# All the maths we know

21 October 2023

## Set theory

### Sets

| | |
|---|---|
| **Set** | A collection of things, called its *elements* (or *members*). |
| $x \in X$ | "$x$ is an element of set $X$." |
| $X \cup Y$ | The **union** of $X$ and $Y$: all elements of $X$ together with all elements of $Y$. |
| $X \cap Y$ | The **intersection** of $X$ and $Y$; its elements are those that are elements of both $X$ and $Y$. |
| $X \setminus Y$ | The **set difference**: all elements of $X$ that are not elements of $Y$. Sometimes $X - Y$. |
| $X \subset Y$ | "Every element of $X$ is an element of $Y$." $X$ is a *subset* of $Y$. |
| $\{x \in X \mid P(x)\}$ | The set of those elements of $X$ satisfying the predicate $P$ (*i.e.*, for which $P(x)$ is true). |
| $\emptyset$ | The **empty set**—the set with no members. |

### Pairs and tuples

| | |
|---|---|
| **Pair** | An ordered list of two things: like a set but the order matters and they can be the same thing. For example: $(1, 2)$. |
| $n$-**tuple** | An ordered list of $n$ things. For example: $(x_1, x_2, \ldots, x_n)$. |
| $X \times Y$ | The **Cartesian product** of $X$ and $Y$ is the set of all pairs $(x, y)$ where $x \in X$ and $y \in Y$. |
| $X^n$ | The set of all $n$-tuples of elements of $X$. The Cartesian product of $X$ with itself $n$ times. |

### Maps

| | |
|---|---|
| **Map** | A rule which assigns, to every element of a set (called the *domain*), an element of another set (called the *codomain*). Sometimes called a *function*, especially when the codomain is numbers. |
| $f\colon X \to Y$ | "$f$ is a map from $X$ to $Y$." |
| $f\colon x \mapsto y$ | "Specifically, $f$ maps the element $x \in X$ to the element $y \in Y$." |
| $f \circ g$ | The map $g$ followed by the map $f$. |
| **Injection** | A map, $f\colon X \to Y$, is *injective* (also *one-to-one*) if no more than one element of $X$ maps to a particular element of $Y$. |
| **Surjection** | A map, $f\colon X \to Y$, is *surjective* (also *onto*) if every element of $Y$ is mapped to by some element of $X$. |
| **Bijection** | A map, $f\colon X \to Y$, is *bijective* if it is both injective and surjective (also "one-to-one and onto"). |
| $X \cong Y$ | There exists a bijection between sets $X$ and $Y$. Equivantly: $X$ and $Y$ are *isomorphic as sets.* |

## Useful maps

**Operator** A *binary operator* on a set $\mathbf{X}$ is a map $\star\colon \mathbf{X} \times \mathbf{X} \to \mathbf{X}$. That is, a binary operator takes two elements of $\mathbf{X}$ and returns an element of $\mathbf{X}$. Operators are typically written in "infix" notation, $x \star y$, rather than in a function notation, $\star(x, y)$.

**Associative** A binary operator, $\star$, is *associative* if

$$(a \star b) \star c = a \star (b \star c).$$

Almost all operators you will meet are associative. Since the order in which the operations are carried out doesn't affect the result, the parentheses are often omitted, as in $a \star b \star c$.

**Commutative** A binary operator, $\star$, is *commutative* if

$$a \star b = b \star a.$$

## Numbers

| | |
|---|---|
| $\mathbf{N}$ | The *natural numbers:* $0, 1, 2, \ldots$. |
| $\mathbf{Z}$ | The *integers:* $\ldots, -2, -1, 0, 1, 2, \ldots$. |
| $\mathbf{Q}$ | The *rationals:* All numbers that can be written as $m/n$ where $m$ and $n$ are integers. |
| $\mathbf{R}$ | The *reals:* The rationals and "all the numbers in between." |
| $\mathbf{R}^+$ | The non-negative reals. |
| $\mathbf{C}$ | The *complex numbers:* Numbers of the form $a + bi$, where $a$ and $b$ are real numbers and $i^2 = -1$. |

## Vector spaces

**Vector space** A *real vector space* is a set, $V$, together with: (i) a commutative, associative, binary operator, $+$, on $V$; (ii) a map, $\cdot: \mathbf{R} \times V \to V$; and (iii) a distinguished element $0 \in V$, such that:

1. $v + 0 = v$ for all $v \in V$;
2. For any $v \in V$ there exists an element $-v \in V$ such that $v + (-v) = 0$;
3. $1 \cdot v = v$ for all $v \in V$;
4. $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ for all $\alpha, \beta \in \mathbf{R}$ and all $v \in V$.
5. $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$ and $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ for all $\alpha, \beta \in \mathbf{R}$ and $v, w \in V$.

