1.

In Shamir's scheme, if the threshold is k, then any k people together can reconstruct the secret. Since the assumption is the secret can be accessed by three people, $k = 3$ That also implies the polynomial $q(x)$ is quadratic with degree $k - 1 = 2$

$$\begin{aligned} \text{Total participants:} \quad & n = 5, \\ \text{Threshold:} \quad & k = 3, \\ \text{Polynomial degree:} \quad & k - 1 = 2 \end{aligned}$$

The interpolation polynomial is

$$q(x) = y_1 L_1(x) + y_2 L_2(x) + y_3 L_3(x)$$

where

$$L_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}, \quad L_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}, \quad L_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

$$\begin{aligned} q(x) &= y_1 L_1(x) + y_2 \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3 L_3(x) \pmod{257} \\ &= y_1 \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} + y_2 \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3 \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)} \pmod{257} \\ &= 13 \cdot \frac{(x - 114)(x - 199)}{(15 - 114)(15 - 199)} + 94 \cdot \frac{(x - 15)(x - 199)}{(114 - 15)(114 - 199)} + 146 \cdot \frac{(x - 15)(x - 114)}{(199 - 15)(199 - 114)} \pmod{257} \\ &= 13 \cdot \frac{(x - 114)(x - 199)}{18216} + 94 \cdot \frac{(x - 15)(x - 199)}{-8415} + 146 \cdot \frac{(x - 15)(x - 114)}{15640} \pmod{257} \\ &= 13 \cdot \frac{(x - 114)(x - 199)}{226} + 94 \cdot \frac{(x - 15)(x - 199)}{66} + 146 \cdot \frac{(x - 15)(x - 114)}{220} \pmod{257} \\ &= 13 \cdot (x - 114)(x - 199) \cdot 226^{-1} + 94 \cdot (x - 15)(x - 199) \cdot 66^{-1} + 146 \cdot (x - 15)(x - 114) \cdot 220^{-1} \pmod{257} \\ &= 13 \cdot (x - 114)(x - 199) \cdot 58 + 94 \cdot (x - 15)(x - 199) \cdot 74 + 146 \cdot (x - 15)(x - 114) \cdot 125 \pmod{257} \\ &= 754 \cdot (x - 114)(x - 199) + 6956 \cdot (x - 15)(x - 199) + 18250 \cdot (x - 15)(x - 114) \pmod{257} \\ &= 240 \cdot (x - 114)(x - 199) + 17 \cdot (x - 15)(x - 199) + 3 \cdot (x - 15)(x - 114) \pmod{257} \end{aligned}$$

To find the secret $N = q(0)$, substitute $x = 0$ into the interpolation polynomial:

$$\begin{aligned} q(0) &= 240 \cdot (0 - 114)(0 - 199) + 17 \cdot (0 - 15)(0 - 199) + 3 \cdot (0 - 15)(0 - 114) \pmod{257} \\ &= 240 \cdot (-114)(-199) + 17 \cdot (-15)(-199) + 3 \cdot (-15)(-114) \pmod{257} \\ &= 240 \cdot 114 \cdot 199 + 17 \cdot 15 \cdot 199 + 3 \cdot 15 \cdot 114 \pmod{257} \\ &= 27360 \cdot 199 + 255 \cdot 199 + 45 \cdot 114 \pmod{257} \quad (\text{where } 27360 \equiv 118 \pmod{257}) \\ &= 118 \cdot 199 + 255 \cdot 199 + 45 \cdot 114 \pmod{257} \\ &= 23482 + 50745 + 5130 \pmod{257} \\ &= 95 + 116 + 247 \pmod{257} \quad (\text{where } 23482 \equiv 95,\ 50745 \equiv 116,\ 5130 \equiv 247 \pmod{257}) \\ &= 458 \equiv 201 \pmod{257} \end{aligned}$$

2.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \text{ with addition and multiplication defined modulo 6}$$

Checking if $(\mathbb{Z}_6, +)$ forms an abelian group.

