---

1. Let F be a field. Identify each of the following statements as true or false:

   (a) The zero vector space has no basis.
   - $\boxed{\text{False}}$: the empty set is a basis for the zero space.

   (b) The set $\{\mathbf{0}\}$ is a basis for the zero vector space.
   - $\boxed{\text{False}}$: the empty set is a basis for the zero space.

   (c) Every vector space has a finite basis.
   - $\boxed{\text{False}}$: there are infinite-dimensional vector spaces, like $F[x]$, which have no finite basis.

   (d) Every vector space has a unique basis.
   - $\boxed{\text{False}}$: most vector spaces (e.g., F^2) have many different bases.

   (e) Every subspace of a finite-dimensional vector space is finite-dimensional.
   - $\boxed{\text{True}}$: if W is a subspace of V then $\dim(W) \le \dim(V)$, so $\dim(W)$ is also finite.

   (f) Every subspace of an infinite-dimensional vector space is infinite-dimensional.
   - $\boxed{\text{False}}$: infinite-dimensional spaces have many finite-dimensional subspaces (e.g., the zero subspace).

   (g) If $V = M_{m\times n}(F)$, then $\dim_F V = mn$.
   - $\boxed{\text{True}}$: a basis is given by the mn matrices with a 1 in one entry and 0s elsewhere.

   (h) If $V = F[x]$, then $\dim_F V$ is undefined.
   - $\boxed{\text{False}}$: $\dim_F F[x]$ is infinite but perfectly well-defined.

   (i) If $V = P_n(F)$, then $\dim_F V = n$.
   - $\boxed{\text{False}}$: $\dim_F V = n + 1$, not n.

   (j) If $\dim(V) = 5$, then there exists a set of 5 vectors in V that span V but are not linearly independent.
   - $\boxed{\text{False}}$: any spanning set with exactly 5 vectors is necessarily also linearly independent.

   (k) If $\dim(V) = 5$, then a set of 4 vectors in V cannot span V.
   - $\boxed{\text{True}}$: any spanning set must contain a basis, which would require at least 5 vectors.

   (l) If $\dim(V) = 5$, then a set of 4 vectors in V cannot be linearly independent.
   - $\boxed{\text{False}}$: if we take the first 4 vectors of any basis, then they are linearly independent.

   (m) If $\dim(V) = 5$, then there is a unique subspace of V of dimension 0.
   - $\boxed{\text{True}}$: the only subspace of dimension 0 is the zero subspace.

   (n) If $\dim(V) = 5$, then there is a unique subspace of V of dimension 1.
   - $\boxed{\text{False}}$: if $\mathbf{v}$ is any nonzero vector, then $\text{span}(\mathbf{v})$ is 1-dimensional, and there are many such $\mathbf{v}$.

   (o) If $\dim(V) = 5$, then there is a unique subspace of V of dimension 5.
   - $\boxed{\text{True}}$: the only subspace of dimension 5 is V itself.

   (p) If V is infinite-dimensional, then any infinite linearly-independent subset is a basis.
   - $\boxed{\text{False}}$: just because the subset is infinite does not force it to span V. For example, if we take $V = F[x]$ and $S = \{1, x^2, x^4, x^6, \dots\}$, then S is a linearly independent set that does not span V.

---

2. For each set S of vectors in the given vector space V, determine whether or not S is a basis of V:

   (a) $S = \{\langle 1,2\rangle\}$ in $V = \mathbb{R}^2$.

   - $\boxed{\text{No}}$: This set does not span V. Alternatively, any basis of $\mathbb{R}^2$ must consist of 2 vectors.

   (b) $S = \{\langle 1,2\rangle, \langle 3,2\rangle\}$ in $V = \mathbb{R}^2$.

   - $\boxed{\text{Yes}}$: we can see that the two vectors in S are linearly independent, so since $\dim \mathrm{V} = 2$ that means S is a basis of V.

   (c) $S = \{\langle 1,2\rangle, \langle 3,2\rangle, \langle 1,1\rangle\}$ in $V = \mathbb{R}^2$.

   - $\boxed{\text{No}}$: This set is not linearly independent. Alternatively, any basis of $\mathbb{R}^2$ must consist of 2 vectors.

   (d) $S = \{\langle 1,2,4\rangle, \langle 3,2,1\rangle, \langle 1,1,1\rangle\}$ in $V = \mathbb{R}^3$.

