{K}$ is complete and that $\mathfrak{P}$ is principal. Show that $\mathbb{K}$ is locally compact if and only if the residue field $\mathcal{O}/\mathfrak{P}$ is finite.

Solution. First assume that $\mathbb{K}$ is locally compact. Then $\mathcal{O}$ is compact, but this is covered by its $\mathfrak{P}$-cosets which are open, so finitely many of them cover $\mathcal{O}$. But the cosets are also disjoint, so there must be finitely many of them.

Conversely assume that $\mathcal{O}/\mathfrak{P}$ is finite. We then show that $\mathcal{O}/\mathfrak{P}^n$ is also finite for all $n \in \mathbb{N}$, where $\mathfrak{P}^n$ is the n-fold product of $\mathfrak{P}$ with itself. We prove this by induction. The case $n = 1$ is true by assumption, so assume that $n > 1$ and that $\mathcal{O}/\mathfrak{P}^{n-1}$ is finite. Since $\mathfrak{P}^n \subseteq \mathfrak{P}$ there is a natural map $\mathcal{O}/\mathfrak{P}^n \to \mathcal{O}/\mathfrak{P}$ whose kernel is $\mathfrak{P}/\mathfrak{P}^n$. We prove that this is finite. To this end, let $x \in \mathfrak{P}$ be a generator of $\mathfrak{P}$, so that it is on the form $x\mathcal{O}$. Then $\mathfrak{P}^n = x^n\mathcal{O}$. Consider the group homomorphism

$$\mathcal{O} \to \frac{x\mathcal{O}}{x^n\mathcal{O}}$$

given by $y \mapsto xy + x^n\mathcal{O}$. The kernel of this homomorphism consists precisely of those $y \in \mathcal{O}$ that are on the form $x^{n-1}z$ for some $z \in \mathcal{O}$, i.e. $x^{n-1}\mathcal{O}$. Thus we have

$$\frac{\mathcal{O}}{\mathfrak{P}^{n-1}} = \frac{\mathcal{O}}{x^{n-1}\mathcal{O}} \cong \frac{x\mathcal{O}}{x^n\mathcal{O}} = \frac{\mathfrak{P}}{\mathfrak{P}^n}$$

But $\mathcal{O}/\mathfrak{P}^{n-1}$ is finite by induction, so $\mathfrak{P}/\mathfrak{P}^n$ is finite. It thus follows that

$$[\mathcal{O} : \mathfrak{P}^n] = [\mathcal{O} : \mathfrak{P}][\mathfrak{P} : \mathfrak{P}^n] < \infty.$$

Hence $\mathcal{O}$ is the union of finitely many translates of the ball $\mathfrak{P}^n = B(0, |x|^n)$, and these can become arbitrarily small since $x \in \mathfrak{P}$, so $|x| < 1$. Thus $\mathcal{O}$ is compact, and hence $\mathbb{K}$ is locally compact. ■

4.3 ⋄ The elements of $\mathbb{Q}_p$

Problem 112. Prove that the inclusion

$$\varphi \colon \mathbb{Z}_p \hookrightarrow \prod_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

is an embedding.

Solution. Notice that each factor φ_n of φ is continuous by Problem 103, so φ is also continuous. It is injective, so for it to be an embedding it suffices that it is open or closed. But $\mathbb{Z}_p$ is compact and the product is Hausdorff (since each factor is), so φ is closed. ■

TODO 113

5 Elementary Analysis In $\mathbb{Q}_p$

5.1 ◇ Sequences and Series

Problem 142. Let (a_n) be a convergent sequence in $\mathbb{Q}_p$. Show that either $\lim_{n\to\infty}|a_n| = 0$ or there exists an integer M such that $|a_n|_p = |a_M|_p$ for every $n \geq M$.

