MATH 423

Linear Algebra II

Lecture 3:
Subspaces of vector spaces.
Review of complex numbers.
Vector space over a field.

Vector space

A *vector space* is a set V equipped with two operations, **addition** $V \times V \ni (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} + \mathbf{y} \in V$ and **scalar multiplication** $\mathbb{R} \times V \ni (r, \mathbf{x}) \mapsto r\mathbf{x} \in V$, that have the following properties:

VS1. $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ for all $\mathbf{x}, \mathbf{y} \in V$.

VS2. $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.

VS3. There exists an element of V, called the *zero vector* and denoted $\mathbf{0}$, such that $\mathbf{x} + \mathbf{0} = \mathbf{0} + \mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in V$.

VS4. For any $\mathbf{x} \in V$ there exists an element of V, denoted $-\mathbf{x}$, such that $\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = \mathbf{0}$.

VS5. $1\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in V$.

VS6. $(rs)\mathbf{x} = r(s\mathbf{x})$ for all $r, s \in \mathbb{R}$ and $\mathbf{x} \in V$.

VS7. $r(\mathbf{x} + \mathbf{y}) = r\mathbf{x} + r\mathbf{y}$ for all $r \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in V$.

VS8. $(r + s)\mathbf{x} = r\mathbf{x} + s\mathbf{x}$ for all $r, s \in \mathbb{R}$ and $\mathbf{x} \in V$.

Additional properties of vector spaces

- The zero vector is unique.
- For any $\mathbf{x} \in V$, the negative $-\mathbf{x}$ is unique.
- $\mathbf{x} + \mathbf{z} = \mathbf{y} + \mathbf{z} \iff \mathbf{x} = \mathbf{y}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.
- $\mathbf{x} + \mathbf{y} = \mathbf{z} \iff \mathbf{x} = \mathbf{z} - \mathbf{y}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.
- $0\mathbf{x} = \mathbf{0}$ for any $\mathbf{x} \in V$.
- $(-1)\mathbf{x} = -\mathbf{x}$ for any $\mathbf{x} \in V$.

Examples of vector spaces

- $\mathbb{R}^n$: n-dimensional coordinate vectors
- $\mathcal{M}_{m,n}(\mathbb{R})$: $m \times n$ matrices with real entries
- $\mathbb{R}^\infty$: infinite sequences $(x_1, x_2, \dots)$, $x_n \in \mathbb{R}$
- $\{\mathbf{0}\}$: the trivial vector space
- $\mathcal{F}(S)$: the set of all functions $f : S \to \mathbb{R}$
- $C(\mathbb{R})$: all continuous functions $f : \mathbb{R} \to \mathbb{R}$
- $\mathcal{P}$: all polynomials $p(x) = a_0 + a_1 x + \cdots + a_n x^n$
- $\mathcal{P}_n$: all polynomials of degree at most n

Subspaces of vector spaces

Definition. A vector space V_0 is a **subspace** of a vector space V if $V_0 \subset V$ and the linear operations on V_0 agree with the linear operations on V.

Examples.

- $\mathcal{F}(\mathbb{R})$: all functions $f : \mathbb{R} \to \mathbb{R}$
- $C(\mathbb{R})$: all continuous functions $f : \mathbb{R} \to \mathbb{R}$

$C(\mathbb{R})$ is a subspace of $\mathcal{F}(\mathbb{R})$.

- $\mathcal{P}$: polynomials $p(x) = a_0 + a_1 x + \cdots + a_k x^k$
- $\mathcal{P}_n$: polynomials of degree at most n

$\mathcal{P}_n$ is a subspace of $\mathcal{P}$.

Subspaces of vector spaces

Counterexamples.

- $\mathbb{R}^n$: n-dimensional coordinate vectors
- $\mathbb{Q}^n$: vectors with rational coordinates

$\mathbb{Q}^n$ is not a subspace of $\mathbb{R}^n$.

$\sqrt{2}(1, 1, \dots, 1) \notin \mathbb{Q}^n \implies \mathbb{Q}^n$ is not a vector space (scaling is not well defined).

- $\mathbb{R}$ with the standard linear operations
- $\mathbb{R}_+$ with the operations $\oplus$ and $\odot$

$\mathbb{R}_+$ is not a subspace of $\mathbb{R}$ since the linear operations do not agree.

If S is a subset of a vector space V then S inherits from V addition and scalar multiplication. However S need not be closed under these operations.