Replacing $\mathbf{R}$ with $\mathbf{C}$ in the above we obtain a *complex vector space*.

**Vector** An element of a vector space.

**Subspace** A subset of a vector space that is itself a vector space with respect to the addition and scalar multiplication inherited from the larger space.
Equivalently: A subset, $U \subset V$ of a vector space, $V$, is a *subspace* if, for all $u, v \in U$ and number $\alpha$, the combination $u + \alpha \cdot v$ is also in $U$.

## Examples of vector spaces

**$\mathbf{R}^n$ (or $\mathbf{C}^n$)** The set of $n$-tuples of $\mathbf{R}$ (or $\mathbf{C}$), together with the operation of "element-wise" addition:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) \stackrel{\text{def}}{=} (x_1 + y_1, \dots, x_n + y_n)$$

and multiplication by $\mathbf{R}$ (or $\mathbf{C}$):

$$\lambda \cdot (x_1, \dots, x_n) \stackrel{\text{def}}{=} (\lambda x_1, \dots, \lambda x_n)$$

**$\mathbf{R}^X$ (or $\mathbf{C}^X$)** For $X$ a set, $\mathbf{R}^X$ denotes the set of all functions $X \to \mathbf{R}$, together with the operation of "pointwise addition":

$$(f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x)$$

and "pointwise multiplication by $\mathbf{R}$":

$$(\alpha f)(x) \stackrel{\text{def}}{=} \alpha f(x).$$

(The notation "$(f + g)(x)$" means "the function $f + g$, where $+$ is addition of functions, evaluated at the point $x$.")

**$\mathcal{P}_m(\mathbf{R})$** The set of polynomials of degree at most $m$. Thus, $f \in \mathcal{P}_m(\mathbf{R})$ implies $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ for some $m$.

**$\mathcal{P}(\mathbf{R})$** The set of all polynomials of finite degree.

## Combining vector spaces

**Sum** (This definition is not commonplace.) For $U_1, U_2, \dots, U_n$ subspaces of $V$, their sum is the set of all sums of vectors from the $U_i$:

$$U_1 + \cdots + U_n \stackrel{\text{def}}{=} \{v_1 + \cdots + v_n \mid v_i \in U_i\}.$$

Equivalently, it is the set of all sums from $\cup_i U_i$ (since sums from within the same $U_i$ are already elements of that $U_i$).
Equivalently, it is the span of $\cup_i U_i$.

**Direct sum** (Version 1: This definition is from Axler.) The sum of subspaces, $U_1 + \cdots + U_n$, is called a *direct sum* if the $U_i$ satisfy the following property: if $v_1 + \cdots + v_n = 0$, where $v_i \in U_i$, then each of the $v_i$ is $0$.
If the sum of the $U_i$ is a direct sum, it is written $U_1 \oplus \cdots \oplus U_n$.

**Direct sum** (Version 2.) Suppose $U_1, \dots, U_n$ are vector spaces (not necessarily subspaces of some other space). Their *direct sum*, $U_1 \oplus \cdots \oplus U_n$, is:

1. The set $U_1 \times \cdots \times U_n$; together with
2. Addition and scalar multiplication given by

$$(u_1, \dots, u_n) + \alpha \cdot (v_1, \dots, v_n) = (u_1 + \alpha \cdot v_1, \dots, u_n + \alpha \cdot v_n).$$

Note that there are natural injective maps $U_i \to U_1 \oplus \cdots \oplus U_n$ which "embed" the $U_i$ as subspaces of the direct sum.

## Linear independence and bases

**Span** — Let $v_1, \dots, v_n$ be vectors in a real vector space, $V$. The *span* of this set is the subspace given by

$$\{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid \alpha_1, \dots \alpha_n \in \mathbf{R}\}$$

(and likewise for a complex vector space).

**Linear independence** — Vectors $v_1, \dots, v_n \in V$ are *linearly independent* if $\alpha_1 v_1 + \cdots + \alpha_n v_m = 0$ implies $\alpha_1 = \cdots = \alpha_n = 0$.

**Basis** — (Of a vector space, $V$.) A collection of vectors that (a) spans $V$; (b) is linearly independent.

**Dimension** — (Of a vector-space, $V$.) The number of elements of any basis of $V$. (Noting that any two bases of $V$ have the same cardinality.)

## Linear maps

**Linear map** — A map, $T\colon V \to W$ (where $V$ and $W$ are vector spaces) such that $T(u+v) = T(u) + T(v)$ and $T(\alpha u) = \alpha T(u)$ for all $u, v \in V$.

