SOLUTIONS MANUAL FOR

Finite Dimensional Linear Algebra

by

Mark S. Gockenbach
Michigan Technological University

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number: 978-1-4398-5659-8 (Paperback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Errata for the first printing **1**

2 Fields and vector spaces **5**
2.1 Fields . . . 5
2.2 Vector spaces . . . 10
2.3 Subspaces . . . 12
2.4 Linear combinations and spanning sets . . . 16
2.5 Linear independence . . . 18
2.6 Basis and dimension . . . 21
2.7 Properties of bases . . . 29
2.8 Polynomial interpolation and the Lagrange basis . . . 37
2.9 Continuous piecewise polynomial functions . . . 43

3 Linear operators **47**
3.1 Linear operators . . . 47
3.2 More properties of linear operators . . . 52
3.3 Isomorphic vector spaces . . . 56
3.4 Linear operator equations . . . 64
3.5 Existence and uniqueness of solutions . . . 67
3.6 The fundamental theorem; inverse operators . . . 73
3.7 Gaussian elimination . . . 81
3.8 Newton's method . . . 82
3.9 Linear ordinary differential equations . . . 83
3.10 Graph theory . . . 85
3.11 Coding theory . . . 86
3.12 Linear programming . . . 87

4 Determinants and eigenvalues **91**
4.1 The determinant function . . . 91
4.2 Further properties of the determinant function . . . 95
4.3 Practical computation of $\det(A)$ . . . 96
4.5 Eigenvalues and the characteristic polynomial . . . 100
4.6 Diagonalization . . . 104
4.7 Eigenvalues of linear operators . . . 108
4.8 Systems of linear ODEs . . . 114
4.9 Integer programming . . . 116

5 The Jordan canonical form **117**
5.1 Invariant subspaces . . . 117
5.2 Generalized eigenspaces . . . 122
5.3 Nilpotent operators . . . 129
5.4 The Jordan canonical form of a matrix . . . 134

5.5 The matrix exponential . . . 145
5.6 Graphs and eigenvalues . . . 147

6 Orthogonality and best approximation 149
6.1 Norms and inner products . . . 149
6.2 The adjoint of a linear operator . . . 156
6.3 Orthogonal vectors and bases . . . 161
6.4 The projection theorem . . . 165
6.5 The Gram-Schmidt process . . . 172
6.6 Orthogonal complements . . . 177
6.7 Complex inner product spaces . . . 181
6.8 More on polynomial approximation . . . 184
6.9 The energy inner product and Galerkin's method . . . 187
6.10 Gaussian quadrature . . . 189
6.11 The Helmholtz decomposition . . . 191

7 The spectral theory of symmetric matrices 193
7.1 The spectral theorem for symmetric matrices . . . 193
7.2 The spectral theorem for normal matrices . . . 198
7.3 Optimization and the Hessian matrix . . . 202
7.4 Lagrange multipliers . . . 204
7.5 Spectral methods for differential equations . . . 206

8 The singular value decomposition 209
8.1 Introduction to the SVD . . . 209
8.2 The SVD for general matrices . . . 212
8.3 Solving least-squares problems using the SVD . . . 216
8.4 The SVD and linear inverse problems . . . 219
8.5 The Smith normal form of a matrix . . . 221

9 Matrix factorizations and numerical linear algebra 223
9.1 The LU factorization . . . 223
9.2 Partial pivoting . . . 227
9.3 The Cholesky factorization . . . 229
9.4 Matrix norms . . . 230
9.5 The sensitivity of linear systems to errors . . . 233
9.6 Numerical stability . . . 236
9.7 The sensitivity of the least-squares problem . . . 238
9.8 The QR factorization . . . 240
9.9 Eigenvalues and simultaneous iteration . . . 242
9.10 The QR algorithm . . . 245

10 Analysis in vector spaces 247
10.1 Analysis in $\mathbf{R}^n$ . . . 247
10.2 Infinite-dimensional vector spaces . . . 249
10.3 Functional analysis . . . 251
10.4 Weak convergence . . . 252

Errata for the first printing

The following corrections will be made in the second printing of the text, expected in 2011. The solutions manual is written as if they have already been made.

Page 65: Exercise 14: belongs in Section 2.7.

Page 65: Exercise 16: should read "(cf. Exercise 2.3.21)", not "(cf. Exercise 2.2.21)".

Page 71: Exercise 9 (b): $\mathbf{Z}_4^5$ should be $\mathbf{Z}_5^4$.

Page 72: Exercise 11: "over V" should be "over F".

Page 72: Exercise 15: "$i = 1, 2, \ldots, k$" should be "$j = 1, 2, \ldots, k$" (twice).

Page 79: Exercise 1: "$x_3 = 2$" should be "$x_3 = 3$".

Page 82: Exercise 14(a): "Each A_i and B_i has degree $2n+1$" should read "$A_i, B_i \in \mathcal{P}_{2n+1}$ for all $i = 0, 1, \ldots, n$".

Page 100, Exercise 11: "$K : C[a,b] \to C[a,b]$" should be "$K : C[c,d] \to C[a,b]$"

Page 114, Line 9: "$L : F^n \to \mathbf{R}^m$" should be "$L : F^n \to F^m$".

Page 115: Exercise 8:

$$\mathcal{S} = \{(1,0,0),(0,1,0),(0,0,1)\}\ \mathcal{X} = \{(1,1,1),(0,1,1),(0,0,1)\}.$$

should be

$$\mathcal{S} = \{(1,0,0),(0,1,0),(0,0,1)\},\ \mathcal{X} = \{(1,1,1),(0,1,1),(0,0,1)\}.$$

Page 116, Exercise 17(b): "$\mathcal{F}^{mn}$" should be "F^{mn}".

Page 121, Exercise 3: "$T : \mathbf{R}^4 \to \mathbf{R}^3$" should be "$T : \mathbf{R}^4 \to \mathbf{R}^4$".

Page 124, Exercise 15: "$T : X/\mathrm{ker}(L) \to \mathcal{R}(U)$" should be "$T : X/\mathrm{ker}(L) \to \mathcal{R}(L)$".

Page 124, Exercise 15:

$$T([x]) = T(x) \text{ for all } [x] \in X/\mathrm{ker}(L)$$

should be

$$T([x]) = L(x) \text{ for all } [x] \in X/\mathrm{ker}(L).$$

Page 129, Exercise 4(b): Period is missing at the end of the sentence.

Page 130, Exercise 8: $L : \mathbf{Z}_3^3 \to \mathbf{Z}_3^3$ should read $L : \mathbf{Z}_5^3 \to \mathbf{Z}_5^3$

Page 130, Exercise 13(b): "T defines $\ldots$" should be "S defines $\ldots$".

Page 131, Exercise 15: "$K : C[a,b] \times C[c,d] \to C[a,b]$" should be "$K : C[c,d] \to C[a,b]$".

Page 138, Exercise 7(b): "define" should be "defined".

Page 139, Exercise 12: In the last line, "$\mathrm{sp}\{x_1, x_2, \ldots, x_n\}$" should be "$\mathrm{sp}\{x_1, x_2, \ldots, x_k\}$".

Page 139, Exercise 12: The proposed plan for the proof is not valid. Instead, the instructions should read: Choose vectors $x_1, \ldots, x_k \in X$ such that $\{T(x_1), \ldots, T(x_k)\}$ is a basis for $\mathcal{R}(T)$, and choose a basis $\{y_1, \ldots, y_\ell\}$ for $\mathrm{ker}(T)$. Prove that $\{x_1, \ldots, x_k, y_1, \ldots, y_\ell\}$ is a basis for X. (Hint: First show that $\mathrm{ker}(T) \cap \mathrm{sp}\{x_1, \ldots, x_k\}$ is trivial.)

Page 140, Exercise 15: In the displayed equation, $|A_{ii}$ should be $|A_{ii}|$.

Page 168: Definition 132 defines the adjacency matrix of a graph, not the incidence matrix (which is something different). The correct term (adjacency matrix) is used throughout the rest of the section. (Change "incidence" to "adjacency" in three places: the title of Section 3.10.1, Page 168 line -2, Page 169 line 1.)

Page 199, Equation (3.41d): "$x_1, x_2 \le 0$" should be "$x_1, x_2 \ge 0$".

Page 204, Exercise 10: "$\alpha_1,\ldots,\alpha_k \in \mathbf{R}$" should be "$\alpha_1,\ldots,\alpha_k \geq 0$". Also, C should not be boldface in the displayed formula.
Page 221, Exercise 9: "$m > n$" should be "$m < n$".
Page 242, Corollary 194: "for each $i = 1, 2, \ldots, t$" should be "for each $i = 1, 2, \ldots, m$".
Page 251, Exercise 18(e):

$$w = \left[\begin{array}{c} 0 \\ \hline v \end{array}\right],$$

should be

$$w = \left[\begin{array}{c} 0 \\ \hline v \end{array}\right].$$

(That is, the comma should be a period.)
Page 256, Exercise 13: First line should read "Let X be a finite-dimensional vector space over $\mathbf{C}$ with basis...". References in part (b) to $F^{n\times n}$, $F^{k\times k}$, $F^{k\times \ell}$, $F^{\ell\times \ell}$ should be replaced with $\mathbf{C}^{n\times n}$, etc. Also, in part (b), "Prove that $[T]_{\mathcal{X}}$" should be replaced with "Prove that $[T]_{\mathcal{X},\mathcal{X}}$".
Page 264, Exercise 3: Add "Assume $\{p, q\}$ is linearly independent."
Page 271, Exercise 3: "...we introduced the incidence matrix ..." should be "...we introduced the adjacency matrix ...".
Page 282, Exercise 6: $S = \mathrm{sp}\{(1, 3, -3, 2), (3, 7, -11, -4)\}$ should be $S = \mathrm{sp}\{(1, 4, -1, 3), (4, 7, -19, 3)\}$.
Page 282, Exercise 7(b): "$\mathcal{N}(A) \cap \mathrm{col}(A)$" should be "$\mathcal{N}(A) \cap \mathrm{col}(A) = \{0\}$".
Page 283, Exercise 12: "Lemma 5.1.2" should be "Lemma 229".
Page 306, Example 252: "$\mathcal{B} = \{p_0, D(p_0), D^2(p_0)\} = \{x^2, 2x, 2\}$" should be "$\mathcal{B} = \{D^2(p_0), D(p_0), p_0\} = \{2, 2x, x^2\}$". Also, "$[T]_{\mathcal{B},\mathcal{B}}$" should be "$[D]_{\mathcal{B},\mathcal{B}}$" (twice). Similarly, $\mathcal{A}$ should be defined as $\{2, -1+2x, 1-x+x^2\}$ and "$[T]_{\mathcal{A},\mathcal{A}}$" should be "$[D]_{\mathcal{A},\mathcal{A}}$".
Page 308, Exercise 3: "Suppose X is a vector space..." should be "Suppose X is a finite-dimensional vector space...".
Page 311, Line 7: "corresponding to λ" should be "corresponding to λ_i".
Page 316, Exercise 6(f): Should end with a ";" instead of a ".".
Page 317, Exercise 15: "$\ker((T-\lambda I)^2) = \ker(A-\lambda I)$" should be "$\ker((T-\lambda I)^2) = \ker(T-\lambda I)$".
Page 322, displayed equation (5.21): The last line should read $v_r' = \lambda v_r$.
Page 325, Exercise 9: "If $U(t_0)$ is singular, say $U(t)c = 0$ for some $c \in \mathbf{C}^n$, $c \neq 0$" should be "If $U(t_0)$ is singular, say $U(t_0)c = 0$ for some $c \in \mathbf{C}^n$, $c \neq 0$".
Page 331, Line 16: "...is at least $t+1$" should be "...is at least $s+1$".
Page 356, Exercise 9: "...such that $\{x_1, x_2, x_3, x_4\}$." should be "...such that $\{x_1, x_2, x_3, x_4\}$ is an orthogonal basis for $\mathbf{R}^4$."
Page 356, Exercise 13: "...be a linearly independent subset of V" should be "...be an orthogonal subset of V"
Page 356, Exercise 14: "...be a linearly independent subset of V" should be "...be an orthogonal subset of V"
Pages 365–368: Miscellaneous exercises 1–21 should be numbered 2–22.
Page 365, Exercise 6 (should be 7): "...under the $L^2(0,1)$ norm" should be "...under the $L^2(0,1)$ inner product".
Page 383, Line 1: "$\mathrm{col}(T)$" should be "$\mathrm{col}(A)$" and "$\mathrm{col}(T)^\perp$" should be "$\mathrm{col}(A)^\perp$".
Page 383, Exercise 3: "...a basis for $\mathbf{R}^4$" should be "...a basis for $\mathbf{R}^3$".
Page 384, Exercise 6: "basis" should be "bases".
Page 385, Exercise 14: "Exercise 6.4.13" should be "Exercise 6.4.1". "That exercise also" should be "Exercise 6.4.13".
Page 385, Exercise 15: "See Exercise 6.4" should be "See Exercise 6.4.14".
Page 400, Exercise 4:

$$\tilde{f}(x) = f\left(a + \frac{b-a}{2}(t+1)\right).$$

should be

$$\tilde{f}(x) = f\left(a + \frac{b-a}{2}(x+1)\right).$$

Page 410, Exercise 1: The problem should specify $\ell = 1$, $k(x) = x + 1$, $f(x) = -4x - 1$.
Page 411, Exercise 6: "$u(\ell) = 0$." should be "$u(\ell) = 0$" (i.e. there should not be a period after 0).
Page 424, Exercise 1: "…prove (1)" should be "…prove (6.50)".
Page 432, Exercise 9: "$G^{-1/2}$ is the inverse of $G^{-1/2}$" should be "$G^{-1/2}$ is the inverse of $G^{1/2}$".
Page 433, Exercise 16: "…so we will try to estimate the values $u(x_1), u(x_2), \ldots, u(x_n)$" should be "…so we will try to estimate the values $u(x_1), u(x_2), \ldots, u(x_{n-1})$".
Page 438, Exercise 3: "…define $T : \mathbf{R}^n \to F^n$" should be "…define $T : F^n \to F^n$".
Page 448, Exercise 8: In the formula for f, $-200x_1^2 x2$ should be $-200x_1^2 x_2$. Also, $(-1.2, 1)$ should be $(1, 1)$.
Page 453, Exercise 6: Add: "Assume $\nabla g(x(0))$ has full rank."
Page 475, Exercise 10: "$A = GH$" should be "$A = GQ$".
Page 476, Exercise 15(a):

$$\|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |A_{ij}^2} \text{ for all } A \in \mathbf{C}^{m\times n}.$$

should be

$$\|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |A_{ij}|^2} \text{ for all } A \in \mathbf{C}^{m\times n}.$$

Page 476, Exercise 15: No need to define $\|C\|_F$ again.
Page 501, last paragraph: The text fails to define $k \equiv \ell \pmod{p}$ for general $k, \ell \in \mathbf{Z}$. The following text should be added: "In general, for $k, \ell \in \mathbf{Z}$, we say that $k \equiv \ell \pmod{p}$ if p divides $k - \ell$, that is, if there exists $m \in \mathbf{Z}$ with $k = \ell + mp$. It is easy to show that, if r is the congruence class of $k \in \mathbf{Z}$, then p divides $k - r$, and hence this is consistent with the earlier definition. Moreover, it is a straightforward exercise to show that $k \equiv \ell \pmod{p}$ if and only if k and ℓ have the same congruence class modulo p."
Page 511, Theorem 381: "$A_{ij}^{(k)} = A_{ij}$" should be "$M_{ij}^{(k)} = A_{ij}$".
Page 516, Exercise 8: "$A^{(1)}, A^{(2)}, \ldots, A^{(n-1)}$" should be "$M^{(1)}, M^{(2)}, \ldots, M^{(n-1)}$".
Page 516, Exercise 10: $n^2/2 - n/2$ should be $n^2 - n$.
Page 523, Exercise 6(b): "…the columns of AP are…" should be "…the columns of AP^T are…".
Page 535, Theorem 401: $\|A\|_1$ should be $\|A\|_\infty$ (twice).
Page 536, Exercise 1: "…be any matrix norm…" should be "…be any induced matrix norm…".
Page 554, Exercise 4: "…b is consider the data …" should be "…b is considered the data …".
Page 554, Exercise 5: "…b is consider the data …" should be "…b is considered the data …".
Page 563, Exercise 7: "Let $v \in \mathbf{R}^m$ be given and define $\alpha = \pm\|x\|_2$, let $\{u_1, u_2, \ldots, u_m\}$ be an orthonormal basis for $\mathbf{R}^m$, where $u_1 = x/\|x\|_2$ …" should be "Let $v \in \mathbf{R}^m$ be given, define $\alpha = \pm\|v\|_2$, $x = \alpha e_1 - v$, $u_1 = x/\|x\|_2$, and let $\{u_1, u_2, \ldots, u_m\}$ be an orthonormal basis for $\mathbf{R}^m$,…".
Page 571, Exercise 3: "Prove that the angle between $A^k v_0$ and x_1 converges to zero as $k \to \infty$" should be "Prove that the angle between $A^k v_0$ and $\mathrm{sp}\{x_1\} = E_A(\lambda_1)$ converges to zero as $k \to \infty$.
Page 575, line 15: $3n^2 - n$ should be $3n^2 + 2n - 5$.
Page 575, line 16: "n square roots" should be "$n - 1$ square roots".
Page 580, Exercise 3: "…requires $3n^2 - n$ arithmetic operations, plus the calculation of n square roots,…" should be "…requires $3n^2 + 2n - 5$ arithmetic operations, plus the calculation of $n - 1$ square roots,…".
Page 585, line 19: "original subsequence" should be "original sequence".
Page 585, line 20: "original subsequence" should be "original sequence".
Page 604, Exercise 4: "Theorem 4" should be "Theorem 451".
Page 608, line 18: "…exists a real number…" should be "…exists as a real number…".