   - $\boxed{\text{Yes}}$: we can check that the determinant $\begin{vmatrix} 1 & 3 & 1 \\ 2 & 2 & 1 \\ 3 & 1 & 1 \end{vmatrix} = 1$, and therefore the three given vectors are linearly independent and yield a basis of $\mathbb{R}^3$.

   (e) $S = \{1, 1+x, x+x^2\}$ in $V = P_2(\mathbb{C})$.

   - $\boxed{\text{Yes}}$: we have $a + bx + cx^2 = (a-b-c)(1) + b(1+x) + c(1+x^2)$ so the given set spans V, and if $a(1) + b(1+x) + c(x+x^2) = 0$ then $a+b = b+c = c = 0$ hence $a = b = c = 0$ so the set is linearly independent.

   (f) $S = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ in $V = M_{2\times 2}(\mathbb{Q})$.

   - $\boxed{\text{No}}$: This set is not linearly independent since $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. It also does not span V since for instance $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is not in the span of these matrices.

---

3. Find a basis for, and the dimension of, each of the following vector spaces:

   (a) The space of 3×3 symmetric matrices over $F = \mathbb{C}$.

   - Such a matrix has the form $M = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix} = a \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + b \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + c \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} +$ $d \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + e \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} + f \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.
   - Thus, $\boxed{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}}$ clearly gives a basis, so the dimension is therefore $\boxed{6}$.

   (b) The row space, column space, and nullspace of $M = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \end{bmatrix}$ over $\mathbb{R}$.

   - Row-reducing M (immediately) yields the reduced row-echelon form $E = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.
   - The row space has a basis given by the row $\boxed{\langle 1,1,1\rangle}$, so the row space has dimension $\boxed{1}$.

- Since there is a pivot in column 1, the column space has basis $\boxed{\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}}$, and also has dimension $\boxed{1}$.

- For the nullspace, solving the linear system $E\mathbf{x} = \mathbf{0}$ (with variables x_1, x_2, x_3, x_4, x_5 and free parameters a, b) yields the solution set $\langle x_1, x_2, x_3 \rangle = a\langle -1, 1, 0\rangle + b\langle -1, 0, 1\rangle$, so the nullspace has a basis $\boxed{\langle -1, 1, 0\rangle, \langle -1, 0, 1\rangle}$ and dimension $\boxed{2}$.

(c) The vectors in $\mathbb{Q}^5$ of the form $\langle a, b, c, d, e\rangle$ with $e = a + b$ and $b = c = d$, over $\mathbb{Q}$.

- Such vectors have the form $\langle a, b, b, b, a + b\rangle = a\langle 1, 0, 0, 0, 1\rangle + b\langle 0, 1, 1, 1, 1\rangle$.
- Clearly, the set $\boxed{\langle 1, 0, 0, 0, 1\rangle, \langle 0, 1, 1, 1, 1\rangle}$ is a basis, so the space has dimension $\boxed{2}$.

(d) The row space, column space, and nullspace of $M = \begin{bmatrix} 1 & 3 & -2 & -6 & 8 \\ 2 & -1 & 2 & 8 & 1 \\ -1 & 1 & 1 & -3 & 3 \end{bmatrix}$ over $\mathbb{C}$.

- Row-reducing M (eventually) yields the reduced row-echelon form $E = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & -2 & 3 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$.

- The row space has a basis given by the rows $\boxed{\langle 1, 0, 0, 2, 1\rangle, \langle 0, 1, 0, -2, 3\rangle, \langle 0, 0, 1, 1, 1\rangle}$, so the row space has dimension $\boxed{3}$.

- Since there are pivots in columns 1, 2, and 3, the column space has a basis $\boxed{\begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 3 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ 2 \\ 1 \end{bmatrix}}$, and also has dimension $\boxed{3}$.
- For the nullspace, solving the linear system $E\mathbf{x} = \mathbf{0}$ (with variables x_1, x_2, x_3, x_4, x_5 and free parameters a, b) yields the solution set $\langle x_1, x_2, x_3, x_4, x_5\rangle = a\langle -1, -3, -1, 0, 1\rangle + b\langle -2, 2, -1, 1, 0\rangle$, so the nullspace has a basis $\boxed{\langle -1, -3, -1, 0, 1\rangle, \langle -2, 2, -1, 1, 0\rangle}$ and dimension $\boxed{2}$.

