Math 672 Lecture 1

Definition: Let F be a field and let V be a set.

Assume that two operations are defined on V and F:

- (vector) addition: $u+v \in V \ \forall u,v \in V$
- scalar multiplication: $\alpha u \in V \ \forall u \in V \ \forall \alpha \in F$.

We say that V is a vector space over F iff the following eight conditions are satisfied:

1. $u+v = v+u \ \forall u,v \in V$ (addition is commutative).
2. $(u+v)+w = u+(v+w) \ \forall u,v,w \in V$ (addition is associative).
3. There exists $0 \in V$ such that $v+0=v \ \forall v \in V$ (existence of an additive identity).
4. For each $v \in V$, there exists $w \in V$ such that $v+w=0$ (existence of additive inverses).
5. $1 \cdot v = v \ \forall v \in V$, where 1 is the multiplicative identity of F.
6. $\alpha(u+v) = \alpha u + \alpha v \ \forall u,v \in V \ \forall \alpha \in F$.
7. $(\alpha+\beta)v = \alpha v + \beta v \ \forall v \in V \ \forall \alpha,\beta \in F$.
8. $(\alpha\beta)v = \alpha(\beta v) \ \forall v \in V \ \forall \alpha,\beta \in F$.

In this course, we will only consider the fields $\mathbb{R}$ (the field of real numbers) or $\mathbb{C}$ (the field of complex numbers). For completeness, though, here is the definition of a field:

Definition: Let F be a set on which are defined two binary operations, addition and multiplication. We say that F is a field if the following properties are satisfied:

1. $\alpha+\beta=\beta+\alpha$ $\forall \alpha,\beta\in F$ (addition is commutative).
2. $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ $\forall \alpha,\beta,\gamma\in F$ (addition is associative).
3. There exists $0\in F$ such that $\alpha+0=\alpha$ $\forall \alpha\in F$ (existence of an additive identity).
4. For each $\alpha\in F$, there exists $\beta\in F$ such that $\alpha+\beta=0$ (existence of additive inverses).
5. $\alpha\beta=\beta\alpha$ $\forall \alpha,\beta\in F$ (multiplication is commutative).
6. $(\alpha\beta)\gamma=\alpha(\beta\gamma)$ $\forall \alpha,\beta,\gamma\in F$ (multiplication is associative).
7. There exists $1\in F$ such that $1\neq 0$ and $\alpha\cdot 1=\alpha$ $\forall \alpha\in F$ (existence of a multiplicative inverse).
8. For each $\alpha\in F$, $\alpha\neq 0$, there exists $\beta\in F$ such that $\alpha\beta=1$ (existence of multiplicative inverses).
9. $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$ $\forall \alpha,\beta,\gamma\in F$ (multiplication distributes over addition).

Examples of vector spaces

1. $F^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in F\}$.

   We write $x = (x_1, x_2, \ldots, x_n) \in F$.

   Addition and scalar multiplication are defined componentwise:

   $$x + y = (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n)$$
   $$= (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

   $$\alpha x = \alpha (x_1, x_2, \ldots, x_n)$$
   $$= (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$$

   I will also write $x \in F^n$ as

   $$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

   It is easy, though tedious, to prove that F^n is a vector space over F.

2. Let P_n be the set of polynomials of degree n or less (where $n \geq 1$ is an integer) with coefficients in F. A typical element in F has the form

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_0, a_1, \ldots, a_n \in F$. We define

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_n x^n)$$

$$= (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_n + b_n) x^n,$$

$$\alpha (a_0 + a_1 x + \cdots + a_n x^n) = (\alpha a_0) + (\alpha a_1) x + \cdots + (\alpha a_n) x^n.$$

Then $\mathcal{P}_n$ is a vector space over F.

<u>Question</u>: Why can't we define $\mathcal{P}_n$ to be the space of polynomials of degree <u>exactly</u> n?

<u>Answer</u>: The sum of two vectors must be another vector.

Consider $1+x+x^2,\ 2+x-x^2 \in \mathcal{P}_2$. We have

$$(1+x+x^2) + (2+x-x^2) = 3+2x,$$

and $3+2x$ doesn't have degree exactly 2.

