2

Matroidal Properties

Certain collections of vectors have special properties. This chapter develops two of these notions: linear independence and spanning. Collections with both properties are exceptionally useful.

2.0 Spanning and Linear Independence

WHAT FEATURES DISTINGUISH COLLECTIONS OF VECTORS? Based on our study of vectors in $\mathbb{K}^n$, we already recognize the following two definitions as crucial in the development of linear algebra.

2.0.0 Definition. Let V be a $\mathbb{K}$-vector space and let n be a nonnegative integer. The ***span*** of the vectors $v_1, v_2, \dots, v_n$ in V is the set of all their linear combinations:

$$\operatorname{Span}(v_1, v_2, \dots, v_n) := \{c_1\, v_2 + c_2\, v_2 + \cdots + c_n\, v_n \in V \mid c_1, c_2, \dots, c_n \in \mathbb{K}\}\,.$$

Since the empty sum of vectors equals the additive identity, the zero subspace is $\operatorname{Span}(\varnothing) = \{\mathbf{0}\}$.

2.0.1 Remark. The subspace test [1.2.0] shows that $\operatorname{Span}(v_1, v_2, \dots, v_n)$ is the smallest linear subspace containing the vectors $v_1, v_2, \dots, v_n$.

2.0.2 Problem. Determine if the polynomial $-t^3 + 2t^2 + 3t + 3$ in $\mathbb{Q}[t]$ lies in the linear subspace $\operatorname{Span}(t^3 + t^2 + t + 1, t^2 + t + 1, t + 1) \subset \mathbb{Q}[t]$.

Solution. From the equation

$$-t^3 + 2t^2 + 3t + 3 = (-1)(t^3 + t^2 + t + 1) + (3)(t^2 + t + 1) + (1)(t + 1)\,,$$

we deduce that the polynomial $-t^3 + 2t^2 + 3t + 3$ lies in the linear subspace $\operatorname{Span}(t^3 + t^2 + t + 1, t^2 + t + 1, t + 1)$. □

2.0.3 Definition. A finite set $\{v_1, v_2, \dots, v_n\}$ of vectors is ***linearly independent*** if the equation $c_1\, v_1 + c_2\, v_2 + \cdots + c_n\, v_n = \mathbf{0}$, where $c_1, c_2, \dots, c_n$ are scalars, implies that $c_1 = c_2 = \cdots = c_n = 0$. Conversely, a set of vectors is ***linearly dependent*** if one vector can be expressed as a linear combination of the other vectors.

When there is a nonzero scalar c_k, for some $1 \leqslant k \leqslant n$, rearranging the linear relation confirms that the vector v_k is a linear combination of the other vectors.

2.0.4 Problem. Verify that the functions $\sin^2(x), \cos^2(x), \cos(2x)$ are linearly dependent in the $\mathbb{R}$-vector space $\mathbb{R}^{\mathbb{R}}$.

Solution. The trigonometric identity $\cos(2x) = \cos^2(x) - \sin^2(x)$ demonstrates that these functions are linearly dependent in $\mathbb{R}^{\mathbb{R}}$. Equivalently, a nonzero linear combination of these functions equals zero: $(1)\, \sin^2(x) + (-1)\, \cos^2(x) + (1)\, \cos(2x) = 0$. □

2.0.5 Proposition (Monomial independence). *Let n be a nonnegative integer. For any subset $\mathcal{X} \subseteq \mathbb{K}$ containing more than n distinct scalars, the monomial functions $f_k(t) := t^k$, for all $0 \leqslant k \leqslant n$, are linearly independent in the $\mathbb{K}$-vector space $\mathbb{K}^{\mathcal{X}}$.*

Proof. Suppose that the scalars $c_0, c_1, \dots, c_n$ in $\mathbb{K}$ satisfy

$$c_0\, f_0(t) + c_1\, f_1(t) + \cdots + c_n\, f_n(t) = c_0\, 1 + c_1\, t + \cdots + c_n\, t^n = 0\,.$$

