Linear Algebra

Lecture 2

Example: $\mathbb{F}_2 = \{0, 1\}$

$\mathbb{P}_n(\mathbb{F}_2)$ = set of all polynomials upto degree n (for a non-negative integer n) with coefficients from $\mathbb{F}_2$.

What is $\mathbb{F}_2$?? (It is a finite field with 2 elements)

Addition in $\mathbb{F}_2$:

$0+0 = 0$

$0+1 = 1$

$1+0 = 1$

$1+1 = 0$

Multiplication in $\mathbb{F}_2$:

$1 \cdot 0 = 0$

$0 \cdot 1 = 0$

$1 \cdot 1 = 1$

$a(x) \in \mathbb{P}_n(\mathbb{F}_2)$

$a(x) = x^2 + x + 1 \qquad (2 \leq n)$

$$b(x) = x^3 + x + 1$$

$$a(x) + b(x) = (x^2 + x + 1) + (x^3 + x + 1)$$

$$= 0x^3 + x^2 + x + 1 + x^3 + 0x^2 + x + 1$$

$$= (0+1)x^3 + (1+0)x^2 + (1+1)x + (1+1)$$

additions in $\mathbb{F}_2$

$$= x^3 + x^2$$

For any $\alpha \in \mathbb{F}_2$

$$\alpha\, a(x) = a(x) \quad \text{if } \alpha = 1$$

$$= 0 \quad \text{if } \alpha = 0$$

Q: Is $\mathbb{P}_n(\mathbb{F}_2)$ "closed" under this definition of addition and scalar multiplication??

What we have done so far!?

Considered several examples of sets with two binary operations.

Set: V, scalars : $\mathbb{F}$ (In most of the examples $\mathbb{F} = \mathbb{R}$

Addition: $+ : V \times V \longrightarrow V$

$(a, b) \longmapsto a + b$

Scalar multiplication: $\cdot : \mathbb{F} \times V \longrightarrow V$

$(\alpha, a) \longmapsto \alpha \cdot a$

We have observed that the V is closed under this addition & scalar multiplication

$\forall\ a, b \in V, \quad a + b = b + a$

$\forall a, b, c \in V, \quad (a+b)+c = a+(b+c)$

$\exists\ 0 \in V, \quad \forall\ x \in V, \quad a + x = x + 0 = x$

$\forall x \in V, \ \exists\ y \in V$ such that $x + y = y + x = 0$

for "special" element $1 \in \mathbb{F}$

$1 \cdot x = x \quad \forall x \in V$

for $a, b \in \mathbb{F}$ and $x \in V$

$a(bx) = (ab)x$

$(a+b)x = ax + bx$

Digression: All the examples studied so far are examples of function spaces / function sets where domain / range needs to be chosen appropriately.

The set of scalars in all these examples are either $\mathbb{R}$ or $\mathbb{F}_2$. These are actually fields.

Definition of Vector space or linear space.

Consider a set V and a field $\mathbb{F}$ with two operations $+ : V+V \to V$ and $\cdot : \mathbb{F} \times V \to V$. ($+$ is called addition and $\cdot$ is called scalar multiplication). Then V is called a vector space over $\mathbb{F}$ if and only if V and $\mathbb{F}$ satisfy following properties. For every $v_1, v_2, v_3 \in V$ and $\alpha, \beta \in \mathbb{F}$

i) $v_1 + v_2 = v_2 + v_1$

ii) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$

iii) $\exists \ 0 \in V$ such that $v_1 + 0 = 0 + v_1 = v_1$

iv) $\forall \ v \in V, \ \exists \ u \in V$ such that

$$v + u = u + v = 0$$

v) $1 \cdot v = v \quad \forall \ v \in V$ and $1 \in \mathbb{F}$

vi) $(\alpha \cdot \beta) v = \alpha \cdot (\beta \cdot v) \quad \forall \ v \in V$

vii) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v \quad \forall \ v \in V$

viii) $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$

Notes:

1) '0' in axiom (iii) is called as "the" additive identity.

2) 'v' in axiom (iv) is called as "additive inverse" of v.

3) + on the LHS of axiom (vii) is different than + on the RHS of axiom (vii).

The LHS + represents addition of scalars (addition in F).

The RHS + represents addition of elements of V defined as earlies.

4) WLOG, the elements of V are called as vectors. and elements of F are called as scalars.

Examples:

1) Let $\mathbb{F}$ be a field. Denote by $\mathbb{F}^n$ the cartesian product $\underbrace{\mathbb{F}\times\mathbb{F}\times\mathbb{F}\times\cdots\times\mathbb{F}}_{n\text{ - times}}$

$$\mathbb{F}^n = \left\{ \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} : v_i \in \mathbb{F} \text{ for } i=1,2,\ldots,n \right\}$$

For $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{F}^n$ and $v \in \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{F}^n$

define $u+v = \begin{pmatrix} u_1+v_1 \\ \vdots \\ u_n+v_n \end{pmatrix}$.

