REU 2010 - Apprentice program

Linear Algebra Exercises

Instructor: László Babai e-mail: laci@cs.uchicago.edu
Compiled by Daniel Studenmund, Ben Fehrman, Laurie Field, Daniele Rosso, Katherine Turner, and the instuctor

Last updated Fri July 23, 8:30pm

1. **(Rational functions)** Prove that the rational functions $\{1/(x-\alpha) : \alpha \in \mathbb{R}\}$ are linearly independent over $\mathbb{R}$. (This will show that the space of rational functions has uncountable dimension.) Recall that an infinite collection is linearly independent if each finite subset is linearly independent.
Challenge: Find a basis for the space of rational functions $\mathbb{R}(x)$ over $\mathbb{R}$.

2. **(Trigonometric functions)** Prove that the functions $\{1, \cos x, \cos 2x, \ldots, \sin x, \sin 2x, \ldots\}$ are linearly independent over $\mathbb{R}$.

3. **(Modular identity)** Let U_1 and U_2 be subspaces of a vector space V. Then,
$$\dim(U_1) + \dim(U_2) = \dim(U_1 + U_2) + \dim(U_1 \cap U_2).$$

4. **(Matrix rank)** (a) Let A be a $k \times \ell$ matrix over $\mathbb{Z}$. Then,
$$\mathrm{rk}_2(A) \le \mathrm{rk}_{\mathbb{Q}}(A) = \mathrm{rk}_{\mathbb{C}}(A),$$
where $\mathrm{rk}_2(A)$ denotes the rank of A over $\mathbb{F}_2$. (b) Find a $(0,1)$-matrix A such that $\mathrm{rk}_2(A) < \mathrm{rk}_{\mathbb{Q}}(A)$. (c) Prove: If A is a $(0,1)$-matrix then $\mathrm{rk}_2(A) > \log_2 \mathrm{rk}_{\mathbb{Q}}(A)$. (d) For every r, find a $(0,1)$-matrix A such that $\mathrm{rk}_2(A) = r$ and $\mathrm{rk}_{\mathbb{Q}}(A) = 2^r - 1$.

5. **(Perpendicular subspace)** Let $V = \mathbb{F}^n$. Let $S \subseteq V$ be a subset. We define the set $S^\perp \le V$ as the set of all those vectors in V that are perpendicular to all vectors in S.
   (a) Prove that $S^\perp$ is a subspace.
   (b) Prove: $S^\perp = \mathrm{Span}(S)^\perp$.
   (c) Prove: if $U \le V$ is a subspace, then
   $$\dim(U) + \dim(U^\perp) = \dim(V).$$
   (d) Prove: $(U^\perp)^\perp = U$.
   (e) U is *totally isotropic* if $U \le U^\perp$. Prove: if U is totally isotropic then $\dim(U) \le n/2$.
   (f) Prove that $\mathbb{C}^{2k}$ contains a totally isotropic subspace of dimension k. Prove the same with $\mathbb{F}_2, \mathbb{F}_5, \mathbb{F}_{13}$ in the place of $\mathbb{C}$.
   (g) Prove: the incidence vectors of a maximal Eventown club system form a maximal totally isotropic subspace of $\mathbb{F}_2^n$. Infer the Eventown Theorem: the number of clubs in Eventown is $\le 2^{\lfloor n/2 \rfloor}$ (See the Puzzle Problem sheet).

(h) Prove: every maximal totally isotropic subspace of $\mathbb{F}_2^n$ has dimension $\lfloor n/2 \rfloor$. Infer that all maximal Eventown club systems are maximum

6. (a) A *collineation* of a finite geometry is a permutation of the set of points which preserves collinearity (the relation of being on a line), i. e., it maps lines to lines. For the Fano plane with seven points (otherwise known as $\mathbb{P}^2\mathbb{F}_2$), find the number of collineations. Also, show that all points are equivalent, in the sense that any point may be sent to any other point by a collineation. (In fact, this is also true of pairs of distinct points.)

   (b) **(Fundamental theorem of projective geometry)** Suppose that (P, L) is a projective plane over the field F. If

$$\begin{cases} a_1, \ldots, a_4 \\ b_1, \ldots, b_4 \end{cases}$$

   are 2×4 points in general position (no three out of each quadruple is on a line), then there exists a collineation $f : P \to P$ satisfying $f(a_i) = b_i$ for each $i = 1, \ldots, 4$.

7. **(One-sided invertibility)** Let $A \in \mathbb{F}^{k \times \ell}$. (a) Prove: A has a right inverse iff A has full row rank; and, A has a left inverse iff A has full column rank. (b) Find a matrix A with multiple right inverses.

8. **(Two-entry determinant)** Find the $n \times n$ determinant

$$\begin{vmatrix} a & b & \ldots & b \\ b & a & \ldots & b \\ \vdots & & \ddots & \vdots \\ b & b & \ldots & a \end{vmatrix}$$

   where the diagonal entries are a and the remaining entries b. Give a simple closed-form expression.

