LINEAR ALGEBRA

ASSIGNMENT-1

Solution 1.

1.1. Let S be the set of sequences that are absolutely summable

(a) A sequence of all zero's in it is absolutely summable, Let $e = \{0, 0, \dots, 0, \dots\}$

$\therefore e \in S$

(b) Let $s_1, s_2 \in S$, such that $\sum_{i=1}^{\infty} |s_{1i}| < \infty$ and

$$\sum_{j=1}^{\infty} |s_{2j}| < \infty$$

then,

$$\sum_{i,j=1}^{\infty} |s_{1i} + s_{2j}| \leq \sum_{i,j=1}^{\infty} (|s_{1i}| + |s_{2j}|)$$

{using triangular inequality $|u+v| \leq |u|+|v|$}

$$= \sum_{i=1}^{\infty} |s_{1i}| + \sum_{j=1}^{\infty} |s_{2j}| < \infty$$

$$\therefore \sum_{ij}^{\infty} |s_{1i} + s_{2j}| < \infty$$

(c) Let $s_k \in S$, such that $\sum_{k=1}^{\infty} |s_k| < \infty$, $a \in \mathbb{R}$

then $$\sum_{k=1}^{\infty} |a s_k| = \sum_{k=1}^{\infty} |a||s_k| < |a| \infty$$

or $$\sum_{k=1}^{\infty} |a s_k| < \infty$$

from (a), (b) & (c), S is a subspace of $\mathbb{R}^\infty$.

1.2. Let $\mathcal{B}$ be the set of all bounded sequences,

(a) sequence of all '0' elements is a bounded seq.

Let $e = \{0, 0, \ldots\}$. $\therefore e \in \mathcal{B}$.

(b) Let $b_1, b_2 \in \mathcal{B}$, then there exists M, N such that

$$|b_1| \leq M \quad \text{and} \quad |b_2| \leq N$$

Again by using triangular inequality

$$|b_1 + b_2| \leq |b_1| + |b_2| \leq M + N$$

hence $(b_1 + b_2)$ is bounded. , $(b_1 + b_2) \in \mathcal{B}$

(c) Let $b \in \mathcal{B}$ & $a \in \mathbb{R}$

$$|ab| = |a||b| \leq |a| M$$

$\therefore \quad ab \in \mathcal{B}$

From (a), (b) & (c) we conclude that $\mathcal{B}$ is a subspace of $\mathbb{R}^\infty$.

1.3 Let A be the set of all sequences in arithmatic progression.

Let $l_1, l_2 \in A$, where,

$$l_1 = (a_1, a_1+k_1, a_1+2k_1, \ldots)$$

$$l_2 = (a_2, a_2+k_2, a_2+2k_2, \ldots)$$

(a) Sequence of all '0's will form an AP (i.e $a=k=0$)

(b) $l_1+l_2 = (a_1+a_2, (a_1+k_1)+(a_2+k_2), \ldots\ldots)$

$= (a_1+a_2, a_1+a_2+(k_1+k_2), \ldots)$

(l_1+l_2) is also an AP with first term $= a_1+a_2$ & common difference $= k_1+k_2$.

(c) For $c \in \mathbb{R}$

$cl_1 = (ca_1, ca_1+ck_1, ca_1+2ck_1, \ldots)$

This is an AP with first term $= ca_1$ & common diff. $= ck_1$

From (a), (b) & (c) A is a subspace of $\mathbb{R}^\infty$

1.4 Let G be a set of all geometric progressions.

Let $g_1, g_2 \in G$, such that

$$g_1 = \{a_1, k_1 a_1, k_1^2 a_1, \ldots\}$$

$$g_2 = \{a_2, k_2 a_2, k_2^2 a_2, \ldots\}$$

put $a_1 = k_1 = 1$ and $a_2 = 1$, $k_2 = 1/2$, we get.

$$g_1 = \{1, 1, 1 \ldots\}$$

$$g_2 = \{1, 1/2, 1/4 \ldots\}$$

$$g_1 + g_2 = (2, 3/2, 5/4, \ldots)$$

but $(g_1 + g_2)$ doesn't form ~~an~~ GP. hence set G is not closed under addition.

Hence G is not a subspace of $\mathbb{R}^\infty$.

Solution-2

To solve this question, we will use the fact that $\mathbb{R}$ is uncountable whereas $\mathbb{Q}^n$ is countable $(n \geq 0)$

Let's prove this question by contradiction,

Suppose $\mathbb{R}$ has finite dimension as a vector space over $\mathbb{Q}$. Let $e_1, e_2 \ldots e_n$ be the basis for this vector space.

Thus, for $r \in \mathbb{R}$, there exist unique rational numbers $c_1, \ldots c_n$ such that $r = c_1 e_1 + \cdots + c_n e_n$.

Hence, there is a mapping,

$(e_1 \ldots e_n)$.

$$(c_1 \ldots c_n) \to (c_1 e_1 + \ldots c_n e_n) : \mathbb{Q}^n \to \mathbb{R}$$

which is both one-one and onto. (bijection)

But $\mathbb{Q}^n$ is countable and $\mathbb{R}$ is uncountable, so there cannot be bijection between these sets. Hence, our assumption was wrong,

Hence $\mathbb{R}$ must have infinite dimension as a vector space over $\mathbb{Q}$.

