RÓBERT FREUD

Linear Algebra: A Problem-Centered Approach
Answers to Selected Exercises

The answers serve for checking that the Reader's solution led to a correct result. Therefore, we suggest to consult the answer only after having solved the problem.

A wrong answer may be the result of a miscalculation but it may be caused by an error or gap in the argument. A thorough and meticulous verification of each step can spot the mistake and lead to the right answer. It is important to write down every small unit carefully. Working through the details clarifies the argument, reveals its most important features, and helps to identify any errors or gaps.

If this analysis does not find the erroneous parts, it is often useful to return to the problem later or to solve first some special case of it. If all these still do not lead to the right answer, it is worth to consult the hint or detailed solution given to many exercises in the other two free online materials.

CONTENTS

1. Determinants

1.1.

1.1.2 (a) 2500; (b) 2550; (c) 4270; (d) 5000.

1.1.3 $n = 4k$ or $n = 4k + 1$.

1.1.4 $(n + 1)/2$ (such a permutation exists only if n is odd).

1.1.5 (a) $2n - 3$. This occurs if and only if we swap 1 and n and they occupy the first and last positions.
(b) $2\lceil (n-4)/5 \rceil + 1$ where $\lceil x \rceil$ is the ceiling of x, i.e., the smallest integer greater than or equal to x.

1.1.6 (a) $\binom{n}{2}$.
(b) $n - 1$.
(c) $\lfloor (3n - 3)/2 \rfloor$, i.e., $3k$ for $n = 2k + 1$, and $3k - 2$ for $n = 2k$.

1.1.7 (a) n is odd.
(b) Every $n > 2$ except $n = 5$.
(c) If k is odd, then every even $n > k$; if $k \neq 0$ is even, then every $n > k$ except $n = 2k + 1$; and if $k = 0$, then every $n > 0$.

1.1.8 (c) $n!$
(d) $\binom{n}{2} n!/2$.
(f) For the middle value(s) of k, i.e., for $k = v/2$ if $v = \binom{n}{2}$ is even, and $k = (v \pm 1)/2$ if v is odd.

1.2.

1.2.1 (a) 90. (b) -192.

1.2.2 True: (a), (d), (g).

1.2.3 (a) 0.
(b) $\alpha_{11}\alpha_{22}\ldots\alpha_{nn}$ (the product of the elements in the main diagonal).
(c) $(-1)^{n(n-1)/2}\,\alpha_{1,n}\alpha_{2,n-1}\cdots\alpha_{n,1}$.

1.2.4 (a) $(-1)^{n-1}$.
(b) 0.
(c) $(-1)^{n/2}$ for n even, and 0 for n odd.

1.2.6 $(n-2)(n-1)!$ if the two elements are in the same row or column, and $(n^2-3n+4)(n-2)!$ otherwise. The same holds if we take also the signs of the products into account.

1.2.7 It always suffices to change a *single* element.

1.2.10 $2^{\lfloor n/2 \rfloor}$.

1.3.

1.3.1 It remains the same if n is of the form $4k$ or $4k+1$, and changes sign otherwise.

1.3.2 If the determinant is not 0, then there are n such complex numbers z, namely the nth roots of -1. If the determinant is 0, then every complex number z works.

1.3.3 (a) 30. (b) 100.

1.3.7 (a) The determinants are equal.
(b) The new determinant is $\alpha^{n(n+1)}$ times the old one.

1.3.8 (a) $(n-1)!$ (b) 1. (c) 0 for $n > 1$. (d) 0 for $n > 2$. (e) 0 for $n > 2$.

1.3.9 0 for $n > 2$.

1.3.11 0 for $n > 2$.

1.3.12 $[\gamma + (n-1)\delta](\gamma - \delta)^{n-1}$.

1.3.13 0.

1.3.15 1. Generalization: The elements are the binomial coefficients in the initial section of (a rotated) Pascal's triangle. Also the general determinant is 1.

1.3.16 (a) $(-1)^n(n-2)$.
(b) $(-1)^{n-1}(n-1)!$.

1.3.17 $n!$

1.3.18 0 for $n > 2$.

1.3.19 For an even n, only the divisibility by $n/2$ follows.

1.4.

1.4.1 nD.

1.4.2 0.

1.4.5 $\delta^{n-1} - (n-1)\beta\gamma\delta^{n-2}$ for $n \geq 2$.

1.4.6 $(\gamma^2 - \delta^2)^k$.

1.4.7 $\gamma^n + \gamma^{n-1}\delta + \gamma^{n-2}\delta^2 + \ldots + \delta^n$.

1.4.8 There is exactly one γ if the sum of all cofactors in the original determinant is not 0, and there is no such γ if this sum is 0.

1.4.10 $1 - \sum_{i=1}^{n} \beta_i^2$.

1.4.12 $[\beta(\gamma-\delta)^n - \delta(\gamma-\beta)^n]/(\beta-\delta)$ if $\beta \neq \delta$. For $\beta = \delta$ see Exercise 1.3.12.

1.4.13 (a) n. (b) $n^2 - n + 1$. (ca) 1. (cb) $n(n-1)/2 + 1$.

1.4.14 It does exist.

1.5.

1.5.1 (a) $(-1)^{n(n-1)/2}\,V$. (b) $(-1)^{n(n-1)/2}\,V^2$.

1.5.2 If γ_i are not all distinct, then every x is a solution. If γ_i are all distinct, then there are $n-1$ solutions. For $\delta \neq 0$, the equation $V(x, \gamma_2, \ldots, \gamma_n) = \delta$ (a) cannot have more than $n-1$ solutions; but (b) can have a smaller number of solutions.

1.5.3 The $n \times n$ determinant is $\delta_1 \ldots \delta_n V(\gamma_1, \ldots, \gamma_n)$ where δ_i and γ_i are the first element and the quotient of the geometric sequence in the ith row.

1.5.4 $n!(n-1)!\ldots 1! = n(n-1)^2(n-2)^3 \ldots 1^n$.

1.5.5 (a) $V(\gamma_1, \ldots, \gamma_n)$ multiplied by the product of the leading coefficients of the polynomials.
(b) 0.

1.5.6 $\prod_{1\leq i<j\leq n}(\alpha_j - \alpha_i)(\beta_j - \beta_i)$.

1.5.7 $\binom{n-1}{1}\binom{n-1}{2}\ldots\binom{n-1}{n-1}\prod_{1\leq i<j\leq n}(\alpha_j - \alpha_i)(\beta_i - \beta_j)$.

1.5.8 The quotient is $2^{(n-1)(n-2)/2}$.

1.5.9 (a) It changes sign.
(b) σ is an even permutation.

1.5.10 $\binom{n+2}{3}$.

1.5.12 $(-1)^{(p+1)/2}$, i.e., 1 if $p = 4k - 1$, and -1 if $p = 4k + 1$.

1.5.13 $(\gamma_1 + \gamma_2 + \ldots + \gamma_n)V(\gamma_1, \ldots, \gamma_n)$.

2. Matrices

2.1.

2.1.1 The sum is a $k \times n$ matrix where every element is $6 \cdot 3^{kn-1}$.

2.1.2 $\alpha/\beta \notin \mathbf{R}$ (and $\alpha, \beta \neq 0$).

2.1.3 A.

2.1.4 (a) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. (b) $\begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}$. (c) $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$.

2.1.5 (a) $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

(b) $\begin{pmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{pmatrix}$.

(c) $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$ if n is odd, and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ if n is even.

2.1.6 (a) $\begin{pmatrix} b & 1-b \\ b & 1-b \end{pmatrix}$. (b) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2.1.7 Both are the zero matrix.

2.1.8 True: (a), (d).

2.1.9 The statement is false, e.g., $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ is a counterexample.

2.1.10 Multiplying by B from the left or right multiplies the first row or column, respectively, by 5. Multiplying by C from the left adds 6 times the second row to the first row. Multiplying by C from the right adds 6 times the first column to the second column.

2.1.11 A permutation is applied to the rows and columns, respectively.

2.1.12 0.

2.1.14 1.

2.1.16 $A^p = I$.

2.1.18 $A = \lambda I$.

2.1.19 γ_{im} shows the quantity of the mth material needed in the ith article.

2.1.20 The law about the scalar multiple is modified to $(\lambda A)^* = \overline{\lambda} A^*$ at the adjoint.

2.1.21 $A = 0$. In the complex case, we have to multiply with the adjoint instead of the transpose.

2.2.

2.2.1 True: (a), (b).

2.2.2 True: (a), (b), (g).

2.2.3 True: (a), (c).

2.2.4 (a) and (d) are invertible, their inverses are

$$\text{(a)}\ \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}; \qquad \text{(d)}\ \begin{pmatrix} -\frac{3}{2} & \frac{5}{2} & -1 \\ \frac{1}{2} & -\frac{7}{2} & 2 \\ \frac{1}{2} & \frac{3}{2} & -1 \end{pmatrix}.$$

(b) and (c) are zero divisors, we get a zero product if they are multiplied from either side, e.g., by

$$\text{(b)}\ \begin{pmatrix} 6 & -2 \\ -3 & 1 \end{pmatrix}; \qquad \text{(c)}\ \begin{pmatrix} 1 & 3 & -2 \\ -2 & -6 & 4 \\ 1 & 3 & -2 \end{pmatrix}.$$

2.2.5 The determinant is ± 1.

2.2.6 It is invertible if and only if no element is 0 in the main diagonal. Also its inverse is an upper triangular matrix.

2.2.7 True: (a), (c), (f).

2.2.12 (a) and (b) are basically the same as $\mathbf{R}$ and (d) is the same as $\mathbf{C}$.

(c) is commutative, it has an identity, the matrices satisfying $a \neq \pm b$ have an inverse, and the other non-zero matrices are two-sided zero divisors.

(e) is non-commutative, the matrices $\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ are the left identities, there is no right identity, every non-zero matrix is a right zero divisor, and the non-zero matrices $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ are the left zero divisors.

2.2.14 $3 \mid n$.

3. Systems of Linear Equations

3.1.

3.1.2 (a) Equivalent transformations: (i), (iv).
(b) For other fields (iv) is not necessarily equivalent, this happens, e.g., for the modulo 2 field F_2.

3.1.3 (a) $x = 1, y = -1, z = 2$.
(b) No solution.
(c) $x = -2 + \nu, y = 5 - \nu, z = \nu$ where $\nu \in \mathbf{R}$ is arbitrary.

3.1.4 25.

3.1.5 (a) $x_1 = -i\nu$, $x_2 = \nu$, $x_3 = i$ where $\nu \in \mathbf{C}$ is arbitrary.
(b) $x_1 = 0$, $x_2 = 1$, $x_3 = i$, $x_4 = -1$, $x_5 = -i$.

3.1.6 If n is odd, then $x_1 = x_2 = \ldots = x_n = 1/2$. If n is even, then $x_1 = x_3 = \ldots = x_{n-1} = 1 - \nu$, $x_2 = x_4 = \ldots = x_n = \nu$ where $\nu \in \mathbf{R}$ is arbitrary.

3.1.7 m and n are coprime.