(e) The polynomials $p(x)$ in $P_4(\mathbb{R})$ such that $p(1) = 0$.

- Polynomials in $P_4(\mathbb{R})$ have the form $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$.
- Then the condition $p(1) = 0$ requires $a_0 + a_1 + a_2 + a_3 + a_4 = 0$, which is equivalent to $a_0 = -a_1 - a_2 - a_3 - a_4$.
- Hence the desired polynomials are of the form $(-a_1 - a_2 - a_3 - a_4) + a_1x + a_2x^2 + a_3x^3 + a_4x^4 = a_1(-1 + x) + a_2(-1 + x^2) + a_3(-1 + x^3) + a_4(-1 + x^4)$.
- Hence we obtain a basis $\boxed{-1 + x, -1 + x^2, -1 + x^3, -1 + x^4}$ so the space has dimension $\boxed{4}$.
- Alternatively, one could observe that $p(1) = 0$ requires the polynomial to be divisible by $x - 1$, which yields the basis $\boxed{x - 1, x(x - 1), x^2(x - 1), x^3(x - 1)}$.

(f) The matrices A in $M_{2\times 2}(\mathbb{Q})$ such that $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

- If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then the given condition requires $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ 2a + 2c & 2b + 2d \end{bmatrix}$, which yields $a = -c$ and $b = -d$.
- Thus the matrices are of the form $\begin{bmatrix} -c & -d \\ c & d \end{bmatrix} = c\begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix}$. Hence we obtain a basis $\boxed{\begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix}}$ and the space has dimension $\boxed{2}$.

---

4. Let W be a vector space. Recall that if A and B are two subspaces of W then their sum is the set $A + B = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in A \text{ and } \mathbf{b} \in B\}$.

   (a) Suppose that $A \cap B = \{\mathbf{0}\}$. If α is a basis for A and β is a basis for B, prove that α and β are disjoint and that $\alpha \cup \beta$ is a basis for $A + B$.

   - First, we show that $\alpha \cup \beta$ spans $A + B$: for any $\mathbf{a} + \mathbf{b} \in A + B$, since $\mathbf{a} \in A$ we can write $\mathbf{a} = a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k$ for some $\mathbf{a}_i \in \alpha$ and likewise since $\mathbf{b} \in B$ we can write $\mathbf{b} = b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l$ for some $\mathbf{b}_i \in \beta$.
   - Then $\mathbf{a} + \mathbf{b} = a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k + b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l$ is in $\text{span}(\alpha \cup \beta)$, as required.
   - Now suppose we had a dependence $a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k + b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l = \mathbf{0}$.
   - Then rearranging gives $a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k = -(b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l)$. Since the left-hand side is a vector in A and the right-hand side is a vector in B, the common expression is an element in $A \cap B$.
   - But then since $A \cap B = \{\mathbf{0}\}$, we have $a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k = \mathbf{0} = -(b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l)$.
   - Then since α and β are both linearly independent, we have $a_1 = \cdots = a_k = 0$ and $b_1 = \cdots = b_l = 0$. Hence $\alpha \cup \beta$ is linearly independent, as claimed.

   (b) Now suppose that α is a basis for A and β is a basis for B. If $\alpha \cup \beta$ is a basis for $A + B$ and α and β are disjoint, prove that $A \cap B = \{\mathbf{0}\}$.

   - Suppose that $\mathbf{v} \in A \cap B$. Then since $\mathbf{v} \in A$ we may write $\mathbf{v} = a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k$ for some $\mathbf{a}_i \in \alpha$, and since $\mathbf{v} \in B$ we may also write $\mathbf{v} = b_1\mathbf{b}_1 + \cdots + b_l\mathbf{b}_l$ for some $\mathbf{b}_i \in \beta$.
   - Then subtracting the expressions yields $a_1\mathbf{a}_1 + \cdots + a_k\mathbf{a}_k - b_1\mathbf{b}_1 - \cdots - b_l\mathbf{b}_l = \mathbf{0}$.
   - But since $\alpha \cup \beta$ is a basis and α, β are linearly independent, all of the scalar coefficients must be zero. Then $\mathbf{v} = 0\mathbf{a}_1 + \cdots + 0\mathbf{a}_k = \mathbf{0}$, and so $A \cap B = \{\mathbf{0}\}$.