Solution. Recall that the image of $\mathbb{Q}_p$ under $|\cdot|_p$ is $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$, and 0 is the only limit point of this set. Furthermore, since (a_n) is convergent so is $(|a_n|_p)$, and the first sequence converges to $0 \in \mathbb{Q}_p$ if and only if the second converges to $0 \in \mathbb{R}$. And if the second does not converge to 0, then since $\{p^n \mid n \in \mathbb{Z}\}$ is discrete it must be eventually constant. ■

Problem 143. Show that absolute convergence implies convergence in $\mathbb{Q}_p$.

Solution. Let $\sum_{n=1}^{\infty} a_n$ be a series with terms in $\mathbb{Q}_p$ such that the series $\sum_{n=1}^{\infty}|a_n|_p$ converges in $\mathbb{R}$. Letting $s_n = \sum_{i=1}^{n} a_i$ we get, for $m \leq n$, that

$$|s_n - s_m|_p = \left|\sum_{i=m+1}^{n} a_i\right|_p \leq \sum_{i=m+1}^{n} |a_i|_p \xrightarrow[m,n\to\infty]{} 0.$$

So (s_n) is a Cauchy sequence, hence convergent.

Notice that this proof is precisely the same as the proof for series with terms in $\mathbb{R}$. That is, the strong triangle inequality is not necessary. ■

TODO (149) 150

5.2 ◇ Functions, Continuity, Derivatives

Problem 153. xx

Solution. xx ■

5.4 ◇ Power Series

TODO (156)

5.5 ◇ Functions Defined by Power Series

TODO 163

6 Vector Spaces and Field Extensions

6.1 ◇ Normed Vector Spaces over Complete Valued Fields

Problem 212. Show that two norms on V are equivalent if and only if they define the same topology on V.

Solution. It is clear that equivalent norms induce the same topology. Conversely, let $\|\cdot\|_1$ and $\|\cdot\|_2$ be norms on V that induce the same topology. Hence the identity function $\mathrm{id}_V : (V, \|\cdot\|_1) \to (V, \|\cdot\|_2)$ is continuous and hence bounded (by Problem 217). It follows that $\|v\|_2 \leq K\|v\|_1$ for all $v \in V$ for some $K > 0$. By symmetry the other inequality also holds. ■

Cohn exercises

Problem 1.1.7. Let $\mathcal{S}$ be a collection of subsets of the set X. Show that for each A in $\sigma(\mathcal{S})$, there is a countable subfamily $\mathcal{C}_A$ of $\mathcal{S}$ such that $A \in \sigma(\mathcal{C}_A)$.

Solution. Let $\mathcal{A}$ be the union the σ-algebras $\sigma(\mathcal{C})$, where $\mathcal{C}$ ranges over the countable subfamilies of $\mathcal{S}$. Then $\mathcal{S} \subseteq \mathcal{A} \subseteq \sigma(\mathcal{S})$, and $\mathcal{A}$ is a σ-algebra, so in fact $\mathcal{A} = \sigma(\mathcal{S})$. The only thing that is not obvious is that $\mathcal{A}$ is closed under countable unions. But if $(A_n)_{n\in\mathbb{N}}$ is a sequence in $\mathcal{A}$, then $A_n \in \sigma(\mathcal{C}_n)$ for some countable $\mathcal{C}_n$, and so

$$\bigcup_{n\in\mathbb{N}} A_n \in \bigcup_{n\in\mathbb{N}} \sigma(\mathcal{C}_n) \subseteq \sigma\left(\bigcup_{n\in\mathbb{N}} \mathcal{C}_n \right) \subseteq \mathcal{A},$$

since the collection $\bigcup_{n\in\mathbb{N}} \mathcal{C}_n$ is a countable subfamily of $\mathcal{S}$.

If $A \in \sigma(\mathcal{S}) = \mathcal{A}$, then there is a $\mathcal{C}_A$ such that $A \in \sigma(\mathcal{C}_A)$, as desired. ■

Problem 1.2.6. Let $(X, \mathcal{A})$ be a measurable space.

