Math 286
Introduction to Differential Equations

Thomas Honold

ZJU-UIUC Institute

Fall Semester 2021

Outline

Introductory Remarks

1. Vector Spaces
   - Fields
   - Vector Spaces and their Basic Properties
   - Examples of Vector Spaces
   - Exchange Lemma and Proof of the Fundamental Theorem of Linear Algebra
   - Field Change
   - Dimension Formula for Subspaces
   - Direct Sums
2. Linear Maps
   - Definition and Basic Properties
   - Dimension Formula
   - Examples
3. Further Basic Linear Algebra Concepts
   - Coordinate Vectors
   - Matrices of Linear Maps
   - Determinants

Today’s Lecture: Linear Algebra Continued (Continued from Calculus III)

Linear Algebra

What it is about

From Calculus III you are familiar with the standard vector spaces $\mathbb{R}^n$, consisting of all n-tuples $\mathbf{x} = (x_1, \dots, x_n)$, $x_i \in \mathbb{R}$, and operations

$$\begin{aligned} \mathbf{x} + \mathbf{y} &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) && \text{(vector addition)} \\ a\mathbf{x} &= (ax_1, ax_2, \dots, ax_n) && \text{(scalar multiplication)} \end{aligned}$$

for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $a \in \mathbb{R}$. We have also discussed the function spaces $\mathbb{R}^I$ for intervals $I \subseteq \mathbb{R}$, which are in a way continuous analogues of $\mathbb{R}^n$. (Think of a function $f\colon I \to \mathbb{R}$ as the “sequence” $\bigl(f(x)\bigr)_{x \in I}$.)

However, there are many further (“non-standard”) vector spaces over $\mathbb{R}$ and also vector spaces over other fields.

Linear Algebra is the axiomatic theory of abstract vector spaces (just like group theory is the axiomatic theory of groups), including computational tools such as coordinate vectors and matrices.

The material in the subsequent sections forms an introduction to Linear Algebra. Most concepts will be developed from scratch, but note the following:

- the presentation assumes familiarity with the Linear Algebra crash course in Calculus III, e.g., by quoting examples from there.
- Certain topics that were discussed in the crash course and admit obvious generalizations to vector spaces over arbitrary fields won't be repeated; e.g., matrices over arbitrary fields and their basic properties (matrix operations, row and column space, rank) are assumed as known, as well as linear systems of equations over arbitrary fields and the machinery to solve them ("Gaussian elimination").

Background references

The following references, given for the Linear Algebra crash course in Calculus III, form good sources for most of the material discussed.

[Rob11] Lorenzo Robbiano, *Linear Algebra for Everyone*, Springer 2011

[NM17] Daniel Norman, Dan Wolczuk, Introduction to Linear Algebra for Science and Engineering, 2nd Edition, Pearson Education 2012

Be warned that zillions of different notations/conventions for Linear Algebra concepts are in use. So don't be surprised if you find three different notations for a particular concept in the lecture and the two references. (The lecturer claims that his notation is the best one, of course;-)

[NM17] takes a more restricted viewpoint than these notes and discusses only vector spaces over $\mathbb{R}$ and $\mathbb{C}$. For a course on differential equations this perspective is sufficient, but to some extent it fails to convey the elegance and ubiquity of "pure" Linear Algebra. I mention only one example: Error-resilient coding for data transmission relies on Linear Algebra over finite fields.

In order to define the concept of a “vector space”, we first need the concept of a “field”. Roughly speaking, a field consists of a set whose elements can be added/subtracted/multiplied/divided in much the same way as the numbers in $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$).

Definition (Field)

A *field* is an algebraic structure consisting of a set F, two distinguished elements $0, 1 \in F$ with $1 \neq 0$, and two binary operations $(x, y) \mapsto x + y$ (“addition”) and $(x, y) \mapsto xy = x \cdot y$ (“multiplication”) satisfying the following 10 axioms:

(A1) $\forall x, y, z \in F\colon (x + y) + z = x + (y + z)$ (*associativity of* $+$)

(A2) $\forall x \in F\colon x + 0 = 0 + x = x;$ (*additive identity*)

(A3) $(\forall x \in F)(\exists y \in F)\colon x + y = y + x = 0;$ (*additive inverse*)

(A4) $\forall x, y \in F\colon x + y = y + x;$ (*commutativity of* $+$)

(M1) $\forall x, y, z \in F\colon (xy)z = x(yz)$ (*associativity of* $\cdot$)

(M2) $\forall x \in F\colon x \cdot 1 = 1 \cdot x = x;$ (*multiplicative identity*)

(M3) $(\forall x \in F \setminus \{0\})(\exists y \in F)\colon xy = yx = 1;$ (*multiplicative inverse*)

(M4) $\forall x, y \in F\colon xy = yx;$ (*commutativity of* $\cdot$)

(D1) $\forall x, y, z \in F\colon x(y + z) = xy + xz;$ (*left distributive law*)

(D2) $\forall x, y, z \in F\colon (x + y)z = xz + yz;$ (*right distributive law*)

◂ Return

Remark

Some of these axioms are redundant.
For example, the second half of (A2) can be omitted, since $x + 0 = x$ together with (A4) implies $0 + x = x$.
Similarly, Axiom (D2) is a consequence of the remaining axioms.

Examples

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual addition and multiplication (and the usual numbers 0 and 1) are fields.
2. $\mathbb{Z}$ is not a field, because it does not satisfy Axiom (M3). For example, there is no integer x satisfying $2x = 1$.

   An algebraic structure such as $\mathbb{Z}$, which satifies all of the 10 axioms except possibly (M3), is called a *commutative ring*. If an algebraic structure satisfies all axioms except possibly (M3) and (M4), such as $\mathbb{R}^{n\times n}$ with matrix addition/multiplication, it is called a *ring*.

   If there is only one operation $(x, y) \mapsto x + y$ and Axioms (A1)–(A4) are satisfied, the algebraic structure is called a *commutative group* (and without the requirement of (A4) just a *group*).

Examples (cont'd)

3. For any prime number p, the set $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, together with addition/multiplication modulo p defined as

$$a \oplus b = (a + b) \bmod p, \qquad a \odot b = (ab) \bmod p,$$

is a field; see the Discrete Mathematics course for a proof. The proof of Axiom (M3) uses the Extended Euclidean Algorithm to find for $a \in \{1, 2, \dots, p-1\}$ integers $x, y \in \mathbb{Z}$ with $ax + py = 1$, which gives $a \odot x = 1$. Since this requires $\gcd(a, p) = 1$ for $1 \leq a \leq p-1$, the number p must be prime.

The fields $\mathbb{Z}_p$ are examples of *finite fields* (i.e., fields with a finite number of elements) and are also denoted by $\mathbb{F}_p$. The reason for the special notation "$\mathbb{F}_p$", which mimics that for $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ but contains an additional parameter, is that finite fields F are uniquely determined up to isomorphism by their order $|F|$. It is thus reasonable to speak of "the" finite field of order q and denote it by "$\mathbb{F}_q$". This theorem can be found in Abstract Algebra books, together with the companion theorem that a finite field of order q exists precisely when $q = p^e > 1$ is a prime power.

Three Fields and a Proper Ring

Which are the fields?

1

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$(\mathbb{F}_2)$

2

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(\mathbb{F}_3)$

3

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(\mathbb{Z}_4)$

4

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$(\mathbb{F}_4)$

Notes

- On the preceding slide the key fact is that $\mathbb{Z}_4$ *is not a field, but there exists a field with* 4 *elements*. This field is denoted by $\mathbb{F}_4$ and specified directly via its addition and multiplication table.
- The addition and multiplication tables of finite fields are symmetric as matrices. This is a consequence of Axioms (A4) resp. (M4).
- The row/column of the addition tables labeled with 0, is identical to the border row/column. Similarly, the row/column of the multiplication table labeled with 1, is identical to the border row/column. These properties follow from Axioms (A2) resp. (M2).
- The row/column labeled with 0 in the multiplication tables contains only zeros. This is due to the law “$0 \cdot x = x \cdot 0 = 0$ for $x \in F$”, which holds in any ring; cf. exercises.

Notes cont'd

- Axioms (A3), (M3) imply that the addition table, resp., the multiplication table of a finite field (the latter with the all-zero row and cloumn removed) form a so-called Latin square; cf. exercises. They are thus reflected combinatorially in the tables.
- That $\mathbb{Z}_4$ is not a field can be seen from its multiplication table. This table contains a '0' other than those in the 1st row and column, indicating the existence of nonzero elements a, b such that $ab = 0$. This cannot happen in a field; cf. exercises.
- The addition and multiplication table of $\mathbb{F}_4$ are uniquely determined by their borders (i.e., once the elements of $\mathbb{F}_4$ have been named); cf. exercises. This reflects the fact that up to isomorphism $\mathbb{F}_4$ is the only field of order 4.
- It is tedious to check directly that $\mathbb{F}_4$ satisfies all 10 field axioms. However, $\mathbb{F}_4$ may also be constructed by mimicking the construction of $\mathbb{C}$ out of $\mathbb{R}$, replacing $\mathbb{R}$ by $\mathbb{F}_2$ and the relation $\mathrm{i}^2 + 1 = 0$ by $a^2 + a + 1 = 0$. Thus $\mathbb{F}_4 = \{0, 1, a, 1 + a\} = \mathbb{F}_2 + \mathbb{F}_2 a$ with addition/multiplication being subject to the usual rules and $a^2 = -1 - a = 1 + a = b$. Using this model, the associative and distributive laws are easy to check (similar to the modulo operations on $\mathbb{Z}_p$).

Exercise

a) Let F be a field and $a, b \in F$. Using only the field axioms, show that the equation $a + x = b$ has a unique solution in F. Similarly, show that $ax = b$ has a unique solution in F, provided that $a \neq 0$.

b) Let F be a finite field and $q = |F|$. Show that the unbordered addition table of F forms a Latin square of order q. Similarly, show that the unbordered multiplication table of F with the row and column labeled '0' deleted forms a Latin square of order $q - 1$.

Note: A *Latin square of order n* is an arrangement of n distinct elements into an $n \times n$ array in such a way that every row and every column contains each element exactly once.

Exercise

Show that the addition and multiplication table of $\mathbb{F}_4$ is uniquely determined, if the row and column labels are $0, 1, a, b$ in this order.

Hint: First determine the multiplication table. Then using the distributive law show that $1 + 1 = a$ (and similarly $1 + 1 = b$) leads to a contradiction. (The distributive law must be involved in the argument, because the addition table of $\mathbb{Z}_4$ with $2 \triangleq a$, $3 \triangleq b$ provides a model satisfying (A1)–(A4).)

Exercise

1. Conclude from Axioms (A1)–(A3) that the only solution of the equation $x + x = x$ in a group/ring/field is $x = 0$.
2. Show that in a ring $0 \cdot x = x \cdot 0 = 0$ for all elements x.

   Hint: Use the distributive laws and a).
3. Show that in a field $xy = 0$ implies $x = 0$ or $y = 0$.
4. Show that in a field the cancellation laws "$x + y = x + z \Longrightarrow y = z$" and "$xy = xz \land x \neq 0 \Longrightarrow y = z$" hold.

Exercise (hard)

For the fields $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$, determine the largest n such that there exists a $3 \times n$ matrix M over the field with every 3×3 submatrix invertible. Further, show that over the rational field $\mathbb{Q}$ there exist $3 \times n$ matrices with this property for all $n \geq 3$.

Note: "3×3-submatrix" of $M = (\mathbf{v}_1|\dots|\mathbf{v}_n)$ refers to any matrix $(\mathbf{v}_{j_1}|\mathbf{v}_{j_2}|\mathbf{v}_{j_3})$ with $1 \leq j_1 < j_2 < j_3 \leq n\}$.

Definition (Vector space)

Let F be a field. A *vector space over F* consists of a set V (whose elements are called *vectors*), a commutative group operation $+$ on V (*vector addition*), and a *scalar multiplication* $F \times V \to V$, $(a, v) \mapsto av$ subject to the axioms

1. $(ab)v = a(bv)$,
2. $(a + b)v = av + bv$,
3. $a(u + v) = au + av$,
4. $1v = v$

for all $u, v \in V$ and $a, b \in F$.

Here $1 = 1_F$ refers to the multiplicative identity of F. We must carefully distinguish $0_V \in V$ (the zero vector) from $0_F \in F$ (the zero of F), although everybody writes just 0 for both.

Definition (Module)

If F is only a ring (not a field), then the algebraic structure defined above is called a *module over F*.

Module theory is much more difficult than Linear Algebra, and the main results on vector spaces do not generalize to modules.

Further Notes

- Unlike in the case $\mathbb{R}^n$, we don't use boldface type for vectors in general, because this makes writing ugly and can be confusing (since scalars of one vector space maybe vectors of another).

- The requirement that V be a commutative group with respect to vector addition means the following: There exist a distinguished vector $0 = 0_V \in V$, and the following axioms hold:

  (A1) $\forall x, y, z \in V\colon (x + y) + z = x + (y + z)$ (*associativity*)

  (A2) $\forall x \in V\colon x + 0 = 0 + x = x$; (*additive identity*)

  (A3) $(\forall x \in V)(\exists y \in V)\colon x + y = y + x = 0$; (*additive inverse*)

  (A4) $\forall x, y \in V\colon x + y = y + x$; (*commutativity*)

- In a vector space V (more generally, in any group), the additive inverse of any vector $x \in V$ is uniquely determined by x, since if y_1, y_2 satisfy the condition in (A3) then $y_1 = y_1 + 0 = y_1 + (x + y_2) = (y_1 + x) + y_2 = 0 + y_2 = y_2$. This justifies writing $-x$ for the inverse of x, so that $-x$ is characterized by the property $x + (-x) = 0$. (The same remark applies, mutatis mutandis, to multiplicative inverses of nonzero elements x in fields, which are denoted by x^{-1} or $1/x$.)

Exercise

Suppose V is a vector space over a field F.

a) Using the vector space axioms, prove the *scalar zero law*

$$0_F\,v = 0_V \quad \text{for all } v \in V.$$

b) Similarly, prove the *vector zero law*

$$a\,0_V = 0_V \quad \text{for all } a \in F.$$

c) Prove that $(-1)x = -x$ for all $x \in V$.

Basic Terminology for Vector Spaces

The definitions of subspaces, generating sets, linear combinations, linear independence, and bases introduced for the special case $\mathbb{R}^n$ can easily be adapted to the case of a general vector space V/F.

Definition (Subspace)

A subset $U \subseteq V$ is said to be a *subspace* of V if U forms itself a vector space under the induced operations. Equivalently, U contains 0_V (which then becomes 0_U) and satisfies $U + U = \{x + y; x, y \in U\} \subseteq U$, $FU = \{ax; a \in F, x \in U\} \subseteq U$.

Definition (Generating set)

A set of vectors $S \subseteq V$ is said to *generate* (or *span*) V if every vector $v \in V$ is a linear combination of vectors in S, i.e., there exist $v_1, \dots, v_r \in S$ and $a_1, \dots, a_r \in F$ such that $v = a_1 v_1 + a_2 v_2 + \cdots + a_r v_r$.

If S generates V, we write $V = \langle S \rangle$ or $V = \mathrm{span}(S)$.

Definition (Linear Independence)

A set of vectors $S \subseteq V$ is said to be *linearly independent* if $a_1 v_1 + a_2 v_2 + \cdots + a_r v_r = 0_V$ with $r \in \mathbb{Z}^+$, elements $a_1, \dots, a_r \in F$ and distinct vectors $v_1, \dots, v_r \in V$ implies $a_1 = a_2 = \cdots = a_r = 0$.

This includes the possibility $|S| = \infty$ and relates to our earlier definition as follows: Vectors $v_1, \dots, v_n$ are linearly independent in the old sense if they are distinct and $\{v_1, \dots, v_n\}$ is a linearly independent set in the new sense.

Definition (Basis)

A set of vectors $S \subseteq V$ is said to form a *basis* of V if every vector $v \in V$ can be written in exactly one way as a linear combination $v = \sum_{i=1}^{r} a_i v_i$ of vectors $v_i \in S$.

The order of the basis vectors does not matter (since vector addition commutative). “In exactly one way” means that the vectors v_i involved in the linear combination and their coefficients a_i are uniquely determined.

As we have done in the case $\mathbb{R}^n$, one shows without difficulty that a basis of a vector space is the same as a linearly independent generating set.

Dimension

The following Theorem is the most important theorem of Linear Algebra.

Theorem (Fundamental Theorem of Linear Algebra)

Let V be a vector space over a field F.

1. *V has a basis.*
2. *If B and B' are bases of V then $|B| = |B'|$ (i.e., any two bases of a given vector space have the same cardinality).*

Definition (Dimension)

The uniquely determined number $|B|$ in the theorem is called the *dimension* of V and denoted by $\mathrm{dim}(V)$.

Note

The theorem includes the possibility that V has a basis B with $|B| = \infty$. In this case Part (2) means the following. If B' is another basis of V then there exists a bijection from B onto B'. (For example, if B is denumerable, i.e., $B = \{b_1, b_2, b_3, \dots\}$ and $b_i \neq b_j$ for $i \neq j$, then the same must be true of B'.)

Isomorphism of Vector Spaces

Definition

Vector spaces V and W over the same field F are said to be *isomorphic* (notation $V \cong W$) if there exists a bijection $f\colon V \to W$ satisfying

(L1) $f(x+y) = f(x) + f(y)$ for all vectors $x, y \in V$;

(L2) $f(ax) = a\,f(x)$ for all vectors $x \in V$ and all scalars $a \in F$.

Notes

- There is a corresponding concept of isomorphism for vector spaces over possibly different fields (→ semilinear isomorphism). This will not be needed in the ODE course, however.
- As in the special case $V = \mathbb{R}^n$, $W = \mathbb{R}^m$, not necessarily bijective maps $f\colon V \to W$ satisfying (L1) and (L2) are said to be *linear* (or F*-linear*, if the scalar field F needs to be specified).

The Fundamental Theorem has the following important corollary, which classifies vector spaces over any given field F completely.

Corollary

Let V be a vector space over the field F. Then there exists a uniquely determined cardinality κ such that $V \cong F^\kappa$ (the standard vector space over F of dimension κ).

In the finite-dimensional case $\kappa = n \in \mathbb{N}$ *standard vector spaces* are defined in the same way as we have done earlier for $\mathbb{R}$, i.e., F^n consists of all n-tuples $x = (x_1, \dots, x_n)$ with $x_i \in F$ and operations

$$\begin{aligned} x + y &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n), && (x, y \in F^n) \\ ax &= (ax_1, ax_2, \dots, ax_n). && (x \in F^n, a \in F) \end{aligned}$$

As in the case $F = \mathbb{R}$ it is immediate that $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \dots)$, ..., $\mathbf{e}_n = (0, \dots, 0, 1)$ form a basis of F^n, so that indeed $\dim(F^n) = n$.

If κ is an infinite cardinality such as $|\mathbb{N}|$ or $|\mathbb{R}|$, we pick a set X with $|X| = \kappa$ and consider the "function space" $F^X = \{f; f \colon X \to F\}$ (i.e., as a set F^X consists of all maps from X to F). The set F^X forms a vector space over F relative to the point-wise operations $(f + g)(x) = f(x) + g(x)$, $(af)(x) = a\,f(x)$.

However, F^X is too large for being a suitable candidate. Instead we define $F^\kappa = \langle \mathrm{e}_x; x \in X \rangle$ as the subspace of F^X generated by the “unit functions”

$$\mathrm{e}_x \colon X \to F,\ y \mapsto \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{if } y \neq x. \end{cases}$$

A linear combination $f = \sum_{i=1}^r a_i \mathrm{e}_{x_i}$ of unit functions satisfies

$$f(x) = \begin{cases} a_i & \text{if } x = x_i \in \{x_1, \dots, x_r\}, \\ 0 & \text{if } x \notin \{x_1, \dots, x_r\}, \end{cases}$$

and hence vanishes outside a finite subset of X.
From this it is clear that F^κ consists precisely of all functions $f \colon X \to F$ with finite support, the *support* of f being defined as $\{x \in X; f(x) \neq 0\}$.
It is obvious that the unit functions are linearly independent. Thus they form a basis of F^κ, and $\dim(F^\kappa) = |\{\mathrm{e}_x; x \in X\}| = |X| = \kappa$, as desired.

Remark

In the infinite-dimensional case the preceding construction of F^κ is not canonical (and hence the term “standard vector space” not really appropriate), since there are many choices to pick the set X. In modern set theory *cardinal numbers* (“cardinalities”) are defined as particular ordered sets having the intended size, and such that there are no bijections between different cardinal numbers. Thus we can take $X = \kappa$ in the preceding construction, making it canonical. (But still be careful not to confuse the so-defined F^κ with the larger function space consisting of all maps from κ to F.)

Example

The first infinite cardinal number is $\aleph_0 = \mathbb{N} = \{0, 1, 2, \dots\}$ (i.e., $\mathbb{N}$ ordered in the natural way). The standard vector space $\mathbb{F}^{\aleph_0}$ consists of all infinite sequences $\mathbf{a} = (a_0, a_1, a_2, \dots)$ with $a_n \in F$ and $a_n = 0$ for all but finitely many n.

Reading $\mathbf{a}$ as the coefficient sequence of a polynomial, we can say that $\mathbb{F}^{\aleph_0}$ is the underlying vector space of the ring $F[X]$ of polynomials in one indeterminate over F.

Proof of the corollary.

Let $\kappa = \dim(V)$ and $B = (b_t)_{t \in \kappa}$ be a basis of V. Then the properties of a vector space basis imply that the map $f \colon V \to F^\kappa$, which sends $v \in V$ to the unique tuple $(a_t)_{t \in \kappa} \in F^\kappa$ satisfying $v = \sum_{i=1}^{r} a_{t_i} b_{t_i}$ with $r \geq 0$, $t_1, \dots, t_r$ distinct and $a_t = 0$ for $t \in \kappa \setminus \{t_1, \dots, t_r\}$ is a vector space isomorphism. □

Remark

The corollary allows us to reduce many questions about general vector spaces to the case of standard vector spaces, and thus in particular any question about finite-dimensional vector spaces over F (in particular this holds for $\mathbb{R}$, $\mathbb{C}$) to the already considered case $V = F^n$ (resp., $\mathbb{R}^n$, $\mathbb{C}^n$):

If $b_1, \dots, b_n$ is an (ordered) basis of V, where $n = \dim V$, then each $v \in V$ has a unique representation $v = a_1 b_1 + \dots + a_n b_n$ with $a_i \in F$, and we can consider the *coordinate vector* $(a_1, \dots, a_n) \in F^n$ of v instead of v itself. This immensely important idea will be worked out later when we discuss coordinate vectors in more detail.

