MTH 100: Lecture 14

Ex: $\mathbb{Z}_2 = \{0, 1\}$ is a field. $\left(\begin{array}{l} 1 * 1 = 1 \\ 1^{-1} = 1 \text{ in } \mathbb{Z}_2 \end{array} \right)$

Ex: $\mathbb{Z}_3 = \{0, 1, 2\}$ is a field.

$1 \times 1 = 1 \pmod 3 = 1$
So, $1^{-1} = 1$ in $\mathbb{Z}_3$
$2 * 2 = 4 \pmod 3 = 1$
So, $2^{-1} = 2$ in $\mathbb{Z}_3$

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

Now $2 \in \mathbb{Z}_4$, $2 \neq 0$

and $2 * 2 = 4 \pmod 4 = 0$

So, $2 * 2 = 0$ in $\mathbb{Z}_4$.

So, 2 is a zero divisor in $\mathbb{Z}_4$.

So, $\mathbb{Z}_4$ can not be a field.

Ex: $\mathbb{Z}_6$ is not a field.

Ex: Let n be a composite integer. Then $\mathbb{Z}_n$ is not a field. $\left(\begin{array}{l} n = rk \\ 1 < r < n \\ 1 < k < n \end{array} \right)$

Zero divisor:

A zero divisor is a non zero element $a\ (\neq 0)$ such that there exists $b\ (\neq 0)$ satisfying

$$a * b = 0$$

- A field cannot have a zero divisor

Proof: Let F be a field and $a \in F$, $a \neq 0$ is a zero divisor in F.

So, there exists $b \in F$ $(b \neq 0)$ such that

$$a * b = 0$$

Since $b \neq 0$ and $b \in F$, $b^{-1} \in F$

Now from the above, $(a * b) * b^{-1} = 0 * b^{-1}$

$\Rightarrow a * (b * b^{-1}) = 0$ (By property of field)

$\Rightarrow a * (e) = 0$ (where e = multiplicative identity in F)

$\Rightarrow a = 0$, a contradiction

So, $\boxed{F \text{ doesnot have a zero divisor}}$

Theorem: $\mathbb{Z}_p$ is a field iff (if and only if) p is a prime.

(Note: will prove one part of the theorem)

Proof: '$\Rightarrow$': **Given:** $\mathbb{Z}_p$ is a field.

Want to show: p is a prime.

We will prove it BWOC (BWOC $\equiv$ By way of contradiction)

Let us assume that p is not a prime.

Then $p = rk$ where $1 < r < p$, $1 < k < p$

$$r * k = rk \pmod p = p \pmod p = 0$$

So, r and k are both divisors of zero in $\mathbb{Z}_p$

Thus $\mathbb{Z}_p$ can not be a field, a contradiction.

Hence p has to be a prime.

'$\Leftarrow$': (This requires more of modular arithmetic).

Consequences of the Vector Space definition:

Proposition: Let V be a vector space over a field F.

Then (a) The zero vector is unique.

(b) The additive inverse vector of any vector u is unique

(We use the notation $-u$ for the inverse vector of u.)

(c) $0.u = \bar{0}$ $\forall\, u \in V$

(d) $c.\bar{0} = \bar{0}$ $\forall\, c \in F$

(e) $-u = (-1)u$ $\forall\, u \in V$

(f) Cancellation Law:

If $u + v = u + w$

then $v = w$ $\forall\, u, v, w \in V$

Proof: Exercise

① let $\bar{0}$ and $\bar{0}_1$ be zero vectors in V

$\bar{0} + u = u + \bar{0} = u \quad \forall\, u \in V \quad \cdots ①$

$\bar{0}_1 + u = u + \bar{0}_1 = u \quad \forall\, u \in V \quad \cdots ②$

Let $u = \bar{0}_1$ in ①. Then $\bar{0} + \bar{0}_1 = \bar{0}_1$ $\}$

Now let $u=\bar{0}$ in ②. Then $\bar{0}+\bar{0}_1=\bar{0}$, | Combining we get $\boxed{\bar{0}=\bar{0}_1}$

② Let $u \in V$, Let v and v_1 be two additive inverses of u

So, $u+v = v+u = \bar{0}$ ....①

and $u+v_1 = v_1+u = \bar{0}$ .....②

From ② $(u+v_1)+v = \bar{0}+v = v$

By ② $(v_1+u)+v = v$

$\Rightarrow v_1+(u+v) = v$

$\Rightarrow v_1+\bar{0} = v$ (By ①)

$\Rightarrow \boxed{v_1 = v}$

So, additive inverse is unique.