9. **(Vandermonde determinant)** Show that the $n \times n$ Vandermonde determinant

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j).$$

   Note that the right-hand side is the product of $\binom{n}{2} = n(n-1)/2$ terms.

10. **(Hilbert matrix)** Fix $2n$-distinct numbers $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$. Then, the $n \times n$ matrix

$$H = \left(\frac{1}{\alpha_i - \beta_j} \right)_{n \times n}$$

    is nonsingular.

11. **(Tridiagonal determinants:)**

(a) Compute the value of the $n \times n$ tridiagonal determinant

$$\begin{vmatrix} 1 & 1 & 0 & & & & & \\ -1 & 1 & 1 & 0 & & & & \\ 0 & -1 & 1 & 1 & 0 & & & \\ & 0 & -1 & 1 & 1 & 0 & & \\ & & 0 & -1 & 1 & 1 & 0 & \\ & & & & & \ddots & & \\ & & & & & 0 & -1 & 1 \end{vmatrix}.$$

(b) Compute the $n \times n$ tridiagonal determinant

$$\begin{vmatrix} 1 & 1 & 0 & & & & & \\ 1 & 1 & 1 & 0 & & & & \\ 0 & 1 & 1 & 1 & 0 & & & \\ & 0 & 1 & 1 & 1 & 0 & & \\ & & 0 & 1 & 1 & 1 & 0 & \\ & & & & & \ddots & & \\ & & & & & 0 & 1 & 1 \end{vmatrix}.$$

12. **(Bases of $\mathbb{F}_p^n$)**

(a) Count the bases of $\mathbb{F}_p^n$. (Not a closed-form expression but a simple expression)

(b) Count the k-dimensional subspaces of $\mathbb{F}_p^n$. Denote this number by $f_p(n,k)$.

(c) Compute $\lim_{p \to 1} f_p(n,k)$. This should be a closed form expression with an intuitive meaning.

13. **(Change of basis)** Let $B = (b_1, \dots, b_n)$ and $B' = (b_1', \dots, b_n')$ be bases of V. For $v \in V$, if $v = \sum_{i=1}^n \beta_i v_i$ then we write $[v]_B = (\beta_1, \dots, \beta_n)^T$, the column vector which lists the coordinates of v with respect to the basis B. ("T" stands for "transpose" and serves typographic convenience here.) Prove: $[v]_{B'} = S^{-1}[v]_B$ where $S = [[b_1']_B, \dots, [b_n']_B]$ is the "basis change matrix."

14. **(Degree of freedom in choosing a linear map)** (a) Let $b_1, \dots, b_n$ be a basis of V and let $w_1, \dots, w_n$ be arbitrary vectors of W.

Prove: $(\exists! \quad \varphi : V \to W)\,(\forall i)(\varphi(b_i) = w_i)$

(b) Use this to give a vector-space isomorphism between $\operatorname{Hom}(V, W)$ and $F^{k \times n}$ where $k = \dim W$.

15. **(Rotations of Conic Sections)** Let $f(x,y) = ax^2 + bxy + cy^2$. Rotate the (x,y)-plane by an angle θ and get new coordinates (x', y'). This induces a linear tranformation on the space of all such polynomials. Write the matrix of this linear transformation with respect to the basis (x^2, xy, y^2).

16. **(Correspondence between the action of a linear map and matrix multiplication)** Let V, W, Z be vector spaces over Let $\varphi : V \to W$ be a linear map, E a basis of V, Φ a basis of W, and $v \in V$.

    Show that $[\varphi]_{E,\Phi}[v]_E = [\varphi(v)]_\Phi$.

17. (a) Let $A, B \in F^{k\times n}$. Prove: if $(\forall x \in F^n)(Ax = Bx)$ then $A = B$.

    (b) **(Correspondence between composition of linear maps and matrix multiplication)** Let V, W, Z be vector spaces over F with bases Ξ, Φ, Ψ. Let $\varphi : V \to W$ and $\psi : W \to Z$ be linear maps. Prove:

    $$[\psi\phi]_{\Xi,\Psi} = [\psi]_{\Phi,\Psi}[\phi]_{\Xi,\Phi}.$$

    (c) Let ρ_θ denote the rotation of the plane by θ about the origin. Recall that the matrix of this transformation with respect to an orthonormal basis (a pair of perpendicular unit vectors) is $[\rho_\theta] = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$. Use this matrix to infer the addition rules for the trigonometric functions.

18. **(Change of bases)** Let $\varphi : V \to W$ be a linear map, E a basis of V and Φ a basis of W. Let $E' = (e'_1, \ldots, e'_n)$ and $\Phi' = (f'_1, \ldots, f'_k)$ be new bases for V and W, respectively.

    Define $A = [\varphi]_{E,\Phi}$ and $A' = [\varphi]_{E',\Phi'}$, $S = [[e'_1]_E, \ldots, [e'_n]_E]$, $T = [[f'_1]_\Phi, \ldots, [f'_k]_\Phi]$.

    Show that $A' = T^{-1}AS$.

19. (a) Let $A \in F^{k\times n}$ and $B \in F^{n\times k}$. Prove: $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. (b) Prove: similar matrices have the same trace. ($A, B \in M_n(F)$ are *similar* if $(\exists S \in M_n(F))(B = S^{-1}AS)$.)

