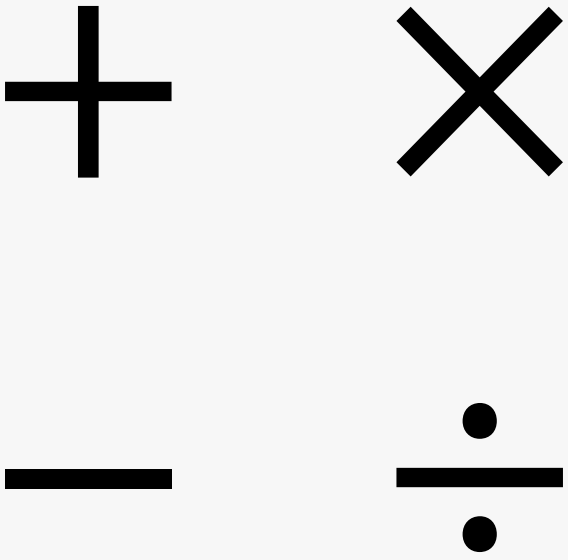
EE 635: Applied Linear Algebra
Assignment 1

Soumen Kumar Mondal
23M2157@iitb.ac.in



32. Let $\mathbb{V}$ be a vector space such that $p, q, r, s \in \mathbb{V}$. Suppose $\mathbb{S} := \langle\{r, s\}\rangle$, $\mathbb{P} := \langle\{p, r, s\}\rangle$, $\mathcal{Q} := \langle\{q, r, s\}\rangle$ are subspaces of $\mathbb{V}$. If $q \in \mathbb{P}$ but $q \notin \mathbb{S}$, show that $p \in \mathcal{Q}$.

Given that $S = \langle \{r, s\} \rangle$
$P = \langle \{p, r, s\} \rangle$
$Q = \langle \{q, r, s\} \rangle$
} S, P, Q are subspaces of $\mathbb{V}$ over field $\mathbb{F}$.

We want to prove that

$$(q \in P) \wedge (q \notin S) \longrightarrow (p \in Q) \qquad \text{(i)}$$

Notations: Vector space $(\mathbb{V}, \mathbb{F}, +_v, \cdot)$
Field $(\mathbb{F}, +, \times)$

span of S, $\langle S \rangle$ is defined as:

$$\langle S \rangle := \left\{ s \in \mathbb{V} \;\middle|\; s = \sum_{i=1}^{n} c_i s_i \;,\; \forall s_i \in S, c_i \in \mathbb{F} \right\}$$

Assume the hypothesis is true
$q \in P$ and $q \notin S$

Since $q \in P$ therefore, q can be expressed as linear combination of $\{p, r, s\}$.

$$q = a \cdot p +_v b \cdot r +_v c \cdot s \quad [a, b, c \in \mathbb{F}] \qquad \text{(ii)}$$

It is also assumed that $q \notin S$ that means,

$q \notin \langle \{r, s\} \rangle$

So $q \neq x \cdot r +_W y \cdot s \quad [x, y \in \mathbb{F}]$. ——— (iii)

From (ii), it is evident that a, b, c can't be all 0 at the same time because if it happens then $q = 0_W$. Then we can express 0_W as linear combination of r, s which is a contradiction of $q \notin S$. Since S is a subspace of W (span of any subset of W is a subspace of W) so 0_W is always part of S.

Therefore, at least one of a, b, c must be non zero.

From (ii), if $a = 0$ and $b \neq 0, c \neq 0$ then also q is expressed in terms of r & s which is contradiction of $q \notin S$ since q can't be expressed by linear comb. of r & s.

Similarly if $a = 0$ then it doesn't matter what value b or c takes because q can always be expressed in terms of r & s. Therefore $a \neq 0$ to avoid contradiction.

So when $a \neq 0$ and $a \in \mathbb{F}$ therefore multiplicative inverse of a (a^{-1}) must exist in $\mathbb{F}$.

Multiply by a^{-1} in equation (ii), we get –

$$\Rightarrow a^{-1} \cdot q = (a^{-1} \times a) \cdot p +_{IV} (a^{-1} \times b) \cdot r +_{IV} (a^{-1} \times c) \cdot s$$

Assume, $a^{-1} \times b = d \in F$, $a^{-1} \times c = e \in F$

$a^{-1} \times a = 1_{IF} \in IF$ (mult. identity of IF)

$$\Rightarrow a^{-1} \cdot q = 1_{IF} \cdot p +_{IV} d \cdot r +_{IV} e \cdot s$$

$$\Rightarrow a^{-1} \cdot q = p +_{IV} d \cdot r +_{IV} e \cdot s$$

Since $(V, +_{IV})$ forms an Abelian group, the additive inverse of a vector $v \in V$, $(-_V v)$ will exist in V.

Add the additive inverse of $d \cdot r$ and $e \cdot s$ in both sides,

$$\Rightarrow a^{-1} \cdot q +_{IV} (-_{IV}(d \cdot r)) +_{V} (-_{IV} (e \cdot s)) = p +_{IV} 0_{IV} +_{IV} 0_{IV}$$

$$\Rightarrow p = a^{-1} \cdot q +_{IV} (-d) \cdot r +_{IV} (-e) \cdot s$$

(Note that $-d$, $-e$ are the additive inverse of d, e in IF)

clearly, p can be expressed as linear combination of q, r, s or $p \in \langle \{q, r, s\} \rangle$ or $p \in Q$. So the conclusion is true after assuming the hypothesis of the statement (i). So the statement (i) must be true.

(Hence Proved)

28. Suppose $\mathbb{V}$ is the vector space (over $\mathbb{R}$) of all functions from $\mathbb{R}$ to $\mathbb{R}$ while $\mathbb{V}_e$ and $\mathbb{V}_o$ are subsets of $\mathbb{V}$ containing functions that satisfy the property $f(x) = f(-x)$ and $f(x) = -f(-x)$, respectively.

(a) Prove that $\mathbb{V}_e$ and $\mathbb{V}_o$ are subspaces of $\mathbb{V}$.

(b) Show that $\mathbb{V} = \mathbb{V}_e \oplus \mathbb{V}_o$.

Vector space: $(\mathbb{V}, \mathbb{R}, +_V, \cdot)$

Field: $(\mathbb{R}, +, \times)$

$\mathbb{V}$ is the set of all functions f such that $f : \mathbb{R} \to \mathbb{R}$

$$\mathbb{V} = \{ f : \mathbb{R} \to \mathbb{R} \mid x \in \mathbb{R},\ f(x) \in \mathbb{R} \}$$

(i) Given that $\mathbb{V}_e \subseteq \mathbb{V}$ (subset)

$\mathbb{V}_e$ contains vectors (or function) such that it satisfies the property $f(x) = f(-x)$.

$$\mathbb{V}_e = \{ f : \mathbb{R} \to \mathbb{R} \mid x \in \mathbb{R},\ f(x) \in \mathbb{R},\ f(x) = f(-x) \}$$

We have to prove that $\mathbb{V}_e$ is a subspace of $\mathbb{V}$ over $\mathbb{R}$.

Subspace test criteria: $\mathbb{W}$ is a subspace of $\mathbb{V}$ over $\mathbb{F}$ if and only if -

$$\forall u, v \in \mathbb{W},\ c \in \mathbb{F} \quad [\, c \cdot u +_V v \in \mathbb{W} \,] \qquad \text{---(i)}$$

Choose 2 arbitrary vectors f, g from $\mathbb{V}_e$.

$f(x) := f(-x)$ and $g(x) := g(-x)$ $\forall x \in \mathbb{R}$

It is easy to see that since $f, g \in W_e$ and f, g are functions from $\mathbb{R}$ to $\mathbb{R}$ so $f, g \in V$ hence $+_{ve}, \cdot$ operations will be closed in V.