(c), (d), (e) : Exercise

(f) Given $u+v = u+w$

Now $-u \in V$

and so, $(-u)+(u+v) = (-u)+(u+w)$

$\Rightarrow ((-u)+u)+v = ((-u)+u)+w$

$\Rightarrow 0+v = 0+w$

$\Rightarrow \boxed{v=w}$

• When we gave examples of vector spaces, we noticed some subsets:

e.g. $C \subset R^{\infty}$, $\quad C^{1}[a,b] \subset \underbrace{C[a,b]}$

$$R_0(t) \subset R_1(t) \subset R_2(t) \subset \dots \subset R_n(t) \subset R(t)$$

Subspace:

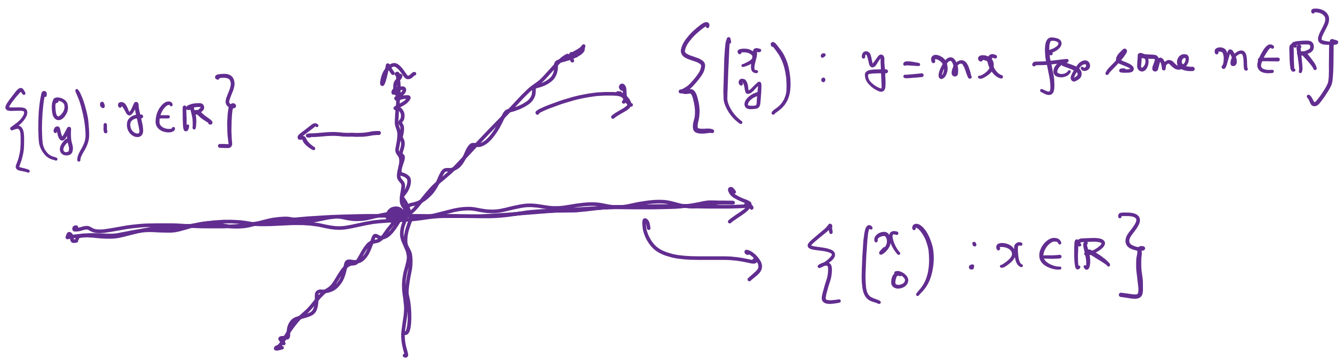
Let V be a vector space over the field F.

A (vector) subspace of V is a nonempty subset of V which is also a vector space over F with the operations of vector addition and scalar multiplication taken from V.

Ex: If V is any vector space over F, then $\{0\}$ (zero subspace) and V are always subspaces of V.

Subspaces other than V and $\{0\}$ are known as proper subspaces.

<u>Ex:</u> $\mathbb{R}^2$ is a vector space over $\mathbb{R}$.



- The set $\left\{\begin{pmatrix}x\\0\end{pmatrix} : x \in \mathbb{R}\right\}$ is a proper subspace of $\mathbb{R}^2$.

- The set $\left\{\begin{pmatrix}0\\y\end{pmatrix} : y \in \mathbb{R}\right\}$ is a proper subspace of $\mathbb{R}^2$.

- The set $\left\{\begin{pmatrix}x\\y\end{pmatrix} : y = mx \text{ for some } m \in \mathbb{R}\right\}$ is a proper subspace of $\mathbb{R}^2$.

Question: Is $\mathbb{R}$ a subspace of $\mathbb{R}^2$?

$\mathbb{R}$ is not even a subset of $\mathbb{R}^2$

$$\mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}$$

(two tuple)

$$\mathbb{R} = \{ x : x \in \mathbb{R} \}$$

(one tuple)

Now $\left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}$ is a subspace of $\mathbb{R}^2$

It behaves very much like $\mathbb{R}$, but is logically distinct from $\mathbb{R}$

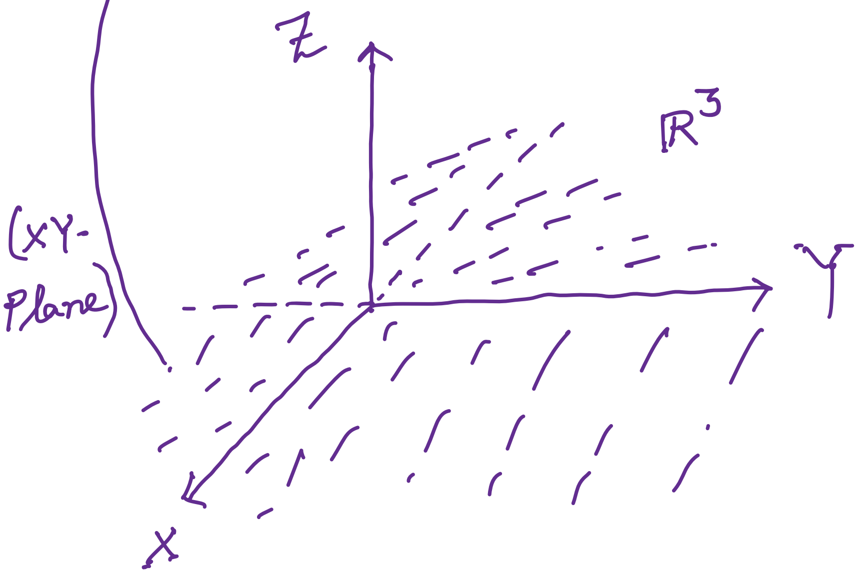
Example: $\mathbb{R}^3$ is a vector space over $\mathbb{R}$.