Evaluating at $n+1$ distinct points $x_0, x_1, \dots, x_n \in \mathcal{X}$ gives

$$\left\{ \begin{aligned} c_0 + c_1\, x_0 + c_2\, x_0^2 + \cdots + c_n\, x_0^n &= 0 \\ c_0 + c_1\, x_1 + c_2\, x_1^2 + \cdots + c_n\, x_1^n &= 0 \\ &\vdots \\ c_0 + c_1\, x_n + c_2\, x_n^2 + \cdots + c_n\, x_n^n &= 0 \end{aligned} \right\} \Leftrightarrow \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{bmatrix} \begin{bmatrix} c_0 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since the coefficient matrix is the transpose of the Vandermonde matrix and scalars $x_0, x_1, \dots, x_n$ are distinct, the determinant of the coefficient matrix is nonzero. Hence, the coefficient matrix is invertible. It follows that $c_0 = c_1 = \cdots = c_n = 0$ is the unique solution to this homogeneous linear system, which shows that the functions $f_0(t), f_1(t), \dots, f_n(t)$ are linearly independent. □

2.0.6 Problem. Determine whether the three polynomials

$$t^3 + 2t^2\,, \qquad -t^2 + 3t + 1\,, \qquad t^3 - t^2 + 2t - 1\,,$$

are linearly independent in $\mathbb{Q}[t]$.

Solution. Suppose that there exists scalars c_1, c_2, c_2 in $\mathbb{Q}$ such that

$$\begin{aligned} 0 &= c_1(t^3 + 2t^2) + c_2(-t^2 + 3t + 1) + c_3(t^3 - t^2 + 2t - 1) \\ &= (c_1 + c_3)t^3 + (2c_1 - c_2 - c_3)t^2 + (3c_2 + 2c_3)t^1 + (c_2 - c_3)t^0\,. \end{aligned}$$

Since the monomials are linear independent, we obtain

$$\left\{ \begin{aligned} c_1 + c_3 &= 0 \\ 2c_1 - c_2 - c_3 &= 0 \\ 3c_2 + 2c_3 &= 0 \\ c_2 - c_3 &= 0 \end{aligned} \right\} \Rightarrow \begin{bmatrix} 1 & 0 & 1 \\ 2 & -1 & -1 \\ 0 & 3 & 2 \\ 0 & 1 & -1 \end{bmatrix} \xrightarrow{r_2 \mapsto r_2 - 2r_1} \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & -3 \\ 0 & 3 & 2 \\ 0 & 1 & -1 \end{bmatrix} \xrightarrow[r_4 \mapsto r_4 + \ r_2]{r_3 \mapsto r_3 + 3r_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & -3 \\ 0 & 0 & 7 \\ 0 & 0 & -4 \end{bmatrix}$$

$$\xrightarrow[r_3 \mapsto 7^{-1} r_3]{r_2 \mapsto -r_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & -4 \end{bmatrix} \xrightarrow[r_4 \mapsto r_4 + 4r_3]{\substack{r_1 \mapsto r_1 - \ r_3 \\ r_2 \mapsto r_2 - 3r_3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Hence, we conclude that $c_1 = c_2 = c_3 = 0$ and the polynomials are linear independent. □

Certain periodic functions provide another example of linearly independent functions arising in approximation theory and the study of Fourier series.

2.0.7 Proposition. *For any nonnegative integer n, the functions*

$$1, \cos(z), \sin(z), \cos(2z), \sin(2z), \dots, \cos(nz), \sin(nz)$$

are linearly independent in the $\mathbb{C}$-vector space $\mathbb{C}^{\mathbb{C}}$.

Proof. Suppose that there are scalars $c_{-n}, \dots, c_{-1}, c_0, c_1, \dots, c_n$ such that $c_0\, 1 + \sum_{k=1}^{n} c_{-k} \cos(kz) + \sum_{k=1}^{n} c_k \sin(kz) = 0$. By definition, we have $\cos(kz) := \frac{1}{2}(e^{\mathrm{i}\,k\,z} + e^{-\mathrm{i}\,k\,z})$ and $\sin(kz) := \frac{1}{2\mathrm{i}}(e^{\mathrm{i}\,k\,z} - e^{-\mathrm{i}\,k\,z})$, so

$$c_0\, e^{\mathrm{i}\,0} + \sum_{k=1}^{n} \tfrac{1}{2}(c_{-k} + \mathrm{i}\, c_k)\, e^{-\mathrm{i}\,k\,z} + \sum_{k=1}^{n} \tfrac{1}{2}(c_{-k} - \mathrm{i}\, c_k)\, e^{\mathrm{i}\,k\,z} = 0\,.$$