(1) Show that if (μ_n) is an increasing sequence of measures on $(X, \mathcal{A})$, then the formula $\mu(A) = \lim_{n\to\infty} \mu_n(A)$ defines a measure on $(X, \mathcal{A})$.

(2) Show that if (μ_n) is an arbitrary sequence of measures on $(X, \mathcal{A})$, then the formula $\mu(A) = \sum_{n=1}^{\infty} \mu_n(A)$ defines a measure on $(X, \mathcal{A})$.

Solution. (a) Clearly $\mu(\emptyset) = 0$, so let (A_j) be a sequence of disjoint sets from $\mathcal{A}$. Then

$$\mu\Big(\bigcup_{j\in\mathbb{N}} A_j\Big) = \lim_{n\to\infty} \mu_n\Big(\bigcup_{j\in\mathbb{N}} A_j\Big) = \lim_{n\to\infty}\lim_{m\to\infty}\sum_{j=1}^{m} \mu_n(A_j).$$

Notice that if $(a_{mn})_{(m,n)\in\mathbb{N}\times\mathbb{N}}$ is any collection of real numbers, then

$$\sup_{m\in\mathbb{N}}\sup_{n\in\mathbb{N}} a_{mn} \le \sup_{m,n\in\mathbb{N}} a_{mn}.$$

The opposite inequality is obvious if the left-hand side is infinite, so assume that it is finite and let $\varepsilon > 0$. Then there are $m, n \in \mathbb{N}$ such that

$$\sup_{m,n\in\mathbb{N}} a_{mn} - \varepsilon \le a_{mn} \le \sup_{m\in\mathbb{N}}\sup_{n\in\mathbb{N}} a_{mn}.$$

Since ε was arbitrary, this implies that

$$\sup_{m\in\mathbb{N}}\sup_{n\in\mathbb{N}} a_{mn} = \sup_{m,n\in\mathbb{N}} a_{mn} = \sup_{n\in\mathbb{N}}\sup_{m\in\mathbb{N}} a_{mn}.$$

Letting $a_{mn} = \sum_{j=1}^{m} \mu_n(A_j)$, the double sequence (a_{mn}) is increasing in the product ordering on $\mathbb{N}\times\mathbb{N}$ (i.e., increasing in m and n separately), so exchanging limits for suprema we get

$$\begin{aligned}\mu\Big(\bigcup_{j\in\mathbb{N}} A_j\Big) &= \sup_{n\in\mathbb{N}}\sup_{m\in\mathbb{N}}\sum_{j=1}^{m} \mu_n(A_j) = \sup_{m\in\mathbb{N}}\sup_{n\in\mathbb{N}}\sum_{j=1}^{m} \mu_n(A_j)\\ &= \lim_{m\to\infty}\sum_{j=1}^{m}\lim_{n\to\infty} \mu_n(A_j) = \sum_{j=1}^{\infty} \mu(A_j).\end{aligned}$$

(b) Use part (a) on the increasing sequence of partial sums.

Problem 1.5.1. Let $(X, \mathcal{A}, \mu)$ be a measure space. Show that $(\mathcal{A}_\mu)_{\overline{\mu}} = \mathcal{A}_\mu$ and $\overline{\overline{\mu}} = \overline{\mu}$.

Solution. If $\mathcal{N}_\mu$ denotes the set of (not necessarily measurable) μ-null sets, then it is easy to show that

$$\mathcal{A}_\mu = \{A \cup N \mid A \in \mathcal{A}, N \in \mathcal{N}_\mu\}.$$

In particular, $\mathcal{A}_\mu = \mathcal{A}$ if and only if $\mathcal{N}_\mu \subseteq \mathcal{A}$, which is the case just when μ is complete. The claim follows since $\overline{\mu}$ is complete. ■

Problem 1.5.3(b). Let μ and ν be finite measures on a measurable space $(X, \mathcal{A})$. Prove or disprove: $\mathcal{A}_\mu = \mathcal{A}_\nu$ if and only if μ and ν have exactly the same sets of measure zero.