Solution. 3

$f(x) = x$

$g(x) = e^x$

$h(x) = e^{-x}$

To prove for all $x \in [0,1]$, $a, b, c \in \mathbb{R}$

$af(x) + bg(x) + ch(x) = 0$ only when

$a = b = c = 0$

~~So Let above eqn~~ v. Let f, g, h are dependent

Then, there ~~is~~ is atleast one non-zero $a, b, c \in \mathbb{R}$ in above eqn. such that

$$ax + be^x + ce^{-x} = 0$$

$x = 0$ $\quad b + c = 0$ ——— (1) $\quad c = -b.$

$x = 1$ $\quad a + be + ce^{-1} = 0$

$ea + be^2 + c = 0 \;\Big|\; ea + b(e^2 - 1) = 0$

$x = \frac{1}{2}$ $\quad \frac{a}{2} + be^{1/2} + ce^{-1/2} = 0$

$\frac{a}{2}e^{+1/2} + be + c = 0 \;\Big\|\; \frac{e^{1/2}}{2}a + b(e-1) = 0$

$$ae + b(e^2-1) = 0 \quad \text{—— (ii)}$$

$$\frac{a e^{1/2}}{2} + b(e-1) = 0$$

$$ae^{1/2} + 2b(e-1) = 0$$

$$ae + 2b(e^{3/2} - e^{1/2}) = 0 \quad \text{—— (iii)}$$

(ii) − (iii)

$$b(e^2-1) - 2b(e^{3/2} - e^{1/2}) = 0$$

$$b(e^2 - 1 - 2e^{3/2} + 2e^{1/2}) = 0$$

$$b(e^2 - 1 - 2e^{1/2}(e-1)) = 0$$

$$b((e+1)(e-1) - 2e^{1/2}(e-1) = 0$$

$$b(e-1)\{e+1 - 2e^{1/2}\} = 0$$

$$b(e-1)((e^{1/2})^2 + 1^2 - 2e^{1/2}\} = 0$$

$$\underbrace{b(e-1)}_{+ve.}(e^{1/2}-1)^2 = 0$$

$\therefore b = 0 \Rightarrow c = 0 \Rightarrow a = 0$ contradiction.

hence $af + bg + ch = 0$ only when $a = b = c = 0$

Q4.

a)

We can verify the following subspace criteria to check W_1 to be subspace of V:

i) The zero vector of V is in W_1

→ The zero vector in V is 2×2 zero matrix O.

By putting $x=0, y=0, z=0$, we get $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in W_1$

so $O \in W_1$ & condition (i) is met.

ii) For any $A, B \in W_1$, the sum $A+B \in W_1$.

→ let $A = \begin{bmatrix} x_1 & -x_1 \\ y_1 & z_1 \end{bmatrix}$ & $B = \begin{bmatrix} x_2 & -x_2 \\ y_2 & z_2 \end{bmatrix}$

$$A+B = \begin{bmatrix} x_1+x_2 & -(x_1+x_2) \\ y_1+y_2 & z_1+z_2 \end{bmatrix} \Rightarrow \begin{bmatrix} x_3 & -x_3 \\ y_3 & z_3 \end{bmatrix}$$

where $x_1+x_2=x_3 \in R$ $y_1+y_2=y_3 \in R$

$z_1+z_2=z_3 \in R$

so resultant A+B also $\in W_1$ since A+B follows the form of matrix given in W_1.

So condition 2 is met.

iii) For any $A \in W_1$ & $r \in R$, the scalar product $rA \in W_1$.

→ let $A = \begin{bmatrix} x_1 & -x_1 \\ y_1 & z_1 \end{bmatrix}$, so $rA = \begin{bmatrix} rx_1 & -rx_1 \\ ry_1 & rz_1 \end{bmatrix}$

$x_1' = rx_1 \in R$ $y_1' = ry_1 \in R$ $rz_1 = z_1' \in R$

so $rA = \begin{bmatrix} x_1' & -x_1' \\ y_1' & z_1' \end{bmatrix}$ follows the form given & thus condition 3 is met.

So we can conclude that W_1 is subspace of V.

Same can be done for proving W_2 is a subspace of V.

b)

Ans → W_1 can be written as:

$$x\begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} + y\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + z\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

so $v_1 = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}$; $v_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$; $v_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

We can see that v_1, v_2, v_3 are linearly independent so these forms the basis of W_1 & thus dimension of $W_1 = 3$.

⇒ W_2 can be written as:

$$a\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

so $v_1 = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $v_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

We can see that v_1, v_2, v_3 are linearly independent, so these forms the basis of W_2 & thus dimension of W_2 are: 3

⇒ W_1 matrice set elements are transpose of elements in W_2 matrice set. So, we can write

$W_1 + W_2$ as:

$$\begin{bmatrix} x & -x \\ y & z \end{bmatrix} + \begin{bmatrix} x & y \\ -x & z \end{bmatrix} = \begin{bmatrix} 2x & y-x \\ y-x & 2z \end{bmatrix}$$

$$\Rightarrow 2x \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + (y-x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + 2z \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$V_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad V_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad V_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

We can see that V_1, V_2, V_3 are linearly independent, so these form basis of $W_1 + W_2$ & thus dimension of $W_1 + W_2 = 3$.