3.1.8 $x_1 = n + 1$, $x_2 = x_3 = \ldots = x_{n-1} = 0$, $x_n = -1$.

3.1.9 (a) p^{n-2}. (b) p^2.

3.1.10 Concerning the second part with reverse roles, (b) and (d) are impossible.

3.1.11 The number of unknowns is the sum of the numbers of the leaders and free parameters.

3.1.14 Equations with two unknowns correspond to the lines in the plane and solutions are their intersection points. So, a system of equations is solvable if and only if all lines share a common point. There are infinitely many solutions if and only if all lines coincide. Similarly, equations with three unknowns correspond to the planes in the space. For more than three variables and/or for other fields we have no direct geometric representation.

3.1.16 True: (a), (c), (f).

3.1.17 Double cannot determine the parity of Triple's integers. Triple can determine the parity of Double's integers and 5 is the minimal number of questions.

3.1.18 True: (a), (b).

3.1.19 True: (b).

3.2.

3.2.1 $x_1 = x_3 = 1$, $x_2 = 2i$, $x_4 = 0$.

3.2.2 $x_1 = \ldots = x_n = 1$.

3.2.3 (a) $x_1 = \ldots = x_{n-1} = 0$, $x_n = n$.

(b) $x_j = \displaystyle\prod_{i \neq j} \frac{\beta - \alpha_i}{\alpha_j - \alpha_i}$.

3.2.4 True: (a).

3.2.7 (a) $-x + 11$; (b) $2x^2 + 1$; (c) ix;
(d) $2(x + 1)(x^2 + 1) + 1 = 2x^3 + 2x^2 + 2x + 3$.

3.2.8 (a) 0 or 1.
(b) Infinitely many for infinite fields, and $|F| - 1$ for finite fields F.

3.2.11 (a) $L_i = \prod_{j \neq i}(x - \gamma_j)/(\gamma_i - \gamma_j)$.

3.2.12 (a) 1. (b1) 1. (b2) 0.

3.2.13 True: (b).

3.3.

3.3.1 (a) Dependent and each vector can be expressed as a linear combination of the others, e.g., $\mathbf{c}_1 = 3\mathbf{c}_3 - 2\mathbf{c}_2$.
(b) Independent.

3.3.2 Only the vectors in (b) are independent over $\mathbf{R}$ and every system is dependent over F_3.

3.3.3 True: (b).

3.3.4 True: (a), (c).

3.3.5 Only $\mathbf{v} = \mathbf{0}$ is possible.

3.3.6 They are necessarily independent.

3.3.7 (a) Yes. (b) No.

3.3.8 The vectors in (a) and (d) are independent, the others are dependent. In the modified problem, the vectors in (a) can be dependent and can be independent, the others are dependent.

3.3.9 (aA), (bA), (bB): necessarily dependent.
(aB), (aC), (bC): can be independent and can be dependent.

3.4.

3.4.2 $\binom{k}{h}\binom{n}{h}$.

3.4.3 (a) 2. (b) 3. (c) 1.

3.4.4 (a) 0 or 1. (b) 0, 1, or 2.

3.4.5 The rank is the minimum of the numbers of rows and columns.

3.4.6 (b) No. (c) No. (d) Yes.

3.4.8 The ranks over $\mathbf{Q}$ and $\mathbf{R}$ are equal and are greater than or equal to the rank over F_2. (The latter can be much smaller than the other two; see Exercise 4.6.16.)

3.4.9 True: (a).

3.4.11 True: (a), (d).

3.4.13 (a) Consider, e.g., a matrix A where the first four columns are independent and $\mathbf{a}_5 = \mathbf{a}_1$, $\mathbf{a}_6 = \mathbf{a}_2$, $\mathbf{a}_7 = \mathbf{a}_3$.

3.4.15 True: (a), (d), (e).

3.4.16 11.

3.4.18 Yes: (c).

3.4.19 (a) k steps.
(b) 1 step if $k > n$, and $n - k + 2$ steps if $k \le n$.

3.5.

3.5.1 (a) $\begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 2 & -1 & -1 \\ 0 & -1 & 0 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 4 & -6 & 4 & -1 \\ -6 & 14 & -11 & 3 \\ 4 & -11 & 10 & -3 \\ -1 & 3 & -3 & 1 \end{pmatrix}$.

3.5.2 (a) $A^{-1} = \begin{pmatrix} n & -1 & -1 & \dots & -1 \\ -1 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \dots & 1 \end{pmatrix}$.

(b) $B^{-1} = \begin{pmatrix} 1 & -2 & 1 & \dots & 0 \\ 0 & 1 & -2 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$.

(c) $C^{-1} = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & -1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & -1 \\ 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}$.

3.5.3 (a) The columns in X are scalar multiples of $(1, 1, -1, -1)$ and so are the rows in Y.

(b) The columns in Z are of the form $(\lambda + 2\mu, -2\lambda - 3\mu, \lambda, \mu)$ and the rows of W are of the form $(\lambda - \mu, -2\lambda - \mu, \lambda, \mu)$ where the scalars λ and μ vary independently in the columns or rows.

3.5.5 A_n is invertible if and only if n is odd. Then, for $n > 1$, every element of A^{-1} is $\pm 1/2$. The signs are alternating in each row starting with + in the main diagonal and cyclically returning to it (so also the element just before the main diagonal gets a + sign).

A_n is a zero divisor if and only if n is even. Then $A_n B = C A_n = 0$ holds if and only if every column of B and every row of C is a scalar multiple of $(1, -1, 1, -1, \dots, 1, -1)$.

3.5.7 No.

3.5.8 (c) Only $A = 0$ has this property.

4. Vector Spaces

4.1.

4.1.1 Vector spaces: (b), (d), (e), (f), (h), (i), (j).

4.1.2 Vector spaces: (a), (c), (d), (e), (j), (l), (m), (o).

4.1.3 Vector spaces: (a), (b), (f), (g), (k).

4.1.4 In Examples E5 and E6, real numbers can be replaced by an arbitrary field. Generalization of E7: Let F_1 be a subfield of F_2, then $V = F_2$ is a vector space over F_1 under the operations of F_2. Moreover, it is sufficient that F_2 is a commutative ring with the same identity as F_1.

4.1.5 Yes. (For deeper reasons; see Exercise 5.2.2.)

4.1.6 Yes. (For deeper reasons; see Exercise 5.2.2.)

4.1.7 No.

4.1.8 Yes: (c), (e), (f).

4.1.9 Just one axiom is false in each case, these are:
(a) (MS1); (b) (MS1); (c) (MS4); (d) (MS3).

4.1.11 True: (a), (b).

4.2.

4.2.1 Each exercise asks to decide whether or not certain subsets are subspaces in a given vector space.

4.2.2 Subspaces: (a), (b), (h), (i), (j).

4.2.3 To determine the kernel we have to solve a homogeneous system of linear equations. As for the image, we have to characterize the constants on the right-hand side that make consistent the system of equations with given coefficients. If we perform the elimination considering these constants as parameters, the echelon form cannot contain forbidden rows. So, if a row in the coefficient part is zero, then the corresponding right-hand side has to be 0, too.

For the given matrix A:

$$\operatorname{Ker} A = \left\{ \lambda \begin{pmatrix} 2 \\ -3 \\ 0 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix} \right\}, \qquad \operatorname{Im} A = \left\{ \alpha \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\},$$

where λ, μ, α, $\beta \in F$. (Both subspaces can be described by other parameters or in another form, too.)

4.2.4 Case (a) is impossible over the fields F_p.

4.2.5 Conditions implying that W is a subspace: (a), (b), (c), (e).

Remark: Each of conditions (a), (b), and (c) is *equivalent* to W being a subspace, and (e) holds exactly if $W = V$.

4.2.6 True: (b), (c).

4.2.7 (a) Either both or none of $\mathbf{u}$ and $\mathbf{v}$ are in W.
(b) At most one of $\mathbf{v}$ and $\mathbf{w}$ is in W.
(c) Both $\mathbf{v}$ and $\mathbf{w}$ are in W.
(d) Neither $\mathbf{v}$ nor $\mathbf{w}$ is in W.
(e) At most one of $\mathbf{v}$ and $\mathbf{w}$ is in W.

Other fields: e.g., for F_{11}, (c) can hold also if neither $\mathbf{v}$ nor $\mathbf{w}$ is in W.

4.2.8 $5\mathbf{v} + 3\mathbf{w} + \mathbf{z} \notin W$, $6\mathbf{v} + 3\mathbf{w} + \mathbf{z} \in W$.

4.2.9 Their elements are scalar multiples of a single vector.

4.2.11 (a) 5. (b) $p + 3$.

4.2.12 (b) One of them contains the other.
(c) No.
(d) Generally not, but it can occur in vector spaces over F_2.

4.2.14 V is not a vector space.

4.2.15 Only (d) is correct.

4.2.16 (a) For the space vectors, these are all points, lines, planes, and the space itself.

4.3.

4.3.1 Only (c) is a spanning set.

4.3.2 Examples in Section 4.1: E1, E2, E3, E7. Exercise 4.1.1: (b). Exercise 4.1.2: (c), (l), (m). Exercise 4.1.3: none.

4.3.3 True: (a), (d), (e).

4.3.4 True: (a), (c), (e).

4.3.6 True: (c), (e).

4.3.7 Only $\mathbf{c} = \mathbf{0}$ works.

4.3.10 (a), (b), (d), (e): V. (c): $\{f \mid f(x) = 0, \text{ if } x \neq 5, x \neq 6\}$.
Direct sums: (a), (c), (d).

4.3.12 (a) $\langle W_1, W_2 \rangle \cap W_3 \supseteq \langle W_1 \cap W_3 \,,\, W_2 \cap W_3 \rangle$.
(b) $\langle W_1 \cap W_2 \,,\, W_3 \rangle \subseteq \langle W_1, W_3 \rangle \cap \langle W_2, W_3 \rangle$.
(c) The two sides are equal.
There is no equality in (a) and (b) in general. This, too, shows that the properties of the span differ from those of the union.

4.3.13 Yes: (b), (c), (e).

4.3.14 A (possible) definition of the span of more than two subspaces:

$$\langle W_1, \ldots, W_k \rangle = W_1 + \ldots + W_k = \{w_1 + \ldots + w_k \mid w_i \in W_i\}.$$

A generalization of Theorem 4.3.6: This representation of the elements is unique if and only if

$$W_i \cap \langle W_1, \ldots, W_{i-1} \,,\, W_{i+1} \,,\, \ldots \,,\, W_k \rangle = \mathbf{0}, \quad i = 1, 2, \ldots, k.$$

In this case we say that the span of the subspaces W_i is their direct sum and denote it by $W_1 \oplus \ldots \oplus W_k$. This condition clearly implies that the intersection of all subspaces or even the intersection of any two subspaces is $\mathbf{0}$ but it is a much stronger restriction than those. E.g., the plane is *not* the direct sum of three distinct lines passing through the origin.

