Discrete Math 37110 - Class 17 (2016-11-22)

Instructor: László Babai
Notes taken by Jacob Burroughs
Revised by instructor

17.1 Determinant, trace

DO 17.1. $\det(AB) = \det(A)\det(B)$

Define $\text{trace}(A) = \sum a_{ii}$ = the sum of diagonal elements

DO 17.2. $\text{trace}(A + B) = \text{trace}(A) + \text{trace}(B)$

DO 17.3. If $A \in \mathbb{R}^{k\times\ell}$ and $B \in \mathbb{R}^{\ell\times k}$ then $\text{trace}(AB) = \text{trace}(BA)$

17.2 Complex numbers

We use the symbol i with the rule $i^2 = -1$. We write the vector $(a, b) \in \mathbb{R}^2$ as $z = a+bi$ and call it a "complex number." So $\mathbb{C} = \{z = a + bi \mid a, b \in \mathbb{R}\}$ is the set of complex numbers. We define addition and multiplication of complex numbers. Addition is componentwise, as we add vectors in $\mathbb{R}^2$; multiplication is defined using the rule $i^2 = -1$:

- (a) $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i$
- (b) $z_1 \cdot z_2 = (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i$

If $b = 0$ we say z is real. If $a = 0$ we say z is imaginary.

The **complex conjugate** of z is $\overline{z} = a - bi$.

a is the "real part": $a = (z + \overline{z})/2$ and b is the "imaginary part": $b = (z - \overline{z})/(2i)$

$z \cdot \overline{z} = a^2 + b^2 = |z|^2$

Theorem 17.4. *If $z \neq 0$, then* $\exists \frac{1}{z}$

Proof.

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2}$$

□

The form $a+bi$ is called the **canonical form** of a complex number. The **polar form** of a complex number is

$$z = r(\cos(\theta) = i\sin(\theta)$$

Here $r = |z|$ is the absolute value and the angle θ is the **argument**. The argument θ is unique modulo 2π.

We obtain the polar form as follows. We observe that $|z_0| = 1$ where $z_0 = z/|z|$. Therefore $z = |z| \cdot z_0 = |z|(\cos\theta + i\sin\theta)$.

DO 17.5. $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$ and then $\arg(z^n) = n \arg z$

DO 17.6. $\cos(\alpha + \beta) + i \sin(\alpha + \beta) = (\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta)$

DO 17.7 (Euler)**.** We note that $\cos \alpha + i \sin \alpha$ can be written as $\mathrm{e}^{i\alpha}$. (Hint: power series.)

DO 17.8. The solutions to $z^n = 1$ are the called the "complex n-th roots of unity." Prove: they are $\cos(\frac{2k\pi}{n}) + i \sin(\frac{2k\pi}{n})$ for $k = 0, 1, \ldots, n-1$.

Theorem 17.9 (Fundamental Theorem of Algebra)**.** *If* $f = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{C}[t]$ *where* $a_n \neq 0$ *then* $(\exists \alpha_1, \cdots, \alpha_n \in \mathbb{C})(f(t) = a_n \prod_{j=1}^{n}(t - \alpha_j))$

The **multiplicity** of a root is the power to which the corresponding term is raised in the factorization. The sum of the multiplicities is n.

DO 17.10. f has no multiple roots if and only if $\gcd(f, f') = 1$

17.3 Fields

Definition 17.11. A field $\mathbb{F}$ is a set with two operations $+, \times$ such that

1. $(\mathbb{F}, +)$ is an abelian group.
2. $(\mathbb{F}^\times, \times)$ is an abelian group, where $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.
3. $a(b + c) = ab + ac$

DO 17.12. In a field, $ab = 0$ if and only if $a = 0$ or $b = 0$

Some examples of fields are $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Q}$ (rational numbers), $\mathbb{F}_p$ (p prime): the residue classes modulo p. The set of integers, $\mathbb{Z}$ does not form a field.