1. **Closure** For all $a, b \in \mathbb{Z}_6$, $(a+b) \bmod 6 \in \mathbb{Z}_6$. Examples:
   - $4+5=9 \equiv 3 \pmod 6$ (and $3 \in \mathbb{Z}_6$)
   - $2+2=4 \equiv 4 \pmod 6$ (and $4 \in \mathbb{Z}_6$)
   - $5+5=10 \equiv 4 \pmod 6$ (and $4 \in \mathbb{Z}_6$)
2. **Associativity** For all $a, b, c \in \mathbb{Z}_6$, $(a+b)+c \equiv a+(b+c) \pmod 6$. Example: Verify $(2+4)+5 = 2+(4+5)$
   - $(2+4)+5 = 6+5 \equiv 0+5 = 5 \pmod 6$
   - $2+(4+5) = 2+9 \equiv 2+3 = 5 \pmod 6$

   Both sides equal 5, confirming associativity.
3. **Identity** There exists $0 \in \mathbb{Z}_6$ such that $a+0 \equiv 0+a \equiv a \pmod 6$ for all $a \in \mathbb{Z}_6$. Examples:
   - $3+0=3 \equiv 3 \pmod 6$ and $0+3=3 \equiv 3 \pmod 6$
   - $4+0=4 \equiv 4 \pmod 6$ and $0+4=4 \equiv 4 \pmod 6$
4. **Inverses** For every $a \in \mathbb{Z}_6$, there exists $-a \in \mathbb{Z}_6$ such that $a+(-a) \equiv 0 \pmod 6$.
   - For $a=0$: We need $0+b \equiv 0 \pmod 6$, so $b=0$. Thus $-0=0$.
   - For $a=1$: We need $1+b \equiv 0 \pmod 6$, so $b=5$. Thus $-1=5$.
   - For $a=2$: We need $2+b \equiv 0 \pmod 6$, so $b=4$. Thus $-2=4$.
   - For $a=3$: We need $3+b \equiv 0 \pmod 6$, so $b=3$. Thus $-3=3$.
   - For $a=4$: We need $4+b \equiv 0 \pmod 6$, so $b=2$. Thus $-4=2$.
   - For $a=5$: We need $5+b \equiv 0 \pmod 6$, so $b=1$. Thus $-5=1$.
5. **Commutativity** For all $a, b \in \mathbb{Z}_6$, $a+b \equiv b+a \pmod 6$.

   Examples:
   - $2+5=7 \equiv 1 \pmod 6$ and $5+2=7 \equiv 1 \pmod 6$
   - $3+4=7 \equiv 1 \pmod 6$ and $4+3=7 \equiv 1 \pmod 6$

All additive axioms (closure, associativity, identity, inverses, and commutativity) are satisfied. Therefore, $(\mathbb{Z}_6, +)$ forms an abelian group.

Checking if $(\mathbb{Z}_6 \setminus \{0\}, \times)$ forms an abelian group. Let $S = \mathbb{Z}_6 \setminus \{0\} = \{1, 2, 3, 4, 5\}$.

1. **Closure** For all $a, b \in S$, $(a \cdot b) \bmod 6 \in S$. Counterexamples:
   - $2 \cdot 3 = 6 \equiv 0 \pmod 6$, but $0 \notin S$
   - $3 \cdot 4 = 12 \equiv 0 \pmod 6$, but $0 \notin S$
   - $2 \cdot 2 \cdot 3 = 12 \equiv 0 \pmod 6$, but $0 \notin S$
2. **Associativity** For all $a, b, c \in S$, $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod 6$. Example: Verify $(2 \cdot 4) \cdot 5 = 2 \cdot (4 \cdot 5)$ in $\mathbb{Z}_6$
   - $(2 \cdot 4) \cdot 5 = 8 \cdot 5 \equiv 2 \cdot 5 = 10 \equiv 4 \pmod 6$
   - $2 \cdot (4 \cdot 5) = 2 \cdot 20 \equiv 2 \cdot 2 = 4 \pmod 6$

   Both sides equal 4, confirming associativity.
3. **Identity** There exists $1 \in S$ such that $a \cdot 1 \equiv 1 \cdot a \equiv a \pmod 6$ for all $a \in S$. Examples:
   - $4 \cdot 1 = 4 \equiv 4 \pmod 6$ and $1 \cdot 4 = 4 \equiv 4 \pmod 6$
   - $5 \cdot 1 = 5 \equiv 5 \pmod 6$ and $1 \cdot 5 = 5 \equiv 5 \pmod 6$
4. **Inverses** For every $a \in S$, there exists $a^{-1} \in S$ such that $a \cdot a^{-1} \equiv 1 \pmod 6$. Case-by-case check:
   - $1 \cdot 1 = 1 \equiv 1 \pmod 6 \quad \Rightarrow \quad 1^{-1} = 1$.