4.3.15 If the subset is a subspace, then its span is itself. The other cases are:
Exercise 4.1.1. (a): the polynomials of degree at most 100 and the 0; (c), (g), (k), (l), (m): all polynomials.
Exercise 4.1.2. (b), (g), (h), (i): all sequences; (f): convergent sequences; (k): the sequences in (j).
Exercise 4.1.3. (c): the functions in (b); (d), (e), (i), (j), (l), (m): all functions.

4.3.16 (a) $f \in \langle H \rangle$.
(b) $g \notin \langle H \rangle$.
(c) The answers remain the same.

4.3.17 Only (c) is a spanning set.

4.4.

4.4.1 True: (b), (e), (g), (i), (j).

4.4.2 (a) They are necessarily dependent.
(b) They are necessarily independent.
(c) They can be dependent and can be independent.

4.4.3 Yes.

4.4.5 If $s \geq 2$ and $\mathbf{w}$, $\mathbf{v}_1$, ..., $\mathbf{v}_{m-s}$ are linearly independent, then take, e.g., $\lambda_1\mathbf{w}, \ldots, \lambda_s\mathbf{w}, \mathbf{v}_1, \ldots, \mathbf{v}_{m-s}$ where $\lambda_1, \ldots, \lambda_s$ are distinct non-zero scalars.

4.4.6 True: (a), (c).

4.4.7 They are necessarily independent.

4.4.8 Only $\mathbf{d} = \mathbf{0}$ is possible.

4.4.9 Necessarily independent: (a), (d).
Necessarily dependent: (b), (c), (f).
Can be independent and can be dependent: (e), (g).

4.4.10 (a) m is odd. (b) $(k\,, m) = 1$.

4.4.11 Only (c) is false.

4.5.

4.5.1 The basis sizes are: (a) 11; (b) 18; (c) 19; (d) 20; (e) 20; (f) 20; (g) 19.

4.5.2 Basis: (a), (d). Independent but not a basis: (f). Spanning set but not a basis: (b).

4.5.6 Dependent.

4.5.7 True: (b), (c), (f).

4.5.8 (a) None.
(b) Independent but not a spanning set.
(c) Basis if n is odd, and none if n is even.
(d) Basis.
(e) Spanning set but dependent.

4.5.12 (a) Yes. (b) No.

4.5.14 (a) F_p^2 : $(p^2 - 1)(p^2 - p)$, F_p^n : $(p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$.
(b) $(p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$.

4.6.

4.6.1 (a) 2. (b) ∞. (c) $n(n+1)/2$. (d) ∞. (e) p.
(f) 84. (g) 210. (h) 20. (i) $n-r$.
(j) The number of columns minus the rank. (k) The rank.

4.6.2 Basis: (a), (b), (c).

4.6.7 (a) ∞. (b) 101, 101, 102.

4.6.8 $\varphi_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$.

4.6.9 $\begin{pmatrix} \beta & \gamma & 3\delta-\gamma-\beta \\ 4\delta-\gamma-2\beta & \delta & 2\beta+\gamma-2\delta \\ \beta+\gamma-\delta & 2\delta-\gamma & 2\delta-\beta \end{pmatrix}$.

4.6.10 (a) 3. (b) 3. (c) 4.

4.6.14 $\dfrac{(p^n-1)(p^n-p)\dots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\dots(p^r-p^{r-1})}$.

4.6.15 $\dfrac{(p^k-1)(p^k-p)\dots(p^k-p^{r-1})(p^n-1)(p^n-p)\dots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\dots(p^r-p^{r-1})}$.

4.6.16 (c) 1010.

4.7.

4.7.1 (a) The corresponding two coordinates are swapped.
(b) The corresponding coordinate is multiplied by $1/\lambda$.
(c) If $\mathbf{b}_i$ is replaced by $\mathbf{b}_i + \lambda\mathbf{b}_j$ and the original coordinates are α_i and α_j, then the new coordinates are α_i and $\alpha_j - \lambda\alpha_i$.

4.7.2 Only $\mathbf{0}$ has this property.

4.7.3 The coordinates of $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ are 26, -21, 19, i.e.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 26\begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix} - 21\begin{pmatrix} 3 \\ 7 \\ 8 \end{pmatrix} + 19\begin{pmatrix} 2 \\ 5 \\ 2 \end{pmatrix}.$$

The coordinates of $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ are -10, 8, -7. The coordinates of $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ are -1, 1, -1.

4.7.4 It can be any vector except the scalar multiples of $\mathbf{v}$.

4.7.5 (a) She survives. (b) She dies.

5. Linear maps

5.1.

5.1.1 Linear transformations: (a), (c), (d), (e), (g), (i). We indicate the dimensions of the kernel and the image in parentheses.
- (a) Kernel: constants (1). Image: $\deg f \leq 99$ (100).
- (c) Kernel: $\{\gamma x\}$ (1). Image: $\{f \mid \alpha_1 = 0\}$ (100).
- (d) Kernel: constants (1). Image: $\deg f \leq 99$ (100).
- (e) Kernel: $\{f \mid \alpha_0 = 0\}$ (100). Image: $\{\gamma x\}$ (1).
- (g) Kernel: $\{f \mid f(1) = 0\}$ (100). Image: $\{\gamma(x + x^2)\}$ (1).
- (i) Kernel: Multiples of $x^7 + 4x + 1$ (94). Image: $\deg f \leq 6$ (7).

5.1.2 Linear transformations: (a), (e), (f), (h). We indicate the dimensions of the kernel and the image in parentheses.
- (a) Kernel: imaginary numbers (1). Image: real numbers (1).
- (e) Kernel: 0 (0). Image: $\mathbf{C}$ (2).
- (f) Kernel: 0 (0). Image: $\mathbf{C}$ (2) (except if we multiply by 0).
- (h) Kernel: 0 (0). Image: $\mathbf{C}$ (2).

5.1.3 Linear maps: (a), (c), (e). We indicate the dimensions of the kernel and the image in parentheses.
- (a) Kernel: matrices with middle column zero (6). Image: F^3 (3).
- (c) Kernel: matrices with trace 0 (8). Image: all coordinates are equal (1).
- (e) Kernel: the sum of every row in the matrix is 0 (6). Image: F^3 (3).

5.1.4 We indicate the dimensions of the kernel and the image in parentheses.
- (a) Kernel: 0 (0). Image: sequences with first element 0 (∞).
- (b) Kernel: every element in the sequence except perhaps the first one is 0 (1). Image: V (∞).
- (c) Kernel: 0 (0). Image: sequences satisfying $\alpha_{2k} = \alpha_{2k+1}$ for $k = 0, 1, 2, \ldots$ (∞).

(d) Kernel: sequences where $\alpha_{10k} = 0$, $k = 0, 1, 2, \ldots$ (∞). Image: V (∞).
(e) Kernel: sequences with all elements equal (1). Image: V (∞).
(f) Kernel: 0 (0). Image: V (∞).
(g) Kernel: sequences $(\gamma, -\gamma, -\gamma, \gamma, \gamma, -\gamma, -\gamma, \gamma, \ldots)$ (1). Image: sequences satisfying $\alpha_{4k} + \alpha_{4k+1} = \alpha_{4k+2} + \alpha_{4k+3}$, $k = 0, 1, 2, \ldots$ (∞).

5.1.5 No. (Cf. Exercise 5.3.1.)

5.1.7 $\dim V \leq 1$.

5.1.8 It is false over $\mathbf{R}$.

5.1.9 True: (b), (d).

5.1.12 101^k, $k = 0, 1, 2, \ldots$ or ∞.

5.1.16. (a) $\mathcal{A}U \cap \mathcal{A}Z \supseteq \mathcal{A}(U \cap Z)$ but they are not equal in general.
(b) $\mathcal{A}\langle U, Z\rangle = \langle \mathcal{A}U\,,\, \mathcal{A}Z\rangle$.

5.2.

5.2.1 5.1.1: none. 5.1.2: (e), (f) (except if we multiply by 0), and (h). 5.1.3: none. 5.1.4: (f).

5.2.3 (c), (d).

5.2.5 $n + 1$.

5.2.6 (a), (b), (d), (f), (g), (i), (j), and (k), all these are 8-dimensional. (e) and (h), both are 43-dimensional.

5.3.

5.3.2 The map $\mathcal{O}$ has this property for any V_1 and V_2. Further, over the modulo 2 field, a linear map is completely determined by the image if $\dim V_1 = 1$ and by the kernel if $\dim V_2 = 1$. In all other cases, to any linear map there exists another one with the same kernel or image. (Moreover, disregarding some exceptions, to any linear map there exists another one with the same kernel *and* image simultaneously.)

5.3.3 (a) 0 or 1. If the spanning set $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is not a basis, then depending on the choice of the vectors $\mathbf{c}_i$ there is no such linear map or there is exactly one such linear map.

(b) 1 or more. If the linearly independent system $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is not a basis, then there exist always at least $|F|$ such linear maps.

5.3.4 (a) 0. (b) 1. (c) ∞.

5.3.5 p^{kn}.

5.4.

5.4.1 $\dim V$ is even.

5.4.2 Yes: (a), (b).

5.4.3 Yes.

5.4.4 Any of the five conditions implies isomorphism.

5.5.

5.5.2 (a) $\mathcal{O}$. (b) $\mathcal{I}$. (c) $\mathcal{I}$. (d) $(2\cos\Phi)\mathcal{I}$.
(e) Rotation around the origin by +45 degrees and magnification by a factor of $\sqrt{2}$.

5.5.3 Subspaces: (c) and (d) in any case; (a) if and only if $U_1 = V_1$; (b) if and only if $\dim V_1 \leq 1$ or $\dim V_2 \leq 1$; and (e) if and only if the given vector is the zero vector.

5.5.4 Apart from some exceptional cases, none of them is a subspace.

5.5.5 True: (a).

5.5.8 True: (a).

5.5.9 (c) 7.

5.6.

5.6.1 Yes: (c), (d).

5.6.2 $\mathcal{AB}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} = \begin{pmatrix}\alpha_3\\ \alpha_1\\ \alpha_2\end{pmatrix}$, $\mathcal{BA}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} = \begin{pmatrix}\alpha_2\\ \alpha_3\\ \alpha_1\end{pmatrix}$, $\mathcal{A}^{101} = \mathcal{A}$, $(\mathcal{AB})^{101} = \mathcal{BA}$.

5.6.3 $\mathcal{A} = \lambda\mathcal{I}$.

5.6.4 $\dim V \leq 1$.

5.6.5 (a) $\operatorname{Ker}\mathcal{AB} \supseteq \operatorname{Ker}\mathcal{B}$.
(b) $\operatorname{Im}\mathcal{AB} \subseteq \operatorname{Im}\mathcal{A}$.

5.6.10 $\mathcal{A}$ has infinitely many left inverses and no right inverse, it is a right zero divisor, but not a left zero divisor. We get the analogous results for $\mathcal{B}$ by swapping the words left and right. (Observe that $\mathcal{BA} = \mathcal{I} \neq \mathcal{AB}$!)