Consider the vector $w = c \cdot f +_v g \quad [w \in V]$

$$w(x) := \left(c \cdot f +_v g\right)(x) \qquad [\because f, g \in V]$$

$$= c \times f(x) + g(x)$$

$$= c \times f(-x) + g(-x)$$

$$= \left(c \cdot f +_v g\right)(-x)$$

$$= w(-x)$$

Therefore, $w \in W_e$ by the definition of W_e.
For any arbitrary, f, g, c we have shown that $w \in W_e$ therefore by universal generalization we can conclude that.

$$\forall_{f, g \in W_e,\, c \in \mathbb{F}} \left[w = c \cdot f +_v g \in W_e \right]$$

Therefore, W_e is a subspace of V over $\mathbb{R}$. (Proved)

(ii) Given that $W_o \subseteq V$ (subset)

W_o contains vectors (or function) such that it satisfies the property $f(x) = -f(-x)$

$$W_o = \{ f : \mathbb{R} \to \mathbb{R} \mid x \in \mathbb{R},\ f(x) \in \mathbb{R},\ f(x) = -f(-x) \}$$

We have to prove that W_o is a subspace of W over $\mathbb{R}$

Choose 2 arbitrary vectors f, g from W_o

$f(x) := -f(-x)$ and $g(x) := -g(-x)$ $\forall x \in \mathbb{R}$

From the previous arguments, $f, g \in W$.

Consider the vector $w = c \cdot f +_v g$ $[w \in W]$

$$w(x) := (c \cdot f +_v g)(x) \qquad [\because f, g \in W]$$

$$= c \times f(x) + g(x)$$

$$= c \times (-f(-x)) + (-g(-x))$$

$$= -(c \times f(-x) + g(-x))$$

$$= -((c \cdot f +_v g)(-x))$$

$$= -(w(-x))$$

$$= -w(-x)$$

Therefore, $w \in W_o$ by the definition of W_o.
By the same universal generalization argument, we can show that W_o is the subspace of V over $\mathbb{R}$.
(proved)

(iii) We need to show that $V = W_e \oplus W_o$

That means we need to prove 2 things —

(i) All vectors $v \in V$ must be uniquely expressed as sum of 2 vectors v_e, v_o from W_e & W_o.

Since W_e, W_o are subspaces of V over $\mathbb{R}$,

$$W_e \oplus W_o := \{ v \in V \mid v = v_e + v_o,\ \exists!\, v_e \in W_e, \exists!\, v_o \in W_o \}$$

(ii) $W_e \oplus W_o$ set must span the whole vector space V because 2 sets are equals when they have same number of elements.

Assume the representation is not unique.
Take an arbitrary vector $v \in V$.
Suppose, $v = v_e +_v v_o$ where $v_e \in W_e, v_o \in W_o$

$v = v_e' +_v v_o'$ where $v_e' \in W_e, v_o' \in W_o$

Also assume that $v_e \neq v_e'$ or $v_o \neq v_o'$ to make sure the representition is not unique.

Since both represent the same vector v, we can equate

$$v_e +_v v_o = v_e' +_v v_o'$$

$$\Rightarrow v_e -_v v_e' = v_o' -_v v_o = p$$

Since W_e and W_o are subspaces of V over $\mathbb{R}$, all the vectors must have additive inverse.

Therefore, $-_v v_e' \in W_e$ and $-_v v_o \in W_o$

Hence $v_e -_v v_e' \in W_e$ as W_e is a subspace.

$v_o' -_v v_o \in W_o$ as W_o is a subspace.

Therefore, p belongs to both W_e and W_o which means $p \in W_e \cap W_o$.

We know that $W_e \cap W_o = \{0_v\} \longrightarrow W_e + W_o = W_e \oplus W_o$

Therefore, we have to show that $W_e \cap W_o = \{0_v\}$.

Suppose, $f \in W_e$ and $f \in W_o$.

$f(x) = f(-x)$ and $f(x) = -f(-x)$.

$\Rightarrow f(x) = f(-x) = -f(x) \quad \forall x \in \mathbb{R}$

$\Rightarrow 2 \times f(x) = 0 \quad \forall x \in \mathbb{R}$.

$\Rightarrow f(x) = 0 \quad \forall x \in \mathbb{R}$

That means $f(x) = 0 \quad \forall x \in \mathbb{R}$ hence f must be the zero vector function which maps all x to 0.

That means $f = 0_{\mathbb{V}}$.

Hence $\mathbb{V}_e \cap \mathbb{V}_o = \{0_{\mathbb{V}}\}$. Therefore, the sum is uniquely represented.

Now we have to show that $\mathbb{V}_e \oplus \mathbb{V}_o = \{f \mid f = f_o + f_e\}$ will span the entire space $\mathbb{V}$ $\forall x \in \mathbb{R}$ where,

$f \in \mathbb{V}$, $f_o \in \mathbb{V}_o$, $f_e \in \mathbb{V}_e$

Consider $f_e(x) = 2^{-1} \times f(x) - 2^{-1} \times f(-x)$

$f_o(x) = 2^{-1} \times f(x) + 2^{-1} \times f(-x)$

Adding 2 equations, we can see that,

$f(x) = f_o(x) + f_e(x) \quad \forall x \in \mathbb{R} \quad \Rightarrow f = f_o +_v f_e$

That means $\forall x \in \mathbb{R}$, $f(x) = (f_o +_v f_e)(x)$ can span the entire space $\mathbb{V}$ and we have proved that the representation is unique. (Hence proved)

26. Denote $\mathcal{F}[\mathbb{N};\mathbb{F}]$, the vector space of all infinite sequences of elements in $\mathbb{F}$, as $\mathbb{F}^\infty$. Which of the following subsets of $\mathbb{R}^\infty$ are subspaces of $\mathbb{R}^\infty$? Justify your answer in each case.
(a) $\mathbb{W} := \{f \in \mathbb{R}^\infty : f(n+1) \leq f(n)\ \forall n \in \mathbb{N}\}$
(b) $\mathbb{W} := \{f \in \mathbb{R}^\infty : \lim_{n\to\infty} f(n) = 0\}$
(c) $\mathbb{W} := \{f \in \mathbb{R}^\infty : \exists a_f, d_f \in \mathbb{R} \text{ so that } f(n) = a_f + (n-1)d_f\}$
(d) $\mathbb{W} := \{f \in \mathbb{R}^\infty : \exists a_f, r_f \in \mathbb{R} \text{ so that } f(n) = a_f r_f^{n-1}\}$
(e) $\mathbb{W} := \{f \in \mathbb{R}^\infty : f(n) \neq 0 \text{ only for finitely many } n \in \mathbb{N}\}$
(f) $\mathbb{W} := \{f \in \mathbb{R}^\infty : f(n) = 0 \text{ for infinitely many } n \in \mathbb{N}\}$

Vector space : $(\mathbb{V}, \mathbb{F}, +_v, \cdot)$

Field : $(\mathbb{F}, +, \times)$

$\mathbb{R}^\infty = \{v_1, v_2, \ldots\}$ where $v_i = (x_1, x_2, \ldots)$

$(\forall x_i \in \mathbb{R})$ where $\mathbb{V} = \mathbb{R}^\infty$ and $\mathbb{F} = \mathbb{R}$.

$\mathbb{R}^\infty$ is the set of all infinite sequences of real numbers. Each element in $\mathbb{R}^\infty$ is a vector of ∞ tuples of real numbers.

(a) $\mathbb{W} := \{ f \in \mathbb{R}^\infty \mid f(n+1) \leq f(n)\ \forall n \in \mathbb{N} \}$

Take 2 arbitrary vectors $g, h \in \mathbb{W}$ and $c \in \mathbb{R}$

Consider $w := c \cdot g +_v h$

Since $g, h \in \mathbb{W}$ so $g, h \in \mathbb{V}$ (by definition of $\mathbb{W}$) hence the $+_v, \cdot$ operations are closed in $\mathbb{V}$. Hence $w \in \mathbb{V}$.

$$w(n) = (c \cdot g +_v h)(n) \quad \text{---(i)}$$

$$w(n+1) = (c \cdot g +_v h)(n+1) \quad \text{---(ii)}$$

We can write -

$$w(n) = c \times g(n) + h(n)$$

$$w(n+1) = c \times g(n+1) + h(n+1)$$

Given $g(n+1) \leq g(n)$ and $h(n+1) \leq h(n)$

Check. $w(n+1) \overset{?}{\leq} w(n)$.