Chapter 2

Fields and vector spaces

2.1 Fields

1. Let F be a field.

   (a) We wish to prove that $-1 \neq 0$. Let us argue by contradiction, and assume that $-1 = 0$. Then $\alpha + (-1) = \alpha$ for all $\alpha \in F$; in particular, $1 + (-1) = 1$. But $1 + (-1) = 0$ by definition of -1, and therefore $1 = 0$ must hold. This contradicts the definition of a field (which states that 1 and 0 are distinct elements), and hence $-1 = 0$ cannot hold in a field.

   (b) It need not be the case that $-1 \neq 1$; in fact, in $\mathbf{Z}_2$, $1 + 1 = 0$, and therefore $-1 = 1$.

2. Let F be a field. We wish to show that the multiplicative identity 1 is unique. Let us suppose that $\gamma \in F$ satisfies $\alpha\gamma = \alpha$ for all $\alpha \in F$. We then have $1 = 1 \cdot \gamma$ (since γ is a multiplicative identity), and also $\gamma = 1 \cdot \gamma$ (since 1 is a multiplicative identity). This implies that $\gamma = 1$, and hence the multiplicative identity is unique.

3. Let F be a field and let $\alpha \in F$ be nonzero. We wish to show that the multiplicative inverse of α is unique. Suppose $\beta \in F$ satisfies $\alpha\beta = 1$. Then, multiplying both sides of the equation by α^{-1}, we obtain $\alpha^{-1}(\alpha\beta) = \alpha^{-1} \cdot 1$, or $(\alpha^{-1}\alpha)\beta = \alpha^{-1}$, or $1 \cdot \beta = \alpha^{-1}$. It follows that $\beta = \alpha^{-1}$, and thus α has a unique multiplicative inverse.

4. Let F be a field, and suppose $\alpha, \beta, \gamma \in F$.

   (a) We have $(-\alpha) + \alpha = 0$; since the additive inverse of $-\alpha$ is unique, this implies that $\alpha = -(-\alpha)$.

   (b) Using the associate and commutative properties of addition, we can rewrite $(\alpha + \beta) + (-\alpha + (-\beta))$ as $(\alpha + (-\alpha)) + (\beta + (-\beta)) = 0 + 0 = 0$. Therefore, $-(\alpha + \beta) = -\alpha + (-\beta)$.

   (c) As in the last part, we can use commutativity and associativity to show that $(\alpha - \beta) + (-\alpha + \beta) = 0$.

   (d) We have $\alpha\beta + \alpha(-\beta) = \alpha(\beta + (-\beta)) = \alpha \cdot 0 = 0$, and this proves that $-(\alpha\beta) = \alpha(-\beta)$.

   (e) This follows from the previous result and the commutative property of multiplication.

   (f) Applying the first, fourth, and fifth results, we have $(-\alpha)(-\beta) = -(\alpha(-\beta)) = -(-(\alpha\beta)) = \alpha\beta$.

   (g) Assume $\alpha \neq 0$. Then $\alpha(\alpha^{-1} + (-\alpha)^{-1}) = \alpha\alpha^{-1} + \alpha(-\alpha)^{-1} = 1 - (-\alpha)(-\alpha)^{-1} = 1 - 1 = 0$. Since $\alpha \neq 0$, $\alpha(\alpha^{-1} + (-\alpha)^{-1}) = 0$ implies that $\alpha^{-1} + (-\alpha)^{-1} = 0$, which in turn implies that $(-\alpha)^{-1} = -(\alpha^{-1})$.

   (h) Using the associative and commutative properties of multiplication, we can rewrite $(\alpha\beta)(\alpha^{-1}\beta^{-1})$ as $(\alpha\alpha^{-1})(\beta\beta^{-1}) = 1 \cdot 1 = 1$. This shows that $\alpha^{-1}\beta^{-1} = (\alpha\beta)^{-1}$.

   (i) Using the definition of subtraction, the distributive property, and the fourth property above, we have $\alpha(\beta - \gamma) = \alpha(\beta + (-\gamma)) = \alpha\beta + \alpha(-\gamma) = \alpha\beta + (-(\alpha\gamma)) = \alpha\beta - \alpha\gamma$.

   (j) This is proved in the same way as the previous result.

5. (a) By definition, $i^2 = (0 + 1 \cdot i)(0 + 1 \cdot i) = (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 1 \cdot 0)i = -1 + 0 \cdot i = -1$.

   (b) We will prove only the existence of multiplicative inverses, the other properties of a field being straightforward (although possibly tedious) to verify. Let $a + bi$ be a nonzero complex number (which means that $a \neq 0$ or $b \neq 0$). We must prove that there exists a complex number $c + di$ such that $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ equals $1 = 1 + 0 \cdot i$. This is equivalent to the pair of equations $ac - bd = 1$, $ad + bc = 0$. If $a \neq 0$, then the second equation yields $d = -bc/a$; substituting into the first equations yields $ac + b^2c/a = 1$, or $c = a/(a^2 + b^2)$. Then $d = -bc/a = -b/(a^2 + b^2)$. This solution is well-defined even if $a = 0$ (since in that case $b \neq 0$), and it can be directly verified that it satisfies $(a + bi)(c + di) = 1$ in that case also. Thus each nonzero complex number has a multiplicative inverse.

6. Let F be a field, and let $\alpha, \beta, \gamma \in F$ with $\gamma \neq 0$. Suppose $\alpha\gamma = \beta\gamma$. Then, multiplying both sides by γ^{-1}, we obtain $(\alpha\gamma)\gamma^{-1} = (\beta\gamma)\gamma^{-1}$, or $\alpha(\gamma\gamma^{-1}) = \beta(\gamma\gamma^{-1})$, which then yields $\alpha \cdot 1 = \beta \cdot 1$, or $\alpha = \beta$.

7. Let F be a field and let α, β be elements of F. We wish to show that the equation $\alpha + x = \beta$ has a unique solution. The proof has two parts. First, if x satisfies $\alpha + x = \beta$, then adding $-\alpha$ to both sides shows that x must equal $-\alpha + \beta = \beta - \alpha$. This shows that the equation has at most one solution. On the other hand, $x = -\alpha + \beta$ is a solution since $\alpha + (-\alpha + \beta) = (\alpha - \alpha) + \beta = 0 + \beta = \beta$. Therefore, $\alpha + x = \beta$ has a unique solution, namely, $x = -\alpha + \beta$.

8. Let F be a field, and let $\alpha, \beta \in F$. We wish to determine if the equation $\alpha x = \beta$ always has a unique solution. The answer is no; in fact, there are three possible cases. First, if $\alpha = 0$ and $\beta = 0$, then $\alpha x = \beta$ is satisfied by every element of F, and there are multiple solutions in this case. Second, if $\alpha = 0$, $\beta \neq 0$, then $\alpha x = \beta$ has no solution (since $\alpha x = 0$ for all $x \in F$ in this case). Third, if $\alpha \neq 0$, then $\alpha x = \beta$ has the unique solution $x = \alpha^{-1}\beta$. (Existence and uniqueness is proved in this case as in the previous exercise.)

9. Let F be a field.

   Let $\alpha, \beta, \gamma, \delta \in F$, with $\beta, \delta \neq 0$. We wish to show that

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta}, \quad \frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}.$$

   Using the definition of division, the commutative and associative properties of multiplication, and finally the distributive property, we obtain

$$\begin{aligned}
\frac{\alpha}{\beta} + \frac{\gamma}{\delta} &= \alpha\beta^{-1} + \gamma\delta^{-1} = (\alpha \cdot 1)\beta^{-1} + (\gamma \cdot 1)\delta^{-1} \\
&= (\alpha(\delta\delta^{-1}))\beta^{-1} + (\gamma(\beta\beta^{-1}))\delta^{-1} = ((\alpha\delta)\delta^{-1})\beta^{-1} + ((\gamma\beta)\beta^{-1})\delta^{-1} \\
&= (\alpha\delta)(\delta^{-1}\beta^{-1}) + (\gamma\beta)(\beta^{-1}\delta^{-1}) = (\alpha\delta)(\delta\beta)^{-1}) + (\gamma\beta)(\beta\delta)^{-1} \\
&= (\alpha\delta)(\beta\delta)^{-1}) + (\gamma\beta)(\beta\delta)^{-1} = ((\alpha\delta) + (\gamma\beta))(\beta\delta)^{-1} \\
&= \frac{\alpha\delta + \beta\gamma}{\beta\delta}.
\end{aligned}$$

   Similarly,

$$\begin{aligned}
\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} &= (\alpha\beta^{-1})(\gamma\delta^{-1}) = ((\alpha\beta^{-1})\gamma)\delta^{-1} = (\alpha(\beta^{-1}\gamma))\delta^{-1} = (\alpha(\gamma\beta^{-1}))\delta^{-1} \\
&= ((\alpha\gamma)\beta^{-1})\delta^{-1} = (\alpha\gamma)(\beta^{-1}\delta^{-1}) = (\alpha\gamma)(\beta\delta)^{-1} = \frac{\alpha\gamma}{\beta\delta}.
\end{aligned}$$

   Now assuming that $\beta, \gamma, \delta \neq 0$, we wish to show that

$$\frac{\alpha/\beta}{\gamma/\delta} = \frac{\alpha\delta}{\beta\gamma}.$$

Using the fact that $(\delta^{-1})^{-1} = \delta$, we have

$$\begin{aligned}\frac{\alpha/\beta}{\gamma/\delta} &= (\alpha\beta^{-1})(\gamma\delta^{-1})^{-1} = (\alpha\beta^{-1})(\gamma^{-1}\delta) = ((\alpha\beta^{-1})\gamma^{-1})\delta \\ &= (\alpha(\beta^{-1}\gamma^{-1}))\delta = (\alpha(\beta\gamma)^{-1})\delta = \alpha((\beta\gamma)^{-1}\delta) \\ &= \alpha(\delta(\beta\gamma)^{-1}) = (\alpha\delta)(\beta\gamma)^{-1} = \frac{\alpha\delta}{\beta\gamma}.\end{aligned}$$

10. Let F be a field, and let $\alpha \in F$ be given. We wish to prove that, for any $\beta_1, \ldots, \beta_n \in F$, $\alpha(\beta_1+\cdots+\beta_n) = \alpha\beta_1+\cdots+\alpha\beta_n$. We argue by induction on n. For $n = 1$, the result is simply $\alpha\beta_1 = \alpha\beta_1$. Suppose that for some $n \geq 2$, $\alpha(\beta_1 + \cdots + \beta_{n-1}) = \alpha\beta_1 + \cdots + \alpha\beta_{n-1}$ for any $\beta_1, \ldots, \beta_{n-1} \in F$. Let $\beta_1, \ldots, \beta_{n-1}, \beta_n \in F$. Then

$$\begin{aligned}&\alpha(\beta_1 + \cdots + \beta_n) = \alpha((\beta_1 + \cdots + \beta_{n-1}) + \beta_n) \\ =&\alpha(\beta_1 + \cdots + \beta_{n-1}) + \alpha\beta_n = \alpha\beta_1 + \cdots + \alpha\beta_{n-1} + \alpha\beta_n.\end{aligned}$$

(In the last step, we applied the induction hypothesis, and in the step preceding that, the distributive property of addition of multiplication.) This shows that $\alpha(\beta_1 + \cdots + \beta_n) = \alpha\beta_1 + \cdots + \alpha\beta_n$, and the general result now follows by induction.

11. (a) The space $\mathbf{Z}$ is not a field because multiplicative inverses do not exist in general. For example, $2 \neq 0$, yet there exists no $n \in \mathbf{Z}$ such that $2n = 1$.

    (b) The space $\mathbf{Q}$ of rational number is a field. Assuming the usual definitions for addition and multiplication, all of the defining properties of a field are straightforward to verify.

    (c) The space of positive real numbers is not a field because there is no additive identity. For any $z \in (0, \infty)$, $x + z > x$ for all $x \in (0, \infty)$.

12. Let $F = \{(\alpha, \beta) : \alpha, \beta \in \mathbf{R}\}$, and define addition and multiplication on F by $(\alpha, \beta)+(\gamma, \delta) = (\alpha+\gamma, \beta+\delta)$, $(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma, \beta\delta)$. With these definitions, F is not a field because multiplicative inverses do not exists. It is straightforward to verify that $(0, 0)$ is an additive inverse and $(1, 1)$ is a multiplicative inverse. Then $(1, 0) \neq (0, 0)$, yet $(1, 0) \cdot (\alpha, \beta) = (\alpha, 0) \neq (1, 1)$ for all $(\alpha, \beta) \in F$. Since F contains a nonzero element with no multiplicative inverse, F is not a field.

13. Let $F = (0, \infty)$, and define addition and multiplication on F by $x \oplus y = xy$, $x \odot y = x^{\ln y}$. We wish to show that F is a field. Commutativity and associativity of addition follow immediately from these properties for ordinary multiplication of real numbers. Obviously 1 is an additive inverse, and the additive inverse of $x \in F$ is its reciprocal $1/x$. The properties of multiplication are less obvious, but note that $x \odot y = e^{\ln(y \odot x)} = e^{\ln(y)\ln(x)}$, and this formula makes both commutativity and associativity easy to verify. We also see that e is a multiplicative identity: $x \odot e = x^{\ln(e)} = x^1 = x$ for all $x \in F$. For any $x \in F$, $x \neq 1$, $y = e^{1/\ln(x)}$ is a multiplicative inverse. Finally, for any $x, y, z \in F$, $x \odot (y \oplus z) = x \odot (yz) = x^{\ln(yz)} = x^{\ln(y)+\ln(z)} = x^{\ln(y)}x^{\ln(z)} = (x \odot y)(x \odot z) = (x \odot y) \oplus (x \odot z)$. Thus the distributive property holds.

14. Suppose F is a set on which are defined two operations, addition and multiplication, such that all the properties of a field are satisfied except that addition is not assumed to be commutative. We wish to show that, in fact, addition must be commutative, and therefore F must be a field. We first note that it is possible to prove that $0 \cdot \gamma = 0$, $-1 \cdot \gamma = -\gamma$, and$-(-\gamma) = \gamma$ for all $\gamma \in F$ without invoking commutativity of addition. Moreover, for all $\alpha, \beta \in F$, $-\beta + (-\alpha) = -(\alpha + \beta)$ since $(\alpha + \beta) + (-\beta + (-\alpha)) = ((\alpha + \beta) + (-\beta)) + (-\alpha) = (\alpha + (\beta + (-\beta))) + (-\alpha) = (\alpha + 0) + (-\alpha) = \alpha + (-\alpha) = 0$. We therefore conclude that $-1 \cdot (\alpha + \beta) = -\beta + (-\alpha)$ for all $\alpha, \beta \in F$. But, by the distributive property, $-1 \cdot (\alpha + \beta) = -1 \cdot \alpha + (-1) \cdot \beta = -\alpha + (-\beta)$, and therefore $-\alpha + (-\beta) = -\beta + (-\alpha)$ for all $\alpha, \beta \in F$. Applying this property to $-\alpha$, $-\beta$ in place of α, β, respectively, yields $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in F$, which is what we wanted to prove.

15. (a) In $\mathbf{Z}_2 = \{0, 1\}$, we have $0 + 0 = 0$, $1 + 0 = 0 + 1 = 1$, and $1 + 1 = 0$. This shows that $-0 = 0$ (as always) and $-1 = 1$. Also, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$, and $1^{-1} = 1$ (as in any field).

(b) The addition and multiplication tables for $\mathbf{Z}_3 = \{0, 1, 2\}$ are

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

We see that $-0 = 0$, $-1 = 2$, $-2 = 1$, $1^{-1} = 1$, $2^{-1} = 2$.

The addition and multiplication tables for $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ are

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

We see that $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

16. Let p be a positive integer that is prime. We wish to show that $\mathbf{Z}_p$ is a field. The commutativity of addition and multiplication in $\mathbf{Z}_p$ follow immediately from the commutativity of addition and multiplication of integers, and similarly for associativity and the distributive property. Obviously 0 is an additive identity and 1 is a multiplicative identity. Also, $1 \neq 0$. For any $\alpha \in \mathbf{Z}_p$, the integer $p - \alpha$, regarded as an element of $\mathbf{Z}_p$, satisfies $\alpha + (p - \alpha) = 0$ in $\mathbf{Z}_p$; therefore every element of $\mathbf{Z}_p$ has an additive inverse. It remains only to prove that every nonzero element of $\mathbf{Z}_p$ has a multiplicative inverse. Suppose $\alpha \in \mathbf{Z}_p$, $\alpha \neq 0$. Since $\mathbf{Z}_p$ has only finitely many elements, $\alpha, \alpha^2, \alpha^3, \ldots$ cannot all be distinct; there must exist positive integers k, ℓ, with $k > \ell$, such that $\alpha^k = \alpha^\ell$ in $\mathbf{Z}_p$. This means that the integers α^k, α^ℓ satisfy $\alpha^k = \lambda^\ell + np$ for some positive integer n, which in turn yields $\alpha^k - \alpha^\ell = np$ or $\alpha^\ell(\alpha^{k-\ell} - 1) = np$. Now, a basic theorem from number theory states that if a prime p divides a product of integers, then it must divide one of the integers in the product. In this case, p must divide α or $\alpha^{k-\ell} - 1$. Since $0 < \alpha < p$, p does not divide α, and therefore p divides $\alpha^{k-\ell} - 1$. Therefore, $\alpha^{k-\ell} - 1 = sp$, where s is a positive integer; this is equivalent to $\alpha^{k-\ell} = 1$ in $\mathbf{Z}_p$. Finally, this means that $\alpha\alpha^{k-\ell-1} = 1$ in $\mathbf{Z}_p$, and therefore α has a multiplicative inverse, namely, $\alpha^{k-\ell-1}$. This completes the proof that $\mathbf{Z}_p$ is a field.