- $2 \cdot 1 = 2 \not\equiv 1 \pmod 6$, $2 \cdot 2 = 4 \not\equiv 1 \pmod 6$, $2 \cdot 3 = 0 \not\equiv 1 \pmod 6$, $2 \cdot 4 = 2 \not\equiv 1 \pmod 6$, $2 \cdot 5 = 4 \not\equiv 1 \pmod 6$.

  No inverse exists.
- $3 \cdot 1 = 3 \not\equiv 1 \pmod 6$, $3 \cdot 2 = 0 \not\equiv 1 \pmod 6$, $3 \cdot 3 = 3 \not\equiv 1 \pmod 6$, $3 \cdot 4 = 0 \not\equiv 1 \pmod 6$, $3 \cdot 5 = 3 \not\equiv 1 \pmod 6$.

  No inverse exists.
- $4 \cdot 1 = 4 \not\equiv 1 \pmod 6$, $4 \cdot 2 = 2 \not\equiv 1 \pmod 6$, $4 \cdot 3 = 0 \not\equiv 1 \pmod 6$, $4 \cdot 4 = 4 \not\equiv 1 \pmod 6$, $4 \cdot 5 = 2 \not\equiv 1 \pmod 6$.

  No inverse exists.
- $5 \cdot 1 = 5 \not\equiv 1 \pmod 6$, $5 \cdot 2 = 4 \not\equiv 1 \pmod 6$, $5 \cdot 3 = 3 \not\equiv 1 \pmod 6$, $5 \cdot 4 = 2 \not\equiv 1 \pmod 6$, $5 \cdot 5 = 25 \equiv 1 \pmod 6$.

  Inverse exists: $5^{-1} = 5$.

5. **Commutativity** For all $a, b \in S$, $a \cdot b \equiv b \cdot a \pmod 6$. Examples:
   - $2 \cdot 5 = 10 \equiv 4 \pmod 6$ and $5 \cdot 2 = 10 \equiv 4 \pmod 6$
   - $3 \cdot 5 = 15 \equiv 3 \pmod 6$ and $5 \cdot 3 = 15 \equiv 3 \pmod 6$

Since closure fails and not all elements have multiplicative inverses, $(\mathbb{Z}_6 \setminus \{0\}, \times)$ is not a group, and therefore $\mathbb{Z}_6$ is not a field.

Distributivity in $\mathbb{Z}_6$: For all $a, b, c \in \mathbb{Z}_6$, $a(b+c) \equiv ab + ac \pmod 6 \quad \text{and} \quad (a+b)c \equiv ac + bc \pmod 6$ Example: Verify $2(4+5) = 2 \cdot 4 + 2 \cdot 5$ in $\mathbb{Z}_6$

- $2(4+5) = 2 \cdot 9 \equiv 2 \cdot 3 = 6 \equiv 0 \pmod 6$
- $2 \cdot 4 + 2 \cdot 5 = 8 + 10 = 18 \equiv 0 \pmod 6$

Both sides equal 0, confirming distributivity holds.

As $(\mathbb{Z}_6, +)$ is an abelian group and $(\mathbb{Z}_6 \setminus \{0\}, \times)$ is not a group, $\mathbb{Z}_6$ is not a field.

3.

a)

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

Taking elements of $\mathbb{Q}(\sqrt{2})$:

$$\begin{aligned} x &= a + b\sqrt{2}, \\ y &= c + d\sqrt{2}, \qquad a, b, c, d \in \mathbb{Q}. \end{aligned}$$

$$\begin{aligned} xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2 \\ &= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\ &= (ac + 2bd) + (ad + bc)\sqrt{2}. \end{aligned}$$

Since rational numbers are closed under multiplication, $ac \in \mathbb{Q}$ and $bd \in \mathbb{Q}$. The closure under scalar multiplication ensures that $2bd \in \mathbb{Q}$, and closure under addition guarantees that $ac+2bd \in \mathbb{Q}$. Similarly, $ad+bc \in \mathbb{Q}$.Therefore, $xy = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

b)

Let $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $a, b \in \mathbb{Q}$, $x \neq 0$. Let $\overline{x} = a - b\sqrt{2}$.