⇒ In $W_1 \cap W_2$, we will have set of symmetric matrices of the form $\begin{bmatrix} x & -x \\ -x & z \end{bmatrix}$ which can be written as

$$x \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} + z \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

so $V_1 = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$ & $V_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Q5.

Ans Let $(u_1, u_2 \dots u_m)$ be basis of W_1 & $(w_1, w_2 \dots w_n)$ be basis of W_2

Let $a_1 = \alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_m u_m$

& $a_2 = \alpha'_1 w_1 + \alpha'_2 w_2 + \dots + \alpha'_n w_n$

$\rightarrow a_1 \in W_1$ & $a_2 \in W_2$

$a = a_1 + a_2$

$= (\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_m u_m) + (\alpha'_1 w_1 + \alpha'_2 w_2 + \dots + \alpha'_n w_n)$ — (1)

Let's assume there exist $b_1 \in W_1$ & $b_2 \in W_2$ such that we can write

$a = b_1 + b_2$

$= (B_1 u_1 + B_2 u_2 + \dots B_m u_m) + (B'_1 w_1 + B'_2 w_2 + \dots + B'_n w_n)$ — (2)

Subtracting (1) & (2)

$0 = [(\alpha_1 - B_1) u_1 + (\alpha_2 - B_2) u_2 + \dots + (\alpha_m - B_m) u_m] + [(\alpha'_1 - B'_1) w_1 + (\alpha'_2 - B'_2) w_2 + \dots + (\alpha'_n - B'_n) w_n]$

As $u_1, u_2, \dots u_m, w_1, w_2, \dots w_n$ forms basis of V & are linearly independent, so

$\alpha_i = B_i \quad i = 1 \text{ to } m$

$\alpha'_j = B'_j \quad j = 1 \text{ to } n$

Hence for each $a \in V$, there are unique $a_1 \in W_1$ & $a_2 \in W_2$

Q6

Ans 1.)

No, it is not always true. Take vector space $V = \mathbb{R}^2$ & let W_1, W_2, W_3 be the lines through the origin: $W_1 = \{(x,x) \mid x \in \mathbb{R}\}$ $W_2 = \{(x,0) \mid x \in \mathbb{R}\}$ & $W_3 = \{(0,x) \mid x \in \mathbb{R}\}$. Then $W_2 + W_3$ is all of V, so $W_1 \cap (W_2 + W_3) = W_1$. However $W_1 \cap W_2$ & $W_1 \cap W_3$ both contain only 0, so $(W_1 \cap W_2) + (W_1 \cap W_3) = \{0\} \neq V = W_1 \cap (W_2 + W_3)$.

Ans 2.) First we show $W_1 \cap (W_2 + (W_1 \cap W_3)) \subset (W_1 \cap W_2) + (W_1 \cap W_3)$. Suppose that $v \in W_1 \cap (W_2 + (W_1 \cap W_3))$. Then $v \in W_1$ & $v \in (W_2 + (W_1 \cap W_3))$, so v can be written as $v_1 + v_2$, $v_1 \in W_2$, $v_2 \in W_1 \cap W_3$. Then $v \in W_1$, $v_2 \in W_1$, so because W_1 is closed under addition & scalar multiplication, $v + (-v_2) = v_1 + v_2 - v_2 = v_1$ is also an element of W_1. So $v_1 \in W_1 \cap W_2$, $v_2 \in W_1 \cap W_3$, hence $v = v_1 + v_2 \in (W_1 \cap W_2) + (W_1 \cap W_3)$.

For the other inclusion, $(W_1 \cap W_2) + (W_1 \cap W_3) \subset W_1 \cap (W_2 + (W_1 \cap W_3))$, suppose $v \in (W_1 \cap W_2) + (W_1 \cap W_3)$. Then we can write $v = v_1 + v_2$, $v_1 \in W_1 \cap W_2$, $v_2 \in W_1 \cap W_3$. Because W_1 is a vector space & $v_1, v_2 \in W_1$, $v = v_1 + v_2 \in W_1$ also. Additionally $v_1 \in W_2$, $v_2 \in W_1 \cap W_3$, so $v \in W_2 + (W_1 \cap W_3)$. As a result, $v \in W_1 \cap (W_2 + (W_1 \cap W_3))$ as desired.

Question 7 :

① Scalar x · Vectors $\rightarrow (1+x, 1-x)$, $(1-x, 1+x)$ in $\mathbb{C}^2$

Find condition on x for the vectors to be linearly dependent

- A subset S of V is said to be <u>linearly dependent</u> if there exists distinct vectors $\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n \in S$ & scalars $c_1, \ldots, c_n \in \mathbb{F}$ s.t. $\sum_{i=1}^{n} c_i \bar{\alpha}_i = \bar{0}$ where not all $c_i \neq 0$

$\Rightarrow$ We must have $c_1(1+x, 1-x) + c_2(1-x, 1+x) = \bar{0}$ where not all $c_1, c_2 \neq 0$ and $c_1, c_2 \in \mathbb{F}$

$\Rightarrow (c_1 + c_2 + (c_1 - c_2)x, \; c_1 + c_2 + x(c_2 - c_1)) = \bar{0}$

$c_1 + c_2 + x(c_1 - c_2) = 0 \quad \rightarrow ①$

$c_1 + c_2 + x(c_2 - c_1) = 0 \quad \rightarrow ②$

① + ② $\Rightarrow 2(c_1 + c_2) = 0 \Rightarrow c_1 + c_2 = 0$

① − ② $\Rightarrow x(c_1 - c_2) = 0 \Rightarrow x = 0$ or $c_1 = c_2 = 0$

Hence $x = 0$ is the condition for the given vectors to be linearly dependent.