17. Let p be a positive integer that is not prime. It is easy to see that 1 is a multiplicative identity in $\mathbf{Z}_p$. Since p is not prime, there exist integers m, n satisfying $1 < m, n < p$ and $mn = p$. But then, if m and n are regarded as elements of $\mathbf{Z}_p$, $m, n \neq 0$ and $mn = 0$, which is impossible in a field. Therefore, $\mathbf{Z}_p$ is not a field when p is not prime.

18. Let F be a finite field.

(a) Consider the elements $1, 1+1, 1+1+1, \ldots$ in F. Since F contains only finitely many elements, there must exist two terms in this sequence that are equal, say $1 + 1 + \cdots + 1$ (ℓ terms) and $1 + 1 + \cdots + 1$ (k terms), where $k > \ell$. We can then add -1 to both sides ℓ times to show that $1 + 1 + \cdots + 1$ ($k - \ell$ terms) equals 0 in F. Since at least one of the sequence $1, 1+1, 1+1+1, \ldots$ equals 0, we can define n to be the smallest integer greater than 1 such that $1 + 1 + \cdots + 1 = 0$ (n terms). We call n the characteristic of the field.

(b) Given that the characteristic of F is n, for any $\alpha \in F$, we have $\alpha + \alpha + \cdots + \alpha = \alpha(1 + 1 + \cdots + 1) = \alpha \cdot 0 = 0$ if the sum has n terms.

(c) We now wish to show that the characteristic n is prime. Suppose, by way of contradiction, that $n = k\ell$, where $1 < k, \ell < n$. Define $\alpha = 1 + 1 + \cdots + 1$ (k terms) and $\beta = 1 + 1 + \cdots + 1$ (ℓ terms). Then $\alpha\beta = 1 + 1 + \cdots + 1$ (n terms), so that $\alpha\beta = 0$. But this implies that $\alpha = 0$ or $\beta = 0$, which contradicts the definition of the characteristic n. This contradiction shows that n must be prime.

19. We are given that **H** represents the space of quaternions and the definitions of addition and multiplication in **H**. The first two parts of the exercise are purely computational.

    (a) $i^2 = j^2 = k^2 = -1$, $ij = k$, $ik = -j$, $jk = i$, $ji = -k$, $ki = j$, $kj = -i$, $ijk = -1$.

    (b) $x\overline{x} = \overline{x}x = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

    (c) The additive identity in **H** is $0 = 0 + 0i + 0j + 0k$. The additive inverse of $x = x_1 + x_2 i + x_3 j + x_4 k$ is $-x = -x_1 - x_2 i - x_3 j - x_4 k$.

    (d) The calculations above show that multiplication is not commutative; for instance, $ij = k$, $ji = -k$.

    (e) It is easy to verify that $1 = 1 + 0i + 0j + 0k$ is a multiplicative identity for **H**.

    (f) If $x \in \mathbf{H}$ is nonzero, then $x\overline{x} = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is also nonzero. It follows that

    $$\frac{\overline{x}}{x\overline{x}} = \frac{x_1}{x\overline{x}} - \frac{x_2}{x\overline{x}}i - \frac{x_3}{x\overline{x}}j - \frac{x_4}{x\overline{x}}k$$

    is a multiplicative inverse for x:

    $$x\frac{\overline{x}}{x\overline{x}} = \frac{x\overline{x}}{x\overline{x}} = 1.$$

20. In order to solve the first two parts of this problem, it is convenient to prove the following result. Suppose F is a field under operations $+, \cdot$, G is a nonempty subset of F, and G is a field under operations $\oplus, \odot$. Moreover, suppose that for all $x, y \in G$, $x + y = x \oplus y$ and $x \cdot y = x \odot y$. Then G is a subfield of F. We already know (since the operations on F reduce to the operations on G when the operands belong to G) that G is closed under $+$ and $\cdot$. We have to prove that the additive and multiplicative identities of F belong to G, which we will do by showing that $0_F = 0_G$ (that is, the additive identity of F equals the additive identity of G under $\oplus$) and $1_F = 1_G$ (which has the analogous meaning). To prove the first, notice that $0_G + 0_G = 0_G \oplus 0_G$ since $0_G \in G$, and therefore $0_G + 0_G = 0_G$. Adding the additive inverse (in F) -0_G to both sides of this equation yields $0_G = 0_F$. A similar proof shows that $1_F = 1_G$. Thus $0_F, 1_F \in G$. We next show that if $x \in G$ and $-x$ denotes the additive inverse of x in F, then $-x \in G$. We write $\ominus x$ for the additive inverse of x in G. We have $x \oplus (\ominus x) = 0$, which implies that $x + (\ominus x) = 0$. But then, adding $-x$ to both sides, we obtain $\ominus x = -x$, and therefore $-x \in G$. Similarly, if $x \in G$, $x \neq 0$, and x^{-1} denotes the multiplicative inverse of x in F, then $x^{-1} \in G$. This completes the proof.

    (a) We wish to show that **R** is a subfield of **C**. It suffices to prove that addition and multiplication in **C** reduce to the usual addition and multiplication in **R** when the operands are real numbers. If $x, y \in \mathbf{R} \subset \mathbf{C}$, then $(x + 0i) + (y + 0i) = (x + y) + (0 + 0)i = (x + y) + 0i = x + y$. Similarly, $(x + 0i)(y + 0i) = (xy - 0 \cdot 0) + (x \cdot 0 + 0 \cdot y)i = xy + 0i = xy$. The the operations on **C** reduce to the operations on **R** when the operands are elements of **R**, and therefore **R** is a subfield of **C**.

    (b) We now wish to show that **C** is a subfield of **H** by showing that the operations of **H** reduce to the operations on **C** when the operands belong to **C**. Let $x = x_1 + x_2 i, y = y_1 + y_2 i$ belong to **C**, so that $x = x_1 + x_2 i + 0j + 0k, y = y_1 + y_2 i + 0j + 0k$ can be regarded as elements of **H**. By definition,

    $$\begin{aligned}
    x + y &= (x_1 + x_2 i + 0j + 0k) + (y_1 + y_2 i + 0j + 0k) \\
    &= (x_1 + y_1) + (x_2 + y_2)i + (0 + 0)j + (0 + 0)k \\
    &= (x_1 + y_1) + (x_2 + y_2)i, \\
    xy =& (x_1 + x_2 i + 0j + 0k)(y_1 + y_2 i + 0j + 0k) \\
    =& (x_1 y_1 - x_2 y_2 - 0 \cdot 0 - 0 \cdot 0) + \\
    & (x_1 y_2 + x_2 y_1 + 0 \cdot 0 - 0 \cdot 0)i + \\
    & (x_1 \cdot 0 - x_2 \cdot 0 + 0 \cdot y_1 + 0 \cdot y_2)j + \\
    & (x_1 \cdot 0 + x_2 \cdot 0 - 0 \cdot y_2 + 0 \cdot y_1)k \\
    =& (x_1 y_1 - x_2 y_2) + (x_1 y_2 + x_2 y_1)i.
    \end{aligned}$$

    Thus both operations on **H** reduce to the usual operations on **C**, which shows that **C** is a subfield of **H**.

(c) Consider the subset $S = \{a + bi + cj : a, b, c \in \mathbf{R}\}$ of $\mathbf{H}$. We wish to determine whether S is a subsfield of $\mathbf{H}$. In fact, S is not a subfield because it is not closed under multiplication. For example, $i, j \in S$, but $ij = k \notin S$.

2.2 Vector spaces

1. Let F be a field, and let $V = \{0\}$, with addition and scalar multiplication on V defined by $0 + 0 = 0$, $\alpha \cdot 0 = 0$ for all $\alpha \in F$. We wish to prove that V is a vector space over F. This is a straightforward verification of the defining properties. The commutative property of addition is vacuous, since V contains a single element. We have $(0 + 0) + 0 = 0 + 0 = 0 + (0 + 0)$, so the associative property holds. The definition $0 + 0 = 0$ shows both that 0 is an additive identity and that 0 is the additive inverse of 0, the only vector in V. Next, for all $\alpha, \beta \in F$, we have $\alpha(\beta \cdot 0) = \alpha \cdot 0 = 0 = (\alpha\beta) \cdot 0$, so the associative property of scalar multiplication is satisfied. Also, $\alpha(0 + 0) = \alpha \cdot 0 = 0 = 0 + 0 = \alpha \cdot 0 + \alpha \cdot 0$ and $(\alpha + \beta) \cdot 0 = 0 = \alpha \cdot 0 + \beta \cdot 0$, so both distributive properties hold. Finally, $1 \cdot 0 = 0$ by definition, so the final property of a vector space holds. Thus V is a vector space over F.

2. Let F be an infinite field, and let V be a nontrivial vector space over F. We wish to show that V contains infinitely many vectors. By definition, V contains a nonzero vector u. It suffices to show that, for all $\alpha, \beta \in F$, $\alpha \neq \beta$ implies $\alpha u \neq \beta u$, since then V contains the infinite subset $\{\alpha u : \alpha \in F\}$. Suppose $\alpha, \beta \in F$, $\alpha \neq \beta$. Then $\alpha u = \beta u$ if and only if $\alpha u - \beta u = 0$, that is, if and only if $(\alpha - \beta)u = 0$. Since $u \neq 0$ by assumption, this implies that $\alpha - \beta = 0$ by Theorem 5. Thus $\alpha u = \beta u$ implies $\alpha = \beta$. which completes the proof.

3. Let V be a vector space over a field F.

    (a) Suppose $z \in V$ is an additive identity. Then $z + 0 = z$ (since 0 is an additive identity) and $0 + z = 0$ (since z is an additive identity). Then $z = z + 0 = 0 + z = 0$, which shows that 0 is the only additive identity in V.

    (b) Let $u \in V$. If $u + v = 0$, then $-u + (u + v) = -u + 0$, which implies that $(-u + u) + v = -u$, or $0 + v = -u$, or finally $v = -u$. Thus the additive inverse $-u$ of u is unique.

    (c) Suppose $u, v \in V$. Then $(u+v)+(-u+(-v)) = ((u+v)+(-u))+(-v) = (u+(v+(-u)))+(-v) = (u+(-u+v))+(-v) = ((u+(-u))+v)+(-v) = (0+v)+(-v) = v+(-v) = 0$. By the preceding result, this shows that $-u + (-v) = -(u + v)$.

    (d) Suppose $u, v, w \in V$ and $u + v = u + w$. Then $-u + (u + v) = -u + (u + w)$, which implies that $(-u + u) + v = (-u + u) + w$, or $0 + v = 0 + w$, or finally $v = w$.

    (e) Suppose $\alpha \in F$ and 0 is the zero vector in V. Then $\alpha 0 + \alpha 0 = \alpha(0 + 0) = \alpha 0$; adding $-(\alpha 0)$ to both sides yields $\alpha 0 = 0$, as desired.

    (f) Suppose $\alpha \in F$, $u \in V$, and $\alpha u = 0$. If $\alpha \neq 0$, then α^{-1} exists and $\alpha^{-1}(\alpha u) = \alpha^{-1} \cdot 0$, which implies $(\alpha^{-1}\alpha)u = 0$ (applying the last result), which in turn yields $1 \cdot u = 0$ or finally $u = 0$. Therefore, $\alpha u = 0$ implies that $\alpha = 0$ or $u = 0$.

    (g) Suppose $u \in V$. Then $0 \cdot u + 0 \cdot u = (0 + 0) \cdot u = 0 \cdot u$. Adding $-(0 \cdot u)$ to both sides yields $0 \cdot u = 0$. We then have $u + (-1)u = 1 \cdot u + (-1)u = (1 + (-1))u = 0 \cdot u = 0$, which shows that $(-1)u = -u$.

4. We are to prove that if F is a field, then F^n is a vector space over F. This is a straightforward verification of the defining properties of a vector space, which follow in this case from the analogous properties of the field F. The details are omitted.

5. We are to prove that $F[a, b]$ (the space of all functions $f : [a, b] \to \mathbf{R}$) is a vector space over $\mathbf{R}$. Like the last exercise, this straightforward verification is omitted.

6. (a) Let p be a prime and n a positive integer. Since each of the n components of $x \in \mathbf{Z}_p^n$ can take on any of the p values $0, 1, \ldots, p - 1$, there are p^n distinct vectors in $\mathbf{Z}_p^n$.

(b) The elements of $\mathbf{Z}_2^2$ are $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. We have $(0,0)+(0,0)=(0,0)$, $(0,0)+(0,1)=(0,1)$, $(0,0)+(1,0)=(1,0)$, $(0,0)+(1,1)=(1,1)$, $(0,1)+(0,1)=(0,0)$, $(0,1)+(1,0)=(1,1)$, $(0,1)+(1,1)=(1,0)$, $(1,0)+(1,0)=(0,0)$, $(1,0)+(1,1)=(0,1)$, $(1,1)+(1,1)=(0,0)$.

7. (a) The elements of $\mathcal{P}_1(\mathbf{Z}_2)$ are the polynomials 0, 1, x, $1+x$, which define distinct functions on $\mathbf{Z}_2$. We have $0+0=0$, $0+1=1$, $0+x=x$, $0+(1+x)=1+x$, $1+1=0$, $1+x=1+x$, $1+(1+x)=x$, $x+x=(1+1)x=0x=0$, $x+(1+x)=1+(x+x)=1$, $(1+x)+(1+x)=(1+1)+(x+x)=0+0=0$.

   (b) Nominally, the elements of $\mathcal{P}_2(\mathbf{Z}_2)$ are $0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2$. However, since these elements are interpreted as functions mapping $\mathbf{Z}_2$ into $\mathbf{Z}_2$, it turns out that the last four functions equal the first four. In particular, $x^2=x$ (as functions), since $0^2=0$ and $1^2=1$. Then $1+x^2=1+x$, $x+x^2=x+x=0$, and $1+x+x^2=1+0=1$. Thus we see that the function spaces $\mathcal{P}_2(\mathbf{Z}_2)$ and $\mathcal{P}_1(\mathbf{Z}_2)$ are the same.

   (c) Let V be the vector space consisting of all functions from $\mathbf{Z}_2$ into $\mathbf{Z}_2$. To specify $f\in V$ means to specify the two values $f(0)$ and $f(1)$. There are exactly four ways to do this: $f(0)=0$, $f(1)=0$ (so $f(x)=0$); $f(0)=1$, $f(1)=1$ (so $f(x)=1$); $f(0)=0$, $f(1)=1$ (so $f(x)=x$); and $f(0)=1$, $f(1)=0$ (so $f(x)=1+x$). Thus we see that $V=\mathcal{P}_1(\mathbf{Z}_2)$.

8. Let $V=(0,\infty)$, with addition $\oplus$ and scalar multiplication $\odot$ defined by $u\oplus v=uv$ for all $u,v\in V$ and $\alpha\odot u=u^\alpha$ for all $\alpha\in\mathbf{R}$ and all $u\in V$. We will prove that V is a vector space over $\mathbf{R}$. First of all, $\oplus$ is commutative and associative (because multiplication of real numbers has these properties). For all $u\in V$, $u\oplus 1=u\cdot 1=u$, so there is an additive identity. Also, if $u\in V$, then $1/u\in V$ satisfies $u\oplus(1/u)=u(1/u)=1$, so each vector has an additive inverse. Next, if $\alpha,\beta\in\mathbf{R}$ and $u,v\in V$, then $\alpha\odot(\beta\odot u)=\alpha\odot(u^\beta)=(u^\beta)^\alpha=u^{\alpha\beta}=(\alpha\beta)\odot u$, so the associative property of scalar multiplication holds. Also, $\alpha\odot(u\oplus v)=\alpha\odot(uv)=(uv)^\alpha=u^\alpha v^\alpha=(\alpha\odot u)\oplus(\alpha\odot v)$ and $(\alpha+\beta)\odot u=u^{\alpha+\beta}=u^\alpha u^\beta=(\alpha\odot u)\oplus(\beta\odot u)$. Thus both distributive properties hold. Finally, $1\odot u=u^1=u$. This completes the proof that V is a vector space over $\mathbf{R}$.

9. Let $V=\mathbf{R}^2$ with the usual scalar multiplication and the following nonstandard vector addition: $u\oplus v=(u_1+v_1,u_2+v_2+1)$ for all $u,v\in\mathbf{R}^2$. It is easy to check that commutativity and associativity of $\oplus$ hold, that $(0,-1)$ is an additive identity, and that each $u=(u_1,u_2)$ has an additive inverse, namely, $(-u_1,-u_2-2)$. Also, $\alpha(\beta u)=(\alpha\beta)u$ for all $u\in V$, $\alpha,\beta\in\mathbf{R}$ (since scalar multiplication is defined in the standard way). However, if $\alpha\in\mathbf{R}$, then $\alpha(u+v)=\alpha(u_1+v_1,u_2+v_2+1)=(\alpha u_1+\alpha v_1,\alpha u_2+\alpha v_2+\alpha)$, while $\alpha u+\alpha v=(\alpha u_1,\alpha u_2)+(\alpha v_1,\alpha v_2)=(\alpha u_1+\alpha v_1,\alpha u_2+\alpha v_2+1)$, and these are unequal if $\alpha\neq 1$. Thus the first distributive property fails to hold, and V is not a vector space over $\mathbf{R}$. (In fact, the second distributive property also fails.)