5.6.11 (a) $\mathcal{A}$ has no left or right inverse and is a two-sided zero divisor, e.g., $\mathcal{AC} = \mathcal{CA} = \mathcal{O}$.
(b) $\mathcal{B}$ is not a zero divisor and

$$\mathcal{B}^{-1} : \mathbf{b}_1 \mapsto \mathbf{b}_1,\ \mathbf{b}_2 \mapsto -\mathbf{b}_1 + \mathbf{b}_2,\ \ldots,\ \mathbf{b}_n \mapsto -\mathbf{b}_1 + \mathbf{b}_n\,.$$

(c) $\mathcal{C}$ has no left or right inverse and is a two-sided zero divisor, e.g., $\mathcal{AC} = \mathcal{CA} = \mathcal{O}$.

5.6.12 $\dim V \leq 1$.

5.6.13 $\dim V \leq 1$.

5.6.14 (a) $\dim V \geq 2$.
(b) There is no such $V(\neq \mathbf{0})$.

5.6.16 True: (a), (b), (c).

5.6.17 $\dim L = \dim R = \dim V \cdot \dim \operatorname{Ker}\mathcal{A}$.

5.6.18 (a) Yes, consider, e.g., in the plane any projection onto a line containing the origin.
(b) Only $\mathcal{I}$.
(d) The "if" part is false, e.g., over the modulo 2 field.

5.6.20 Algebras: (a), (c), (d), (e), (g), (i) (the last one is isomorphic to the algebra of quaternions).

5.6.21 (a) 0. (b) 3^{50}. (c) 8.

5.6.22 (a) $v\overline{v} = \overline{v}v = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$.
(b) $v^{-1} = \dfrac{1}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}\overline{v}$ if $(v \neq 0)$.

5.6.23 Infinitely many. All solutions are: $\alpha_1 i + \alpha_2 j + \alpha_3 k$ where $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1$. The theorem about the bound for the zeroes of a polynomial is valid for *commutative* fields (or more generally, for commutative rings without zero divisors).

5.6.24 n.

5.7.

5.7.1 (a) In the basis $1, x, \ldots, x^6$, the matrix is $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

(b) Yes. (c) Yes. (d) No. (e) No.

For a generalization of (c); see Exercise 5.8.7(b).

5.7.4 (a1) The first two columns are swapped.
(a2) The first two rows are swapped.
(b1) The third column is multiplied by λ.
(b2) The third row is multiplied by $1/\lambda$.
(c1) μ times the second column is added to the third column.
(c2) μ times the third column is subtracted from the second column.

Note that modifying the basis vectors $\mathbf{a}_j$ causes a similar, *covariant* change in the *columns* of the matrix, whereas modifying the basis vectors $\mathbf{b}_i$ causes a reverse, *contravariant* change in the *rows* of the matrix. For a general formula yielding the matrix in a new pair of bases; see Theorem 5.8.1.

5.7.5 The matrices belong to the same linear transformation in (b), (c), and (d).

5.7.9 $\mathcal{A} = \lambda\mathcal{I}$.

5.7.13 No.

5.8.

5.8.1 (a) $\begin{pmatrix} 1/2 & 3/2 & 1 \\ -1/2 & 1/2 & 1 \\ 1/2 & -1/2 & -1 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & -1 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 1 \end{pmatrix}$; (c) $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$.

5.8.5 Yes: (c), (d).

5.8.7 (a) $\mathcal{A} \neq \mathcal{O}$. (b) $\mathcal{A} \neq \lambda\mathcal{I}$.

6. Eigenvalue, Minimal Polynomial

6.1.

6.1.1

	eigenvalues	eigenspaces	dimensions	diag?
(a)	0	constants	1	no
(b)	$0, 1, \ldots, 6$	monoterms	each is 1	yes
(c)	$0, 6^6$	$x - 6 \mid f$; γx^6	$6, 1$	yes
(d)	$0, 1$	$x^2 + 3 \mid f$; $\deg f \le 1$	$5, 2$	yes

6.1.2 True for (a), (c), (e). The corresponding eigenvalues are: $\mu\alpha$, α^2, and α^{-1}.

6.1.3 Each is true. If the eigenvalues belonging to $\mathbf{v}$ are α for $\mathcal{A}$ and β for $\mathcal{B}$, then they are $\alpha + \beta$ for $\mathcal{A} + \mathcal{B}$, $\alpha\beta$ for $\mathcal{AB}$, and the values given in the previous answer for the other three transformations.

6.1.4 True: (b), (c).

6.1.5 True: (a), (d), (e).

6.1.6 E.g., a rotation around an axis (containing the origin) where the angle is not a multiple of π has 1 eigenvalue; a reflection across a plain (containing the origin) has 2 eigenvalues; and a magnification in the direction of the three axes with different factors has 3 eigenvalues.

6.1.7 The same eigenvalue belongs to $\mathbf{u}$ and $\mathbf{v}$, and $\mathbf{u} \neq -\mathbf{v}$.

6.1.8 $\lambda\mathcal{I}$.

6.2.

6.2.1 (a) $(-x)^7$. (b) $-x(x-1)(x-2)\ldots(x-6)$. (c) $-x^6(x-6^6)$. (d) $-x^5(x-1)^2$.

6.2.2 (a) $x^2 - 1$. (b) $x^2 - x$. (c) $x^2 + 1$. (d) $x^2 - x + 1$. (e) $(x-1)^2$. (f) $(x+1)^2$. (g) $(x-5)^2$.

6.2.3 $g(x) = k_{\mu\mathcal{A}}(x) = \mu^n f(x/\mu)$ where $n = \dim V$. In more detail: If

$$f(x) = (-1)^n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0,$$

then

$$g(x) = (-1)^n x^n + \mu\alpha_{n-1}x^{n-1} + \ldots + \mu^{n-1}\alpha_1 x + \mu^n \alpha_0 \,.$$

6.2.6 (a) Yes. (b) No.

6.2.7 ChP=characteristic polynomial, EV=eigenvalues, ES=eigenspaces.

(a) ChP: $x^4 - 1$. EV: $1, -1$. ES: $\langle \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3 + \mathbf{b}_4 \rangle$, $\langle \mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b}_3 - \mathbf{b}_4 \rangle$. It has no diagonal matrix.

(b) ChP: $x(x+1)(x-1)^2$. EV: $0, 1, -1$. ES: $\langle \mathbf{b}_3 - \mathbf{b}_4 \rangle, \langle \mathbf{b}_4, \mathbf{b}_1 + \mathbf{b}_2 \rangle$, $\langle \mathbf{b}_1 - \mathbf{b}_2 \rangle$. It has a diagonal matrix.

(c) ChP: $(1-x)^4 - 1$. EV: $0, 2$. ES: $\langle \mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b}_3 - \mathbf{b}_4 \rangle$, $\langle \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3 + \mathbf{b}_4 \rangle$. It has no diagonal matrix.

Over $\mathbf{C}$, we get two further eigenvalues both in (a) and (c), and both transformations have a diagonal matrix.

6.2.8 It equals the number of permutations of the elements in the main diagonal. There cannot be more since the multiplicities of the roots of the characteristic polynomial are uniquely determined.

6.3.

6.3.1 6.1.1: (a) x^7. (b) $x(x-1)(x-2)\ldots(x-6)$. (c) $x^2 - 6^6 x$. (d) $x^2 - x$.
6.2.2: (a) $x^2 - 1$. (b) $x^2 - x$. (c) $x^2 + 1$. (d) $x^2 - x + 1$.
(e) $x - 1$. (f) $x + 1$. (g) $x - 5$.
6.2.7: (a) $x^4 - 1$. (b) $x^3 - 1$. (c) $(1-x)^4 - 1$.

6.3.2 $\lambda\mathcal{I}$.

6.3.3 The constant term is not zero.

6.3.5 If $m_{\mathcal{A}} = \alpha_0 + \ldots + \alpha_k x^k$, then $m_{\mathcal{A}^{-1}} = \alpha_k + \ldots + \alpha_0 x^k$.

6.3.6 True: (b), (c), (e), (f).

6.3.9 (a) Yes. (b) No.

6.3.10 They are equal or differ in a factor x.

6.3.13 Its dimension is the degree of the minimal polynomial.

6.3.14 It can be any integer in the closed interval $[k/2, k]$.

6.3.17 The minimal polynomials and so the eigenvalues are the same, but the characteristic polynomials do not even have the same degree.

6.3.22 (b) $3 \mid n$.

6.4.

6.4.2 True: (a), (c), (d).

6.4.3 It is invariant if and only if the last $n-k$ elements in the first k columns are 0.

6.4.4 (b) $n^2 - nk + k^2$.

6.4.5 (a) $\lambda\mathcal{I}$.
(b) $\lambda\mathcal{I}$ if $\dim V > 13$.

6.4.7 (b) No.

6.4.8 $n+2$.

6.4.9 (d) $m_{\mathcal{A}}$ is irreducible over F and $\deg m_{\mathcal{A}} = \dim V$. This is equivalent to the irreducibility of $k_{\mathcal{A}}$ over F.

6.4.11 (a) Yes. (b) No.

6.4.13 0: $\mathbf{u} = \mathbf{0}$. 1: $\mathbf{u}$ is an eigenvector. (Cf. Theorem 6.5.4.)

6.4.14 E.g., V itself if $\dim \operatorname{Im} \mathcal{A} \le \dim V - 2$, or any subspace of dimension 2 or more if $\mathcal{A} = \mathcal{I}$.

6.4.15 True: (a), (c), (e).

6.5.

6.5.1 (a) If $\lambda \neq 0$, then $o(\mathbf{u}) = o(\lambda\mathbf{u})$.
(b) $o(\mathcal{A}\mathbf{u}) = o(\mathbf{u})/x$ or $o(\mathbf{u})$ depending on whether or not the constant term of $o(\mathbf{u})$ is 0.
(c) $o[f(\mathcal{A})\mathbf{u}] = o(\mathbf{u})/\big(o(\mathbf{u}), f\big)$.

6.5.3 $o_{\mathcal{A}}(\mathbf{u})$.

6.5.6 True: (a), (c).

6.5.7 The same bound holds for the minimal polynomial, too.

6.5.10 The quoted statement (i) is the special case $\big(o(\mathbf{u}), o(\mathbf{v})\big) = 1$.

6.5.11 If $\lambda \neq 0$, then the degrees of $o_{\lambda\mathcal{A}}(\mathbf{u})$ and $o_{\mathcal{A}}(\mathbf{u})$ are equal. The answer to the other question is analogous to the situation seen for the minimal polynomials (Exercise 6.3.14).

6.5.12 (c) E.g., $[\mathcal{A}] = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $[\mathcal{B}] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ works over both $\mathbf{R}$ and $\mathbf{C}$. Simpler examples over $\mathbf{R}$ are the rotations around the origin by 120 and 240 degrees, or any two transformations having the same irreducible minimal polynomial.

6.6.

6.6.3 Both the minimal and characteristic polynomials of the restriction divide the original ones.

6.6.8 (a) $\lambda\mathcal{I}$. (d) No. (f) The converse is false.

6.6.9 $\lambda\mathcal{I}$.