Solution. This is true, since in this case $\mathcal{N}_\mu = \mathcal{N}_\nu$. ■

Problem 4.1.3. Let μ_1 and μ_2 be finite signed measures on the measurable space $(X, \mathcal{A})$. Define signed measures $\mu_1 \vee \mu_2$ and $\mu_1 \wedge \mu_2$ on $(X, \mathcal{A})$ by $\mu_1 \vee \mu_2 = \mu_1 + (\mu_2 - \mu_1)^+$ and $\mu_1 \wedge \mu_2 = \mu_1 - (\mu_1 - \mu_2)^+$.

(1) Show that $\mu_1 \vee \mu_2$ is the smallest of those finite signed measures ν that satisfy $\nu(A) \geq \mu_1(A)$ and $\nu(A) \geq \mu_2(A)$ for all A in $\mathcal{A}$.

(2) Find and prove an analogous characterization of $\mu_1 \wedge \mu_2$.

Solution. (a) Since $(\mu_2 - \mu_1)^+$ is a positive measure, we clearly have $\mu_1 + (\mu_2 - \mu_1)^+ \geq \mu_1$. Since $(\mu_2 - \mu_1)^+ \geq \mu_2 - \mu_1$, we also have

$$\mu_1 + (\mu_2 - \mu_1)^+ \geq \mu_1 + \mu_2 - \mu_1 = \mu_2.$$

Next let ν be a finite signed measure with $\mu_1, \mu_2 \leq \nu$. Then

$$\mu_2 - \mu_1 \leq \nu - \mu_1,$$

and $\nu - \mu_1$ is positive so $(\mu_2 - \mu_1)^+ \leq \nu - \mu_1$, proving that $\mu_1 + (\mu_2 - \mu_1)^+$ is minimal.

(b) Similarly, $\mu_1 \wedge \mu_2$ is the largest finite signed measure smaller than both μ_1 and μ_2.

In particular, $M(\mathcal{A}, \mathbb{R})$ is a lattice when equipped with the product order from $\mathbb{R}^{\mathcal{A}}$. We also have $\mu_1 \vee \mu_2 = \mu_2 \vee \mu_1$, and similary for meets. ■

Problem 4.1.5. Let μ be a signed or complex measure on $(X, \mathcal{A})$, and let ν be a positive measure on $(X, \mathcal{A})$ such that $|\mu(A)| \leq \nu(A)$ holds for each A in $\mathcal{A}$. Show that $|\mu|(A) \leq \nu(A)$ holds for each A in $\mathcal{A}$. Hence $|\mu|$ is the smallest positive measure greater than μ, i.e. $|\mu| = \mu \vee 0$.

Solution. If (A_j) is a partition of A, then

$$\sum_{j=1}^{n} |\mu(A_j)| \leq \sum_{j=1}^{n} \nu(A_j) = \nu(A).$$

Taking the supremum on the left-hand side yields the claim. ■

Problem 4.1.8. Let μ and $\mu_1, \mu_2, \ldots$ be finite signed or complex measures on $(X, \mathcal{A})$. Show that $\lim_{n\to\infty} \|\mu_n - \mu\| = 0$ holds if and only if $\mu_n(A)$ converges to $\mu(A)$ uniformly in A as n approaches infinity.

In particular, the norms $\|\cdot\|$ and $\|\cdot\|_{\sup}$ are equivalent and thus have the same Cauchy sequences.[1]

Furthermore, $M(\mathcal{A}, \mathbb{K})$ is complete.

[1] Recall that topological and Lipschitz equivalence are equivalent for metrics induced by a norm.

Solution. Notice that the set $M(\mathcal{A},\mathbb{K})$ is a subspace of the space of bounded functions $\mathcal{A} \to \mathbb{K}$. In particular, it inherits the supremum norm $\|\cdot\|_{\sup}$, and uniform convergence is just convergence with respect to this norm.