Examples of Vector Spaces

Example (Standard vector spaces)

For any field F and any cardinal number κ there is exactly one standard vector space F^κ (cf. previous discussion).

Example (Function spaces)

Let F be a field an X a set. The set F^X of all maps $f\colon X \to F$ forms a vector space over F relative to the point-wise operations

$$(f+g)(x) = f(x) + g(x), \quad (af)(x) = a\,f(x)$$

for $f, g \in F^X$, $a \in F$, $x \in X$. Note that F^X is standard iff $|X| < \infty$.

Example (Matrix spaces)

For any field F and any $m, n \in \mathbb{N}$ the set $F^{m\times n}$ of $m \times n$-matrices $\mathbf{A} = (a_{ij})$ with entries in F forms an mn-dimensional vector space over F relative to the operations $\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij})$, $c\mathbf{A} = (c\,a_{ij})$ ($c \in F$). The special case $F = \mathbb{R}$ was discussed in Calculus III. Note that $F^{m\times n}$ is the particular case $X = \{1, \dots, m\} \times \{1, \dots, n\}$ or, in Python parlance, $X = \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$ of the preceding example.

Example (Matrix spaces cont'd)

Matrix spaces are well-suited to illustrate the concept of subspaces.

Problem

Consider the following subsets of $\mathbb{Q}^{3\times 3}$*:*

1. $S = \{\mathbf{A} \in \mathbb{Q}^{3\times 3}; \mathbf{A} = \mathbf{A}^{\mathsf{T}}\}$;
2. $Z = \{\mathbf{A} \in \mathbb{Q}^{3\times 3}; \mathbf{A}$ *has all row and column sums equal to zero*$\}$;
3. $E = \{\mathbf{A} \in \mathbb{Q}^{3\times 3}; \mathbf{A}$ *has all row and column sums equal*$\}$.

Show that S, Z, E *are subspaces of* $\mathbb{Q}^{3\times 3}$ *and find their dimension.*

Solution: (1) A symmetric 3×3 matrix has 6 degrees of freedom (the entries above and on the main diagonal), so the dimension is probably 6. For a rigorous proof we write

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = a_{11}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + a_{22}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + a_{33}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$+ a_{12}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + a_{13}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + a_{23}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Example (Matrix spaces cont'd)

The 6 symmetric matrices on the right-hand side are linearly independent, because in the upper-right window $\begin{pmatrix} * & * & * \\ & * & * \\ & & * \end{pmatrix}$ they look like the 6 standard unit vectors in $\mathbb{Q}^6$ (or $\mathbb{R}^6$).
$\Longrightarrow$ They form a basis of S, and hence $\dim(S) = 6$.
(That S is a subspace of $\mathbb{Q}^{3\times 3}$ follows as a by-product: In a vector space the linear combinations of any fixed set B of vectors form a subspace, viz. $\langle B\rangle$. But it can also be shown directly from the definition.)

(2) Here we can choose the entries in the upper-left 2×2 matrix freely. The remaining entries are then determined as $a_{13} = -a_{11} - a_{12}$, etc., and notably a_{33} (which is overdetermined) doesn't make problems.
$\Longrightarrow$ A basis of Z is

$$\left(\begin{array}{rr|r} 1 & 0 & -1 \\ 0 & 0 & 0 \\ \hline -1 & 0 & 1 \end{array}\right), \left(\begin{array}{rr|r} 0 & 1 & -1 \\ 0 & 0 & 0 \\ \hline 0 & -1 & 1 \end{array}\right), \left(\begin{array}{rr|r} 0 & 0 & 0 \\ 1 & 0 & -1 \\ \hline -1 & 0 & 1 \end{array}\right), \left(\begin{array}{rr|r} 0 & 0 & 0 \\ 0 & 1 & -1 \\ \hline 0 & -1 & 1 \end{array}\right),$$

and $\dim(Z) = 4$.

Example (Matrix spaces cont'd)

Was this a rigorous proof?
I think it was not, because we should verify that every matrix in Z can be written as a linear combination of the 4 basis matrices.

$$\left(\begin{array}{cc|c} a & b & -a-b \\ c & d & -c-d \\ \hline -a-c & -b-d & a+b+c+d \end{array}\right) = a\left(\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 0 & 0 \\ \hline -1 & 0 & 1 \end{array}\right)$$

$$+\, b\left(\begin{array}{cc|c} 0 & 1 & -1 \\ 0 & 0 & 0 \\ \hline 0 & -1 & 1 \end{array}\right) + c\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 1 & 0 & -1 \\ \hline -1 & 0 & 1 \end{array}\right) + d\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & 1 & -1 \\ \hline 0 & -1 & 1 \end{array}\right),$$

Now the proof is complete.

(3) Here we can choose the entry a_{13} freely, so that the 4 matrices in (2) together with

$$\left(\begin{array}{cc|c} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \hline 1 & 1 & -1 \end{array}\right), \quad \text{or} \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{if you like,}$$

form a basis of E, which therefore has dimension 5.

Example (Polynomials)

The ring $F[X]$ of all polynomials $a(X) = a_0 + a_1X + \cdots + a_dX^d$ with coefficients in F forms a vector space over F with respect to the operations $a(X) + b(X) = a_0 + b_0 + (a_1 + b_1)X + \cdots$, $\lambda\, a(X) = \lambda a_0 + \lambda a_1 X + \cdots$ $(\lambda \in F)$. This vector space has the basis $\{1, X, X^2, \dots\}$ and is standard with $\kappa = \mathbb{N} = \{0, 1, 2, \dots\}$.

Example (Formal power series)

If in the preceding example we replace $\sum_{i=0}^{d} a_iX^i$ by $\sum_{i=0}^{\infty} a_iX^i$, we obtain the ring of formal power series $F[[X]]$, which forms a vector space over F in the same way. This vector space is isomorphic to the function space $F^{\mathbb{N}}$ (every sequence is the coefficient sequence of a formal power series) and not standard, since $|\mathbb{N}| = \infty$ (there are many more formal power series than polynomials).

Example (Linear recurring sequences)

The set of solutions of a fixed homogeneous linear recurrence relation of order n with coefficients in F forms an n-dimensional vector space S over F; cf. our earlier discussion (and also the Discrete Mathematics course) for the special case $F = \mathbb{R}$ or $\mathbb{C}$.

Example (Linear recurring sequences cont'd)

A basis of S is formed by the sequences $\mathbf{e}_0 = (1, 0, \dots, 0, *, *, \dots)$, $\mathbf{e}_1 = (0, 1, 0, \dots, 0, *, *, \dots)$, ..., $\mathbf{e}_{n-1} = (0, \dots, 0, 1, *, *, \dots)$, which have the standard unit vectors of F^n as their initial parts (prefixes of length n).

For any solution $\mathbf{a} = (a_0, a_1, a_2, \dots) \in S$ we have

$$\mathbf{a} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \cdots + a_{n-1}\mathbf{e}_{n-1}.$$

Thus the coordinate vector $(a_0, \dots, a_{n-1})$ of $\mathbf{a}$ with respect to the basis $\{\mathbf{e}_0, \dots, \mathbf{e}_{n-1}\}$ is just the prefix of length n of $\mathbf{a}$.

The basis $\{\mathbf{e}_0, \dots, \mathbf{e}_{n-1}\}$ is usually inconvenient to work with, because its members are only specified in implicit (recursive) form. Explicit bases derived from the roots of the characteristic polynomial, and how to express a solution with given prefix $(a_0, \dots, a_{n-1})$ in terms of the explicit basis, was discussed for $F = \mathbb{R}, \mathbb{C}$ earlier in this course through examples (and in general in the Discrete Mathematics course). Binary linear recurring sequences (the case $F = \mathbb{F}_2$) have important applications in several areas of digital communication.

Example (Solution spaces of homogeneous linear ODE's)

We have seen that the real solutions $\phi\colon I \to \mathbb{R}$ of a higher-order (time-dependent) scalar ODE

$$y^{(n)} + a_{n-1}(t)y^{(n-1)} + \cdots + a_1(t)y' + a_0(t)y = 0 \qquad \text{(H)}$$

form a subspace S of the function space $\mathbb{R}^I$ (and hence a vector space over $\mathbb{R}$), provided the domain I is considered as fixed. Similarly the complex solutions $\phi\colon I \to \mathbb{C}$ form a subspace of $\mathbb{C}^I$ and hence a vector space over $\mathbb{C}$.

Question (concept check): What is $\dim S$?

Answer: $\dim S = n$, provided that the coefficient functions $a_i(t)$ are real-valued. (The complex solution space always has dimension n.)

For the proof choose $t_0 \in I$ and consider the "evaluation" map

$$E\colon S \to \mathbb{R}^n, \quad \phi \mapsto \bigl(\phi(t_0), \phi'(t_0), \phi''(t_0), \dots, \phi^{(n-1)}(t_0)\bigr).$$

E is obviously $\mathbb{R}$-linear, and the Existence and Uniqueness Theorems for solutions of ODEs yield that E is bijective.
$\Longrightarrow$ S is a vector space isomorphism and $\dim S = \dim \mathbb{R}^n = n$.

Example (cont'd)

There is one fundamental system of solutions that is particularly convenient for solving IVP's associated with (H) (and most useful for solving several instances simultaneously):
For $i \in \{0, 1, \dots, n-1\}$ let $\phi_i(t)$ be the unique solution of the IVP with initial conditions

$$y^{(i)}(t_0) = 1, \quad y^{(j)}(t_0) = 0 \quad \text{for } j \in \{0, 1, \dots, n-1\} \setminus \{i\}.$$

Then $\phi_0(t), \phi_1(t), \dots, \phi_{n-1}(t)$ is a fundamental system of solutions of (H), and the general solution $\phi(t) = a_0\phi_0(t) + a_1\phi_1(t) + \cdots + a_{n-1}\phi_{n-1}(t)$ satisfies

$$\phi^{(i)}(t_0) = a_0\phi_0^{(i)}(t_0) + a_1\phi_1^{(i)}(t_0) + \cdots + a_{n-1}\phi_{n-1}^{(i)}(t_0) = a_i.$$

In other words, if we want to solve an IVP associated to (H) with initial conditions $y^{(i)}(t) = a_i$, $0 \leq i \leq n-1$, we can (and must) just pick the linear combination of the fundamental solutions with coefficients a_i (i.e., the solution with coordinate vector $(a_0, \dots, a_{n-1})$).

The computation of $\phi_0(t), \phi_1(t), \dots, \phi_{n-1}(t)$ requires only elementary Linear Algebra that you already know.

Example (cont'd)

We illustrate this for the Euler equation $t^2y'' + ty' - y = 0$. This ODE is non-singular on $(0,\infty)$ and there has the fundamental system $y_1(t) = t$, $y_2(t) = t^{-1}$, because the indicial equation is $r^2 - 1 = 0$. The Wronski matrix of (y_1, y_2) is

$$\mathbf{W}(t) = \begin{pmatrix} y_1(t) & y_2(t) \\ y_1'(t) & y_2'(t) \end{pmatrix} = \begin{pmatrix} t & t^{-1} \\ 1 & -1/t^2 \end{pmatrix}.$$

For the general solution $y(t) = c_1y_1(t) + c_2y_2(t)$ we have

$$\begin{pmatrix} y(t) \\ y'(t) \end{pmatrix} = \begin{pmatrix} c_1y_1(t) + c_2y_2(t) \\ c_1y_1'(t) + c_2'y_2(t) \end{pmatrix} = \mathbf{W}(t)\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$

$$\Longrightarrow \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \mathbf{W}(t_0)^{-1}\begin{pmatrix} y(t_0) \\ y'(t_0) \end{pmatrix} = \frac{1}{-2/t_0}\begin{pmatrix} -1/t_0^2 & -t_0^{-1} \\ -1 & t_0 \end{pmatrix}\begin{pmatrix} y(t_0) \\ y'(t_0) \end{pmatrix}$$
$$= \begin{pmatrix} 1/(2t_0) & 1/2 \\ t_0/2 & -t_0^2/2 \end{pmatrix}\begin{pmatrix} y(t_0) \\ y'(t_0) \end{pmatrix}$$

We see that in order to realize the initial conditions $\bigl(y(t_0), y'(t_0)\bigr) = (1,0)$ and $(0,1)$, respectively, the coefficient vector $(c_1,c_2)^{\mathsf{T}}$ must be chosen as the 1st and 2nd column of $\mathbf{W}(t_0)^{-1}$.

Example (cont'd)

Now suppose we want to fit the initial conditions $y(1) = 1$, $y'(1) = 2$, say.

For $t_0 = 1$ we have $\mathbf{W}(1)^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}$ and obtain

$$\phi_1(t) = \tfrac{1}{2}t + \tfrac{1}{2}t^{-1}, \quad \phi_2(t) = \tfrac{1}{2}t - \tfrac{1}{2}t^{-1}.$$

The initial conditions $\bigl(y(1), y'(1)\bigr) = (1, 2)$ are then realized by

$$y(t) = 1\,\phi_1(t) + 2\,\phi_2(t) = \tfrac{3}{2}t - \tfrac{1}{2}t^{-1}.$$

For solving this particular IVP, however, the computation of $\mathbf{W}(1)^{-1}$ is not necessary. The advantage of the present approach lies in the observation that now we can write down the solution of any associated IVP $t^2y'' + ty' - y = 0$, $y(1) = a$, $y'(1) = b$ simply as

$$y(t) = a\,\phi_1(t) + b\,\phi_2(t) = \frac{a}{2}\left(t + t^{-1}\right) + \frac{b}{2}\left(t - t^{-1}\right).$$

This example generalizes to the $n \times n$ case: The inverse Wronski matrix $\mathbf{W}(t_0)^{-1} = (b_{ij})$ of any fundamental system $y_1, \dots, y_n$ yields the special fundamental system $\phi_1, \dots, \phi_n$ via $\phi_j(t) = \sum_{i=1}^n b_{ij}y_i(t)$.

Return to Power Series

An example of a semilinear module isomorphism

Earlier we have discussed the analogy between solutions of higher-order linear ODE's with constant coefficients and linear recurring sequences. Using power series, we can now establish the precise correspondence.

Consider the map

$$\mathrm{egf}\colon \mathbb{C}^{\mathbb{N}} \to \mathbb{C}^{\mathbb{R}},\ (a_0, a_1, a_2, \dots) \mapsto \left(t \mapsto \sum_{n=0}^{\infty} \frac{a_n}{n!}\, t^n\right)$$

with domain the set of all complex linear recurring sequences. (It can be shown that for such sequences **a** the corresponding power series $\mathrm{egf}(\mathbf{a})$ converges for all $t \in \mathbb{R}$.)

The power series $\mathrm{egf}(\mathbf{a})$ is called *exponential generating function* of the sequence $\mathbf{a} = (a_0, a_1, a_2, \dots)$.

Such generating functions are used in Enumerative Combinatorics, and students of Discrete Mathematics may have met them before.

We have

$$\mathrm{D}[\operatorname{egf}(a)]=\frac{\mathrm{d}}{\mathrm{d}t}\sum_{n=0}^{\infty}\frac{a_n}{n!}\,t^n=\sum_{n=1}^{\infty}\frac{na_n}{n!}\,t^{n-1}=\sum_{n=0}^{\infty}\frac{a_{n+1}}{n!}\,t^n=\operatorname{egf}(\mathrm{S}\mathbf{a})$$

This implies $\mathrm{D}^k\operatorname{egf}(\mathbf{a})=\operatorname{egf}(\mathrm{S}^k\mathbf{a})$ for $k\in\mathbb{N}$ and, since egf is $\mathbb{C}$-linear,

$$p(\mathrm{D})\operatorname{egf}(\mathbf{a})=\operatorname{egf}\bigl(p(\mathrm{S})\mathbf{a}\bigr)\quad\text{for all polynomials } p(X)\in\mathbb{C}[X].$$

This implies that egf defines a semilinear module isomorphism from the $\mathbb{C}[\mathrm{S}]$-module of all linear recurring sequences onto the $\mathbb{C}[\mathrm{D}]$-module of all exponential polynomials, and in particular that

$$p(\mathrm{D})\operatorname{egf}(\mathbf{a})=0\iff p(\mathrm{S})\mathbf{a}=0.$$

In other words, $\mathbf{a}=(a_0,a_1,a_2,\dots)$ solves the linear recurrence relation with characteristic polynomial $p(X)$ iff $\operatorname{egf}(\mathbf{a})$ solves the ODE $p(\mathrm{D})y=0$ (the ODE with the same characteristic polynomial).

Examples

- We have seen earlier that for a root r of $p(X)=X^d+\sum_{i=0}^{d-1}p_iX^i$ the sequence $(1,r,r^2,r^3,\dots)$ solves the linear recurrence relation $p(\mathrm{S})\mathbf{y}=\mathbf{0}$, i.e., $y_{n+d}=-\sum_{i=0}^{d-1}p_iy_{n+i}$. $\Longrightarrow$ $\operatorname{egf}(1,r,r^2,r^3,\dots)$ must be a solution of the corresponding ODE $p(\mathrm{D})y=0$.

$$\operatorname{egf}(1,r,r^2,r^3,\dots)=\sum_{n=0}^{\infty}\frac{r^n}{n!}t^n=\sum_{n=0}^{\infty}\frac{(rt)^n}{n!}=\mathrm{e}^{rt},$$

  which is a solution of $p(\mathrm{D})y=0$, as we know of course.

- Suppose you haven't attended Math286 for a while and don't know how to solve, say, $y''-y=\mathrm{e}^t-2$. But you are good at sequences and remember the generating function stuff from Discrete Mathematics. Here is how you can proceed:

$$\mathrm{e}^t=\operatorname{egf}(1,1,1,\dots),\quad -2=\operatorname{egf}(-2,0,0,,\dots),\quad p(X)=X^2-1$$

  Solve the two recurrence relations $p(\mathrm{S})\mathbf{y}=(1,1,1,\dots)$ and $p(\mathrm{S})\mathbf{y}=(-2,0,0,\dots)$.

Examples con't

- (cont'd) The first is $y_{n+2} - y_n = 1$ for $n \in \mathbb{N}$, which is solved by $\mathbf{y} = (0, \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \dots)$, i.e., $y_n = n/2$. The second is

$$y_{n+2} - y_n = \begin{cases} -2 & \text{if } n = 0, \\ 0 & \text{if } n \geq 1, \end{cases}$$

and is solved by $\mathbf{y} = (2, 0, 0, \dots)$.

$\Longrightarrow$ A particular solution of $y'' - y = \mathrm{e}^t - 2$ is

$$\begin{aligned} y(t) &= \operatorname{egf}(2, 0, 0, \dots) + \operatorname{egf}(0, \tfrac{1}{2}, 1, \tfrac{3}{2}, 2, \tfrac{5}{2}, \dots) \\ &= 2 + \sum_{n=0}^{\infty} \frac{n/2}{n!}\, t^n = 2 + \frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{(n-1)!}\, t^n \\ &= 2 + \tfrac{1}{2} t \mathrm{e}^t. \end{aligned}$$

Similarly, students of this course who haven't attended Discrete Mathematics can use the isomorphism backwards to solve any linear recurrence relation with constant coefficients.

Exercise

1. Show that the collection A of all linear recurring sequences over F (of any order, with arbitrary characteristic polynomial) forms a subspace of the vector space $F^{\mathbb{N}}$ of all F-valued infinite sequences.
2. Show that $A \subsetneqq F^{\mathbb{N}}$.
3. What is the subspace of $\mathbb{C}^{\mathbb{R}}$ corresponding to A under the map egf in the case $F = \mathbb{C}$? Can you specify nice bases of both spaces?

Example (Binary linear codes)

A binary linear $[n, k, d]$ code C is a k-dimensional subspace of $\mathbb{F}_2^n$ of minimum Hamming distance

$$\mathrm{d}_{\mathrm{Ham}}(C) = \min\bigl\{\mathrm{d}_{\mathrm{Ham}}(\mathbf{x}, \mathbf{y}); \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\bigr\} = d;$$

see Example **??** for metric spaces. The integer n is called *length* of the code. Binary linear codes are used in virtually every modern communication system to protect messages against transmission errors (more precisely, to reduce the probability of transmission errors to a very small but still positive number); see our Discrete Mathematics textbook [Ro13], Chapters 12.6 and 12.7, for a very short introduction to Algebraic Coding Theory.

$\mathbb{F}_2^n$ is just the set of n-bit strings with addition modulo 2 (i.e., the bit-wise XOR) as its vector addition. Scalar multiplication of $\mathbb{F}_2^n$ is trivial,

$$\begin{aligned} 0 \cdot \mathbf{x} &= (0 \cdot x_1, \dots, 0 \cdot x_n) = (0, \dots, 0) = \mathbf{0}, \\ 1 \cdot \mathbf{x} &= \mathbf{x}, \end{aligned}$$

and hence the subspace test for C reduces to $C \neq \emptyset$ and $\mathbf{x}, \mathbf{y} \in C \Longrightarrow \mathbf{x} + \mathbf{y} \in C$.

Example (cont'd)

The number of codewords in an $[n, k, d]$ code is 2^k, the number of different linear combinations of k basis vectors $\mathbf{c}_1, \dots, \mathbf{c}_k$ over $\mathbb{F}_2$ (there are 2 choices for each coefficient).

Perhaps the most famous binary linear code is the row space of the following matrix:

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

This code has parameters $[7, 4, 3]$ (hence $2^4 = 16$ codewords) and is the smallest member of the family of Hamming codes.

Exercise

The *Hamming weight* $\mathrm{w}_{\mathrm{Ham}}(\mathbf{x})$ of $\mathbf{x} \in \mathbb{F}_2^n$ is the number of nonzero entries (entries equal to 1). Show that

$$\mathrm{d}_{\mathrm{Ham}}(C) = \min\left\{\mathrm{w}_{\mathrm{Ham}}(\mathbf{x}); \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\right\}$$

for any binary linear code C. (This reduces the complexity of minimum distance computations from $(2^k - 1)(2^k - 2)/2$ to $2^k - 1$.)