Since $g(n+1) \leq g(n)$

$\Rightarrow g(n+1) = g(n) - K_1$ where $K \in \mathbb{R}$ and $K_1 \geq 0$

and $h(n+1) \leq h(n)$

$\Rightarrow h(n+1) = h(n) - K_2$ where $K_2 \in \mathbb{R}$ and $K_2 \geq 0$

Consider $w(n+1) = c \times g(n+1) + h(n+1)$

$$= c \times (g(n) - K_1) + h(n) - K_2$$

$$= (c \times g(n) + h(n)) - (c \times K_1 + K_2)$$

$$= w(n) - (c \times K_1 + K_2)$$

We know that $K_1 \geq 0$, $K_2 \geq 0$ but c can be anything hence there may be a case when $K_2 = 0$ and $c < 0$ then $w(n+1) < w(n)$ thus failing to be in set $\mathbb{W}$.

Therefore $w(n+1) \leq w(n)\ \forall n \in \mathbb{N}$ is not true.
Hence $\mathbb{W}$ is not a subspace of $\mathbb{R}^\infty$ over $\mathbb{R}$.

(b) $$\mathbb{W} = \left\{ f \in \mathbb{R}^\infty \;\middle|\; \lim_{n\to\infty} f(n) = 0 \right\}$$

Take 2 arbitrary vectors $g \& h \in \mathbb{W}$ and $c \in \mathbb{R}$.
Consider,
$$w := c \cdot g +_v h$$

Since $g, h \in \mathbb{W}$ so $g, h \in \mathbb{V}$ (by definition of $\mathbb{W}$) hence the $+_v, \cdot$ operations are closed in $\mathbb{V}$. Hence $w \in \mathbb{V}$.

$$w(n) = \left(c \cdot g +_v h\right)(n) = c \times g(n) + h(n)$$

Taking limits on both sides –

$$\lim_{n\to\infty} w(n) = \lim_{n\to\infty} \left(c \times g(n) + h(n) \right)$$

$$= \lim_{n\to\infty} c \times g(n) + \lim_{n\to\infty} h(n)$$

$$= c \times \left[\lim_{n\to\infty} g(n)\right] + \left[\lim_{n\to\infty} h(n)\right]$$

Since we have $\lim_{n\to\infty} g(n) = 0$ as $g \in W$

$\lim_{n\to\infty} h(n) = 0$ as $h \in W$

Therefore, $\lim_{n\to\infty} w(n) = c \times 0 + 0 = 0$

which implies $w \in W$.

By the argument of universal generalization, we can conclude that W is a subspace of V over F.

(c) $W := \{ f \in \mathbb{R}^{\infty} \mid \exists a_f, d_f \in \mathbb{R} \text{ s.t. } f(n) = a_f + (n-1) d_f \}$

Take 2 arbitrary vectors $g \& h \in W$ and $c \in \mathbb{R}$.

Consider,

$$w := c \cdot g +_v h$$

Since $g, h \in W$ so $g, h \in V$ (by definition of W) hence the $+_v, \cdot$ operations are closed in V. Hence $w \in V$.

$$w(n) = (c \cdot g +_v h)(n)$$

$$= c \times g(n) + h(n)$$

$$= c \times \left(a_f + (n-1) \times d_f\right) + \left(a_f' + (n-1) \times d_f'\right)$$

$[a_f, d_f, a_f', d_f' \in \mathbb{R}]$

$$= c \times a_f + c \times (n-1) \times d_f + a_f' + (n-1) \times d_f'$$

$$= \left(c \times a_f + a_f'\right) + (n-1) \times \left(c \times d_f + d_f'\right)$$

Let, $a_f'' = c \times a_f + a_f'$

$d_f'' = c \times d_f + d_f'$

Since $(\mathbb{R}, +, \times)$ is a field so all the operations are closed in $\mathbb{R}$. Therefore $a_f'' \in \mathbb{R}$ and $d_f'' \in \mathbb{R}$.

Therefore $w(n) = a_f'' + (n-1)\, d_f''$

Hence by the definition of $\mathbb{W}$ we can say $w \in \mathbb{W}$.

Therefore, $\mathbb{W}$ is a subspace of $\mathbb{V}$ over $\mathbb{F}$

(d) $\mathbb{W} := \{ f \in \mathbb{R}^{\infty} \mid \exists\, a_f, d_f \in \mathbb{R} \text{ s.t. } f(n) = a_f \times r_f^{\,n-1} \}$

Take 2 arbitrary vectors $g \& h \in \mathbb{W}$ and $c \in \mathbb{R}$.

Consider,

$$w := c \cdot g +_v h$$

Since $g, h \in \mathbb{W}$ so $g, h \in \mathbb{V}$ (by definition of $\mathbb{W}$) hence the $+_v, \cdot$ operations are closed in $\mathbb{V}$. Hence $w \in \mathbb{V}$.

$$w(n) = (c \cdot g +_v h)(n)$$

$$= c \times g(n) + h(n)$$

$$= c \times \left(a_f \times r_f^{\,n-1} \right) + \left(a_f' \times r_f'^{\,n-1} \right)$$

$[a_f, r_f, a_f', r_f' \in \mathbb{R}]$

In order $w(n)$ to be in the form of $a_f'' \times r_f''^{\,n-1}$ we have to represent a_f'', r_f'' in terms of a_f, r_f, a_f', r_f' and c.

For the sake of contradiction, assume that,

$w(n) = a_f'' \times r_f''^{\,n-1} \quad \forall n \in \mathbb{N}$.

Suppose $w(1) = a_f'' \times r_f''^{\,0} = a_f''$

$$w(2) = a_f'' \times r_f''^{\,1} = a_f'' \times r_f''$$

It is a contradiction of the assumption that $w(n)$ form of $a_f'' \times r_f''^{\,n-1}$ is true for $\forall n \in \mathbb{N}$ but for $n = 1, 2$ we got 2 different form hence it is not possible to express $w(n)$ in the desired form.

Hence W is not a subspace of V over F

(e) $W := \{ f \in \mathbb{R}^{\infty} \mid f(n) \neq 0 \text{ only for finitely many } n \in \mathbb{N} \}$

Take 2 arbitrary vectors $g \& h \in W$ and $c \in \mathbb{R}$.
Consider,

$$w := c \cdot g +_v h$$

Since $g, h \in W$ so $g, h \in V$ (by definition of W) hence the $+_v, \cdot$ operations are closed in V. Hence $w \in V$.

$$w(n) = (c \cdot g +_v h)(n)$$

$$= c \times g(n) + h(n).$$

$g(n) \neq 0$ only for finitely many $n \in \mathbb{N}$.
$h(n) \neq 0$ only for finitely many $n \in \mathbb{N}$.

Suppose, $g(n) \neq 0$ for $n = n_1 < \infty$, $n_1 \in \mathbb{N}$
$h(n) \neq 0$ for $n = n_2 < \infty$, $n_2 \in \mathbb{N}$

If $c = 0$ then $w(n) \neq 0$ for n_2 number of n's. which is finite. So we can say $w \in W$ when $c = 0$

If $c \neq 0$ then $w(n) \neq 0$ for $\max(n_1, n_2)$ number of n's which is again finite. Because sum of 2 finite natural number is a finite natural number.

Hence we can say, $w(n) \neq 0$ for finite $n \in \mathbb{N}$. Which implies $w \in W$. Using arguments of universal generalization, we conclude that W is a subspace of V over F.