20. **(Determinant is multiplicative)** If $A, B \in M_n(F)$, then $\det(AB) = \det(A)\det(B)$.

21. **(Powers of a Matrix)** (a) Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. What is A^n? (Experiment, observe pattern, prove.) (b) Let $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. What is B^n?

22. **(Fibonacci-type sequences)**

    Let $\mathbb{R}^\mathbb{Z} = \{$ functions $\mathbb{Z} \to \mathbb{R}\} = \{\underline{a} = (\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots) | a_i \in \mathbb{R}\}$ be the space of doubly infinite sequences.

    We say that $\underline{a} \in \mathbb{R}^\mathbb{Z}$ is a <u>Fibonacci-type</u> sequence if $(\forall n \in \mathbb{Z})\,(a_n = a_{n-1} + a_{n-2})$. We denote the set of Fibonacci-type sequences by Fib. Let F_n denote the n-th Fibonacci number: $F_0 = 0$, $F_1 = 1$, $(F_n : n \in \mathbb{Z}) \in$ Fib.

    (a) Prove: $\mathrm{Fib} \le \mathbb{R}^\mathbb{Z}$ (subspace); $\dim \mathrm{Fib} = 2$. Prove that the Fibonacci sequence $\{F_n\}$ and the shifted Fibonacci sequence $\{F_{n+1}\}$ form a basis of Fib.

    (b) Find a basis of Fib consisting of geometric progressions $u_n = q_1^n$ and $v_n = q_2^n$. Determine q_1, q_2.

(c) **(Explicit formula for the Fibonacci numbers)** Prove: $F_n = \alpha q_1^n + \beta q_2^n$. Determine α, β.

23. **(Shift operator)** Let us define $\sigma : \mathbb{R}^{\mathbb{Z}} \to \mathbb{R}^{\mathbb{Z}}$ by $\sigma : \{a_n\} \mapsto \{a_{n+1}\}$.

    (a) Find all eigenvectors of σ.

    (b) Notice that Fib is invariant under σ. Let σ' denote the restriction of σ to Fib; so this is a linear transformation of Fib. Describe the matrix of σ' (a 2×2 matrix) with respect to the basis given in item (a) of the preceding problem.

    (b) Find a basis of Fib consisting of eigenvectors of σ'. Describe the matrix of σ' in this basis.

24. $\mathrm{rk}(A)$ is the size of the largest non-singular (square) matrix

25. Prove that the volume of the n-dim parallelpiped spanned by the basis $a_1, \ldots, a_n \in \mathbb{R}^n$ satisfies
$$\mathrm{Vol}(a_1, \ldots, a_n) = |\det(a_1, \ldots, a_n)|.$$
(Use only that volume is additive, translation invariant and satisfies that if $a_1, \ldots, a_n$ are orthogonal then $\mathrm{Vol} = \prod_{i=}^n \|a_i\|$.)

26. An *eigenbasis* for $A \in M_n(F)$ is a basis of F^n that consists of eigenvectors of A. Find the eigenvalues and an eigenbasis of the rotation matrix ρ_θ (Ex. 17 (c)) over $\mathbb{C}$. (Reward problem!)

27. (a) $A \in M_n(F)$ has an eigenbasis $\iff$ A is similar to a diagonal matrix D.

    (b) Ther diagonal entries of D are the eigenvalues of A.

28. The **Cayley-Hamilton Theorem** says that if $f_A(\lambda)$ is the characteristic polynomial of the matrix $A \in M_n(F)$ then $f_A(A) = 0$.

    (a) Verify the Cayley-Hamilton Theorem for 2×2 matrices.

    (b) Verify the Cayley-Hamilton Theorem for diagonal matrices.

29. Find an $n \times n$ matrix B of rank $n-1$ with $f_B(\lambda) = \lambda^n$.

30. $A \in M_n(F)$ is non-singular $\iff$ $\lambda = 0$ is not an eigenvalue.

31. **(Complex matrices)**

    (a) Prove that every matrix $A \in M_n(\mathbb{C})$ is similar to a triangular matrix over $\mathbb{C}$.

    (b) Show that the same is true over any algebraically closed field.

    (c) Show that the same is true over any splitting field of the characteristic polynomial of A. (F is a splitting field for the polynomial f if f can be written as a product of linear factors over F.)

32. **(Eigenvectors to distinct eigenvalues)** Suppose that $v_1, \ldots, v_k$ are eigenvectors of $\varphi : V \to V$ corresponding to distinct eigenvalues. Show that $v_1, \ldots, v_k$ are linearly independent.

33. **(Eigenvalue multiplicity)** Let $A \in M_n(F)$ and $\lambda \in F$. The *geometric multiplicity* of the eigenvalue λ is the dimension of the eigensubspace $U_\lambda = \mathrm{Ker}(\lambda I - A)$. (This dimension is zero exactly if λ is not an eigenvalue.) The *algebraic multiplicity* of λ is the largest k such that $(x - \lambda)^k$ divides the characteristic polynomial $f_A(x) = \det(xI - A)$. Prove that the geometric multiplicity of an eigenvalue is less than or equal to its algebraic multiplicity.