For a scalar $\alpha \in \mathbb{F}$, define

$$\alpha \cdot u = \begin{pmatrix} \alpha u_1 \\ \alpha_2 u_2 \\ \vdots \\ \alpha u_n \end{pmatrix}$$

Then $\mathbb{F}^n$ is a vector space over $\mathbb{F}$.

In order to prove that $\mathbb{F}^n$ is a vector space over $\mathbb{F}$, we need to check all the axioms in the definition.
verify

axiom 1: Commutative property of vector addition.

For $u, v \in \mathbb{F}^n$

$$u+v = \begin{pmatrix} u_1+v_1 \\ u_2+v_2 \\ \vdots \\ u_n+v_n \end{pmatrix} \quad \text{and} \quad v+u = \begin{pmatrix} v_1+u_1 \\ v_2+u_2 \\ \vdots \\ v_n+u_n \end{pmatrix}$$

Is $u+v \overset{??}{=} v+u$

$\Leftrightarrow$ $u_i+v_i \overset{??}{=} v_i+u_i \quad \forall\, i=1,2,\ldots,n$

is always true in $\mathbb{F}$.

axiom: 2:

axiom 3: $0 \in \mathbb{F}^n$ = $0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ additive identity in $\mathbb{F}$.

axiom 4: Additive inverse:

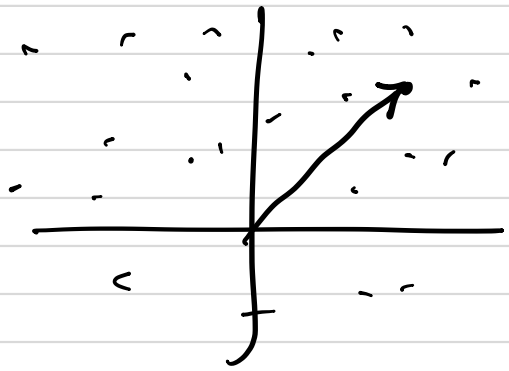
$u \in \mathbb{F}^n$ then $v = \begin{pmatrix} -u_1 \\ -u_2 \\ \vdots \\ -u_n \end{pmatrix}$ is such that $u+v=v+u=0$

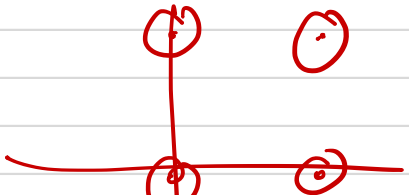
Continuing in this way, easy to prove that $\mathbb{F}^n$ is an $\mathbb{F}$- vector space.

(In order to prove this, we essentially use the fact that $\mathbb{F}$ is an abelian group under addition and $\mathbb{F}^*$ is an abelian group under multiplication).

In particular, let $\mathbb{F} = \mathbb{R}$, $n = 2$.

$\mathbb{R}^2$ is a vector space over $\mathbb{R}$.





$\mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$

Another interesting example is the case when $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$

$$\mathbb{F}_2^n = \left\{ \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} : v_i \in \{0,1\} \text{ for } i = 1, 2, \ldots, n \right\}$$

is a vector space over $\mathbb{F}_2$.

Example:

Let $S = \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} : a_1, a_2 \in \mathbb{R} \right\}$

For $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in S$ and $c \in \mathbb{R}$

define $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 - b_2 \end{pmatrix}$

$$c\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} ca_1 \\ ca_2 \end{pmatrix}.$$

Is S an $\mathbb{R}$-vector space??

Example:

Let $S = \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} : a_1, a_2 \in \mathbb{R} \right\}$

For $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in S$ and $c \in \mathbb{R}$

define $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ 0 \end{pmatrix}$

$$c\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} ca_1 \\ 0 \end{pmatrix}$$

Is S an $\mathbb{R}$-vector space??

Theorem: (Cancelation law for vector addition).

Let V be an $\mathbb{F}$-vector space. Let $x, y, z \in V$ such that

$$x + z = y + z$$

$$\Rightarrow \quad x = y$$

Proof: By axiom (iv) in the definition of a vector space,

$$\exists\ v \in V \quad \text{such that} \quad z + v = 0$$

$$\begin{aligned} x &= x + 0 && \text{... by axiom (3)} \\ &= x + (z + v) \\ &= (x + z) + v && \text{... by axiom (2)} \\ &= (y + z) + v && \text{... given hypothesis} \\ &= y + (z + v) && \text{... by axiom (2)} \\ &= y + 0 \\ &= y && \text{... by axiom (3)} \end{aligned}$$