② Let $\bar{\alpha} = (x, 1, 0)$, $\bar{\beta} = (1, x, 1)$, $\bar{\gamma} = (0, 1, x)$

The vectors $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ in $\mathbb{R}^3$ will be linearly dependent if

$c_1\bar{\alpha} + c_2\bar{\beta} + c_3\bar{\gamma} = \bar{0}$ for not all $c_1, c_2, c_3 \neq 0$ and $c_1, c_2, c_3 \in \mathbb{F}$

$c_1(x, 1, 0) + c_2(1, x, 1) + c_3(0, 1, x) = \bar{0}$

$\Rightarrow (c_1 x + c_2, \; c_1 + c_2 x + c_3, \; c_2 + c_3 x) = \bar{0}$

This can be represented by equations,

$c_1 x + c_2 = 0 \qquad c_1 + c_2 x + c_3 = 0 \qquad c_2 + c_3 x = 0$

The matrix representation for the above equations is :

$$\begin{bmatrix} x & 1 & 0 \\ 1 & x & 1 \\ 0 & 1 & x \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_1 \to R_1 - x R_2$

$$\begin{bmatrix} 0 & 1-x^2 & -x \\ 1 & x & 1 \\ 0 & 1 & x \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_1 \to R_1 + R_3$

$$\begin{bmatrix} 0 & 2-x^2 & 0 \\ 1 & x & 1 \\ 0 & 1 & x \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow x(2-x^2) = 0$ or $\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

c_1, c_2, c_3 are not all $\bar{0}$. $\Rightarrow$ $\boxed{x = 0 \quad \text{or} \quad x = \pm\sqrt{2}}$ → condition for linear dependence of given vectors.

③ If we have $\mathbb{Q}^3$ in place of $\mathbb{R}^3$ in previous question, then $x = 0$ is the only condition for the vectors to be linearly dependent since $x = \pm\sqrt{2} \notin \mathbb{Q}$.

Question 8:

① Conditions for $Q(\sqrt{2})$ to be a field:

i) $(Q(\sqrt{2}), +)$ must form an abelian Group

ii) $(Q(\sqrt{2}) \setminus \{0\}, \cdot)$ must form an abelian Group

iii) $Q(\sqrt{2})$ must satisfy distributive property.

i) To check whether $(Q(\sqrt{2}), +)$ is an abelian Group:

~~① closure~~: Let $x = \alpha_1 + \beta_1\sqrt{2}$, $y = \alpha_2 + \beta_2\sqrt{2}$, $z = \alpha_3 + \beta_3\sqrt{2}$ be elements of $Q(\sqrt{2})$ where $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{Q}$

① closure: $x = \alpha_1 + \beta_1\sqrt{2}$ $\quad y = \alpha_2 + \beta_2\sqrt{2}$

$$x + y = \alpha_1 + \beta_1\sqrt{2} + \alpha_2 + \beta_2\sqrt{2} = (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)\sqrt{2}$$

Since $\alpha_1 + \alpha_2, \beta_1 + \beta_2 \in \mathbb{Q}$, $x + y \in Q(\sqrt{2})$ $\Rightarrow$ closure property satisfied under addition

② Associativity: $(x+y) + z = (\alpha_1 + \beta_1\sqrt{2} + \alpha_2 + \beta_2\sqrt{2}) + \alpha_3 + \beta_3\sqrt{2}$

$$= (\alpha_1 + \alpha_2) + \sqrt{2}(\beta_1 + \beta_2) + \alpha_3 + \beta_3\sqrt{2}$$

$$= \alpha_1 + (\alpha_2 + \alpha_3) + \sqrt{2}\beta_1 + \sqrt{2}(\beta_2 + \beta_3) \quad (\text{since } \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{Q})$$

$$= \alpha_1 + \sqrt{2}\beta_1 + (\alpha_2 + \sqrt{2}\beta_2 + \alpha_3 + \sqrt{2}\beta_3)$$

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

$\therefore Q(\sqrt{2})$ satisfies associativity under addition

③ Existence of Identity: Let $e = e_1 + e_2\sqrt{2} \in \mathbb{Q}\sqrt{2}$ where $e_1, e_2 \in \mathbb{Q}$

The identity element is e if $x + e = x$ ~~where e is identity element~~

$$x + e = x$$

$$\alpha_1 + \beta_1\sqrt{2} + e_1 + e_2\sqrt{2} = \alpha_1 + \beta_1\sqrt{2}$$

$$(\alpha_1 + e_1) + \sqrt{2}(\beta_1 + e_2) = \alpha_1 + \beta_1\sqrt{2}$$

$\alpha_1 + e_1 = \alpha_1$ $\qquad$ $\beta_1 + e_2 = \beta_1$

$\Rightarrow e_1 = 0$ $\qquad$ $\Rightarrow e_2 = 0$

$\therefore$ $e = 0 + 0\sqrt{2} = 0$ is the identity element under addition

④ Existence of Inverse: Let y be the inverse of x

$\Rightarrow$ $x + y = e = 0$

$$\alpha_1 + \beta_1\sqrt{2} + \alpha_2 + \beta_2\sqrt{2} = e_1 + e_2\sqrt{2} = 0 + 0\sqrt{2}$$