Exercise

a) Using Gaussian elimination over $\mathbb{F}_2$, compute a generating matrix $\mathbf{G}'$ of the form $(\mathbf{I}_4|\mathbf{A})$ (so-called *systematic* generating matrix) for the $[7,4,3]$ Hamming code C in the preceding example. Then specify the corresponding systematic encoder $\gamma\colon \mathbb{F}_2^4 \to C$, $(x_1, x_2, x_3, x_4) \to (x_1, x_2, x_3, x_4)\mathbf{G}'$ exactly in terms of bit operations.

b) Use the matrix in a) to list all 16 codewords and, together with the preceding exercise, to verify that $d = 3$.

c) Show that $\mathbb{F}_2^7$ is the disjoint union of the balls of radius 1 centered at the codewords of C. (A code with this property is called a *perfect single-error-correcting code*.)

d) Which combinatorial property of the matrix $\mathbf{A}$ in a) is responsible for $d = 3$? Can you generalize this construction?

Example (Magic squares)

A (generalized) *magic square* of *order n* over a field F is a matrix $\mathbf{A} = (a_{ij}) \in F^{n\times n}$ with equal row, column and diagonal sums. A magic square is *classical* if $F = \mathbb{Q}$ and its entries are the integers $1, 2, \dots, n^2$ in some order. A famous example is Albrecht Dürer’s magic square:

$$\begin{pmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{pmatrix}$$

The common value s of the row, column and diagonal sums of a magic square is called its *magic number*. A classical 4×4 magic square necessarily has $s = 34$ (why?).

The magic squares of order n over F form a subspace M of $F^{n\times n}$, and the magic squares in M with magic number $s = 0$ form another subspace M_0 with $M_0 \subseteq M$. This follows from the fact that the defining conditions for magic squares represent linear equations in the entries a_{ij}. We illustrate this for $n = 3$:

Example (cont'd)

$$\mathbf{A} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} \in F^{3\times 3}$$

is a magic square with magic number s iff

$$\begin{aligned} x_1 + x_2 + x_3 &= s \\ x_4 + x_5 + x_6 &= s \\ x_7 + x_8 + x_9 &= s \\ x_1 + x_4 + x_7 &= s \\ x_2 + x_5 + x_8 &= s \\ x_3 + x_6 + x_9 &= s \\ x_1 + x_5 + x_9 &= s \\ x_3 + x_5 + x_7 &= s \end{aligned}$$

If $s = 0$, these are 8 homogeneous linear equations for $x_1, \dots, x_9$, whose solution space (with the entries arranged in a 3×3 matrix) is M_0. If s is undetermined, the system is equivalent to the one with 7 homogeneous linear equations that is obtained by subtracting the 1st equation from the remaining equations and discarding it.

Example (cont'd)

Problem: For given F and n, determine the dimension of M and a basis of M. Use this information to classify all magic squares of order n over F with a given magic sum s, say, and similarly for classical magic squares of order n.

Note: For $F = \mathbb{Q}$ the first problem reduces to the case $s = 0$ (i.e., the determination of all magic squares in M_0) as follows: The all-one $n \times n$ matrix $\mathbf{J}$ is a “special” magic square with magic number n. It follows that $(s/n)\mathbf{J}$ has magic number $(s/n)n = s$ and that the “general” magic square in M with magic number s differs from $(s/n)\mathbf{J}$ by an element of M_0 (an instance of the reduction of inhomogeneous systems $\mathbf{Ax} = \mathbf{b}$ to the homogeneous case $\mathbf{Ax} = \mathbf{0}$).

Exercise

a) Write down the linear system of equations satisfied by a classical 3×3 magic square and transform this system into row-echelon form. (What is the magic number in this case?)

b) Use the equations in a) to show that up to obvious symmetries there exists exactly one classical 3×3 magic square.

Exercise (quite hard)

Show that for $F = \mathbb{Q}$ the dimensions of M and M_0 are $n^2 - 2n$ and $n^2 - 2n - 1$, respectively, and determine bases of these vector spaces for $n = 2, 3, 4$.

Dimension

The following Theorem is the most important theorem of Linear Algebra.

Theorem (Fundamental Theorem of Linear Algebra)

Let V be a vector space over a field F.

1. *V has a basis.*
2. *If B and B' are bases of V then $|B| = |B'|$ (i.e., any two bases of a given vector space have the same cardinality).*

Definition (Dimension)

The uniquely determined number $|B|$ in the theorem is called the *dimension* of V and denoted by $\dim(V)$.

Note

The theorem includes the possibility that V has a basis B with $|B| = \infty$. In this case Part (2) means the following. If B' is another basis of V then there exists a bijection from B onto B'. (For example, if B is denumerable, i.e., $B = \{b_1, b_2, b_3, \dots\}$ and $b_i \neq b_j$ for $i \neq j$, then the same must be true of B'.)

Proof of the Fundamental Theorem.

We only consider the case of finite-dimensional (i.e., finitely generated) vector spaces. The proof in the infinite-dimensional case depends on subtle notions from set theory (but poses no essential difficulty).

Let V/F be a vector space and suppose $V = \langle B \rangle$ for some finite subset $B = \{b_1, \dots, b_n\}$ of V.

The key step in the proof is the following

Lemma (Exchange Lemma)

If $A \subseteq V$ is linearly independent then $m = |A| \leq n$ and there exists a subset $B' \subseteq B$ with $|B'| = m$ and such that $A \cup (B \setminus B')$ also generates V.

Proof: First we assume $m = |A| \leq n$ and prove the assertion by induction on m. If $m = 0$, the assertion is trivially true.
Now assume $m \geq 1$ and let $A = \{a_1, \dots, a_m\}$, $A' = \{a_1, \dots, a_{m-1}\}$. Then for A' (which is also linearly independent) the assertion is true by the inductive hypothesis. Reordering $b_1, \dots, b_n$, if necessary, we may assume that $V = \langle a_1, \dots, a_{m-1}, b_m, b_{m+1}, \dots, b_n \rangle$.

Proof cont'd.

Hence there exist scalars $\lambda_i \in F$ such that

$$a_m = \lambda_1 a_1 + \dots + \lambda_{m-1} a_{m-1} + \lambda_m b_m + \lambda_{m+1} b_{m+1} + \dots + \lambda_n b_n.$$

If $\lambda_i = 0$ for $i \geq m$ we obtain that A is linearly dependent, a contradiction.
Hence there exist $i \geq m$ with $\lambda_i \neq 0$; w.l.o.g. let $i = m$.

$$\implies b_m = \frac{1}{\lambda_m}\left(a_m - \sum_{i=1}^{m-1} \lambda_i a_i - \sum_{i=m+1}^{n} \lambda_i b_i\right)$$
$$\in \langle a_1, \dots, a_m, b_{m+1}, \dots, b_n \rangle.$$

Since V is generated by $a_1, \dots, a_{m-1}, b_m, b_{m+1}, \dots, b_n$ and b_m is a linear combination of these vectors and a_m, we must have $V = \langle a_1, \dots, a_m, b_{m+1}, \dots, b_n \rangle$, as asserted.
Finally suppose $|A| > n$. Then the preceding proof gives $V = \langle A' \rangle$ for any n-set $A' \subseteq A$. Fixing such a set A' and choosing $a \in A \setminus A'$, we have that a is a linear combination of the elements in A'. Thus $A' \cup \{a\}$, and hence A, is linearly dependent. This contradiction completes the proof of the lemma.

Proof cont'd.

(1) Choose a linearly independent set $A \subseteq V$ of maximum cardinality. By the lemma, such a set A exists and has $|A| \leq n$.

Let $v \in V \setminus A$. Then $A \cup \{v\}$ is linearly dependent. In a corresponding dependency relation v must appear with a nonzero coefficient (otherwise A would be linearly dependent). Hence we can solve for v and obtain $v \in \langle A \rangle$. This shows $V = \langle A \rangle$, i.e., A is a basis of V.

(2) Let B, B' be bases of V with $|B'| = m$, $|B| = n$. Applying the lemma with $A = B'$ (B has the same meaning as in the lemma), we obtain $m \leq n$.

Interchanging the roles of B and B' (which is possible, since B is linearly independent and B' generates V), we obtain $n \leq m$. Hence $m = n$ as asserted. □

The Exchange Lemma has further important consequences:

Theorem

Let V/F be a vector space.

1. *If $A \subseteq V$ is linearly independent, there exists a basis B of V with $B \supseteq A$. In other words, every linearly independent subset of V can be augmented to a basis of V.*
2. *If $C \subseteq V$ generates V, there exists a basis B of V with $B \subseteq C$. In other words, every generating set of V can be expurgated to a basis of V.*

Proof.

(1) can be proved in much the same way as Part (1) of the Fundamental Theorem, by choosing a linearly independent set $B \supseteq A$ of maximum cardinality and showing that B generates V. Similarly, for the proof of (2) choose a generating set $B \subseteq C$ of minimum cardinality and show that B is linearly independent. □

Note

Like the Fundamental Theorem, this theorem remains true for infinite-dimensional vector spaces. But a proof of this requires more subtle notions from set theory.

If V is a vector space and U is a subspace of V, we generally have $\dim U \leq \dim V$. (In the infinite-dimensional case this means that for any bases B of V and B' of U there exists an injection $B' \to B$ or, equivalently, a surjection $B \to B'$.)

Theorem

Let V be a vector space of finite dimension n and U a subspace of V. Then $\dim U \leq \dim V$ with equality iff $U = V$.

Similarly we have:

Theorem

Let V be a vector space of finite dimension n. For a subset B of V, any two of the following properties imply the third property (and show that B is a basis of V).

1. *B is linearly independent;*
2. *B generates V;*
3. *$|B| = n$.*

This theorem provides justification, e.g., for the often-used fact that, two solutions ϕ_1, ϕ_2 of an explicit 2nd-order linear ODE must form a fundamental system provided only that they are linearly independent. We don't need to check that any other solution is a linear combination of ϕ_1 and ϕ_2.

Exercise

In each of the following cases, let S be the set of vectors $(\alpha, \beta, \gamma) \in \mathbb{C}^3$ satisfying the given condition. Decide whether S is a subspace of $\mathbb{C}^3/\mathbb{C}$ and, if so, determine the dimension of S.

a) $\alpha = 0$;

b) $\alpha\beta = 0$;

c) $\alpha + \beta = 1$;

d) $\alpha + \beta = 0$;

e) $\alpha = 3\beta \wedge \beta = (2 - \mathrm{i})\gamma$;

f) $\alpha \in \mathbb{R}$

Exercise

Let P_3 be the vector space (over $\mathbb{R}$) of polynomials $p(X) \in \mathbb{R}[X]$ of degree at most 3. Repeat the previous exercise for the sets $S \subseteq P_3$ defined by each of the following conditions:

a) $p(X)$ has degree 3;

b) $2p(0) = p(1)$;

c) $p(t) \geq 0$ for $0 \leq t \leq 1$;

d) $p(t) = p(1 - t)$ for all $t \in \mathbb{R}$.

Field Change

Definition

Suppose F is a field and $E \subseteq F$. The subset E is said to be a *subfield* of F if E forms itself a field with respect to the induced operations. Equivalently, E contains the distinguished elements 0, 1 of F, and $a, b \in E$ implies $a \pm b \in E$, $ab \in E$, and in the case $b \neq 0$ also $a/b \in E$.

If E is a subfield of F, we also say that F is an *extension field* of E and write F/E.

Examples

$\mathbb{R}$ is a subfield of $\mathbb{C}$, and $\mathbb{Q}$ is a subfield of both $\mathbb{R}$ and $\mathbb{C}$. The set $\{0, 1\} \subset \mathbb{F}_4$ forms a subfield of $\mathbb{F}_4$ isomorphic to $\mathbb{F}_2$. (The latter means that addition and multiplication for $\{0, 1\}$ within $\mathbb{F}_4$ are the same as in $\mathbb{F}_2$.)

Observation

If F/E is a field extension then F is in particular a vector space over E.

Field Change Cont'd

Examples (cont'd)

$\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$ with basis $\{1, \mathrm{i}\}$ (and many other bases).

$\mathbb{R}$ and $\mathbb{C}$ are infinite-dimensional vector spaces over $\mathbb{Q}$.

(*Reason:* If $\mathbb{R}/\mathbb{Q}$ had a finite basis $\{b_1, \dots, b_n\}$ then $\mathbb{R} \cong \mathbb{Q}^n$ would be countable (just like $\mathbb{Q}$), but this is not the case.

$\mathbb{F}_4/\mathbb{F}_2$ is a 2-dimensional vector space with basis $\{1, a\}$.

(For this note that $0 = 0 \cdot 1 + 0 \cdot a$, $1 = 1 \cdot 1 + 0 \cdot a$, $a = 0 \cdot 1 + 1 \cdot a$, $b = 1 + a = 1 \cdot 1 + 1 \cdot a$.)

Theorem (Field reduction)

Let V be a vector space over F and E a subfield of F. Then V forms also a vector space over E, and $\dim(V/E) = \dim(V/F)\dim(F/E)$.

Sketch of proof.

Let $v_1, \dots, v_n$ be a basis of V/F and $c_1, \dots, c_m$ be a basis of F/E. Then the $mn = \dim(V/F)\dim(F/E)$ elements $c_i v_j \in V$ (these are the vectors $v_j \in V$ multiplied by the scalars $c_i \in F$) can be shown to form a basis of V/E. □

Examples

The standard vector space $\mathbb{C}^n$, which is n-dimensional over $\mathbb{C}$ with basis $\mathbf{e}_1 = (1, 0, \dots, 1)$, $\mathbf{e}_2 = (0, 1, 0, \dots, 0)$, ..., $\mathbf{e}_n = (0, \dots, 0, 1)$ (the standard unit vectors), has dimension $2n$ over $\mathbb{R}$. A basis of $\mathbb{C}^n/\mathbb{R}$ is formed by the standard unit vectors and the vectors $\mathrm{i}\mathbf{e}_1 = (\mathrm{i}, 0, \dots, 0)$, $\mathrm{i}\mathbf{e}_2 = (0, \mathrm{i}, 0, \dots, 0)$, ..., $\mathrm{i}\mathbf{e}_n = (0, \dots, 0, \mathrm{i})$.

The complex solution space $S/\mathbb{C}$ of the ODE $y'' + y = 0$, which has dimension 2 and the two bases $\{\mathrm{e}^{\mathrm{i}x}, \mathrm{e}^{-\mathrm{i}x}\}$ and $\{\cos x, \sin x\}$ (because $\cos x = \frac{1}{2}(\mathrm{e}^{\mathrm{i}x} + \mathrm{e}^{-\mathrm{i}x})$, $\sin x = \frac{1}{2\mathrm{i}}(\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x})$), corresponds to a 4-dimensional vector space $S/\mathbb{R}$ with basis $\{\cos x, \mathrm{i}\cos x, \sin x, \mathrm{i}\sin x\}$, say.

For subspaces of function spaces we can go the other way round: Suppose that U is a subspace of $E^X = \{f; f\colon X \to E\}$ and F is an extension field of E. Then, since $E^X \subseteq F^X$, we can multiply the maps in U with scalars in F and consider $\widetilde{U} = \langle U \rangle_F$, which is a subspace of F^X.

Question

Does the dimension drop when $U \to \widetilde{U}$, i.e., can maps that are linearly independent over E become linearly dependent over the larger field F?

The answer is “No”.

Theorem (Field extension)

Let X be a set, F/E a field extension and $S \subseteq E^X$ a linearly independent set of maps. Then S is linearly independent over F as well.

Consequently, in the setting above we have $\dim U = \dim \widetilde{U}$.

Proof.

Let C be a basis of F/E, and suppose $\sum_{i=1}^{r} \alpha_i f_i(x) = 0$ for $x \in X$ with distinct $f_i \in S$, $\alpha_i \in F$. Expressing each α_i as an E-linear combination of elements in C, we have $\alpha_i = \sum_{j=1}^{m} a_{ij} c_j$ for $1 \leq i \leq r$, some $c_1, \dots, c_m \in C$ and some $a_{ij} \in E$. Plugging this into the linear dependency relation and interchanging the summation gives

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{r} a_{ij} f_i(x) \right) c_j = 0.$$

Since $f_i(x) \in E$ (the key point!), this is a representation of $0 \in F$ as an E-linear combination. Hence, since C is a basis of F/E, we must have $\sum_{i=1}^{r} a_{ij} f_i(x) = 0$ for all $x \in X$, $1 \leq j \leq m$.
Finally, since $f_1, \dots, f_r$ are linearly independent over E, this gives $a_{ij} = 0$ for all i, j and hence $\alpha_i = 0$ for all i. □

Examples (cont'd)

The spaces $\mathbb{R}^n$ and $\mathbb{C}^n$ are special cases of function spaces (with $X = \{1, 2, \dots, n\}$). Hence the field extension theorem applies and gives that any linearly independent set of vectors in $\mathbb{R}^n$ remains linearly independent in $\mathbb{C}^n$. In particular, any basis of $\mathbb{R}^n$ is a basis of $\mathbb{C}^n$ as well (because it is linearly independent over $\mathbb{C}$ and consists of n vectors).

For the standard basis of $\mathbb{R}^n$ this is hardly surprising, isn't it, but for other bases? (As a student the lecturer was puzzled by this fact, too, but finally he resolved it in the following way: Linear independence in $\mathbb{R}^n$ can be checked using Gaussian elimination, and the resulting computation remains valid over $\mathbb{C}$. Hence the answer must be the same for $\mathbb{R}^n$ and $\mathbb{C}^n$.)

As a second example consider again solutions (defined on $\mathbb{R}$) of the ODE $y'' + y = 0$. This ODE makes sense for C^2-functions $f \colon \mathbb{R} \to \mathbb{R}$ as well as $f \colon \mathbb{R} \to \mathbb{C}$.

Question: We know from an earlier lecture that $\cos x$, $\sin x$ form a basis of the real solution space. Can we conclude from this that $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i} \sin x$, $\mathrm{e}^{-\mathrm{i}x} = \cos x - \mathrm{i} \sin x$ form a basis of the complex solution space?

Examples (cont'd)

Answer: Yes, we can.

If $f\colon\mathbb{R}\to\mathbb{C}$ satisfies $f''+f=0$ then $u=\operatorname{Re}f$ and $v=\operatorname{Im}f$ must be solutions as well (to see this, substitute $f=u+\mathrm{i}v$ into the ODE and rearrange. Hence the complex solution space is spanned by real solutions, and $\cos x$, $\sin x$ form a basis of the complex solution space as well. Since $\cos x=\frac{1}{2}(\mathrm{e}^{\mathrm{i}x}+\mathrm{e}^{-\mathrm{i}x})$, $\sin x=\frac{1}{2\mathrm{i}}(\mathrm{e}^{\mathrm{i}x}-\mathrm{e}^{-\mathrm{i}x})$, it is then immediate that $\mathrm{e}^{\mathrm{i}x}$, $\mathrm{e}^{-\mathrm{i}x}$ is another basis of the complex solution space.

Of course you know this already (and in more generality) from an earlier lecture on linear ODE's with constant coefficients.

The Dimension Formula for Subspaces

There are two important operations on subspaces of a given vector space V/F. (The notation "V/F" is used as an abbreviation for "V is a vector space over F".)

Definition

For subspaces U_1, U_2 of V we set

$$\begin{aligned} U_1 \cap U_2 &= \{v \in V; v \in U_1 \wedge v \in U_2\}, \\ U_1 + U_2 &= \{x + y; x \in U_1, y \in U_2\}. \end{aligned}$$

The subspace $U_1 \cap U_2$ is called the *intersection* or *meet* of U_1, U_2, and the subspace $U_1 + U_2$ is called the *sum* or *join* of U_1, U_2.

Note

Clearly $U_1 \cap U_2$ is the largest subspace of V contained in both U_1 and U_2. Dually, $U_1 + U_2$ is the smallest subspace of V containing both U_1 and U_2 (because it is a subspace, as is easily verified, and any subspace containing U_1 and U_2 must contain all sums $x + y$ with $x \in U_1$, $y \in U_2$).

Exercise

Show that the union $U_1 \cup U_2$ of two subspaces U_1, U_2 of V is not a subspace except in the cases $U_1 \subseteq U_2$ or $U_2 \subseteq U_1$.

Exercise

Show that the meet and join operations on subspaces of a given vector space V satisfy the so-called *modular law*

$$(X + Y) \cap Z = X + (Y \cap Z) \quad \text{if } X \subseteq Z.$$

Exercise

Let $\mathcal{S}$ be a set of subspaces of a fixed vector space V/F. Show that

$$\bigcap \mathcal{S} = \bigcap_{S \in \mathcal{S}} S = \{x \in V; x \in S \text{ for all } S \in \mathcal{S}\}$$

is a subspace of V, and describe $\bigcap \mathcal{S}$ in terms of linear combinations.

Remark

This shows that for $X \subseteq V$ there is a smallest subspace of V containing X, viz., $\bigcap\{S;\ S \text{ is a subspace of } V \text{ with } S \supseteq X\}$. This subspace is called the *subspace generated by* X and denoted by $\langle X \rangle$ or $\mathrm{span}(X)$.

Theorem (Dimension formula for subspaces)

For subspaces U_1, U_2 of a finite-dimensional vector space V we have

$$\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim(U_1) + \dim(U_2).$$

Proof.

Writing $\dim(U_1) = r$, $\dim(U_2) = s$ and $\dim(U_1 \cap U_2) = t$, we must show $\dim(U_1 + U_2) = r + s - t$.

Choose a basis $A = \{a_1, \dots, a_t\}$ of $U_1 \cap U_2$ and augment it to bases $B = \{a_1, \dots, a_t, b_1, \dots, b_{r-t}\}$ of U_1 and $C = \{a_1, \dots, a_t, c_1, \dots, c_{s-t}\}$ of U_2. Then

$$|B \cup C| = t + (r - t) + (s - t) = r + s - t.$$

We will show that $B \cup C$ is a basis of $U_1 + U_2$.

Clearly every vector in $U_1 + U_2$ is a linear combination of the vectors in $B \cup C$.

