Math 55a: Honors Abstract Algebra

Homework Assignment #10 (14 November 2016):
Linear Algebra X (determinants and distances);
representations of finite abelian groups (Discrete Fourier transform)

The fast Fourier transform . . . is the most important numerical algorithm of our lifetime.

Determinants and inner products (and another application of Gram-Schmidt):

1. i) Let $F = \mathbb{R}$ or $\mathbb{C}$, and $v_1, v_2, \ldots, v_n \in F^n$ the column vectors of an $n \times n$ matrix $A$.
Prove that
$$|\det A| \leq \prod_{i=1}^{n} ||v_i||$$
where $||\cdot||$ is the usual norm on $F^n$, with equality if and only if the $v_i$ are orthogonal
with respect to the corresponding inner product.

ii) Deduce that if $M$ is a positive-definite symmetric or Hermitian $n \times n$ matrix with
entries $a_{i,j}$ then
$$\det M \leq \prod_{i=1}^{n} a_{i,i},$$
with equality if and only if $M$ is diagonal.

(We know already that $\det M$ and the diagonal entries $a_{i,i}$ are positive real numbers.)

Some classical product formulas for determinants:

2. For elements $x_1, x_2, \ldots, x_n$ of any field $F$, let $V(x_1, x_2, \ldots, x_n)$ be the $n \times n$ matrix
whose $(i,j)$ entry is $x_j^{i-1}$. Find a homomorphism $T$ from the group $(F, +)$ to the
group of upper triangular $n \times n$ matrices over $F$, such that
$$V(x_1 + t, x_2 + t, \ldots, x_n + t) = V(x_1, x_2, \ldots, x_n) T(t)$$
for all $t$ and $x_i$. Use this to derive inductively the formula
$$\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (x_j - x_i)$$
for the Vandermonde determinant $\Delta(x_1, x_2, \ldots, x_n) = \det V(x_1, x_2, \ldots, x_n)$. What
is the determinant of the $n \times n$ matrix whose $(j,k)$ entry is $\sum_{i=1}^{n} x_i^{j+k-2}$?

3. i) Let $x_i, y_j$ ($1 \leq i, j \leq n$) be any elements of a field $F$ such that $x_i + y_j \neq 0$ for each
$i, j$. Let $A$ be the $n \times n$ matrix whose $(i,j)$ entry is $1/(x_i + y_j)$. Prove that
$$\det(A) = \Delta(x_1, \ldots, x_n) \Delta(y_1, \ldots, y_n) / \prod_{i=1}^{n-1} \prod_{j=1}^{n} (x_i + y_j)$$
where $\Delta$ is the Vandermonde determinant of the previous problem.
It follows via Cramer that each entry of $A^{-1}$ is a product of linear polynomials
in the $x_i$ and $y_j$; in particular this explains the form of the inverse of the Hilbert
matrix, which has $x_i = i$ and $y_j = j - 1.$

ii) In particular, if $F = \mathbb{R}$, $x_i = y_i > 0$ for each $i$, and the $x_i$ are distinct, deduce that
the symmetric matrix $A$ is positive definite (without invoking the interpretation of
the associated inner product on $\mathbb{R}^n$ given in part (iii)).
iii) Now let $V$ be the inner product space of continuous functions on $(0, 1)$ with $(f, g) = \int_0^1 f(t)g(t)\, dt$, and $W$ the subspace spanned by the functions $t^{x_i}$ for some distinct nonnegative $x_i \in \mathbb{R}$. Give a formula for the distance from $W$ to the element $t^x$ of $V$ for any real $x \geq 0$. [Hint: first find, for any linearly independent vectors $x_0, x_1, \ldots, x_n$ in a real inner product space, a formula for the distance between $x_0$ to the span of $x_1, \ldots, x_n$ as a quotient of determinants.]

This is the key to one of the proofs we’ll give next term of Mintz’s theorem on sequences $\{x_i\}$ such that the span of $\{t^{x_i}\}$ is dense in the space of continuous functions on $[0, 1]$.

The remaining problems concern Fourier analysis on finite abelian groups, which is a bridge between linear algebra and representation theory.

The Pontryagin dual $\hat{G}$ of a finite abelian group $G$ is the set of homomorphisms from $G$ to the multiplicative group $\mathbb{C}^\times$. 1 Pointwise multiplication gives $\hat{G}$ the structure of an abelian group (that is, the product of $\hat{g}_1, \hat{g}_2 \in \hat{G}$ is the homomorphism $g \mapsto \hat{g}_1(g)\hat{g}_2(g)$, and likewise for the identity and group inverse). While the definition doesn’t say this, any $\hat{g}$ must be a root of unity, because $g^n = 1$ for some integer $n > 0$, whence $(\hat{g}(g))^n = \hat{g}(g^n) = 1$. It follows that $|\hat{g}(g)| = 1$ for all $g \in G$ and $\hat{g} \in \hat{G}$. Elements of $\hat{G}$ are also called “characters” of $G$. We next explore Pontryagin duality for finite abelian groups and some applications.

4. i) Prove that if $G = \mathbb{Z}/n\mathbb{Z}$ for some positive integer $n$ then $\hat{G} \cong \mathbb{Z}/n\mathbb{Z}$.

ii) Prove that if $G_1, G_2, \ldots, G_r$ are any finite abelian groups then the Pontryagin dual of $G_1 \times G_2 \times \cdots \times G_r$ is $\hat{G}_1 \times \hat{G}_2 \times \cdots \times \hat{G}_r$.