$\Rightarrow \alpha_1 + \alpha_2 = 0$ $\qquad$ $\beta_1 + \beta_2 = 0$

$\Rightarrow \alpha_2 = -\alpha_1$ $\qquad$ $\beta_2 = -\beta_1$

$\therefore y = -\alpha_1 - \beta_1\sqrt{2} \in \mathbb{Q}\sqrt{2}$ is the unique inverse of x.

~~ii) To check whether $(\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ is an a~~

⑤ Commutativity: $x + y = \alpha_1 + \beta_1\sqrt{2} + \alpha_2 + \beta_2\sqrt{2}$

$$= (\alpha_1 + \alpha_2) + \sqrt{2}(\beta_1 + \beta_2)$$
$$= (\alpha_2 + \alpha_1) + \sqrt{2}(\beta_2 + \beta_1)$$
$$= \alpha_2 + \sqrt{2}\beta_2 + \alpha_1 + \beta_1\sqrt{2}$$
$$= y + x$$

$\therefore$ $\mathbb{Q}\sqrt{2}$ satisfies commutative property under addition.

$\therefore$ $(\mathbb{Q}\sqrt{2}, +)$ is an abelian group.

ii) To check whether $(\mathbb{Q}\sqrt{2} \setminus \{0\}, \cdot)$ is an abelian Group:

Let $x = \alpha_1 + \beta_1\sqrt{2}$, $y = \alpha_2 + \beta_2\sqrt{2}$, $z = \alpha_3 + \beta_3\sqrt{2} \in \mathbb{Q}\sqrt{2} \setminus \{0\}$ where $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{Q}$

① Closure: $x \cdot y = (\alpha_1 + \beta_1\sqrt{2}) \cdot (\alpha_2 + \beta_2\sqrt{2})$

$$= \alpha_1\alpha_2 + \sqrt{2}\alpha_1\beta_2 + \sqrt{2}\alpha_2\beta_2 + 2\beta_1\beta_2$$
$$= (\alpha_1\alpha_2 + 2\beta_1\beta_2) + \sqrt{2}(\alpha_1\beta_2 + \alpha_2\beta_2) \in \mathbb{Q}(\sqrt{2})$$

since $\alpha_1\alpha_2 + 2\beta_1\beta_2 \in \mathbb{Q}$ & $\alpha_1\beta_2 + \alpha_2\beta_2 \in \mathbb{Q}$

$\therefore$ $(\mathbb{Q}\sqrt{2} \setminus \{0\})$ is closed under multiplication.

② Associativity: $(x * y) * z = (\alpha_1 + \beta_1\sqrt{2}) \cdot (\alpha_2 + \beta_2\sqrt{2}) \cdot (\alpha_3 + \beta_3\sqrt{2})$

$= (\alpha_1 + \beta_1\sqrt{2}) \cdot ((\alpha_2 + \beta_2\sqrt{2}) \cdot (\alpha_3 + \beta_3\sqrt{2}))$

$= x \cdot (y \cdot z)$

$\therefore (\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ satisfies associativity under multiplication.

③ Multiplicative Identity: Let $e = e_1 + e_2\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \setminus \{0\}$ where $e_1, e_2 \in \mathbb{Q}$ be the multipercative identity.

$\Rightarrow x \cdot e = x$

$(\alpha_1 + \beta_1\sqrt{2})(e_1 + e_2\sqrt{2}) = \alpha_1 + \beta_1\sqrt{2}$

$(\alpha_1 e_1 + 2\beta_1 e_2) + \sqrt{2}(\alpha_1 e_2 + \beta_1 e_1) = \alpha_1 + \beta_1\sqrt{2}$

$\alpha_1 e_1 + 2\beta_1 e_2 = \alpha_1 \qquad \alpha_1 e_2 + \beta_1 e_1 = \beta_1$

$\Rightarrow e_1 = 1, \quad e_2 = 0$

$\therefore e = 1 + 0\sqrt{2} = 1$ is the multipercative identity of $(\mathbb{Q}(\sqrt{2}) \setminus \{0\})$

④ Multiplicative Inverse: Let y be the inverse of x

$\Rightarrow x * y = e \Rightarrow (\alpha_1 + \beta_1\sqrt{2}) \cdot (\alpha_2 + \beta_2\sqrt{2}) = (1 + 0\sqrt{2})$

$\alpha_1\alpha_2 + 2\beta_1\beta_2 + \sqrt{2}(\alpha_1\beta_2 + \alpha_2\beta_1) = 1 + 0\sqrt{2}$

$\alpha_1\alpha_2 + 2\beta_1\beta_2 = 1 \qquad \alpha_1\beta_2 + \alpha_2\beta_1 = 0$