Now suppose $\sum_{i=1}^{t} \lambda_i a_i + \sum_{j=1}^{r-t} \mu_j b_j + \sum_{k=1}^{s-t} \nu_k c_k = 0$ with $\lambda_i, \mu_j, \nu_k \in F$.

Proof cont'd.

$$\Longrightarrow \sum_{k=1}^{s-t} \nu_k c_k = -\sum_{i=1}^{t} \lambda_i a_i - \sum_{j=1}^{r-t} \mu_j b_j \in U_2 \cap U_1$$

$\Longrightarrow \sum_{k=1}^{s-t} \nu_k c_k$ is a linear combination of $a_1, \dots, a_t$.
The linear independence of $a_1, \dots, a_t, c_1, \dots, c_{s-t}$ then implies
$\nu_1 = \dots = \nu_{s-t} = 0$.
$\Longrightarrow \lambda_1 = \dots = \lambda_t = \mu_1 = \dots = \mu_{r-t} = 0$,
since $a_1, \dots, a_t, b_1, \dots, b_{r-t}$ is a basis of U_1 (and hence linearly independent).
In all we have shown that $B \cup C$ is linearly independent and hence a basis of $U_1 + U_2$. □

Example

For 2-dimensional subspaces E_1, E_2 of $\mathbb{R}^3$ (planes through the origin) we have

$$\dim(E_1 \cap E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 + E_2) = 4 - \dim(E_1 + E_2).$$

$E_1 \neq E_2$ Then $E_1 + E_2 = \mathbb{R}^3$ and $\dim(E_1 \cap E_2) = 1$, i.e., $E_1 \cap E_2$ is a line.

$E_1 = E_2$ Then $E_1, E_2, E_1 \cap E_2, E_1 + E_2$ are all equal, of course.

Better Example

The importance of the dimension formula can hardly be seen in the preceding example, because the dimension of $\mathbb{R}^3$ is too small.

Problem: Let $U = \langle \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3 \rangle$, $V = \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \rangle$ be the subspaces of $\mathbb{R}^5$ generated by the following vectors:

$$\mathbf{u}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \mathbf{u}_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \mathbf{u}_3 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \\ -1 \end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

Determine bases of $U \cap V$ and $U + V$.

Solution: It is readily checked (for example, by looking at the first 3 coordinates of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ and the last 3 coordinates of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$) that both spanning sets are linearly independent.
$\Longrightarrow$ $\dim(U) = \dim(V) = 3$ and $\dim(U_1 \cap U_2) = 2 \cdot 3 - \dim(U_1 + U_2)$ $\geq 6 - 5 = 1$. $\Longrightarrow$ The possibilities are:

$\dim(U_1 + U_2)$	5	4	3
$\dim(U_1 \cap U_2)$	1	2	3

Example (cont'd)

A basis of $U+V$ can be determined by setting $\mathbf{A}=(\mathbf{u}_1|\mathbf{u}_2|\mathbf{u}_3|\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)$, so that $U+V=\operatorname{csp}(\mathbf{A})$, and using one of the known methods to determine a basis of the column space of a matrix.

$\mathbf{v}\in\mathbb{R}^5$ is in $U\cap V$ iff there exist $\lambda_1,\lambda_2,\lambda_3,\mu_1,\mu_2,\mu_3\in\mathbb{R}$ such that

$$\begin{aligned} &\mathbf{v}=\lambda_1\mathbf{u}_1+\lambda_2\mathbf{u}_2+\lambda_3\mathbf{u}_3=\mu_1\mathbf{v}_1+\mu_2\mathbf{v}_2+\mu_3\mathbf{v}_3\\ \iff\ &(\mathbf{u}_1|\mathbf{u}_2|\mathbf{u}_3|-\mathbf{v}_1|-\mathbf{v}_2|-\mathbf{v}_3)\,(\lambda_1,\lambda_2,\lambda_3,\mu_1,\mu_2,\mu_3)^{\mathsf{T}}=\mathbf{0}\end{aligned}$$

and $\mathbf{v}=\lambda_1\mathbf{u}_1+\lambda_2\mathbf{u}_2+\lambda_3\mathbf{u}_3$, say.

Hence, using $\mathbf{A}'=(\mathbf{u}_1|\mathbf{u}_2|\mathbf{u}_3|-\mathbf{v}_1|-\mathbf{v}_2|-\mathbf{v}_3)$ instead (which has the same column space as $\mathbf{A}$), we can determine bases of $U+V$ and $U\cap V$ by applying Gaussian elimination to $\mathbf{A}'$. This requires only one pass of the algorithm.

Example (cont'd)

In what follows we have changed the order of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$, because this speeds up Gaussian elimination:

$$\mathbf{A}' = \left[\begin{array}{ccc|ccc} -1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & -2 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & 2 & 2 & -1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 & 1 \end{array}\right] \to \begin{bmatrix} -1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & -2 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & 2 & -2 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 & 1 \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & -2 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 \end{bmatrix} \to \begin{bmatrix} \boxed{-1} & -1 & 0 & -1 & 0 & 0 \\ 0 & \boxed{1} & 1 & -1 & -2 & -1 \\ 0 & 0 & \boxed{1} & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$\Longrightarrow$ A basis of $U + V$ is formed by the columns of $\mathbf{A}'$ corresponding to the pivot columns of the last matrix, i.e., by $\mathbf{u}_3, \mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_2$; in particular, $\dim(U + V) = 4$ and $\dim(U \cap V) = 2$.

For determining a basis of $U \cap V$ it suffices to compute the μ-part of 2 linearly independent solutions of $\mathbf{A}'\mathbf{x} = \mathbf{0}$.

Example (cont'd)

Setting the free variables (μ_1, μ_3) to $(1, 0)$ and $(0, 1)$ gives $(\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3) = (*, *, *, 1, 0, 0)$ and $(*, *, *, 0, -1, 1)$, respectively.

$\Longrightarrow$ A basis of $U \cap V$ is formed by the vectors

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{and} \quad -\mathbf{v}_2 + \mathbf{v}_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Remark

One can also use column-oriented Gaussian elimination on the matrix $\begin{pmatrix} \mathbf{A}' \\ \mathbf{I} \end{pmatrix}$ to determine bases of the column space and the right kernel of $\mathbf{A}'$ (cf. Exercise H18 of Calculus III). Exploiting the observation that not all rows of $\begin{pmatrix} \mathbf{A}' \\ \mathbf{I} \end{pmatrix}$ are needed for the present purpose, this takes roughly the same effort.

Direct Sums

Definition

A vector space V is said to be the (internal) *direct sum* of subspaces U_1, U_2 (notation $V = U_1 \oplus U_2$) if $U_1 \cap U_2 = \{0\}$ and $U_1 + U_2 = V$.

In this case the dimension formula yields $\dim(V) = \dim(U_1) + \dim(U_2)$.

Theorem

Let V/F be a vector space and U_1, U_2 subspaces of V with bases B_1 and B_2, respectively. The following are equivalent:

1. $V = U_1 \oplus U_2$;
2. *every* $v \in V$ *has a unique representation* $v = x + y$ *with* $x \in U_1, y \in U_2$;
3. $B_1 \cap B_2 = \emptyset$ *and* $B = B_1 \cup B_2$ *is a basis of* V.

Proof.

(1)$\Longrightarrow$(2): Since $V = U_1 + U_2$, there exists at least one such representation.

Suppose $v = x + y = x' + y'$ with $x, x' \in U_1$ and $y, y' \in U_2$.

$\Longrightarrow x - x' = y' - y \in U_1 \cap U_2 = \{0\} \Longrightarrow x = x' \wedge y = y'$

Proof cont'd.

(2)$\Longrightarrow$(3): If there existed $b \in B_1 \cap B_2$, we would have the two representations $b = b + 0 = 0 + b$ (these are distinct, since basis vectors are always nonzero), contradicting (2).

From (2) we have $V = U_1 + U_2 = \langle B_1 \rangle + \langle B_2 \rangle = \langle B \rangle$.

If B were linearly dependent, $\sum_{i=1}^{r} \lambda_i b_i + \sum_{j=1}^{s} \lambda_j' b_j' = 0$ with $b_i \in B_1$, $b_j \in B_2$ and $\lambda_i, \lambda_j' \in F$ not all zero, we would have $x = \sum_{i=1}^{r} \lambda_i b_i \neq 0$ (since B_1 is linearly independent), and similarly for y, and thus arrive at a second representation $0 = x + y \in U_1 + U_2$ in addition to $0 = 0 + 0$. Contradiction.

(3)$\Longrightarrow$(1): $V = \langle B \rangle = \langle B_1 \rangle + \langle B_2 \rangle = U_1 + U_2$

If $v \in U_1 \cap U_2$ then $v = \sum_{i=1}^{r} \lambda_i b_i = \sum_{j=1}^{s} \lambda_j' b_j'$ for some $b_i \in B_1$, $b_j' \in B_2$ and $\lambda_i, \lambda_j' \in F$, and the linear independence of B together with $B_1 \cap B_2 = \emptyset$ implies $\lambda_i = \lambda_j' = 0$ for all i and j, i.e., $v = 0$. □

Examples

1. $\mathbb{R}^n$ is the direct sum of two subspaces in various ways, for example $\mathbb{R}^n = U_1 \oplus U_2$, where
$U_1 = \bigl\{(x_1, \dots, x_k, 0, \dots, 0); x_i \in \mathbb{R}\bigr\}$,
$U_2 = \bigl\{(0, \dots, 0, x_{k+1}, \dots, x_n); x_i \in \mathbb{R}\bigr\}$, and $0 \leq k \leq n$.
A less trivial example is $\mathbb{R}^n = H_0 \oplus \mathbb{R}(1, 1, \dots, 1)$, where

$$H_0 = \{\mathbf{x} \in \mathbb{R}^n; x_1 + x_2 + \dots + x_n = 0\}.$$

Reason: A vector $\lambda(1, \dots, 1) \in \mathbb{R}(1, \dots, 1)$ has entry sum $\lambda + \dots + \lambda = n\lambda = 0 \iff \lambda = 0$, showing $H_0 \cap \mathbb{R}(1, \dots, 1) = \{\mathbf{0}\}$, and every $\mathbf{x} \in \mathbb{R}^n$ admits the following decomposition with $s = x_1 + \dots + x_n$:

$$\mathbf{x} = \underbrace{\left(x_1 - \frac{s}{n}, \dots, x_n - \frac{s}{n}\right)}_{\in H_0} + \frac{s}{n}(1, \dots, 1)$$

A similar decomposition exists for any vector $\mathbf{v} \in \mathbb{R}^n \setminus H_0$, showing that $\mathbb{R}^n = H_0 \oplus \mathbb{R}\mathbf{v}$ in this more general case; cf. also the accompanying exercises.

Examples (cont'd)

2. The matrix space $\mathbb{R}^{n\times n}$ is the direct sum of the two subspaces

$$S=\{\mathbf{A}\in\mathbb{R}^{n\times n};\mathbf{A}^{\mathsf{T}}=\mathbf{A}\},\quad T=\{\mathbf{A}\in\mathbb{R}^{n\times n};\mathbf{A}^{\mathsf{T}}=-\mathbf{A}\}.$$

The non-obvious part $\mathbb{R}^{n\times n}=S+T$ follows from

$$\mathbf{A}=\underbrace{\tfrac{1}{2}\left(\mathbf{A}+\mathbf{A}^{\mathsf{T}}\right)}_{\in S}+\underbrace{\tfrac{1}{2}\left(\mathbf{A}-\mathbf{A}^{\mathsf{T}}\right)}_{\in T}.$$

The matrices in S, T are called *symmetric* and *skew-symmetric*, respectively.

3. The function space $\mathbb{R}^{\mathbb{R}}=\{f;f\colon\mathbb{R}\to\mathbb{R}\}$ is the direct sum of the subspaces of even and odd functions, viz.

$$E=\left\{f\in\mathbb{R}^{\mathbb{R}};f(x)=f(-x)\text{ for all }x\in\mathbb{R}\right\},$$
$$O=\left\{f\in\mathbb{R}^{\mathbb{R}};f(x)=-f(-x)\text{ for all }x\in\mathbb{R}\right\}.$$

This follows from $f(x)=\underbrace{\tfrac{1}{2}\big(f(x)+f(-x)\big)}_{\in E}+\underbrace{\tfrac{1}{2}\big(f(x)-f(-x)\big)}_{\in O}.$

External direct sums

If V_1, V_2 are vector spaces over F, we can turn the cartesian product $V_1 \times V_2 = \{(x,y); x \in V_1, y \in V_2\}$ into a vector space over F by defining the operations componentwise: $(x,y) + (x',y') = (x+x', y+y')$, $a(x,y) = (ax, ay)$ for $x, x' \in V_1$, $y, y' \in V_2$ and $a \in F$. The space $(V_1 \times V_2)/F$ is called *external direct sum* of V_1 and V_2.

It is easy to see that $V_1 \times V_2 = (V_1 \times \{0\}) \oplus (\{0\} \times V_2)$ is the internal direct sum of the subspaces $V_1 \times \{0\} \cong V_1$, $\{0\} \times V_2 \cong V_2$, and hence external and internal sums are in a way equivalent concepts.

More than two summands

(Internal) Direct sums of subspaces $U_1, U_2, \dots, U_r$ are defined in such a way that $V = U_1 \oplus U_2 \oplus \dots \oplus U_r$ iff every $v \in V$ has a unique representation $v = x_1 + x_2 + \dots + x_r$ with $x_i \in U_i$ for $1 \leq i \leq r$. The correct generalization of the condition $U_1 \cap U_2 = \{0\}$ to $r > 2$ summands is $U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\}$ for $1 \leq i \leq r$ (and not merely $U_i \cap U_j = \{0\}$ for $i \neq j$, as one might think in the first place).

Exercise

Show that in the finite-dimensional case $\dim(V) = n$ any two of the following properties imply the third property (and are equivalent to $V = U_1 \oplus U_2$):

1. $U_1 \cap U_2 = \{0\}$;
2. $U_1 + U_2 = V$;
3. $\dim(U_1) + \dim(U_2) = \dim(V)$.

Exercise

Investigate the analogue of the direct sum decomposition $\mathbb{R}^n = H_0 + \mathbb{R}(1, \dots, 1)$, cf. Example 1, for the spaces $\mathbb{F}_2^n$. The binary analogue of H_0 is called the *(full) even-weight code* of length n. Can you explain this terminology?

Exercise

Show that there exist subspaces U_1, U_2, U_3 of $\mathbb{R}^2$ such that $U_i \cap U_j = \{0\}$ for $1 \leq i < j \leq 3$, but the representation of $\mathbf{v} \in \mathbb{R}^2$ as $\mathbf{v} = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3$ with $\mathbf{x}_i \in U_i$ is not unique.

Linear Maps

First recall the following

Definition

Let V and W be vector spaces over the same field F. A map $f\colon V \to W$ is said to be *linear* (or F-linear, if the particular field needs to be emphasized) if

$$f(x+y) = f(x)+f(y), \quad f(ax) = a\,f(x) \quad \text{for all } x, y \in V \text{ and } a \in F.$$

A linear map $f\colon V \to W$, W is also referred to as a (vector space) *homomorphism*. Further, f is said to be an *endomorphism* if $V = W$, a *monomorphism* if f is injective, an *epimorphism* if f is surjective, an *isomorphism* if f bijective, and an *automorphism* if f is an isomorphism and $V = W$.

Proposition (Properties of linear maps)

Suppose V/F, W/F are vector spaces, B is a basis of V, and $f\colon V \to W$ is linear.

1. $f(0_V) = 0_W$
2. *For any subspace S of V, the image $f(S) = \{f(x); x \in S\}$ is a subspace of W.*
3. *For any subspace T of W, the preimage $f^{-1}(T) = \{x \in V; f(x) \in T\}$ is a subspace of V.*
4. *f is completely determined by the images $f(b)$, $b \in B$, and conversely an assignment of images $f(b) \in W$ for all $b \in B$ is realized by a (unique) linear map.*

Proof.

(1) We have $f(0_V) = f(0_V + 0_V) = f(0_V) + f(0_V)$. Adding the inverse $-f(0_V)$ on both sides gives $f(0_V) = 0_W$.

(2) and (3) are easily proved using the subspace test.

(4) Observe that $f\left(\sum_{i=1}^{r} \lambda_i b_i\right) = \sum_{i=1}^{r} \lambda_i f(b_i)$ for $r \in \mathbb{N}$, $b_i \in B$, $\lambda_i \in F$. This proves the first assertion.

Proof cont'd.

Conversely, suppose that for each $b \in B$ an image $f(b) \in W$ has been preassigned. Since any $v \in V$ has a unique representation $v = \sum_{i=1}^{r} \lambda_i b_i$ as linear combination of the basis vectors in B, we can define $f(v)$ as $\sum_{i=1}^{r} \lambda_i f(b_i)$. It is then readily checked that with this definition f is indeed a linear map from V to W. □

Linear maps from V to W can be added and multiplied with scalars point-wise, i.e., $(f+g)(x) = f(x) + g(x)$, $(af)(x) = a\,f(x)$ for $f, g \colon V \to W$, $x \in V$, $a \in F$. The resulting maps $f + g \colon V \to W$ and $af \colon V \to W$ are again linear, and the set of all linear maps from V to W forms a vector space over F with respect to these operations. This vector space is denoted by $\mathrm{Hom}(V, W)$.

Theorem

If V, W are finite-dimensional then $\dim \mathrm{Hom}(V, W) = (\dim V)(\dim W)$.

Note

We have seen earlier (in Calculus III) that linear maps $f \colon \mathbb{R}^n \to \mathbb{R}^m$ are in 1-1 correspondence with matrices $\mathbf{A} \in \mathbb{R}^{m \times n}$ via $f(\mathbf{x}) = \mathbf{A}\mathbf{x}$. Since $\dim(\mathbb{R}^{m\times n}) = mn = (\dim \mathbb{R}^n)(\dim \mathbb{R}^m)$, this result is hardly surprising.

Proof of the theorem.

Let $B = \{b_1, \dots, b_n\}$, $C = \{c_1, \dots, c_m\}$ be bases of V and W, respectively, and define $\delta_{ij} \in \mathrm{Hom}(V, W)$ by

$$\delta_{ij}(b_k) = \begin{cases} c_i & \text{if } k = j, \\ 0 & \text{if } k \neq j. \end{cases}$$

We show that $\{\delta_{ij}; 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of $\mathrm{Hom}(V, W)$.

Let $f\colon V \to W$ be a linear map. There exist $a_{ij} \in F$ such that $f(b_j) = \sum_{i=1}^n a_{ij} c_i$ for $1 \leq j \leq n$. Now consider the map $g = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\delta_{ij}$.

$$g(b_k) = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\delta_{ij}(b_k) = \sum_{i=1}^m a_{ik} c_i = f(b_k)$$

$\Longrightarrow g = f$; cf. Part (4) of the preceding proposition. This shows $\mathrm{Hom}(V, W) = \langle \delta_{ij} \rangle$.

Finally suppose $\sum_{i=1}^m \sum_{j=1}^n a_{ij}\delta_{ij} = 0$ (the all-zero map from V to W) for some $a_{ij} \in F$. Evaluating this map at b_k gives $\sum_{i=1}^m a_{ik} c_i = 0$. Since C is linearly independent, this implies $a_{ik} = 0$ for all i, k, completing the proof. □

Exercise

1. Suppose U, V, W are vector spaces over the same field F and $f\colon U \to V$, $g\colon V \to W$ are linear maps. Show that the composition $g \circ f\colon U \to W$ is linear as well.

2. Show that the inverse function $f^{-1}\colon W \to V$ of a bijective linear map $f\colon V \to W$ is linear as well.

3. Consider $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ with respect to the operations $(f, g) \to f + g$ (addition) and $(f, g) \mapsto f \circ g$ (multiplication). Which of the 10 field axioms does this structure satisfy?

   Note: First make appropriate choices for the distinguished elements 0, 1.

The Dimension Formula for Linear Maps

Definition

Let $f\colon V\to W$ be a linear map. The subspace

$$f^{-1}\bigl(\{0_W\}\bigr)=\bigl\{x\in V; f(x)=0_W\bigr\}$$

is called the *kernel* of f and denoted by $\ker f$.

Theorem (Dimension formula for linear maps)

Let V/F be a finite-dimensional vector space and $f\colon V\to W$ be a linear map from V to another vector space W/F. Then the range $f(V)$ is also finite-dimensional, and we have

$$\dim V=\dim(\ker f)+\dim f(V).$$

Note

$\dim(\ker f)$ is also referred to as the *nullity* of f, $\dim f(V)$ as the *rank* of f, and the dimension formula as *rank-nullity* formula.

Proof.

Suppose $\dim(V) = n$. The range $f(V)$ is generated by the images $f(b_1), \dots, f(b_n)$ of a basis $\{b_1, \dots, b_n\}$ of V, implying $m = \dim f(V) \leq n$. In particular $f(V)$ is finite-dimensional.

Let $K = \ker f$, $C = \{c_1, \dots, c_m\}$ a basis of $f(V)$ and $L = \langle v_1, \dots, v_m \rangle$ the subspace generated by a fixed preimage of C (i.e., $f(v_j) = c_j$ for $1 \leq j \leq m$). It suffices to show $V = K \oplus L$.

For $v \in V$ there exist $\lambda_i \in F$ such that

$$f(v) = \sum_{i=1}^{m} \lambda_i c_i = \sum_{i=1}^{m} \lambda_i f(v_i) = f\left(\sum_{i=1}^{m} \lambda_i v_i\right).$$

$\implies f\left(v - \sum_{i=1}^{m} \lambda_i v_i\right) = 0$
$\implies v - \sum_{i=1}^{m} \lambda_i v_i \in K$
$\implies V = K + L.$

Suppose $v \in K \cap L$. Then $v = \sum_{i=1}^{m} \lambda_i v_i$ for some $\lambda_i \in F$.

$$0 = f(v) = f\left(\sum_{i=1}^{m} \lambda_i v_i\right) = \sum_{i=1}^{m} \lambda_i f(v_i) = \sum_{i=1}^{m} \lambda_i c_i$$

$\implies \lambda_i = 0$ for $1 \leq i \leq m \implies v = 0 \implies K \cap L = \{0\}.$ □

For linear maps we have a handy injectivity test:

Lemma

A linear map $f\colon V \to W$ is injective iff $\ker f = \{0\}$.

Proof.