$$\begin{aligned} x\overline{x} &= (a + b\sqrt{2})(a - b\sqrt{2}) \\ &= a^2 - ab\sqrt{2} + ab\sqrt{2} - b^2(\sqrt{2})^2 \\ &= a^2 - b^2 \cdot 2 \\ &= a^2 - 2b^2 \end{aligned}$$

Since $a, b \in \mathbb{Q}$, we have $a^2 \in \mathbb{Q}$ and $2b^2 \in \mathbb{Q}$, hence $a^2 - 2b^2 \in \mathbb{Q}$.
If $b = 0$, then $x = a \neq 0$, so $a^2 - 2b^2 = a^2 \neq 0$. If $b \neq 0$ and $a^2 - 2b^2 = 0$, then $(a/b)^2 = 2$, forcing $a/b = \sqrt{2} \notin \mathbb{Q}$, a contradiction.
Hence $a^2 - 2b^2 \neq 0$.

$$\begin{aligned} x^{-1} &= \frac{\overline{x}}{x\overline{x}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \end{aligned}$$

Since $a, b \in \mathbb{Q}$ and $a^2 - 2b^2 \in \mathbb{Q} \setminus \{0\}$, both coefficients $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are rational. Therefore, $x^{-1} = p + q\sqrt{2}$ with $p, q \in \mathbb{Q}$, proving that $x^{-1} \in \mathbb{Q}(\sqrt{2})$.

$$\begin{aligned} x \cdot x^{-1} &= (a + b\sqrt{2}) \cdot \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{(a + b\sqrt{2})(a - b\sqrt{2})}{a^2 - 2b^2} \\ &= \frac{a^2 - 2b^2}{a^2 - 2b^2} \\ &= 1 \end{aligned}$$

4.

A subset S of a vector space V is a subspace if:

1. $S \neq \emptyset$ (non-empty), equivalently $0 \in S$.
2. For all $u, v \in S$, we have $u + v \in S$ (closed under addition).
3. For all $u \in S$ and $c \in \mathbb{R}$, we have $cu \in S$ (closed under scalar multiplication).

a)

$$S = \left\{A \in \mathbb{R}^{2\times 2} : \det(A) = 0\right\}$$

For a 2×2 matrix in vector space $\mathbb{R}^{2\times 2}$

$$A = \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \quad x, y, z, w \in \mathbb{R}$$

the determinant is given by $\det(A) = xw - yz$
Thus, the set

$$S = \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in \mathbb{R}^{2\times 2} : xw - yz = 0 \right\}$$

is the collection of all 2×2 matrices with determinant zero.
The zero matrix in $\mathbb{R}^{2\times 2}$ is

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Determinant of the zero matrix O: $\det(O) = (0)(0) - (0)(0) = 0$
Therefore, the zero matrix satisfies the first requirement of the subspace conditions as $S \neq \emptyset$ (non-empty) since $\det(O) = 0 \implies O \in S$.
Picking any two matrices in S:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Determinant of A: $\det(A) = (1)(0) - (0)(0) = 0 \implies A \in S$
Determinant of B: $\det(B) = (0)(1) - (0)(0) = 0 \implies B \in S$
Thus, both A and B belong to the set S.

$$A + B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Determinant of $A + B$: $\det(A + B) = (1)(1) - (0)(0) = 1$
Since $\det(A + B) = 1 \neq 0$: $A + B \notin S$

Even though both A and B are in S, their sum $A + B$ is not in S. Therefore, S is not closed under addition, and the second subspace condition fails, since $A, B \in S$ but $A + B \notin S$.

Let $A \in S$. Then

$$A = \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \qquad \det(A) = xw - yz = 0$$

Scale A by $c \in \mathbb{R}$:

$$cA = c \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} cx & cy \\ cz & cw \end{bmatrix}$$

Determinant of cA:$\det(cA) = (cx)(cw) - (cy)(cz) = c^2(xw - yz)$
Since $\det(A) = xw - yz = 0$: $\det(cA) = c^2 \cdot 0 = 0 \implies cA \in S$
Thus, cA belongs to the set S.