$(\alpha_2 + \beta_2\sqrt{2}) = y = \dfrac{1}{\alpha_1 + \beta_1\sqrt{2}} = \dfrac{\alpha_1 - \beta_1\sqrt{2}}{\alpha_1^2 - 2\beta_1^2}$

$= \dfrac{\alpha_1}{\alpha_1^2 - 2\beta_1^2} - \dfrac{\beta_1\sqrt{2}}{\alpha_1^2 - 2\beta_1^2} \in \mathbb{Q}\sqrt{2}$

since $\dfrac{\alpha_1}{\alpha_1^2 - 2\beta_1^2}, \dfrac{\beta_1}{\alpha_1^2 - 2\beta_1^2} \in \mathbb{Q}$ if $\alpha_1^2 + 2\beta_1^2$

$\therefore$ y is the unique inverse of x.

⑤ Commutativity: $x \cdot y = (\alpha_1 + \beta_1\sqrt{2}) \cdot (\alpha_2 + \beta_2\sqrt{2})$

$= \alpha_1\alpha_2 + 2\beta_1\beta_2 + \sqrt{2}(\alpha_1\beta_2 + \alpha_2\beta_1)$

$= (\alpha_2 + \beta_2\sqrt{2}) \cdot (\alpha_1 + \beta_1\sqrt{2}) = y \cdot x$

$\therefore (\mathbb{Q}(\sqrt{2}) \setminus \{0\})$ satisfies commutative property under multiplication

$\therefore (\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ forms abelian group under multiplication.

iii) Distributive Property: $x \cdot (y+z) = (\alpha_1 + \beta_1\sqrt{2}) \cdot (\alpha_2+\beta_2\sqrt{2}+\alpha_3+\beta_3\sqrt{2})$

where $x = \alpha_1+\beta_1\sqrt{2}$, $y = \alpha_2+\beta_2\sqrt{2}$, $z = \alpha_3+\beta_3\sqrt{2}$ $\Big\} \in \mathbb{Q}(\sqrt{2})$

& $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{Q}$

~~$= \alpha_1+\beta_1\sqrt{2}$~~

$= \alpha_1\alpha_2 + \alpha_1\alpha_3 + 2\beta_1\beta_2 + 2\beta_1\beta_3$

$+\sqrt{2}(\alpha_2\beta_1 + \alpha_1\beta_2 + \alpha_3\beta_1 + \alpha_1\beta_3)$

$= (\alpha_1\alpha_2 + 2\beta_1\beta_2 + \sqrt{2}(\alpha_2\beta_1 + \alpha_1\beta_2))$

$+ (\alpha_1\alpha_3 + 2\beta_1\beta_3 + \sqrt{2}(\alpha_3\beta_1 + \alpha_1\beta_3))$

$= (\alpha_1+\beta_1\sqrt{2}) \cdot (\alpha_2+\beta_2\sqrt{2}) + (\alpha_1+\beta_1\sqrt{2}) \cdot (\alpha_3+\beta_3\sqrt{2})$

$= x \cdot y + x \cdot z$

$\therefore \mathbb{Q}(\sqrt{2})$ satisfies distributive property

$\therefore \mathbb{Q}(\sqrt{2})$ forms a field.

(2) If α, β in previous question (1) are integers only, then while finding the multiplicative inverse,

$x \cdot y = e = 1$

$y = \frac{1}{x} = \frac{1}{\alpha_1+\beta_1\sqrt{2}} = \frac{\alpha_1}{\alpha_1^2-2\beta_1^2} - \frac{\beta_1\sqrt{2}}{\alpha_1^2-2\beta_1^2}$

But $\frac{\alpha_1}{\alpha_1^2-2\beta_1^2}$, $\frac{\beta_1\sqrt{2}}{\alpha_1^2-2\beta_1^2} \notin \mathbb{Z}$

$\therefore$ x doesn't have inverse.

$\therefore$ $\mathbb{Q}(\sqrt{2})$ with $\alpha, \beta \in \mathbb{Z}$ is not a field.

(3) $\mathbb{Q}(\sqrt{2})$ is a vector space if

(i) $(\mathbb{Q}(\sqrt{2}), +)$ forms an abelian Group

This has already been proved in previous part

(ii) satisfies properties of scalar multiplication

① ~~closure~~: Let $x = \alpha_1 + \beta_1\sqrt{2}$ $y = \alpha_2 + \beta_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $c, c_1, c_2 \in \mathbb{Q}$

where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Q}$

① closure: $c.\bar{x} = c.(\alpha_1 + \beta_1\sqrt{2}) = c\alpha_1 + c\beta_1\sqrt{2} \in \mathbb{Q}\sqrt{2}$

since $c\alpha_1, c\beta_1 \in \mathbb{Q}$.

$\therefore$ $\mathbb{Q}(\sqrt{2})$ is closed under scalar multiplication.