Theorem A subset S of a vector space V is a subspace of V if and only if S is **nonempty** and **closed under linear operations**, i.e.,

$$\mathbf{x}, \mathbf{y} \in S \implies \mathbf{x} + \mathbf{y} \in S,$$

$$\mathbf{x} \in S \implies r\mathbf{x} \in S \text{ for all } r \in \mathbb{R}.$$

Proof: "only if" is obvious.
"if": properties like associative, commutative, or distributive law hold for S because they hold for V. We only need to verify properties VS3 and VS4. Take any $\mathbf{x} \in S$ (note that S is nonempty). Then $\mathbf{0} = 0\mathbf{x} \in S$. Also, $-\mathbf{x} = (-1)\mathbf{x} \in S$. Thus $\mathbf{0}$ and $-\mathbf{x}$ in S are the same as in V.

Examples of subspaces

Each of the following functional vector spaces is a subspace of all preceding spaces:

- $\mathcal{F}(\mathbb{R})$: the set of all functions $f : \mathbb{R} \to \mathbb{R}$
- $C(\mathbb{R})$: all continuous functions $f : \mathbb{R} \to \mathbb{R}$
- $C^1(\mathbb{R})$: all continuously differentiable functions $f : \mathbb{R} \to \mathbb{R}$
- $C^\infty(\mathbb{R})$: all smooth functions $f : \mathbb{R} \to \mathbb{R}$
- $\mathcal{P}$: all polynomials $p(x) = a_0 + a_1 x + \cdots + a_n x^n$
- $\mathcal{P}_n$: all polynomials of degree at most n

Here polynomials are regarded as functions on the real line (otherwise $\mathcal{P}$ is not a subset of $\mathcal{F}(\mathbb{R})$).

Examples of subspaces

Each of the following nested sets of infinite sequences is a subspace of $\mathbb{R}^\infty$:

- $\mathbb{R}^\infty$: all sequences $\mathbf{x} = (x_1, x_2, \dots)$, $x_n \in \mathbb{R}$.
- ℓ^∞: the set of bounded sequences.
- the set of converging sequences.
- the set of decaying sequences: $\lim_{n\to\infty} x_n = 0$.
- the set of summable sequences: the series $x_1 + x_2 + \cdots$ is convergent.
- ℓ^1: the set of absolutely summable sequences; $\mathbf{x} = (x_1, x_2, \dots)$ belongs to ℓ^1 if $\sum_{n=1}^\infty |x_n| < \infty$.
- $\mathbb{R}_0^\infty$: the set of sequences $\mathbf{x} = (x_1, x_2, \dots)$ such that $x_n = 0$ for all but finitely many indices.

Complex numbers

$\mathbb{C}$: complex numbers.

Complex number: $\boxed{z = x + iy,}$

where $x, y \in \mathbb{R}$ and $i^2 = -1$.

$i = \sqrt{-1}$: imaginary unit

Alternative notation: $z = x + yi$.

$x =$ real part of z,
$iy =$ imaginary part of z

$y = 0 \implies z = x$ (real number)
$x = 0 \implies z = iy$ (purely imaginary number)

We add, subtract, and multiply complex numbers as polynomials in i (but keep in mind that $i^2 = -1$).

If $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, then

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2),$$

$$z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2),$$

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1).$$

Given $z = x + iy$, the **complex conjugate** of z is $\bar{z} = x - iy$. The **modulus** of z is $|z| = \sqrt{x^2 + y^2}$.

$$z\bar{z} = (x + iy)(x - iy) = x^2 - (iy)^2 = x^2 + y^2 = |z|^2.$$

$$z^{-1} = \frac{\bar{z}}{|z|^2}, \qquad (x + iy)^{-1} = \frac{x - iy}{x^2 + y^2}.$$

Complex exponentials

Definition. For any $z \in \mathbb{C}$ let

$$e^z = 1 + z + \frac{z^2}{2!} + \cdots + \frac{z^n}{n!} + \cdots$$

Remark. A sequence of complex numbers $z_1 = x_1 + iy_1,\ z_2 = x_2 + iy_2, \dots$ converges to $z = x + iy$ if $x_n \to x$ and $y_n \to y$ as $n \to \infty$.

Theorem 1 If $z = x + iy,\ x, y \in \mathbb{R},$ then

$$e^z = e^x(\cos y + i \sin y).$$

In particular, $e^{i\phi} = \cos\phi + i\sin\phi,\ \phi \in \mathbb{R}.$

Theorem 2 $e^{z+w} = e^z \cdot e^w$ for all $z, w \in \mathbb{C}.$

Proposition $e^{i\phi} = \cos\phi + i\sin\phi$ for all $\phi \in \mathbb{R}$.

