# Discrete Math, Third Problem Set (June 25)

REU 2003

Instructor: Laszlo Babai
Scribe: David Balduzzi

## 1 Number Theory

**Exercise 1.1. (Erdős)**
If $A \subset \{1, \dots, 2n\}$ with $|A| = n + 1$, show two elements of $A$ are relatively prime.

**Exercise 1.2.** **(Erdős)**
In the above situation; show some element of $A$ divides another. *Hint.* Pigeon hole principle.

**Theorem 1.3. (Dirichlet's theorem on simultaneous Diophantine approximation)**
*For all* $(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$ *and* $\epsilon > 0$ *there exist* $p_1, \dots, p_n, q \in \mathbb{Z}$ *such that*

$$1 \leq q \leq \left(\frac{1}{\epsilon}\right)^n \text{ and } \left|\alpha_i - \frac{p_i}{q}\right| < \frac{\epsilon}{q} \text{ for all } i.$$

The proof is a striking application of the Pigeon Hole Principle.

**Exercise 1.4.** **(Erdős)**
Consider a collection of arithmetic progressions $A_1, \dots, A_k$ for $k \geq 2$, with $\mathbb{N} = A_1 \cup \ldots \cup A_k$ and $A_i \cap A_j = \emptyset$. Show it is not possible for all the increments to be distinct. (In fact the largest increment must occur at least twice).

## 2 Linear algebra

**Example 2.1.** (Dissimilar matrices with same characteristic polynomial)

$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the characteristic polynomials are $f_A(x) = f_B(x) = (x-1)^2$.

**Definition 2.2.** $\mathbf{x}$ is an **eigenvector** to the **geometric eigenvalue** $\lambda$ for matrix $A$ if $\mathbf{x} \neq 0$ and $A\mathbf{x} = \lambda\mathbf{x}$. An **algebraic** eigenvalue of $A$ is a root of the characteristic polynomial $f_A(x)$.

**Exercise 2.3.** $A\mathbf{x} = \mathbf{b}$ is an inhomogeneous system of equations. Show it has a solution iff $\mathbf{b} \in \text{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ iff rk $A$ =rk $(A \mid \mathbf{b})$.

**Exercise 2.4.** $A\mathbf{x} = \mathbf{0}$ is a homogeneous system of equations. Show it has a nontrivial solution iff columns are linearly dependent.

**Determinants - quick and dirty**[1].

Given an $n \times n$ matrix $A$, let $A_{ij}$ denote the matrix formed by deleting the $i^{th}$ row and $j^{th}$ column. The determinat-expansion by the $j$-th column is

$$\det\ A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \text{ – the choice of } j \text{ doesn't matter,}$$

$$\text{where } \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc.$$

We could also reverse the roles of $i$ and $j$ in the above equation. Switching two rows or two columns changes the sign of the determinant. Adding some linear combination of rows (or columns) to another row (or column respectively) does not affect the determinant.

Note that the above rules are rules of calculation, not **definition.** It is far from obvious that these rules actually result in a unique number regardless of the choices made along the way. (What is the definition?)

**Theorem 2.5.** $\det A = 0$ *iff the columns are linearly dependent.*

**Exercise 2.6.** $\lambda$ is an eigenvalue of $A$ iff $f_A(\lambda) = 0$. (In other words the two definitions of eigenvalue are equivalent).

**Exercise 2.7.** Let $U = \{\mathbf{x} : A\mathbf{x} = \mathbf{0}\}$. This is a subspace of $F^n$. Show dim $U = n-$rk $A$, where by rk $A$ we mean the row rank.

**Exercise 2.8.** Show that for any matrix the row rank equals the column rank.

**Definition 2.9.** The **algebraic multiplicity** of an eigenvalue is its multiplicity as a root of the characteristic polynomial. The **geometric multiplicity** of $\lambda$ is dim $U_\lambda = \{\mathbf{x} : A\mathbf{x} = \lambda\mathbf{x}\} = n - \text{rk}(\lambda I - A)$.

**Example 2.10.**

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has eigenvalue 1 with algebraic multiplicity 2 and geometric multiplicity 1.

[1]Scribe's adjectives are not necessarily shared by instructor.

**Example 2.11.**

$$R_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \text{ is a matrix with no eigenvalues over } \mathbb{R} \text{ (unless } \pi \mid a).$$

However if we extend our base field to $\mathbb{C}$ then $R_\alpha$ has eigenvectors

$$\begin{bmatrix} i \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} -i \\ 1 \end{bmatrix} \text{ and eigenvalues } e^{\pm i\alpha} = \cos\alpha \pm i \sin\alpha.$$

**Exercise 2.12.** Show that over $\mathbb{C}$ a matrix $A$ is diagonalizable (i. e., it has an eigenbasis) iff the geometric and algebraic multiplicities of all its eigenvalues coincide.

# 3 Euclidean spaces

Let $\mathbb{F}$ denote $\mathbb{C}$ or $\mathbb{R}$.