For one implication, notice that for $A \in \mathcal{A}$ we have

$$|\mu(A)| \leq |\mu|(A) \leq \|\mu\|,$$

which implies that $\|\mu\|_{\sup} \leq \|\mu\|$. For the other implication, notice that it suffices to show that if $\|\mu_n\|_{\sup} \to 0$, then also $\|\mu\| \to 0$. If $\varepsilon > 0$, then there is a partition $(A_j)_{j=1}^n$ of X such that

$$\|\mu_n\| - \varepsilon \leq \sum_{j=1}^k |\mu_n(A_j)| \leq k\|\mu_n\|_{\sup}.$$

It follows that

$$\limsup_{n\to\infty} \|\mu_n\| = 0,$$

proving the claim.

In particular, the norms $\|\cdot\|$ and $\|\cdot\|_{\sup}$ are topologically equivalent (since $M(\mathcal{A},\mathbb{K})$ is a metric space and hence is a sequential space).

To show that $M(\mathcal{A},\mathbb{K})$ is complete, it suffices to show that it is closed as a subset of the space of bounded functions $\mathcal{A} \to \mathbb{K}$, so let $(\mu_n)_{n\in\mathbb{N}}$ be a sequence in $M(\mathcal{A},\mathbb{K})$ that converges to some μ. It is then clear that μ is finitely additive, and to show that it is countably additive, let $(A_k)_{k\in\mathbb{N}}$ be a decreasing sequence in $\mathcal{A}$ with $\bigcap_{k\in\mathbb{N}} A_k = \emptyset$. Let $\varepsilon > 0$ and choose $N \in \mathbb{N}$ such that $\|\mu_N - \mu\|_{\sup} < \varepsilon$. Since μ_N is countably additive, there is a $K \in \mathbb{N}$ such that $k \geq K$ implies $|\mu_N(A_k)| < \varepsilon$. Hence

$$|\mu(A_k)| \leq |\mu(A_k) - \mu_N(A_k)| + |\mu_N(A_k)| < 2\varepsilon.$$

(Notice the similarity with the proof that a uniform limit of continuous functions is continuous. Indeed, countable additivity of measures is a kind of continuity.) ■

Problem 4.2.5. Let $(X,\mathcal{A})$ be a measurable space, let μ be a positive measure on $(X,\mathcal{A})$, and let ν_1 and ν_2 be finite signed measures on $(X,\mathcal{A})$ that are absolutely continuous with respect to μ.

(1) Show that $\nu_1 \vee \nu_2 \ll \mu$ and $\nu_1 \wedge \nu_2 \ll \mu$.

(2) Show that if ν_1 and ν_2 have densities with respect to μ, then so do $\nu_1 \vee \nu_2$ and $\nu_1 \wedge \nu_2$, and find them.

Solution. (a) Both of these follow since $\mu^{\ll} := \{\nu \in M(\mathcal{A},\mathbb{R}) \mid \nu \ll \mu\}$ is a subspace.

(b) Denote by $\mathcal{D}_\mu$ the set of those measures in $M(\mathcal{A},\mathbb{R})$ that have a density with respect to μ. Notice that such a density can be chosen to lie in $\mathcal{L}^1(\mu)$. If $\nu_1 = h_1\mu$, $\nu_2 = h_2\mu$ and $\alpha \in \mathbb{R}$, then

$$(\alpha\nu_1 + \nu_2)(A) = \alpha\nu_1(A) + \nu_2(A) = \alpha \int_A h_1 \,\mathrm{d}\mu + \int_A h_2 \,\mathrm{d}\mu = \int_A (\alpha h_1 + h_2)\,\mathrm{d}\mu.$$

In particular, $\mathcal{D}_\mu$ is a subspace. Furthermore, if $\nu = h\mu$ then $\nu = h^+\mu - h^-\mu$. But we clearly have $h^+\mu \perp h^-\mu$, so by uniqueness of Jordan decompositions we have $\nu^+ = h^+\mu$ and $\nu^- = h^-\mu$. In particular, $\nu^+, \nu^- \in \mathcal{D}_\mu$. We finally find that

$$\nu_1 \vee \nu_2 = \nu_1 + (\nu_2 - \nu_1)^+ = \big(h_1 + (h_2 - h_1)^+)\big)\mu = (h_1 \vee h_2)\mu,$$

and we similarly have $\nu_1 \wedge \nu_2 = (h_1 \wedge h_2)\mu$. In particular, $\mathcal{D}_\mu$ is a sublattice of $M(\mathcal{A},\mathbb{R})$.