3. Define $C[a,b] = \{f : [a,b] \to \mathbb{R} \mid f \text{ is continuous}\}$. For $f, g \in C[a,b]$, define

$$(f+g) : [a,b] \to \mathbb{R} \text{ by } (f+g)(x) = f(x) + g(x) \ \forall x \in [a,b].$$

Also, for $f \in C[a,b]$ and $\alpha \in \mathbb{R}$, define

$(\alpha f):[a,b]\to\mathbb{R}$, $(\alpha f)(x)=\alpha f(x)$ $\forall x\in[a,b]$.

Then $C[a,b]$ is a vector space over $\mathbb{R}$.

Note: We must know the follow theorems from calculus (analysis):

- The sum of two continuous functions is continuous.
- The product of a real number and a continuous function is a continuous function.

<u>Theorem</u>: Let F be a field and let V be a vector space over F.

Then:

1. The additive identity 0 of V is unique.
2. Each element v of V has a <u>unique</u> additive inverse, denoted $-v$.
3. $0v=0$ $\forall v\in V$. (To be more precise: $0_F v=0_V$ $\forall v\in V$.)
4. $\alpha 0=0$ $\forall \alpha\in F$. (To be more precise: $\alpha 0_V=0_V$ $\forall \alpha\in F$.)
5. $-1\cdot v=-v$ $\forall v\in F$.

<u>Proof</u>: 1. Suppose 0 and z are two elements of V satisfying

$$v+0=v \ \forall v\in V, \quad v+z=v \ \forall v\in V.$$

We then have

$$z=z+0 \quad (\text{since } 0 \text{ is an additive identity})$$

$= 0 + z$ (since addition is commutative)

$= 0$ (since z is an additive identity).

Thus $z = 0$, that is, 0 is the unique additive identity in V.

2. Let $v \in V$ and suppose $-v, w$ are both additive inverses of v:

$$v + (-v) = 0 \quad \text{and} \quad v + w = 0.$$

We then have

$-v = -v + 0$ (since 0 is an additive identity)

$= -v + (v + w)$ (since w is an additive inverse of v)

$= (-v + v) + w$ (since addition is associative)

$= 0 + w$ (since $-v$ is an additive inverse of v)

$= w$ (since 0 is the additive identity).

Thus $w = -v$, that is, $-v$ is the unique additive inverse of v.

(Note: The above proofs illustrate the following technique: To show that something is unique, assume that there are two of them, and prove that the two must be equal.)

3. Let $v \in V$. Then

$$0v = (0+0)v \quad (\text{since } 0+0=0 \text{ in } F)$$

$$= 0v + 0v \quad (\text{by property \#7 of a vector space}).$$

Now, $0v \in V$, so $0v$ has an additive inverse, $-(0v)$.

Thus

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

$$\Rightarrow -(0v) + 0v = -(0v) + (0v + 0v) \quad (\text{Why?})$$

$$\Rightarrow -(0v) + 0v = (-(0v) + 0v) + 0v \quad (\text{since addition is associative})$$

$$\Rightarrow 0 = 0 + 0v \quad (\text{by definition of } -(0v))$$

$$\Rightarrow 0 = 0v \quad (\text{since } 0 \text{ is the additive inverse in } V).$$

4. The proof is similar to the previous one:

$$\alpha 0 = \alpha(0+0) = \alpha 0 + \alpha 0$$

$$\Rightarrow -(\alpha 0) + \alpha 0 = -(\alpha 0) + (\alpha 0 + \alpha 0)$$

$$\Rightarrow 0 = (-(\alpha 0) + \alpha 0) + \alpha 0$$

$$\Rightarrow 0 = 0 + \alpha 0$$

$\Rightarrow \; 0 = \alpha 0.$

5. Let $v \in V$ be given. Then

$$0v = 0 \quad \text{(from above)}$$

$\Rightarrow (1+(-1))v = 0$ (since $1+(-1)=0$ in $\mathbb{F}$)

$\Rightarrow 1v + (-1)v = 0$ (by property #7 of a vector space)

$\Rightarrow v + (-1)v = 0$ (since $1v = v$, which is property #5 of a vector space)

$\Rightarrow -1 \cdot v = -v$ (since additive inverses are unique). //

Definition: If V is a vector space and $u, v \in V$, then $u - v$ is defined by

$$u - v = u + (-v).$$