10. Let $V=\mathbf{R}^2$ with the usual scalar multiplication, and with addition defined by $u\oplus v=(\alpha_1u_1+\beta_1v_1,\alpha_2u_2+\beta_2v_2)$, where $\alpha_1,\alpha_2,\beta_1,\beta_2\in\mathbf{R}$ are fixed. We wish to determine what values of $\alpha_1,\alpha_2,\beta_1,\beta_2$ will make V a vector space over $\mathbf{R}$. We first note that $\oplus$ is commutative if and only if $\alpha_1=\beta_1$, $\alpha_2=\beta_2$. We therefore redefine $u\oplus v$ as $(\alpha_1u_1+\alpha_1v_1,\alpha_2u_2+\alpha_2v_2)=(\alpha_1(u_1+v_1),\alpha_2(u_2+v_2))$. Next, we have $(u\oplus v)\oplus w=(\alpha_1^2u_1+\alpha_1^2v_1+\alpha_1w_1,\alpha_2^2u_2+\alpha_2^2v_2+\alpha_2w_2)$, $u\oplus(v\oplus w)=(\alpha_1u_1+\alpha_1^2v_1+\alpha_1^2w_1,\alpha_2u_2+\alpha_2^2v_2+\alpha_2^2w_2)$. From this, it is easy to show that $(u\oplus v)\oplus w=u\oplus(v\oplus w)$ for all $u,v,w\in\mathbf{R}$ if and only if $\alpha_1^2=\alpha_1$ and $\alpha_2^2=\alpha_2$, that is, if and only if $\alpha_1=0$ or $\alpha_1=1$, and similarly for α_2. However, if $\alpha_1=0$ or $\alpha_2=0$, then no additive identity can exist. For suppose $\alpha_1=0$. Then $u\oplus v=(0,\alpha_2(u_2+v_2))$ for all $u,v\in\mathcal{V}$, and no $z\in V$ can satisfy $u\oplus z=u$ if $u_1\neq 0$. Similarly, if $\alpha_2=0$, then no additive identity can exist. Therefore, if V is to be a field over $\mathbf{R}^2$, then we must have $\alpha_1=\beta_1=\alpha_2=\beta_2=1$, and V reduces to $\mathbf{R}^2$ under the usual vector space operations.

11. Suppose V is the set of all polynomials (over $\mathbf{R}$) of degree exactly two, together with the zero polynomial. Addition and scalar multiplication are defined on V in the usual fashion. Then V is *not* a vector space over $\mathbf{R}$ because it is not closed under addition. For example, $1+x+x^2\in V$, $1+x-x^2\in V$, but $(1+x+x^2)+(1+x-x^2)=2+2x\notin V$.

12. (a) We wish to find a function lying in $C(0,1)$ but not in $C[0,1]$. A suitable function with a discontinuity at one of the endpoints provides an example. For example, $f(x)=1/x$ satisfies $f\in C(0,1)$ and

$f \notin C[0,1]$, as does $f(x) = 1/(1-x)$ or $f(x) = 1/(x-x^2)$. A different type of example is provided by $f(x) = \sin(1/x)$.

(b) The function $f(x) = |x|$ belongs to $C[-1,1]$ but not to $C^1[-1,1]$.

13. Let V be the space of all infinite sequences of real numbers, and define $\{x_n\} + \{y_n\} = \{x_n + y_n\}$, $\alpha\{x_n\} = \{\alpha x_n\}$. The proof that V is a vector space is a straightforward verification of the defining properties, no different than for $\mathbf{R}^n$, and will not be given here.

14. Let V be the set of all piecewise continuous functions $f : [a,b] \to \mathbf{R}$, with addition and scalar multiplication defined as usual for functions. We wish to show that V is a vector space over $\mathbf{R}$. Most of the properties of a vector space are automatically satisfied by V because it is a subset of the space of all real-valued functions on $[a,b]$, which is known to be a vector space. Specifically, commutativity and associativity of addition, the associative property of scalar multiplication, the two distributive laws, and the fact that $1 \cdot u = u$ for all $u \in V$ are all obviously satisfied. Moreover, the 0 function is continuous and hence by definition piecewise continuous, and therefore $0 \in V$. It remains only to show that V is closed under addition and scalar multiplication (then, since $-u = -1 \cdot u$ for any function u, each function $u \in V$ must have an additive inverse in V). Let $u \in V$, $\alpha \in \mathbf{R}$, and suppose u has points of discontinuity $x_1 < x_2 < \cdots < x_{k-1}$, where $x_1 > x_0 = a$ and $x_{k-1} < x_k = b$. Then u is continuous on each interval (x_{i-1}, x_i), $i = 1, 2, \ldots, k$, and therefore, by a simple theorem of calculus (any multiple of a continuous function is continuous), αu is also continuous on each (x_{i-1}, x_i). The one-sided limits of αu at $x_0, x_1, \ldots, x_k$ exist since, for example,

$$\lim_{x \to x_i^+} \alpha u(x) = \alpha \lim_{x \to x_i^+} u(x)$$

(and similarly for left-hand limits). Therefore, αu is piecewise continuous and therefore $\alpha u \in V$. Now suppose u, v belong to V. Let $\{x_1, x_2, \ldots, x_{\ell-1}\}$ be the union of the sets of points of discontinuity of u and of v, ordered so that $a = x_0 < x_1 < \cdots < x_{\ell-1} = x_\ell = b$. Then, since both u and v are continuous at all other points in (a,b), $u+v$ is continuous on every interval (x_{i-1}, x_i). Also, at each x_i, either $\lim_{x \to x_i} u(x)$ exists (if u is continuous at x_i, that is, if x_i is a point of discontinuity only for v), or the one-sided limits $\lim_{x \to x_i^+} u(x)$ and $\lim_{x \to x_i^-} u(x)$ both exist. In the first case, the two one-sided limits exist (and are equal), so in any case the two one-sided limits exist. The same is true for v. Thus, for each x_i, $i = 0, 1, \ldots, \ell - 1$,

$$\lim_{x \to x_i^+} (u(x) + v(x)) = \lim_{x \to x_i^+} u(x) + \lim_{x \to x_i^+} v(x),$$

and similarly for the left-hand limits at $x_1, x_2, \ldots, x_\ell$. This shows that $u+v$ is piecewise continuous, and therefore belongs to V. This completes the proof.

15. Suppose U and V are vector spaces over a field F, and define addition and scalar multiplication on $U \times V$ by $(u,v) + (w,z) = (u+w, v+z)$, $\alpha(u,v) = (\alpha u, \alpha v)$. We wish to prove that $U \times V$ is a vector space over F. In fact, the verifications of all the defining properties of a vector space are straightforward. For instance, $(u,v) + (w,z) = (u+w, v+z) = (w+u, z+v) = (w,z) + (u,v)$ (using the commutativity of addition in U and V), and therefore addition in $U \times V$ is commutative. Note that the additive identity in $U \times V$ is $(0,0)$, where the first 0 is the zero vector in U and the second is the zero vector in V. We will not verify the remaining properties here.

2.3 Subspaces

1. Let V be a vector space over F.

   (a) Let $S = \{0\}$. Then $0 \in S$, S is closed under addition since $0 + 0 = 0 \in S$, and S is closed under scalar multiplication since $\alpha \cdot 0 = 0 \in S$ for all $\alpha \in F$. Thus S is a subspace of V.

   (b) The entire space V is a subspace of V since $0 \in V$ and V is closed under addition and scalar multiplication by definition.

2. Suppose we adopt an alternate definition of subspace, in which "$0 \in S$" is replaced with "S is nonempty." We wish to show that the alternate definition is equivalent to the original definition. If S is a subspace according to the original definition, then $0 \in S$, and therefore S is nonempty. Hence S is a subspace according to the alternate definition. Conversely, suppose S satisfies the alternate definition. Then S is nonempty, so there exists $x \in S$. Since S is closed under scalar multiplication and addition, it follows that $-x = -1 \cdot x \in S$, and hence $0 = -x + x \in S$. Therefore, S satisfies the original definition of subspace.

3. Let V be a vector space over $\mathbf{R}$, and let $v \in V$ be nonzero. We wish to prove that $S = \{0, v\}$ is not a subspace of V. If S were a subspace, then $2v$ would lie in S. But $2v \neq 0$ by Theorem 5, and $2v \neq v$ (since otherwise adding $-v$ to both sides would imply that $v = 0$). Hence $2v \notin S$, and therefore S is not a subspace of V.

4. We wish to determine which of the given subsets are subspaces of $\mathbf{Z}_2^3$. Notice that since $\mathbf{Z}_2 = \{0, 1\}$, if S contains the zero vector, then it is automatically closed under scalar multiplication. Therefore, we need only check whether the given subset contains $(0, 0, 0)$ and is closed under addition.
   (a) $S = \{(0, 0, 0), (1, 0, 0)\}$. This set contains $(0, 0, 0)$ and is closed under addition since $(0, 0, 0) + (0, 0, 0) = (0, 0, 0)$, $(0, 0, 0) + (1, 0, 0) = (1, 0, 0)$, and $(1, 0, 0) + (1, 0, 0) = (0, 0, 0)$. Thus S is a subspace.
   (b) $S = \{(0, 0, 0), (0, 1, 0), (1, 0, 1), (1, 1, 1)\}$. This set contains $(0, 0, 0)$ and it can be verified that it is closed under addition (for instance, $(0, 1, 0) + (1, 0, 1) = (1, 1, 1)$, $(1, 1, 1) + (0, 1, 0) = (1, 0, 1)$, etc.). Thus S is a subspace.
   (c) $S = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 1)\}$ is not a subspace because it is not closed under addition: $(1, 0, 0) + (0, 1, 0) = (1, 1, 0) \notin S$.

5. Suppose S is a subset of $\mathbf{Z}_2^n$. We wish to show that S is a subspace of $\mathbf{Z}_2^n$ if and only if $0 \in S$ and S is closed under addition. Of course, the "only if" direction is trivial. The other direction follows as in the preceding exercise: If $0 \in S$, then S is automatically closed under scalar multiplication, since 0 and 1 are the only elements of the field $\mathbf{Z}_2$, and $0 \cdot v = 0$ for all $v \in S$, $1 \cdot v = v$ for all $v \in S$.

6. Define $S = \{x \in \mathbf{R}^2 : x_1 \geq 0, x_2 \geq 0\}$. Then S is not a subspace of $\mathbf{R}^2$, since it is not closed under scalar multiplication. For instance, $(1, 1) \in S$ but $-1 \cdot (1, 1) = (-1, -1) \notin S$.

7. Define $S = \{x \in \mathbf{R}^2 : ax_1 + bx_2 = 0\}$, where $a, b \in \mathbf{R}$ are constants. We will show that S is subspace of $\mathbf{R}^2$. First, $(0, 0) \in S$, since $a \cdot 0 + b \cdot 0 = 0$. Next, suppose $x \in S$ and $\alpha \in \mathbf{R}$. Then $ax_1 + bx_2 = 0$, and therefore $a(\alpha x_1) + b(\alpha x_2) = \alpha(ax_1 + bx_2) = \alpha \cdot 0 = 0$. This shows that $\alpha x \in S$, and therefore S is closed under scalar multiplication. Finally, suppose $x, y \in S$, so that $ax_1 + bx_2 = 0$ and $ay_1 + by_2 = 0$. Then $a(x_1 + y_1) + b(x_2 + y_2) = (ax_1 + bx_2) + (ay_1 + by_2) = 0 + 0 = 0$, which shows that $x + y \in S$, and therefore that S is closed under addition. This completes the proof.

8. (a) The set $A = \{x \in \mathbf{R}^2 : x_1 = 0 \text{ or } x_2 = 0\}$ is closed under scalar multiplication but not addition. Closure under scalar multiplication holds since if $x_1 = 0$, then $(\alpha x)_1 = \alpha x_1 = \alpha \cdot 0 = 0$, and similarly for the second component. The set is not closed under addition; for instance, $(1, 0), (0, 1) \in A$, but $(1, 0) + (0, 1) = (1, 1) \notin A$.
   (b) The set $Q = \{x \in \mathbf{R}^2 : x_1 \geq 0, x_2 \geq 0\}$ is closed under addition but not scalar multiplication. Since $(1, 1) \in Q$ but $-1 \cdot (1, 1) = (-1, -1) \notin Q$, we see that Q is not closed under scalar multiplication. On the other hand, if $x, y \in Q$, so that $x_1, x_2, y_1, y_2 \geq 0$, we see that $(x + y)_1 = x_1 + y_1 \geq 0 + 0 = 0$ and $(x + y)_2 = x_2 + y_2 \geq 0 + 0 = 0$. This shows that $x + y \in Q$, and therefore Q is closed under addition.

9. Let V be a vector space over a field F, let $u \in V$, and define $S = \{\alpha u : \alpha \in F\}$. We will show that S is a subspace of V. First, $0 \in V$ because $0 = 0 \cdot u$. Next, suppose $x \in S$ and $\beta \in F$. Since $x \in S$, there exists $\alpha \in F$ such that $x = \alpha u$. Therefore, $\beta x = \beta(\alpha u) = (\beta\alpha)u$ (using the associative property of scalar multiplication, which shows that βx belongs to S. Thus S is closed under scalar multiplication. Finally, suppose $x, y \in S$; then there exist $\alpha, \beta \in F$ such that $x = \alpha u$, $y = \beta u$, and $x + y = \alpha u + \beta u = (\alpha + \beta)u$

by the second distributive property. Therefore S is closed under addition, and we have shown that S is a subspace.

10. Let $\mathbf{R}$ be regarded as a vector space over $\mathbf{R}$. We wish to prove that $\mathbf{R}$ has no proper subspaces. It suffices to prove that if S is a nontrivial subspace of $\mathbf{R}$, then $S=\mathbf{R}$. So suppose S is a nontrivial subspace, which means that there exists $x \neq 0$ belonging to S. But then, given any $y \in \mathbf{R}$, $y=(yx^{-1})x$ belongs to S because S is closed under scalar multiplication. Thus $\mathbf{R} \subset S$, and hence $S=\mathbf{R}$.

11. We wish to describe all proper subspaces of $\mathbf{R}^2$. We claim that every proper subspace of $\mathbf{R}^2$ has the form $\{\alpha x : \alpha \in \mathbf{R}, \alpha \neq 0\}$, where $x \in \mathbf{R}^2$ is nonzero (geometrically, such a set is a line through the origin). To prove, this, let us suppose S is a proper subspace of $\mathbf{R}^2$. Then there exists $x \in S$, $x \neq 0$. Since S is closed under scalar multiplication, every vector of the form αx, $\alpha \in \mathbf{R}$, must belong to S. Therefore, S contains the set $\{\alpha x : \alpha \in \mathbf{R}, \alpha \neq 0\}$. Let us suppose that there exists $y \in S$ such that y cannot be written as $y=\alpha x$ for some $\alpha \in \mathbf{R}$. In this case, we argue that every $z \in \mathbf{R}^2$ belongs to S, and hence S is not a proper subspace of $\mathbf{R}^2$. To justify this conclusion, we first note that, since y is not a multiple of x, $x_1y_2-x_2y_1 \neq 0$. Let $z \in \mathbf{R}^2$ be given and consider the equation $\alpha x+\beta y=z$. It can be verified directly that $\alpha=(y_2z_1-y_1z_2)/(x_1y_2-x_2y_1)$, $\beta=(x_1z_2-x_2z_1)/(x_1y_2-x_2y_1)$ satisfy this equation, from which it follows that $z \in S$ (since S is closed under addition and scalar multiplication). Therefore, if S contains any vector not lying in $\{\alpha x : \alpha \in \mathbf{R}, \alpha \neq 0\}$, then S consists of all of $\mathbf{R}^2$, and S is not a proper subspace of $\mathbf{R}^2$.

12. We wish to find a proper subspace of $\mathbf{R}^3$ that is not a plane. One such subspace is the x_1-axis: $S=\{x \in \mathbf{R}^3 : x_2=x_3=0\}$. It is easy to verify that S is a subspace of $\mathbf{R}^3$, and geometrically, S is a line.

    More generally, using the results of Exercise 10, we can show that $\{\alpha x : \alpha \in \mathbf{R}\}$, where $x \neq 0$ is a given vector, is a proper subspace of $\mathbf{R}^3$. Such a subspace represents a line through the origin.

13. Consider the subset $\mathbf{R}^n$ of $\mathbf{C}^n$. Although $\mathbf{R}^n$ contains the zero vector and is closed under addition, it is not closed under scalar multiplication, and hence is not a subspace of $\mathbf{C}^n$. Here the scalars are complex numbers (since $\mathbf{C}^n$ is a vector space over $\mathbf{C}$), and, for example, $(1,0,\ldots,0) \in \mathbf{R}^n$, $i \in \mathbf{C}$, and $i(1,0,\ldots,0)=(i,0,\ldots,0)$ does not belong to $\mathbf{R}^n$.

14. Let $S=\{u \in C[a,b] : u(a)=u(b)=0\}$. Then S is a subspace of $C[a,b]$. The zero function clearly belongs to S. Suppose $u \in S$ and $\alpha \in \mathbf{R}$. Then $(\alpha u)(a)=\alpha u(a)=\alpha \cdot 0=0$, and similarly $(\alpha u)(b)=0$. It follows that $\alpha u \in S$, and S is closed under scalar multiplication. If $u,v \in S$, then $(u+v)(a)=u(a)+v(a)=0+0=0$, and similarly $(u+v)(b)=0$. Therefore S is closed under addition, and we have shown that S is a subspace of $C[a,b]$.

15. Let $S=\{u \in C[a,b] : u(a)=1\}$. Then S is not a subspace of $C[a,b]$ because the zero function does not belong to S.

16. Let $S=\left\{u \in C[a,b] : \int_a^b u(x)\,dx=0\right\}$. We will show that S is a subspace of $C[a,b]$. First, since the integral of the zero function is zero, we see that the zero function belongs to S. Next, suppose $u \in S$ and $\alpha \in \mathbf{R}$. Then $\int_a^b (\alpha u)(x)\,dx=\int_a^b \alpha u(x)\,dx=\alpha\int_a^b u(x)\,dx=\alpha \cdot 0=0$, and therefore $\alpha u \in S$. Finally, suppose $u,v \in S$. Then $\int_a^b (u+v)(x)\,dx=\int_a^b (u(x)+v(x))\,dx=\int_a^b u(x)\,dx+\int_a^b v(x)\,dx=0+0=0$. This shows that $u+v \in S$, and we have proved that S is a subspace of $C[a,b]$.