(f) $W := \{ f \in \mathbb{R}^{\infty} \mid f(n) = 0 \text{ for infinitely many } n \in \mathbb{N} \}$

Take 2 arbitrary vectors $g \& h \in W$ and $c \in \mathbb{R}$.
Consider,

$$w := c \cdot g +_v h$$

Since $g, h \in W$ so $g, h \in V$ (by definition of W) hence the $+_v, \cdot$ operations are closed in V. Hence $w \in V$.

$$w(n) = (c \cdot g +_v h)(n)$$
$$= c \times g(n) + h(n).$$

$g(n) = 0$ for n_1 times where $n_1 \to \infty$
$h(n) = 0$ for n_2 times where $n_2 \to \infty$

Since ∞ is not a number, we can't really say $\infty \in \mathbb{N}$ so we say $n_1, n_2 \in \mathbb{N}$ but it approaches to ∞.

Suppose $c = 0$, $w(n) = 0$ for n_2 times where $n_2 \to \infty$.
So we can say $w \in W$ for $c = 0$.

Suppose $c \neq 0$, $w(n) = 0$ for $\min(n_1, n_2)$ times where $n_1, n_2 \to \infty$. The minimum (n_1, n_2) is actually infinity because minimum 2 infinity quantity results to an infinity quantity. Therefore $w \in W$ for $c \neq 0$ also.

Hence for 2 arbitrary vectors u & v, we have shown that $w = c.u +_v v$ belongs to W hence by universal generalization, we can say for all $u, v \in W$, $w = c.u +_v v \in W$. Therefore, W is a subspace of V over $\mathbb{R}$.

22. Consider $\mathbb{W}_1 := \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix} : \alpha, \beta, \gamma \in \mathbb{F} \right\}$, and $\mathbb{W}_2 := \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} : x, y \in \mathbb{F} \right\}$, where $\mathbb{F}$ is a field. Show that $\mathbb{W}_1 \cap \mathbb{W}_2 = \text{span}\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right)$ and $\mathbb{W}_1 + \mathbb{W}_2 = \mathbb{F}^{2\times 2}$.

$$W_1 := \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix} \;\middle|\; \alpha, \beta, \gamma \in F \right\}$$

$$W_2 := \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \;\middle|\; x, y \in F \right\}$$

To find the intersection of W_1, W_2, we have to find the matrices that are present in both W_1 and W_2. $W_1 \cap W_2$ will be set of matrices that satisfies both the form given by W_1 and W_2.

Consider $W_1 \cap W_2 := \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| \forall_{ij}\ a_{ij} \in F \right\}$

$\left.\begin{aligned} a_{11} &= \alpha \\ a_{12} &= \beta \\ a_{21} &= \gamma \\ a_{22} &= 0 \end{aligned}\right\}$ from W_1 matrices and $\left.\begin{aligned} a_{11} &= x \\ a_{12} &= 0 \\ a_{21} &= 0 \\ a_{22} &= y \end{aligned}\right\}$ from W_2 matrices

Since these 2 forms are not compatible, the only way for a matrix to be in the intersection $W_1 \cap W_2$ is if it satisfies both form simultaneously.

$\left.\begin{aligned} a_{12} &= \beta \\ a_{12} &= 0 \end{aligned}\right\}$ if $\beta \neq 0$ then $a_{12} \neq 0$ and $a_{12} = 0$ so a_{12} can't exist in F.

Therefore the only way for a_{12} that exists in F is the possibility when $\beta = 0$ hence $a_{12} = 0$

By the similar arguments, $a_{21} = 0$, $a_{22} = 0$

$\left.\begin{aligned} a_{11} &= \alpha \\ a_{11} &= x \end{aligned}\right\}$ The solution a_{11} exists in F if $\alpha = x$

Assume that $\alpha = x = c_1$ (say) therefore, $a_{11} = c_1$ where $c_1 \in F$.

Therefore, $W_1 \cap W_2 = \left\{ \begin{bmatrix} c_1 & 0 \\ 0 & 0 \end{bmatrix} \;\middle|\; c_1 \in \mathbb{F} \right\}$

$W_1 \cap W_2 = \left\{ c_1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \;\middle|\; c_1 \in \mathbb{F} \right\}$.

suppose, a set $S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

$$\text{span}(S) := \left\{ w \in S \;\middle|\; w = \sum_{i=1}^{1} c_i s_i \,,\; s_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\; \forall_i\, c_i \in \mathbb{F},\; \forall s_i \in S \right\}$$

$$= \left\{ c_1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \;\middle|\; c_1 \in \mathbb{F} \right\}$$

$= W_1 \cap W_2$ (Hence proved)

We have to prove that $W_1 + W_2 = \mathbb{F}^{2\times 2}$

That means the sum of sets W_1 and W_2 will span the entire vector space $\mathbb{F}^{2\times 2}$

$$\mathbb{F}^{2\times 2} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \;\middle|\; \forall_{ij}\, a_{ij} \in \mathbb{F} \right\} = V \text{ (let)}$$

$\{ij\}$

$\mathbb{F}^{2\times2}$ is a vector space over field $\mathbb{F}$.

$$\mathbb{W}_1 + \mathbb{W}_2 = \left\{ \omega \in \mathbb{W} \;\middle|\; \omega = \omega_1 +_V \omega_2 \text{ , } \omega_1 \in \mathbb{W}_1 \text{ , } \omega_2 \in \mathbb{W}_2 \right\}$$

Since, $\omega_1 = \begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix}$, $\alpha, \beta, \gamma \in \mathbb{F}$

$$\omega_2 = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \text{ , } x, y \in \mathbb{F}$$

Consider $\omega = \omega_1 +_V \omega_2$

Since $\omega_1 \in \mathbb{F}^{2\times2}$ and $\omega_2 \in \mathbb{F}^{2\times2}$ therefore $+_V$ is closed in $\mathbb{F}^{2\times2}$ hence $\omega \in \mathbb{F}^{2\times2}$.

$$\omega = \begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix} +_{\mathbb{W}} \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} := \begin{bmatrix} \alpha+x & \beta+0 \\ \gamma+0 & 0+y \end{bmatrix}$$

$$= \begin{bmatrix} \delta & \beta \\ \gamma & y \end{bmatrix}$$

(consider $\delta = \alpha + x$, since $\mathbb{F}$ is a field so $+$ operation is closed in $\mathbb{F}$ hence $\delta \in \mathbb{F}$)

Note that $\delta, \beta, \gamma, y \in \mathbb{F}$ and ω takes the form

defined in $\mathbb{F}^{2\times 2}$ in equation (1). Therefore, we can write the $W_1 + W_2$ as -

$$W_1 + W_2 = \left\{ \begin{bmatrix} \delta & \beta \\ \gamma & y \end{bmatrix} \;\middle|\; \delta, \beta, \gamma, y \in \mathbb{F} \right\}$$

$$= \mathbb{F}^{2\times 2}$$

So $W_1 + W_2$ spans the entire space $\mathbb{F}^{2\times 2}$. (Hence proved)

15. Consider the set of integers, $\mathbb{Z}$, with 'addition', $\oplus$ and 'multiplication', $\otimes$ defined as: $x \oplus y = x + y - 1$, and $x \otimes y = x + y - xy$. Determine the multiplicative and additive identities, if they exist. Is $(\mathbb{Z}, \oplus, \otimes)$ an integral domain?

Set of integers = $\mathbb{Z}$.

The operation $\oplus$ is defined as $x \oplus y = x + y - 1$

The operation $\otimes$ is defined as $x \otimes y = x + y - xy$

Let's check first whether $(\mathbb{Z}, \oplus)$ is an Abelian group.

(i) Closure of $\oplus$: $x \in \mathbb{Z}$, $y \in \mathbb{Z}$.

clearly, $x \oplus y = x + y - 1 \in \mathbb{Z}$.

Hence $\mathbb{Z}$ is closed under $\oplus$ operation.

(ii) Associativity of $\oplus$:

$$\forall a,b,c \in \mathbb{Z} \left[(a \oplus b) \oplus c = a \oplus (b \oplus c) \right]$$

Choose an arbitrary $a, b, c \in \mathbb{Z}$.