The situation in (a)-(b) is very important and arises often. Explicitly, if A and B are two subspaces of W such that $A + B = W$ and $A \cap B = \{\mathbf{0}\}$ is the trivial subspace, we write $W = A \oplus B$ and call W the (internal) direct sum of A and B. (The idea is that we may "decompose" W into two independent pieces A and B.)

   (c) Show that $\mathbb{R}^2$ is the direct sum of the subspaces given by the x-axis and the y-axis, and is also the direct sum of the subspaces given by the x-axis and the line $y = 3x$.

   - First for $X = \{\langle x, 0\rangle\}$ and $Y = \{\langle 0, y\rangle\}$, since $\langle x, y\rangle = \langle x, 0\rangle + \langle 0, y\rangle$, we have $\mathbb{R}^2 = X + Y$. Furthermore, $X \cap Y = \{\langle 0, 0\rangle\}$ so the sum is a direct sum.
   - Second with $Z = \{\langle y/3, y\rangle\}$, since $\langle x, y\rangle = \langle x - y/3, 0\rangle + \langle y/3, y\rangle$, we have $\mathbb{R}^2 = X + Z$. Furthermore, $X \cap Z = \{\langle 0, 0\rangle\}$ so the sum is a direct sum.

   (d) Prove that $W = A \oplus B$ if and only if every vector $\mathbf{w} \in W$ can be written uniquely in the form $\mathbf{w} = \mathbf{a} + \mathbf{b}$ where $\mathbf{a} \in A$ and $\mathbf{b} \in B$.

   - First suppose that every vector $\mathbf{w} \in W$ can be written uniquely in the form $\mathbf{w} = \mathbf{a} + \mathbf{b}$ where $\mathbf{a} \in A$ and $\mathbf{b} \in B$. Then clearly $W = A + B$.
   - Furthermore, for any $\mathbf{w} \in A \cap B$, we may write $\mathbf{w} = \mathbf{w} + \mathbf{0} = \mathbf{0} + \mathbf{w}$. Hence by uniqueness, we must have $\mathbf{w} = \mathbf{0}$, and therefore $A \cap B = \{\mathbf{0}\}$. Hence $W = A \oplus B$ as required.
   - Conversely, suppose $W = A \oplus B$. Then every vector $\mathbf{w} \in W$ can be written as $\mathbf{a} + \mathbf{b}$, so we need only consider uniqueness: if $\mathbf{w} = \mathbf{a} + \mathbf{b} = \mathbf{a}' + \mathbf{b}'$, then subtracting yields $\mathbf{a} - \mathbf{a}' = \mathbf{b}' - \mathbf{b}$.
   - Since the vector $\mathbf{a} - \mathbf{a}' = \mathbf{b}' - \mathbf{b}$ is in both A and B, it must be the zero vector: hence $\mathbf{a} = \mathbf{a}'$ and $\mathbf{b} = \mathbf{b}'$, so the representation of $\mathbf{w}$ is unique as required.

   (e) Show that if $W = A \oplus B$ then $\dim(W) = \dim(A) + \dim(B)$. Show using an explicit counterexample that the converse statement need not hold.

   - The first part is simply a rewriting of part (b). For the second part, if for example we take $W = \mathbb{R}^2$ with $A = B = \text{span}(\langle 1, 0\rangle)$, then the dimensions sum correctly, but $A + B = A = \text{span}(\langle 1, 0\rangle) \neq W$.

---

5. Let V be a vector space such that $\dim_{\mathbb{C}} V = n$. Prove that if V is now considered a vector space over $\mathbb{R}$ (using the same addition and scalar multiplication), then $\dim_{\mathbb{R}} V = 2n$.