The set S satisfies:

- $S \neq \emptyset$
- Not closed under addition
- Closed under scalar multiplication

Therefore S is not a subspace of $\mathbb{R}^{2\times 2}$

b)

$$S = \left\{ A \in \mathbb{R}^{2\times 2} : \operatorname{tr}(A) = 0 \right\}.$$

For a 2×2 matrix

$$A = \begin{bmatrix} x & y \\ z & w \end{bmatrix},$$

the trace is defined as $\operatorname{tr}(A) = x + w$
Thus, the set

$$S = \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in \mathbb{R}^{2\times 2} : x + w = 0 \right\}$$

is the collection of all 2×2 matrices with zero trace.

The zero matrix in $\mathbb{R}^{2\times 2}$ is

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Trace of the zero matrix O:$\text{tr}(O) = 0 + 0 = 0 \implies O \in S$ Therefore, the zero matrix satisfies the first requirement of the subspace conditions as $S \neq \emptyset$ (non-empty) since $\text{tr}(O) = 0 \implies O \in S$.

Picking any two matrices in S:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} -4 & 0 \\ 5 & 4 \end{bmatrix}$$

Trace of A: $\text{tr}(A) = 1 + (-1) = 0 \implies A \in S$
Trace of B: $\text{tr}(B) = -4 + 4 = 0 \implies B \in S$
Thus, both A and B belong to the set S.

$$A + B = \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} + \begin{bmatrix} -4 & 0 \\ 5 & 4 \end{bmatrix} = \begin{bmatrix} -3 & 2 \\ 8 & 3 \end{bmatrix}$$

Trace of $A + B$: $\text{tr}(A + B) = -3 + 3 = 0 \implies A + B \in S$
Since $\text{tr}(A + B) = 0$: $A + B \in S$

A and B are in S and their sum $A + B$ is in S. Therefore, S is closed under addition, and the second subspace condition is satisfied, since $A, B \in S$ but $A + B \in S$.

Scaling A by $c \in \mathbb{R}$:

$$cA = c\begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} = \begin{bmatrix} c & 2c \\ 3c & -c \end{bmatrix}$$

Determinant of cA:$\text{tr}(cA) = c + (-c) = 0 \implies cA \in S$
Thus, cA belongs to the set S and S is closed under scalar multiplication.
The set S satisfies:

- $S \neq \emptyset$
- Closed under addition
- Closed under scalar multiplication

Therefore, S is a subspace of $\mathbb{R}^{2\times 2}$.

5.

a)

Pivot Column Theorem. If U is a row-echelon form of a matrix A, then the columns in A corresponding to the pivots in U are linearly independent and form a basis for the column space of A.

Row-reducing A to RREF yields pivots in columns $1, 2, 5$. By the Pivot Column Theorem, the corresponding original columns of A form a basis for the column space:

$$\mathcal{C}(A) = \text{span}\{\text{col}_1(A), \text{col}_2(A), \text{col}_5(A)\} = \text{span}\{v_1,\, v_2,\, w_2\}.$$

Since $\mathcal{C}(A) = W_1 + W_2$, it follows that

$$W_1 + W_2 = \text{span}\{v_1,\, v_2,\, w_2\}, \qquad \dim(W_1 + W_2) = 3.$$

b)

Let $U = \operatorname{span}\{v_1, v_2\} \subseteq W_1$ and $V = \operatorname{span}\{w_2\} \subseteq W_2$, where $v_1 = (1, 2, 1, 0)$, $v_2 = (1, 0, 0, 1)$, and $w_2 = (1, 1, 0, 0)$. Every element of U has the form $u = av_1 + bv_2$ with $a, b \in \mathbb{R}$, and every element of V has the form $v = cw_2$ with $c \in \mathbb{R}$.

Suppose $x \in U \cap V$. By definition, this means $x \in U$ and $x \in V$ simultaneously. Since $x \in U = \operatorname{span}\{v_1, v_2\}$, there exist scalars $a, b \in \mathbb{R}$ such that $x = av_1 + bv_2$. Similarly, since $x \in V = \operatorname{span}\{w_2\}$, there exists $c \in \mathbb{R}$ such that $x = cw_2$.

Combining these two expressions for x gives $x = av_1 + bv_2 = cw_2$, or equivalently $av_1 + bv_2 - cw_2 = 0$. This is a linear relation among the three vectors $\{v_1, v_2, w_2\}$. From the row-reduction we know that columns $1, 2, 5$ of A (corresponding to v_1, v_2, w_2) are pivot columns. By the Pivot Column Theorem, pivot columns are linearly independent, so the only solution to $av_1+bv_2-cw_2 = 0$ is $a = 0,\ b = 0,\ c = 0$.