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c$$
$$= (a+b-1) + c - 1$$
$$= a+b+c-2$$

$$a \oplus (b \oplus c) = a \oplus (b+c-1)$$
$$= a + (b+c-1) - 1$$
$$= a+b+c-2$$

Therefore $\oplus$ is associative under $\mathbb{Z}$

(iii) Additive identity of $\mathbb{Z}$: e^+ is the add. identity of $\mathbb{Z}$.

$$\forall a \in \mathbb{Z} \left[(a \oplus e^+ = a) \wedge (e^+ \oplus a = a) \right]$$

Consider an arbitrary $a \in \mathbb{Z}$,

$$a \oplus e^+ = a + e^+ - 1 \quad , \quad e^+ \oplus a = e^+ + a - 1 = a + e^+ - 1$$

if $e^+ = 1$ then $a \oplus e^+ = a + 1 - 1 = a$ and $e^+ \in \mathbb{Z}$

Therefore, $\underline{e^+ = 1 \text{ for } \forall a \in \mathbb{Z} \text{ (additive identity)}}$

(iv) Additive inverse of elements of $\mathbb{Z}$:

$$\forall a \in \mathbb{Z} \left[\left(a \oplus i^+ = e^+ \right) \wedge \left(i^+ \oplus a = e^+ \right) \right]$$

where i^+ is the additive inverse of a.

$$a \oplus i^+ = a + i^+ - 1 = 1 \; ; \; i^+ \oplus a = i^+ + a - 1 = a + i^+ - 1$$

$$\Rightarrow i^+ = -a + 2 \in \mathbb{Z}.$$

Hence $\forall a \in \mathbb{Z}$ [additive inverse of a, $i^+ = -a+2$ exists in $\mathbb{Z}$]

(v) Commutativity of $\oplus$:

$$\forall a, b \in \mathbb{Z} \left[a \oplus b = b \oplus a \right]$$

Take arbitrary $a \& b \in \mathbb{Z}$

$$a \oplus b = a + b - 1$$

$$b \oplus a = b + a - 1 = a + b - 1$$ (since $+$ is commutative on $\mathbb{Z}$)

$$\Rightarrow a \oplus b = b \oplus a$$

Hence $\oplus$ is commutative on $\mathbb{Z}$.

Therefore, $(\mathbb{Z}, \oplus)$ forms an Abelian group.

Next we will check if $(\mathbb{Z}, \oplus, \otimes)$ is a Ring.

(i) $(\mathbb{Z}, \oplus)$ is an Abelian group (checked above)

(ii) Closure of $\otimes$ on $\mathbb{Z}$:

$$\forall x, y \in \mathbb{Z} \left[x \otimes y \in \mathbb{Z} \right]$$

Take arbitrary $x, y \in \mathbb{Z}$.

$$x \otimes y := x + y - xy$$

Since $+, \cdot$ are closed in $\mathbb{Z}$ hence $x \otimes y$ is also closed in $\mathbb{Z}$.

(iii) Associativity of $\otimes$ on $\mathbb{Z}$.

$$\forall x, y, z \in \mathbb{Z} \left[(x \otimes y) \otimes z = x \otimes (y \otimes z) \right]$$

Choose arbitrary $x, y, z \in \mathbb{Z}$.

$$(x \otimes y) \otimes z = (x + y - xy) \otimes z$$

$$= (x + y - xy) + z - (x + y - xy) \cdot z$$

$$= x + y - xy + z - xz - yz + xyz.$$

$$x \otimes (y \otimes z) = x \otimes (y + z - yz)$$

$$= x + (y+z-yz) - x\cdot(y+z-yz)$$

$$= x+y+z-yz-xy-xz+xyz$$

Numerically $(x \otimes y) \otimes z = x \otimes (y \otimes z)$.

Hence $\otimes$ is associative on $\mathbb{Z}$.

(iv) Distributivity of $\otimes$ over $\oplus$:

$$\forall x,y,z \in \mathbb{Z} \left[x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \quad \wedge \right.$$

$$\left. (x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z) \right]$$

Choose arbitrary $x,y,z \in \mathbb{Z}$.

$$x \otimes (y \oplus z) = x \otimes (y+z-1)$$

$$= x+(y+z-1) - x(y+z-1)$$

$$= x+y+z-1-xy-xz+x$$

$$= 2x+y+z-xy-xz-1$$

$$(x \otimes y) \oplus (x \otimes z) = (x+y-xy) \oplus (x+z-xz)$$

$$= x+y-xy+x+z-xz-1$$

$$= 2x+y+z-xy-xz-1$$

Hence $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Similarly,

$$(x \oplus y) \otimes z = (x+y-1) \otimes z$$

$$= (x+y-1) + z - (x+y-1)z$$

$$= x+y-1+z-xz-yz+z$$

$$= x+y+2z-xz-yz-1.$$

$$(x \otimes z) \oplus (y \otimes z)$$

$$= (x+z-xz) \oplus (y+z-yz)$$

$$= (x+z-xz) + (y+z-yz) - 1$$

$$= x+y+2z-xz-yz-1$$

Hence $(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$.

Therefore $\otimes$ is distributive over $\oplus$ on $\mathbb{Z}$.

Hence $(\mathbb{Z}, \oplus, \otimes)$ is a Ring.

Now we will check whether it is a Ring with multiplicative identity?

Check for multiplicative identity:

$$\forall x \in \mathbb{Z} \left[(x \otimes e^x = x) \wedge (e^x \otimes x = x) \right]$$

Choose arbitrary x in $\mathbb{Z}$.

$$x \otimes e^x = x + e^x - xe^x = x$$

$$\Rightarrow e^x - xe^x = 0$$

$$\Rightarrow e^x(1-x) = 0$$

Since $e^x \in \mathbb{Z}$, $x \in \mathbb{Z}$ so we can consider the operations $+, \cdot$ as usual integer addition and multiplication.

Hence $e^x = 0$ or $x = 1$.

If $e^x = 0$ then, $x \otimes e^x = x + e^x - xe^x = x + 0 - 0 = x$

and $e^x \otimes x = e^x + x - e^x \cdot x = 0 + x - 0 = x$

Therefore, $\forall x \in \mathbb{Z} \left[x \otimes 0 = 0 \otimes x = x \right]$

Hence 0 is the multiplicative identity of the ring $(\mathbb{Z}, \oplus, \otimes)$.

Next we have to check if it is commutative ring. under $\otimes$

$$\forall_{x,y \in \mathbb{Z}} \left[x \otimes y = y \otimes x \right]$$

Choose arbitrary $x, y \in \mathbb{Z}$.

$$x \otimes y = x + y - xy$$

$$y \otimes x = y + x - yx = x + y - xy \quad \text{since } +, \cdot$$

is commutative on $\mathbb{Z}$ (with usual addition & multiplication)

Therefore, $x \otimes y = y \otimes x$.

Hence $(\mathbb{Z}, \oplus, \otimes)$ is a commutative ring with identity.

Now we have to check for integral domain.

If $(\mathbb{Z}, \oplus, \otimes)$ has no zero divisor then it will be an integral domain.

$(\mathbb{Z}, \oplus, \otimes)$ is a commutative ring with identity (CRI)

$z \in \mathbb{Z}$ is called zero divisor if and only if

$$\forall_{x \in \mathbb{Z}} \left[(z \neq e^+) \wedge (x \neq e^+) \longrightarrow z \otimes x = e^+ \right]$$

where e^+ is the additive identity of the CRI.

Now $(\mathbb{Z}, \oplus, \otimes)$ is an integral domain if and only if

(i) $\forall_{z,x \in \mathbb{Z}} \left[(z \neq e^+) \wedge (x \neq e^+) \longrightarrow (z \otimes x \neq e^+) \right]$

$\equiv$

(ii) $\forall_{z,x \in \mathbb{Z}} \left[(z \otimes x = e^+) \longrightarrow (z = e^+) \vee (x = e^+) \right]$

We take the (ii) definition of integral domain.

Choose arbitrary $x \in \mathbb{Z}$, $z \in \mathbb{Z}$.

