MTH:100 : Lecture 13

Question: Is $\mathbb{R}^n$ a vector space over $\mathbb{Q}$?

We know $\mathbb{R}^n$ is a vector space over the field $\mathbb{R}$

- The additive properties are satisfied.
- The properties of scalar multiplication is satisfied for all scalar in $\mathbb{R}$ and so is satisfied for all rational numbers (since $\mathbb{Q} \subset \mathbb{R}$). So, $\mathbb{R}^n$ is a vector space over $\mathbb{Q}$.

Question: Is $\mathbb{R}^n$ a vector space over $\mathbb{C}$?

Let $\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \in \mathbb{R}^n$, $\underset{(\text{scalar})}{i \in \mathbb{C}}$ $\quad i \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} i \\ i \\ \vdots \\ i \end{pmatrix} \notin \mathbb{R}^n$

So, it is not closed under multiplication by complex numbers. Hence $\mathbb{R}^n$ is not a vector space over $\mathbb{C}$.

Ex:

Let $C[a,b] = \{ f : [a,b] \to \mathbb{R} \ : \ f \text{ is continuous} \}$

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

Note: Two functions are equal if they have the same values at all points in their common domain. ($\forall \equiv$ for all)

- The addition and scalar multiplication in $C[a,b]$ is defined as:

- For $f, g \in C[a,b]$, $f+g$ is defined as $\boxed{(f+g)(x) = f(x) + g(x) \quad \forall x \in [a,b]}$

• and for $c \in \mathbb{R}$ and $f \in C[a,b]$, cf is defined as $\boxed{(cf)(x) = c(f(x)) \ \forall \ x \in [a,b]}$

First we check closure property:

We know that sum of two continuous function is continuous.

So, if $f, g \in C[a,b]$, $f+g \in C[a,b]$

Also constant multiple of a continuous function is continuous.

So, if $f \in C[a,b]$ and $c \in \mathbb{R}$, then $cf \in C[a,b]$.

• Now let $f, g, h \in C[a,b]$.

$$\begin{aligned}
[(f+g)+h](x) &= (f+g)(x) + h(x) \\
&= [f(x)+g(x)] + h(x) \\
&= f(x) + [g(x)+h(x)] \quad \text{(By associative property of real numbers)} \\
&= [f+(g+h)](x) \quad \forall x \in [a,b]
\end{aligned}$$

So, $(f+g)+h = f+(g+h)$

Now the function $\bar{0}$ defined by

$$\bar{0}(x) = 0 \quad \forall\ x \in [a, b]$$

is a continuous function and so

$\bar{0} \in C[a, b]$.

Now $(f + \bar{0})(x) = f(x) + \bar{0}(x) = f(x) + 0$

$= f(x) \ \forall x \in [a, b]$

$(\bar{0} + f)(x) = \bar{0}(x) + f(x)$

$= 0 + f(x) = f(x) \ \forall x \in [a, b]$

So, $f + \bar{0} = \bar{0} + f = f \quad \forall f \in [a, b]$

Now for any $f \in C[a, b]$,

define $-f$ as $(-f)(x) = -f(x)$

$\forall x \in [a, b]$

Then $-f \in C[a, b]$

and $[f + (-f)](x) = f(x) + (-f)(x)$

$= f(x) - f(x) = 0$

$= \bar{0}(x)$

$[(-f) + f](x) = (-f)(x) + f(x)$

$= -f(x) + f(x) = 0 = \bar{0}(x)$

$\forall x \in [a, b]$

So, $f + (-f) = (-f) + f = \bar{0}$
$\forall f \in C[a,b]$

Now $(f+g)(x) = f(x) + g(x)$
$= g(x) + f(x)$ (By commutative property of addition of real numbers)
$= (g+f)(x) \quad \forall x \in [a,b]$

So, $f+g = g+f$

So, Commutative property is satisfied

Now for $c, d \in \mathbb{R}$ and $f, g \in C[a,b]$

$$[c(f+g)](x) = c\,(f+g)(x)$$
$$= c\,[f(x)+g(x)]$$
$$= c f(x) + c g(x) = (cf)(x) + (cg)(x)$$
$$= (cf+cg)(x) \quad \forall x \in [a,b]$$

$$\Rightarrow c(f+g) = cf + cg$$

Now $[(c+d)f](x) = (c+d).f(x)$
$$= c f(x) + d f(x) = (cf)(x) + (df)(x)$$

$$= (cf + df)(x) \quad \forall x \in [a,b]$$

$$\Rightarrow (c+d)f = cf + df$$

Now, $[c(df)](x) = c(df)(x)$

$$= c[d \cdot f(x)] = (cd) f(x)$$

$$= [(cd)f](x) \quad \forall x \in [a,b]$$

So, $c(df) = (cd)f$

Also $(1.f)(x) = 1 f(x) = f(x)$
$\forall x \in [a,b]$

$$\Rightarrow \boxed{1.f = f}$$

(1 is the unit element of the field $\mathbb{R}$)