Proof: $e^{i\phi} = 1 + i\phi + \frac{(i\phi)^2}{2!} + \cdots + \frac{(i\phi)^n}{n!} + \cdots$

The sequence $1, i, i^2, i^3, \ldots, i^n, \ldots$ is periodic:

$\underbrace{1, i, -1, -i}, \underbrace{1, i, -1, -i}, \ldots$

It follows that

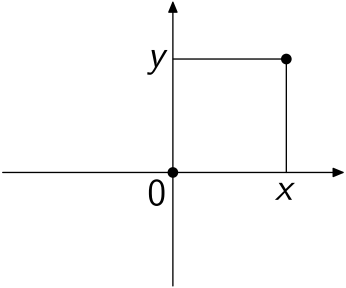
$$e^{i\phi} = 1 - \frac{\phi^2}{2!} + \frac{\phi^4}{4!} - \cdots + (-1)^k \frac{\phi^{2k}}{(2k)!} + \cdots$$

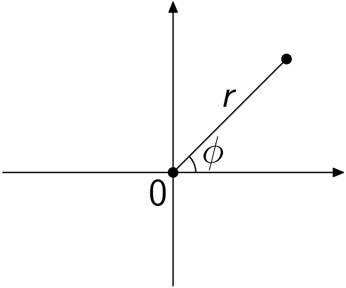
$$+ \ i\left(\phi - \frac{\phi^3}{3!} + \frac{\phi^5}{5!} - \cdots + (-1)^k \frac{\phi^{2k+1}}{(2k+1)!} + \cdots\right)$$

$$= \cos\phi + i\sin\phi.$$

Geometric representation

Any complex number $z = x + iy$ is represented by the vector/point $(x, y) \in \mathbb{R}^2$.





$$x = r\cos\phi, \; y = r\sin\phi \implies z = r(\cos\phi + i\sin\phi) = re^{i\phi}$$

If $z_1 = r_1 e^{i\phi_1}$ and $z_2 = r_2 e^{i\phi_2}$, then
$z_1 z_2 = r_1 r_2 e^{i(\phi_1+\phi_2)}, \; z_1/z_2 = (r_1/r_2)e^{i(\phi_1-\phi_2)}$.

Fundamental Theorem of Algebra

Any polynomial of degree $n \geq 1$, with complex coefficients, has exactly n roots (counting with multiplicities).

Equivalently, if

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

where $a_i \in \mathbb{C}$ and $a_n \neq 0$, then there exist complex numbers $z_1, z_2, \ldots, z_n$ such that

$$p(z) = a_n (z - z_1)(z - z_2) \ldots (z - z_n).$$

Field

The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ motivated the introduction of an abstract algebraic structure called a **field**. Informally, a field is a set with 4 arithmetic operations (addition, subtraction, multiplication, and division) that have roughly the same properties as those of real (or complex) numbers.

As far as the linear algebra is concerned, a field is a set that can serve as a set of scalars for a vector space.

Examples of fields: • Real numbers $\mathbb{R}$.

- Complex numbers $\mathbb{C}$.
- Rational numbers $\mathbb{Q}$.
- $\mathbb{Q}[\sqrt{2}]$: all numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$.
- $\mathbb{R}(X)$: rational functions in variable X with real coefficients.

Field: formal definition

A **field** is a set F equipped with two operations, **addition** $F \times F \ni (a, b) \mapsto a + b \in F$ and **multiplication** $F \times F \ni (a, b) \mapsto a \cdot b \in F$, such that:

F1. $a + b = b + a$ for all $a, b \in F$.
F2. $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.
F3. There exists an element of F, denoted 0, such that $a + 0 = 0 + a = a$ for all $a \in F$.
F4. For any $a \in F$ there exists an element of F, denoted $-a$, such that $a + (-a) = (-a) + a = 0$.

F1′. $a \cdot b = b \cdot a$ for all $a, b \in F$.
F2′. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in F$.
F3′. There exists an element of F different from 0, denoted 1, such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in F$.
F4′. For any $a \in F$, $a \neq 0$ there exists an element of F, denoted a^{-1}, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

F5. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in F$.

Vector space over a field

The definition of a vector space over an arbitrary field F is obtained from the definition of the usual vector space by changing $\mathbb{R}$ to F everywhere in the latter.

Examples of vector spaces over a field F:

- The space F^n of n-dimensional coordinate vectors $(x_1, x_2, \dots, x_n)$ with coordinates in F.
- The space $\mathcal{M}_{m,n}(F)$ of $m \times n$ matrices with entries in F.
- The space $F[X]$ of polynomials in variable X $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- Any field F' that is an extension of F (i.e., $F \subset F'$ and the operations on F are restrictions of the corresponding operations on F'). In particular, $\mathbb{C}$ is a vector space over $\mathbb{R}$ and over $\mathbb{Q}$, $\mathbb{R}$ is a vector space over $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$ is a vector space over $\mathbb{Q}$.