For all $1 \leqslant k \leqslant n$, set $d_{-k} := \frac{1}{2}(c_{-k} + \mathrm{i}\, c_k)$, $d_k := \frac{1}{2}(c_{-k} - \mathrm{i}\, c_k)$, and $d_0 := c_0$ to obtain the equation

$$d_{-n}\, e^{-\mathrm{i}\,n\,z} + d_{-n+1}\, e^{-\mathrm{i}\,(n-1)\,z} + \cdots + d_n\, e^{\mathrm{i}nz} = 0\,.$$

Let $w := e^{\mathrm{i}\,z}$. It follows that $w^k = e^{\mathrm{i}\,k\,z}$ and

$$d_{-n}\, w^{-n} + d_{-n+1}\, w^{-n+1} + \cdots + d_n\, w^n = 0\,.$$

Multiplying by w^n gives $d_{-n} + d_{-n+1}\, w + \cdots + d_n\, w^{2n} = 0$. Since $w \neq 0$ and the monomial functions $w \mapsto w^j$, for all $0 \leqslant j \leqslant 2n$, are linearly independent [2.0.6], we have $d_{-n} = d_{-n+1} = \cdots = d_n = 0$. From the equations $c_{-k} = d_{-k} + d_k$, $c_0 = d_0$, and $c_k = \mathrm{i}\,(d_k - d_{-k})$ for all $1 \leqslant k \leqslant n$, we see that $c_{-n} = c_{-n+1} = \cdots = c_n = 0$. Thus, the set $\{1, \cos(z), \sin(z), \cos(2z), \sin(2z), \dots, \cos(nz), \sin(nz)\}$ is linearly independent in the complex vector space $\mathbb{C}^{\mathbb{C}}$. □

2.0.8 Definition. For any nonnegative integer n, the ***linear space of trigonometric polynomials*** of degree at most n is the linear subspace of $\mathbb{C}^{\mathbb{C}}$ with basis $1, \cos(z), \sin(z), \cos(2z), \sin(2z), \dots, \cos(nz), \sin(nz)$.

Exercises

2.0.9 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

i. The span of any collection of vectors forms a linear subspace.
ii. The zero function is never apart of a linearly independent collection of functions.
iii. The functions $\cos^3(\theta), \cos(3\theta), \cos(\theta)$ are linearly independent.
iv. Any subset of a linearly independent collection of vectors is also linearly independent.
v. Any subset of a linearly dependent collection of vectors is also linearly dependent.
vi. The empty set spans a linear subspace.
vii. The empty set of vectors is linearly independent.

2.0.10 Problem. Consider functions $f_1, f_2, \dots, f_n$ in $C^{n-1}(\mathbb{R})$, the $\mathbb{R}$-vectors space of all real-valued functions on the real line that have continuous first $(n-1)$ derivatives. The determinant

$$\mathrm{W}(x) := \begin{bmatrix} f_1(x) & f_2(x) & \cdots & f_n(x) \\ f_1'(x) & f_2'(x) & \cdots & f_n'(x) \\ f_1''(x) & f_2''(x) & \cdots & f_n''(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)}(x) & f_2^{(n-1)}(x) & \cdots & f_n^{(n-1)}(x) \end{bmatrix}$$

is called the ***Wronskian***. If there exists a point $x \in \mathbb{R}$ such that the Wronskian is nonzero, then show that the functions $f_1, f_2, \dots, f_n$ are linearly independent.

2.1 Dimension

HOW DO WE MEASURE THE SIZE OF A VECTOR SPACE? Combining our two favourite features for a collection of vectors, we obtain the following fundamental concept.

2.1.0 Definition. A ***basis*** of a vector space is a linearly-independent spanning set of vectors.

2.1.1 Remark. Most popular vector spaces have a canonical basis. For instance, the coordinate space $\mathbb{K}^n$ has the standard basis $\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n$, the matrix space $\mathbb{K}^{m \times n}$ has the matrix units $\mathbf{E}_{j,k}$ for all $1 \leqslant j \leqslant m$ and all $1 \leqslant k \leqslant n$, and the space $\mathbb{K}[t]$ has the monomials $1, t, t^2, \dots$.

We start with a powerful way of exchanging linearly independent vectors with elements in a spanning set to obtain a new spanning set.