Question: Is $\mathbb{R}^2$ a subspace of $\mathbb{R}^3$?

No: $\mathbb{R}^2$ is not even a subset of $\mathbb{R}^3$

The set $\left\{ \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} : x, y \in \mathbb{R} \right\}$

is a subspace of $\mathbb{R}^3$ which behaves very much like $\mathbb{R}^2$, but is logically distinct from $\mathbb{R}^2$.



Test for Subspaces

Proposition: Let V be a vector space over a field F.

A subset W of V is a subspace if and only if it satisfies the following three properties:

(1) The zero vector 0 is in W

(2) W is closed under addition

i.e. $u+v \in W \quad \forall\, u, v \in W$

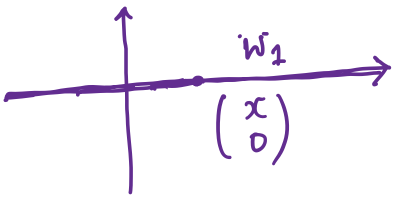
(3) W is closed under scalar multiplication

i.e. $cu \in W \quad \forall\, c \in F$ and $\forall\, u \in W$

Note: (1) can be replaced by (1')

(1') : W is nonempty.

Ex(1) $\mathbb{R}^2$ is a vector space over $\mathbb{R}$



$W_1 = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}$ is a subspace.

Check:

(1) $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \in W_1$

(2) If $\begin{pmatrix} x_1 \\ 0 \end{pmatrix}, \begin{pmatrix} x_2 \\ 0 \end{pmatrix} \in W_1$, then

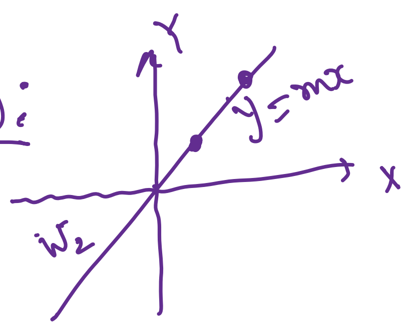
$$\begin{pmatrix} x_1 \\ 0 \end{pmatrix} + \begin{pmatrix} x_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix} \in W_1$$

(3) If $\begin{pmatrix} x \\ 0 \end{pmatrix} \in W_1$ and $c \in \mathbb{R}$,

then $c \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} cx \\ 0 \end{pmatrix} \in W_1$

Hence, W_1 is a subspace of $\mathbb{R}^2$

Ex(2):



$W_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y = mx \atop x, y \in \mathbb{R} \right\}$

Check

(1) $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \in W_2$

(2) If $\begin{pmatrix} x_1 \\ mx_1 \end{pmatrix}$ and $\begin{pmatrix} x_2 \\ mx_2 \end{pmatrix} \in W_2$

then $\begin{pmatrix} x_1 \\ mx_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ mx_2 \end{pmatrix} = \begin{pmatrix} x_1+x_2 \\ mx_1+mx_2 \end{pmatrix}$

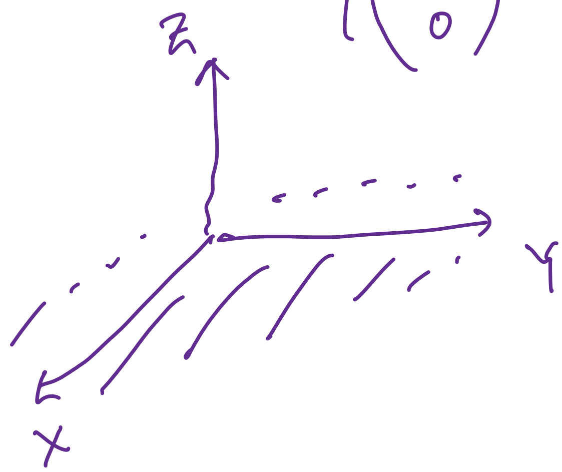
$$= \begin{pmatrix} x_1+x_2 \\ m(x_1+x_2) \end{pmatrix} \in W_2$$

(3) If $c \in \mathbb{R}$ and $\begin{pmatrix} x \\ mx \end{pmatrix} \in W_2$

then $c \begin{pmatrix} x \\ mx \end{pmatrix} = \begin{pmatrix} cx \\ c(mx) \end{pmatrix} = \begin{pmatrix} cx \\ m(cx) \end{pmatrix} \in W_2$

Hence W_2 is a subspace of $\mathbb{R}^2$.

Ex: Let $W = \left\{ \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} : x, y \in \mathbb{R} \right\} \subset \mathbb{R}^3$



Show that W is a subspace of $\mathbb{R}^3$