Hence the only possibility is $a = b = c = 0$, which implies $x = av_1 + bv_2 = 0$. Therefore the only vector common to both U and V is the zero vector, so $U \cap V = \{0\}$. Since $U + V = W_1 + W_2$ and $U \cap V = \{0\}$, it follows by the definition of the direct sum that $U \oplus V = W_1 + W_2$.

c)

$$
\begin{aligned}
&W_1 = \operatorname{span}\{v_1, v_2, v_3\}, \quad v_1 = (1, 2, 1, 0),\ v_2 = (1, 0, 0, 1),\ v_3 = (2, 6, 3, -1),\\
&W_2 = \operatorname{span}\{w_1, w_2, w_3\}, \quad w_1 = (7, 4, 2, 5),\ w_2 = (1, 1, 0, 0),\ w_3 = (3, 0, -2, 1),
\end{aligned}
$$

Let $x \in W_1 \cap W_2$. Since $x \in W_1 = \operatorname{span}\{v_1, v_2, v_3\}$, there exist $c_1, c_2, c_3 \in \mathbb{R}$ with $x = c_1v_1 + c_2v_2 + c_3v_3$; and since $x \in W_2 = \operatorname{span}\{w_1, w_2, w_3\}$, there exist $d_1, d_2, d_3 \in \mathbb{R}$ with $x = d_1w_1 + d_2w_2 + d_3w_3$.

$$
0 = \big(c_1v_1 + c_2v_2 + c_3v_3\big) - \big(d_1w_1 + d_2w_2 + d_3w_3\big) = c_1v_1 + c_2v_2 + c_3v_3 - d_1w_1 - d_2w_2 - d_3w_3.
$$

In the RREF, each non-pivot column shows how that vector is written as a combination of pivot vectors. Since the pivots are in columns 1, 2, 5 (corresponding to v_1, v_2, w_2), we have:

$$
\begin{aligned}
v_3 &= 3v_1 - v_2, \quad \text{from column 3 entries } (3, -1, 0),\\
w_1 &= 2v_1 + 5v_2, \quad \text{from column 4 entries } (2, 5, 0),\\
w_3 &= -2v_1 + v_2 + 4w_2, \quad \text{from column 6 entries } (-2, 1, 4).
\end{aligned}
$$

Each non-pivot column gives the coefficients of the pivot columns. Substituting these into the expression for x and collecting terms on the pivot set $\{v_1, v_2, w_2\}$ gives:

$$
\begin{aligned}
x &= c_1v_1 + c_2v_2 + c_3(3v_1 - v_2)\\
&= d_1(2v_1 + 5v_2) + d_2w_2 + d_3(-2v_1 + v_2 + 4w_2),
\end{aligned}
$$

$$
0 = (c_1 + 3c_3 - 2d_1 + 2d_3)v_1 + (c_2 - c_3 - 5d_1 - d_3)v_2 + (-d_2 - 4d_3)w_2.
$$

As $\{v_1, v_2, w_2\}$ is linearly independent:

$$
\begin{aligned}
c_1 + 3c_3 - 2d_1 + 2d_3 &= 0\\
c_2 - c_3 - 5d_1 - d_3 &= 0\\
-d_2 - 4d_3 &= 0
\end{aligned}
$$

Solving for c_1, c_2, and d_2:

$$
\begin{aligned}
d_2 &= -4d_3\\
c_2 &= c_3 + 5d_1 + d_3\\
c_1 &= -3c_3 + 2d_1 - 2d_3
\end{aligned}
$$

$$
\begin{aligned}
x &= c_1v_1 + c_2v_2 + c_3v_3 \\
&= (-3c_3 + 2d_1 - 2d_3)v_1 \ + \ (c_3 + 5d_1 + d_3)v_2 \ + \ c_3v_3 \\
&= (-3c_3 + 2d_1 - 2d_3)v_1 + (c_3 + 5d_1 + d_3)v_2 + c_3(3v_1 - v_2) \\
&= \big((-3c_3) + 3c_3 + 2d_1 - 2d_3\big)v_1 \ + \ \big((c_3 - c_3) + 5d_1 + d_3\big)v_2 \\
&= (2d_1 - 2d_3)v_1 \ + \ (5d_1 + d_3)v_2
\end{aligned}
$$

$$
\begin{aligned}
x &= d_1w_1 + d_2w_2 + d_3w_3 \\
&= d_1w_1 + (-4d_3)w_2 + d_3w_3 \qquad \text{(since } d_2 = -4d_3) \\
&= d_1w_1 + d_3\,(w_3 - 4w_2).
\end{aligned}
$$