6.6.10 (a) $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(b) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$ where ω is a primitive third root of unity;

(c) $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(d) $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

6.6.11 (a) The elements just below the main diagonal are 1, all other elements are 0 (the entire matrix is a single Jordan sub-block).

(b) A diagonal matrix with the nth roots of unity in the main diagonal.

(c) The elements just below the main diagonal are 1 except for row $\lfloor (n+2)/2 \rfloor$, all other elements are 0 (the entire matrix is a single Jordan bloc consisting of two sub-blocks of size $\lfloor n/2 \rfloor$ and $\lfloor (n+1)/2 \rfloor$).

(d) Same as in (a).

(e) The upper left corner is n, all other elements are 0.

(f) A diagonal matrix where $\lfloor (n+1)/2 \rfloor$ elements are 1 and $\lfloor n/2 \rfloor$ elements are -1 in the main diagonal.

6.6.12 The exponentiation runs independently for the blocks and the sub-blocks within a block. In the mth power of a $k \times k$ Jordan sub-block
$$A = \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix},$$
all elements are 0 above the main diagonal, they are λ^m in the main diagonal, $m\lambda^{m-1}$ just below the main diagonal, $\binom{m}{2}\lambda^{m-2}$ in the next diagonal, and in general, $\binom{m}{j}\lambda^{m-j}$ in the jth diagonal. We get $f(\mathcal{A})$ similarly for any polynomial f.

6.6.13 Let s_i be the multiplicity of λ_i in the main diagonal, i.e., s_i is the size of the block belonging to λ_i, and let t_i be the maximal size of sub-blocks in this block. Then

$$k_{\mathcal{A}} = \prod (x - \lambda_i)^{s_i} \quad \text{and} \quad m_{\mathcal{A}} = \prod (x - \lambda_i)^{t_i} .$$

Remark: This yields immediately $k_{\mathcal{A}} \mid m_{\mathcal{A}}$ providing a new proof to the Cayley–Hamilton Theorem 6.3.5 over $F = \mathbf{C}$. The same applies to any algebraically closed field where every non-constant polynomial has a root. This implies the divisibility for an arbitrary field, too, if we switch to its algebraic closure and observe that this does not affect the minimal and characteristic polynomials (see the remark after the hint to Exercise 6.3.21).

6.6.15 (a) $\deg m_{\mathcal{A}} = 1$ or $\deg m_{\mathcal{A}} = n (= \dim V)$ or $m_{\mathcal{A}} = (x - \lambda)^{n-1}$.

(b) The characteristic polynomial has no multiple roots.

(c) For every root of the characteristic polynomial, its multiplicity in the minimal polynomial is the same or by one less or is 1.

6.6.17 (a) $A^n = \dfrac{1}{3} \begin{pmatrix} 5^n + 2^{n+1} & 5^n - 2^n \\ 2 \cdot 5^n - 2^{n+1} & 2 \cdot 5^n + 2^n \end{pmatrix}$.

(b) $B^n = \begin{pmatrix} n2^{n-1} + 2^n & n2^{n-1} \\ -n2^{n-1} & 2^n - n2^{n-1} \end{pmatrix}$.

7. Bilinear Functions

7.1.

7.1.1 (a) and (b) are not bilinear functions.

(c) $\alpha_{ij} = 2^{j-1}$.

(d) $\alpha_{ij} = (i-1)2^{j-1}$.

(e) $\alpha_{ij} = 1$ if $i + j = 4$, and 0 otherwise.

7.1.2 E2: I.

E3: Every $\alpha_{ij} = 0$ except for $\alpha_{12} = 1$ and $\alpha_{21} = 2$ in the first function and $\alpha_{11} = 1$ and $\alpha_{22} = -3$ in the second function.

E4: 0.

7.1.3 Except for the zero function, the range of every other bilinear function is the set of *all* real numbers.

7.1.4 (a) There exists at most one **A**.

(b) If the set is not a basis, then infinitely many functions **A** satisfy the condition.

7.1.5 The dimension is n^2 if $\dim V = n$.

7.1.6 (a) Both the first two rows and the first two columns get swapped.

(b) The third row and column are multiplied by λ (so α_{33} gets multiplied by λ^2).

(c) We add μ times the second row/column to the third row/column (so the third element in the new third row is $\alpha'_{33} = \alpha_{33} + \mu\alpha_{23} + \mu\alpha_{32} + \mu^2\alpha_{22}$.

7.1.7 Only the **0** bilinear function has this property.

7.1.9 (a) 1 (except if $\mathbf{A} = \mathbf{0}$).

(b) The minimal value of r is the rank of any matrix of **A**.

7.2.

7.2.3 (b) If $\dim V = n$, then $\dim S = n(n+1)/2$ and $\dim A = n(n-1)/2$.

7.2.4 True: (a).

7.2.5 We show just one example for each subspace.

(a) $\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix};$

(b) $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}-3\\-1\\1\\3\end{pmatrix};$

(c) $\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}.$

7.2.6 dm = the main diagonal of a diagonal matrix, **A**-OB = an **A**-orthogonal basis.

(a) dm: $1, 0, 0, 0, 0$. **A**-OB: 1, $x-1$, x^2-1, x^3-1, x^4-1.

(b) dm: $1, 1, -1, 0, 0$. **A**-OB: x, $1/2+x^2$, $1/2-x^2$, x^3, x^4.

(c) dm: $1, 1, 1, 1, 1$. **A**-OB: $f_i = \lambda_i F/(x-i)$ with $F = \prod_{i=1}^{5}(x-i)$ and suitable scalars λ_i.

7.2.7 dm = the main diagonal of a diagonal matrix, **A**-OB=an **A**-orthogonal basis.

(a) dm: $1, 0, 0$. **A**-OB: $\mathbf{b}_1$, $\mathbf{b}_2 - 2\mathbf{b}_1$, $\mathbf{b}_3 - 3\mathbf{b}_1$.

(b) dm: $1, -1, 0$. **A**-OB: $\mathbf{b}_1$, $\mathbf{b}_2 - 2\mathbf{b}_1$, $\mathbf{b}_3 - 2\mathbf{b}_2 + \mathbf{b}_1$.

7.2.9 The dimension is n or $n-1$.

7.2.10 $(n+2)(n+1)/2$.

7.3.

7.3.2 7.2.5: PD.
7.2.6: (a) PS. (b) I. (c) PD.
7.2.7: (a) PS. (b) I.

7.3.3 PD, PS: non-negative real numbers. ND, NS: non-positive real numbers. I: all real numbers. **0**: zero alone.

If we only consider the values assumed at non-zero vectors, then PD: positive numbers, ND: negative numbers, and there is no change for the other types. (Here we need also Exercise 7.2.8 for indefinite forms.)

7.3.4 (a) $\tilde{\mathbf{A}}(\lambda\mathbf{x}) = \lambda^2\tilde{\mathbf{A}}(\mathbf{x})$.

(b) $\mathbf{x}$ and $\mathbf{z}$ are $\mathbf{A}$-orthogonal.

7.3.5 (a) If $\lambda > 0$, then $\mathbf{A}$ and $\lambda\mathbf{A}$ have the same type. If $\lambda < 0$, then there is no change for $\mathbf{0}$ and indefinite forms, whereas the other forms change sign. If $\lambda = 0$, then $\lambda\mathbf{A} = \mathbf{0}$.

(b) PD+PD=PD; PD+PS=PD; PS+PS=PD or PS; PD+I, PS+I, and PD+NS: PD or PS or I; further six cases follow from swapping letters P and N; PS+NS: PS or NS or I or $\mathbf{0}$; finally I+I, PD+ND can be of any type.

7.3.6 There are several other possible representations, too, besides the ones listed below.

(a) $[(x_1 + x_2)/2]^2 - [(x_1 - x_2)/2]^2$.

(b) $[(x_1 + x_2 + x_3)/2]^2 - [(x_1 - x_2 + x_3)/2]^2$.

(c) $[(x_1 + 2x_2 + x_3)/2]^2 - [(x_1 - x_3)/2]^2 - x_2^2$.

(d) $(x_1 - x_2 + x_3)^2 - (x_2 + 2x_3)^2$.

(e) $(x_1 + 2x_2 + x_3)^2 - (x_2\sqrt{3} + x_3/\sqrt{3})^2 + (x_3\sqrt{7/3})^2$.

7.3.7 There are several other possible representations, too, besides the ones listed below.

(a) $(x_1 + x_2 + x_3 + x_4)^2$.

(b) $[(x_1+x_2+x_3)/2]^2-[(x_1-x_2+x_3)/2]^2+[(x_3+x_4)/2]^2-[(x_3-x_4)/2]^2$.

(c) $[(x_1 + x_2 + x_3 + x_4)/2]^2 - [(x_1 - x_2 + x_3 - x_4)/2]^2$.

(d) $[(x_1+x_2+2x_3+2x_4)/2]^2-[(x_1-x_2)/2]^2-[(2x_3+x_4)/2]^2-(x_4\sqrt{3}/2)^2$.

7.3.8 The law of inertia refers to signed sums of squares of coordinates obtained for an ($\mathbf{A}$-orthogonal) *basis*. This does not hold for the sums of squares in the exercise as the representation of a two-dimensional quadratic form can contain the signed sum of at most *two* squares. A proper representation of this form is $(x_1\sqrt{2} + x_2/\sqrt{2})^2 + (x_2\sqrt{3/2})^2$.

7.3.10 True: (a).

7.3.11 PD, ND: 1; PS, NS: $n - 1$; I: $n(n - 1)/2$. (The function $\mathbf{0}$ does not belong to any of these classes, therefore the sum of the above numbers is by one less than the result in Exercise 7.2.10.)

7.3.12 $\mathbf{A}$ is (positive or negative) definite.

7.3.13 $\mathbf{A}$ is *not* indefinite.

7.3.14 (a) $\mathbf{A}$ is *not* indefinite.

(b) $\mathbf{A}$ is indefinite or $\mathbf{A} = \mathbf{0}$.

(c) PD, ND: 0; PS, NS: the number of zeros in the main diagonal of the diagonal matrix; I, $\mathbf{0}$: $\dim V$.

(d) The same as (c) except for I having a maximum $\dim V - \max(r, s)$ where r and s are the numbers of positive and negative entries in the main diagonal of a diagonal matrix. (This formula is correct for every other type, too.)

7.4.

7.4.2 Only $\mathbf{A} = \mathbf{0}$ has this property.

7.4.3 True: (a).

7.4.6 We write diagonal matrices with entries 1, −1, or 0 in the main diagonal. The elements of the $\mathbf{A}$-orthogonal bases below have to be multiplied by suitable scalars to yield these matrices.

(a) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\mathbf{A}$-orthogonal basis (as coordinate vectors corresponding to the original basis): $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix}$, $\tilde{\mathbf{A}}(\mathbf{x}) = |x_1 + ix_2|^2$, PS.