DO 17.13. The set of residue classes modulo m forms a field if and only if m is a prime. (Hint: you will need to use the prime property.)

Henceforth $\mathbb{F}$ denotes any field, but most of the time you can think of $\mathbb{F}$ being $\mathbb{R}$ or $\mathbb{C}$.

17.4 Basis, rank, dimension. First miracle

In this section V is a vector space over a field $\mathbb{F}$, i.e., $\mathbb{F}$ is the set of scalars.

Definition 17.14. Let B be a list of elements of V. We say that B is a *basis* of V if B is linearly independent and B spans V.

DO 17.15. B is a basis if and only if each $v \in V$ is a unique linear combination of B. So if $B = (b_1, \ldots, b_n)$ then $(\forall v \in V)(\exists! \alpha_1, \ldots, \alpha_n \in \mathbb{F})(v = \sum_{i=1}^{n} \alpha_i b_i)$. — The coefficients α_i are called the **coordinates** of v wrt B. (wrt = "with respect to")

DO 17.16. B is a basis if and only if it is a maximal linearly independent set.

To prove this, use the following exercise.

DO 17.17. If $b_1, \cdots, b_k$ are linearly independent and $b_1, \cdots b_k, c$ are linearly dependent, then $c \in \text{span}(b_1, \cdots, b_k)$

DO 17.18. Every vector space has a basis. Hint: This is immediate from Exercise 17.16 if the size of linear independent sets in V is bounded. Otherwise it follows from Zorn's lemma (set theory).

Theorem 17.19 (1st miracle of linear algebra)**.** *If $v_1, \ldots, v_k$ are linearly independent, $w_1, \ldots, w_\ell$ are any vectors and $v_1, \ldots, v_k \in span(w_1, \ldots, w_\ell)$ then $k \leq \ell$*

DO 17.20. Study proof of the above

DO 17.21. $\dim \mathbb{F}^n = n$ (equivalent to 1st miracle if dim defined as max number of lin indep vectors)

The **rank** of a set S of vectors is the maximum number of linearly independent vectors from S

17.5 Rank of a matrix

The **column-rank** of A is the rank of the set of columns

The **column-space** of A is the span of the columns

DO 17.22. The column-rank is the dimension of the column-space. (This is also equivalent to the First Miracle.)

DO 17.23. A basis of $F[t]$ is $\{1, t, t^2, t^3, \ldots\}$

DO 17.24. Show that the column-rank of $A + B \leq$ column-rank of A + column-rank of B

DO 17.25. Elementary column operations do not change column-rank

DO 17.26. Elementary row operations do not change column-rank

DO 17.27. Starting from any matrix, through a sequence of elementary row and column operations we can obtain a matrix that has at most one non-zero entry in each row and in each column.

DO 17.28. Prove: if a matrix has at most one non-zero entry in each row and in each column then its column-rank is equal to the number of non-zero entries and the row-rank is also equal to the number of non-zero entries.

Theorem 17.29 (2nd miracle of linear algebra)**.** *The column-rank of A is equal to the row-rank of A*

DO 17.30. Prove this theorem. (Hint: combine the preceding four exercises.)

Proof. Use column and row-operations until there is at most one nonzero entry in each row and column. Let r be the number of nonzero entries remaining. Then both the row-rank and the column-rank are equal to r. Now use exercises 17.25 and 17.26. □

Definition 17.31. The rank of A is the column-rank/row-rank

DO 17.32. $\text{rk}(A) = \text{rk}(A^T)$

17.6 Systems of linear equations

A system of k linear equations in n unknowns can be written as a matrix equation $Ax = b$ where $A \in \mathbb{F}^{k \times n}$, $b \in \mathbb{F}^k$ and $x \in \mathbb{F}^n$.

DO 17.33. $Ax = b$ is solvable if and only if the rank of A = the rank of the $k \times (n+1)$ matrix $[A \mid b]$. (Hint: use the next exercise.)