**Definition 3.1.** A bilinear map $f : V \times V \to \mathbb{F}$ is a **Hermitian form** if

- for fixed $\mathbf{u}$, $F(\mathbf{u}, \bullet) : V \to \mathbb{F}$ is linear
- $f(\mathbf{u}, \mathbf{v}) = \overline{f(\mathbf{v}, \mathbf{u})}$.

**Example 3.2.** Define $A^* = \overline{A}^t$. A matrix $A$ is **Hermitian** if $A^*{=}A$. Given such a matrix, then $f(\mathbf{u}, \mathbf{v}) = \mathbf{u}^* A \mathbf{v}$ is a Hermitian form.

**Exercise 3.3.** Show that any Hermitian form can be written as above for some Hermitian matrix $A$.

**Definition 3.4.** Let $Q_f(\mathbf{u}) = f(\mathbf{u}, \mathbf{u}) : V \to \mathbb{R}$. (Why is this always real?) This is a **quadratic form**.

- $Q_f$ is **positive semidefinite** if for all $\mathbf{u}$, $Q_f(\mathbf{u}) \geq 0$.
- $Q_f$ is **positive definite** if for all $\mathbf{u} \neq 0$, $Q_f(\mathbf{u}) > 0$.

**Definition 3.5.** A **Euclidean space** is a pair $(V, f)$ consisting of a vector space $V$ (over $\mathbb{C}$ or $\mathbb{R}$) and a positive definite Hermitian form $f$.

**Example 3.6.** $\mathbb{R}^2$ with the usual dot product $\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}| \cdot |\mathbf{b}| \cos\theta$, where $\theta$ is the angle between $\mathbf{a}$ and $\mathbf{b}$ is an example; this is the same as $\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + a_2 b_2$.

**Definition 3.7.** $\mathbf{u}$ is **perpendicular** to $\mathbf{v}$, denoted by $\mathbf{u} \perp \mathbf{v}$, if $f(\mathbf{u}, \mathbf{v}) = 0$. We define the **norm** of $\mathbf{u}$ by $\|\mathbf{u}\| = \sqrt{f(\mathbf{u}, \mathbf{u})}$.

**Definition 3.8.** An **orthonormal basis** is a basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ such that $f(\mathbf{e}_i, \mathbf{e}_\mathbf{j}) = \delta_{ij}$.

**Theorem 3.9.** *Every finite-dimensional Euclidean space has an orthonormal basis.*

Expressing a vector in coordinates involves solving an inhomogeneous system of equations. However if we wish to express $\mathbf{u}$ in orthonormal coordinates

$$\mathbf{u} = \alpha_1 \mathbf{e}_1 + \cdots + \alpha_n \mathbf{e}_n, \text{ we calculate } \alpha_i = f(\mathbf{e}_i, \mathbf{u}).$$

# 4 Isometries of Euclidean spaces

**Exercise 4.1.** An **isometry** is a linear isomorphism $\phi : (V, f) \to (W, g)$ such that $\|\mathbf{u}\| = \|\phi(\mathbf{u})\|$ for all $\mathbf{u} \in V$. Show $\phi$ is an isometry iff $f(\mathbf{u}_1, \mathbf{u}_2) = g(\phi(\mathbf{u}_1), \phi(\mathbf{u}_2))$ for all vectors $\mathbf{u}_1$ and $\mathbf{u}_2$ in $V$.

**Exercise 4.2.** Show $\phi$ is an isometry iff it maps an orthonormal basis to an orthonormal basis.

**Theorem 4.3.** $f(\mathbf{u}, \mathbf{v}) = [\mathbf{u}]_{\underline{e}}^*[\mathbf{v}]_{\underline{e}} = \overline{u}_1 v_1 + \cdots + \overline{u}_n v_n$ *where* $\underline{e}$ *is an orthonormal basis.*

**Exercise 4.4.** Show that $A : V \to V$ is an isometry iff the columns of $A$ form an orthonormal basis of $\mathbb{F}^n$, where $n$ is the dimension of $V$.

**Exercise 4.5.** Show $A$ is an isometry iff $A^*A = I$ iff $A^* = A^{-1}$ iff $AA^* = I$. Such a matrix is called **unitary**.

**Example 4.6.** Unitary matrices living in real vector spaces are known as **orthogonal matrices**. The rotations and reflections of last lecture are examples under the standard inner product on $\mathbb{R}^2$.

When are diagonal matrices unitary?

If and only if $AA^* = I$ iff $|\lambda_i| = 1$ for all $i$ iff all eigenvalues have unit length.

**Definition 4.7.** $A$ and $B$ are **similar under unitary transforms**, denoted $A \sim_u B$, if there exists a unitary matrix $S$ such that

$$B = S^{-1}AS = S^*AS.$$

**Theorem 4.8. (Spectral Theorem)**
$A = A^*$ *if and only if* $A$ *is similar under unitary transforms to*

$$\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} \text{ with the } \lambda_i \text{ real numbers.}$$