2.1.2 Lemma (Exchange)**.** *Let V be a $\mathbb{K}$-vector space. Fix nonnegative integers m and n. Given linearly independent vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m$ in V and vectors $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n$ satisfying* $\operatorname{Span}(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n) = V$, *we have the inequality $m \leqslant n$ and, after reindexing the vectors $\boldsymbol{w}_k$ if necessary,*

Ernst Steinitz first stated and proved this lemma in 1913.

$$\operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_m, \boldsymbol{w}_{m+1}, \boldsymbol{w}_{m+2}, \dots, \boldsymbol{w}_n) = V\,.$$

Inductive proof. Up to reindexing the vectors $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n$, we claim that $\operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k, \boldsymbol{w}_{k+1}, \boldsymbol{w}_{k+2}, \dots, \boldsymbol{w}_n) = V$ for all $0 \leqslant k \leqslant m$. We proceed by induction on k. Since $\operatorname{Span}(\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_n) = V$, the base case $k = 0$ holds. As the induction hypothesis, assume that the claim holds for some index k satisfying $0 \leqslant k < m$. Since $\boldsymbol{v}_{k+1}$ lies in $V = \operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_k, \boldsymbol{w}_{k+1}, \boldsymbol{w}_{k+2}, \dots, \boldsymbol{w}_n)$, there exists scalars $c_1, c_2, \dots, c_n$ in $\mathbb{K}$ such that

$$\boldsymbol{v}_{k+1} = c_1\,\boldsymbol{v}_1 + c_2\,\boldsymbol{v}_2 + \cdots + c_k\,\boldsymbol{v}_k + c_{k+1}\,\boldsymbol{w}_{k+1} + c_{k+2}\,\boldsymbol{w}_{k+2} + \cdots + c_n\,\boldsymbol{w}_n\,.$$

At least one of the scalars $c_{k+1}, c_{k+2}, \dots, c_n$ must be nonzero, otherwise this equation would contradict the linear independence of the vectors $v_1, v_2, \dots, v_n$. It follows that $k < n$. By reindexing the vectors $w_{k+1}, w_{k+2}, \dots, w_n$ if necessary, we may assume that $c_{k+1} \neq 0$, so

$$w_{k+1} = \tfrac{1}{c_{k+1}} \left(v_{k+1} - c_1\, v_1 - c_2\, v_2 - \cdots - c_k\, v_k - c_{k+2}\, w_{k+2} - c_{k+3}\, w_{k+3} - \cdots - c_n\, w_n \right),$$

and $w_{k+1} \in \operatorname{Span}(v_1, v_2, \dots, v_{k+1}, w_{k+2}, w_{k+3}, \dots, w_n)$. We see that

$$\operatorname{Span}(v_1, v_2, \dots, v_{k+1}, w_{k+2}, w_{k+3}, \dots, w_n) \supseteq \operatorname{Span}(v_1, v_2, \dots, v_k, w_{k+1}, w_{k+2}, \dots, w_n) = V$$

completing the induction step. The case $k = m$ is the lemma. □

As with linear subspaces in $\mathbb{K}^n$, the number of vectors in a basis for a $\mathbb{K}$-vector space is a numerical invariant of the vector space.

2.1.3 Theorem (Equicardinality of bases)**.** *Any two bases of a vector space have the same number of vectors.*

Proof. Consider a $\mathbb{K}$-vector space V with two bases $v_1, v_2, \dots, v_m$ and $w_1, w_2, \dots, w_n$. Since $\{v_1, v_2, \dots, v_m\}$ is linearly independent and $V = \operatorname{Span}(w_1, w_2, \dots, w_n)$, the exchange lemma [2.1.2] implies that $m \leqslant n$. On the other hand, the set $\{w_1, w_2, \dots, w_n\}$ is also linearly independent and $V = \operatorname{Span}(v_1, v_2, \dots, v_m)$, so the exchange lemma [2.1.2] implies that $n \leqslant m$. We conclude that $m = n$ and any two bases of V have the same number of vectors. □

2.1.4 Definition. The ***dimension*** of a $\mathbb{K}$-vector space V is the number of vectors in any basis of V. It is denoted by $\dim(V)$.

2.1.5 Remark. For all nonnegative integers m and n, the canonical bases establish that $\dim(\mathbb{K}^n) = n$, $\dim(\mathbb{K}^{m \times n}) = mn$, $\dim(\mathbb{K}[t]) = \infty$, and the linear space of trigonometric polynomials of degree at most n has dimension $2n + 1$.