Suppose $\ker f = \{0\}$ and $f(x) = f(y)$.

$\Longrightarrow 0 = f(x) - f(y) = f(x - y)$, i.e., $x - y \in \ker f$.

$\Longrightarrow x - y = 0 \Longrightarrow x = y$.

This proves the if-part. The only-if-part is obvious. □

The dimension formula for linear maps has the following important

Corollary

Suppose V and W are finite-dimensional vector spaces over F of the same dimension and $f\colon V \to W$ is linear. Then the following are equivalent:

1. *f is injective;*
2. *f is surjective;*
3. *f is bijective.*

Proof.

We only need to show “(1) $\Longleftrightarrow$ (2)”.

Proof cont'd.

(1)$\Longrightarrow$(2): We have

$$\dim W = \dim V = \dim(\ker f) + \dim f(V) = \dim f(V),$$

since $\ker f = \{0\}$. But $f(V) \subseteq W$ and $\dim f(V) = \dim W$ imply $f(V) = W$, as we have seen earlier. Thus f is surjective.

(2)$\Longrightarrow$(1): Since $f(V) = W$, the dimension formula implies conversely that $\dim(\ker f) = 0$. Hence $\ker f = \{0\}$, and f is injective. □

Examples of Linear Maps

Examples of linear maps are abound. We discuss only a small selection.

Example (Matrix-vector multiplication)

Recall that every linear map (more precisely, $\mathbb{R}$-linear map) from $\mathbb{R}^n$ to $\mathbb{R}^m$ has the form $f_{\mathbf{A}} \colon \mathbb{R}^n \to \mathbb{R}^m$, $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$. We now apply the dimension formula to such maps:

$\ker(f_{\mathbf{A}}) = \{\mathbf{x} \in \mathbb{R}^n; \mathbf{A}\mathbf{x} = \mathbf{0}\}$ is the solution space of the homogeneous linear system of equations with coefficient matrix **A**.

$f_{\mathbf{A}}(\mathbb{R}^n) = \{\mathbf{A}\mathbf{x}; \mathbf{x} \in \mathbb{R}^n\} = \operatorname{csp}(\mathbf{A})$ is the column space of **A**, and hence $\dim f_{\mathbf{A}}(\mathbb{R}^n)$ is equal to the rank of **A**.

The dimension formula says

$$\begin{aligned} n &= \dim\{\mathbf{x} \in \mathbb{R}^n; \mathbf{A}\mathbf{x} = \mathbf{0}\} + \operatorname{rk}(\mathbf{A}) \\ &= \dim \operatorname{rker}(\mathbf{A}) + \operatorname{rk}(\mathbf{A}), \end{aligned}$$

which is nothing but the well-known fact that the number of basis solutions of $\mathbf{A}\mathbf{x} = \mathbf{0}$ ($\triangleq$ free variables) and the number of pivots of **A** add up to n (cf. the Calculus III lecture).

Example (Vector-matrix multiplication)

Viewing vectors as row vectors, $\mathbf{A} \in \mathbb{R}^{m\times n}$ also gives rise to the linear map $g\colon \mathbb{R}^m \to \mathbb{R}^n$, $\mathbf{x} \mapsto \mathbf{xA}$. Here $\ker g = \{\mathbf{x} \in \mathbb{R}^m; \mathbf{xA} = \mathbf{0}\} = \operatorname{lker}(\mathbf{A})$ (the left kernel of $\mathbf{A}$) and $g(\mathbf{A}) = \{\mathbf{xA}; \mathbf{x} \in \mathbb{R}^m\} = \operatorname{rsp}(\mathbf{A})$ (the row space of $\mathbf{A}$), which has the same dimension as $\operatorname{csp}(\mathbf{A})$.

$\Longrightarrow$ The dimension formula also says

$$m = \dim \operatorname{lker}(\mathbf{A}) + \operatorname{rk}(\mathbf{A}).$$

Alternatively, matrix transposition $\mathbf{A} \to \mathbf{A}^{\mathsf{T}}$ can be used to derive this formula from the one in the previous example.

Example (Differentiation)

Let V be the subspace of $\mathbb{R}^{\mathbb{R}}$ consisting of the (everywhere) differentiable functions $f\colon \mathbb{R} \to \mathbb{R}$, and consider $\mathrm{D}\colon V \to \mathbb{R}^{\mathbb{R}}$, $f \mapsto f'$.

The rules for differentiating functions from Calculus I give in particular that D is a linear map.

The kernel of D consists of all constant functions $f(t) \equiv c \in \mathbb{R}$. Thus $\ker \mathrm{D}$ is generated by $f(t) \equiv 1$ and has dimension 1.

The range of D is not equal to V, because there exist functions which are differentiable only once. (In fact, V is properly contained in the range of D, because every differentiable function has an antiderivative.

Restricting the domain of D to the subspace $W = \mathrm{C}^\infty(\mathbb{R}) \subset V$ of functions which have derivatives of all orders, we obtain a linear map $\mathrm{D}\colon W \to W$.
In fact $\mathrm{D}(W) = W$ (check it!), i.e., D induces a surjective (but not injective) endomorphism of W.

Since domain and range of D have infinite dimension, we can't apply the dimension formula for linear maps.

Example (cont'd)

However, if we restrict D to a finite-dimensional subspace U of V, we can apply the dimension formula to $\mathrm{D}|_U \colon U \to \mathbb{R}^{\mathbb{R}}$.

For example, take U as the space P_2 of polynomial functions $a(x) = a_0 + a_1 x + a_2 x^2$ ($a_i \in \mathbb{R}$). Then $(\mathrm{D}a)(x) = a_1 + 2a_2 x$, so D has range $P_1 = \{x \mapsto b_0 + b_1 x; b_0, b_1 \in \mathbb{R}\}$.
The dimension formula gives

$$3 = \dim P_2 = \dim(\ker \mathrm{D}|_U) + \dim P_1 = \dim(\ker \mathrm{D}|_U) + 2,$$

so $\ker(\mathrm{D}|_U)$ should have dimension 1.
In fact $\ker(\mathrm{D}|_U)$ consists of the constant functions (which are polynomial), and is spanned by $x \mapsto 1$.

In general there are two possible cases for $K = \ker(\mathrm{D}_U)$:

1. If U contains the constant functions (i.e., U contains $x \mapsto 1$) then $\dim K = 1$ and $\dim \mathrm{D}(U) = \dim U - 1$.
2. If U does not contain the constant functions then $K = \{0\}$ and D induces a bijection from U onto $\mathrm{D}(U)$.

Note that $K = \ker(\mathrm{D}_U) = \big\{f \in U; \mathrm{D}f = 0\big\} = \ker(D) \cap U$.

The preceding example easily generalizes to complex-valued functions on $\mathbb{R}$ and functions on intervals $I \subset \mathbb{R}$.

Example (Polynomial differential operators)

Suppose $n \in \mathbb{N}$ and $p(X) = \sum_{i=0}^{n} p_i X^i \in \mathbb{C}[X]$ has degree n. The polynomial differential operator $p(\mathrm{D})$ associated with $p(X)$ was defined as the map

$$p(\mathrm{D})\colon\, f \mapsto p_n f^{(n)} + p_{n-1} f^{(n-1)} + \cdots + p_1 f' + p_0 f, \quad \text{i.e., as}$$

$\bigl(p(\mathrm{D})f\bigr)(t) = p_n f^{(n)}(t) + p_{n-1} f^{(n-1)}(t) + \cdots + p_1 f'(t) + p_0 f(t)$ for $t \in \mathbb{R}$. The domain of $p(\mathrm{D})$ can be taken as the vector space $\mathrm{C}^n(\mathbb{R})$ (over the field $\mathbb{C}$) of n times continuously differentiable functions $f\colon \mathbb{R} \to \mathbb{C}$ (and the codomain as $\mathbb{C}^{\mathbb{R}}$).

The range of $p(\mathrm{D})$ is $\mathrm{C}^{(0)}(\mathbb{R})$ (the subspace of $\mathbb{C}^{\mathbb{R}}$ consisting of the continuous functions).

The map $p(\mathrm{D})$ is $\mathbb{C}$-linear, and the kernel of $p(\mathrm{D})$ is precisely the solution space of the time-independent homogeneous linear ODE

$$p_n y^{(n)} + p_{n-1} y^{(n-1)} + \cdots + p_1 y' + p_0 y = 0.$$

From the general theory we know $\dim\bigl(\ker p(\mathrm{D})\bigr) = n$, but domain and range of $p(\mathrm{D})$ have infinite dimension.

Example (cont'd)

For a continuous function $b\colon \mathbb{R} \to \mathbb{C}$ the inhomogeneous ODE

$$p_n y^{(n)} + p_{n-1} y^{(n-1)} + \cdots + p_1 y' + p_0 y = b(t)$$

is solvable iff b is in the range of $p(\mathrm{D})$, say $p(\mathrm{D})y_{\mathrm{p}} = b(t)$, and if this is the case then the set of all solutions ("general solution") is precisely the coset

$$y_{\mathrm{p}} + \ker p(\mathrm{D}) = \bigl\{ y_{\mathrm{p}} + y_{\mathrm{h}} ; y_{\mathrm{h}} \in \ker p(\mathrm{D}) \bigr\}.$$

Now we re-examine the derivation of the main results for time-independent linear ODE's in the Linear Algebra setting. For this we switch notation back to that used earlier and consider the time-independent linear ODE $a(\mathrm{D})y = 0$ with characteristic polynomial $a(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$.

The key idea used in the proofs was the factorization

$$a(\mathrm{D})y = (\mathrm{D} - \lambda_1 \mathrm{id})(\mathrm{D} - \lambda_2 \mathrm{id}) \cdots (\mathrm{D} - \lambda_n \mathrm{id}) y = 0,$$

where $\lambda_i \in \mathbb{C}$ are the roots of $a(X)$ counted with their multiplicity.

Example (cont'd)

This time we will not use the rather advanced Existence and Uniqueness Theorem but only the elementary fact that the kernel of $\mathrm{D}-\lambda\mathrm{id}$ is 1-dimensional and spanned by $\mathrm{e}^{\lambda t}$. For this recall that the 1st-order linear ODE $(\mathrm{D}-\lambda\mathrm{id})y = y' - \lambda y = 0$ has general solution $y(t) = c\,\mathrm{e}^{\lambda t}$, $c \in \mathbb{C}$.

The map $\mathrm{D}-\lambda\mathrm{id}$ is $\mathbb{C}$-linear and acts on the subspace

$$E = \left\langle t^k\mathrm{e}^{\mu t}; k \in \mathbb{N}, \mu \in \mathbb{C}\right\rangle$$

consisting of the exponential polynomials by

$$(\mathrm{D}-\lambda\mathrm{id})[t^k\mathrm{e}^{\mu t}] = \left(kt^{k-1} + (\mu-\lambda)t^k\right)\mathrm{e}^{\mu t}.$$

(Because the exponential monomials $t^k\mathrm{e}^{\mu t}$ form a basis of E, this specifies the action of $\mathrm{D}-\lambda\mathrm{id}$ on E completely.)

Now $E = \bigoplus_{\mu\in\mathbb{C}} E(\mu)$ is the direct sum of the subspaces $E(\mu) = \{t^k\mathrm{e}^{\mu t}; k \in \mathbb{N}\}$, which are mapped by D onto itself: $\mathrm{D}-\lambda\mathrm{id}$ acts on $E(\mu)$, $\mu \neq \lambda$, as a bijection (since it preserves the degree of the polynomial factor) and like polynomial differentiation, viz. $t^k\mathrm{e}^{\lambda t} \mapsto kt^{k-1}\mathrm{e}^{\lambda t}$, on $E(\lambda)$. $\implies \mathrm{D}-\lambda\mathrm{id}\colon E \to E$ is surjective.

Example (cont'd)

$\Longrightarrow$ $a(D)$ is surjective (since a composition of surjective maps is surjective.)

In other words, if $b(t) \in E$ is an exponential polynomial then $a(\mathrm{D})y = b(t)$ is solvable in E. This re-establishes the main result for the inhomogeneous case derived earlier (using essentially the same proof). The proper „Ansatz“ for actually computing a solution in the monomial case $b(t) = t^k \mathrm{e}^{\mu t}$ can also be seen from this.

Secondly, we show by induction on $n = \deg a(X)$ that

$$\ker a(\mathrm{D}) \subset E \quad \text{and} \quad \dim\bigl(\ker a(\mathrm{D})\bigr) = n.$$

This re-establishes the main result for the homogeneous case without relying on the Existence and Uniqueness Theorem. (Again the proof can be easily extended to yield a fundamental system of solutions.)

For $n = 0$ this is trivially true. For $n \geq 1$ we can write $a(X) = (X - \lambda)b(X)$ and apply the inductive hypothesis to $b(X)$.
Let $\{y_1, \dots, y_{n-1}\} \subset E$ be a basis of $\ker b(\mathrm{D})$.
Since $b(\mathrm{D})\colon E \to E$ is surjective, there exists $y_n \in E$ such that $b(\mathrm{D})y_n = \mathrm{e}^{\lambda t}$.
$\Longrightarrow$ $y_1, \dots, y_{n-1}, y_n$ are in $\ker a(\mathrm{D})$ and linearly independent.

Example (cont'd)

It remains to show that $y_1, \dots, y_n$ span $\ker a(\mathrm{D})$.
Suppose $a(\mathrm{D})y = (\mathrm{D} - \lambda\mathrm{id})b(\mathrm{D})y = 0$.
Then $b(\mathrm{D})y \in \ker(\mathrm{D} - \lambda\mathrm{id})$ and there exists $c \in \mathbb{C}$ such that $b(\mathrm{D})y = c\,\mathrm{e}^{\lambda t} = b(\mathrm{D})[c\,y_n]$.
$\implies y - c\,y_n \in \ker b(\mathrm{D}) = \langle y_1, \dots, y_{n-1} \rangle$
$\implies y \in \langle y_1, \dots, y_{n-1}, y_n \rangle$
This completes the proof.

Example

We determine $\int(1+x+x^2)\mathrm{e}^x\,\mathrm{d}x$ using Linear Algebra.

The problem is equivalent to finding a differentiable function $f\colon\mathbb{R}\to\mathbb{R}$ satisfying $(\mathrm{D}f)(x)=(1+x+x^2)\mathrm{e}^x\,\mathrm{d}x$.

Our Calculus I knowledge suggests that f is a linear combination of e^x, $x\mathrm{e}^x$, $x^2\mathrm{e}^x$.

$$\begin{aligned}\mathrm{D}(\mathrm{e}^x)&=\mathrm{e}^x,\\ \mathrm{D}(x\,\mathrm{e}^x)&=\mathrm{e}^x+x\,\mathrm{e}^x,\\ \mathrm{D}(x^2\mathrm{e}^x)&=2x\mathrm{e}^x+x^2\mathrm{e}^x.\end{aligned}$$

$\Longrightarrow$ D maps the subspace $\langle\mathrm{e}^x,x\mathrm{e}^x,x^2\mathrm{e}^x\rangle$ bijectively onto itself, and we can solve

$$\begin{aligned}(1+x+x^2)\mathrm{e}^x&=\mathrm{D}(c_1\mathrm{e}^x+c_2x\mathrm{e}^x+c_3x^2\mathrm{e}^x)\\ &=c_1\mathrm{e}^x+c_2(\mathrm{e}^x+x\mathrm{e}^x)+c_3(2x\mathrm{e}^x+x^2\mathrm{e}^x)\\ &=(c_1+c_2)\mathrm{e}^x+(c_2+2c_3)x\mathrm{e}^x+c_3x^2\mathrm{e}^x.\end{aligned}$$

The solution is $c_3=1$, $c_2=-1$, $c_1=2$, and hence $\int(1+x+x^2)\mathrm{e}^x\,\mathrm{d}x=(2-x+x^2)\mathrm{e}^x$.

Example (Numerical Integration)

For evaluating an integral $\int_a^b f(x)\,\mathrm{d}x$ numerically with a certain accuracy, we can sample f at points $x_1 < x_2 < \cdots < x_n$ in the domain $[a,b]$ and use a weighted average of $f(x_i)$ as approximation:

$$\int_a^b f(x)\,\mathrm{d}x \approx \sum_{i=1}^n A_i f(x_i) \quad \text{for certain weights } A_i \in \mathbb{R}.$$

Problem: How to determine the sample points and the weights?

A reasonable approach is to demand that the approximation is exact for well-known functions f, for example for $f(x) = 1$, x, x^2, etc. Since the approximation formula involves the $2n$ unknowns x_i, A_i, we may be able to solve

$$\int_a^b x^k\,\mathrm{d}x = \sum_{i=1}^n A_i f(x_i) \quad \text{for } 0 \leq k \leq 2n-1. \tag{$\star$}$$

Important observation: Since $\mathrm{I}(f) = \int_a^b f(x)\,\mathrm{d}x$ and $\mathrm{S}(f) = \sum_{i=1}^n A_i f(x_i)$ are both linear maps, the conditions $(\star)$ ensure that the approximation will be exact for all polynomials of degree $\leq 2n-1$ (the span of $1, x, \dots, x^{2n-1}$).

$n = 1$ Here the conditions ($\star$) are

$$A_1 = \int_a^b 1\,\mathrm{d}x = b - a,$$

$$A_1 x_1 = \int_a^b x\,\mathrm{d}x = \tfrac{1}{2}(b^2 - a^2).$$

The unique solution is $\mathrm{S}(f) = (b-a)\cdot f\left(\frac{a+b}{2}\right)$ (*midpoint rule*).

$n = 2$ Here we have 4 conditions:

$$A_1 + A_2 = \int_a^b 1\,\mathrm{d}x = b - a,$$

$$A_1 x_1 + A_2 x_2 = \int_a^b x\,\mathrm{d}x = \tfrac{1}{2}(b^2 - a^2),$$

$$A_1 x_1^2 + A_2 x_2^2 = \int_a^b x\,\mathrm{d}x = \tfrac{1}{3}(b^3 - a^3),$$

$$A_1 x_1^3 + A_2 x_2^3 = \int_a^b x\,\mathrm{d}x = \tfrac{1}{4}(b^4 - a^4).$$

Again there is a unique solution, but it is more tedious to find; cf. the subsequent exercise.

Exercise

For fixed $\mu_0, \mu_1, \mu_2, \mu_3 \in \mathbb{R}$ consider the system of equations

$$A_1 x_1^k + A_2 x_2^k = \mu_k, \quad 0 \leq k \leq 3,$$

for the unknowns x_1, x_2, A_1, A_2.

a) Show that

$$\begin{aligned} \mu_2 - (x_1 + x_2)\mu_1 + x_1 x_2 \mu_0 &= 0, \\ \mu_3 - (x_1 + x_2)\mu_2 + x_1 x_2 \mu_1 &= 0. \end{aligned}$$

b) Assuming $\mu_1^2 - \mu_0\mu_2 \neq 0$, express $\sigma_1 = x_1 + x_2$ and $\sigma_2 = x_1 x_2$ in terms of μ_k.

c) Show that under the assumption in b) the system has a unique solution.

d) Apply this to the preceding example and compute the sample points x_1, x_2 and weights A_1, A_2 for

$$\int_{-1}^{1} f(x)\,\mathrm{d}x \approx A_1 f(x_1) + A_2 f(x_2).$$

Review Question

Determine the ranks of the following matrices over $\mathbb{F}_2$:

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad \mathbf{A}_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Answer

Since $\mathbf{A}_3$ is a submatrix of $\mathbf{A}_2$ and $\mathbf{A}_2$ is a submatrix of $\mathbf{A}_1$, we have $\operatorname{rk}(\mathbf{A}_3) \leq \operatorname{rk}(\mathbf{A}_2) \leq \operatorname{rk}(\mathbf{A}_1) \leq 3$.

$\operatorname{rk}(\mathbf{A}_1) = 3$, since $\mathbf{A}_1$ contains an invertible 3×3 submatrix (the 3×3 identity matrix).

$\operatorname{rk}(\mathbf{A}_3) = 2$, since the columns (or the rows) of $\mathbf{A}_3$ are distinct and sum to zero.

$\operatorname{rk}(\mathbf{A}_2) = 3$, since $(1,1,1)^{\mathsf{T}}$ is not in the column space of $\mathbf{A}_3$, which contains the $2^2 = 4$ vectors $(0,0,0)^{\mathsf{T}}$, $(0,1,1)^{\mathsf{T}}$, $(1,0,1)^{\mathsf{T}}$, $(1,1,0)^{\mathsf{T}}$.

Of course, Gaussian elimination over $\mathbb{F}_2$ can also be used to determine these ranks.

The ranks over $\mathbb{Q}$ (and $\mathbb{R}$, $\mathbb{C}$) are all equal to 3, so the particular field F considered really matters!

Exercise

Show that the rank of $\mathbf{A} \in F^{m\times n}$ is the largest integer $k \geq 0$ such that $\mathbf{A}$ has an invertible $k \times k$ submatrix.

"*Submatrix of* **A**" refers to any matrix obtained from **A** by deleting zero or more rows and/or columns. The remaining rows/columns are re-indexed but their relative order is preserved. It follows that the number of $k \times l$ submatrices of **A**, counted with their frequencies of appearance in **A**, equals $\binom{m}{k}\binom{n}{l}$.

Coordinate Vectors

Suppose V is a vector space over F of finite dimension n and $B = \{b_1, \dots, b_n\}$ is an *ordered* basis of V.
$\Longrightarrow v \in V$ admits a unique representation $v = \sum_{i=1}^{n} x_i b_i$ with $x_i \in F$.

Definition

The vector $\mathbf{x} = (x_1, \dots, x_n) \in F^n$ called *coordinate vector* of v with respect to the ordered basis B and denoted by $\phi_B(v)$.

When working with matrices of linear maps, the shorthand ${}_B(v)$ for $\phi_B(v)$ is very convenient; cf. subsequent discussion.

Observation

The coordinate vectors of $b_1, \dots, b_n$ are the standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_n$ of F^n (in this order), and the coordinate map $\phi_B \colon V \to F^n$, $v \mapsto \mathbf{x}$ is a vector space isomorphism (the linear map determined by $b_i \to \mathbf{e}_i$).

Change of Basis

First recall that every linear map $f\colon F^n \to F^m$ has the form $f(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for a unique matrix $\mathbf{A} \in F^{m\times n}$. (We are now viewing vectors as column vectors.)