$\mathcal{L}(V, W)$ — The set of all linear maps $V \to W$ with the vector space structure given by $(S + \alpha T)(v) \equiv S(v) + \alpha T(v)$ for any $S, T \in V$.

$\mathbf{1}_V$ — The identity map $\mathbf{1}_V\colon V \to V$ where $\mathbf{1}_V\colon v \mapsto v$.

$\circ$ — Composition of linear maps. For linear maps $T\colon V \to W$ and $S\colon W \to X$, their composition $S \circ T$ is that linear map given by $(S \circ T)(v) \equiv S(T(v))$.
Composition is associative and the identity map is a left and right identity.

**Image** — Of a linear map, that subspace of the codomain that is mapped to by *some* element of the domain. Sometimes called the *range*. However, range used to mean "codomain" so the term can be ambiguous.

**Null space** — (Or "kernel".) Of a linear map, that subspace of the domain whose image is the subspace containing only the zero vector.

**Inverse** — For $T : V \to W$ a linear map, the *inverse* (if it exists) is the linear map $T^{-1}$ such that $TT^{-1} = \mathbf{1}_V$ and $T^{-1}T = \mathbf{1}_W$.

**Isomorphism** — An isomorphism of vector spaces $V$ and $W$ is an invertible, linear map between the two. If an isophormism exists the vector spaces are said to be *isomorphic*.

## Quotient space

$a + U$ — The set $\{a + u \mid u \in U\}$. What you get by "translating" $U$ by $a$.

**Coset** — (Or "translate," in Axler's terminology.) For $U$ a subspace of $V$, a coset of $U$ in $V$ is the set $a + U$ for some $a \in V$.
Two cosets are either identical or disjoint. Every vector in $V$ lies in one and only one coset.

**Quotient** — Of a vector space $V$ by a subspace $U$:

1. The set of all cosets of $U$; together with
2. The vector space structure given by

$$(a + U) + \alpha \cdot (b + U) = (a + \alpha \cdot b) + U,$$

noting that this formula does not depend on which representatives $a$ and $b$ are chosen.

$V/U$ — The quotient of $V$ by a subspace $U$.

**Quotient map** — The map, $\pi\colon V \to V/U$, which takes $v \in V$ to its coset $v + U$.

# Dual space

**Dual space** The dual of a real (respectively, complex) vector space $V$ is the vector space $V^* = \mathcal{L}(V, \mathbf{R})$ (respectively, $V^* = \mathcal{L}(V, \mathbf{C})$). An element of $V^*$ is sometimes called a *linear functional*.

**Dual basis** For $(e_{(1)}, \ldots, e_{(n)})$ a basis of $V$, the dual basis is that basis $(f^{(1)}, \ldots, f^{(n)})$ of $V^*$ such that

$$f^{(i)}(e_{(j)}) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

**Dual map** For $\phi\colon U \to V$ a linear map, its dual (sometimes called its transpose), is that map $\phi^*\colon V^* \to U^*$ such that, for all $u \in U$ and $\tilde{v} \in V^*$,

$$\tilde{v}(\phi(u)) = (\phi^*(\tilde{v}))(u).$$

**Annihilator** For $U \subset V$ a subset of $V$, the annihilator of $U$ is that subspace $U^0 \subset V^*$ of the dual of $V$ given by

$$U^0 = \{\tilde{u} \in V^* \mid \tilde{u}(w) = 0 \text{ for all } w \in U\}.$$

# Operators I

**Operator** A linear map from a vector space to itself.

**Invariant subspace** A subspace $U \subset V$ is *invariant* under operator $T$ if $Tu \in U$ for all $u \in U$.

**Minimal polynomial** Of an operator, $T$ on a finite-dimensional vector space over field $\mathbf{F}$. The (unique) monic polynomial $p \in \mathcal{P}(\mathbf{F})$ such that $p(T) = 0$. ("Monic" means that the coefficient of the highest-degree term is 1.)

# Matrices

**Matrix** An $m \times n$ matrix $A$ is $m \times n$ numbers, $A_{ij}$, indexed by $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$. (Axler writes the elements as $A_{i,j}$.)
Conventionally, the matrix is written as a rectangular array of the numbers, with $A_{ij}$ being written in the $i$th row (starting at the top) and $j$th column (starting from the left).
If $T\colon V \to W$ is a linear map and $\vec{e}_j \in V$ a basis of $V$ and $\vec{f}_i \in W$ a basis of $W$, the **matrix of** $T$ is given by:

$$T(\vec{e}_j) = \sum_i T_{ij} \vec{f}_i.$$

(That is, $T_{ij}$ is the $i$th component of $T(\vec{e}_j)$ with respect to the basis $\vec{f}_i$.)