Problem 4.2.7. Let $\mu \in M(\mathcal{A},\mathbb{K})$.

(1) Show that
$$\mu^{\ll} := \{\nu \in M(\mathcal{A},\mathbb{K}) \mid \nu \ll \mu\}$$
is a closed linear subspace of the normed linear space $M(\mathcal{A},\mathbb{K})$.

(2) Assume that μ is σ-finite. Find an isometric isomorphism of $L^1(\mu,\mathbb{K})$ onto $\mu^{\ll}$.

Solution. (a) Clearly $\mu^{\ll}$ is a subspace of $M(\mathcal{A},\mathbb{K})$. To show that it is closed, let (ν_n) be a sequence in $\mu^{\ll}$ that converges to some $\nu \in M(\mathcal{A},\mathbb{K})$. By Exercise 4.1.8 we have $|\nu_n(A) - \nu(A)| \to 0$, so if A is a μ-null set then $\nu_n(A) = 0$, and so $\nu(A) \to 0$. But this just means that $\nu(A) = 0$, so $\nu \ll \mu$.

(b) First consider the map

$$\begin{aligned} \mathcal{L}^1(\mu,\mathbb{K}) &\to \mu^{\ll}, \\ h &\mapsto h\mu. \end{aligned}$$

This is clearly well-defined and linear. Furthermore, by Proposition 4.2.5 we have
$$\|h\mu\| = |h\mu|(X) = \int_X |h|\,\mathrm{d}\mu = \|h\|_1,$$
so the map is an isometry. Descending to the normed space $L^1(\mu,\mathbb{K})$ we thus obtain an injection. If μ is σ-finite, then the Radon–Nikodym theorem yields surjectivity.

Also notice that if we know that $L^1(\mu,\mathbb{K})$ is complete, then (a) follows.

Problem 4.2.9. Let μ and ν be σ-finite positive measures on $(X, \mathcal{A})$. Show that the conditions

(1) $\nu \ll \mu$ and $\mu \ll \nu$,

(2) μ and ν have exactly the same sets of measure zero, and

(3) there is an $\mathcal{A}$-measurable function g that satisfies $0 < g(x) < \infty$ at each x in X and is such that $\nu(A) = \int_A g \, \mathrm{d}\mu$ holds for each A in $\mathcal{A}$

are equivalent.

Solution. Clearly (i) and (ii) are equivalent. Assuming (i) and (ii), ν has a density g with respect to μ. Let (A_n) be a sequence of ν-finite sets that increases to X. Notice that

$$\nu(\{g = \infty\} \cap A_n) = \int_{\{g=\infty\}\cap A_n} g \, \mathrm{d}\mu = \infty\mu(\{g = \infty\} \cap A_n).$$

Since $\{g = \infty\} \cap A_n$ is ν-finite, it must be μ-null. But then

$$\{g = \infty\} = \{g = \infty\} \cap \bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} \Big(\{g = \infty\} \cap A_n\Big)$$

is also a μ-null set. Hence we may replace g with $g\mathbf{1}_{\{g<\infty\}}$ so that g is finite. Next notice that

$$\nu(\{g = 0\}) = \int_{\{g=0\}} g \, \mathrm{d}\mu = 0,$$

so also $\mu(\{g = 0\}) = 0$. Hence

$$\nu(A) = \int_A g \, \mathrm{d}\mu + \mu(A \cap \{g = 0\}) = \int_A (g + \mathbf{1}_{\{g=0\}}) \, \mathrm{d}\mu$$

for all $A \in \mathcal{A}$, so replacing g with $g + \mathbf{1}_{\{g=0\}}$ we may also assume that $g > 0$ everywhere. In total $0 < g < \infty$ everywhere.