Now suppose $B = \{b_1, \dots, b_n\}$ and $C = \{c_1, \dots, c_n\}$ are ordered bases of V. Then there exists a unique matrix $\mathbf{A} \in F^{n\times n}$ making the diagram on the right “commutative”, i.e., $f_{\mathbf{A}} \circ \phi_B = \phi_C$.

$$\begin{tikzcd}
V \arrow[r, "\phi_B"] \arrow[dr, "\phi_C"'] & F^n \arrow[d, "f_{\mathbf{A}}"] \\
 & F^n
\end{tikzcd}$$

Reason: $\phi_C \circ \phi_B^{-1}\colon F^n \to F^n$ is linear, hence must be of the form $f_{\mathbf{A}}$ for a unique $\mathbf{A}$.

Definition

The matrix $\mathbf{A}$ is called the *change-of-basis matrix* from B to C.

The columns of $\mathbf{A}$ are

$$\mathbf{A}\mathbf{e}_j = f_{\mathbf{A}}(\mathbf{e}_j) = f_{\mathbf{A}}\big(\phi_B(b_j)\big) = \phi_C(b_j),$$

i.e., the “old” basis vectors expressed in terms of the “new” basis.
$\Longrightarrow$ $\mathbf{A}$ is defined by $b_j = \sum_{i=1}^n a_{ij} c_i$ for $1 \leq i \leq n$.

Main purpose

Multiplication with **A** switches from coordinates w.r.t. B to coordinates w.r.t. C. This is clear from

$$\phi_C(v) = f_{\mathbf{A}}\bigl(\phi_B(v)\bigr) = \mathbf{A}\phi_B(v).$$

Generalization

Suppose that in the change-of-basis setting we know that B is a basis of V, but for C this is yet unknown. How can we check whether C is a basis?

Answer: Compute the coordinate vectors $\phi_B(c_1), \dots, \phi_B(c_n)$ and arrange them as columns of an $n \times n$ matrix **M**. Then C is a basis of V iff **M** is invertible. (In particular change-of-basis matrices are invertible.)

Reason: The coordinate map $\phi_B \colon V \to F^n$ is a vector space isomorphism. Hence C is a basis of V iff $\phi_B(C)$ (i.e., the set of columns of **M**) is a basis of F^n.

The same reasoning shows that for any $v_1, \dots, v_k \in V$ the dimension of $\langle v_1, \dots, v_k \rangle$ is equal to the rank of the matrix $\mathbf{M} = \bigl(\phi_B(v_1) | \dots | \phi_B(v_k)\bigr)$.

Further properties of change-of-basis matrices

Suppose B, C, D are bases of the same finite-dimensional vector space V, $\mathbf{A}$ is the change-of-basis matrix from B to C, and $\mathbf{B}$ is the change-of-basis matrix from C to D.

1. The change-of-basis matrix from B to D is $\mathbf{BA}$.
2. The change-of-basis matrix from C to B is $\mathbf{A}^{-1}$.

These properties follow easily from $f_{\mathbf{B}} \circ f_{\mathbf{A}} = f_{\mathbf{BA}}$ and $(f_{\mathbf{A}})^{-1} = f_{\mathbf{A}^{-1}}$.

Remark

Change-of-basis matrices can be viewed as a special case of the concept of matrices representing linear maps between finite-dimensional vector spaces. This concept is discussed subsequently in the slides (in the subsection *Matrices of Linear Maps*), but will be skipped in this year's lectures. The change-of-basis matrix $\mathbf{A}$ from B to C is equal to the matrix representing the identity map $\mathrm{id}\colon V \to V$, $v \to v$ w.r.t. B and C, i.e. $\mathbf{A} = {}_C(\mathrm{id}_V)_B$, borrowing the notation from the subsequent discussion.

Examples

The first example illustrates how coordinates are introduced in a non-standard real vector space (i.e., a real vector space not of the form $\mathbb{R}^\kappa$).

Example

The symmetric matrices in $\mathbb{R}^{2\times 2}$ form a 3-dimensional vector space S_2 over $\mathbb{R}$ with (ordered) basis $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. The coordinate vector of $\mathbf{A}=\left(\begin{smallmatrix}a&b\\b&c\end{smallmatrix}\right)\in S_2$ with respect to this basis is (a,c,b), since

$$\begin{pmatrix}a&b\\b&c\end{pmatrix}=a\begin{pmatrix}1&0\\0&0\end{pmatrix}+c\begin{pmatrix}0&0\\0&1\end{pmatrix}+b\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

If we order the basis matrices instead as $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, the coordinate vector of $\mathbf{A}$ becomes (a,b,c).

In this example we have still sort of a “standard basis”. In the next example there is no such basis.

Example

Consider the hyperplane $H_0 = \{\mathbf{x} \in \mathbb{R}^4; x_1 + \cdots + x_4 = 0\}$ in $\mathbb{R}^4$. We have $\dim H_0 = 3$, but H_0 has no obvious standard basis. Two equally good choices (from the computational point-of-view) are

$$\begin{aligned} B &= \bigl\{(1,-1,0,0),(0,1,-1,0),(0,0,1,-1)\bigr\},\\ C &= \bigl\{(1,0,0,-1),(0,1,0,-1),(0,0,1,-1)\bigr\}. \end{aligned}$$

The vector $\mathbf{v} = (2,-5,1,2)$ is in H_0 and the corresponding coordinate vectors are, using

$$\begin{aligned} (2,-5,1,2) &= 2(1,-1,0,0) - 3(0,1,-1,0) - 2(0,0,1,-1),\\ &= 2(1,0,0,-1) - 5(0,1,0,-1) + (0,0,1,-1) \end{aligned}$$

and column vectors, $\phi_B(v) = (2,-3,-2)^{\mathsf{T}}$, $\phi_C(v) = (2,-5,1)^{\mathsf{T}}$. We can also compute $\phi_B(v)$ from $\phi_C(v)$ (which is easier to obtain) and the change-of-basis from C to B, which is $\bigl(\phi_B(c_1)\big|\phi_B(c_2)\big|\phi_B(c_3)\bigr) = \left(\begin{smallmatrix} 1 & 0 & 0\\ 1 & 1 & 0\\ 1 & 1 & 1\end{smallmatrix}\right)$, as $\phi_B(v) = \mathbf{A}\phi_C(v)$.

Indeed, you can verify that $\left(\begin{smallmatrix} 2\\ -3\\ -2\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 & 0\\ 1 & 1 & 0\\ 1 & 1 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} 2\\ -5\\ 1\end{smallmatrix}\right)$.

Example (cont'd)

In fact the statement "H_0 has no obvious standard basis" is true only at the first glance. If you have studied the slides on the reduced row-echelon form of a matrix in the crash course, you know already that for every subspace S of $\mathbb{R}^n$ (or F^n in general) there exists a unique matrix $\mathbf{M}$ in reduced row-echelon form, without all-zero rows, and such that the row space of $\mathbf{M}$ is equal to S. The rows $\mathbf{r}_1, \dots, \mathbf{r}_k$ of $\mathbf{M}$ (in the usual order), where $k = \dim S$ may then serve as a canonical basis of S.

Note that in the case under consideration the canonical basis of H_0 is in fact C, since the matrix formed from C, viz.

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix},$$

is in reduced row-echelon form.

Example (Polynomial interpolation)

Recall from Calculus I that, given $n \in \mathbb{N}$ and n points (x_i, y_i), $1 \leq i \leq n$, in $\mathbb{R}^2$ with $x_1 < x_2 < \cdots < x_n$, there exists exactly one polynomial $a(X) \in \mathbb{R}[X]$ of degree $< n$ satisfying $a(x_i) = y_i$ for $1 \leq i \leq n$ (so-called *interpolation polynomial*).

In Linear Algebra terms, the "evaluation map"

$$E\colon P_{n-1} \to \mathbb{R}^n,\ a(X) \mapsto \bigl(a(x_1), \dots, a(x_n)\bigr)$$

is a vector space isomorphism.

The *power basis* $1, X, X^2, \dots, X^{n-1}$ of P_{n-1} is not particularly suited to computing interpolation polynomials. Better choices are

$$\mathrm{n}_i(X) = \prod_{j=1}^{i} (X - x_j) \quad 0 \leq i \leq n-1, \qquad \textit{(Newton basis)}$$

$$\ell_i(X) = \prod_{\substack{j=1\\ j \neq i}}^{n} \frac{X - x_j}{x_i - x_j}, \quad 1 \leq i \leq n. \qquad \textit{(Lagrange basis)}$$

Example (cont'd)

The Lagrange polynomials $\ell_i(X)$ have degree $n-1$ and are defined in such a way that the relations

$$\ell_i(x_j)=\begin{cases}1 & \text{if } i=j,\\ 0 & \text{if } i\neq j.\end{cases}$$

hold. This means $E(\ell_i)=\mathbf{e}_i$ for $1\leq i\leq n$ (the standard unit vectors of $\mathbb{R}^n$).

$\Longrightarrow \mathrm{L}=\{\ell_1,\dots,\ell_n\}$ is a basis of P_{n-1} and satisfies $E=\phi_{\mathrm{L}}$.

$$\Longrightarrow \quad a(X)=\sum_{i=1}^{n}a(x_i)\ell_i(X) \quad \text{for all } a(X)\in P_{n-1}$$

(coordinate vectors are evaluation vectors).

In other words, the interpolation problem $a(x_i)=y_i$ is solved uniquely in P_{n-1} by $a(X)=\sum_{i=1}^{n}y_i\,\ell_i(X)$.

Example (cont'd)

The Newton polynomial $\mathrm{n}_i(X) = \prod_{j=1}^{i}(X - x_i)$ is monic of degree i, hence of the form $\mathrm{n}_i(X) = \sum_{s=0}^{i} n_{si} X^i$ with $n_{si} \in \mathbb{R}$, $n_{ii} = 1$.
$\Longrightarrow$ $\mathbf{N} = (n_{si})$ is upper-triangular with 1's on the main diagonal.
$\Longrightarrow$ $\mathbf{N}$ is invertible
$\Longrightarrow$ $\mathrm{N} = \{\mathrm{n}_1, \dots, \mathrm{n}_n\}$ is a basis of P_{n-1} and $\mathbf{N}$ is the change-of-basis matrix from N to the power basis.

However, we are more interested in the coordinate vector of the interpolation polynomial $a(X)$ with respect to N.
We write $\phi_{\mathrm{N}}\bigl(a(X)\bigr) = (y_1, y_{12}, y_{123}, \dots, y_{12\dots n})$, since then

$$a(X) = y_1 + y_{12}(X - x_1) + y_{123}(X - x_1)(X - x_2) + \dots + y_{12\dots n} \prod_{j=1}^{n-1}(X - x_j)$$

and $y_{12\dots i}$ is the coefficient of X^{i-1} in the corresponding interpolation polynomial for $(x_1, y_1), \dots, (x_i, y_i)$ in P_{i-1}.
The notation makes sense for other index sets, e.g., y_{23} is defined as the coefficient of X^1 in the interpolation polynomial for (x_2, y_2), (x_3, y_3) in P_1.

Example (cont'd)

With this notation we have

$$y_{i,i+1,\dots,j}=\frac{y_{i+1,i+2,\dots,j}-y_{i,i+1,\dots,j-1}}{x_j-x_i}\quad\text{for } 1\leq i<j\leq n,\qquad\text{(dd)}$$

and hence these "divided differences" can be computed easily in a doubly-triangular array.

Proof of (dd).

Let $b(X)=\sum_{t=0}^{j-i-1}b_tX^t$ and $c(X)=\sum_{t=0}^{j-i-1}c_tX^t$ be the interpolation polynomials in P_{j-i-1} through $(x_i,y_i),\dots,(x_{j-1},y_{j-1})$ and $(x_{i+1},y_{i+1}),\dots,(x_j,y_j)$, respectively. Then we have

$$a(X)=\frac{c(X)(X-x_i)-b(X)(X-x_j)}{x_j-x_i},$$

since $a(X)\in P_{j-i}$ and $a(x_t)=y_t$ for $i\leq t\leq j$ (check this!). Hence the leading coefficient of $a(X)$, viz. $y_{i,i+1,\dots,j}$, is equal to

$$\frac{c_{j-i-1}-b_{j-i-1}}{x_j-x_i}=\frac{y_{i+1,i+2,\dots,j}-y_{i,i+1,\dots,j-1}}{x_j-x_i}.$$

□

Example (cont'd)

As a concrete example we consider the interpolation problem

i	1	2	3
x_i	0	1	3
y_i	1	3	2

First we compute the corresponding Lagrange basis of P_2, which consists of quadratic polynomials:

$$\begin{aligned}
\ell_1(X) &= \frac{(X-1)(X-3)}{(0-1)(0-3)} = \tfrac{1}{3}X^2 - \tfrac{4}{3}X + 1,\\
\ell_2(X) &= \frac{(X-0)(X-3)}{(1-0)(1-3)} = -\tfrac{1}{2}X^2 + \tfrac{3}{2}X,\\
\ell_3(X) &= \frac{(X-0)(X-1)}{(3-0)(3-1)} = \tfrac{1}{6}X^2 - \tfrac{1}{6}X.
\end{aligned}$$

$$\begin{aligned}
\Longrightarrow a(X) &= \ell_1(X) + 3\ell_2(X) + 2\ell_3(X)\\
&= \tfrac{1}{3}X^2 - \tfrac{4}{3}X + 1 + 3\left(-\tfrac{1}{2}X^2 + \tfrac{3}{2}X\right) + 2\left(\tfrac{1}{6}X^2 - \tfrac{1}{6}X\right)\\
&= -\tfrac{5}{6}X^2 + \tfrac{17}{6}X + 1.
\end{aligned}$$

Example (cont'd)

For the Newton interpolation we use a doubly-triangular array, which initially contains two columns containing x_i and y_i and is extended to the left by computing the differences $x_j - x_i$ and to the right by computing divided differences:

		x_i	y_i		
		0	$\boxed{1}$		
	1			$\boxed{2}$	
3		1	3		$\boxed{-\frac{5}{6}}$
	2			$-\frac{1}{2}$	
		3	2		

$$\begin{aligned} \Longrightarrow a(X) &= 1 + 2(X-0) - \tfrac{5}{6}(X-0)(X-1) \\ &= -\tfrac{5}{6}X^2 + \tfrac{17}{6}X + 1, \end{aligned}$$

the same result as before.

Example (cont'd)

Another way to compute the coefficients y_1, y_{12}, y_{123} in the "Newton expansion" of $a(X)$ is to use the change-of-basis matrix $\mathbf{A}$ from the Lagrange basis $\{\frac{1}{3}X^2-\frac{4}{3}X+1, -\frac{1}{2}X^2+\frac{3}{2}X, \frac{1}{6}X^2-\frac{1}{6}X\}$ to the Newton basis $\{1, X, X(X-1)\}$.

$$\begin{aligned}\ell_1(X)&=\tfrac{1}{3}X^2-\tfrac{4}{3}X+1=\tfrac{1}{3}(X^2-X)-X+1,\\ \ell_2(X)&=-\tfrac{1}{2}X^2+\tfrac{3}{2}X=-\tfrac{1}{2}(X^2-X)+X,\\ \ell_3(X)&=\tfrac{1}{6}(X^2-X)\end{aligned}$$

$$\Longrightarrow\quad \mathbf{A}=\begin{pmatrix}1&0&0\\-1&1&0\\\frac{1}{3}&-\frac{1}{2}&\frac{1}{6}\end{pmatrix}$$

$$\Longrightarrow\quad \phi_N\big(a(X)\big)=\mathbf{A}\phi_B\big(a(X)\big)=\begin{pmatrix}1&0&0\\-1&1&0\\\frac{1}{3}&-\frac{1}{2}&\frac{1}{6}\end{pmatrix}\begin{pmatrix}1\\3\\2\end{pmatrix}=\begin{pmatrix}1\\2\\-\frac{5}{6}\end{pmatrix},$$

in sync with the previous result.

Exercise

a) Repeat the previous example (computation of the Newton and Lagrange basis and the representation of the interpolation polynomial in terms of both bases) for the data

i	1	2	3	4
x_i	0	1	3	2
y_i	1	3	2	5

Hint: For the Newton interpolation part the computation in the example can be reused.

b) Plot the interpolation polynomial together with that in the example using, e.g., Matlab or SageMath. The plot should also indicate the four points (x_i, y_i).

Example

A sequence of polynomials $b_0(X), b_1(X), b_2(X), \dots$ in $\mathbb{R}[X]$, say, with $\deg b_j(X) = j$ is necessarily a basis of $\mathbb{R}[X]/\mathbb{R}$, and for every $n \geq 0$ the first $n+1$ polynomials $b_0(X), \dots, b_n(X)$ form a basis of P_n. The change-of-basis matrix $\mathbf{M}$ from the basis $\bigl(b_j(X)\bigr)$ to the power basis $1, X, X^2, \dots$ is in an infinite upper-triangular matrix, which contains, for every n, the change-of-basis matrix from $b_0(X), \dots, b_n(X)$ to $1, X, X^2, \dots, X^n$ in its upper-left corner.

Interesting examples are $b_j(X) = (X+1)^j = \sum_{i=0}^{j} \binom{j}{i} X^i$, which gives

$$\mathbf{M} = \left(\binom{j}{i}\right) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ 0 & 0 & 1 & 3 & 6 & 10 & \dots \\ 0 & 0 & 0 & 1 & 4 & 10 & \dots \\ 0 & 0 & 0 & 0 & 1 & 5 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & \dots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}$$

and $\mathbf{M}^{-1} = \left((-1)^{j-i}\binom{j}{i}\right)$ (change the sign of the entries in every second diagonal band, starting with the second band).

Exercise

Let $\mathbf{S} = (s_{ij})$ be the infinite change-of-basis matrix from the basis of falling factorials $X^{\underline{j}} = X(X-1)\dots(X-j+1)$, $j = 0, 1, 2, \dots$, to the power basis $1, X, X^2, \dots$ and $\mathbf{T} = (t_{ij}) = \mathbf{S}^{-1}$. Show that s_{ij} and t_{ij} satisfy the boundary conditions $s_{00} = t_{00} = 1$, $s_{0,j} = t_{0,j} = 0$ for $j \geq 1$, $s_{i,0} = 1$, $t_{i,0} = 0$ for $i \geq 1$, and the recurrence relations

$$\begin{aligned} s_{i,j+1} &= s_{i-1,j} - j\,s_{ij}, \\ t_{i,j+1} &= t_{i-1,j} + i\,t_{ij}. \end{aligned}$$

Note

The numbers $t_{ij} = \left\{ {j \atop i} \right\}$ are the *Stirling subset numbers* (Stirling numbers of the second kind) introduced in Math 213. The numbers s_{ij} are related to the *Stirling cycle numbers* (Stirling numbers of the first kind) $\left[{i \atop j} \right]$ by $s_{ij} = (-1)^{j-i} \left[{j \atop i} \right]$. This gives the interesting relations

$$X^{\underline{n}} = \sum_{k=0}^{n} (-1)^{n-k} \left[{n \atop k} \right] X^k, \quad X^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} X^{\underline{k}}.$$

Matrices of Linear Maps

A generalization of base change

Suppose V, W are finite-dimensional vector spaces over F with bases $\{b_1, \dots, b_n\}$ and $\{c_1, \dots, c_m\}$, respectively, and $f \colon V \to W$ is a linear map.

As in the base-change setting, there exists a unique matrix $\mathbf{A} \in F^{m \times n}$ making the diagram on the right "commutative", i.e., $f_{\mathbf{A}} \circ \phi_B = \phi_C \circ f$.

$$\begin{tikzcd} V \arrow[r, "\phi_B"] \arrow[d, "f"'] & F^n \arrow[d, "f_{\mathbf{A}}"] \\ W \arrow[r, "\phi_C"'] & F^m \end{tikzcd}$$

Reason: $\phi_C \circ f \circ \phi_B^{-1} \colon F^n \to F^m$ is linear, hence must be of the form $f_{\mathbf{A}}$ for a unique $\mathbf{A} \in F^{m \times n}$.

Definition

$\mathbf{A}$ is called the *matrix of f with respect to the bases B and C* and is also denoted by ${}_C(f)_B$.

The columns of $\mathbf{A} = (a_{ij})$ are
$\mathbf{A}\mathbf{e}_j = f_{\mathbf{A}}(\mathbf{e}_j) = f_{\mathbf{A}}\bigl(\phi_B(b_j)\bigr) = \phi_C\bigl(f(b_j)\bigr)$,
i.e., the images of the basis vectors in B expressed in terms of the basis C (i.e., $f(b_j) = \sum_{i=1}^n a_{ij} c_i$ for $1 \leq i \leq n$).

Note

The base-change setting corresponds to the special case $V = W$, $f = \mathrm{id}_V$. In this case the images $\mathrm{id}_V(b_j) = b_j$ are the basis vectors in B themselves, and are expressed in terms of the "new" basis C to find the columns of the base-change matrix.

Basic Properties

1. For every $v \in V$ the coordinate vectors ${}_B(v) = \phi_B(v)$ and ${}_C\bigl(f(v)\bigr) = \phi_C\bigl(f(v)\bigr)$ are related by $\phi_C\bigl(f(v)\bigr) = {}_C(f)_B\,\phi_B(v)$ or, in more lucid notation,

$$ {}_C\bigl(f(v)\bigr) = {}_C(f)_B\,{}_B(v). $$

2. In the situation depicted on the right-hand side, the matrix of $g \circ f$ with respect to the bases A and C is $\mathbf{BA}$, i.e., we have

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[d, "\phi_A"'] & V \arrow[r, "g"] \arrow[d, "\phi_B"'] & W \arrow[d, "\phi_C"'] \\ F^p \arrow[r, "f_{\mathbf{A}}"] & F^n \arrow[r, "f_{\mathbf{B}}"] & F^m \end{tikzcd}$$

$$ {}_C(g \circ f)_A = {}_C(g)_B\,{}_B(f)_A. $$

The proof of (1) is trivial, and that of (2) uses $f_{\mathbf{B}} \circ f_{\mathbf{A}} = f_{\mathbf{BA}}$.

Property (2) is especially useful and provides easy proofs of further important facts about representing matrices.