② Associativity: $c_1.(c_2.x) = c_1.(c_2.(\alpha_1 + \beta_1\sqrt{2}))$

$= c_1.(c c_2\alpha_1 + c_2\beta_1\sqrt{2})$

$= c_1 c_2 \alpha_1 + c_1 c_2 \beta_1\sqrt{2}$

$= (c_1.c_2)(\alpha_1 + \beta_1\sqrt{2}) = (c_1.c_2)x$

③ Distributive: $(c_1 + c_2).x = (c_1 + c_2).(\alpha_1 + \beta_1\sqrt{2})$

$= c_1\alpha_1 + c_1\beta_1\sqrt{2} + c_2\alpha_1 + c_2\beta_1\sqrt{2}$

$= c_1.(\alpha_1 + \beta_1\sqrt{2}) + c_2.(\alpha_1 + \beta_1\sqrt{2})$

$= c_1.x + c_2.x$

$c.(x+y) = c.(\alpha_1 + \beta_1\sqrt{2} + \alpha_2 + \beta_2\sqrt{2})$

$= c\alpha_1 + c\beta_1\sqrt{2} + c\alpha_2 + c\beta_2\sqrt{2}$

$= c(\alpha_1 + \beta_1\sqrt{2}) + c(\alpha_2 + \beta_2\sqrt{2})$

$= c.x + c.y$

$\therefore$ $\mathbb{Q}(\sqrt{2})$ satisfies all properties of scalar multiplication.

$\therefore$ $\mathbb{Q}(\sqrt{2})$ forms a vector space over $\mathbb{Q}$.

Consider $B = \{1, \sqrt{2}\}$ where $x = 1 = 1 + 0\sqrt{2}$ and $y = \sqrt{2} = 0 + 1.\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

we see that $c_1x + c_2y = c_1 + \sqrt{2}c_2 = 0$ iff $c_1 = c_2 = 0$

$\Rightarrow$ B is linearly independent subset of $\mathbb{Q}(\sqrt{2})$.

Moreover any vector in $\mathbb{Q}(\sqrt{2})$ can be represented as a linear combination of the elements in B.

$\therefore$ ~~B {1,√2} Suppose~~ Take any arbitrary element $\alpha + \beta\sqrt{2} \in \mathbb{Q}\sqrt{2}$

$\alpha + \beta\sqrt{2} = \alpha(1 + 0\sqrt{2}) + \beta(0 + 1\sqrt{2})$

$\therefore$ B spans the vector space $\mathbb{Q}(\sqrt{2})$

$\therefore$ $B = \{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$.

(9) (i) $\mathbb{Z}_p = \{0, 1, \ldots p-1\}$. We have to show that $(\mathbb{Z}_p, +, \cdot)$ is a field iff p is prime. Note that addition & multiplication operations are over mod p.

To show $(\mathbb{Z}_p, +, \cdot)$ is field, we have to show that

(a) $(\mathbb{Z}_p, +)$ — forms an abelian group.

(b) $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ — Abelian group.

(c) For any $c_1, c_2, c_3 \in \mathbb{Z}_p$, $c_1 \cdot (c_2 + c_3) = c_1c_2 + c_1c_3$ → Distributive property holds.

(a) A set G with some operation will be called as abelian group if function (ai) Satisfies associativity property

(aii) has identity element

(aiii) Every element of G has inverse with respect to operation defined on G.

(aiv) Commutative property holds.

(ai) For any $a, b, c \in \mathbb{Z}_p$, $a + (b + c) = (a + b) + c$.

closure: For any $a, b \in \mathbb{Z}_p$ $(a+b) \bmod p \in \mathbb{Z}_p$.

(aii) For any $a \in \mathbb{Z}_p \setminus \{0\}$, $a + 0 = a = 0 + a$. '0' is additive-identity.

(aiii) For any $a \in \mathbb{Z}_p$, $a + (p - a) = 0$, So, 'p-a' is the additive-inverse of a.

(aiv) For any $a, b \in \mathbb{Z}_p$, $a + b = b + a$

(b) (bi) For any $a, b, c \in \mathbb{Z}_p \setminus \{0\}$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(bii) For any $a \in \mathbb{Z}_p \setminus \{0\}$, $a \cdot 1 = 1 \cdot a = a$,

∴ '1' is the multiplicative identity.

(b(ii)) , (b(iv)) $a \cdot b = b \cdot a$ for any $a, b \in Z_p \setminus \{0\}$.

Note that all properties are satisfied irrespective of Value of p (prime or not) except (biii).

(biii) Existence of multiplicative inverse.

For any two integers a, b, there exists two integers l, s such that

$$la + sb = \gcd(a, b)$$

let $a = p$, $b \in Z_p$., then

$$lp + sb = \gcd(p, b), \text{ Apply mod } p \text{ on both sides,}$$

$$lp \bmod p + sb \bmod p = \gcd(p, b) \bmod p.$$

$$0 + sb \bmod p = \gcd(p, b) \bmod p.$$

$$b(s \bmod p) = \gcd(p, b) \bmod p.$$

For any $b \in Z_p$, $\gcd(p, b) = 1$ if p is prime.

if p is not prime, $\gcd(p, b)$ will not be '1' for all values of $b \in Z_p$. So, if p is not prime, few elements of Z_p will have multiplicative inverse while others don't.

So, Z_p is a field if and only if p is prime.

9) (ii) To show Z_{p^m} is a field.

Given Z_{p^m} consists of polynomials in $Z_p(x)$ (modulo $g(x)$). So, the elements in Z_{p^m} will be of the form $a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$. Where $a_i \in Z_p$, $\forall\ i = \{1, \ldots m\}$.