Next assume (iii). Then we clearly have $\nu \ll \mu$. Furthermore, if $\nu(A) = 0$ then

$$\int_X g\mathbf{1}_A \, \mathrm{d}\mu = \int_A g \, \mathrm{d}\mu = \nu(A) = 0,$$

so $g\mathbf{1}_A = 0$ μ-a.e. since it is positive. But since $g > 0$, A must be μ-null. Thus we also have $\mu \ll \nu$. ■

Problem 4.2.10. Show that if μ is a σ-finite measure on $(X, \mathcal{A})$, then there is a finite measure ν on $(X, \mathcal{A})$ such that $\nu \ll \mu$ and $\mu \ll \nu$.

Solution. If μ is trivial then choose $\nu = \mu$. Otherwise let (A_n) be a sequence of disjoint sets from $\mathcal{A}$ with $0 < \mu(A_n) < \infty$ and whose union is X, and define a function $g\colon X \to \mathbb{R}$ by

$$g = \sum_{n=1}^{\infty} \frac{1}{2^n \mu(A_n)} \mathbf{1}_{A_n}.$$

Then $g \in \mathcal{L}^1(\mu)$ and $0 < g < \infty$ everywhere, so the claim follows from Exercise 4.2.9. ■

PROBLEM 4.3.2. Let $\mu \in M(\mathcal{A}, \mathbb{K})$. Show that

$$\mu^{\perp} := \{\nu \in M(\mathcal{A}, \mathbb{K}) \mid \nu \perp \mu\}$$

is a closed subspace.

Solution. Clearly $\mu^{\perp}$ is closed under scalar multiplication. If $\nu_1 \perp \mu$ and $\nu_2 \perp \mu$ with ν_j concentrated on A_j, μ concentrated on B_j, and with $A_j \cap B_j = \emptyset$ and $A_j \cup B_j = X$. Then A_j are μ-null, so $A_1 \cup A_2$ is also μ-null. Hence μ is concentrated on $B_1 \cap B_2$ and $\nu_1 + \nu_2$ is concentrated on $A_1 \cup A_2$. Thus $\mu^{\perp}$ is a subspace.

To show that it is closed, let (ν_n) be a sequence in $\mu^{\perp}$ converging to a $\nu \in M(\mathcal{A}, \mathbb{K})$, and let A_n and B_n be as above. Then $A = \bigcup_{n\in\mathbb{N}} A_n$ is also μ-null and $B = \bigcap_{n\in\mathbb{N}} B_n$ is ν_n-null. If $B' \subseteq B$, then

$$|\nu(B')| = |\nu_n(B') - \nu(B')| \xrightarrow[n\to\infty]{} 0.$$

So B is also ν-null, so $\nu \perp \mu$. ■

PROBLEM 4.3.3. Show that if ν_1 and ν_2 are singular signed or complex measures such that $\nu_1 + \nu_2$ is well-defined. Then

$$|\nu_1 + \nu_2|(A) = |\nu_1|(A) + |\nu_2|(A)$$

for all $A \in \mathcal{A}$. In particular,

$$\|\nu_1 + \nu_2\| = \|\nu_1\| + \|\nu_2\|.$$

Furthermore, let μ be a positive measure on $(X, \mathcal{A})$, let ν be a signed or complex measure on $(X, \mathcal{A})$, and let $\nu = \nu_a + \nu_s$ be the Lebesgue decomposition of ν. Then $\|\nu\| = \|\nu_a\| + \|\nu_s\|$.