(b) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathbf{A}$-OB: $\begin{pmatrix} 1 \\ -i \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix}$,

$\tilde{\mathbf{A}}(\mathbf{x}) = |(x_1 + ix_2)/\sqrt{2}|^2 - |(x_1 - ix_2)/\sqrt{2}|^2$, I.

c) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\mathbf{A}$-OB: $\begin{pmatrix} 1 \\ \rho^2 \\ \rho \end{pmatrix}, \begin{pmatrix} 1 \\ \rho \\ \rho^2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$,

$\tilde{\mathbf{A}}(\mathbf{x}) = |x_1 + \rho x_2 + \rho^2 x_3|^2$, PS.

7.4.7 (a) The set of non-negative, non-positive, or all real numbers, or the 0 alone.

7.4.8 (a) The matrix is the negative of its adjoint.

(c) There are only imaginary numbers in the range of the quadratic form.

7.4.9 True: (c).

8. Euclidean Spaces

8.1.

8.1.4 Orthonormal bases:
- (a) $1/\sqrt{2}, x\sqrt{3/2}, (x^2 - 1/3)\sqrt{45/8}$;
- (b) $1, x - 1, (x - 1)^2/2$;
- (c) $1/3, x/\sqrt{60}, (x^2 - 20/3)/\sqrt{308}$;
- (d) $1/3, (x - 5)/\sqrt{60}, [(x - 5)^2 - 20/3]/\sqrt{308}$.

8.1.7
- (a) $W_1^\perp = \{\mathbf{v} \mid v_3 = v_4 = v_5 = 0\}$.
- (b) $W_2^\perp = \{\mathbf{v} \mid \sum_{j=1}^5 v_i = 0\}$.
- (c) $W_3^\perp = \{\mathbf{v} \mid v_1, \ldots, v_5$ is an arithmetic progression$\}$.

8.1.12 There are infinitely many such inner products.

8.1.15 (c) $\mathbf{0}$.

8.2.

8.2.1 $\sqrt{2}$.

8.2.2 $60°$.

8.2.3
- (a) The Pythagorean theorem and its converse.
- (b) A parallelogram is a rhombus if and only if its diagonals are perpendicular.
- (c) The sum of squares of the sides in a parallelogram is equal to the sum of squares of the diagonals.

8.2.4 Normed spaces: (b), (d), (e).

8.2.6 Metric space: (b), (c).

8.2.7 Example (c) in the previous exercise works.

8.2.8 Equality holds if and only if every x_j is equal and is non-negative.

8.2.9 True: (a).

8.2.10 (a) $30°$. (b) $120°$. (c) $45°$.

8.2.11
- (a) 16 vertices, 32 edges, and 8 body diagonals.
- (b) 2.
- (c) $60°$.

(d) 60°, 90°, or 120°.
(e) Circumsphere radius is 1, insphere radius is 1/2.

8.2.12 The distance of two sets is the infimum of distances of their points. In the example, the distance of the vector and the subspace is 5.

8.2.15 Equality holds if and only if $\mathbf{x} \in \langle \mathbf{c}_1, \ldots, \mathbf{c}_k \rangle$.

8.2.17 (a) n. (b) 3 (if $n \geq 2$).

8.3.

8.3.3 In (a) only $\Rightarrow$ holds; in (b) only $\Leftarrow$ holds; (c) remains valid.

8.4.

8.4.2 (a), (b), (e), (f): $\mathcal{A}^* = \mathcal{A}$.
(c), (d): $\mathcal{A}^* = A^{-1}$.
(g) and (h) are adjoints of each other.

8.4.3 $\mathcal{A}^* = -\mathcal{A}$.

8.4.4 Let $h = \beta_0 + \beta_1 x + \beta_2 x^2$.
(a) $\mathcal{A}^* h = (15\beta_0 + 5\beta_2)(3x^2 - 1)/2$.
(b) $\mathcal{A}^* h = (\beta_0 + \beta_1 + \beta_2)(x - 1)^2/2$.
(c) and (d) $\mathcal{A}^* h = (3\beta_0 + 20\beta_2)(3x^2 - 20)/154$.

8.4.5 The converse is true only in a complex Euclidean space.

8.4.12 The converse is true in (a) and false in (b).

8.4.14 (a) $\mathcal{A} = \lambda\mathcal{I}$.

8.5.

8.5.1 (b) False.

8.5.4 False.

8.5.5 $\mathcal{A}$ and $\mathcal{C}$ are not normal; $\mathcal{B}$ is unitary; $\mathcal{D}$ is self-adjoint; and $\mathcal{E}$ is normal (but is neither self-adjoint, nor unitary).

8.5.6 If $\mathcal{A}$ and $\mathcal{B}$ are self-adjoint, then $\mathcal{A} + \mathcal{B}$ and $\mathcal{A}^2$ are self-adjoint, but $\lambda\mathcal{A}$ and $\mathcal{A}\mathcal{B}$ are not necessarily self-adjoint.

If $\mathcal{A}$ and $\mathcal{B}$ are unitary, then $\mathcal{AB}$ and consequently $\mathcal{A}^2$ are unitary, but this is not necessarily true for $\lambda\mathcal{A}$ and $\mathcal{A}+\mathcal{B}$.

If $\mathcal{A}$ and $\mathcal{B}$ are normal, then $\lambda\mathcal{A}$ and $\mathcal{A}^2$ are normal, but $\mathcal{A}+\mathcal{B}$ and $\mathcal{AB}$ are not necessarily normal.

8.5.7 (a) The claim is false.

8.5.8 The converse is false.

8.5.9 True: (a).

8.6.

8.6.1 The converse is false

8.6.3 S=orthonormal eigenbasis, O=orthonormal basis given in Theorem 8.6.4.

(a) $\mathcal{A}$ is both symmetric and orthogonal.

S: $1/\sqrt{2}$ times $\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$.

The main diagonal of the diagonal matrix is $1, 1, -1, -1$.

(b) $\mathcal{B}$ is symmetric.

S: multiples of $\begin{pmatrix}-1\\1+\sqrt{2}\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1+\sqrt{2}\end{pmatrix}, \begin{pmatrix}-1\\1-\sqrt{2}\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1-\sqrt{2}\end{pmatrix}$.

The main diagonal of the diagonal matrix is $-\sqrt{2}, -\sqrt{2}, \sqrt{2}, \sqrt{2}$.

(c) $\mathcal{C}$ is orthogonal.

O: 1/2 times $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}$.

Matrix: $\begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}$ (the lower right 2×2 block corresponds to a rotation of 90 degrees).

(d) $\mathcal{D}$ is symmetric.

S: same as for $\mathcal{C}$. The main diagonal of the diagonal matrix is $4, 0, 0, 0$.

(e) $\mathcal{E}$ is orthogonal.

O: $1/\sqrt{2}$ times $\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\-1\end{pmatrix}, \begin{pmatrix}1\\0\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$.

The matrix is the same as for $\mathcal{C}$.

8.6.4 No.

8.6.5 True: (a), (d).

8.6.6 The analogue for symmetric transformations is false.

8.6.10 Symmetric transformations: we stretch (or compress) in the plane/space in two/three pairwise orthogonal directions by not necessarily equal rates. We can even reflect through one or more lines/planes perpendicular to a direction.

Orthogonal transformations: In the plane: reflections across axes (containing the origin) and rotations (around the origin, by any angle). In the space: reflections across planes (containing the origin), rotations around axes (containing the origin, by any angle) possibly combined with a reflection across a plane perpendicular to the axis (this includes the reflection across the origin, too).

8.6.11 The converse is false.

9. Combinatorial Applications

9.1.

9.1.1 The minimal number of questions is (a) 20; (b) 2; (c) 1.

9.1.3 It is no longer valid.

9.1.4 (a) (i): $\lceil \log_2 m \rceil$ where $\lceil x \rceil$ denotes the ceiling or upper integer part of x (i.e., the minimum of integers not less than x). (ii): $m-1$ (if $m \geq 2$).

(b) (i): $\lceil \log_k m \rceil$. (ii): $\lceil (m-1)/(k-1) \rceil$ (if $m \geq k$).

(c) We consider only the analogues of (a) (i.e., when $k = 2$), the general question (b) (for arbitrary k) can be discussed similarly. Concerning (i), the minimum for $p < m$ is $\lceil \log_2 p \rceil$ (instead of $\lceil \log_2 m \rceil$). There is also a change in (ii) if p is not too large compared to m: as $\lceil \log_2 p \rceil$ boring vectors are sufficient anyway, the minimum will be less than $m-1$ for $p \leq 2^{m-2}$. If, however p is sufficiently large compared to

m, then we have the same minimum $m-1$ as over the reals (or any infinite field).

9.1.5 (a) 5. (b) 31.

9.1.6 (a) The answer is yes for both questions.
(b) There exist countably many sets but not more.

9.1.7 Yes: (a).

9.1.9 Yes: (b).

9.1.10 Yes: (a2), (b2).

9.2.

9.2.1 (a) $(2^{1000}-1)/3$.
(b) $\big((1+\sqrt{2})^{999}+(1-\sqrt{2})^{999}\big)/2$.

9.2.2 (a) 4443. (b) 3. (c) 3.

9.2.5 $\beta_n = \varphi_{n+3} - 2$ (where φ_n is the nth Fibonacci number).

9.2.7 (a) φ_{n+1}.
(b) For n odd, there is no such tiling, and for $n = 2k$, the number of tilings is $\big((3+\sqrt{3})(2+\sqrt{3})^k + (3-\sqrt{3})(2-\sqrt{3})^k\big)/6$.

9.2.8 φ_{n+2}.

9.2.11 Also the second neighbors are coprime. The gcd of third neighbors with indices divisible by 3 is 2, the others are coprime. (Cf. Exercise 9.2.13.)

9.2.14 (a) φ_{n+1}.
(b) $\big((1+\sqrt{2})^n - (1-\sqrt{2})^n\big)/(2\sqrt{2})$. These are called *Lucas numbers* and are obtained as the solution of the recursion $\alpha_{i+1} = 2\alpha_i + \alpha_{i-1}$, $\alpha_0 = 0, \alpha_1 = 1$.

9.2.15 $(5-\sqrt{5})/2$.

9.2.16 $\binom{2n-2}{n-1}/n$.

9.2.17 $\binom{2n-4}{n-2}/(n-1)$.

9.3.

9.3.4 The suitable condition is $t \geq (q-1)k+1$.

9.3.8 (c) $86519 = 241 \cdot 359$ and $584189 = 613 \cdot 953$.

9.4.

9.4.1 (a) 2^{k-1}.

(b) $\left(2^k + 2\cos(k\pi/3)\right)/3$. The (smallest) period of $\cos(k\pi/3)$ is 6, so we can rewrite this result according to the modulo 6 remainder of k. We get $(2^k + 2)/3$ if $k \equiv 0 \pmod 6$; $(2^k + 1)/3$ if $k \equiv \pm 1 \pmod 6$; $(2^k - 2)/3$ if $k \equiv 3 \pmod 6$; and $(2^k - 1)/3$ if $k \equiv \pm 2 \pmod 6$.

9.4.2 (a) H and H' are complements.

(b) It is the symmetric difference of H and H'.

9.4.4 (a) $\beta_{ij} = |H_i \cap H_j|$ modulo 2.

9.4.6 k, if k is odd; and $k-1$, if k is even.

9.4.7 (a) k. (b) k.