17. Let V be the vector space of all (infinite) sequences of real numbers.

    (a) Define $Z=\{\{x_n\} \in V : \lim_{n\to\infty} x_n=0\}$. Clearly the zero seqence converges to zero, and hence belongs to Z. If $\{x_n\} \in Z$ and $\alpha \in \mathbf{R}$, then $\lim_{n\to\infty} \alpha x_n=\alpha\lim_{n\to\infty} x_n=\alpha \cdot 0=0$, which implies that $\alpha\{x_n\}=\{\alpha x_n\}$ belongs to Z, and therefore Z is closed under scalar multiplication. Now suppose $\{x_n\}$, $\{y_n\}$ both belong to Z. Then $\lim_{n\to\infty}(x_n+y_n)=\lim_{n\to\infty} x_n+\lim_{n\to\infty} y_n=0+0=0$. Therefore $\{x_n\}+\{y_n\}=\{x_n+y_n\}$ belongs to Z, Z is closed under addition, and we have shown that Z is a subspace of V.

(b) Define $S = \{\{x_n\} \in V : \sum_{n=1}^{\infty} x_n < \infty\}$. From calculus, we know that if $\sum_{n=1}^{\infty} x_n$ converges, then so does $\sum_{n=1}^{\infty} \alpha x_n = \alpha \sum_{n=1}^{\infty} x_n$ for any $\alpha \in \mathbf{R}$. Similarly, if $\sum_{n=1}^{\infty} x_n$, $\sum_{n=1}^{\infty} y_n$ converge, then so does $\sum_{n=1}^{\infty}(x_n + y_n) = \sum_{n=1}^{\infty} x_n + \sum_{n=1}^{\infty} y_n$. Using these facts, it is straightforward to show that S is closed under addition and scalar multiplication. Obviously the zero sequence belongs to S.

(c) Define $L = \{\{x_n\} \in V : \sum_{n=1}^{\infty} x_n^2 < \infty\}$. Here is it obvious that the zero sequence belongs to L and that L is closed under scalar multiplication. To prove that L is closed under addition, notice that, for any $x, y \in \mathbf{R}$, $(x - y)^2 \geq 0$ and $(x + y)^2 \geq 0$ together imply that $|xy| \leq (x^2 + y^2)/2$. It follows that $(x_n + y_n)^2 = x_n^2 + 2x_n y_n + y_n^2 \leq 2(x_n^2 + y_n^2)$. It follows that if $\sum_{n=1}^{\infty} x_n^2$ and $\sum_{n=1}^{\infty} y_n^2$ both converge, and so does $\sum_{n=1}^{\infty}(x_n + y_n)^2$, with $\sum_{n=1}^{\infty}(x_n + y_n)^2 \leq 2\sum_{n=1}^{\infty} x_n^2 + 2\sum_{n=1}^{\infty} y_n^2$. From this we see that L is closed under addition, and thus L is a subspace.

By a common theorem of calculus, we know that if $\sum_{n=1}^{\infty} x_n$ converges, then $\lim_{n\to\infty} x_n = 0$, and the same is true if $\sum_{n=1}^{\infty} x_n^2$ converges. Therefore, S and L are subspaces of Z. However, the converse of this result is not true (if the sequence converges to zero, this does not imply that the corresponding series converges). Therefore, S and L are proper subspaces of Z. We know that L is not a subspace of S; for instance $\sum_{n=1}^{\infty}(1/n^2)$ converges, but $\sum_{n=1}^{\infty}(1/n)$ does not, which shows that $\{1/n\}$ belongs to L but not to S. Also, S is not a subspace of L, since $\{(-1)^n/\sqrt{n}\}$ belongs to S (by the alternating series test) but not to L.

18. Let V be a vector space over a field F, and let X and Y be subspaces of V.

(a) We will show that $X \cap Y$ is also a subspace of V. First of all, since $0 \in X$ and $0 \in Y$, it follows that $0 \in X \cap Y$. Next, suppose $x \in X \cap Y$ and $\alpha \in F$. Then, by definition of intersection, $x \in X$ and $x \in Y$. Since X and Y are subspaces, both are closed under scalar multiplication and therefore $\alpha x \in X$ and $\alpha x \in Y$, from which it follows that $\alpha \in X \cap Y$. Thus $X \cap Y$ is closed under scalar multiplication. Finally, suppose $x, y \in X \cap Y$. Then $x, y \in X$ and $x, y \in Y$. Since X and Y are closed under addition, we have $x + y \in X$ and $x + y \in Y$, from which we see that $x + y \in X \cap Y$. Therefore, $X \cap Y$ is closed under addition, and we have proved that $X \cap Y$ is a subspace of V.

(b) It is not necessarily that case that $X \cup Y$ is a subspace of V. For instance, let $V = \mathbf{R}^2$, and define $X = \{x \in \mathbf{R}^2 : x_2 = 0\}$, $Y = \{x \in \mathbf{R}^2 : x_1 = 0\}$. Thus $X \cup Y$ is not closed under addition, and hence is not a subspace of $\mathbf{R}^2$. For instance, $(1, 0) \in X \subset X \cup Y$ and $(0, 1) \in Y \subset X \cup Y$; however, $(1, 0) + (0, 1) = (1, 1) \notin X \cup Y$.

19. Let V be a vector space over a field F, and let S be a nonempty subset of V. Define T to be the intersection of all subspaces of V that contain S.

(a) We wish to show that T is a subspace of V. First, 0 belongs to every subspace of V that contains S, and therefore 0 belongs to the intersection T. Next, suppose $x \in T$ and $\alpha \in F$. Then x belongs to every subspace of V containing S. Since each of these subspaces is closed under scalar multiplication, it follows that αx also belongs to each subspace, and therefore $\alpha x \in T$. Therefore, T is closed under scalar multiplication. Finally, suppose $x, y \in T$. Then both x and y belong to every subspace of V containing S. Since each subspace is closed under addition, it follows that $x + y$ belongs to every subspace of V containing S. Therefore $x + y \in T$, T is closed under addition, and we have shown that T is a subspace.

(b) Now suppose U is any subspace of V containing S. Then U is one of the sets whose intersection defines T, and therefore every element of T belongs to U by definition of intersection. It follows that $T \subset U$. This means that T is the smallest subspace of V containing S.

20. Let V be a vector space over a field F, and let S, T be subspaces of V. Define $S+T = \{s+t : s \in S, t \in T\}$. We wish to show that $S + T$ is a subspace of V. First of all, $0 \in S$ and $0 \in T$ because S and T are subspaces. Therefore, $0 = 0+0 \in S+T$. Next, suppose $x \in S+T$ and $\alpha \in F$. Then, by definition of $S+T$, there exist $s \in S$, $t \in T$ such that $x = s + t$. Since S and T are subspaces, they are closed under scalar multiplication, and therefore $\alpha s \in S$ and $\alpha t \in T$. It follows that $\alpha x = \alpha(s + t) = \alpha s + \alpha t \in S + T$. Thus $S + T$ is closed under scalar multiplication. Finally, suppose $x, y \in S + T$. Then there exist $s_1, s_2 \in S$,

$t_1, t_2 \in T$ such that $x = s_1 + t_1$, $y = s_2 + t_2$. Since S and T are closed under addition, we see that $s_1 + s_2 \in S$, $t_1 + t_2 \in T$, and therefore $x + y = (s_1 + t_1) + (s_2 + t_2) = (s_1 + s_2) + (t_1 + t_2) \in S + T$. It follows that $S + T$ is closed under addition, and we have shown that $S + T$ is a field.

2.4 Linear combinations and spanning sets

1. Write $u_1 = (-1, -2, 4, -2)$, $u_2 = (0, 1, -5, 4)$.

   (a) With $v = (-1, 0, -6, 6)$, the equation $\alpha_1 u_1 + \alpha_2 u_2 = v$ has a (unique) solution: $\alpha_1 = 1$, $\alpha_2 = 2$. This shows that $v \in \mathrm{sp}\{u_1, u_2\}$.

   (b) With $v = (1, 1, 1, 1)$, the equation $\alpha_1 u_1 + \alpha_2 u_2 = v$ has no solution, and therefore $v \notin \mathrm{sp}\{u_1, u_2\}$.

2. Let $S = \mathrm{sp}\{e^x, e^{-x}\} \subset C[0, 1]$.

   (a) The function $f(x) = \cosh(x)$ belongs to S because $\cosh(x) = (1/2)e^x + (1/2)e^{-x}$.

   (b) The function $f(x) = 1$ does not belong to S because there are no scalars α_1, α_2 satisfying $\alpha_1 e^x + \alpha_2 e^{-x} = 1$ for all $x \in [0, 1]$. To prove this, note that any solution α_1, α_2 would have to satisfy the equations that result from substituting any three values of x from the interval $[0, 1]$. For instance, if we choose $x = 0$, $x = 1/2$, $x = 1$, then we obtain the equations

$$\begin{aligned} \alpha_1 + \alpha_2 &= 1, \\ \alpha_1 e^{1/2} + \alpha_2 e^{-1/2} &= 1, \\ \alpha_1 e + \alpha_2 e^{-1} &= 1. \end{aligned}$$

   A direct calculation shows that this system is inconsistent. Therefore no solution α_1, α_2 exists, and $f \notin S$.

3. Let $S = \mathrm{sp}\{1 + 2x + 3x^2, x - x^2\} \subset \mathcal{P}_2$.

   (a) There is a (unique) solution $\alpha_1 = 2$, $\alpha_2 = 1$ to $\alpha_1(1 + 2x + 3x^2) + \alpha_2(x - x^2) = 2 + 5x + 5x^2$. Therefore, $2 + 5x + 5x^2 \in S$.

   (b) There is no solution α_1, α_2 to $\alpha_1(1 + 2x + 3x^2) + \alpha_2(x - x^2) = 1 - x + x^2$. Therefore, $1 - x + x^2 \notin S$.

4. Let $u_1 = (1 + i, i, 2)$, $u_2 = (1, 2i, 2 - i)$, and define $S = \mathrm{sp}\{u_1, u_2\} \subset \mathbf{C}^3$. The vector $v = (2 + 3i, -2 + 2i, 5 + 2i)$ belongs to S because $2u_1 + iu_2 = v$.

5. Let $S = \mathrm{sp}\{(1, 2, 0, 1), (2, 0, 1, 2)\} \subset \mathbf{Z}_3^4$.

   (a) The vector $(1, 1, 1, 1)$ belongs to S because $2(1, 2, 0, 1) + (2, 0, 1, 2) = (1, 1, 1, 1)$.

   (b) The vector $(1, 0, 1, 1)$ does not belong to S because $\alpha_1(1, 2, 0, 1) + \alpha_2(2, 0, 1, 2) = (1, 0, 1, 1)$ has no solution.

6. Let $S = \mathrm{sp}\{1 + x, x + x^2, 2 + x + x^2\} \subset \mathcal{P}_3(\mathbf{Z}_3)$.

   (a) If $p(x) = 1 + x + x^2$, then $0(1 + x) + 2(x + x^2) + 2(2 + x + x^2) = p(x)$, and therefore $p \in S$.

   (b) Let $q(x) = x^3$. Recalling that $\mathcal{P}_3(\mathbf{Z}_3)$ is a space of polynomials functions, we notice that $q(0) = 0$, $q(1) = 1$, $q(2) = 2$, which means that $q(x) = x$ for all $x \in \mathbf{Z}_3$. We have $1(1 + x) + 2(x + x^2) + 1(2 + x + x^2) = x = q(x)$, and therefore $q \in S$.

7. Let $u = (1, 1, -1)$, $v = (1, 0, 2)$ be vectors in $\mathbf{R}^3$. We wish to show that $S = \mathrm{sp}\{u, v\}$ is a plane in $\mathbf{R}^3$. First note that if $S = \{x \in \mathbf{R}^3 : ax_1 + bx_2 + cx_3 = 0\}$, then (taking $x = u$, $x = v$) we see that a, b, c must satisfy $a + b - c = 0$, $a + 2c = 0$. One solution is $a = 2$, $b = -3$, $c = -1$. We will now prove that $S = \{x \in \mathbf{R}^3 : 2x_1 - 3x_2 - x_3 = 0\}$. First, suppose $x \in S$. Then there exist $\alpha, \beta \in \mathbf{R}$ such that $x = \alpha u + \beta v = \alpha(1, 1, -1) + \beta(1, 0, 2) = (\alpha + \beta, \alpha, -\alpha + 2\beta)$, and $2x_1 - 3x_2 - x_3 = 2(\alpha + \beta) - 3\alpha - (-\alpha + 2\beta) =$

$2\alpha + 2\beta - 3\alpha + \alpha - 2\beta = 0$. Therefore, $x \in \{x \in \mathbf{R}^3 : 2x_1 - 3x_2 - x_3 = 0\}$. Conversely, suppose $x \in \{x \in \mathbf{R}^3 : 2x_1 - 3x_2 - x_3 = 0\}$. If we solve the equation $\alpha u + \beta v = x$, we see that it has the solution $\alpha = x_2$, $\beta = x_1 - x_2$, and therefore $x \in S$. (Notice that $x_2(1,1,-1) + (x_1 - x_2)(1,0,2) = (x_1, x_2, 2x_1 - 3x_2)$, and the assumption $2x_1 - 3x_2 - x_3 = 0$ implies that $2x_1 - 3x_2 = x_3$.) This completes the proof.

8. The previous exercise does not hold true for every choice of $u, v \in \mathbf{R}^3$. For instance, if $u = (1,1,1)$, $v = (2,2,2)$, then $S = \text{sp}\{u, v\}$ is not a plane; in fact, S is easily seen to be the line passing through $(0,0,0)$ and $(1,1,1)$.

9. Let $v_1 = (1,-2,1,2)$, $v_2 = (-1,1,2,1)$, and $v_3 = (-7,9,8,1)$ be vectors in $\mathbf{R}^4$, and let $S = \text{sp}\{v_1, v_2, v_3\}$. Suppose $x \in S$, say $x = \beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3 = (\beta_1 - \beta_2 - 7\beta_3, -2\beta_1 + \beta_2 + 9\beta_3, \beta_1 + 2\beta_2 + 8\beta_3, 2\beta_1 + \beta_2 + \beta_3)$. The equation $\alpha_1 v_1 + \alpha_2 v_2 = (\beta_1 - \beta_2 - 7\beta_3, -2\beta_1 + \beta_2 + 9\beta_3, \beta_1 + 2\beta_2 + 8\beta_3, 2\beta_1 + \beta_2 + \beta_3)$ has a unique solution, namely, $\alpha_1 = \beta_1 - 2\beta_3$, $\alpha_2 = \beta_2 + 5\beta_3$. This shows that x is a linear combination of v_1, v_2 alone.

   Alternate solution: We can solve $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$ to obtain $\alpha_1 = -2$, $\alpha_2 = 5$, $\alpha_3 = -1$, which means that $-2v_1 + 5v_2 - v_3 = 0$ or $v_3 = -2v_1 + 5v_2$. Now suppose $x \in S$, say $x = \beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3$. It follows that $x = \beta_1 v_1 + \beta_2 v_2 + \beta_3(-2v_1 + 5v_2) = (\beta_1 - 2\beta_3)v_1 + (\beta_2 + 5\beta_3)v_2$, and therefore x can be written as a linear combination of v_1 and v_2 alone.

10. Let $u_1 = (1,1,1)$, $u_2 = (1,-1,1)$, $u_3 = (1,0,1)$, and define $S_1 = \text{sp}\{u_1, u_2\}$, $S_2 = \text{sp}\{u_1, u_2, u_3\}$. We wish to prove that $S_1 = S_2$. We first note that if $x \in S_1$, then there exists scalars α_1, α_2 such that $x = \alpha_1 u_1 + \alpha_2 u_2$. But then x can be written as $x = \alpha_1 u_1 + \alpha_2 u_2 + 0 \cdot u_3$, which shows that x is a linear combination of u_1, u_2, u_3, and hence $x \in S_2$. Conversely, suppose that $x \in S_2$, say $x = \beta_1 u_1 + \beta_2 u_2 + \beta_3 u_3 = (\beta_1 + \beta_2 + \beta_3, \beta_1 - \beta_2, \beta_1 + \beta_2 + \beta_3)$. We wish to show that x can be written as a linear combination of u_1, u_2 alone, that is, that there exist scalars α_1, α_2 such that $\alpha_1 u_1 + \alpha_2 u_2 = x$. A direct calculation shows that this equation has a unique solution, namely, $\alpha_1 = \beta_1 + \beta_3/2$, $\alpha_2 = \beta_2 + \beta_3/2$. This shows that $x \in \text{sp}\{u_1, u_2\} = S_1$, and the proof is complete. (The second part of the proof can be done as in the previous solution, by first showing that $u_3 = (1/2)u_1 + (1/2)u_2$.)

11. Let $S = \text{sp}\{(-1,-3,3), (-1,-4,3), (-1,-1,4)\} \subset \mathbf{R}^3$. We wish to determine if $S = \mathbf{R}^3$ or if S is a proper subspace of $\mathbf{R}^3$. Given an arbitrary $x \in \mathbf{R}^3$, we solve $\alpha_1(-1,-1,3) + \alpha_2(-1,-4,3) + \alpha_3(-1,-1,4) = (x_1, x_2, x_3)$ and find that there is a unique solution, namely, $\alpha_1 = -13x_1 + x_2 - 3x_3$, $\alpha_2 = 9x_1 - x_2 + 2x_3$, $\alpha_3 = 3x_1 + x_3$. This shows that every $x \in \mathbf{R}^3$ lies in S, and therefore $S = \mathbf{R}^3$.