$z \otimes x = e^+$; we have to show it implies $z = e^+$ or $x = e^+$

$\Rightarrow z + x - zx = 1 \quad [\because e^+ = 1]$

$\Rightarrow z(1-x) + x - 1 = 0$

$\Rightarrow z(1-x) - 1(1-x) = 0$

$\Rightarrow (z-1)(1-x) = 0$

$\Rightarrow z' \cdot x' = 0$

Therefore either $z' = 0$ or $x' = 0$

$\Rightarrow z = 1$ or $x = 1$

Therefore, the implication is true. Hence $(\mathbb{Z}, \otimes, \oplus)$ is indeed an integral domain.

12. The *characteristic* of a field is defined as the smallest number of times one must add the multiplicative identity in the field to get the additive identity (i.e., for $\underbrace{1+1+\ldots+1}_{n} = 0$, the characteristic is n provided no number smaller than n results in the equality). Prove that the characteristic of a field is either 0 (which is when no finite n exists) or a prime number. [Hint: You may use the field axioms.]

Suppose $(\mathbb{F}, +, \cdot)$ is a field with 2 operations.

Char$[\mathbb{F}]$ = n s.t. minimum n for which

$$\underbrace{1_F + 1_F + \cdots + 1_F}_{n \text{ times}} = 0_F \text{ is true.}$$

Assume that char$[\mathbb{F}]$ is not prime and not 0.

$\Rightarrow$ There exists a positive integer n such that n is not a prime number and it is not 0. Therefore, $n > 1$ (since 1 is also not a prime number).

Suppose n is a composite number. So n can be expressed as multiplication of a and b where $1 < a < n$ and $1 < b < n$ where a, b are part of positive integers.

Therefore, we can write - $\underbrace{1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{n \text{ - times}} = 0_{\mathbb{F}}$

$$\Rightarrow \underbrace{\left(1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}\right)}_{a \text{ times}} + \left(1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}\right) + \cdots$$

$$\underbrace{\cdots + \left(1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}\right)}_{b \text{ times}} = 0_{\mathbb{F}}.$$

Invoking closure property – $\underbrace{1_{IF} + \cdots + 1_{IF}}_{a \text{ times}} \in IF$.

Let, $\underbrace{1_{IF} + 1_{IF} + \cdots + 1_{IF}}_{a \text{ times}} = \alpha \quad (\alpha \in IF)$

(since a need not belong to IF therefore α need not be equal to a)

Now 2 things can happen –

(i) $\alpha = 0_{IF}$: Since $\underbrace{1_{IF} + 1_{IF} + \cdots + 1_{IF}}_{a \text{ times}} = 0_{IF}$

therefore, $char[IF] = a$ (since $1 < a < n$)

It is contradiction because we assumed $char[IF] = n$

Hence this is not possible.

(ii) $\alpha \neq 0_{IF}$: That means α^{-1} must exist in IF.

We have already seen that $\alpha \in IF$.

$$\underbrace{\alpha + \alpha + \cdots + \alpha}_{b \text{ times}} = 0_{IF}$$

Multiply with α^{-1} in both sides-

$$\alpha^{-1} \underbrace{(\alpha + \alpha + \cdots + \alpha)}_{b\text{-times}} = \alpha^{-1} \cdot 0_{IF} = 0_{IF}.$$

$$\Rightarrow \underbrace{\alpha^{-1}\cdot\alpha + \alpha^{-1}\cdot\alpha + \cdots + \alpha^{-1}\cdot\alpha}_{b\text{-times}} = 0_{\mathbb{F}}$$

$$\Rightarrow \underbrace{1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{b\text{-times}} = 0_{\mathbb{F}}$$

Therefore, $\text{char}[\mathbb{F}] = b$ $(\text{as } 1 < b < n)$

which is again a contradiction because we assumed $\text{char}[\mathbb{F}] = n$. Hence it is not possible.

Since both the cases are not possible so we say n can't be a composite number that means n has to be a prime number.

By definition, we say $\text{char}[\mathbb{F}] = 0$ if no such n exists such that $1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}$ (n times) $= 0_{\mathbb{F}}$.

Therefore, <u>Char[F] can be either 0 or prime number.</u>

5. For $A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \in \mathbb{Z}_7^{2\times 2}$, show through explicit computation of P^{-1}, where $P = \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \in \mathbb{Z}_7^{2\times 2}$, that $P^{-1}AP = \begin{bmatrix} 3 & 0 \\ 0 & 4 \end{bmatrix} \in \mathbb{Z}_7^{2\times 2}$.

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

All the matrices are members of $\mathbb{Z}_7^{2\times 2}$

By the definition of P^{-1} we know that, $P \cdot P^{-1} = I = P^{-1} \cdot P$

It is easy to see that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{Z}_7^{2\times 2}$ which means if we multiply, any matrix M with I then we will get back M.

Given, $P = \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}$

Consider $P^{-1} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ where $a_{ij} \in \mathbb{Z}_7$

$$P^{-1} = \frac{1}{\det(P)} \begin{bmatrix} 2 & -1 \\ -1 & 3 \end{bmatrix}$$

$\det(P) = 3\times 2 - 1\times 1 = 6 - 1 = 5$ in $\mathbb{Z}_7$

$\frac{1}{\det(P)} = \frac{1}{5} = 5^{-1} = 3$ in $\mathbb{Z}_7$ as $5 \times 3 = 1 \pmod 7$

↳ multiplicative inverse of 5

-1 = Additive inverse of $1. = 6$ as $6 + 1 = 0 \pmod 7$

Therefore, $P^{-1} = 3 \cdot \begin{bmatrix} 2 & 6 \\ 6 & 3 \end{bmatrix} = \begin{bmatrix} 6 & 18 \\ 18 & 9 \end{bmatrix} \pmod 7$

$$= \begin{bmatrix} 6 & 4 \\ 4 & 2 \end{bmatrix}$$

since $18 \equiv 4 \pmod 7$

$9 \equiv 2 \pmod 7$

Consider: $P^{-1} \cdot A \cdot P$

$$= \begin{bmatrix} 6 & 4 \\ 4 & 2 \end{bmatrix} \left(\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \right)$$

$$= \begin{bmatrix} 6 & 4 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} (12+12) & (24+4) \\ (8+6) & (16+2) \end{bmatrix} \pmod 7$$

$$= \begin{bmatrix} 24 & 28 \\ 14 & 18 \end{bmatrix} \pmod 7$$

$$= \begin{bmatrix} 3 & 0 \\ 0 & 4 \end{bmatrix} \in \mathbb{Z}_7^{2\times 2}$$

(Hence Proved)

3. Show that $x^2 = 0$ has a unique solution in $\mathbb{Z}_n$, where $n = pq$ and p, q are distinct prime numbers. Consider the relevant operations to be modulo n. [**Hint**: If a prime number divides a product of two integers, then it must divide at least one of them.]

$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$.

We have to prove that $x^2 = 0$ has a unique solution. Which means there is only one value of x that satisfies this equation. For x^2 to be congruent to $0 \pmod n$, x^2 must be divisible by n.

$x^2 = 0$ can be written as $x^2 \equiv 0 \pmod{n}$

Hence n must divide x^2.

Therefore pq must divide x^2. $[\because n = pq]$

It is given that p and q are distinct primes $(p \neq q)$

If a prime number divides a product of two integers then it must divide at least one of them. —(i)

pq divides x^2

$\Rightarrow pq$ divides $x \cdot x$

We can also write p divides $x \cdot x$ and q divides $x \cdot x$

$\Rightarrow p$ divides x and q divides x (from proposition (i))

We know $x \in \{0, 1, \ldots, n-1\}$

$p > 1$, $q > 1$ } prime numbers.

p divides $x \iff x \equiv 0 \pmod{p}$

q divides $x \iff x \equiv 0 \pmod{q}$

That means, $x \equiv 0 \pmod{n}$ $[n = pq]$

Therefore, $x = 0$ (since x range is 0 to $n-1$) is the only integer solution to $x^2 \equiv 0 \pmod{n}$.

7. For the matrix $A = \begin{bmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{bmatrix}$, obtain $x \in \mathbb{R}^3$ such that $Ax = \lambda x$ for some scalar λ, if possible.