Thus if $G$ is the product of groups $Z/n_j Z$ then $\hat{G} \cong G$. In particular $\#(\hat{G}) = \#(G)$. It turns out that every finite abelian group $G$ is of the form $\prod_{j=1}^r Z/n_j Z$, but we won’t need this to prove that $\#(\hat{G}) = \#(G)$ because we will obtain this fact in the course of proving the next few results.

5. i) Suppose $\hat{g} \in \hat{G}$ is not the identity character. Prove that $\sum_{g \in G} \hat{g}(g) = 0$.

ii) Let $C^G$ be the complex inner product space of functions $G \to \mathbb{C}$ with the usual inner product $\langle f_1, f_2 \rangle = \sum_{g \in G} f_1(g)\overline{f_2(g)}$. Prove that distinct characters of $G$, considered as elements of $C^G$, are orthogonal. Deduce that $\#(\hat{G}) \leq \#(G)$.

6. i) Let $\varphi : H \to G$ be any homomorphism of finite abelian groups. Obtain a dual homomorphism $\hat{\varphi} : \hat{G} \to \hat{H}$, and construct an isomorphism between $\ker(\hat{\varphi})$ and the Pontryagin dual of the quotient group $G/\varphi(H)$.

ii) Deduce that if $0 \to H \to G \to Q \to 0$ is a short exact sequence of finite abelian groups, and $\#(\hat{G}) = \#(G)$, then the dual homomorphisms $0 \to \hat{Q} \to \hat{G} \to \hat{H} \to 0$ also form a short exact sequence, and moreover $\#(\hat{H}) = \#(H)$ and $\#(\hat{Q}) = \#(Q)$.

iii) Show that for any finite abelian group $G$ there is a surjective homomorphism $\hat{G} \to G$ for some abelian group $\hat{G}$ of the form $\prod_{j=1}^r Z/n_j Z$. Deduce that $\#(\hat{G}) = \#(G)$, and thus that the dual of any short exact sequence of finite abelian groups is again exact. [Hint: It’s easy to construct a surjective homomorphism $\hat{G} \to G$ if you don’t mind $r$ being quite large.]

---

1 The “ya” in “Pontryagin” (transliterated a single Russian letter that looks like a backward R) is sometimes written “ia” or “ja”.

2 The standard proof is to let $N = \#(G)$ and consider the $N + 1$ group elements $1, g, g^2, \ldots, g^N$. By the pigeonhole principle, two of them must coincide, say $g^n = g^b$ with $a < b$, and then $g^{b-a} = 1$. In fact we may always take $n = N$, but this will not be needed here.

Fourier analysis leads to a more general notion of Pontryagin dual of an arbitrary “locally compact” abelian group, such as $\mathbb{Z}$ or $\mathbb{R}$, and in that setting one must explicitly impose the condition that $|\hat{g}(g)| = 1$. 

7. i) Let \( G \) be any finite abelian group. Construct a homomorphism from \( G \) to the Pontryagin dual of \( \hat{G} \), and prove that this homomorphism is an isomorphism.

ii) The discrete Fourier transform is a linear transformation \( C^G \rightarrow C^\hat{G}, f \mapsto \hat{f} \) defined by \( \hat{f}(\hat{g}) = \sum_{g \in G} \hat{g}(g) f(g) \); we call \( \hat{f} \) the “(discrete) Fourier transform of \( f \). By the previous two problems this transformation is invertible (and indeed \( f \mapsto (\#(G))^{-1/2} \hat{f} \) is an isometry). Construct an explicit inverse by showing that the Fourier transform of \( \hat{f} \) is \( g \mapsto \#(G) f(g-1) \) [using the identification of \( G \) with the dual of \( \hat{G} \) from part (i)].

With respect to the natural bases on \( C^G \) and \( C^\hat{G} \), the matrix of the discrete Fourier transform (DFT for short) has \( \hat{g}(g) \) in the \((g, \hat{g})\) entry. So for example if \( G = (\mathbb{Z}/2\mathbb{Z})^r \) we get a matrix each of whose entries is \( \pm 1 \) that achieves the bound \( N^{N/2} \) from problem 1 on the absolute value of the determinant of an \( N \times N \) matrix all of whose entries are \( \pm 1 \). This \( G \) is about as far as a finite abelian group can get from being cyclic; we next explore and exploit the DFT in the cyclic case.

8. i) Fix \( N > 0 \) and let \( \zeta = e^{2\pi i/N} \), an \( N \)-th root of unity. Let \( A \) be the \( N \times N \) matrix whose \((j,k)\) entry is \( \zeta^{jk} \). Use the result of the previous problem to evaluate \( A^2 \) and deduce that \( A^4 = N^2 \), and thus that \( C^N \) is the direct sum of its \( \lambda \)-eigenspaces for \( \lambda = \pm N^{1/2} \) and \( \lambda = \pm iN^{1/2} \) (why does this follow)? Use this to show that \( N^{-1/2} \sum_{j=1}^N \zeta^{j^2} \) has integer real and imaginary parts.

ii) Now suppose \( N \) is an odd prime. Prove that \( \left( \sum_{j=1}^N \zeta^{j^2} \right)^2 = \epsilon N \) where \( \epsilon = \pm 1 \) and is chosen so that \( \epsilon \equiv N \mod 4 \). Evaluate \( \det A \) and use it to determine the square root of \( \epsilon N \) that equals \( \sum_{j=1}^N \zeta^{j^2} \). [Hint: you can already deduce the value of \( |\det A| \) from (i), so need only determine where on the unit circle \( \det A/|\det A| \) lies.]

The value of \( \sum_{j=1}^N \zeta^{j^2} \) is known for all \( N \), but this more-or-less elementary approach does not generalize easily from the prime case.

This problem set is due Monday, 21 November, at the beginning of class.