Any 0-dimensional vector subspace must have the empty set as a basis. Thus, a 0-dimensional vector subspace contains one vector: the additive identity $\mathbf{0}$.

Although the vector space of polynomials is infinite-dimensional, it has some natural finite-dimensional linear subspaces.

2.1.6 Definition. The ***degree*** of a nonzero polynomial is the largest integer j such that coefficient of the monomial t^j is nonzero.

2.1.7 Proposition (Polynomials of bounded degree)**.** *Let n be a nonnegative integer. The set $\mathbb{K}[t]_{\leqslant n}$, consisting of the zero polynomial and all polynomials of degree at most n, is a linear subspace of $\mathbb{K}[t]$. Moreover, we have* $\dim(\mathbb{K}[t]_{\leqslant n}) = n + 1$.

Proof. The zero polynomial belongs to the given set, so $\mathbb{K}[t]_{\leqslant n} \neq \varnothing$. Given polynomials $f, g \in \mathbb{K}[t]_{\leqslant n}$ and scalars $c, d \in \mathbb{K}$, it follows that $f = a_0 + a_1\, t + \cdots + a_n\, t^n$ for some scalars $a_0, a_1, \dots, a_n \in \mathbb{K}$, $g = b_0 + b_1\, t + \cdots + b_n\, t^n$ for some scalars $b_0, b_1, \dots, b_n \in \mathbb{K}$, and $c\, f + d\, g = (ca_0 + db_0) + (ca_1 + db_1)\, t + \cdots + (ca_n + db_n)\, t^n$. Since

$a_k = 0 = b_k$ for all $k > n$, we deduce that $ca_k + db_k = 0$ for all $k > n$ and the linear combination $c\,f + d\,g$ lies in $\mathbb{K}[t]_{\leqslant n}$. Hence, the subspace test [1.2.0] proves that $\mathbb{K}[t]_{\leqslant n}$ is a linear subspace of $\mathbb{K}[t]$. By definition, the monomials $1, t, t^2, \dots, t^n$ span $\mathbb{K}[t]_{\leqslant n}$. Since these monomials are linearly independent [2.0.6], they form a basis of $\mathbb{K}[t]_{\leqslant n}$ and $\dim(\mathbb{K}[t]_{\leqslant n}) = n + 1$. □

2.1.8 Problem. Show that $1, t, t(t-1), (t-1)^2, 1 + t + t^2 \in \mathbb{Q}[t]$ are linearly dependent.

Solution. The exchange lemma [2.1.2] establishes that the number of vectors in a linearly independent set is less than or equal to the dimension of the ambient vector space. The 5 given vectors lie in the 3-dimensional vector space $\mathbb{Q}[t]_{\leqslant 2}$, so they are linear dependent. □

Exercises

2.1.9 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

i. The $\mathbb{K}$-vector space $\mathbb{K}[t]_{\leqslant n}$ has a unique basis.

ii. The functions $1, \cos(x), \sin(x), \cos(2x), \sin(2x), \dots, \cos(nx), \sin(nx)$ are linearly independent in the real vector space $\mathbb{R}^{\mathbb{R}}$.

iii. The complex vector space $\mathbb{C}^{\mathbb{C}}$ of all functions from the complex numbers to the complex numbers has a finite dimension.

iv. Every linear independent set in $\mathbb{K}^n$ is part of a basis for $\mathbb{K}^n$.

2.1.10 Problem. Let $a_0, a_1, \dots, a_n$ be $n+1$ distinct real numbers. The ***Lagrange polynomials*** are defined by

$$\mathrm{L}_j(t) := \frac{(t-a_0)\cdots(t-a_{j-1})(t-a_{j+1})\cdots(t-a_n)}{(a_j-a_0)\cdots(a_j-a_{j-1})(a_j-a_{j+1})\cdots(a_j-a_n)} = \prod_{\substack{k=0\\k\neq j}}^{n} \frac{t-a_k}{a_j-a_k} \qquad \text{where } 0 \leqslant j \leqslant n.$$

i. Compute the Lagrange polynomials associated with the three real numbers $a_0 = 1$, $a_1 = 2$, and $a_2 = 3$.

ii. Prove that the polynomials $\mathrm{L}_0, \mathrm{L}_1, \dots, \mathrm{L}_n$ form a basis for $\mathbb{R}[t]_{\leqslant n}$.

iii. Deduce the Lagrange interpolation formula which states that, for all $q \in \mathbb{R}[t]_{\leqslant n}$, we have

$$q(t) = \sum_{j=0}^{n} q(a_j)\,\mathrm{L}_j(t)\,.$$

2.1.11 Problem. For any square matrix $\mathbf{B}$ with entries in $\mathbb{K}$, prove that there is a nonzero polynomial $p \in \mathbb{K}[t]$ which has $\mathbf{B}$ as a root.