   - Suppose that $\dim_{\mathbb{C}} V = n$. Choose a basis $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ for V, as a complex vector space. We claim that the set $S' = \{\mathbf{v}_1, i\mathbf{v}_1, \mathbf{v}_2, i\mathbf{v}_2, \dots, \mathbf{v}_n, i\mathbf{v}_n\}$ is a basis for V considered as a real vector space, which would immediately imply that $\dim_{\mathbb{R}} V = 2n$.
   - S' spans V: Let $\mathbf{x}$ be a vector in V. By the assumption that S spans V, there exist (complex) scalars with $\mathbf{x} = (a_1 + b_1 i)\mathbf{v}_1 + \cdots + (a_n + b_n i)\mathbf{v}_n$. But by rearranging, we see that $\mathbf{x} = a_1\mathbf{v}_1 + b_1(i\mathbf{v}_1) + \cdots + a_n\mathbf{v}_n + b_n(i\mathbf{v}_n)$, meaning that $\mathbf{x}$ is a linear combination of the vectors in S' using real coefficients, as required.
   - S' is linearly independent: Suppose there exist real numbers a_i, b_i such that $\mathbf{0} = a_1\mathbf{v}_1 + b_1(i\mathbf{v}_1) + \cdots + a_n\mathbf{v}_n + b_n(i\mathbf{v}_n)$. By rearranging this yields $\mathbf{0} = (a_1 + b_1 i)\mathbf{v}_1 + \cdots + (a_n + b_n i)\mathbf{v}_n$. But by the hypothesis that S is linearly independent, all of these (complex) coefficients must be zero.

---

6. Let F be a finite field with q elements. The goal of this problem is to count the invertible matrices in $M_{n\times n}(F)$.

   (a) Suppose W is a k-dimensional subspace of F^n. Show that W contains exactly q^k vectors.

   - Choose a basis $\mathbf{w}_1, \dots, \mathbf{w}_k$ for W. Then every vector in W may be written as a linear combination $a_1\mathbf{w}_1 + \cdots + a_k\mathbf{w}_k$ for unique scalars $a_1, \dots, a_k$.
   - Since there are q choices for each scalar a_i for each $1 \le i \le k$, there are q^k total choices for the coefficients and thus q^k possible vectors.

   (b) Show that the number of invertible $n \times n$ matrices in $M_{n\times n}(F)$ is equal to the number of ordered lists $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_n$ of n linearly independent vectors from F^n.

   - From our discussion of bases of F^n, we know that a list $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_n$ of n vectors in F^n is linearly independent if and only if it is a basis.
   - Also from our discussion, we know that the matrix whose columns are the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_n$ is invertible if and only if the columns are linearly independent.
   - Thus, by combining these two facts, we see that the number of invertible $n \times n$ matrices in $M_{n\times n}(F)$ is equal to the number of ordered lists $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_n$ of n linearly independent vectors from F^n.

   (c) For any integer $0 \le k \le n$, show that there are exactly $(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})$ ordered lists $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ of k linearly independent vectors from F^n. [Hint: Count the number of ways to choose the vector $\mathbf{v}_{k+1}$ not in $\text{span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$.]

   - Since subsets of linearly independent sets are linearly independent, we see that each of $\{\mathbf{v}_1\}$, $\{\mathbf{v}_1, \mathbf{v}_2\}$, ... , $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_k\}$ is linearly independent.
   - So we simply need to count the number of selections of the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ (in order) where each of the sets $\{\mathbf{v}_1\}$, $\{\mathbf{v}_1, \mathbf{v}_2\}$, ... , $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_k\}$ is linearly independent.
   - If we have chosen $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}$, then $\mathbf{v}_i$ may be any vector not in $\text{span}(\mathbf{v}_1, \dots, \mathbf{v}_{i-1})$. By part (a), there are q^{i-1} vectors in this span, so there are $q^n - q^{i-1}$ possible choices for $\mathbf{v}_i$.
   - Multiplying, we obtain the total number of lists as $(q^n - 1)(q^n - q)\cdots(q^n - q^k)$, as required.

   (d) Deduce that the number of invertible $n \times n$ matrices in $M_{n\times n}(F)$ is equal to $(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})\cdots(q^n - q^{n-1})$. In particular, find the number of invertible 5×5 matrices over the field $\mathbb{F}_2$.

   - The first result follows immediately from setting $k = n$ in part (c).
   - For the second part, taking $n = 5$ and $q = 2$ yields the total $31 \cdot 30 \cdot 28 \cdot 24 \cdot 16 = 9999360$.