34. **(Symmetric polynomial in eigenvalues)** Suppose A is a matrix with with characteristic polynomial $f_A(x) = (x - \lambda_1) \ldots (x - \lambda_n)$ (so the λ_i are the eigenvalues). Let σ_k denote the k^{th} elementary symmetric polynomial. Show that

$$\sigma_k(\lambda_1, \ldots, \lambda_n) = \sum_{\binom{n}{k}} \det(k \times k \text{ symmetric minor}).$$

In particular, $\sum \lambda_i = \mathrm{Tr}(A)$ and $\prod \lambda_i = \det(A)$.

35. **(!!!)** Find the characterisitc polynomial and find all eigenvectors of the 'all-ones' matrix

$$J = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}.$$

36. Let $A = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 0 \\ 0 & 0 \end{bmatrix}$. Verify, using the definition of similarity, that these two matrices are similar: find C such that $B = C^{-1}AC$.

37. Prove: similar matrices have the same characteristic polynomial: if $A \sim B$ then $f_A(x) = f_B(x)$ where $f_A(x) = \det(xI - A)$.

38. (a) Prove that $A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ are not similar. (b) Prove that $B_1 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ are similar. The proofs should not involve any calculation.

39. (a) Prove that $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ is diagonalizable. Find the diagonal matrix similar to A. (b) Prove that $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is not diagonalizable.

40. **(Irreducible charcateristic polynomial)** Let $A \in M_n(\mathbb{Z})$. Prove: if the characteristic polynomial $f_A(x)$ is irreducible over $\mathbb{Q}$ then A is diagonalizable over $\mathbb{C}$.

41. **(Circulant determinants)** Fix an n-tuple $(a_0, \ldots, a_{n-1}) \in \mathbb{C}^n$. Define the *circulant matrix* as

$$C(a_0, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}.$$

Let $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ and set $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Show that

$$\det(C(a_0, \ldots, a_1)) = \prod_{j=0}^{n-1} f(\omega^j).$$

Hint: Find an eigenbasis shared by all circulant matrices. To do this, let $P = C(0, 1, 0, \ldots, 0)$. Note that $P^k = C(b_0, \ldots, b_{n-1})$ where $b_j = \delta_{jk}$; in particular, $P^n = I$. Find an eigenbasis for P; show that the eigenvalues of P are the n-th roots of unity; then use the equation $f(P) = C(a_0, \ldots, a_{n-1})$ to compute the eigenvalues of $C(a_0, \ldots, a_{n-1})$ (show that the eigenbasis of P is also an eigenbasis of $f(P)$).

42. If A and B are symmetric matrices (i. e., $A = A^T$ and $B = B^T$), then show that (a) AB is not necessarily symmetric, but (b) A^n is symmetric for any positive integer n.

43. If $U \leq \mathbb{R}[x]$ and U is invariant under the linear map d/dx then $(\exists k \in \mathbb{N} \cup \{\infty\})$ (U is the set of all polynomials of degree $< k$).

44. Prove: a matrix $A \in M_n(F)$ is diagonalizable if and only if F^n is the sum of the eigensubspaces of A.

45. $A_1, \ldots, A_m$ are $n \times n$ matrices that are diagonalizable over F and they pairwise commute. Show that they have a common eigenbasis. - Use the following fact: if $\varphi : V \to V$ is a linear transformation which has an eigenbasis and $U \leq V$ is a φ-invariant subspace (i. e., $(\forall u \in U)(\varphi(u) \in U)$) then the restriction of φ to U also has an eigenbasis.

46. Prove:

    (a) If $A, B \in M_n(\mathbb{C})$, then $AB - BA \neq I$.

    (b) The same is not true over all fields. Find a counterexample over $\mathbb{F}_p$ for every prime p.

47. Consider the linear transformations defined on $\mathbb{C}[x]$ by

$$A : f \mapsto \frac{df}{dx}, \qquad B : f \mapsto x \cdot f.$$

What is $AB - BA$?

48. If the Cayley-Hamilton theorem is true for A and $A \sim B$, then it is true for B.

49. Suppose $A_1, A_2, \ldots \in M_n(\mathbb{C})$ such that $\lim_{k\to\infty} A_k = B$. Assume that $(\forall k)($ C-H is true for $A_k)$. Prove: C-H is true for B.

50. If A has n distinct eigenvalues in F, then A is diagonalizable.

51. Among the triangular matrices over $\mathbb{C}$, the diagonalizable ones are everywhere dense.

52. Combine the preceding statements to a proof that the C-H Theorem is true for all complex matrices.

53. (a) Let $f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ and suppose f is identically zero. (Ex: $x^2 - y^2 - (x+y)(x-y) = 0$) Then f is identically zero over any field. (b) Infer that C-H is true over every field.

54. Let $A \in M_n(\mathbb{C})$.

    (a) Define $\mathrm{e}^A \in M_n(\mathbb{C})$.