Using $w_3 = -2v_1 + v_2 + 4w_2$, we get $w_3 - 4w_2 = -2v_1 + v_2$, so equivalently

$$x = d_1w_1 \ + \ d_3(-2v_1 + v_2).$$

Intersection basis
Taking $(d_1, d_3) = (1, 0)$ gives $x = w_1$, and $(d_1, d_3) = (0, 1)$ gives $x = -2v_1 + v_2$. Hence

$$W_1 \cap W_2 = \operatorname{span}\{\, w_1,\ -2v_1 + v_2 \,\}, \qquad \dim(W_1 \cap W_2) = 2.$$

6.

a)

Given W_1 and W_2 are subspaces of a vector space V.

A subset S of a vector space V is a subspace if:

1. $S \neq \emptyset$ (non-empty), equivalently $0 \in S$.
2. For all $u, v \in S$, we have $u + v \in S$ (closed under addition).
3. For all $u \in S$ and $c \in \mathbb{R}$, we have $cu \in S$ (closed under scalar multiplication).

Because W_1 is a subspace of V, it contains the zero vector, so $0 \in W_1$. Similarly, since W_2 is a subspace of V, it also contains the zero vector, so $0 \in W_2$. By the definition of the sum $W_1 + W_2 = \{\, w_1 + w_2 : w_1 \in W_1,\ w_2 \in W_2 \,\}$, choosing $w_1 = 0 \in W_1$ and $w_2 = 0 \in W_2$ gives $0 + 0 = 0 \in W_1 + W_2$. Hence $W_1 + W_2$ contains 0 and is therefore non-empty.

Let $x, y \in W_1 + W_2$. By definition:

$$
\begin{aligned}
x &= w_1 + w_2, \quad \text{with } w_1 \in W_1,\ w_2 \in W_2, \\
y &= u_1 + u_2, \quad \text{with } u_1 \in W_1,\ u_2 \in W_2.
\end{aligned}
$$

$$
\begin{aligned}
x + y &= (w_1 + w_2) + (u_1 + u_2) \\
&= (w_1 + u_1) + (w_2 + u_2)
\end{aligned}
$$

Since W_1 is a subspace, it is closed under addition, so $w_1 + u_1 \in W_1$. Since W_2 is also a subspace, it is closed under addition, so $w_2 + u_2 \in W_2$. Thus $x + y = (w_1 + u_1) + (w_2 + u_2) \in W_1 + W_2$. Therefore, $W_1 + W_2$ is closed under addition.

Let $x \in W_1 + W_2$. By definition,

$$x = w_1 + w_2, \quad \text{with } w_1 \in W_1,\ w_2 \in W_2.$$

Multiply by a scalar $c \in \mathbb{R}$:

$$
\begin{aligned}
cx &= c(w_1 + w_2) \\
&= cw_1 + cw_2.
\end{aligned}
$$

Since W_1 is a subspace, it is closed under scalar multiplication, so $cw_1 \in W_1$. Since W_2 is also a subspace, it is closed under scalar multiplication, so $cw_2 \in W_2$. Thus $cx = cw_1 + cw_2$, with $cw_1 \in W_1$ and $cw_2 \in W_2$, and by the definition of $W_1 + W_2$ this means $cx \in W_1 + W_2$. Therefore, $W_1 + W_2$ is closed under scalar multiplication.

Since $W_1 + W_2$ is non-empty and closed under addition and scalar multiplication, $W_1 + W_2$ is a subspace of V by the subspace criterion.

b)

Let $V = \mathbb{R}^2$. Let two subspaces of V be

$$W_1 = \{(x, 0) : x \in \mathbb{R}\}, \qquad W_2 = \{(0, y) : y \in \mathbb{R}\}.$$

Both W_1 and W_2 satisfy the subspace properties. For $W_1 = \{(x, 0) : x \in \mathbb{R}\}$: it contains $0 = (0, 0)$ (when $x = 0$); it is closed under addition since $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0) \in W_1$; and it is closed under scalar multiplication since $c(x, 0) = (cx, 0) \in W_1$ for any $c \in \mathbb{R}$.