12. Let $S = \text{sp}\{(-1,-5,1), (3,14,-4), (1,4,-2)\}$. Given an arbitary $x \in \mathbf{R}^3$, if we try to solve $\alpha_1(-1,-5,1) + \alpha_2(3,14,-4) + \alpha_3(1,4,-2) = (x_1, x_2, x_3)$, we find that there is a solution if and only if $6x_1 - x_2 + x_3 = 0$. Since not all $x \in \mathbf{R}^3$ satisfy this condition, S is a proper subspace of $\mathbf{R}^3$.

13. Let $S = \text{sp}\{1 - x, 2 - 2x + x^2, 1 - 3x^2\} \subset \mathcal{P}_2$. We wish to determine if S is a proper subspace of $\mathcal{P}_2$. Given any $p \in \mathcal{P}_2$, say $p(x) = c_0 + c_1 x + c_2 x^2$, we try to solve $\alpha_1(1 - x) + \alpha_2(2 - 2x + x^2) + \alpha_3(1 - 3x^2) = c_0 + c_1 x + c_2 x^2$. We find that there is a unique solution, $\alpha_1 = -6c_0 - 7c_1 - 2c_2$, $\alpha_2 = 3c_0 + 3c_1 + c_2$, $\alpha_3 = c_0 + c_1$. Therefore, each $p \in \mathcal{P}_2$ belongs to S, and therefore $S = \mathcal{P}_2$.

14. Suppose V is a vector space over a field F and S is a subspace of V. We wish to prove that $u_1, \ldots, u_k \in S$, $\alpha_1, \ldots, \alpha_k \in F$ imply that $\alpha_1 u_1 + \cdots + \alpha_k u_k \in S$. We argue by induction on k. For $k = 1$, we have that $\alpha_1 u_1 \in S$ because S is a subspace and therefore closed under scalar multiplication. Now suppose that, for some $k \geq 2$, $\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1} \in S$ for any $u_1, \ldots, u_{k-1} \in S$, $\alpha_1, \ldots, \alpha_{k-1} \in F$. Let $u_1, \ldots, u_k \in S$, $\alpha_1, \ldots, \alpha_k \in F$ be arbitrary. Then $\alpha_1 u_1 + \ldots + \alpha_k u_k = (\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1}) + \alpha_k u_k$. By the induction hypothesis, $\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1} \in S$, and $\alpha_k u_k \in S$ because S is closed under scalar multiplication. But then $\alpha_1 u_1 + \ldots + \alpha_k u_k = (\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1}) + \alpha_k u_k \in S$ because S is closed under addition. Therefore, by induction, the result holds for all $k \geq 1$, and the proof is complete.

15. Let V be a vector space over a field F, and let $u \in V$, $u \neq 0$, $\alpha \in F$. We wish to prove that $\text{sp}\{u\} = \text{sp}\{u, \alpha u\}$. First, if $x \in \text{sp}\{u\}$, then $x = \beta u$ for some $\beta \in F$, in which case we can write $x = \beta u + 0(\alpha u)$, which shows that x also belongs to $\text{sp}\{u, \alpha u\}$. Conversely, if $x \in \text{sp}\{u, \alpha u\}$, then there exist scalars $\beta, \gamma \in F$ such that $x = \beta u + \gamma(\alpha u)$. But then $x = (\beta + \gamma\alpha)u$, and therefore $x \in \text{sp}\{u\}$. Thus $\text{sp}\{u\} = \text{sp}\{u, \alpha u\}$.

16. Let V be a vector space over a field F, and suppose $x, u_1, \ldots, u_k, v_1, \ldots, v_\ell$ are vectors in V. Assume $x \in \mathrm{sp}\{u_1, \ldots, u_k\}$ and $u_j \in \mathrm{sp}\{v_1, \ldots, v_\ell\}$ for $j = 1, \ldots, k$. We wish to show that $x \in \mathrm{sp}\{v_1, \ldots, v_\ell\}$. Since $u_j \in \mathrm{sp}\{v_1, \ldots, v_\ell\}$, there exist scalars $\beta_{j,1}, \ldots, \beta_{j,\ell}$ such that $u_j = \beta_{j,1}v_1 + \cdots + \beta_{j,\ell}v_\ell$. This is true for each u_j, $j = 1, \ldots, k$. Also, $x \in \mathrm{sp}\{u_1, \ldots, u_k\}$, so there exist $\alpha_1, \ldots, \alpha_k \in F$ such that $x = \alpha_1 u_1 + \cdots + \alpha_k u_k$. It follows that

$$\begin{aligned}
x &= \alpha_1(\beta_{1,1}v_1 + \cdots + \beta_{1,\ell}v_\ell) + \alpha_2(\beta_{2,1}v_1 + \cdots + \beta_{2,\ell}v_\ell) + \cdots + \alpha_k(\beta_{k,1}v_1 + \cdots + \beta_{k,\ell}v_\ell) \\
&= \alpha_1\beta_{1,1}v_1 + \cdots + \alpha_1\beta_{1,\ell}v_\ell + \alpha_2\beta_{2,1}v_1 + \cdots + \alpha_2\beta_{2,\ell}v_\ell + \cdots + \alpha_k\beta_{k,1}v_1 + \cdots + \alpha_k\beta_{k,\ell}v_\ell \\
&= (\alpha_1\beta_{1,1} + \alpha_2\beta_{2,1} + \cdots + \alpha_k\beta_{k,1})v_1 + (\alpha_1\beta_{1,2} + \alpha_2\beta_{2,2} + \cdots + \alpha_k\beta_{k,2})v_2 + \cdots + \\
&\quad (\alpha_1\beta_{1,\ell} + \alpha_2\beta_{2,\ell} + \cdots + \alpha_k\beta_{k,\ell})v_\ell.
\end{aligned}$$

This shows that $x \in \mathrm{sp}\{v_1, \ldots, v_\ell\}$.

17. (a) Let V be a vector space over $\mathbf{R}$, and let u, v be any two vectors in V. We wish to prove that $\mathrm{sp}\{u, v\} = \mathrm{sp}\{u+v, u-v\}$. We first suppose that $x \in \mathrm{sp}\{u+v, u-v\}$, say $x = \alpha(u+v) + \beta(u-v)$. Then $x = \alpha u + \alpha v + \beta u - \beta v = (\alpha+\beta)u + (\alpha-\beta)v$, which shows that $x \in \mathrm{sp}\{u, v\}$. Conversely, suppose that $x \in \mathrm{sp}\{u, v\}$, say $x = \alpha u + \beta v$. We notice that $u = (1/2)(u+v) + (1/2)(u-v)$, and $v = (1/2)(u+v) - (1/2)(u-v)$. Therefore, $x = \alpha((1/2)(u+v) + (1/2)(u-v)) + \beta((1/2)(u+v) - (1/2)(u-v)) = (\alpha/2 + \beta/2)(u+v) + (\alpha/2 - \beta/2)(u-v)$, which shows that $x \in \mathrm{sp}\{u+v, u-v\}$. Therefore, $x \in \mathrm{sp}\{u, v\}$ if and only if $x \in \mathrm{sp}\{u+v, u-v\}$, and hence the two subspaces are equal.

    (b) The result just proved does not necessarily hold if V is a vector space over an arbitrary field F. More specifically, the first part of the proof is always valid, and therefore $\mathrm{sp}\{u+v, u-v\} \subset \mathrm{sp}\{u, v\}$ always holds. However, it is not always possible to write u and v in terms of $u+v$ and $u-v$, and therefore $\mathrm{sp}\{u, v\} \subset \mathrm{sp}\{u+v, u-v\}$ need not hold. For example, if $F = \mathbf{Z}_2$, $V = \mathbf{Z}_2^2$, $u = (1, 0)$, $v = (0, 1)$, then we have $u + v = (1, 1)$ and $u - v = (1, 1)$ (since $-1 = 1$ in $\mathbf{Z}_2$). It follows that $\mathrm{sp}\{u+v, u-v\} = \{(0,0), (1,1)\}$, and hence $u, v \notin \mathrm{sp}\{u+v, u-v\}$, which in turn means that $\mathrm{sp}\{u, v\} \not\subset \mathrm{sp}\{u+v, u-v\}$.

2.5 Linear independence

1. Let V be a vector space over a field F, and let $u_1, u_2 \in V$. We wish to prove that $\{u_1, u_2\}$ is linearly dependent if and only if one of these vectors is a multiple of the other. Suppose first that $\{u, v\}$ is linearly dependent. Then there exist scalars α_1, α_2, not both zero, such that $\alpha_1 u_1 + \alpha_2 u_2 = 0$. Suppose $\alpha_1 \neq 0$; then α_1^{-1} exists, and we have $\alpha_1 u_1 + \alpha_2 u_2 = 0 \Rightarrow \alpha_1 u_1 = -\alpha_2 u_2 \Rightarrow u_1 = -\alpha_1^{-1}\alpha_2 u_2$. Therefore, in this case, u_1 is a multiple of u_2. Similarly, if $\alpha_2 \neq 0$, we can show that u_2 is a multiple of u_1. Conversely, suppose one of u_1, u_2 is a multiple of the other, say $u_1 = \alpha u_2$. We can then write $u_1 - \alpha u_2 = 0$, or $1 \cdot u_1 + (-\alpha)u_2 = 0$, which, since $1 \neq 0$, shows that $\{u_1, u_2\}$ is linearly dependent. A similar proof shows that if u_2 is a multiple of u_1, then $\{u_1, u_2\}$ is linearly dependent. This completes the proof.

2. Let V be a vector space over a field F, and suppose $v \in V$. We wish to prove that $\{v\}$ is linearly independent if and only if $v \neq 0$. First, if $v \neq 0$, then $\alpha v = 0$ implies that $\alpha = 0$ by Theorem 5. It follows that $\{v\}$ is linearly independent if $v \neq 0$. On the other hand, if $v = 0$, then $1 \cdot v = 0$, which shows that $\{v\}$ is linearly dependent (there is a nontrivial solution to $\alpha v = 0$). Thus $\{v\}$ is linearly independent if and only if $v \neq 0$.

3. Let V be a vector space over a field F, and let $u_1, \ldots, u_n \in V$. Suppose $u_i = 0$ for some i, $1 \leq i \leq n$, and define scalars $\alpha_1, \ldots, \alpha_n \in F$ by $\alpha_k = 0$ if $k \neq i$, $\alpha_i = 1$. Then $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0 \cdot u_1 + \cdots + 0 \cdot u_{i-1} + 1 \cdot 0 + 0 \cdot u_{i+1} + \cdots + 0 \cdot u_n = 0$, and hence there is a nontrivial solution to $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0$. This shows that $\{u_1, \ldots, u_n\}$ is linearly dependent.

4. Let V be a vector space over a field F, let $\{u_1, \ldots, u_k\}$ be a linearly independent subspace of V, and assume $v \in V$, $v \notin \mathrm{sp}\{u_1, \ldots, u_k\}$. We wish to show that $\{u_1, \ldots, u_k, v\}$ is also linearly independent. We argue by contradiction and assume that $\{u_1, \ldots, u_k, v\}$ is linearly dependent. Then there exist scalars

$\alpha_1, \ldots, \alpha_k, \beta$, not all zero, such that $\alpha_1 u_1 + \cdots + \alpha_k u_k + \beta v = 0$. We now consider two cases. First, if $\beta = 0$, then not all of $\alpha_1, \ldots, \alpha_k$ are zero, and we see that $\alpha_1 u_1 + \cdots + \alpha_k u_k = \alpha_1 u_1 + \cdots + \alpha_k u_k + 0 \cdot v = 0$. This contradicts the fact that $\{u_1, \ldots, u_k\}$ is linearly independent. Second, if $\beta \neq 0$, then we can solve $\alpha_1 u_1 + \cdots + \alpha_k u_k + \beta v = 0$ to obtain $v = -\beta^{-1}\alpha_1 u_1 - \cdots - \beta^{-1}\alpha_k u_k$, which contradicts that $v \notin \mathrm{sp}\{u_1, \ldots, u_k\}$. Thus, in either case, we obtain a contradiction, and the proof is complete.

5. We wish to determine whether each of the following sets is linearly independent or not.

   (a) The set $\{(1,2),(1,-1)\} \subset \mathbf{R}^2$ is linearly independent by Exercise 1, since neither vector is a multiple of the other.

   (b) The set $\{(-1,-1,4),(-4,-4,17),(1,1,-3)\}$ is linearly dependent. Solving
   $$\alpha_1(-1,-1,4) + \alpha_2(-4,-4,17) + \alpha_3(1,1,-3) = 0$$
   shows that $\alpha_1 = 5, \alpha_2 = -1, \alpha_3 = 1$ is a nontrivial solution.

   (c) The set $\{(-1,3,-2),(3,-10,7),(-1,3,-1)\}$ is linearly independent. Solving
   $$\alpha_1(-1,3,-2) + \alpha_2(3,-10,7) + \alpha_3(-1,3,-1) = 0$$
   shows that the only solution is $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

6. We wish to determine whether each of the following sets of polynomials is linearly independent or not.

   (a) The set $\{1 - x^2, x + x^2, 3 + 3x - 4x^2\} \subset \mathcal{P}_2$ is linearly independent since the only solution to $\alpha_1(1 - x^2) + \alpha_2(x + x^2) + \alpha_3(3 + 3x - 4x^2) = 0$ is $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

   (b) The set $\{1 + x^2, 4 + 3x^2 + 3x^3, 3 - x + 10x^3, 1 + 7x^2 - 18x^3\} \subset \mathcal{P}_3$ is linearly dependent. Solving $\alpha_1(1 + x^2) + \alpha_2(4 + 3x^2 + 3x^3) + \alpha_3(3 - x + 10x^3) + \alpha_4(1 + 7x^2 - 18x^3) = 0$ yields a nontrivial solution $\alpha_1 = -25$, $\alpha_2 = 6$, $\alpha_3 = 0$, $\alpha_4 = 1$.

7. The set $\{e^x, e^{-x}, \cosh(x)\} \subset C[0,1]$ is linearly dependent since $(1/2)e^x + (1/2)e^{-x} - \cosh(x) = 0$ for all $x \in [0,1]$.

8. The subset $\{(0,1,2),(1,2,0),(2,0,1)\}$ of $\mathbf{Z}_3^3$ is linearly dependent because $1 \cdot (0,1,2) + 1 \cdot (1,2,0) + 1 \cdot (2,0,1) = (0,0,0)$.

9. We wish to show that $\{1, x, x^2\}$ is linearly dependent in $\mathcal{P}_2(\mathbf{Z}_2)$. The equation $\alpha_1 \cdot 1 + \alpha_2 x + \alpha_3 x^2 = 0$ has the nontrivial solution $\alpha_1 = 0, \alpha_2 = 1, \alpha_3 = 1$. To verify this, we must simply verify that $x + x^2$ is the zero function in $\mathcal{P}_2(\mathbf{Z}_2)$. Substituting $x = 0$, we obtain $0 + 0^2 = 0 + 0 = 0$, and with $x = 1$, we obtain $1 + 1^2 = 1 + 1 = 0$.

10. The set $\{(i,1,2i),(1,1+i,i),(1,3+5i,-4+3i)\} \subset \mathbf{C}^3$ is linearly dependent, because $\alpha_1(i,1,2i) + \alpha_2(1,1+i,i) + \alpha_3(1,3+5i,-4+3i) = (0,0,0)$ has the nontrivial solution $\alpha_1 = -2i, \alpha_2 = -3, \alpha_3 = 1$.

11. We have already seen that $\{(3,2,2,3),(3,2,1,2),(3,2,0,1)\} \subset \mathbf{R}^4$ is linearly dependent, because $(3,2,2,3) - 2(3,2,1,2) + (3,2,0,1) = (0,0,0,0)$.

    (a) We can solve this equation for any one of the vectors in terms of the other two; for instance, $(3,2,2,3) = 2(3,2,1,2) - (3,2,0,1)$.

    (b) We can show that $(-3,-2,2,1) \in \mathrm{sp}\{(3,2,2,3),(3,2,1,2),(3,2,0,1)\}$ by solving $\alpha_1(3,2,2,3) + \alpha_2(3,2,1,2) + \alpha_3(3,2,0,1) = (-3,-2,2,1)$. One solution is $(-3,-2,2,1) = 3(3,2,2,3) - 4(3,2,1,2)$. Substituting $(3,2,2,3) = 2(3,2,1,2) - (3,2,0,1)$, we obtain another solution: $(-3,-2,2,1) = 2(3,2,1,2) - 3(3,2,0,1)$.

12. We wish to show that $\{(-1,1,3),(1,-1,-2),(-3,3,13)\} \subset \mathbf{R}^3$ is linearly dependent by writing one of the vectors as a linear combination of the others. We will try to solve for the third vector in terms of the other two. (There is an element of trial and error involved here: Even if the three vectors form a linearly independent set, there is no guarantee that this will work; it could be, for instance, that the first two vectors form a linearly dependent set and the third vector does not lie in the span of the first two.) Solving $\alpha_1(-1,1,3)+\alpha_2(1,-1,-2)=(-3,3,13)$ yields a unique solution: $(-3,3,13)=7(-1,1,3)+4(1,-1,-2)$. This shows that the set is linearly dependent.

    Alternate solution: We begin by solving $\alpha_1(-1,1,3)+\alpha_2(1,-1,-2)+\alpha_3(-3,3,13)=(0,0,0)$ to obtain $7(-1,1,3)+4(1,-1,-2)-(-3,3,13)=(0,0,0)$. We can easily solve this for the third vector: $(-3,3,13)=7(-1,1,3)+4(1,-1,-2)$.