    (b) Prove that e^{A+B} is not always equal to $\mathrm{e}^A\mathrm{e}^B$.

    (c) $\mathrm{e}^{A+B} = \mathrm{e}^A\mathrm{e}^B$ does hold under a natural condition on A, B. What is it?

    (d) Compute $\frac{d}{dt}\mathrm{e}^{At} \stackrel{?}{=} A \cdot \mathrm{e}^{At}$

    (e) Define $\cos(A), \sin(A)$. Comment on $\cos(A+B) =?$

55. Let $B \in M_n(\mathbb{R})$. Prove: the columns of B are orthonormal if and only if its rows are, i. e., $B^TB = I \Leftrightarrow BB^T = I$.

56. If $C = (c_1, \ldots, c_n)$ is an orthonormal basis for $\mathbb{R}^n$, then $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal transformation if and only if $[\varphi]_C$ is an orthogonal matrix.

57. **(Similar Matrices)** Consider the following three matrices.

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

    Compute the characteristic polynomial and eigenvalues of each matrix, together with the algebraic and geometric multiplicity of each eigenvalue. Which among the matrices A, B, C are similar?

58. **(Diagonalizable matrices)** Show that a matrix $A \in M_n(\mathbb{F})$ is diagonalizable iff

    (a) The characteristic polynomial f_A splits over $\mathbb{F}$, and
    (b) $\mathbb{F}^n = \sum_\lambda U_\lambda$.

    Here U_λ denotes the eigenspace corresponding to the eigenvalue λ, i. e., $U_\lambda = \ker(\lambda I - A)$.

59. **(Invariant subspaces)** Let V be a vector space. If $\phi : V \to V$ is a linear map then a subspace U is *invariant* under ϕ if $\phi(U) \subseteq U$. Show that if every subspace of V is invariant under ϕ then $\phi = \lambda \cdot \mathbf{I}$ is a scalar multiple of the identity map.

60. **(Primitive roots of unity)** Let $\omega = \cos(\frac{2\pi}{6}) + i\sin(\frac{2\pi}{6})$ be a primitive sixth root of unity. Given $f \in \mathbb{Q}[x]$ show that $f(\omega) = 0$ iff the polynomial $x^2 - x + 1$ divides f.

61. **(Minimal polynomials)** Let α be an algebraic number. Let $m_\alpha \in \mathbb{Q}[x]$ be a monic polynomial such that

    (a) $m_\alpha(\alpha) = 0$
    (b) If $f \in \mathbb{Q}[x]$ satisfies $f(\alpha) = 0$ then $\deg(m_\alpha) \leq \deg(f)$.

    Show that

    (i) The polynomial m_α is irreducible over $\mathbb{Q}$.
    (ii) If $f \in \mathbb{Q}[x]$ satisfies $f(\alpha) = 0$ then $m_\alpha | f$.
    (iii) The polynomial m_α is unique.

62. **(Minimal polynomials for matrices)** Let $A \in M_n(\mathbb{F})$. A monic polynomial $m_A \in \mathbb{F}[x]$ is called a *minimal polynomial of* A if

    (a) $m_A(A) = 0$
    (b) If $f \in \mathbb{F}[x]$ satisfies $f(A) = 0$ then $\deg(m_A) \leq \deg(f)$.

    Show that

    (i) For $f \in \mathbb{F}[x]$, $f(A) = 0$ iff $m_A \mid f$. In particular, $m_A \mid f_A$.
    (ii) The polynomial m_A is unique.
    (iii) If $A = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ then $m_A(x) = \prod'(x - \lambda_i)$ where the product is taken over distinct eigenvalues λ_i (so m_A has no multiple roots).
    (iv) The roots of m_A are exactly the eigenvalues of A.
    (v) The matrix A is diagonalizable iff m_A splits over $\mathbb{F}$ and m_A has no multiple roots.

63. **(Orthogonal polynomials)** Given an interval $I \subseteq \mathbb{R}$ a density function is a positive real-valued function $\rho : I \to (0, \infty)$ satisfying

$$\int_I x^{2n} \rho(x) dx < \infty$$

for each n. Given a density function ρ define an inner product on $\mathbb{R}[x]$ by the rule

$$\langle f, g \rangle = \int_I f(x) g(x) \rho(x) dx.$$

Show that with respect to this inner product there exists an orthogonal basis $\{f_n\}$ of $\mathbb{R}[x]$ such that $\deg(f_n) = n$; and f_n is unique up to scalar multiples.

64. **(Examples to research)**
    (a) **Chebyshev polynomials:** Take $I = (-1, 1)$ in the above. Then, the normalized basis of $\mathbb{R}[x]$ corresponding to $\rho(x) = 1/\sqrt{1 - x^2}$ and $\rho(x) = \sqrt{1 - x^2}$ are the Chebyshev polynomials of first and second kind, respectively.
    (b) **Hermite polynomials:** Take $I = \mathbb{R}$ in the above. Then, the normalized basis of $\mathbb{R}[x]$ corresponding to $\rho(x) = \mathrm{e}^{-x^2/2}$ are the Hermite polynomials.