DO 17.34. If the columns of $A \in \mathbb{F}^{k \times n}$ are $a_1, \ldots, a_n$ and $x = (x_1, \ldots, x_n)^n$ then $Ax = x_1a_1 + \cdots + x_na_n$. So the column space of A is $\{Ax \mid x \in \mathbb{R}^n\}$.

Homogeneous system of linear equations: where $b = 0$ — always has trivial solution $x = 0$.

Want to find $U = \{x \mid Ax = 0\} \subseteq \mathbb{F}^n$ (the set of solutions)

DO 17.35. Prove $U \leq \mathbb{F}^n$. The dimension of U is called the **nullity** of A.

DO 17.36. Rank-nullity theorem: $\dim(U) + \text{rk}(A) = n$

DO 17.37. There exists a non-trivial solution to $A \in M_n(\mathbb{F})$ if and only if $\text{rk}(A) < n$

Theorem 17.38. *The following statements are equivalent for $A \in M_n(\mathbb{F})$*

(a) $\text{rk}(A) = n$

(b) $Ax = 0$ *has no no-trivial solutions*

(c) $\exists A^{-1}$ *such that* $A^{-1}A = AA^{-1} = I$

(d) $\det(A) \neq 0$

If either of these conditions (and therefore all of them) hold then we call A "non-singular"

17.7 Eigenvalues, characteristic polynomial

Theorem 17.39. *$\lambda \in \mathbb{F}$ is an eigenvalue of $A \in M_n(\mathbb{F})$ if and only if* $\det(\lambda I - A) = 0$

DO 17.40. A polynomial of degree n with a lead coefficent of 1 is called **monic**.

Definition 17.41. The **characteristic polynomial** of $A \in M_n(\mathbb{F})$ is $f_A(t) = \det(tI - A)$

DO 17.42. (a) The characteristic polynomial of $A \in M_n(\mathbb{F})$ is a monic polynomial of degree n. (b) Let $f_A(t) = a_0 + a_1 t + \cdots + a_n t^n$. Then $a_n = 1$ (monic), $a_{n-1} = -\operatorname{trace}(A)$, and $a_0 = (-1)^n \det(A)$.

Theorem 17.43. *The eigenvalues of A are precisely the roots of its characteristic polynomial*

Corollary 17.44. *$A \in M_n(\mathbb{F})$ has at most n eigenvalues.*

HW 17.45. Find the eigenvalues in $\mathbb{C}$ of the rotation matrix:

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Also find the corresponding eigenvectors in $\mathbb{C}^2$

DO 17.46. Prove: the $x \mapsto R_\theta x$ transformation rotates $\mathbb{R}^2$ by θ.

Definition 17.47. An **eigenbasis** of A is a basis of $\mathbb{F}^n$ consisting of eigenvectors of A.

HW 17.48. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has no eigenbasis over $\mathbb{R}$ or $\mathbb{C}$

17.8 Standard dot product, orthogonality, Spectral Theorem

Definition 17.49. For $a, b \in \mathbb{R}^n$ we write $a \cdot b = a^T b = \sum_{i=1}^n a_i b_i$, the standard dot product. We call a, b **orthogonal** if $a \cdot b = 0$. The **norm** of the vector a is $||a|| = \sqrt{\sum_{i=1}^n a_i^2}$. A list of vectors, $v_1, \ldots, v_k \in \mathbb{R}^n$, is *orthogonal* if they are pairwise orthogonal. It is *orthonormal* if in addition $||v_i|| = 1$. So $v_1, \ldots, v_k$ are orthonormal exactly if $v_i v_j = \delta_{ij}$ (Kronecker delta). (δ_{ij} are the entries of the identity matrix.)

Theorem 17.50 (Spectral Theorem)**.** *If $A \in M_n(\mathbb{R})$ and $A = A^T$, then A has an orthonormal eigenbasis*

HW 17.51. Find the orthonormal eigenbasis of $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and find the corresponding eigenvalues.