(a) $(Z_{p^m}, +)$. is an abelian group.

Here addition operation is done over mod p. (modulo p addition)

Consider a polynomial $f(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \in Z_{p^m}$.

Additive ~~identity~~ inverse of $f(x)$ is $(p-a_0) + (p-a_1)x + \cdots + (p-a_{m-1}) x^{m-1}$. Which lies in Z_{p^m}.

Consider $f'(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} \in Z_{p^m}$.

For any $f(x), f'(x) \in Z_{p^m}$, $f(x) + f'(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_{m-1}+b_{m-1}) x^{m-1}$

$f(x) + f'(x) \in Z_{p^m}$, since $a_i + b_i \in Z_p\ \forall\ i = \{1, \ldots m-1\}$.

Additive identity for any $f(x) \in Z_{p^m}$ is $\underline{0}$.

For any $f(x), f'(x), f''(x) \in Z_{p^m}$, $f(x) + (f'(x) + f''(x)) = (f(x) + f'(x)) + f''(x)$ i.e associativity holds.

For any $f(x), f'(x) \in Z_{p^m}$, $f(x) + f'(x) = f'(x) + f(x) \rightarrow$ Commutativity holds.

So, $(Z_{p^m}, +)$ is an abelian group.

(b) $(Z_{p^m}, \cdot)$ is an abelian group.

Here multiplication operation is over mod $g(x)$. where $g(x)$ is irreducible polynomial.

Consider two polynomials $f(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$,

$f'(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1}$. $f(x), f'(x) \in Z_{p^m}$.

$$f(x) \cdot f'(x) = (a_0 + a_1 x + \cdots + a_{m-1} x^{m-1})(b_0 + b_1 x + \cdots + b_{m-1} x^{m-1})$$

$$= a_{m-1} b_{m-1}$$

For any k, polynomial of degree k modulo $g(x)$ where $g(x)$ $(k > m)$ is polynomial of degree m gives polynomial of degree $< m$.

So, Z_{p^m} is closed under multiplication.

For any $f(x) \in Z_{p^m}$, 1 is the multiplicative identity.

Existence of multiplicative inverse:

For any two polynomials $a(x)$, $b(x)$ in $Z_p[x]$, there exists polynomials $l(x), s(x)$ in $Z_p[x]$ such that

$$l(x)\, a(x) + s(x)\, b(x) = \gcd(a(x), b(x))$$

put $a(x) = g(x)$, then

$$l(x)\, g(x) + s(x)\, b(x) = \gcd(g(x), b(x))$$

Apply mod $g(x)$ on both sides

$$s(x)\, b(x) = \gcd(g(x), b(x)) \bmod g(x) \bmod g(x)$$

$$b(x)(s(x) \bmod g(x)) = 1$$

$\gcd(g(x), b(x)) = 1$ Since $g(x)$ is irreducible polynomial.

$s(x) \bmod g(x) \in Z_{p^m}$ is the multiplicative inverse of $b(x)$

10) (i) Suppose Basis (say B) is not the maximal linear Independent set.

Let $B = \{b_1, b_2, \ldots b_n\}$ be a basis for some Vector Space V.

Consider a non-zero vector $\alpha \in V$, $\alpha \notin B$. We can observe that $B \cup \{\alpha\}$ is linear dependent set as any non-zero vector $\alpha \in V$ can be represented as linear Combination of b_i's of B. For any $\alpha \in V$,

ie $\alpha = \sum_{i=1}^{n} c_i b_i$, not all c_i's are zero.

$\therefore$ B is maximal linear independent Set.

Suppose there exists a Spanning set, A for V such that $|A| < |B|$ (Basis B), then every vector $\alpha \in V$ can be written as linear Combination of elements in A. So, A is another basis set for V. Which is a Contradiction as $|A| < |B|$.

(ii) Given W is a Subspace of V and basis of W is $\{\alpha_i : i = 1 \text{ to } m\}$.

We have to show that $\{\alpha_i + \beta : i = 1, 2, \ldots m\}$ Spans an m-dimensional Subspace of V where $\beta \in V/W$.

First let's check whether the set $\{\alpha_i + \beta : i = 1, \ldots m\}$ is linear independent-set & not.

$$c_1(\alpha_1 + \beta) + c_2(\alpha_2 + \beta) + \ldots + c_m(\alpha_m + \beta) = 0.$$

$$c_1\alpha_1 + \ldots + c_m\alpha_m + \beta(c_1 + \ldots + c_m) = 0. \quad \text{---} \quad (1)$$

The only possible Case is $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$ and $c_1 + c_2 + \ldots + c_m = 0$.

because β can't be written as $-\frac{\sum_{i}^{m} c_i\alpha_i}{\sum_{i}^{m} c_i}$ $(\because \beta \in V/W)$

Note that $\{\alpha_i : i = 1, 2, \ldots m\}$ is basis for W,

So, $\sum_{i=1}^{m} c_i \alpha_i = 0$, iff $c_i = 0 \ \forall \ i = \{1, \ldots m\}$.

Therefore, the set $\{\alpha_i + \beta : i = 1, \ldots m\}$ is a linear independent set of size m. and it spans ~~Some~~ m dimensional space of V with basis $= \{\alpha_i + \beta : i = 1, \ldots m\}$.