65. **(Trigonometric functions)** Show that the trigonometric functions $\{1, \cos(nx), \sin(nx)\}_{n=1}^{\infty}$ are pairwise orthogonal with respect to the inner product

$$\langle f, g\rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} fg dx.$$

This will in particular prove that they are linearly independent.

66. **(Cauchy-Schwarz)** Let $(V, \langle, \rangle)$ be a Euclidean space. Then, for each $v, w \in V$,

$$|\langle v, w\rangle| \leq \|v\| \, \|w\| \, .$$

67. **(Gram-Schmidt orthogonalization)** Given vectors $v_1, v_2, \ldots \in V$ let $b_1, b_2, \ldots \in V$ denote the corresponding vectors obtained via the Gram-Schmidt process. This means that for all n,

(i) $v_n - b_n \in \mathrm{Span}(v_1, \ldots, v_{n-1})$, and

(ii) $\langle b_i, b_n\rangle = 0$ for all $i < n$.

Show that

(a) $\mathrm{Span}(v_1, \ldots, v_n) = \mathrm{Span}(b_1, \ldots, b_n)$ for each n.
(b) The vector $b_n = 0$ iff $\mathrm{Span}(v_1, \ldots, v_{n-1}) = \mathrm{Span}(v_1, \ldots, v_n)$.

68. **(Symmetric/Orthogonal operators)** Let $\varphi, \psi : V \to V$ be linear transformations of a Euclidean space V. Recall that φ is a *symmetric* transformation if $(\forall x, y \in V)(\langle x, \varphi(y)\rangle = \langle \varphi(x), y\rangle)$; and ψ is an *orthogonal* transformation if $(\forall x, y \in V)(\langle \psi(x), \psi(y)\rangle = \langle x, y\rangle)$. Let $\mathbf{B}$ be an orthonormal basis (ONB) of V. Then,

(a) φ is symmetric iff the matrix $[\varphi]_{\mathbf{B}}$ is a symmetric matrix.
(b) ψ is orthogonal iff $[\varphi]_{\mathbf{B}}$ is an orthogonal matrix.

69. **(A calculus lemma)** Consider the real function

$$f(t) = \frac{at^2 + bt + c}{dt^2 + e}$$

where $a, b, c, d, e \in \mathbb{R}$ and $e \neq 0$. Show that if $f(t)$ attains its macximum value at $t = 0$ (i. e., $f(0) \geq f(t)$ for all t) then $b = 0$.

70. **(Orthogonal complement)** Let $U \leq V$ be a subspace of a Euclidean space V. Then,

(a) $\dim(U) + \dim(U^{\perp}) = \dim(V)$
(b) $U + U^{\perp} = V$.

Recall that (a) was proven previously in class in a different context (standard dot product over any field F). Part (b) is false in that context.

71. **(Rayleigh quotient)** Let φ be a symmetric transformation of the Euclidean space V. Define the *Rayleigh quotient*

$$R_\varphi(x) = \frac{\langle x, \varphi(x)\rangle}{\langle x, x\rangle}$$

for $x \in V$, $x \neq 0$. It follows from the Spectral Theorem that all the n eigenvalues of φ are real. Denote them by $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$. Show that

(a) $\lambda_1 = \max R_\varphi(x)$

(b) $\lambda_n = \min R_\varphi(x)$

(c) **(Courant-Fischer)** $\lambda_i = \max\limits_{\substack{U \leq V \\ \dim(U)=i}} \min\limits_{\substack{x \in U \\ x \neq 0}} R_\varphi(x)$.

72. **(Interlacing theorem)** Let $A = A^t$ be a symmetric $n \times n$ real matrix with eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$. Let B denote the symmetric $(n-1) \times (n-1)$ matrix obtained by deleting the i^{th} row and the i^{th} column from A. Let $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_{n-1}$ denote the eigenvalues of B. Prove that

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \ldots \geq \lambda_{n-1} \geq \mu_{n-1} \geq \lambda_n.$$

73. **(Adjacency matrix)** Let $G = (V, E)$ be an undirected graph. The adjacency matrix of G is the symmetric matrix $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} 1 & i \sim j \\ 0 & i \nsim j. \end{cases}$$

If the eigenvalues of A are $\lambda_1 \geq \ldots \geq \lambda_n$ prove that

(a) $(\forall i)(|\lambda_i| \leq \max_{v \in V} \deg(v))$

(b) $\lambda_1 \geq \frac{1}{n} \sum_{v \in V} \deg(v) =$ average degree

(c) If G is connected then $\lambda_n = -\lambda_1$ iff G is bipartite.

74. **(Orthogonal polynomials)** Suppose that $f_1, f_2, f_3, \ldots$ form a sequence of orthogonal polynomials with respect to a density function ρ such that $(\forall n)(\deg(f_n) = n)$. Then,

(a) The roots of f_n are real for each n.

(b) **(Interlacing)** The roots of f_{n-1} interlace the roots of f_n.

75. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ such that $a_n a_0 \neq 0$. Let $r = \frac{p}{q} \in \mathbb{Q}$, with $\gcd(p, q) = 1$ such that $f(r) = 0$. Prove that $p \mid a_0$ and $q \mid a_n$.

76. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $g(x) = a_n + a_{n-1} x + \ldots + a_0 x^n$, with $a_i \in F$, $a_0 a_n \neq 0$.

(a) If $\alpha \in F$ is a root of f, find a root of g.

(b) If $\alpha_1, \ldots, \alpha_n$ are all the roots of f (counting multiplicities), find all the roots of g.

77. Let $A \in M_n(\mathbb{R})$ be an orthogonal matrix. Let $\lambda \in \mathbb{C}$ be a (complex!) eigenvalue of A. Show that $|\lambda| = 1$.

78. **(Fisher inequality)** Let

$$H = \begin{bmatrix} a_1 & b & b & \cdots & b \\ b & a_2 & b & \cdots & b \\ b & b & a_3 & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a_n \end{bmatrix}.$$

   (a) Compute $\det(H)$. Your answer should be a product of very simple expressions. Compare your result with the case when $a_1 = \cdots = a_n$ (done in class).

   (b) Prove that if $a_1, \ldots, a_n > b \geq 0$, then H is positive definite.

79. **(Finding quadratic forms)** Find $n \times n$ symmetric real matrices A, B such that

   (a) A is positive definite but some of its entries are negative, and

   (b) B is indefinite but all its entries are positive.

80. **(Secret sharing II)** We discussed in class how to share a secret number $x \in \{0, \ldots, p-1\}$ among n committee members such that any k members together can compute the secret but no $k-1$ of them will have any clue (Puzzle Problem 70). We solved this in class for the case when $p > n$. Now suppose the president wants only to share the outcome of a coin flip. How is this possible?

81. **(Hermitian inner product)** Let V be a complex vector space with Hermitian inner product $\langle , \rangle$. Show that $\langle 0, v \rangle = \langle v, 0 \rangle = 0$ for all v in V using the axioms of sesquilinearity.

In the next several exercises, V is a finite-dimensional complex vector space with Hermitian inner product $\langle , \rangle$.

82. **(Gram-Schmidt)** Show that V has an orthonormal basis, and, that any orthonormal set $\{v_1, \ldots, v_k\}$ can be extended to an orthonormal basis.

83. **(Unitary transformation)** We say that the linear transformation $\varphi : V \to V$ is *unitary* if $(\forall x, y \in V)(\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle)$. Prove that all eigenvalues of a unitary transformation have unit absolute value.

84. **(Self-adjoint transformation)** We say that the linear transformation $\varphi : V \to V$ is *self-adjoint* if $(\forall x, y \in V)(\langle x, \varphi(y) \rangle = \langle \varphi(x), y \rangle)$. Prove that all eigenvalues of a self-adjoint transformation are real.

85. **(Spectral theorem)** Let $\varphi : V \to V$ be a self-adjoint transformation. Prove that there exists an orthonormal eigenbasis of V corresponding to real eigenvalues.

86. **(Adjoint)** Show that for all $\varphi : V \to V$ there exists unique $\psi : V \to V$ such that

$$\langle x, \varphi(y) \rangle = \langle \psi(x), y \rangle$$

for each x, y in V. The *adjoint* ψ is denoted φ^*. Prove that for all $\varphi_1, \varphi_2 : V \to V$ and for all $\lambda \in \mathbb{C}$,

(a) $(\varphi_1\varphi_2)^* = \varphi_2^*\varphi_1^*$

(b) $(\varphi_1 + \varphi_2)^* = \varphi_1^* + \varphi_2^*$

(c) $(\lambda\varphi)^* = \bar{\lambda}\varphi^*$

(d) φ is self-adjoint iff $\varphi = \varphi^*$.

(e) φ is unitary iff $\varphi^* = \varphi^{-1}$.

87. **(Matrix adjoint)** For a complex matrix A, the matrix A^* is the conjugate-transpose of A. Let $\varphi : V \to V$ be a linear map. Then, with respect to an orthonormal basis $\mathbf{B}$, show that

$$[\varphi^*]_{\mathbf{B}} = [\varphi]_{\mathbf{B}}^*.$$

88. **(Upper-triangularity via unitary transformation)** Let $A \in M_n(\mathbb{C})$. Then, there exists a unitary matrix C such that $C^{-1}AC$ is upper-triangular. Equivalently, given $\varphi : V \to V$ there exists an orthonormal basis $\mathbf{B}$ such that $[\varphi]_{\mathbf{B}}$ is upper-triangular.

89. **(Orthogonal complement)** If $U \leq V$ is a subspace,

(a) Define $U^\perp$.

(b) Prove that $\dim(U) + \dim(U^\perp) = \dim(V)$.

(c) Prove that $U + U^\perp = V$.

90. **(Normal, upper-triangular matrices)** A matrix $A \in M_n(\mathbb{C})$ is *normal* if $AA^* = A^*A$. Prove that A is normal and upper-triangular iff A is diagonal.

91. **(Normality under unitary similarity)** Prove that if A is normal and $A \sim_{\mathbf{U}} B$ then B is normal, where $A \sim_{\mathbf{U}} B$ denotes that A is similar to B via a unitary transformation, i. e., that $B = C^{-1}AC$ for some unitary matrix C.