Further Properties

3. The change-of-basis-matrix from C to B is the inverse of the change-of-basis-matrix from B to C.

   Proof: For $\mathrm{id} = \mathrm{id}_V$ we have $\mathrm{id}^2 = \mathrm{id}$ and hence ${}_C(\mathrm{id})_B\,{}_B(\mathrm{id})_C = {}_C(\mathrm{id})_C = \mathbf{I}_n$, where $n = \dim V$.

4. $\mathbf{A}, \mathbf{A}' \in F^{m\times n}$ represent the same linear map $f\colon V \to W$ (with respect to possibly different bases of V and/or W) iff there exist invertible matrices $\mathbf{S} \in F^{m\times m}$ and $\mathbf{T} \in F^{n\times n}$ such that $\mathbf{A}' = \mathbf{SAT}$.

   Proof: The only-if-part follows from
   ${}_{C'}(f)_{B'} = {}_{C'}(\mathrm{id}_W \circ f \circ \mathrm{id}_V)_{B'} = {}_{C'}(\mathrm{id}_W)_C\,{}_C(f)_B\,{}_B(\mathrm{id}_V)_{B'}$
   together with the fact that change-of-basis matrices are invertible; cf. Property (3).
   For the if-part, suppose $\mathbf{A} = {}_C(f)_B$ (after choosing B, C freely, this determines $f = \phi_C^{-1} f_{\mathbf{A}} \phi_B$ uniquely). We must show that there exists a basis C' of W such that $\mathbf{S} = {}_{C'}(\mathrm{id}_W)_C$ or, equivalently, $\mathbf{S}^{-1} = {}_C(\mathrm{id}_W)_{C'}$ (and similarly for $\mathbf{T}$).
   Define $C' = \{c_1, \dots, c_m'\}$ by $c_j' = \sum_{i=1}^m s_{ij}' c_i$, where $\mathbf{S}^{-1} = (s_{ij}')$.

Further Properties Cont'd

4. *Proof cont'd:* Since $\mathbf{S}^{-1}$ is invertible, C' is indeed a basis of W, and then $\mathbf{S}^{-1} = {}_{C}(\mathrm{id}_W)_{C'}$ holds by definition of C'.

5. In the case $V = W$ (i.e., f is an endomorphism of V) it is natural to demand $B = C$ as well, i.e., consider only representing matrices of the form ${}_B(f)_B$.
   The computation in (4) changes to
   $${}_C(f)_C = {}_C(\mathrm{id})_B\,{}_B(f)_B\,{}_B(\mathrm{id})_C = \bigl({}_B(\mathrm{id})_C\bigr)^{-1}{}_B(f)_B\,{}_B(\mathrm{id})_C.$$
   It follows that matrices $\mathbf{A}, \mathbf{A}' \in F^{n\times n}$ represent the same linear map $f\colon V \to V$ with respect to possibly different bases of V iff there exists an invertible matrix $\mathbf{S} \in F^{n\times n}$ such that $\mathbf{A}' = \mathbf{S}^{-1}\mathbf{A}\mathbf{S}$.

Definition

Matrices $\mathbf{A}, \mathbf{A}' \in F^{n\times n}$ are said to be *similar* (notation $\mathbf{A} \sim \mathbf{B}$) if $\mathbf{A}' = \mathbf{S}^{-1}\mathbf{A}\mathbf{S}$ for some invertible matrix $\mathbf{S} \in F^{n\times n}$.

6. The rank of the linear map f, i.e. $\dim f(V)$, equals the rank of any representing matrix ${}_B(f)_C$.
   Proof: Use $f_{\mathbf{A}} = \phi_C \circ f \circ \phi_B^{-1}$ and $\dim f_{\mathbf{A}}(\mathbb{R}^n) = \dim \operatorname{csp}(\mathbf{A}) = \operatorname{rk}(\mathbf{A})$.

Exercise

Show that similarity of $n \times n$ matrices over F defines an equivalence relation on $F^{n\times n}$.

Exercise

Define the relation $\approx$ on $F^{m\times n}$ by $\mathbf{A} \approx \mathbf{B}$ if there exist invertible matrices $\mathbf{S} \in F^{m\times m}$, $\mathbf{T} \in F^{n\times n}$ such that $\mathbf{B} = \mathbf{SAT}$.

a) Show that $\approx$ is an equivalence relation on $F^{m\times n}$.

b) Show that $\mathbf{A} \approx \mathbf{B}$ iff $\mathbf{A}$ and $\mathbf{B}$ have the same rank.

Hint: Show that a linear map $f\colon V \to W$ of rank r has a representing matrix of the form $\left(\begin{smallmatrix}\mathbf{I}_r & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{smallmatrix}\right) \in F^{m\times n}$, where $\mathbf{I}_r$ is the $r \times r$ identity matrix and the $\mathbf{0}$'s denote all-zero matrices of the appropriate sizes.

Example

Let $V = \langle cost, \sin t\rangle_{\mathbb{C}}$ and consider the differentiation operator $\mathrm{D}\colon V \to V$, $f \to f'$. Since

$$\mathrm{D}(\cos t) = -\sin t, \quad \mathrm{D}(\sin t) = \cos t,$$

the matrix of D with respect to the (ordered) basis $B = \{\cos t, \sin t\}$ of V is

$$_B(\mathrm{D})_B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Another basis of V is $C = \{\mathrm{e}^{\mathrm{i}t}, \mathrm{e}^{-\mathrm{i}t}\}$ (ordered as indicated), and the corresponding matrix of D is

$$_C(\mathrm{D})_C = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}$$

Accordingly, these two matrices should be similar in $\mathbb{C}^{2\times 2}$.

A particular matrix **S** affording the similarity transformation from $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right)$ should be the change-of-basis matrix $_B(\mathrm{id})_C = \left(\begin{smallmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{smallmatrix}\right)$, inferred from $\mathrm{e}^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t$, $\mathrm{e}^{-\mathrm{i}t} = \cos t - \mathrm{i}\sin t$.

Example (cont'd)

Indeed we have

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

Notes

Since $\left(\begin{smallmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{smallmatrix}\right)$ is a diagonal matrix, we say that $\mathbf{S} = \left(\begin{smallmatrix}1 & 1\\ \mathrm{i} & -\mathrm{i}\end{smallmatrix}\right)$ *diagonalizes* $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$. This property reflects the fact that

$$\mathrm{D}(\mathrm{e}^{\mathrm{i}t}) \in \mathbb{C}\mathrm{e}^{\mathrm{i}t}, \quad \mathrm{D}(\mathrm{e}^{-\mathrm{i}t}) \in \mathbb{C}\mathrm{e}^{-\mathrm{i}t}$$

($\mathrm{e}^{\mathrm{i}t}$, $\mathrm{e}^{-\mathrm{i}t}$ are so-called *eigenvectors* of D).

In this year's course we will look at this example from a different point of view, which doesn't require the concept of matrices representing linear maps; cf. next lecture.

Determinants

Recall our discussion of determinants of real 2 × 2 and 3 × 3 matrices from Calculus III. Here we provide a rigorous development of determinants of $n \times n$ matrices and endomorphisms of n-dimensional vector spaces over any field F.

Theorem

Let F be a field and n a positive integer. There exists exactly one function $\delta\colon F^{n\times n} \to F$ with the following properties:

(D1) *δ is linear in each column, i.e., the map $F^n \to F$, $\mathbf{x} \mapsto \delta\big((\mathbf{a}_1|\dots|\mathbf{a}_{j-1}|\mathbf{x}|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n)\big)$ is linear for any choice of vectors $\mathbf{a}_s \in F^n$.*

(D2) *If $\mathbf{A}$ has two equal columns then $\delta(\mathbf{A}) = 0$.*

(D3) *$\delta(\mathbf{I}_n) = 1$.*

Definition

The function δ in the theorem is called *determinant* and denoted by $\mathbf{A} \mapsto \det(\mathbf{A})$ or $\mathbf{A} \mapsto |\mathbf{A}|$.

Before we can prove the theorem, we need to develop an important concept for permutations of a finite set, viz. the so-called signature (or sign) of a permutation.

Cycle Notation for Permutations

W.l.o.g. we consider only permutations of $\{1, \dots, n\}$ (i.e., bijections from $\{1, \dots, n\}$ onto itself).

The set of all permutations of $\{1, \dots, n\}$ is denoted by S_n. With respect to map composition $(\pi_1, \pi_2) \mapsto \pi_1 \circ \pi_2$, S_n forms a group of order (cardinality) $n!$, called *symmetric group of degree n*.

k-cycles

A permutation $\pi \in \mathsf{S}_n$ is called a *k-cycle*, $k \geq 2$, if it moves some k distinct letters $i_1, \dots, i_k$ in a cycle of length k $(i_1 \to i_2 \to \dots \to i_k \to i_1)$ and fixes the remaining $n - k$ letters. Notation: $\pi = (i_1, i_2, \dots, i_k)$; 2-cycles are also called *transpositions*.

Observation

Every $\pi \in \mathsf{S}_n$ can be represented as a product $\pi = \zeta_1 \circ \zeta_2 \circ \dots \circ \zeta_r$ of disjoint cycles. Here the order of the factors does not matter, and the factors are uniquely determined up to reordering.

Reason: We can represent π as a directed graph with vertex set $\{1, \dots, n\}$ in the obvious way. This graph must have indegree and outdegree 1 at each vertex, hence be a disjoint union of directed cycles and possibly some loops (fixed points of π).

Example

We list all $4! = 24$ permutations in S_4 in cycle notation.

$$\begin{aligned}S_4 = \{&(1),\\ &(12),(13),(14),(23),(24),(34),\\ &(12)(34),(13)(24),(14)(23),\\ &(123),(132),(124),(142),(134),(143),(234),(243),\\ &(1234),(1243),(1324),(1342),(1423),(1432)\}\end{aligned}$$

Cycle notation is much more convenient for computing products in S_n, e.g.,

$$(12)(34)\circ(1342) = (14)(2)(3) = (14).$$

Fixed points (“1-cycles”) are usually suppressed, but are in fact an essential part of the permutation (because they are needed to specify the domain) and may be added for clarity.

Theorem

Let n be a positive integer.

1. *Every permutation $\pi \in \mathrm{S}_n$ can be represented as a product of transpositions.*
2. *If $\pi = \sigma_1 \circ \cdots \circ \sigma_r = \tau_1 \circ \cdots \circ \tau_s$ are representations as in (1) then $r \equiv s \pmod{2}$.*

Definition

The integer $(-1)^r \in \{\pm 1\}$ in Part (2) of the theorem is called *signature* (or *sign*) of π, and π is called *even* (*odd*) if r is even (resp., odd) or, equivalently, π has signature $+1$ (resp., -1).

The signature of π can then conveniently be denoted by $(-1)^\pi$.

Proof of the theorem.

(1) Since π is a product of cycles, it suffices to prove the assertion for a k-cycle, which w.l.o.g. we can assume to be $(1, 2, \dots, k)$. In this case one verifies easily that

$$(1, 2, \dots, k) = (1, 2) \circ (2, 3) \circ \cdots \circ (k - 1, k).$$

(2) This is the difficult part.
Assume, by contradiction, that π has representations with $r \not\equiv s \pmod 2$. Then, since $\tau_i^{-1} = \tau_i$, we have a representation

$$\mathrm{id} = \sigma_1 \circ \cdots \circ \sigma_r \circ \tau_s \circ \tau_{s-1} \circ \cdots \circ \tau_1 \qquad (\star)$$

of the identity map on $\{1, \dots, n\}$ as a product of an odd number (viz., $r + s$) of transpositions.

Let $\mathrm{n}(\pi)$ be the number of cycles, including fixed points, in the cycle representation of $\pi \in S_n$. We will show that

$$\mathrm{n}(\tau \circ \pi) = \mathrm{n}(\pi) \pm 1$$

for any transposition τ. Together with $(\star)$ this implies $n = \mathrm{n}(\mathrm{id}) = n + r + s \pmod 2$ and yields the desired contradiction.

Proof cont'd.

Suppose $\tau = (i, j)$.

Case 1: i and j are contained in the same cycle ζ of π.
We may assume $i < j$ and $\zeta = (i, i+1, \dots, j-1, j, j+1, k)$.
Then we find that

$$\tau \circ \zeta = (i, i+1, \dots, j-1) \circ (j, j+1, \dots, k).$$

Hence $\tau \circ \pi$ has one more cycle than π.

Case 1: i and j are contained in different cycles ζ_1, ζ_2 of π.
Assuming $\zeta_1 = (1, 2, \dots, k)$, $\zeta_2 = (k+1, k+2, \dots, l)$ and $\tau = (1, k+1)$, we find

$$\tau \circ \zeta_1 \circ \zeta_2 = (1, 2, \dots, k, k+1, \dots, l) = (1, \dots, l).$$

Hence $\tau \circ \pi$ has one cycle less than π.

The two cases are exhaustive and show that indeed $\mathrm{n}(\tau \circ \pi) = \mathrm{n}(\pi) \pm 1$. □

Proof of the characterization theorem for the determinant function.

Using Property (D1) repeatedly, we can expand $\delta(\mathbf{A})$ as

$$\delta(\mathbf{A}) = \sum_{\pi} a_{\pi(1),1} \cdots a_{\pi(n),n} \delta\big((\mathbf{e}_{\pi(1)}| \dots |\mathbf{e}_{\pi(n)})\big),$$

where the sum is over all maps $\pi\colon \{1,\dots,n\} \to \{1,\dots,n\}$.
We illustrate this for the case $n = 2$:

$$\begin{aligned}
\delta\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) &= \delta\big((a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2)\big) \\
&= a_{11}\delta\big((\mathbf{e}_1 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2)\big) + a_{21}\delta\big(\mathbf{e}_2 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2)\big) \\
&= a_{11}a_{12}\delta\big(\mathbf{e}_1|\mathbf{e}_1\big) + a_{11}a_{22}\delta\big(\mathbf{e}_1|\mathbf{e}_2\big) + \cdots \\
&= a_{11}a_{12}\delta\left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\right) + a_{11}a_{22}\delta\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \\
&\quad + a_{21}a_{12}\delta\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) + a_{21}a_{22}\delta\left(\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right).
\end{aligned}$$

By Property (D2), the contribution of maps that are not permutations is zero, because the corresponding 0-1 matrices have two equal columns.

Proof cont'd.

Next we show that interchanging two columns of $\mathbf{A}$ changes the sign of $\delta(\mathbf{A})$. W.l.o.g. we can assume that Columns 1 and 2 are interchanged.

$$\begin{aligned}0&=\delta\big((\mathbf{a}_1+\mathbf{a}_2|\mathbf{a}_1+\mathbf{a}_2|\mathbf{a}_3|\dots)\big)\\&=\delta\big((\mathbf{a}_1|\mathbf{a}_1|\dots)\big)+\delta\big((\mathbf{a}_1|\mathbf{a}_2|\dots)\big)+\delta\big((\mathbf{a}_2|\mathbf{a}_1|\dots)\big)+\delta\big((\mathbf{a}_2|\mathbf{a}_2|\dots)\big)\\&=\delta\big((\mathbf{a}_1|\mathbf{a}_2|\dots)\big)+\delta\big((\mathbf{a}_2|\mathbf{a}_1|\dots)\big)\end{aligned}$$

This implies the assertion.

Writing $\pi\in S_n$ as a product $\pi=\tau_1\circ\dots\circ\tau_r$ of transpositions and setting $\pi_i=\tau_1\circ\dots\circ\tau_i$ for $0\leq i\leq r$, we obtain

$$\begin{aligned}\delta\big((\mathbf{e}_{\pi(1)}|\dots|\mathbf{e}_{\pi(n)})\big)&=-\delta\big((\mathbf{e}_{\pi_{r-1}(1)}|\dots|\mathbf{e}_{\pi_{r-1}(n)})\big)=\dots=\\&=(-1)^r\delta\big((\mathbf{e}_{\pi_0(1)}|\dots|\mathbf{e}_{\pi_{r0}(n)})\big)=(-1)^\pi\delta(\mathbf{I}_n)\\&=(-1)^\pi\qquad\text{(by Prop. (D3))}\end{aligned}$$

$$\begin{aligned}\Longrightarrow\quad\delta(\mathbf{A})&=\sum_{\pi\in S_n}(-1)^\pi a_{\pi(1),1}\cdots a_{\pi(n),n}\\&=\sum_{\sigma\in S_n}(-1)^\sigma a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}\qquad(\sigma:=\pi^{-1})\end{aligned}$$

Proof cont'd.

This shows that δ is uniquely determined by (D1), (D2) and (D3) and gives the usual defining formula for the determinant attributed to Leibniz.

Conversely, in order to show existence, we define δ by Leibniz's formula and prove that δ satisfies (D1), (D2), (D3). This is straightforward for (D1) and (D3).
For (D2) we use the easily verified fact that $\mathrm{S}_n = \mathrm{A}_n \uplus \mathrm{A}_n \circ \tau$ for any transposition τ. (The set $\mathrm{A}_n \circ \tau = \{\pi \circ \tau; \pi \in \mathrm{A}_n\}$ contains precisely the odd permutations in S_n.)
If Columns i and j of $\mathbf{A}$ are equal, $\tau = (i, j)$ satisfies

$$a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} = a_{\pi(\tau(1)),1} a_{\pi(\tau(2)),2} \cdots a_{\pi(\tau(n)),n}$$

for any $\pi \in \mathrm{A}_n$, and hence every such product appears twice with opposite signs in Leibniz's formula. $\implies \delta(\mathbf{A}) = 0$ □

Remark

In the proof of the theorem we have not used field axiom (M3) (existence of the multiplicative inverse of any $x \in F \setminus \{0\}$). Hence the theorem remains true if F is replaced by a commutative ring, e.g., the ring $\mathbb{Z}$ of integers or a polynomial ring $F[X]$.

Properties of the Determinant

For us the most important property of the determinant is the following, which requires F to be a field.

1. For $\mathbf{A} \in F^{n \times n}$ we have $\det(\mathbf{A}) \neq 0$ iff $\mathbf{A}$ has rank n (i.e., $\mathbf{A}$ is invertible).

The proof of this fact relies on the next three properties:

2. $\det(\mathbf{A}^{\mathsf{T}}) = \det(\mathbf{A})$.
3. The determinant of an upper-triangular (or lower-triangular) matrix $\mathbf{A} \in F^{n \times n}$ is equal to the product $a_{11} a_{22} \cdots a_{nn}$ of the elements on the main diagonal.
4. Under elementary row (or column) operations, $\det(\mathbf{A})$ transforms as follows:
   - (i) If a row of $\mathbf{A}$ is multiplied by $\lambda \in F$, $\det(\mathbf{A}') = \lambda \det(\mathbf{A})$ for the resulting matrix $\mathbf{A}'$.
   - (ii) Interchanging two rows of $\mathbf{A}$ changes the sign of $\det(\mathbf{A})$.
   - (iii) Adding a scalar multiple of one row to another row doesn't change $\det(\mathbf{A})$.

Proofs.

(2) is proved by subsituting $\sigma = \pi^{-1}$ in Leibniz's formula; cf. the proof of the preceding theorem.

(3) If $\pi \neq \mathrm{id}$, there exists $i \in \{1, \dots, n\}$ such that $i > \pi(i)$. Since $\mathbf{A} = (a_{ij})$ has $a_{ij} = 0$ for $i > j$, this implies $a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)} = 0$. Hence in Leibniz's formula only the identity permutation contributes to the sum, and $\det(\mathbf{A}) = (-1)^0 a_{11} a_{22} \cdots a_{nn}$ as claimed.

(4) For column operations, Property (i) follows from Axiom (D1), and (ii) was shown in the proof of the theorem. For the proof of (iii) we may assume w.l.o.g. that Column 1 is multiplied by λ and added to Column 2. Denoting the new matrix by $\mathbf{A}'$, we have

$$\begin{aligned}
\det(\mathbf{A}') &= \det\bigl((\mathbf{a}_1, \mathbf{a}_2 + \lambda \mathbf{a}_1 | \mathbf{a}_3 | \dots)\bigr) \\
&= \det\bigl((\mathbf{a}_1, \mathbf{a}_2 | \dots)\bigr) + \lambda \det\bigl((\mathbf{a}_1, \mathbf{a}_1 | \dots)\bigr) && \text{(by (D1))} \\
&= \det(\mathbf{A}) + 0 && \text{(by (D2))} \\
&= \det(\mathbf{A})
\end{aligned}$$

Since $\det(\mathbf{A}) = \det(\mathbf{A}^{\mathsf{T}})$, Properties (i)–(iii) also hold for row operations.

Proofs cont'd.

(1) Using Gaussian elimination, we can transform **A** into a matrix **B** in row-echelon form. Provided we don't scale the pivot rows, this changes at most the sign of $\det(\mathbf{A})$. Hence, by Property (2),

$$\det(\mathbf{A}) = \pm\det(\mathbf{B}) = \pm b_{11}b_{22}\dots b_{nn}.$$

$\Longrightarrow$ $\det(\mathbf{A}) = 0$ iff $b_{ii} = 0$ for some i. This in turn means that the number of pivot rows (or columns) of **B** is less than n, and is equivalent to $\operatorname{rk}(\mathbf{A}) = \operatorname{rk}(\mathbf{B}) < n$. □

Note

The preceding proof also provides an algorithm for computing $\det(\mathbf{A})$: Apply the Gaussian elimination algorithm (without scaling rows) to **A** (returning **B** as result) and record the number r of row interchanges done during execution of the algorithm. Then

$$\det(\mathbf{A}) = (-1)^r \times \text{product of the pivots of } \mathbf{B},$$

provided **B** has n pivots. If **B** has $< n$ pivots then $\det(\mathbf{A}) = 0$.

Further Properties

Theorem (multiplicativity of the determinant)

For $\mathbf{A}, \mathbf{B} \in F^{n \times n}$ *we have*

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}).$$

Proof.

If $\det(\mathbf{A}) = 0$ then $\mathbf{A}$ and $\mathbf{AB}$ (whose columns are linear combinations of the columns of $\mathbf{A}$) are singular and the assertion is trivial.