---

7. [Challenge] Zorn's lemma states that if $\mathcal{F}$ is a nonempty partially-ordered set in which every chain has an upper bound (i.e., an element $U \in \mathcal{F}$ such that $X \leq U$ for all X in the chain), then $\mathcal{F}$ contains a maximal element (i.e., an element $M \in \mathcal{F}$ such that if $M \leq Y$ for some $Y \in \mathcal{F}$, then in fact $Y = M$). The goal of this problem is to use Zorn's lemma to prove that any linearly independent set can be extended to a basis and that any spanning set contains a basis.

   (a) Suppose that S is a maximal linearly-independent subset of a vector space V (this means that if T is any linearly-independent subset of V containing S, then in fact $T = S$). Prove that S is a basis of V.

   - Suppose S does not span V: then there exists a vector $\mathbf{w} \in V$ such that $\mathbf{w} \notin \operatorname{span}(S)$.
   - Then by our results on linear independence and span, the set $S \cup \{\mathbf{w}\}$ would also be linearly independent. But this contradicts the assumption that S is maximal, since $T = S \cup \{\mathbf{w}\}$ would be a linearly independent set containing S with $T \neq S$.
   - This is impossible, so there cannot exist any vector $\mathbf{w} \in V$ with $\mathbf{w} \notin \operatorname{span}(S)$. Hence S spans V, so since it is linearly independent, it is a basis.

   (b) Suppose $\mathcal{C}$ is a chain of linearly independent subsets of V (i.e., a collection of linearly independent subsets with the property that $A \subseteq B$ or $B \subseteq A$ for any $A, B \in \mathcal{C}$). Show that $U = \bigcup_{A \in \mathcal{C}} A$ is also linearly independent. [Hint: A linear dependence can only involve finitely many vectors.]

   - Suppose that there exist vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ in U and scalars $a_1, \ldots, a_k$ such that $a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k = \mathbf{0}$.
   - Suppose the vectors $\mathbf{v}_i$ lie in the subsets $A_i \in \mathcal{C}$. Then since $\mathcal{C}$ is a chain, since $A_i \subseteq A_j$ for each pair (i, j), by a trivial induction we see that one of the A_i must contain all of the others, hence contains all of the vectors $\mathbf{v}_i$.
   - But since this subset A_i is linearly independent, we must have $a_1 = \cdots = a_k = 0$, and so $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are linearly independent.
   - Thus, since every finite subset of U is linearly independent, U is linearly independent.

   (c) Prove that every linearly independent subset of V can be extended to a basis.

   - Let $\mathcal{F}$ be the collection of all linearly-independent subsets of V containing the given set, partially ordered by inclusion. Note that $\mathcal{F}$ is not empty since it contains the original linearly independent set.
   - By part (b), if $\mathcal{C}$ is any chain in $\mathcal{F}$ contains a maximal element. Such a maximal element is a maximal linearly-independent subset of V, which by part (a) is a basis of V.

   (d) Suppose that S is a minimal spanning set of a vector space V (this means that if T is any subset of S that spans V, then in fact $T = S$). Prove that S is a basis of V.

   - Suppose S is not a basis of V: then necessarily S must be linearly dependent, so there exists vector $\mathbf{w} \in S$ such that $\mathbf{w} \in \operatorname{span}(S')$ where $S' = S \backslash \{\mathbf{w}\}$.
   - Then by our results on span, we have $\operatorname{span}(S') = \operatorname{span}(S) = V$, but S' is a proper subset of S, contradicting minimality. Hence S must be linearly independent hence a basis.

   (e) Let $V = \mathbb{Q}$ with scalar field $F = \mathbb{Q}$ and let $S_n = \{n, n+1, n+2, \ldots\}$ for each positive integer n. Show that each set S_n is a spanning set and that the sets S_n form a chain, but that the intersection $\bigcap_{n=1}^{\infty} S_n$ is not a spanning set.

   - Since V is 1-dimensional, any set containing something other than 0 automatically spans V. Since each S_n is infinite, they all span V, and clearly $S_1 \supseteq S_2 \supseteq S_3 \supseteq \cdots$ so they form a chain.
   - However, the intersection $\bigcap_{n=1}^{\infty} S_n$ is empty, because any positive integer k is not in S_{k+1}, and so the intersection is not a spanning set.

Remark: It is natural to try to use Zorn's lemma to prove that a minimal spanning set must exist, in analogy to (b). This does not work, as (e) shows: the intersection of a chain of spanning sets need not span V!