92. **(Normal vs. self-adjoint/unitary)** A linear map $\varphi : V \to V$ is normal if $\varphi\varphi^* = \varphi^*\varphi$. Prove that if φ is normal then,

(a) $\varphi = \varphi^*$ iff the eigenvalues of φ are real.

(b) $\varphi^* = \varphi^{-1}$ iff the eigenvalues of φ have norm one.

(This ends the sequence of exercises about Hermitian spaces.)

93. **(Lovász-reduced basis)** Let $(a_1, \ldots, a_n)$ be a basis of $\mathbb{R}^n$. Let $(b_1, \ldots, b_n)$ denote the orthogonalized basis obtained via the Gram-Schmidt process. Then,

$$\begin{aligned}
b_1 &= a_1 \\
b_2 &= a_2 + \mu_{2,1} b_1 \\
b_3 &= a_3 + \mu_{3,2} b_2 + \mu_{3,1} b_1 \\
&\vdots \\
b_n &= a_n + \textstyle\sum_{i=1}^{n-1} \mu_{n,i} b_i
\end{aligned}$$

for $\mu_{i,j} \in \mathbb{R}$. The basis $(a_1, \ldots, a_n)$ is *Lovász reduced* if

(a) $|\mu_{i,j}| \leq \frac{1}{2}$ for all i, j.

(b) $\|b_{i+1}\| \geq \frac{1}{\sqrt{2}} \cdot \|b_i\|$ for each $1 \leq i \leq n-1$.

Prove that if (a) is violated then elementary row operations $a_i \mapsto a_i + k a_j$ for $k \in \mathbb{Z}$ and $j < i$ can be used to eliminate this violation. Note that these operations do not alter the corresponding orthogonal basis $(b_1, \ldots, b_n)$; nor do they change the lattice $L := \sum_{i=1}^n \mathbb{Z} a_i$.

94. **(Lovász's lattice reduction algorithm)** The purpose of this algorithm is to convert a basis $(a_1, \ldots, a_n)$ of $\mathbb{R}^n$ into a Lovász-reduced basis $(a'_1, \ldots, a'_n)$ without changing the lattice L generated by the basis: $L = \sum_{i=1}^n \mathbb{Z} a_i = \sum_{i=1}^n \mathbb{Z} a'_i$.

The algorithm proceeds in phases:

while $(a_1, \ldots, a_n)$ not Lovász-reduced

(A) **if** (a) is violated, fix it as described in the preceding exercise

(B) **else** find i such that (b) is violated by b_{i-1} and b_i; swap a_{i-1} and a_i

return $(a_1, \ldots, a_n)$

Prove:

(i) The algorithm terminates in a finite number of phases.

(ii) If all coordinates of the input basis are integers, the algorithm terminates in a polynomial number of phases (polynomial in the bit-length of the input).

Hint: Find a **potential** function $P : \{\text{ bases of } \mathbb{R}^n\} \to \mathbb{R}$ (assign a real number to each basis of $\mathbb{R}^n$; remember that a basis is an ordered list, rathar than a set, of vectors, so the value of P may change when we permute the basis) such that

(1) P is always positive

(2) line (A) of the algorithm does not affect P

(3) each execution of line (B) of the algorithm reduces the value of P at least by a constant factor $c < 1$

(4) if all basis vectors are integral then $P \geq 1$

(5) in any case, P satisfies a positive lower bound that only depends on the lattice L and not on the particular $\mathbb{Z}$-basis of L.

95. **(Deciding positive definiteness)** Let $A \in M_n(\mathbb{R})$ be a symmetric real matrix.

    (a) Show that if A is positive definite, then every symmetric minor of A has positive determinant. (A $k \times k$ symmetric minor is the submatrix located at the intersection of k rows and the corresponding k columns; so a symmetric minor of a symmetric matrix is symmetric.)

    This condition is necessary and sufficient for positive definiteness; but in fact much less already suffices, as the next question shows.

    (b) Show that if every corner minor of A has positive determinant then A is positive definite. (A *corner minor* is a minor corresponding to rows $1, \ldots, k$ and columns $1, \ldots, k$.)

96. **(Inequality between the arithmetic and quadratic means)** Given $a_i \geq 0$, show that

$$\frac{a_1 + \cdots + a_n}{n} \leq \sqrt{\frac{a_1^2 + \cdots + a_n^2}{n}}.$$

97. Let the n vertices of the graph G have degrees $d_1, \ldots, d_n$. Let λ be the largest eigenvalue of the adjacency matrix of G. We have shown that λ is not less than the arithmetic mean of the d_i. Show that in fact λ is not less than the *quadratic* mean of the d_i:

$$\lambda \geq \sqrt{\frac{d_1^2 + \cdots + d_n^2}{n}}.$$

98. Calculate the largest eigenvalue of the adjacency matrix of the "star graph" $K_{1,n-1}$ (a tree with one vertex adjacent to all other vertices). Compare your result with the bound from the preceding exercise.