9.4.8 (a) k. (b) $k-1$.

9.4.9 k.

9.4.10 k.

9.4.11 1 (and every inhabitant is a member in this club).

9.4.12 $\sum_{i=0}^{m} \binom{k}{i}$.

9.4.13 (b) p^2, i.e., the maximal dimension of the subspace is 2.

9.4.14 (a) $k \geq 3$ for $p \equiv 3 \pmod 4$ and $k \geq 2$ for other primes.

(b) If only the zero vector is orthogonal to itself, i.e., $k = 1$ and p is arbitrary or $k = 2$ and $p \equiv 3 \pmod 4$, then this is a trivial subspace of dimension 0. Otherwise only $p = 2$ yields a subspace and k can be arbitrary. This subspace consists of the vectors with an even number of components 1 and its dimension is $k - 1$.

9.4.16 There exists a subspace U: (a), (c), (e).

9.4.17 (a) Not necessarily. (b) We can always form a new club.

9.4.19 8.

9.5.

9.5.1 (b) The eigenvalues are 3, 1, and -2 with multiplicities 1, 5, and 4.

9.5.3 (a) $n-1$ and -1 with multiplicities 1 and $n-1$.

(b) 1 and -1, both with multiplicity k.

(c) k, $-k$, and 0 with multiplicities 1, 1, and $n-2$.

(d) $\sqrt{n-1}$, $-\sqrt{n-1}$, and 0 with multiplicities 1, 1, and $n-2$.

(e) $2\cos(2j\pi/n)$, $0 \le j \le n-1$ (with multiplicity 1).

9.5.4 Let $d, \lambda_2, \ldots, \lambda_n$ be the n (not necessarily distinct) eigenvalues of the adjacency matrix of the original graph where d denotes the degree of each vertex. Then $n-1-d, -1-\lambda_2, \ldots, -1-\lambda_n$ are the corresponding eigenvalues of the complement.

9.5.6 The 10×15 incidence matrix of the Petersen graph consists of six 5×5 blocks C_{ij}, $i = 1, 2$, $j = 1, 2, 3$, where $C_{12} = C_{21} = 0$, $C_{13} = C_{23} = I$,

$$C_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad C_{22} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Incidence matrices of the graphs in Exercise 9.5.3.

(a) The non-zero entries in the columns of an $n \times n(n-1)/2$ matrix are all possible pairs of 1.

(b) Two $k \times k$ identity matrices I_k one above the other.

(c) The non-zero entries in the columns of a $(2k) \times (k^2)$ matrix are all possible pairs of 1 with one element from the upper k rows and the other element from the lower k rows.

(d) A row with entries 1 above an $(n-1) \times (n-1)$ identity matrix I_{n-1}.

(e) The $2n$ entries 1 are in and just below the main diagonal and in the upper right corner of an $n \times n$ matrix and all other entries are 0.

9.5.7 $M = C^T C$ is an $m \times m$ matrix, where every entry μ_{ii} in the main diagonal is 2 and μ_{ij} is 1 or 0 for $i \ne j$ according to whether or not the ith and jth edges share a common vertex

$N = CC^T$ is an $n \times n$ matrix, where ν_{ii} in the main diagonal is the degree of the ith vertex and ν_{ij} is 1 or 0 for $i \ne j$ according to whether or not there is an edge between the ith and jth vertices.

9.5.8 Unions of disjoint triangles.

9.6.

9.6.7 (a) The powers of two are pretty.

9.7.

9.7.4 (a) Yes. (b) No.

9.8.

9.8.5 (b) The four points are coplanar if and only if the determinant $\begin{vmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} & \gamma_{24} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} & \gamma_{34} \\ 1 & 1 & 1 & 1 \end{vmatrix}$ formed of the coordinates is 0.

(c) The results are true in any coordinate system.

10. Codes

10.1.

10.1.1 (a) $(1-p)^k$. (b) $kp(1-p)^{k-1}$. (c) $1-\sum_{i=0}^{3}\binom{k}{i}p^i(1-p)^{k-i}$.

10.1.2 1-error detecting: (a), (b), (e), (f).
1-error correcting: (e).

10.1.3 In general, the error-detecting and error-correcting capacities of a code are not affected if (i) we change the digits at an arbitrary number of fixed places, i.e., we add the same vector to all codewords (translation of the codewords); (ii) we apply the same permutation to the digits of all codewords; (iii) we perform the composition of (i) and (ii). The resulting codes are called *equivalent* to the original one.

10.1.4 (b) m is odd.

10.1.5 There is no such $\mathbf{z}$ if $r+q-d$ is odd and there are $\binom{k-d}{j}\binom{d}{q-j}$ such vectors $\mathbf{z}$ if $r+q-d$ is even.

10.1.7 The minimal distance increases by 1 if d is odd and does not change if d is even.

10.1.9 $n=2$: (aA) 1. (aB) 3. (bA) 3. (bB) 6.
$n=3$: (aA) 1. (aB) 3. (bA) 3. (bB) 7.

10.2.

10.2.1 True: (b).

10.2.2 Two or three $n \times n$ identity matrices one above the other.

10.2.3 Generator matrices:

$$\text{(b)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{(e)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{(f)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

As (b) and (f) are not 1-error correcting, we only construct a decoding table of (e):

000000	100110	010101	001011	110011	101101	011110	111000
100000	000110	110101	101011	010011	001101	111110	011000
010000	110110	000101	011011	100011	111101	001110	101000
001000	101110	011101	000011	111011	100101	010110	110000
000100	100010	010001	001111	110111	101001	011010	111100
000010	100100	010111	001001	110001	101111	011100	111010
000001	100111	010100	001010	110010	101100	011111	111001
100001	000111	110100	101010	010010	001100	111111	011001

10.2.6 The dimension is $n-1$ or n.

10.2.7 (a) $d_3 \geq d_1 + d_2$; $\quad d_4 = \min(d_1, d_2)$; $\quad d_5 = \min(2d_1, d_2)$.

(b) $G_3 = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$; $\quad G_4 = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$; $\quad G_5 = \begin{pmatrix} G_1 & 0 \\ G_1 & G_2 \end{pmatrix}$.

10.2.8 (a) Let $g = \sum_{r=0}^{s} \delta_r x^r$. Then the elements of the $k \times n$ generator matrix G are $\gamma_{ij} = \begin{cases} \delta_r, & \text{if } i = j + r,\ 0 \leq r \leq s \\ 0, & \text{otherwise.} \end{cases}$ (i.e., we write the coefficients of g into every column starting from the main diagonal of G).

10.3.

10.3.2 Each code is systematic, i.e., the generator matrix is of the form $G = \begin{pmatrix} I_{n\times n} \\ B_{s\times n} \end{pmatrix}$, so $P = (\, B_{s\times n} \quad I_{s\times s}\,)$ is a parity-check matrix (cf. Exercise 10.3.5(a)).

10.3.10 The transpose of the generator matrix of C is a parity-check matrix of $C^\perp$ and vice versa.

10.3.12. 3.

10.4.

10.4.4 (a) 10.

A. Basic Algebra

A.1.

A.1.4 $a_n = 2^n - 1$.

A.1.6 $\binom{1999}{3}$.

A.1.8 (a) 2^{n-1}. (b) $(-1)^n$.

A.1.9 (a) (a1) 0. (a2) $n!$. (a3) The formula in part (b). (This is valid also for $k < n$ and $k = n$, but then the direct argument is much simpler.)

A.1.10 Equivalence relation: (b), (c), (d). A class of (b) contains all integers giving the same residue upon division by 3, so there are 3 infinite classes. Relation (c) is equal to (b) by $4a + 5b = 3(a + 2b) + a - b$. A class of (d) contains an integer and its negative, so there are infinitely many 2-element classes plus the 1-element class $\{0\}$.

A.1.11 No.

A.1.12 (a) 2^{n^2}. (b) 2^{n^2-n}. (c) $2^{n(n+1)/2}$.

A.2.

A.2.2 True: (a), (c), (e), (h).

A.2.4 (c) 8.

A.2.5 True: (a), (d), (e), (h).

A.2.7 0 for n odd, and $n/2$ for n even.

A.2.8 It is possible: (a).

A.2.9 (a) m is odd or is a multiple of 4.
(b) m is odd.

A.2.10 (a) $\varphi(p^k) = p^k - p^{k-1}$.
(b) (b1) $n = 1, 2$. (b2) $n = 2^k p_1 \dots p_r$ where $k \geq 0$, $r \geq 0$, and p_i are distinct primes of the form $2^s + 1$.

A.2.11 49.

A.2.13 $x \equiv 3 \pmod{11}$.

A.2.14 496.

A.2.15 36.

A.3.

A.3.1 (a) $3 + 2i$. (b) $-i$. (c) $\pm(3 - 2i)$. (d) $\sqrt{2}e^{i(1+4k\pi)/12}$, $0 \leq k \leq 5$.
(e) $\sqrt[10]{12}e^{i(7+12k\pi)/30}$, $0 \leq k \leq 4$.

A.3.2 (a) A horizontal line 4/5 units below the x-axis.
(b) The lower open half-plane bounded by the horizontal line 2 units below the x-axis.
(c) A closed disc with center $(3, -8)$ and radius 1.
(d) Two closed half-lines starting from the origin.
(e) The lower closed half-plane bounded by the horizontal line $b = 2$.
(f) A line through the origin.
(g) A circle with center $(-2, 0)$ and radius 1 except the point $(-3, 0)$.

A.3.3 (a) $\pm 2\sqrt{2}i$. (b) $-1 \pm i$. (c) $1 - 2i$ and $-2 + i$.

A.3.5 The converse and the analog for three squares are false.

A.3.6 (a) $(-4, 3)$. (b) $\big((3 - 4\sqrt{3})/2, (4 + 3\sqrt{3})/2\big)$.

A.3.8 $16(\sin x)^5 - 20(\sin x)^3 + 5\sin x$.

A.3.9 (b) $2^{n/2}\cos(n\pi/4)$.

A.3.10 (a) $1, (-1 \pm i\sqrt{3})/2$. (b) $\pm 1, (\pm 1 \pm i\sqrt{3})/2$.

A.3.11 (b) The difference of their arguments is $\pm 2\pi/3$.

A.3.12 Sum: $S_n = 0$ if $n > 1$. Product: $P_n = 1$ if n is odd, and $P_n = -1$ if n is even. (So $P_n = (-1)^{n+1}$.)

A.3.13 (a) $k/(k,t)$.

A.3.14 (a) 1 for $n \neq 2$, and -1 for $n = 2$.
(b) Let T_n denote the sum of all primitive nth roots of unity. Then $T_7 = -1$, $T_{27} = 0$, and $T_n = (-1)^r$ if n is the product of r distinct primes factors, and 0 otherwise.

A.3.16 $\dfrac{\sin(nx/2)\cos((n+1)x/2)}{\sin(x/2)}$ if $x \neq 2m\pi$, and n if $x = 2m\pi$ where m is an integer.

A.4.

A.4.1 Not an operation: (b1), (d1), (d2), (e2), (i3).