Given that $Ax = \lambda x$

$\Rightarrow Ax = \lambda \cdot I \cdot x$

$\Rightarrow Ax - \lambda \cdot Ix = 0$

$\Rightarrow (A - \lambda I) \cdot x = 0$

If $(A - \lambda I)$ is invertible then $x = 0$ is the only solution (Here 0 is vector). But it is trivial solution. So for any non trivial solution to exist, the matrix $(A - \lambda I)$ should not be invertible.

Hence $|A - \lambda I| = 0$ for non trivial solution to exist.

$$\Rightarrow \begin{vmatrix} 5-\lambda & 1 & 0 \\ 0 & 5-\lambda & 1 \\ 0 & 0 & 5-\lambda \end{vmatrix} = 0$$

$\Rightarrow (5-\lambda)^3 = 0$

Therefore, $\lambda = 5, 5, 5$ (all 3 solutions are same as 5)

To obtain $x \in \mathbb{R}^3$, we will use $[A - \lambda I]\, x = 0$.

$$\begin{bmatrix} 5-5 & 1 & 0 \\ 0 & 5-5 & 1 \\ 0 & 0 & 5-5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 0 & \textcircled{1} & 0 \\ 0 & 0 & \textcircled{1} \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

pivot variables $= x_2, x_3$

Free variables $= x_1$.

We will write the pivots in terms of free variables.

$$\left.\begin{aligned} x_2 &= 0 \\ x_3 &= 0 \\ 0 &= 0 \end{aligned}\right\} \quad x = \begin{bmatrix} x_1 \\ 0 \\ 0 \end{bmatrix} = c \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad (c \text{ is any scalar})$$

Therefore, the solution $x \in \mathbb{R}^3$ is possible.

11. (*Optimization*) For a particular crop, each square foot of ground requires 10 units of phosphorous, 9 units of potassium, and 19 units of nitrogen. Suppose there are three brands of fertilizer $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, which are all sold in packets weighing 1 kg each. One kg of the three brands contain minerals in the following quantities.
$\mathcal{X}$: 2 units of phosphorous, 3 units of potassium, and 5 units of nitrogen.
$\mathcal{Y}$: 1 unit of phosphorous, 3 units of potassium, and 4 units of nitrogen.
$\mathcal{Z}$: 1 unit of phosphorous and 1 unit of nitrogen.
(a) Suppose farmers can only buy an integral number of packets of each brand. Does this problem have a *meaningful* solution? If it exists, is the solution unique? Justify your answer. Determine all possible solutions to the problem, if any.
(b) Suppose fertilizer of brand $\mathcal{X}$ costs INR 100 per kg, brand $\mathcal{Y}$ costs INR 600 per kg, and brand $\mathcal{Z}$ costs INR 300 per kg. Determine the least expensive solution (even if no exact solution exists) that will satisfy the recommendations (as best as possible).

Fertilizer Brand	Phosphorous (unit)	Potassium (unit)	Nitrogen (unit)
X (1 kg)	2	3	5
Y (1kg)	1	3	4
Z (1kg)	1	0	1
Requirement :	10	9	19

Suppose, the farmer purchases x packets of X, y packets of Y and z packets of Z where x, y, z are all non-negative integers.

Phosphorous requirement: $2x + y + z = 10$

Potassium requirement: $3x + 3y + 0z = 9$

Nitrogen requirement: $5x + 4y + z = 19$

Writing in matrix form -

$$\begin{bmatrix} 2 & 1 & 1 \\ 3 & 3 & 0 \\ 5 & 4 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 10 \\ 9 \\ 19 \end{bmatrix}$$

Construct an augmented matrix as -

$$\left[\begin{array}{ccc|c} 2 & 1 & 1 & 10 \\ 3 & 3 & 0 & 9 \\ 5 & 4 & 1 & 19 \end{array}\right] \xrightarrow[R_3' \to R_3 - \frac{5}{2}R_1]{R_2' \to R_2 - \frac{3}{2}R_1} \left[\begin{array}{ccc|c} 2 & 1 & 1 & 10 \\ 0 & \frac{3}{2} & -\frac{3}{2} & -6 \\ 0 & \frac{3}{2} & -\frac{3}{2} & -6 \end{array}\right]$$

$$R_3' \to R_3 - R_2 \quad \downarrow$$

$$\left[\begin{array}{ccc|c} 2 & 1 & 1 & 10 \\ 0 & 3/2 & -3/2 & -6 \\ 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow{R_2' \to R_2 \times 2} \left[\begin{array}{ccc|c} 2 & 1 & 1 & 10 \\ 0 & 3 & -3 & -12 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

pivot variables = x, y

free variable = z

First we find the null solutions – $Ax_n = 0$

$3y - 3z = 0 \quad \Rightarrow \quad y = z$

$2x + y + z = 0 \quad \Rightarrow \quad x = -z$

Therefore, $x_{null} = \begin{bmatrix} -z \\ z \\ z \end{bmatrix} = c \cdot \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}$

(where c is any scalar)

Let's find a particular solution - $Ax_p = b$

We can find a particular solution by choosing $z = 0$ (free variable as 0).

$3y - 3z = -12 \Rightarrow y = -4$

$2x + y + z = 10 \Rightarrow 2x - 4 = 10 \Rightarrow x = 7$

Therefore,

$$x_p = \begin{bmatrix} 7 \\ -4 \\ 0 \end{bmatrix}.$$

Complete solution $x_{complete} = x_p + x_{null}$

$$= \begin{bmatrix} 7 \\ -4 \\ 0 \end{bmatrix} + c \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 7 - c \\ -4 + c \\ c \end{bmatrix}$$

Since the number of packets can't be negative, so -

$7 - c \geq 0 \Rightarrow c \leq 7$

$-4 + c \geq 0 \Rightarrow c \geq 4$

$c \geq 0 \Rightarrow c \geq 0$

} and c must be an integer because number of packet can't be fraction.

By combining all the inequalities -
We can say that $c = 4$ or $c = 5$ or $c = 6$ or $c = 7$

Therefore, the system does have a meaningful solution.
But the solution is not unique.

We can determine all possible solution as -

$$x^{(1)} = \begin{bmatrix} 7-4 \\ -4+4 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 4 \end{bmatrix} \text{ (kg)} \quad [\text{for } c = 4]$$

$$x^{(2)} = \begin{bmatrix} 7-5 \\ -4+5 \\ 5 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \text{ (kg)} \quad [\text{for } c = 5]$$

$$x^{(3)} = \begin{bmatrix} 7-6 \\ -4+6 \\ 6 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 6 \end{bmatrix} \text{ (kg)} \quad [\text{for } c = 6]$$

$$x^{(4)} = \begin{bmatrix} 7-7 \\ -4+7 \\ 7 \end{bmatrix} = \begin{bmatrix} 0 \\ 3 \\ 7 \end{bmatrix} \text{ (kg)} \quad [\text{for } c = 7]$$

Given that X costs Rs. 100/kg
Y costs Rs 600/kg
Z costs Rs. 300/kg.

Therefore cost of the solutions –

$\text{cost}(x^{(1)}) = 3\times100 + 0\times600 + 4\times300$
$= 300 + 1200 = \text{Rs. } 1500$

$\text{Cost}(x^{(2)}) = 2\times100 + 1\times600 + 5\times300$
$= 200 + 600 + 1500 = \text{Rs. } 2300$

$\text{Cost}(x^{(3)}) = 1\times100 + 2\times600 + 6\times300$
$= 100 + 1200 + 1800 = \text{Rs. } 3100$

$\text{Cost}(x^{(4)}) = 0\times100 + 3\times600 + 7\times300$
$= 1800 + 2100 = \text{Rs. } 3900$

Therefore, the least expensive solution is $x^{(1)}$ which recommends 3 kg of brand X, 0 kg of brand Y and 4 kg of brand Z. to satisfy the requirement.