**$\mathbf{R}^{m,n}$** The set of all $m \times n$ matrices over $\mathbf{R}$ (or $\mathbf{C}$, *mutatis mutandis*).
Addition of matrices and multiplication of matrices by numbers is defined elementwise:

$$(A + B)_{ij} \stackrel{\text{def}}{=} A_{ij} + B_{ij}$$
$$(\lambda A)_{ij} \stackrel{\text{def}}{=} \lambda A_{ij}.$$

Under these definitions, $\mathbf{R}^{m,n}$ is a vector space. (The zero element of this space is the matrix $0_{ij} = 0$.)
"Multiplication" of matrices is defined between an $l \times m$ and and $m \times n$ matrix, the result being an $l \times n$ matrix:

$$(AB)_{ij} = \sum_{k=1}^{m} A_{ik} B_{kj}.$$

**Transpose** The transpose of $A_{ij}$ is the matrix $A_{ji}$.

**Rank** The rank of a matrix $A_{ij} \in \mathbf{R}^{m,n}$ is the dimension of the span of the $n$ vectors $\vec{c}_j \in \mathbf{R}^m$ where $\vec{c}_j = A_{ij}$ (that is, the $\vec{c}_j$ are the "columns" of $A_{ij}$).
The dimension of the span of the "rows" of $A_{ij}$ is also the rank.

**Upper triangular** Of a matrix, having zero for all entries below the diagonal.

**Diagonal** Of a matrix, having zero for all entries except on the diagonal.

# Eigenvalues

**Eigenvalue** Of an operator, $T$. A number $\lambda$ such that there exists a vector $v \neq 0$ with $Tv = \lambda v$.

**Eigenvector** Of an operator, $T$. A non-zero vector, $v$, such that $Tv = \lambda v$ for some number $\lambda$.

# Operators II

**Commuting** Operators $A$ and $B$ commute if $AB - BA = 0$.

## Inner product spaces

**Inner product** On a real or complex vector space, $V$, a conjugate-symmetric, positive-definite map $V \times V \to \mathbb{F}$, written $\langle v, w\rangle$ for $v, w \in \mathbb{F}$, which is linear in its first argument (and conjugate linear in its second). That is:

$$\langle v, w\rangle \geqslant 0 \qquad \text{(positive)}$$

$$\langle v, v\rangle = 0 \implies v = 0 \qquad \text{(definite)}$$

$$\langle v, w\rangle = \overline{\langle w, v\rangle} \qquad \text{(conj. symm.)}$$

$$\langle v, x + \lambda y\rangle = \langle v, x\rangle + \lambda\langle v, y\rangle \qquad \text{(linear)}$$

An **inner product space** is a vector space, $V$, together with an inner product on $V$.

**Norm** (Given an inner product) the norm of $v$ is

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Most authors give an independent definition of a norm, from which it follows that the above construction gives rise to a norm, in those authors' sense.
The *Cauchy-Schwarz inequality* is that $|\langle v, w\rangle| \leqslant \|v\|\|w\|$ with the inequality saturated only if $v$ and $w$ are colinear. The *triangle inequality* is that $\|v + w\| \leqslant \|v\| + \|w\|$.

**Orthogonal** Describes two vectors, $v$ and $w$, having the property that $\langle v, w\rangle = 0$.

## Orthonormal bases

**Orthonormal** Of a list of vectors, having the property that every vector in the list has norm 1 and is orthogonal to every other vector in the list. Orthonormal lists are linearly independent.

**Orthonomal basis** A basis that is orthonormal.

**Gram-Schmidt procedure** The Gram-Schmidt procedure is an algorithm for constructing, from a list of vectors, an orthonormal list having the same span as the original list.

## Assorted results

**Schur's theorem** Every operator on a finite-dimensional, complex inner product space has an upper-triangular matrix with respect to some orthonormal basis.

**Reisz representation theorem** For finite-dimensional $V$, let $\phi \in V'$ be a linear functional on $V$. Then there exists a unique $v \in V$ such that

$$\phi(u) = \langle u, v\rangle$$

for every $u \in V$.

## Orthogonal complements

**Orthogonal complement** Of a subset $U \subset V$, the set, $U^\perp$, of all vectors in $V$ that are orthogonal to every vector in $U$. Usually $U$ is a subspace. When $U$ is a finite-dimensional subspace, $(U^\perp)^\perp = U$.

**Orthogonal projection** Of a subspace $U$ of $V$, the operator $P_U$ define by $P_U v = u$ where $v = u + w$ and $u \in U$ and $w \in W^\perp$.