2.2 Recognizing Bases

How does dimension help identify bases in a vector space? A basis for a linear subspace can typically be obtain from a basis of its ambient vector space.

2.2.0 Problem. Let n be a positive integer. Determine the dimension of the linear subspace of all symmetric matrices in $\mathbb{R}$-vector space $\mathbb{R}^{n\times n}$.

Solution. For all $1 \leqslant j \leqslant n$ and all $1 \leqslant k \leqslant n$, let $a_{j,k}$ denote the (j,k)-entry in an $(n \times n)$-matrix $\mathbf{A}$. The matrix $\mathbf{A}$ is symmetric if $\mathbf{A}^{\mathsf{T}} = \mathbf{A}$ or equivalently $a_{j,k} = a_{k,j}$. Hence, any symmetric matrix $\mathbf{A}$ can be expressed as

$$\mathbf{A} = \left(\sum_{j=1}^{n} a_{j,j}\, \mathbf{E}_{j,j} \right) + \left(\sum_{j=1}^{n-1} \sum_{k=j+1}^{n} a_{j,k}\, (\mathbf{E}_{j,k} + \mathbf{E}_{k,j}) \right) = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & \cdots & a_{n,n} \end{bmatrix},$$

which shows that the set

$$\mathcal{B} := \{\mathbf{E}_{j,j} \mid 1 \leqslant j \leqslant n\} \cup \{\mathbf{E}_{j,k} + \mathbf{E}_{k,j} \mid 1 \leqslant j < k \leqslant n\}$$

spans the linear subspace of symmetric matrices. Because no two matrices in $\mathcal{B}$ are nonzero in the same entry, this set is also linearly independent. Thus, the set $\mathcal{B}$ is a basis for the space of symmetric matrices and its dimension is

$$n + (n-1) + (n-2) + \cdots + 2 + 1 = \frac{n(n+1)}{2} = \binom{n+1}{2}. \qquad \square$$

The next result shows that a maximal linearly independent set is a basis and a minimal spanning set is a basis.

2.2.1 Proposition (Extremal properties of a basis)**.** *Let n be a nonnegative integer and consider the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ in the $\mathbb{K}$-vector space V.*

i. *When the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ are linearly independent, they are contained in a basis of V and $n \leqslant \dim(V)$. Moreover, we have $n = \dim(V)$ if and only if the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ form a basis of V.*
ii. *When* $\operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n) = V$, *the vectors contain a basis of V and $n \geqslant \dim(V)$. Moreover, we have $n = \dim(V)$ if and only if the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ form a basis for V.*

Proof. The inequalities in both part *i* and part *ii* follow from the exchange lemma [2.1.2]. When the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ form a basis, the definition of dimension establishes that $\dim(V) = n$. It remains to show that, in both cases, the equality $n = \dim(V)$ implies that the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ do form a basis. Assume that $n = \dim(V)$.

i. Suppose that $\operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n) \neq V$. There exists a vector $\boldsymbol{w}$ in V that is not a linear combination of the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$. Hence, in any linear relation $c_1\, \boldsymbol{v}_1 + c_2\, \boldsymbol{v}_2 + \cdots + c_n\, \boldsymbol{v}_n + d\, \boldsymbol{w} = \mathbf{0}$, we must have $d = 0$. Since the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ are linearly independent, we also have $c_1 = c_2 = \cdots = c_n = 0$ and the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n, \boldsymbol{w}$ are linearly independent. The exchange lemma [2.1.2] shows that $n = \dim(V) \geqslant n+1$ which is absurd. Thus, the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ do span V and form a basis of V.