Commutative: (a1), (a2), (b2), (c1), (c2), (c3), (d3), (e1), (f1), (f2), (g), (h), (i2).

Associative: (a1), (a2), (b2), (c1), (c2), (c3), (d3), (e1), (e3), (f1), (f2), (i1), (i2).

Identities and inverses:

(a1) $e = 0$ and every element has an inverse.
(a3) 0 is a right identity.
(b2) $e = 1$ and only ± 1 have an inverse.
(c1) and (c3): $e = 1$ and only 1 has an inverse.
(d3) $e = 0$ and every element has an inverse.
(e1) and (e3): e is the identity transformation and every element has an inverse.
(f1) $e = \emptyset$ and only e has an inverse.
(f2) $e = \emptyset$ and every element is the inverse of itself.
(h) $e = 5$, the inverse of 5 is itself, and every other element is the inverse of every other element.
(i1) All matrices with upper left element 1 are left identities.
(i2) $e = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ and every non-zero matrix has an inverse.

A.4.2 The identity is the identical transformation (mapping every element to itself). The *bijections* have an inverse which is unique due to associativity. If X is finite, then no other functions have a right or left inverse. Let X be infinite, and by the usual convention, the composition fg of functions f and g means that we apply first g and then f. In this case, exactly the *injections* (where the images of distinct elements are distinct) have a left inverse and each injection that is not a bijection has infinitely many left inverses. Similarly, exactly the *surjections* (where every element of X is an image) have a right inverse and each surjection that is not a bijection has infinitely many right inverses.

A.4.3 Operations: n^{n^2}. Commutative ones: $n^{n(n+1)/2}$. Operations with an identity: n^{n^2-2n+2}.

A.4.4 The converse is false.

A.4.5 Only (d) is true.

A.4.7 We can infer that the equation $xb = a$ has at least one solution, and the equation $by = a$ has at most one solution.

A.5.

A.5.1 Field: (a2), (b1), (c2), (d2), (d3), (d5).

A.5.2 Field: $m = 3$.

A.5.3 Field: (a), (c), (d), (e), (g).

A.5.4 (b) A.5.1: (b1) is isomorphic to F_5; (c2), (d2), (d3) are isomorphic to $\mathbf{R}$; (d5) is isomorphic to $\mathbf{C}$.
A.5.3: (a), (c), (d), (e) are isomorphic to $\mathbf{R}$; (g) is isomorphic to $\mathbf{C}$.

A.5.6 Only (c) can be a field.

A.6.

A.6.2 (a) (A): ± 1. (B): $c + d\sqrt{2}$ satisfying $c^2 - 2d^2 = \pm 1$. There are infinitely solutions: $\pm(1+\sqrt{2})^n$ where n is any integer. (C): $\pm 1, \pm i$. (D): The non-zero constant polynomials. (E): ± 1.

(b) A sequence has an inverse if and only if no element in it is 0, and all other non-zero sequences are zero divisors. Similarly, a function has an inverse if and only if it assumes nowhere the value 0, and all other non-zero functions are zero divisors.

(c) The residue class $\{\ldots, -127, -27, 73, 173, \ldots\}$, or, equivalently, the remainder 73.

A.6.3 As 0 is excluded from the zero divisors and it cannot have an inverse, we investigate the non-zero elements.

A.5.1: (a1) No zero divisors. The fractions with odd numerators have an inverse. (b2) Every element is a zero divisor, there is no identity. (c1) The functions having a non-zero root are zero divisors, all other functions have an inverse. (d1) The product of any two elements is 0, so every element is a zero divisor and there is no identity. (d4) There is no identity (but there are infinitely many left identities: the matrices satisfying $a+b=1$). Every element is a right zero divisor, and the left zero divisors are the matrices with $a+b=0$.

A.5.2: (a) 1 and i have an inverse, and $1+i$ is a zero divisor. (c) The eight non-zero elements satisfying $5 \mid a^2+b^2$ are zero divisors, the other sixteen non-zero elements have an inverse.

A.5.3: (f) $a+bi$ is a zero divisor if and only if exactly one of a and b is 0, all other non-zero elements have an inverse.

A.6.5 (b) The last property implies the other two. Such rings are called *Boolean rings*.

A.6.6 Left cancellation is possible if and only if c is neither 0, nor a left zero divisor. So, we can cancel any non-zero element if the ring is zero divisor free, including fields and the ring of integers. In $\mathbf{Z}_m$, exactly the reduced residue classes enable cancellation: $ca \equiv cb \pmod{m}$ implies $a \equiv b \pmod{m}$ if and only if $(c, m) = 1$.

A.6.7 True: (a), (d).

A.6.11 True: (c).

A.7.

A.7.2 If zero divisors are allowed, then only II. remains valid.

A.7.3 (c) $|F|^{|F|} - (|F|-1)^{|F|} - 1$.

A.7.6 (a) The one element subsets, $H^a = \{x \geq a\}$, $H_a = \{x \leq a\}$, and the entire $\mathbf{R}$. (In other words, the points, the closed half-lines, and the entire number line.)

(b) Only the one element subsets and the entire $\mathbf{C}$.

A.7.12 $f = \alpha_n(x-\gamma)^n$.

A.7.13 True: (a), (c).

A.7.14 (a) The divisibilities over $\mathbf{Q}$ and $\mathbf{C}$ are equivalent. The divisibility over $\mathbf{Z}$ implies every other divisibility, but the converse is false. There is no connection between the divisibilities over F_2 and $\mathbf{Q}$ or $\mathbf{C}$.

(b) Now the divisibilities over $\mathbf{Q}$, $\mathbf{C}$, and $\mathbf{Z}$ are equivalent, and these imply the divisibility over F_2, but the converse is false. (The same holds if we only assume f to be monic.)

A.7.16 $x^{(n,k)} - 1$.

A.7.17 There is no such polynomial.

A.7.18 The equation is solvable if and only if $(f,g) \mid h$. There are infinitely many solutions. We can obtain a solution u_0, v_0 from the Euclidean algorithm. All solutions are $u = u_0 + wg/(f,g)$, $v = v_0 - wf/(f,g)$ where $w \in F[x]$ is an arbitrary polynomial.

A.7.19 I. $n \geq 2$. II. $n = 2$ or 3.

A.7.20 (a) $\prod_{k=1}^{4}(x-\vartheta_k)$ where $\vartheta_k = e^{i(2k+1)\pi/4}$.

(b) $(x^2 + x\sqrt{2} + 1)(x^2 - x\sqrt{2} + 1)$.

(c) Irreducible($= \Phi_8$).

(d) $(x+1)^4$.

(e) $(x^2 + x - 1)(x^2 - x - 1)$.

A.7.22 Irreducible: (a), (c), (d).

A.7.24 For m even, $\Phi_{2m}(x) = \Phi_m(x^2)$, and for $m > 1$ odd, $\Phi_{2m}(x) = \Phi_m(-x)$ (for $m = 1$ we have $\Phi_2(x) = -\Phi_1(-x)$).

A.7.26 (a) The $5k$th complex roots of unity that are *not* kth roots of unity.

(b) $k = 5^s$, $s = 0, 1, 2, \ldots$

A.7.27 n.

A.7.29 $2b^3 - 9abc + 27a^2d = 0$.

A.7.30. All other coefficients are 0.

A.8.

A.8.1 Tetrahedron: 24, cube and octadehron: 48, dodecahedron and icosahedron: 120.

A.8.2 One of the directions is false for fourth powers.

A.8.4 It can occur.

A.8.5 True: (a), (c).

A.8.7 (a) If there is exactly one element of order 2, then the product equals this element, otherwise the product is the identity.

(b) -1.

A.8.8 Each group has 8 elements but they are of five different "types": (i) ab; (ii) chj; (iii) de; (iv) f; (v) gi. (So, e.g., (c), (h), and (j) are isomorphic, but they are not isomorphic to any other group in the list.)

Remark: It can be proved that there do not exist eight element groups of other type, i.e., every eight element group is isomorphic to some of the groups in the list.

A.8.10. (a) $|G|$ is 1 or a prime. (b) G is finite.

A.8.11 The symmetry group of the rectangle has this property. A group of odd size cannot satisfy the condition.

A.8.12 (a) $d(n)$, i.e., the number of positive divisors of n.

(b) $d(n) + \sigma(n)$ where $\sigma(n)$ is the sum of the positive divisors of n.

A.9.

A.9.1 The ideals are the subgroups of the additive group.

A.9.2 Prime powers (including the first power, i.e., the primes when this ideal contains only 0).

A.9.5 (b) k and m/k are coprime.

A.9.7 The analog of Theorem A.9.3 can be summarized as $(a_1, \ldots, a_k)$ is the tightest ideal containing the elements a_i.

A.9.8 (a) The principal ideal (A) consists of the subsets of A.

A.9.9 (a) $I = (6)$; $\mathbf{Z}/I = Z_6$.

(b) $I = (2)$; $\mathbf{Z}_{100}/I \cong F_2$.

(c) I consists of the polynomials (with integer coefficients) having an even constant term; $\mathbf{Z}[x]/I \cong F_2$.

A.9.11 $|R/I| = 16$ and $R/I \cong F_2^{2\times 2}$ (the ring of 2×2 matrices over F_2).

A.9.12 (a) $g \in (f) \iff g(c) = 0$ for every $c < 5$.

A.9.13 True: (a), (c).

A.9.14 Field: (c), (d).

A.10.

A.10.7 The sum of an algebraic and a transcendental number is always transcendental. The sum of two transcendental numbers can be algebraic or transcendental.

A.10.8 (a) (i) Both are transcendental. (ii) Both are transcendental, or one of them is 0, and the other is transcendental. (iii) At least one of them is transcendental (show examples when both are transcendental, and when one of them is algebraic). (iv) Both are algebraic.

(b) We get analogous answers except at (iv) where the two original numbers can be irrational (of a special form).

Remark: In (i)–(iii) we use just the field properties, but in (iv) we have to take square roots, too, and this causes the difference in the answers to (iv).

A.10.10 Transcendental: (c), (d). Degrees: (a) 100; (b) 4; (e) 3; (f) 3; (g) $\deg 1 = 1$, the others have degree 100; (h) $\deg \pm 1 = 1$, the others have degree 2; (i) $\varphi(n)$; (j) 48.

A.10.11 Yes.

A.10.12 ± 1.

A.10.13 $\deg(\Theta^2) = k$ or $k/2$.

A.11.

A.11.2 The sum is $S = 0$ except for the field of two elements and the product is $P = -1$ (and $-1 = 1$ for $p = 2$).

A.11.3 $(m, p^k - 1)$.

A.11.4 1 if k is odd, and 3 if k is even (we do not distinguish the pairs (Θ, Ψ) and (Ψ, Θ)).

A.11.12 (a) $\varphi(p^k - 1)/k$.

(b) $(1/k) \sum_{d \mid k} \mu(d) p^{k/d}$ where $\mu(n)$ is the *Möbius function*: $\mu(1) = 1$, $\mu(n) = (-1)^s$, if n is the product of s distinct primes, and $\mu(n) = 0$ otherwise.