Similarly, for $W_2 = \{(0, y) : y \in \mathbb{R}\}$: it contains $0 = (0, 0)$ (when $y = 0$); it is closed under addition since $(0, y_1) + (0, y_2) = (0, y_1 + y_2) \in W_2$; and it is closed under scalar multiplication since $c(0, y) = (0, cy) \in W_2$ for any $c \in \mathbb{R}$. Therefore, both are subspaces of $\mathbb{R}^2$.

$$W_1 \cup W_2 = \{(x, 0) : x \in \mathbb{R}\} \cup \{(0, y) : y \in \mathbb{R}\}$$

contains all vectors of the form $(x, 0)$ and all vectors of the form $(0, y)$. Let

$$u = (1, 0) \in W_1 \subseteq W_1 \cup W_2, \qquad v = (0, 1) \in W_2 \subseteq W_1 \cup W_2$$

Then

$$u + v = (1, 0) + (0, 1) = (1, 1)$$

The set W_1 contains only vectors where the second coordinate is zero, and the set W_2 contains only vectors where the first coordinate is zero. For the vector $(1, 1)$, the second coordinate is $1 \neq 0$, so $(1, 1) \notin W_1$, and the first coordinate is $1 \neq 0$, so $(1, 1) \notin W_2$. Hence $(1, 1)$ is in neither W_1 nor W_2, and therefore $(1, 1) \notin W_1 \cup W_2$.

Thus we have found $u, v \in W_1 \cup W_2$ such that $u + v \notin W_1 \cup W_2$. Therefore, $W_1 \cup W_2$ is not closed under addition, and so it is not a subspace of V.

7.

Let $U = \text{span}\{(1, 0, 0)\} = \{(t, 0, 0) : t \in \mathbb{R}\} \subset \mathbb{R}^3$.

Two vectors $u, v \in \mathbb{R}^3$ are congruent modulo U if $u \equiv v \pmod{U} \iff u - v \in U$.

The equivalence class (coset) of $v = (x, y, z)$ is $[v] = v + U = \{v + u : u \in U\} = \{(x + t,\ y,\ z) : t \in \mathbb{R}\}$.

The quotient space is the set of all cosets:$\mathbb{R}^3/U = \{[v] : v \in \mathbb{R}^3\}$.

On cosets we define

$$[v] + [w] = [\,v + w\,], \qquad c[v] = [\,cv\,].$$

If $v \equiv v' \pmod{U}$ and $w \equiv w' \pmod{U}$, then

$$[v + w] = [v' + w'] \quad \text{and} \quad [cv] = [cv'],$$

so addition and scalar multiplication are defined. With these operations, $\mathbb{R}^3/U$ is a vector space.

Two vectors (x_1, y_1, z_1) and (x_2, y_2, z_2) are in the same equivalence class if $(x_1, y_1, z_1) - (x_2, y_2, z_2) \in U$, i.e., of the form $(t, 0, 0)$ for some $t \in \mathbb{R}$. This forces $y_1 = y_2 \text{and} z_1 = z_2$. Thus, the congruence relation partitions $\mathbb{R}^3$ into disjoint cosets of the form for $v = (x, y, z)$:

$$[v] = \{(x + t, y, z) : t \in \mathbb{R}\}.$$

Taking $v = (0, 1, 0)$, the coset is $[(0, 1, 0)] = \{(t, 1, 0) : t \in \mathbb{R}\}$

Taking $v = (0, 0, 1)$, the coset is $[(0, 0, 1)] = \{(t, 0, 1) : t \in \mathbb{R}\}$

For a general $v = (x, y, z)$, the coset $[v]$ is determined by the pair (y, z), taking y multiples of $[(0, 1, 0)]$, and taking z multiples of $[(0, 0, 1)]$. Thus,

$$[(x, y, z)] = y[(0, 1, 0)] + z[(0, 0, 1)].$$

This shows that every coset in $\mathbb{R}^3/U$ is a linear combination of these two cosets. Since $[(0, 1, 0)]$ and $[(0, 0, 1)]$ are linearly independent, they form a basis.

$$\text{Basis: } \{[(0, 1, 0)], [(0, 0, 1)]\}, \qquad \dim(\mathbb{R}^3/U) = 2.$$