13. We wish to show that $\{p_1,p_2,p_3\}$, where $p_1(x)=1-x^2$, $p_2(x)=1+x-6x^2$, $p_3(x)=3-2x^2$, is linearly independent and spans $\mathcal{P}_2$. We first verify that the set is linearly independent by solving $\alpha_1(1-x^2)+\alpha_2(1+x-6x^2)+\alpha_3(3-2x^2)=0$. This equation is equivalent to the system $\alpha_1+\alpha_2+3\alpha_2=0$, $\alpha_2=0$, $-\alpha_1-6\alpha_2-2\alpha_3=0$, and a direct calculation shows that the only solution is $\alpha_1=\alpha_2=\alpha_3=0$. To show that the set spans $\mathcal{P}_2$, we take an arbitrary $p\in\mathcal{P}_2$, say $p(x)=c_0+c_1x+c_2x^2$, and solve $\alpha_1(1-x^2)+\alpha_2(1+x-6x^2)+\alpha_3(3-2x^2)=c_0+c_1x+c_2x^2$. This is equivalent to the system $\alpha_1+\alpha_2+3\alpha_2=c_0$, $\alpha_2=c_1$, $-\alpha_1-6\alpha_2-2\alpha_3=c_2$. There is a unique solution: $\alpha_1=-2c_0-16c_1-3c_2$, $\alpha_2=c_1$, $\alpha_3=c_0+5c_1+c_2$. This shows that $p\in\mathrm{sp}\{p_1,p_2,p_3\}$, and, since p was arbitrary, that $\{p_1,p_2,p_3\}$ spans all of $\mathcal{P}_2$.

14. Let V be a vector space over a field F and let $\{u_1,\ldots,u_k\}$ be a linearly independent subset of V. Suppose $u,v\in V$, $\{u,v\}$ is linearly independent, and $u,v\not\in\mathrm{sp}\{u_1,\ldots,u_k\}$. We wish to determine whether $\{u_1,\ldots,u_k,u,v\}$ is necessarily linearly independent. In fact, this set need not be linearly independent. For example, take $V=\mathbf{R}^4$, $F=\mathbf{R}$, $k=3$, and $u_1=(1,0,0,0)$, $u_2=(0,1,0,0)$, $u_3=(0,0,1,0)$. With $u=(0,0,0,1)$, $v=(1,1,1,1)$, we see immediately that $\{u,v\}$ is linearly independent (neither vector is a multiple of the other), and that neither u nor v belongs to $\mathrm{sp}\{u_1,u_2,u_3\}$. Nevertheless, $\{u_1,u_2,u_3,u,v\}$ is linear dependent because $v=u_1+u_2+u_3+u$.

15. Let V be a vector space over a field F, and suppose S and T are subspaces of V satisfying $S\cap T=\{0\}$. Suppose $\{s_1,\ldots,s_k\}\subset S$ and $\{t_1,\ldots,t_\ell\}\subset T$ are both linearly independent sets. We wish to prove that $\{s_1,\ldots,s_k,t_1,\ldots,t_\ell\}$ is linearly independent. Suppose scalars $\alpha_1,\ldots,\alpha_k$, $\beta_1,\ldots,\beta_\ell$ satisfy $\alpha_1s_1+\cdots+\alpha_ks_k+\beta_1t_1+\cdots+\beta_\ell t_\ell=0$. We can rearrange this equation to read $\alpha_1s_1+\cdots+\alpha_ks_k=-\beta_1t_1-\cdots-\beta_\ell t_\ell$. If v is the vector represented by these two expressions, then $v\in S$ (since v is a linear combination of $s_1,\ldots,s_k$) and $v\in T$ (since v is a linear combination of $t_1,\ldots,t_\ell$). But the only vector in $S\cap T$ is the zero vector, and hence $\alpha_1s_1+\cdots+\alpha_ks_k=0$, $-\beta_1t_1-\cdots-\beta_\ell t_\ell=0$. The first equation implies that $\alpha_1=\cdots=\alpha_k=0$ (since $\{s_1,\ldots,s_k\}$ is linearly independent), while the second equation implies that $\beta_1=\cdots=\beta_\ell=0$ (since $\{t_1,\ldots,t_\ell\}$ is linearly independent). Therefore, $\alpha_1s_1+\cdots+\alpha_ks_k+\beta_1t_1+\cdots+\beta_\ell t_\ell=0$ implies that all the scalars are zero, and hence $\{s_1,\ldots,s_k,t_1,\ldots,t_\ell\}$ is linearly independent.

16. Let V be a vector space over a field F, and let $\{u_1,\ldots,u_k\}$ and $\{v_1,\ldots,v_\ell\}$ be two linearly independent subsets of V. We wish to find a condition that implies that $\{u_1,\ldots,u_k,v_1,\ldots,v_\ell\}$ is linearly independent. By the previous exercise, a sufficient condition for $\{u_1,\ldots,u_k,v_1,\ldots,v_\ell\}$ to be linearly independent is that $S=\mathrm{sp}\{u_1,\ldots,u_k\}$, $T=\mathrm{sp}\{v_1,\ldots,v_\ell\}$ satisfy $S\cap T=\{0\}$. We will prove that this condition is also necessary. Suppose $\{u_1,\ldots,u_k\}$ and $\{v_1,\ldots,v_\ell\}$ are linearly independent subsets of V, and that $\{u_1,\ldots,u_k,v_1,\ldots,v_\ell\}$ is also linearly independent. Define S and T as above. If $x\in S\cap T$, then there exist scalars $\alpha_1,\ldots,\alpha_k\in F$ such that $x=\alpha_1u_1+\cdots+\alpha_ku_k$ (since $x\in S$), and also scalars $\beta_1,\ldots,\beta_\ell\in F$ such that $x=\beta_1v_1+\cdots+\beta_\ell v_\ell$ (since $x\in T$). But then $\alpha_1u_1+\cdots+\alpha_ku_k=\beta_1v_1+\cdots+\beta_\ell v_\ell$, which implies that $\alpha_1u_1+\cdots+\alpha_ku_k-\beta_1v_1-\cdots-\beta_\ell v_\ell=0$. Since $\{u_1,\ldots,u_k,v_1,\ldots,v_\ell\}$ is linearly independent by assumption, this implies that $\alpha_1=\cdots=\alpha_k=\beta_1=\cdots=\beta_\ell=0$, which in turn shows that $x=0$. Therefore $S\cap T=\{0\}$, and the proof is complete.

17. (a) Let V be a vector space over $\mathbf{R}$, and suppose $\{x,y,z\}$ is a linearly independent subset of V. We wish to show that $\{x+y,y+z,x+z\}$ is also linearly independent. Let $\alpha_1,\alpha_2,\alpha_3\in\mathbf{R}$ satisfy $\alpha_1(x+y)+$

$\alpha_2(y+z)+\alpha_3(x+z)=0$. This equation is equivalent to $(\alpha_1+\alpha_3)x+(\alpha_1+\alpha_2)y+(\alpha_2+\alpha_3)z=0$. Since $\{x,y,z\}$ is linearly independent, it follows that $\alpha_1+\alpha_3=\alpha_1+\alpha_2=\alpha_2+\alpha_3=0$. This system can be solved directly to show that $\alpha_1=\alpha_2=\alpha_3=0$, which proves that $\{x+y,y+z,x+z\}$ is linearly independent.

(b) We now show, by example, that the previous result is not necessarily true if V is a vector space over some field $F\neq\mathbf{R}$. Let $V=\mathbf{Z}_2^3$, and define $x=(1,0,0)$, $y=(0,1,0)$, and $z=(0,0,1)$. Obviously $\{x,y,z\}$ is linearly independent. On the other hand, we have $(x+y)+(y+z)+(x+z)=(1,1,0)+(0,1,1)+(1,0,1)=(1+0+1,1+1+0,0+1+1)=(0,0,0)$, which shows that $\{x+y,y+z,x+z\}$ is linearly dependent.

18. Let U and V be vector spaces over a field F, and define $W=U\times V$. Suppose $\{u_1,\ldots,u_k\}\subset U$ and $\{v_1,\ldots,v_\ell\}\subset V$ are linearly independent. We wish to show that $\{(u_1,0),\ldots,(u_k,0),(0,v_1),\ldots,(0,v_\ell)\}$ is also linearly independent. Suppose $\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_\ell\in F$ satisfy $\alpha_1(u_1,0)+\cdots+\alpha_k(u_k,0)+\beta_1(0,v_1)+\cdots+\beta_\ell(0,v_\ell)=(0,0)$. This reduces to $(\alpha_1u_1+\cdots+\alpha_ku_k,\beta_1v_1+\cdots+\beta_\ell v_\ell)=(0,0)$, which holds if and only if $\alpha_1u_1+\cdots+\alpha_ku_k=0$ and $\beta_1v_1+\cdots+\beta_\ell v_\ell=0$. Since $\{u_1,\ldots,u_k\}$ is linearly independent, the first equation implies that $\alpha_1=\cdots=\alpha_k=0$, and, since $\{v_1,\ldots,v_\ell\}$ is linearly independent, the second implies that $\beta_1=\cdots=\beta_\ell=0$. Since all the scalars are necessarily zero, we see that $\{(u_1,0),\ldots,(u_k,0),(0,v_1),\ldots,(0,v_\ell)\}$ is linearly independent.

19. Let V be a vector space over a field F, and let $u_1,u_2,\ldots,u_n$ be vectors in V. Suppose a nonempty subset of $\{u_1,u_2,\ldots,u_n\}$, say $\{u_{i_1},\ldots,u_{i_k}\}$, is linearly dependent. (Here $1\leq k<n$ and $i_1,\ldots,i_k$ are distinct integers each satisfying $1\leq i_j\leq n$.) We wish to prove that $\{u_1,u_2,\ldots,u_n\}$ itself is linearly dependent. By assumption, there exist scalars $\alpha_{i_1},\ldots,\alpha_{i_k}\in F$, not all zero, such that $\alpha_{i_1}u_{i_1}+\cdots+\alpha_{i_k}u_{i_k}=0$. For each $i\in\{1,\ldots,n\}\setminus\{i_1,\ldots,i_k\}$, define $\alpha_i=0$. Then we have $\alpha_1u_1+\cdots+\alpha_nu_n=0+\alpha_{i_1}u_{i_1}+\cdots+\alpha_{i_k}u_{i_k}=0$, and not all of $\alpha_1,\ldots,\alpha_n$ are zero since at least one α_{i_j} is nonzero. This shows that $\{u_1,\ldots,u_n\}$ is linearly dependent.

20. Let V be a vector space over a field F, and suppose $\{u_1,u_2,\ldots,u_n\}$ is a linearly independent subset of V. We wish to prove that every nonempty subset of $\{u_1,u_2,\ldots,u_n\}$ is also linearly independent. The result to be proved is simply the contrapositive of the statement in the previous exercise, and therefore holds by the previous proof.

21. Let V be a vector space over a field F, and suppose $\{u_1,u_2,\ldots,u_n\}$ is linearly dependent. We wish to prove that, given any i, $1\leq i\leq n$, either u_i is a linear combination of $u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_n$ or these vectors form a linearly dependent set. By assumption, there exist scalars $\alpha_1,\ldots,\alpha_n\in F$, not all zero, such that $\alpha_1u_1+\cdots+\alpha_iu_i+\cdots+\alpha_nu_n=0$. We now consider two cases. If $\alpha_i\neq0$, the we can solve the latter equation for u_i to obtain $u_i=-\alpha_i^{-1}\alpha_1u_1-\cdots-\alpha_i^{-1}\alpha_{i-1}u_{i-1}-\alpha_i^{-1}\alpha_{i+1}u_{i+1}-\cdots-\alpha_i^{-1}\alpha_nu_n$. In this case, u_i is a linear combination of the remaining vectors. The second case is that $\alpha_i=0$, in which case at least one of $\alpha_1,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_n$ is nonzero, and we have $\alpha_1u_1+\cdots+\alpha_{i-1}u_{i-1}+\alpha_{i+1}u_{i+1}+\cdots+\alpha_nu_n=0$. This shows that $\{u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_n\}$ is linearly dependent.

2.6 Basis and dimension

1. Suppose $\{v_1,v_2,\ldots,v_n\}$ is a basis for a vector space V.

(a) We wish to show that if any v_j is removed from the basis, the resulting set of $n-1$ vectors does not span V and hence is not a basis. This follows from Theorem 24: Since $\{v_1,v_2,\ldots,v_n\}$ is linearly independent, no v_j, $j=1,2,\ldots,n$, can be written as a linear combination of the remaining vectors. Therefore,

$$v_j\notin\mathrm{sp}\{v_1,\ldots,v_{j-1},v_{j+1},\ldots,v_n\},$$

which proves the desired result.

(b) Now we wish to show that if any vector $u\in V$, $u\notin\{v_1,v_2,\ldots,v_n\}$, is added to the basis, the resulting set of $n+1$ vectors is linearly dependent. This is immediate from Theorem 34: Since the dimension of V is n, every set containing more than n vectors is linearly dependent. Since $\{v_1, v_2, \ldots, v_n, u\}$ contains $n+1$ vectors, it must be linearly dependent.

2. Consider the following vectors in $\mathbf{R}^3$: $v_1 = (-1, 4, -2)$, $v_2 = (5, -20, 9)$, $v_3 = (2, -7, 6)$. We wish to determine if $\{v_1, v_2, v_3\}$ is a basis for $\mathbf{R}^3$. If we solve $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = x$ for an arbitrary $x \in \mathbf{R}^3$, we find a unique solution: $\alpha_1 = 57x_1 + 12x_2 - 5x_3$, $\alpha_2 = 10x_1 + 2x_2 - x_3$ $\alpha_3 = 4x_1 + x_2$. By Theorem 28, this implies that $\{v_1, v_2, v_3\}$ is a basis for $\mathbf{R}^3$.

3. We now repeat the previous exercise for the vectors $v_1 = (-1, 3, -1)$, $v_2 = (1, -2, -2)$, $v_3 = (-1, 7, -13)$. If we try to solve $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = x$ for an arbitrary $x \in \mathbf{R}^3$, we find that this equation is equivalent to the following system:

$$\begin{aligned} -\alpha_1 + \alpha_2 - \alpha_3 &= x_1 \\ \alpha_2 + 4\alpha_3 &= 3x_1 + x_2 \\ 0 &= 8x_1 + 3x_2 + x_3. \end{aligned}$$

Since this system is inconsistent for most $x \in \mathbf{R}^3$ (the system is consistent only if x happens to satisfy $8x_1 + 3x_2 + x_3 = 0$), $\{v_1, v_2, v_3\}$ does not span $\mathbf{R}^3$ and therefore is not a basis.

4. Let $S = \mathrm{sp}\{e^x, e^{-x}\}$ be regarded as a subspace of $C(\mathbf{R})$. We will show that $\{e^x, e^{-x}\}$, $\{\cosh(x), \sinh(x)\}$ are two different bases for S. First, to verify that $\{e^x, e^{-x}\}$ is a basis, we merely need to verify that it is linearly independent (since it spans S by definition). This can be done as follows: If $c_1 e^x + c_2 e^{-x} = 0$, where 0 represents the zero function, then the equation must hold for all values of $x \in \mathbf{R}$. So choose $x = 0$ and $x = \ln 2$; then c_1 and c_2 must satisfy

$$\begin{aligned} c_1 + c_2 &= 0, \\ 2c_1 + \frac{1}{2}c_2 &= 0. \end{aligned}$$

It is straightforward to show that the only solution of this system is $c_1 = c_2 = 0$, and hence $\{e^x, e^{-x}\}$ is linearly independent.

Next, since

$$\cosh(x) = \frac{1}{2}e^x + \frac{1}{2}e^{-x}, \ \cosh(x) = \frac{1}{2}e^x - \frac{1}{2}e^{-x},$$

we see that $\cosh(x), \sinh(x) \in S = \mathrm{sp}\{e^x, e^{-x}\}$. We can verify that $\{\cosh(x), \sinh(x)\}$ is linearly independent directly: If $c_1 \cosh(x) + c_2 \sinh(x) = 0$, then, substituting $x = 0$ and $x = \ln 2$, we obtain the system

$$1 \cdot c_1 + 0 \cdot c_2 = 0, \ \frac{5}{4}c_1 + \frac{3}{4}c_2 = 0,$$

and the only solution is $c_1 = c_2 = 0$. Thus $\{\cosh(x), \sinh(x)\}$ is linearly independent. Finally, let f be any function in S. Then, by definition, f can be written as $f(x) = \alpha_1 e^x + \alpha_2 e^{-x}$ for some $\alpha_1, \alpha_2 \in \mathbf{R}$. We must show that $f \in \mathrm{sp}\{\cosh(x), \sinh(x)\}$, that is, that there exist $c_1, c_2 \in \mathbf{R}$ such that

$$c_1 \cosh(x) + c_2 \sinh(x) = f(x).$$

This equation can be manipulated as follows:

$$\begin{aligned} & c_1 \cosh(x) + c_2 \sinh(x) = f(x) \\ \Leftrightarrow\ & c_1 \left(\frac{1}{2}e^x + \frac{1}{2}e^{-x}\right) + c_2 \left(\frac{1}{2}e^x - \frac{1}{2}e^{-x}\right) = \alpha_1 e^x + \alpha_2 e^{-x} \\ \Leftrightarrow\ & \left(\frac{1}{2}c_1 + \frac{1}{2}c_2\right) e^x + \left(\frac{1}{2}c_1 - \frac{1}{2}c_2\right) e^{-x} = \alpha_1 e^x + \alpha_2 e^{-x}. \end{aligned}$$

Since $\{\{e^x, e^{-x}\}$ is linearly independent, Theorem 26 implies that the last equation can hold only if

$$\frac{1}{2}c_1 + \frac{1}{2}c_2 = \alpha_1,\ \frac{1}{2}c_1 - \frac{1}{2}c_2\alpha_2.$$

This last system has a unique solution:

$$c_1 = \alpha_1 + \alpha_2,\ c_2 = \alpha_1 - \alpha_2.$$

This shows that $f \in \mathrm{sp}\{\cosh(x), \sinh(x)\}$, and the proof is complete.

