Math 55a: Honors Abstract Algebra

Homework Assignment #10 (10 November 2017):
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.
> —Gilbert Strang, in "Wavelets", *American Scientist* **82** (3): 250–255 (May–June 1994), page 253 (quoted in Wikipedia's article on the fast Fourier transform)

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

1. i) Let $F = \mathbf{R}$ or $\mathbf{C}$, 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_i^{j-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

$$\det(A) = \Delta(x_1, \ldots, x_n)\Delta(y_1, \ldots, y_n) \Big/ \prod_{i=1}^{n} \prod_{j=1}^{n} (x_i + y_j)$$

where Δ 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 $F = \mathbf{R}$, $x_i = y_i > 0$ 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 $\mathbf{R}^n$ given in part (iii)).

iii) Now let V be the inner product space of continuous functions on $(0,1)$ with $\langle f,g\rangle = \int_0^1 f(t)g(t)\,dt$, and W the subspace spanned by the functions t^{x_i} for some distinct nonnegative $x_i \in \mathbf{R}$. 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 Müntz'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* $\widehat{G}$ of a finite abelian group G is the set of homomorphisms from G to the multiplicative group $\mathbf{C}^*$.[1] Pointwise multiplication gives $\widehat{G}$ the structure of an abelian group (that is, the product of $\widehat{g}_1, \widehat{g}_2 \in \widehat{G}$ is the homomorphism $g \mapsto \widehat{g}_1(g)\widehat{g}_2(g)$, and likewise for the identity and group inverse). While the definition doesn't say this, any $\widehat{g}$ must be a root of unity, because $g^n = 1$ for some integer $n > 0$,[2] whence $(\widehat{g}(g))^n = \widehat{g}(g^n) = 1$. It follows that $|\widehat{g}(g)| = 1$ for all $g \in G$ and $\widehat{g} \in \widehat{G}$. Elements of $\widehat{G}$ are also called "characters" of G. We next explore Pontryagin duality for finite abelian groups and some applications.

4. i) Prove that if $G = \mathbf{Z}/n\mathbf{Z}$ for some positive integer n then $\widehat{G} \cong \mathbf{Z}/n\mathbf{Z}$.
   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 $\widehat{G}_1 \times \widehat{G}_2 \times \cdots \times \widehat{G}_r$.

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

5. i) Suppose $\widehat{g} \in \widehat{G}$ is not the identity character. Prove that $\sum_{g\in G} \widehat{g}(g) = 0$.
   ii) Let $\mathbf{C}^G$ be the complex inner product space of functions $G \to \mathbf{C}$ 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 $\mathbf{C}^G$, are orthogonal. Deduce that $\#(\widehat{G}) \leq \#(G)$.

6. i) Let $\varphi : H \to G$ be any homomorphism of finite abelian groups. Obtain a dual homomorphism $\widehat{\varphi} : \widehat{G} \to \widehat{H}$, and construct an isomorphism between $\ker(\widehat{\varphi})$ 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 $\#(\widehat{G}) = \#(G)$, then the dual homomorphisms $0 \to \widehat{Q} \to \widehat{G} \to \widehat{H} \to 0$ also form a short exact sequence, and moreover $\#(\widehat{H}) = \#(H)$ and $\#(\widehat{Q}) = \#(Q)$.
   iii) Show that for any finite abelian group G there is a surjective homomorphism $\mathcal{G} \to G$ for some abelian group $\mathcal{G}$ of the form $\prod_{j=1}^r \mathbf{Z}/n_j\mathbf{Z}$. Deduce that $\#(\widehat{G}) = \#(G)$, 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 $\mathcal{G} \to G$ if you don't mind r being quite large.]

[1] The "ya" in "Pontryagin" (transliterating 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 $g^a = g^b$ 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 $\mathbf{Z}$ or $\mathbf{R}$, 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 $\widehat{G}$, and prove that this homomorphism is an isomorphism.

   ii) The *discrete Fourier transform* is a linear transformation $\mathbf{C}^G \to \mathbf{C}^{\widehat{G}}$, $f \mapsto \hat{f}$ 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 $\widehat{G}$ from part (i)].

With respect to the natural bases on $\mathbf{C}^G$ and $\mathbf{C}^{\widehat{G}}$, the matrix of the discrete Fourier transform (DFT for short) has $\widehat{g}(g)$ in the $(g, \widehat{g})$ entry. So for example if $G = (\mathbf{Z}/2\mathbf{Z})^r$ we get a matrix each of whose entries is ± 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 ± 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. The two (independent) parts of the next problem work for any finite abelian G, but the usual application takes $G = \mathbf{Z}/2^r\mathbf{Z}$ and yields efficient multiplication of large numbers or polynomials of high degree (once one has worked out how to deal computationally with the roots of unity).

8. i) Let G be any finite group. The *convolution* $f_1 * f_2$ of any functions $f_1, f_2 : G \to \mathbf{C}$ is the function on G whose value at any $g \in G$ is $\sum_{g_1 \in G} f_1(g_1) f_2(g_1^{-1} g)$. If G is abelian, express the DFT of $f_1 * f_2$ in terms of $\hat{f}_1$ and $\hat{f}_2$. [Check that your answer is consistent with the associativity of convolution: $f_1 * (f_2 * f_3) = (f_1 * f_2) * f_3$.]

   ii) If H is a subgroup of a finite group G, express the DFT on G in terms of the DFT's on H and G/H, and whatever auxiliary information about the short exact sequence $0 \to H \to G \to G/H \to 0$ you'll need to put them together.

9. 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 ζ^{jk}. Use the result of the previous problem to evaluate A^2 and deduce that $A^4 = N^2$, and thus that $\mathbf{C}^N$ is the direct sum of its λ-eigenspaces for $\lambda = \pm N^{1/2}$ and $\lambda = \pm i N^{1/2}$ (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 $\epsilon \equiv N \bmod 4$. Evaluate $\det A$ and use it to determine the square root of ϵN 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, 20 November, at the beginning of class.