Solution. Assume that $\nu_1 \perp \nu_2$, with ν_1 concentrated on E and ν_2 on E^c. Let $(A_i)_{i=1}^m$ and $(B_j)_{j=1}^n$ be partitions of a set A, and consider their common refinement $(C_l)_{l=1}^k$. By further refining (C_j) we may assume that either $C_l \subseteq E$ or $C_l \subseteq E^c$ for each C_l. Notice that

$$|\nu_1(C_l)| + |\nu_2(C_l)| = |\nu_1(C_l) + \nu_2(C_l)|,$$

since either $\nu_1(C_l)$ or $\nu_2(C_l)$ is zero. Hence we get

$$\begin{aligned}\sum_{i=1}^m |\nu_1(A_i)| + \sum_{j=1}^n |\nu_2(B_j)| &\le \sum_{l=1}^k |\nu_1(C_l)| + \sum_{l=1}^k |\nu_2(C_l)| \\ &= \sum_{l=1}^k |\nu_1(C_l) + \nu_2(C_l)| \\ &\le |\nu_1 + \nu_2|(A).\end{aligned}$$

Taking suprema on the left-hand side we get $|\nu_1|(A) + |\nu_2|(A) \le |\nu_1 + \nu_2|(A)$. For the opposite inequality, we simply have

$$\sum_{i=1}^m |\nu_1(A_i) + \nu_2(A_i)| \le \sum_{i=1}^m |\nu_1(A_i)| + \sum_{i=1}^m |\nu_2(A_i)| \le |\nu_1|(A) + |\nu_2|(A).$$

Again taking the supremum on the left-hand side we get $|\nu_1 + \nu_2|(A) \le |\nu_1|(A) + |\nu_2|(A)$. Letting $A = X$ we get $\|\nu_1 + \nu_2\| = \|\nu_1\| + \|\nu_2\|$.

If $\nu = \nu_a + \nu_s$ is a Lebesgue decomposition, we have $\nu_a \ll \mu$ and $\nu_s \perp \mu$, then it follows that $\nu_a \perp \nu_s$. The above then implies the claim. ■

Problem 4.3.7. Let $\mu, \nu \in M(\mathcal{A}, \mathbb{R})$. Then

$$\mu \vee \nu + \mu \wedge \nu = \mu + \nu. \tag{6.1}$$

In particular, if μ and ν are positive, then the conditions

(1) $\mu \perp \nu$,

(2) $\mu \wedge \nu = 0$, and

(3) $\mu \vee \nu = \mu + \nu$

are equivalent.

Compare the identity **??** with the identity

$$\operatorname{lcm}(a,b)\gcd(a,b) = ab$$

for $a, b \in \mathbb{Z}$, and the identity

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

for subgroups H, K of an abelian group. Note also that if $\mu \wedge \nu = 0$, then μ and ν are automatically positive.

Solution. Simply notice that

$$\mu \vee \nu + \mu \wedge \nu = \mu + (\nu - \mu)^+ + \nu - (\nu - \mu)^+ = \mu + \nu.$$

If μ and ν are positive, then the second and third conditions are clearly equivalent. If $\mu \perp \nu$ and μ is concentrated on E and ν on E^c, then

$$(\mu \wedge \nu)(A) = (\mu \wedge \nu)(A \cap E) + (\mu \wedge \nu)(A \cap E^c) \leq \nu(A \cap E) + \mu(A \cap E^c) = 0.$$

For the converse, assume that $\mu \wedge \nu = 0$, and let μ have Hahn decomposition (E_1, F_1) and ν have Hahn decomposition (F_2, E_2). We claim that (E, F) with $E = E_1 \cup E_1$ and $F = F_1 \cap F_2$ is a Hahn decomposition for μ and (F, E) for ν. But $\mu \wedge \nu = 0$ implies that $\mu = (\mu - \nu)^+ = (\mu - \nu) \vee 0$, so if $\mu(A) > 0$ then $\nu(A) = 0$. And if $\nu(A) > 0$ then $\mu(A) = 0$. The claim easily follows from these considerations.■

Bibliography