Otherwise we consider the function

$$\delta(\mathbf{B}) := \frac{\det(\mathbf{AB})}{\det(\mathbf{A})} \quad \text{for } \mathbf{B} \in F^{n \times n}.$$

One verifies easily that δ satisfies Axioms (D1)–(D3). Since the determinant is the unique function with these properties, this implies $\delta(\mathbf{B}) = \det(\mathbf{B})$, and hence the theorem. □

Further Properties Cont'd

Theorem (Laplace expansion)

Given $\mathbf{A} = (a_{ij}) \in F^{n \times n}$*, denote by* $\mathbf{A}_{ij} \in F^{(n-1)\times(n-1)}$ *the matrix obtained from* $\mathbf{A}$ *by deleting Row i and Column j. Then we have*

$$\begin{aligned}\det(\mathbf{A}) &= \sum_{s=1}^{n} (-1)^{i+s} a_{is} \det(\mathbf{A}_{is}) \\ &= \sum_{r=1}^{n} (-1)^{r+j} a_{rj} \det(\mathbf{A}_{rj})\end{aligned}$$

for any $i, j \in \{1, \dots, n\}$.

Proof.

This can be proved in several ways—either using Leibniz's formula (which is a little tedious, I suppose) or by induction on n using an argument similar to the proof of the preceding theorem.

Proof cont'd.

Using the second approach, one defines, e.g., in the case $i = 1$ the function $\delta\colon F^{n\times n} \to F$ as

$$\delta(\mathbf{A}) = \sum_{s=1}^{n} (-1)^{s+1} a_{1s} \det(\mathbf{A}_{1s}).$$

Properties (D1) and (D3) are easy to verify for $\mathbf{A} \to \delta(\mathbf{A})$, as is (D2) for row interchanges not involving the first row.

Using induction we can expand $\det(\mathbf{A}_{1s})$ along Row $i - 1$ (which corresponds to Row i of $\mathbf{A}$) and obtain

$$\delta(\mathbf{A}) = \sum_{1\leq s<t\leq n} (-1)^{i+1+s+t} (a_{1s}a_{it} - a_{is}a_{1t}) \det(\mathbf{A}_{1,i,s,t}),$$

where $\mathbf{A}_{1,i,s,t}$ denotes the matrix obtained from $\mathbf{A}$ by deleting Rows $1, i$ and Columns s, t. The cofactor of $\det(\mathbf{A}_{1,i,s,t})$ is the determinant of $\begin{pmatrix} a_{1s} & a_{1t} \\ a_{is} & a_{it} \end{pmatrix}$, which vanishes if Rows 1 and i of $\mathbf{A}$ are equal. This verifies (D2) for the remaining case. Then, as in the proof of the preceding theorem, uniqueness of the determinant gives $\delta(\mathbf{A}) = \det(\mathbf{A})$. □

The Adjoint Matrix

The Laplace expansion formula for rows can be put into the more general form

$$\sum_{s=1}^{n} a_{is}(-1)^{j+s}\det(\mathbf{A}_{js}) = \begin{cases}\det(\mathbf{A}) & \text{if } i=j,\\ 0 & \text{if } i\neq j.\end{cases}$$

The case $i=j$ corresponds to ordinary Laplace expansion of $\det(\mathbf{A})$ and $i\neq j$ to ordinary Laplace expansion of $\det(\mathbf{A}')$, which arises from $\mathbf{A}$ by replacing Row j by Row i. The matrix $\mathbf{A}'$ has two equal rows, and hence $\det(\mathbf{A}') = \sum_{s=1}^{n} a_{is}(-1)^{j+s}\det(\mathbf{A}_{js}) = 0$.

Definition

The *adjoint matrix* of $\mathbf{A}=(a_{ij})\in F^{n\times n}$ is the $n\times n$ matrix with (i,j) entry equal to $(-1)^{i+j}\det(\mathbf{A}_{ji})$, i.e. the transpose of the matrix containing the cofactors of a_{ij} in the Laplace expansion formulas (in the same positions and with the same signs). The adjoint matrix of $\mathbf{A}$ is denoted by $\mathrm{Adj}(\mathbf{A})$.

The Adjoint Matrix Cont'd

Writing $\operatorname{Adj}(\mathbf{A}) = (b_{ij})$, the generalized Laplace expansion formula just says

$$\sum_{s=1}^{n} a_{is}b_{sj} = \begin{cases} \det(\mathbf{A}) & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

i.e., $\mathbf{A} \operatorname{Adj}(\mathbf{A}) = \det(A)\, \mathbf{I}_n$.

Theorem

For an invertible matrix $\mathbf{A} \in F^{n \times n}$ we have

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \operatorname{Adj}(\mathbf{A}).$$

Proof.

Let $\mathbf{B} = \frac{1}{\det \mathbf{A}} \operatorname{Adj}(\mathbf{A})$ and multiply the preceding formula by $1/\det(\mathbf{A})$ to obtain $\mathbf{AB} = \mathbf{I}_n$. Then, as we know from Calculus III, we also have $\mathbf{BA} = \mathbf{I}_n$, so that $\mathbf{B} = \mathbf{A}^{-1}$. □

Kramer's Rule

Recall from Calculus III that a linear system of equations with for n unknowns (the "square" case $m = n$) over a field F can be put into the form $\mathbf{Ax} = \mathbf{b}$ with $\mathbf{A} \in F^{n \times n}$, $\mathbf{b} \in F^n$, and has a unique solution iff $\operatorname{rk}(\mathbf{A}) = n$. (Strictly speaking, this was only discussed for $F = \mathbb{R}$, but it remains of course true for any field F.)

Theorem (Kramer's Rule)

Suppose that $\mathbf{A} \in F^{n \times n}$ has rank n and $\mathbf{b} \in F^n$ is any vector. Then $\mathbf{Ax} = \mathbf{b}$ is solved uniquely by

$$x_j = \frac{\det(\mathbf{A}_j)}{\det(\mathbf{A})} \quad \textit{for } 1 \leq j \leq n,$$

where $\mathbf{A}_j$ denotes the matrix obtained from $\mathbf{A}$ by replacing Column j by $\mathbf{b}$.

Proof.

The solution is $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b} = \frac{1}{\det \mathbf{A}} \operatorname{Adj}(\mathbf{A})\mathbf{b}$, and hence

$$x_i = \frac{1}{\det \mathbf{A}} \sum_{j=1}^{n} (-1)^{i+j} \det(\mathbf{A}_{ji}) b_j = \frac{\det(\mathbf{A}_i)}{\det(\mathbf{A})}. \qquad \square$$

Some applications

VANDERMONDE matrices

A matrix of the form

$$\mathbf{V}=\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix} \quad \text{with } x_1,\dots,x_n \in F$$

is called a *Vandermonde matrix* over F. In the language of polynomial interpolation (which generalizes to any field F as long as $n \leq |F|$), $\mathbf{V}$ is the matrix of the evaluation map $E\colon P_{n-1} \to F^n$, $a(X) \mapsto \bigl(a(x_1),\dots,a(x_n)\bigr)$ with respect to the bases $\{1, X, \dots, X^{n-1}\}$ of P_{n-1} and $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$ of F^n.

Theorem

$\det(\mathbf{V}) = \prod_{1\leq i<j\leq n}(x_j - x_i)$.

In particular, $\mathbf{V}$ is invertible iff $x_1,\dots,x_n$ are distinct.

Proof of the theorem.

Consider the polynomial

$$v(X)=\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & X \\ x_1^2 & x_2^2 & \dots & X^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & X^{n-1} \end{pmatrix} \in F[X].$$

Expanding the determinant along the last column shows that $v(X)$ is indeed a polynomial in X with coefficients in F.
The degree of $v(X)$ is at most $n-1$, and the coefficient of X^{n-1} in $v(X)$ is $\det(\mathbf{V}')$, where $\mathbf{V}'$ is the Vandermonde matrix corresponding to $x_1,\dots,x_{n-1}$.

Axiom (D2) implies $v(x_i)=0$ for $i=1,2,\dots,n-1$.

$$\implies \quad v(X)=\det(\mathbf{V}')(X-x_1)(X-x_2)\cdots(X-x_{n-1})$$

$$\implies \quad v(x_n)=\det(\mathbf{V}')\prod_{i=1}^{n-1}(x_n-x_i).$$

The proof is then finished by induction on n. □

Example

$$\begin{aligned}\begin{vmatrix}1 & 1 & 1 & 1\\ 1 & 2 & 3 & 4\\ 1 & 2^2 & 3^2 & 4^2\\ 1 & 2^3 & 3^3 & 4^3\end{vmatrix} &= (4-1)(4-2)(4-3)(3-1)(3-2)(2-1)\\ &= 3^1 2^2 1^3 = 12.\end{aligned}$$

Example

The *Fourier matrix* of order n is defined as $\mathbf{F}_n = (\zeta^{ij})_{0\leq i,j\leq n-1}$ with $\zeta = \mathrm{e}^{2\pi\mathrm{i}/n}$.

The first few examples are $\mathbf{F}_1 = (1)$, $\mathbf{F}_2 = \left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$,

$$\mathbf{F}_3 = \begin{pmatrix}1 & 1 & 1\\ 1 & -\frac{1}{2}+\frac{\sqrt{3}}{2}\,\mathrm{i} & -\frac{1}{2}-\frac{\sqrt{3}}{2}\,\mathrm{i}\\ 1 & -\frac{1}{2}-\frac{\sqrt{3}}{2}\,\mathrm{i} & -\frac{1}{2}+\frac{\sqrt{3}}{2}\,\mathrm{i}\end{pmatrix}, \quad \mathbf{F}_4 = \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & \mathrm{i} & -1 & -\mathrm{i}\\ 1 & -1 & 1 & -1\\ 1 & -\mathrm{i} & -1 & \mathrm{i}\end{pmatrix}.$$

Problem: Evaluate $\det(\mathbf{F}_n)$ for all n.

Example (cont'd)

Rather precise information on $\det(\mathbf{F}_n)$ can be obtained by squaring $\mathbf{F}_n$, which also squares $\det(\mathbf{F}_n)$.

The (i,j) entry of $\mathbf{F}_n^2$ is

$$\sum_{k=0}^{n-1} \zeta^{ik}\zeta^{kj} = \sum_{k=0}^{n-1} \zeta^{(i+j)k} = \begin{cases} n & \text{if } i+j \equiv 0 \pmod{n}, \\ 0 & \text{otherwise.} \end{cases}$$

This gives

$$\mathbf{F}_n^2 = \left(\begin{array}{c|ccc} n & & & \\ \hline & & & n \\ & & \iddots & \\ & n & & \end{array}\right), \quad \det(\mathbf{F}_n)^2 = \det(\mathbf{F}_n^2) = (-1)^{\lfloor (n-1)/2 \rfloor} n^n.$$

$$\Longrightarrow \quad \det(\mathbf{F}_n) = \begin{cases} \pm n^{n/2} & \text{if } n \equiv 1,2 \pmod{4}, \\ \pm\mathrm{i}\, n^{n/2} & \text{if } n \equiv 0,3 \pmod{4}. \end{cases}$$

The correct signs remain yet to be determined.

Abel's Theorem

An application of the determinant to ODE's

Suppose that $\mathbf{y}_1(t), \dots, \mathbf{y}_n(t)$ are solutions of the system $\mathbf{y}' = \mathbf{A}(t)\mathbf{y}$ with $\mathbf{A}\colon I \to \mathbb{C}^{n\times n}$. Recall that the Wronskian of $\mathbf{y}_1(t), \dots, \mathbf{y}_n(t)$ was defined as

$$\mathrm{W}(t) = \det\bigl(\mathbf{y}_1(t)|\dots|\mathbf{y}_n(t)\bigr).$$

Theorem (Abel's Theorem)

$\mathrm{W}(t)$ *solves the scalar ODE*

$$y' = \bigl(a_{11}(t) + a_{22}(t) + \dots + a_{nn}(t)\bigr)y.$$

Proof of the general case.

Since the determinant is linear in each column, we have

$$\begin{aligned}
\mathrm{W}'(t) &= \det\bigl(\mathbf{y}_1'|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr) + \det\bigl(\mathbf{y}_1|\mathbf{y}_2'|\mathbf{y}_3|\dots|\mathbf{y}_n\bigr) \\
&\qquad + \dots + \det\bigl(\mathbf{y}_1|\dots|\mathbf{y}_{n-1}|\mathbf{y}_n'\bigr) \\
&= \det\bigl(\mathbf{A}(t)\mathbf{y}_1|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr) + \det\bigl(\mathbf{y}_1|\mathbf{A}(t)\mathbf{y}_2|\mathbf{y}_3|\dots|\mathbf{y}_n\bigr) \\
&\qquad + \dots + \det\bigl(\mathbf{y}_1|\dots|\mathbf{y}_{n-1}|\mathbf{A}(t)\mathbf{y}_n\bigr).
\end{aligned}$$

Proof cont'd.

Our goal is to show that the latter sum is equal to $\bigl(a_{11}(t)+a_{22}(t)+\dots+a_{nn}(t)\bigr)\mathrm{W}(t)$. This turns out to be a purely algebraic identity, which holds for any vectors $\mathbf{y}_1,\dots,\mathbf{y}_n\in F^n$ and any matrix $\mathbf{A}\in F^{n\times n}$; see the Lemma below. The proof of Abel's Theorem is then completed by applying, for each $t\in I$, the lemma to $\mathbf{y}_1(t),\dots,\mathbf{y}_n(t)$ and $\mathbf{A}(t)$. □

Lemma

For $\mathbf{y}_1,\dots,\mathbf{y}_n\in F^n$ and $\mathbf{A}=(a_{ij})\in F^{n\times n}$ we have

$$\begin{aligned}\det\bigl(\mathbf{A}\mathbf{y}_1|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr)+\det\bigl(\mathbf{y}_1|\mathbf{A}\mathbf{y}_2|\mathbf{y}_3|\dots|\mathbf{y}_n\bigr)+\dots+\det\bigl(\mathbf{y}_1|\dots|\mathbf{y}_{n-1}|\mathbf{A}\mathbf{y}_n\bigr)\\=(a_{11}+a_{22}+\dots+a_{nn})\det\bigl(\mathbf{y}_1|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr).\end{aligned}$$

Proof of the lemma.

Writing $\mathbf{Y}=\bigl(\mathbf{y}_1|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr)=(y_{ij})$, we have

$$\mathbf{A}\mathbf{y}_1=\begin{pmatrix}\sum_{j=1}^n a_{1j}y_{j1}\\ \dots\\ \sum_{j=1}^n a_{nj}y_{j1}\end{pmatrix}=\sum_{i,j=1}^n a_{ij}y_{j1}\mathbf{e}_i.$$

Proof of the lemma (cont'd).

Using the linearity of the determinant in the first column, this implies

$$\begin{aligned}\det\bigl(\mathbf{A}\mathbf{y}_1|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr) &= \sum_{i,j=1}^{n} a_{ij}y_{j1}\det\bigl(\mathbf{e}_i|\mathbf{y}_2|\dots|\mathbf{y}_n\bigr)\\ &= \sum_{i,j=1}^{n} a_{ij}y_{j1}(-1)^{i+1}\det(\mathbf{Y}_{i1}),\end{aligned}$$

where as usual $\mathbf{Y}_{i1}$ denotes the matrix obtained from $\mathbf{Y}$ by deleting Row i and Column 1.

Applying the same reasoning to the other summands on the left-hand side of the equation, shows that the left-hand side is equal to

$$\sum_{k=1}^{n}\sum_{i,j=1}^{n} a_{ij}y_{jk}(-1)^{i+k}\det(\mathbf{Y}_{ik}) = \sum_{i,j=1}^{n} a_{ij}\sum_{k=1}^{n}(-1)^{i+k}y_{jk}\det(\mathbf{Y}_{ik}).$$

The inner sum is the (j,i)-entry of the product $\mathbf{Y}\,\mathrm{Adj}(\mathbf{Y})$ ("generalized Laplace expansion"), and hence equal to $\det\mathbf{Y}$ if $i=j$ and zero otherwise. □

Exercise

a) If $\mathbf{A} \in F^{n\times n}$ is invertible, show that

$$\det(\mathbf{A}^{-1}) = \frac{1}{\det \mathbf{A}}.$$

b) Show that similar matrices have the same determinant.

c) For an endomorphism $f \colon V \to V$ of an n-dimensional vector space one defines its determinant as

$$\det(f) = \det\bigl({}_B(f)_B\bigr),$$

where B is any basis of V. Explain why this is a valid definition.

Exercise

Suppose that $\mathbf{M} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{B} \end{array}\right)$ is a *block triangular matrix* with square blocks $\mathbf{A} \in F^{r\times r}$, $\mathbf{B} \in F^{s\times s}$ and a zero block of the appropriate size (i.e., $\mathbf{0} \in F^{s\times r}$) in the lower left corner. Show that $\det(\mathbf{M}) = \det(\mathbf{A})\det(\mathbf{B})$.

Exercise

a) Show that orthogonal matrices in $\mathbb{R}^{n\times n}$ have determinant $+1$ or -1.

b) What is the determinant of a reflection at some plane in $\mathbb{R}^3$ through the origin? (Such a reflection represents an endomorphism of $\mathbb{R}^3/\mathbb{R}$.)

c) What is the determinant of a rotation around some line through the origin in $\mathbb{R}^3$? (Likewise, such a rotation represents an endomorphism of $\mathbb{R}^3/\mathbb{R}$.)

d) A matrix $\mathbf{U} = (u_{ij}) \in \mathbb{C}^{n\times n}$ is said to be *unitary* if $\mathbf{U}^* = (\overline{u}_{ji})$ (the *conjugate transpose* of $\mathbf{U}$) satisfies $\mathbf{U}^*\mathbf{U} = \mathbf{I}_n$. What can you say about the determinant of a unitary matrix?

Exercise

For a matrix $\mathbf{A} \in F^{m\times n}$ with $m \geq n$ and $I \subseteq \{1, \dots, m\}$ with $|I| = n$ denote by $\mathbf{A}_I$ the $n \times n$ submatrix of $\mathbf{A}$ formed by the rows that are indexed by the elements of I. Prove the *Cauchy-Binet formula*

$$\det(\mathbf{A}^\mathsf{T}\mathbf{B}) = \sum_{\substack{I\subseteq\{1,\dots,m\}\\ |I|=n}} \det(\mathbf{A}_I)\det(\mathbf{B}_I)$$

for matrices $\mathbf{A}, \mathbf{B} \in F^{m\times n}$, $m \geq n$.

Hint: Proceed in a way similar to the proof of the characterization theorem for the determinant. Both sides of the identity can be expanded using the linearity in each column of **A** and **B**. This leaves only a very special case of the identity to be proved.

Exercise

One evening Dr. Matrix discovered the following remarkable identities:

$$\begin{aligned}
\frac{1}{(a-b)(a-c)}+\frac{1}{(b-c)(b-a)}+\frac{1}{(c-a)(c-b)}&=0,\\
\frac{a}{(a-b)(a-c)}+\frac{b}{(b-c)(b-a)}+\frac{c}{(c-a)(c-b)}&=0\\
\frac{a^2}{(a-b)(a-c)}+\frac{b^2}{(b-c)(b-a)}+\frac{c^2}{(c-a)(c-b)}&=1\\
\frac{a^3}{(a-b)(a-c)}+\frac{b^3}{(b-c)(b-a)}+\frac{c^3}{(c-a)(c-b)}&=a+b+c.
\end{aligned}$$

Show that these form a special case of the following general law: For distinct elements $x_1,\dots,x_n$ in a field F we have

$$\sum_{j=1}^{n}\frac{x_j^r}{\prod_{k=1,k\neq j}^{n}(x_j-x_k)}=\begin{cases}0 & \text{if } 0\leq r\leq n-2,\\ 1 & \text{if } r=n-1,\\ \sum_{j=1}^{n}x_j & \text{if } r=n.\end{cases}$$

Then prove this law!

Exercise (circulant matrices)

$\mathbf{A} \in F^{n \times n}$ is said to be *circulant* if it has the following structure:

$$\mathbf{A} = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & \dots & a_{n-1} & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{pmatrix},$$

i.e., the $(i+1)$-th row is obtained from the i-th row by a cyclic shift to the right with wrap-around. In the following we assume $F = \mathbb{C}$.

a) Show that the Fourier matrix $\mathbf{F}_n$ diagonalizes $\mathbf{A}$ and determine the eigenvalues and the determinant of $\mathbf{A}$ in terms of $a(X) = \sum_{j=0}^{n-1} a_j X^j$.

b) For which integers $n \in \mathbb{Z}^+$ is the $n \times n$ circulant matrix over $\mathbb{R}$ with first row $(1, -1, 1, -1, \dots, \pm 1)$ invertible?

Exercise

Let $\mathbf{A}_n$ be the circulant matrix in $\mathbb{R}^{n\times n}$ with first row $(1, 2, \dots, n)$.

a) Show that $n(n+1)/2$ is an eigenvalue of $\mathbf{A}_n$.

b) Using a computer algebra system, compute $\det(\mathbf{A}_n)\left(\frac{n(n+1)}{2}\right)^{-1}$ for a few small values of n (say, $n \leq 10$). Which general formula for $\det(\mathbf{A}_n)$ does this computation suggest?

c) Prove the formula conjectured in b).

Note: Part c) seems to be quite hard.

Exercise

Complete the evaluation of the determinants of the Fourier matrices $\mathbf{F}_n$ by determining the correct signs.

Hint: The Vandermonde determinant formula gives an alternative expression for $\det(\mathbf{F}_n)$. The factors can be changed to values of $x \mapsto \sin(x)$ by multiplying them with an apppropriate power of ζ.

Exercise

Compute the determinant of

$$\mathbf{M}_n = \begin{pmatrix} b & a & a & \dots & a \\ a & b & a & \dots & a \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a & \dots & a & b & a \\ a & \dots & a & a & b \end{pmatrix} \in \mathbb{R}^{n\times n}.$$

Hint: Write $\mathbf{M}_n = (b-a)\mathbf{I}_n + a\mathbf{J}_n$, where $\mathbf{J}$ is the $n \times n$ all-one matrix. Diagonalize $\mathbf{J}_n$ and use this to find the eigenvalues of $\mathbf{M}_n$.

Exercise

Compute the determinant d_n of the “tridiagonal” matrix

$$\mathbf{D}_n = \begin{pmatrix} 5 & 2 & & \\ 2 & 5 & \ddots & \\ & \ddots & \ddots & 2 \\ & & 2 & 5 \end{pmatrix} \in \mathbb{R}^{n\times n} \qquad \text{for } n = 1, 2, 3, \dots$$

Hint: First establish a recurrence relation for d_n.