ii. Suppose that the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ are linear dependent. There exists a nonzero linear relation $c_1\, \boldsymbol{v}_1 + c_2\, \boldsymbol{v}_2 + \cdots + c_n\, \boldsymbol{v}_n = \mathbf{0}$. In particular, there is an index k such that $1 \leqslant k \leqslant n$, $c_k \neq 0$, and

$$\boldsymbol{v}_k = -\tfrac{c_1}{c_k}\boldsymbol{v}_1 - \tfrac{c_2}{c_k}\boldsymbol{v}_2 - \cdots \tfrac{c_{k-1}}{c_k}\boldsymbol{v}_{k-1} - \tfrac{c_{k+1}}{c_k}\boldsymbol{v}_{k+1} - \tfrac{c_{k+2}}{c_k}\boldsymbol{v}_{k+2} - \cdots - \tfrac{c_n}{c_k}\boldsymbol{v}_n \,.$$

It follows that $\operatorname{Span}(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_{k-1}, \boldsymbol{v}_{k+1}, \boldsymbol{v}_{k+2}, \dots, \boldsymbol{v}_n) = V$. Thus, the exchange lemma [2.1.2] shows that $n = \dim(V) \leqslant n - 1$ which is absurd. Therefore, the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n$ are linearly independent and do form a basis of V. □

Using these extremal properties, we identify a common basis for the polynomials of bounded degree.

2.2.2 Problem. Let n be a nonnegative integer and fix a scalar a in $\mathbb{K}$. Prove that that the $n+1$ polynomials $1, (t-a), (t-a)^2, \dots, (t-a)^n$ form a basis of $\mathbb{K}[t]_{\leqslant n}$.

Solution. The $\mathbb{K}$-vector space $\mathbb{K}[t]_{\leqslant n}$ has dimension $n+1$; see [2.1.7]. Given $n+1$ polynomials having degree at most n, it suffices by the extremal properties of bases [2.2.1] to show that these polynomials are linearly independent. Suppose that there exists scalars $c_0, c_1, \dots, c_n$ in $\mathbb{K}$ such that $c_0\, 1 + c_1\,(t-a) + c_2\,(t-a)^2 + \cdots + c_n\,(t-a)^n = 0$. It remains to demonstrate that $c_0 = c_1 = \cdots = c_n = 0$.

For all $0 \leqslant k \leqslant n$, we prove that $c_k = 0$ by induction on k. Evaluating at a, we see that $c_0\, 1 + c_1\, 0 + \cdots + c_n\, 0 = 0$ establishing that the base case $c_0 = 0$. For some index k satisfying $0 \leqslant k < n$, assume that $c_0 = c_1 = \cdots = c_k = 0$. Thus, our linear relation becomes

$$\begin{aligned} 0 &= c_0\, 1 + c_1\,(t-a) + c_2\,(t-a)^2 + \cdots + c_n\,(t-a)^n \\ &= (t-a)^{k+1}\big(c_{k+1}\, 1 + c_{k+2}\,(t-a) + \cdots + c_n\,(t-a)^{n-k-1}\big) \,. \end{aligned}$$

and we deduce that $c_{k+1}\, 1 + c_{k+2}\,(t-a) + \cdots + c_n\,(t-a)^{n-k-1} = 0$. Evaluating at a implies that $c_{k+1} = 0$ completing the induction step. We conclude that the polynomials $1, (t-a), (t-a)^2, \dots, (t-a)^n$ form a basis of the $\mathbb{K}$-vector space $\mathbb{K}[t]_{\leqslant n}$. □

2.2.3 Problem. Let $V := \{ f \in \mathbb{C}[t]_{\leqslant 3} \mid f(1) = 0\}$. Show that V is a linear subspace and find its dimension.

Solution. The zero polynomial belongs V, so $V \neq \varnothing$. For any $f, g \in V$ and any $b, c \in \mathbb{C}$, we have

$$(b\, f + c\, g)(1) = b\, f(1) + c\, g(1) = b(0) + c(0) = 0 \,,$$

so the subspace test [1.2.0] proves that V is a linear subspace of $\mathbb{C}[t]$. Since the set $\{1, t-1, (t-1)^2, (t-1)^3\}$ span $\mathbb{C}[t]_{\leqslant 3}$, it follows that $\{t-1, (t-1)^2, (t-1)^3\}$ spans V. As a subset of a basis, this set is clearly linearly independent, whence $\dim V = 3$. □