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

$\underline{\text{Ex:}}$ $\quad \mathbb{R}^{\infty} = \{ (a_n) : (a_n)$ is a sequence of real numbers $\}$

This is a vector space over $\mathbb{R}$

$$(a_n) + (b_n) = (a_n + b_n)$$

$$c\,(a_n) = (c\,a_n) \text{ where } c \in \mathbb{R}.$$

$$\begin{array}{lllllll}
\mathbb{N} = & 1 & 2 & 3 & 4 & 5 & 6 \\
(a_n): & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \; \cdots \\
(b_n): & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \; \cdots
\end{array}$$

$$\boxed{(a_n)+(b_n)} \rightarrow \{ a_1+b_1 \;\; a_2+b_2 \;\; a_3+b_3 \;, \cdots \}$$

$$\boxed{c\,(a_n)} \rightarrow \{ ca_1 \;\; ca_2 \;\; ca_3 \,, \cdots \}$$

Ex: Let $R_n(t)$ be the set of all polynomials (in variable t) of degree $\leq n$ with with real coefficients.

e.g. For $n=3$, $R_3(t)$ is the set of polynomials (in variable t) of degree ≤ 3.

Note: $a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n$ is a polynomial (in variable of t) of degree n

Show that $R_n(t)$ is a vector space over the field $\mathbb{R}$.

(The zero polynomial is regarded as an element of $R_n(t)$ for $n = 0, 1, 2, \dots$)

Note: The set of all polynomials of degree n with real coefficients is not a vector space over $\mathbb{R}$.
(Closure property of addition is not satisfied)

Ex: The set $R(t)$ of all polynomials with real coefficients is a vector space over $\mathbb{R}$.

- Note that $R_n(t) \subset R(t)$ for any positive integer n.

Note: Vector spaces can also be defined over $\mathbb{C}$ or any other field.

Back to field:

Consider $\{0, 1\} = \mathbb{Z}_2$ (notation)

Define: addition and multiplication by:

$\oplus$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

(Arithmatic modulo 2)

- $\mathbb{Z}_2$ is a field. (Check!)

So, we can consider $\mathbb{Z}_2^n$: The set of n-tuples whose entries are from $\mathbb{Z}_2$.

$$= \{ (x_1, x_2, \dots x_n) : x_i = 0 \text{ or } 1 \}$$

A typical element of $\mathbb{Z}_2^n$ is the n-tuple $(0, 1, 1, 0, \dots \dots 0)$

$\mathbb{Z}_2^n$ is extremely important in coding.

Ex: $1.((1+0)+1)+1$

$$= 1.(1+1)+1 = 1.0+1 = 0+1$$
$$= \boxed{1}$$

Ex: Using modular arithmatic (mod 2) find

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Modular Arithmatic :

Let n be a positive integer.

For any integer a,

define $a \pmod{n}$ = The remainder when a is divided by n

Note that $0 \le$ remainder $< n$

Ex: $10 \pmod{3} = 1$

$7 \pmod{4} = 3$

Now for any positive integer n

define $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

Define : $\left.\begin{array}{l} a \oplus b = (a+b) \bmod n \\ a * b = (a \cdot b) \bmod n \end{array}\right\}$ for all $a, b \in \mathbb{Z}_n$

So, $\mathbb{Z}_2 = \{0, 1\}$ In $\mathbb{Z}_2$, $1 + 1 = 2 = 0$ since $2 \pmod{2} = 0$

$\mathbb{Z}_3 = \{0, 1, 2\}$

In $\mathbb{Z}_3$, $2 + 1 = 3 = 0$ (since $3 \pmod{3} = 0$)

$2 + 2 = 4 = 1$ (since $4 \pmod{3} = 1$)

Ex: Show that $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are fields.

Ex: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Show that $\mathbb{Z}_4$ is not a field.

Proposition: $\mathbb{Z}_p$ is a field if and only if p is a prime.

Note: One direction '$\Rightarrow$' will be proved.
The other direction '$\Leftarrow$' will not be proved since it will need more modular arithmatic.

Ex: We have seen examples of fields such as: $\underbrace{\mathbb{Q} \subset \mathbb{R}} \subset \mathbb{C}$

Question: Are there any field between $\mathbb{Q}$ and $\mathbb{R}$?

Define:

$$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \ : \ a, b \in \mathbb{Q} \}$$

clearly $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$

- Show that $\mathbb{Q}(\sqrt{2})$ is a field with respect to usual addition and multiplication of real numbers.