Math 493 Lecture 5

Thomas Cohn

9/18/2019

We define $\mathbb{R}^n$ to be the set of column vectors of size z. It has two important operations: addition and scalar multiplication.

Most things in linear algebra work with $\mathbb{R}$ replaced by $\mathbb{C}$ or $\mathbb{Q}$. $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are examples of fields.

Defn: A **field** is a set K equipped with 2 composition laws, $+$ (addition) and $\cdot$ (multiplication) s.t.

- $(K, +)$ is an abelian group with identity element 0.
- $(K^\times, \cdot)$ is an abelian group with identity element 1. ($K^\times \stackrel{\text{def}}{=} K \setminus \{0\}$).
- $\forall a, b, c \in K$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (multiplicative distribution).

Ex: If K is any field, define $K(T)$ to be the set of rational functions with coefficients in K. A rational function looks like

$$\frac{a_n T^n + \cdots + a_0}{b_m T^m + \cdots + b_0} \quad a_i, b_j \in K$$

Ex: $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is field.
$\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ is a field.

Ex: For p prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. Addition and multiplication are the usual modular operations. (See paper notes for justification.)
Observe: If K is a field, and $a, b \in K^\times$, then $ab \neq 0$. This is because $K^\times$ is closed under multiplication, and $0 \notin K^\times$.

Ex: $\mathbb{Z}/6\mathbb{Z}$ is not a field.
$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$. But $\bar{2}, \bar{3} \neq \bar{0}$.

More generally, if n is composite, $n = ab$, for $1 < a, b < n$. So $\bar{a} \cdot \bar{b} = \bar{n} = \bar{0}$, but $\bar{a}, \bar{b} \neq \bar{0}$.
Thus, $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Ex: Suppose K is a field, $a \in K$ is not a square (i.e. $a \neq b^2$, for any $b \in K$). Then we define $K(\sqrt{a}) = \{b + c\sqrt{a} \mid b, c \in K\}$, with the obvious addition and multiplication. This is a field.
Note: we get inversion by

$$\frac{1}{b + c\sqrt{a}} = \frac{b - c\sqrt{a}}{b^2 - c^2 a}$$

The denominator is nonzero because $b^2/c^2 = (b/c)^2$ is a perfect square, and a is not.

Ex: $K = \mathbb{F}_3 = \{0, 1, 2\}$, $2 = -1$ is not a square. $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 1$. So there's a field $\mathbb{F}_3(\sqrt{-1})$.
$\#\mathbb{F}_3(\sqrt{-1}) = 9$.

Ex: $K = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. -1 is a square – $-1 = 4 = 2^2$. 2 is not so we get a field $\mathbb{F}_5(\sqrt{2})$.
$\#\mathbb{F}_5(\sqrt{2}) = 25$.

Vector Spaces

Fix a field K.

Defn: A **vector space** over K is a set V equipped with two operations:

- $+ : V \times V \to V$ (addition)
- $\cdot : K \times V \to V$ (scalar multiplication)

  Such that

- $(V, +)$ is an abelian group (write 0 for the identity element).
- Given $a, b \in K$, $v \in V$, then $a(bV) = (ab)V$.
- $1 \cdot v = v$.
- Distributive law: for $a, b \in K$ and $v, w \in V$, $(a + b)v = av + bv$ and $a(v + w) = av + aw$.

Ex: $V = K[t]$ (all polynomials with coefficients in K) is a vector space.
$V = M_n(K) \cong K^{n^2}$ ($n \times n$ matrices in K) is a vector space.

Defn: V, W vector spaces over K. A **linear map** is a function $T : V \to W$ s.t. $T(v_1 + v_2) = T(v_1) + T(v_2)$ and $T(av_1) = aT(v_1)$, for all $a \in K$ and $v_1, v_2 \in V$.

Defn: An **isomorphism** is a bijective linear map.

Ex: $\mathbb{C}$ is a vector space over $\mathbb{R}$. As an $\mathbb{R}$-vector space, $\mathbb{C} \cong \mathbb{R}^2$, where $a + bi \mapsto \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$.
More generally, if K is a subfield of L, then L is naturally a K-vector space.

Defn: Let V be a K-vector space, and $S \subseteq V$. Define the **span** of S, denoted span(S), to be the set of all finite linear combinations of elements of S.

Defn: A set $S \subseteq V$ which is closed under addition and scalar multiplication is a **subspace** of V.

Note: span(S) is closed under addition and scalar multiplication, so it's a subspace of V.

Defn: We say S **spans** V, or is a **spanning set** if span$(S) = V$.

Defn: We say S is **linearly independent** if given $v_1, \ldots, v_n \in S$ distinct, if $\sum_{i=1}^n a_i v_i = 0$, then $a_i = 0$, $\forall i$.

Defn: S is a **basis** if it's a spanning set and linearly independent.

Ex: $V = K^3$, $S = \left\{ \left[\begin{smallmatrix} 1 \\ 1 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right] \right\}$, span$(S) = \left\{ \left[\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right] \mid b = a + c \right\}$.
S is not a spanning set, but it is linearly independent.

Prop: Let S be a subset of V. The following are equivalent:

1. S is a basis.
2. S is a minimal spanning set, i.e., S is a spanning set, but no proper subset of S is.
3. S is a maximal linearly independent set, i.e., S is linearly independent, but no proper superset of S is.

Proof:
(1) $\Rightarrow$ (2): S is a basis. By definition, S spans. Let $T \subsetneq S$ that spans, and let $v \in S \setminus T$. Since T spans, $\exists w_1, \ldots, w_n \in T, a_1, \ldots, a_n \in K$ s.t. $v = a_1 w_1 + \cdots + a_n w_n$. But $0 = -v + a_1 w_1 + \cdots + a_n w_n$, so S is not linearly independent. Oops!

(2) $\Rightarrow$ (1): S is a minimal spanning set. We need to show that S is linearly independent, so suppose not. Then we have $a_1 v_1 + \cdots + a_n v_n = 0$ with not all $a_i = 0$, and $v_i \in S$ distinct. WOLOG $a_1 = a$. Then $v_1 = -a_2 v_2 - \cdots - a_n v_n$. We will show that $T = S \setminus \{v_1\}$ spans.
Let $x \in V$ be given. Since S spans, $x = b_1 w_1 + \cdots + b_m w_m$. If no $w_i = v_1$, then $x \in \operatorname{span}(T)$. Otherwise, WOLOG $w_m = v_1$. Then
$x = b_1 w_1 + \cdots + b_{m-1} w_{m-1} + b_m(-a_2 v_2 - \cdots - a_n v_n) \in \operatorname{span}(S \setminus \{v_1\}) = \operatorname{span}(T)$.