17. Based on the ideas in Problem 16, can you suggest how to constructively cook up a family of fields, $\{\mathbb{F}_1, \mathbb{F}_2, \dots\}$ satisfying the relation $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \cdots \subset \mathbb{R}$? Outline your steps through proper arguments. Note that $\mathbb{F}_1 \subset \mathbb{F}_2$ implies that $\mathbb{F}_1$, the sub-field of $\mathbb{F}_2$ is a field under the same same addition and multiplication as defined in $\mathbb{F}_2$ and the set $\mathbb{F}_1$ is a subset of $\mathbb{F}_2$. Construct a field, $\mathbb{F} \not\subset \mathbb{R}$, such that $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{C}$.

$\mathbb{Q}$: Set of all rational numbers which can be expressed in the form a/b where $a, b \in \mathbb{Z}$ and $b \neq 0$

$\mathbb{R}$: Set of all real numbers that includes the rational number also.

Let's construct the field $\mathbb{F}_1$ first. s.t. $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{R}$.

We know that $\mathbb{Q}$ is already a field. Introducing a number α_1 that is a root of the polynomial with rational coefficient only.

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \quad \text{where}$$

$\forall i \; a_i \in \mathbb{Q}$. We assume α_1 is the solution to $p(x) = 0$ therefore $p(\alpha_1) = 0$. Such a solution is guarented to exist from fundamental theorem of algebra.

Definitely $\alpha_1 \notin \mathbb{Q}$ since we are trying to extend the set $\mathbb{Q}$ to form a new field and clearly $\alpha_1 \in \mathbb{F}_1$.

We construct a set, $S_1 = \mathbb{Q} \cup \{\alpha_1\}$
When we apply $+$ and $\cdot$ operations on set S_1 elements, the new elements are also added to S_1 recursively so that the operation on S_1 becomes closed under $+$ and $\cdot$

Let's try to construct the field $\mathbb{F}_1$.

(i) Closure: $\forall a, b \in \mathbb{Q} \left[a \cdot \alpha_1 + b\alpha_1 \in \mathbb{F}_1 \right]$

Therefore we add the results of this combination in $\mathbb{F}_1$

$$\forall a, b \in \mathbb{Q} \left[(a \cdot \alpha_1) \cdot (b\alpha_1) \in \mathbb{F}_1 \right]$$

Therefore we have to add $\alpha_1^2, \alpha_1^3, \alpha_1^4, \ldots$ in $\mathbb{F}_1$ to satisfy closure property.

(ii) mult-inverse: α^{-1} must exist in $\mathbb{F}$.

(iii) Add-inverse: $-\alpha_1$ must exist in $\mathbb{F}$.

Therefore, $\mathbb{F}_1 = \mathbb{Q} \cup \{\alpha_1^n\} \cup \{-\alpha_1\} \cup \{-\alpha_1^{-n}\}$ and their combinations with $\mathbb{Q}$ to satisfy closure.

Similarly $\mathbb{F}_2$ can be constructed by extending $\mathbb{F}_1$ with similar arguments.

Introducing $\alpha_2 \in \mathbb{F}_2$ but $\notin \mathbb{F}_1$ such that, $p(\alpha_2) = 0$

Therefore,

$\mathbb{F}_2 = \mathbb{F}_1 \cup \{\alpha_2^n\} \cup \{-\alpha_2\} \cup \{-\alpha_2^{-n}\}$ and all their combinations with $\mathbb{F}_1$ to satisfy closure.

It is not possible to cover the entire $\mathbb{R}$ by extending $\mathbb{Q}$ recursively with adding an algebraic number Because real number $\mathbb{R}$ includes. algebraic number (solution of polynomials) as well as trascendental numbers so naturally $\mathbb{F}_n$ is a subset of $\mathbb{R}$.

therefore, $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \cdots \subset \mathbb{R}$ (proved)

Similarly, consider the equation, $p(x) = x^2 + 1 = 0$ where the coefficients are rational. The algebraic number i can be the solution of $p(x) = 0$ therefore in the field $\mathbb{F}$ we include i.

We start with set $\mathbb{Q}$. Choose an algebric number i and add their mult, add. inverses and all combination with $\mathbb{Q}$ elements to satisfy closure.

$\mathbb{F} = \mathbb{Q} \cup \{ i^n \} \cup \{ -i^n \} \cup \{$ all combinations of $i^n, -i^n$ with $\mathbb{Q}$ elements $\}$.

Definitely $\mathbb{F} \neq \mathbb{C}$ because $\mathbb{F}$ doesn't contain the transcendantal number but $\mathbb{C}$ contains it so we have proved that $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{C}$.

18. Argue whether a field is a vector space over all its subfields.

Consider a field $\mathbb{F}$.
Suppose the subfields of $\mathbb{F}$ are $\mathbb{F}_1, \mathbb{F}_2, \ldots \subseteq \mathbb{F}$.

We have to check whether $\mathbb{F}$ is a vector space over all its subfields $\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3, \ldots$

Consider $(\mathbb{F}, +, \times)$ as Field with its operations.

$(\mathbb{F}_i, +, \times)$ & $\mathbb{F}_i \subseteq \mathbb{F}$ $(\forall i)$.

When we check whether $\mathbb{F}$ is a vector space over $\mathbb{F}_i$, we introduce 2 additional operations that is vector addition $(+_V)$ and scalar multiplication $(\cdot)$.

Consider $V = \mathbb{F}$. over field $\mathbb{H}$ where $\mathbb{H} = \mathbb{F}_i$.

(i) V is vector space $\longrightarrow$ $(V, +_V)$ is an Abelian group.

$(V, +_V) = (\mathbb{F}, +_{\mathbb{F}}) = (\mathbb{F}, +)$

since $\mathbb{F}$ is already a field so $(\mathbb{F}, +)$ is an Abelian group so (i) check is done.

(ii) $\forall v \in V, c \in \mathbb{H}$ $\left(c \cdot v \in V \right)$

Take any scalar $c \in \mathbb{F}_i$ and $v \in \mathbb{F}$. Then we have to prove that $c \cdot v \in \mathbb{F}$.

Since $c \in \mathbb{F}_i$ and $v \in \mathbb{F}$ so $c \cdot v \equiv c \times v \in \mathbb{F}$ since $\mathbb{F}_i$ is a subfield and $\mathbb{F}$ is a field.

Therefore, $\mathbb{F}$ is closed under $\cdot$ over $\mathbb{F}_i$.

When $c = \mathbb{1}_{\mathbb{F}_i} = \mathbb{1}_{\mathbb{F}}$ therefore $\mathbb{1}_F \cdot v \equiv \mathbb{1}_F \times v = v$

(iii) $\forall_{v \in \mathbb{V}},\ a, b \in \mathbb{H} \left((a \times b) \cdot v = a \cdot (b \cdot v) \right)$

Take any scalar $a, b \in \mathbb{F}_i$ and $v \in \mathbb{F}$.

$(a \times b) \cdot v = (a \times b) \times v = a \cdot (b \cdot v)$ since

$a, b, v \in \mathbb{F}$ so we can associate the $\times$ operation and $\times$, $\cdot$ becomes same operation.

(iv) $\forall_{v,u \in \mathbb{V}},\ a \in \mathbb{H} \left(a \cdot (u +_{\mathbb{V}} v) = a \cdot u +_{\mathbb{V}} a \cdot v \right)$

Take $u, v \in \mathbb{F}$ and $a \in \mathbb{F}_i$

So $a \times (u + v) = a \times u + a \times v$ (because $\mathbb{F}$ is a field)

and since $\mathbb{F}$ is distributive also $(u +_{\mathbb{V}} v) \cdot a = u \cdot a +_{\mathbb{V}} v \cdot a$ is also true.

(v) $\forall u \in V, a, b \in \mathbb{H} \left((a+b) \cdot u = a \cdot u +_V b \cdot u \right)$

Take $u \in \mathbb{F}$ and $a, b \in \mathbb{F}_i$.

So $(a+b) \times u = a \times u + b \times u$ (because $\mathbb{F}$ is a field).

Therefore, we can see that $\mathbb{F}$ satisfies all the properties of vector space over all its subfields $\mathbb{F}_i$.