5. Let $p_1(x) = 1 - 4x + 4x^2$, $p_2(x) = x + x^2$, $p_3(x) = -2 + 11x - 6x^2$. We will determine whether $\{p_1, p_2, p_3\}$ is a basis for $\mathcal{P}_2$ or not by solving $\alpha_1 p_1(x) + \alpha_2 p_2(x) + \alpha_3 p_3(x) = c_0 + c_1 x + c_2 x^2$, where $c_0 + c_1 x + c_2 x^2$ is an arbitrary element of $\mathcal{P}_2$. A direct calculation shows that there is a unique solution for α_1, α_2, α_3:

$$\alpha_1 = 17c_0 + 2c_1 - 2c_2,\ \alpha_2 = 3c_2 - 2c_1 - 20c_0,\ \alpha_3 = 8c_0 + c_1 - c_2.$$

By Theorem 28, it follows that $\{p_1, p_2, p_3\}$ is a basis for $\mathcal{P}_2$.

6. Let $p_1(x) = 1 - x^2$, $p_2(x) = 2 + x$, $p_3(x) = x + 2x^2$. We will determine whether $\{p_1, p_2, p_3\}$ a basis for $\mathcal{P}_2$ by trying to solve
$$\alpha_1 p_1(x) + \alpha_2 p_2(x) + \alpha_3 p_3(x) = c_0 + c_1 x + c_2 x^2,$$
where c_0, c_1, c_2 are arbitrary real numbers. This equation is equivalent to the system
$$\begin{aligned} \alpha_1 + 2\alpha_2 &= c_0, \\ \alpha_2 + \alpha_3 &= c_1, \\ -\alpha_1 + 2\alpha_3 &= c_2. \end{aligned}$$
Solving this system by elimination leads to
$$\begin{aligned} \alpha_1 + 2\alpha_2 &= c_0, \\ \alpha_2 + \alpha_3 &= c_1, \\ 0 &= c_0 - 2c_1 + c_2, \end{aligned}$$
which is inconsistent for most values of c_0, c_1, c_2. Therefore, $\{p_1, p_2, p_3\}$ does not span $\mathcal{P}_2$ and hence is not a basis for $\mathcal{P}_2$.

7. Consider the subspace $S = \mathrm{sp}\{p_1, p_2, p_3, p_4, p_5\}$ of $\mathcal{P}_3$, where
$$\begin{aligned} &p_1(x) = -1 + 4x - x^2 + 3x^3,\ p_2(x) = 2 - 8x + 2x^2 - 5x^3, \\ &p_3(x) = 3 - 11x + 3x^2 - 8x^3,\ p_4(x) = -2 + 8x - 2x^2 - 3x^3, \\ &p_5(x) = 2 - 8x + 2x^2 + 3x^3. \end{aligned}$$
   (a) The set $\{p_1, p_2, p_3, p_4, p_5\}$ is linearly dependent (by Theorem 34) because it contains five elements and the dimension of $\mathcal{P}_3$ is only four.
   (b) As illustrated in Example 39, we begin by solving
   $$\alpha_1 p_1(x) + \alpha_2 p_2(x) + \alpha_3 p_3(x) + \alpha_4 p_4(x) + \alpha_5 p_5(x) = 0;$$
   this is equivalent to the system
   $$\begin{aligned} -\alpha_1 + 2\alpha_2 + 3\alpha_3 - 2\alpha_4 + 2\alpha_5 &= 0, \\ 4\alpha_1 - 8\alpha_2 - 11\alpha_3 + 8\alpha_4 - 8\alpha_5 &= 0, \\ -\alpha_1 + 2\alpha_2 + 3\alpha_3 - 2\alpha_4 + 2\alpha_5 &= 0, \\ 3\alpha_1 - 5\alpha_2 - 8\alpha_3 - 3\alpha_4 + 3\alpha_5 &= 0, \end{aligned}$$

which reduces to

$$\begin{aligned}\alpha_1 &= 16\alpha_4 - 16\alpha_5,\\ \alpha_2 &= 9\alpha_4 - 9\alpha_5,\\ \alpha_3 &= 0.\end{aligned}$$

Since there are nontrivial solutions, $\{p_1, p_2, p_3, p_4, p_5\}$ is linearly dependent (which we already knew), but we can deduce more than that. By taking $\alpha_4 = 1$, $\alpha_5 = 0$, we see that $\alpha_1 = 16$, $\alpha_2 = 9$, $\alpha_3 = 0$, $\alpha_4 = 1$, $\alpha_5 = 0$ is one solution, which means that

$$16p_1(x) + 9p_2(x) + p_4(x) = 0 \;\Rightarrow\; p_4(x) = -16p_1(x) - 9p_2(x).$$

This shows that $p_4 \in \mathrm{sp}\{p_1, p_2\} \subset \mathrm{sp}\{p_1, p_2, p_3\}$. Similarly, taking $\alpha_4 = 0$, $\alpha_5 = 0$, we find that

$$-16p_1(x) - 9p_2(x) + p_5(x) = 0 \;\Rightarrow\; p_5(x) = 16p_1(x) + 9p_2(x),$$

and hence $p_5 \in \mathrm{sp}\{p_1, p_2\} \subset \mathrm{sp}\{p_1, p_2, p_3\}$. It follows from Lemma 19 that $\mathrm{sp}\{p_1, p_2, p_3, p_4, p_5\} = \mathrm{sp}\{p_1, p_2, p_3\}$. Our calculations above show that $\{p_1, p_2, p_3\}$ is linearly independent (if $\alpha_4 = \alpha_5 = 0$, then also $\alpha_1 = \alpha_2 = \alpha_3 = 0$). Therefore, $\{p_1, p_2, p_3\}$ is a linearly independent spanning set of S and hence a basis for S.

8. We wish to find a basis for $\mathrm{sp}\{(1, 2, 1), (0, 1, 1), (1, 1, 0)\} \subset \mathbf{R}^3$. We will name the vectors v_1, v_2, v_3, respectively, and begin by testing the linear independence of $\{v_1, v_2, v_3\}$. The equation $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$ is equivalent to

$$\begin{aligned}\alpha_1 + \alpha_3 &= 0,\\ 2\alpha_2 + \alpha_2 + \alpha_3 &= 0,\\ \alpha_1 + \alpha_2 &= 0,\end{aligned}$$

which reduces to

$$\alpha_1 = -\alpha_3,\ \alpha_2 = \alpha_3.$$

One solution is $\alpha_1 = -1$, $\alpha_2 = 1$, $\alpha_3 = 1$, which shows that $-v_1 + v_2 + v_3 = 0$, or $v_3 = v_1 - v_2$. This in turns shows that $\mathrm{sp}\{v_1, v_2, v_3\} = \mathrm{sp}\{v_1, v_2\}$ (by Lemma 19). Clearly $\{v_1, v_2\}$ is linearly independent (since neither vector is a multiple of the other), and hence $\{v_1, v_2\}$ is a basis for $\mathrm{sp}\{v_1, v_2, v_3\}$.

9. We wish to find a basis for $S = \mathrm{sp}\{(1, 2, 1, 2, 1), (1, 1, 2, 2, 1), (0, 1, 2, 0, 2)\}$ in $\mathbf{Z}_3^5$. The equation

$$\alpha_1(1, 2, 1, 2, 1) + \alpha_2(1, 1, 2, 2, 1) + \alpha_3(0, 1, 2, 0, 2) = (0, 0, 0, 0, 0)$$

is equivalent to the system

$$\begin{aligned}\alpha_1 + \alpha_2 &= 0,\\ 2\alpha_1 + \alpha_2 + \alpha_3 &= 0,\\ \alpha_1 + 2\alpha_2 + 2\alpha_3 &= 0,\\ 2\alpha_1 + 2\alpha_2 &= 0,\\ \alpha_1 + \alpha_2 + 2\alpha_3 &= 0.\end{aligned}$$

Reducing this system by Gaussian elimination (in modulo 3 arithmetic), we obtain

$$\alpha_1 = \alpha_2 = \alpha_3 = 0,$$

which shows that the given vectors form a linearly independent set and therefore a basis for S.

10. We will show that $\{1+x+x^2, 1-x+x^2, 1+x+2x^2\}$ is a basis for $\mathcal{P}_2(\mathbf{Z}_3)$ by showing that there is a unique solution to

$$\alpha_1\left(1+x+x^2\right)+\alpha_2\left(1-x+x^2\right)+\alpha_3\left(1+x+2x^2\right)=c_0+c_1x+c_2x^2.$$

We first note that $1-x+x^2=1+2x+x^2$ in $\mathcal{P}_2(\mathbf{Z}_3)$, so we can write our equation as

$$\alpha_1\left(1+x+x^2\right)+\alpha_2\left(1+2x+x^2\right)+\alpha_3\left(1+x+2x^2\right)=c_0+c_1x+c_2x^2.$$

We rearrange the previous equation in the form

$$(\alpha_1+\alpha_2+\alpha_3)+(\alpha_1+2\alpha_2+\alpha_3)x+(\alpha_1+\alpha_2+2\alpha_3)x^2=c_0+c_1x+c_2x^2.$$

Since the polynomials involved are of degree 2 and the field $\mathbf{Z}_3$ contains 3 elements, this last equation is is equivalent to the system

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3&=c_0,\\ \alpha_1+2\alpha_2+\alpha_3&=c_1,\\ \alpha_1+\alpha_2+2\alpha_3&=c_2\end{aligned}$$

(cf. the discussion on page 45 of the text). Applying Gaussian elimination (modulo 3) shows that there is a unique solution:

$$\begin{aligned}\alpha_1&=c_0+2c_1+c_2,\\ \alpha_2&=2c_0+c_1,\\ \alpha_3&=2c_0+c_2.\end{aligned}$$

This in turn proves (by Theorem 28) that the given polynomials form a basis for $\mathcal{P}_2(\mathbf{Z}_3)$.

11. Suppose F is a finite field with q distinct elements.

    (a) Assume $n\le q-1$. We wish to show that $\{1,x,x^2,\ldots,x^n\}$ is a linearly independent subset of $\mathcal{P}_n(F)$. (Since $\{1,x,x^2,\ldots,x^n\}$ clearly spans $\mathcal{P}_n(F)$, this will show that it is a basis for $\mathcal{P}_n(F)$, and hence that $\dim(\mathcal{P}_n(F))=n+1$ in the case that $n\le q-1$.) The desired conclusion follows from the discussion on page 45 of the text. If $c_0\cdot 1+c_1x+\cdots+c_nx^n=0$ (where 0 is the zero function), then every element of F is a root of $c_0\cdot 1+c_1x+\cdots+c_nx^n$. Since F contains more than n elements and a nonzero polynomial of degree n can have at most n distinct roots, this is impossible unless $c_0=c_1=\ldots=c_n=0$. Thus $\{1,x,\ldots,x^n\}$ is linearly independent.

    (b) Now suppose that $n\ge q$. The reasoning above shows that $\{1,x,x^2,\ldots,x^{q-1}\}$ is linearly independent in $\mathcal{P}_n(F)$ ($c_0\cdot 1+c_1x+\cdots+c_{q-1}x^{q-1}$ has at most $q-1$ distinct roots, and F contains more than $q-1$ elements, etc.). This implies that $\dim\left(\mathcal{P}_n(F)\right)\ge q$ in the case $n\ge q$.

12. Suppose V is a vector space over a field F, and S, T are two n-dimensional subspaces of V. We wish to prove that if $S\subset T$, then in fact $S=T$. Let $\{s_1,s_2,\ldots,s_n\}$ be a basis for S. Since $S\subset T$, this implies that $\{s_1,s_2,\ldots,s_n\}$ is a linearly independent subset of T. We will now show that $\{s_1,s_2,\ldots,s_n\}$ also spans T. Let $t\in T$ be arbitrary. Since T has dimension n, the set $\{s_1,s_2,\ldots,s_n,t\}$ is linearly dependent by Theorem 34. But then, by Lemma 33, t must be a linear combination of $s_1,s_2,\ldots,s_n$ (since no s_k is a linear combination of $s_1,s_2,\ldots,s_{k-1}$). This shows that $t\in\operatorname{sp}\{s_1,s_2,\ldots,s_n\}$, and hence we have shown that $\{s_1,s_2,\ldots,s_n\}$ is a basis for T. But then

$$T=\operatorname{sp}\{s_1,s_2,\ldots,s_n\}=S,$$

as desired.

13. Suppose V is a vector space over a field F, and S, T are two finite-dimensional subspaces of V with $S\subset T$. We are asked to prove that $\dim(S)\le\dim(T)$. Let $\{s_1,s_2,\ldots,s_n\}$ be a basis for S. Since $S\subset T$, it follows that $\{s_1,s_2,\ldots,s_n\}$ is a linearly independent subset of T, and hence, by Theorem 34, any basis for T must have at least n vectors. It follows that $\dim(T)\ge n=\dim(S)$.

14. **(Note: This exercise belongs in Section 2.7 since the most natural solution uses Theorem 43.)** Let V be a vector space over a field F, and let S and T be finite-dimensional subspaces of V. We wish to prove that

$$\dim(S+T)=\dim(S)+\dim(T)-\dim(S\cap T).$$

We know from Exercise 2.3.19 that $S\cap T$ is a subspace of V, and since it is a subset of S, $\dim(S\cap T)\leq\dim(S)$. Since S is finite-dimensional by assumption, it follows that $S\cap T$ is also finite-dimensional, and therefore either $S\cap T=\{0\}$ or $S\cap T$ has a basis.

Suppose first that $S\cap T=\{0\}$, so that $\dim(S\cap T)=0$. Let $\{s_1,s_2,\ldots,s_m\}$ be a basis for S and $\{t_1,t_2,\ldots,t_n\}$ be a basis for T. We will show that $\{s_1,\ldots,s_m,t_1,\ldots,t_n\}$ is a basis for $S+T$, from which it follows that

$$\dim(S+T)=m+n=m+n-0=\dim(S)+\dim(T)-\dim(S\cap T).$$

The set $\{s_1,\ldots,s_m,t_1,\ldots,t_n\}$ is linearly independent by Exercise 2.5.15. Given any $v\in S+T$, there exist $s\in S$, $t\in T$ such that $v=s+t$. But since $s\in S$, there exist scalars $\alpha_1,\ldots,\alpha_m\in F$ such that $s=\alpha_1s_1+\cdots+\alpha_ms_m$. Similarly, since $t\in T$, there exist $\beta_1,\ldots,\beta_n\in F$ such that $t=\beta_1t_1+\cdots+\beta_nt_n$. But then

$$v=s+t=\alpha_1s_1+\cdots+\alpha_ms_m+\beta_1t_1+\cdots+\beta_nt_n,$$

which shows that $v\in\mathrm{sp}\{s_1,\ldots,s_m,t_1,\ldots,t_n\}$. Thus we have shown that $\{s_1,\ldots,s_m,t_1,\ldots,t_n\}$ is a basis for $S+T$, which completes the proof in the case that $S\cap T=\{0\}$.

Now suppose $S\cap T$ is nontrivial, with basis $\{v_1,\ldots,v_k\}$. Since $S\cap T$ is a subset of S, $\{v_1,\ldots,v_k\}$ is a linearly independent subset of S and hence, by Theorem 43, can be extended to a basis $\{v_1,\ldots,v_k,s_1,\ldots,s_p\}$ of S. Similarly, $\{v_1,\ldots,v_k\}$ can be extended to a basis $\{v_1,\ldots,v_k,t_1,\ldots,t_q\}$ of T. We will show that $\{v_1,\ldots,v_k,s_1,\ldots,s_p,t_1,\ldots,t_q\}$ is a basis of $S+T$. Then we will have

$$\dim(S)=k+p,\ \dim(T)=k+q,\ \dim(S\cap T)=k$$

and

$$\dim(S+T)=k+p+q=(k+p)+(k+q)-k=\dim(S)+\dim(T)-\dim(S\cap T),$$

as desired. First, suppose $v\in S+T$. Then, by definition of $S+T$, there exist $s\in S$ and $t\in T$ such that $v=s+t$. Since $\{v_1,\ldots,v_k,s_1,\ldots,s_p\}$ is a basis for S, there exist scalars $\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_p\in F$ such that

$$s=\alpha_1v_1+\cdots+\alpha_kv_k+\beta_1s_1+\cdots+\beta_ps_p.$$

Similarly, there exist $\gamma_1,\ldots,\gamma_k,\delta_1,\ldots,\delta_q\in F$ such that

$$t=\gamma_1v_1+\cdots+\gamma_kv_k+\delta_1s_1+\cdots+\delta_qs_q.$$

But then

$$\begin{aligned}v=s+t&=\alpha_1v_1+\cdots+\alpha_kv_k+\beta_1s_1+\cdots+\beta_ps_p+\\&\quad\gamma_1v_1+\cdots+\gamma_kv_k+\delta_1s_1+\cdots+\delta_qs_q\\&=(\alpha_1+\gamma_1)v_1+\cdots+(\alpha_k+\gamma_k)v_k+\beta_1s_1+\cdots+\beta_ps_p+\\&\quad\delta_1t_1+\cdots+\delta_qt_q\\&\in\mathrm{sp}\{v_1,\ldots,v_k,s_1,\ldots,s_p,t_1,\ldots,t_q\}.\end{aligned}$$

This shows that $\{v_1,\ldots,v_k,s_1,\ldots,s_p,t_1,\ldots,t_q\}$ spans $S+T$. Now suppose $\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_p,\gamma_1,\ldots,\gamma_q\in F$ satisfy

$$\alpha_1v_1+\cdots+\alpha_kv_k+\beta_1s_1+\cdots+\beta_ps_p+\gamma_1t_1+\cdots+\gamma_qt_q=0.$$

This implies that

$$\alpha_1v_1+\cdots+\alpha_kv_k+\beta_1s_1+\cdots+\beta_ps_p=-\gamma_1t_1-\cdots-\gamma_qt_q.$$