## Math 55a: Honors Abstract Algebra

Homework Assignment #10 (10 November 2010):
Linear Algebra X:
Signatures and real polynomials; determinants and distances; Pontrjagin duality[0]

> Quotes? We don't need no stinkin' quotes!
> —adapted or misquoted from *Blazing Saddles* (1974), in turn adapted or misquoted from *The Treasure of the Sierra Madre*[1]

Using the signature of a pairing to describe the roots of a real polynomial without repeated factors:

1. i) (Chinese Remainder Theorem for polynomials) Let $F$ be a field, $P \in F[X]$ a nonzero polynomial, and assume $P = \prod_{j=1}^m P_j$ for some polynomials $P_j$ such that there is no polynomial $Q$ of positive degree that divides more than one of the $P_j$. Let $A$ be the $F$-algebra $F[X]/(P)$, and for each $j$ let $A_j$ be the $F$-algebra $F[X]/(P_j)$. [Recall that $(f)$ is the ideal in $A[X]$ generated by $f$.] Prove that the algebra homomorphism $A \to \prod_{j=1}^m A_j$ whose $j$-th coordinate is reduction mod $P_j$ is an isomorphism. Deduce (using a result from the previous problem set) that if the $P_j$ are irreducible then $F[X]/(P)$ is a product of fields. [Yes, the usual Chinese Remainder Theorem can be phrased in such terms as well, but linear algebra makes the polynomial version simpler.]

   ii) Now suppose $F = \mathbf{R}$ and the $P_j$ are irreducible. Show that $A_j$ is isomorphic with $\mathbf{R}$ or $\mathbf{C}$ according as $\deg(P_j) = 1$ or 2. Let $\langle \cdot, \cdot \rangle$ be the pairing on $A$ defined by $\langle f, g \rangle = \operatorname{tr}(fg)$, that is, the trace of the multiplication-by-$fg$ map on the finite-dimensional real vector space $A$. Prove that this pairing is nondegenerate, and that its signature is $(r, s)$ where $s$ is the number of $j$ for which $P_j$ is quadratic and $r - s$ is the number of $j$ for which $P_j$ is linear.

   iii) Suppose that moreover each $P_j$ is linear and none equals $X$, so that the roots are all real and nonzero (as happens if $P$ is the characteristic polynomial of an invertible Hermitian matrix, though if we have such a matrix we already know how to count the roots of each sign.) Construct a polynomial for which the signature formula of part (ii) yields the counts of positive and negative roots of $P$.

The formula $\langle f, g \rangle = \operatorname{tr}(fg)$ yields a pairing on $F[X]/(P)$ for any $F$ and $P$. It is nondegenerate if and only if $P$ has no repeated factors; this will be easier to see once we have developed some more field algebra, but for now you can easily check it if $P$ factors completely in $F[X]$ (i.e. has all roots in $F$).

Next 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 $\sum_{i=1}^n x_i^{j+k-2}$?

[0] The "j" in "Pontrjagin" is pronounced as a "y".

[1] According to Wikipedia's "Stinking badges" page. Yes, Wikipedia has a page on "Stinking badges"!

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 $\Delta$ 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 $F = \mathbf{R}$, $x_i = y_i > 0$ for each $i$, and the $x_i$ are distinct, deduce that the symmetric matrix $A$ is positive definite (without invoking the calculus interpretation of the associated inner product on $\mathbf{R}^n$).

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 $x \geq 0$.

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. The *Pontrjagin dual* $\widehat{G}$ of a finite abelian group $G$ is the set of homomorphisms from $G$ to the multiplicative group $\mathbf{C}^*$. 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 Pontrjagin 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 Pontrjagin 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 Pontrjagin 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

[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 Pontrjagin 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 $|\hat{g}(g)| = 1$.

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.]

7. i) Let $G$ be any finite abelian group. Construct a homomorphism from $G$ to the Pontrjagin 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 Hadamard bound $N^{N/2}$ on the absolute value of the determinant of a square ±1 matrix of order $N$. 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 $\zeta^{jk}$. 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 $\lambda$-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 $\epsilon N$ 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.

Six of these nine problems (your choice) are due Wednesday, 17 November, at the beginning of class, and the remaining three are due Wednesday, 24 November, at the beginning of class.