

**BABAI DISCRETE MATHEMATICS REU 2008**  
**EXERCISES FROM LECTURE 14, MONDAY AUGUST 4**

SCRIBE: MATTHEW STROM BORMAN

Recall that we are considering only finite abelian groups.

**Definition.** A **character**  $\chi$  of an abelian group  $G$  is a group homomorphism  $\chi : G \rightarrow \mathbb{T}$ , where  $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ .

**Definition.** The  $j$ -th character  $\chi_j$  of  $\mathbb{Z}/n\mathbb{Z}$  is given by  $\chi_j(m) = \omega_n^{mj}$  where  $\omega_n = e^{2\pi i/n}$ .

**Definition.** The **product character** for  $\chi_1 : H \rightarrow \mathbb{T}$  and  $\chi_2 : K \rightarrow \mathbb{T}$  is  $\chi_1\chi_2(h, k) = \chi_1(h)\chi_2(k)$ .

**Theorem.** The characters of  $G$  are an orthonormal basis for  $\mathbb{C}^G$ , the  $\mathbb{C}$ -vector space of functions  $G \rightarrow \mathbb{C}$  with the Hermitian inner product

$$(f, h) = \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} h(g).$$

So in particular there are  $|G|$  characters of  $G$ .

**Definition.** For a finite abelian group  $G$ , the **dual group**  $\widehat{G}$  is the set of characters of  $G$ , with the group operation on  $\widehat{G}$  given by  $(\chi\eta)(g) = \chi(g)\eta(g)$ .

**Exercise 1.** Prove that  $G \cong \widehat{\widehat{G}}$ . *Hint:* First prove for cyclic groups and then use structure theorem for finite abelian groups.

**Exercise 2.** Prove that a finite abelian group  $G$  is canonically isomorphic to  $\widehat{\widehat{G}}$  under the map  $g \mapsto f_g$  where  $f_g(\chi) = \chi(g)$ .

**Theorem.** If  $f \in \mathbb{C}^G$ , then  $f = \sum_{\chi \in \widehat{G}} c_\chi \chi$  where  $c_\chi = (\chi, f)$ .

**Definition.** The **Fourier transform** is a linear map  $F : \mathbb{C}^G \rightarrow \mathbb{C}^{\widehat{G}}$  such that  $F(f) = \hat{f}$  where

$$\hat{f}(\chi) = n(\chi, f) = \sum_g \overline{\chi(g)} f(g) = \sum_g \chi(-g) f(g).$$

In matrix form, using the basis  $\widehat{G}$  for  $\mathbb{C}^{\widehat{G}}$  and basis  $G = \widehat{\widehat{G}}$  for  $\mathbb{C}^G$ , the Fourier transform is  $C = (\chi(-g))$ , where the rows are indexed by characters and the columns by group elements. This matrix is called the **character table for  $G$** .

**Definition.** A **unitary transformation** is a linear transformation  $\phi : V \rightarrow V$  such that  $(x, y) = (\phi x, \phi y)$ , where  $V$  is a  $\mathbb{C}$ -vector space with inner product  $(\cdot, \cdot)$ . In matrix form, this is equivalent to  $T^*T = TT^* = I$ , where  $T^*$  is conjugate-transpose.

**Theorem.** If  $C$  is the character table for  $G$ , then  $|G|^{-1/2} C$  is a unitary matrix. This statement is equivalent to the statement that the characters are orthonormal in the  $\mathbb{C}^G$  inner product.

**Theorem (First Orthogonality Relation).** Let  $\chi_1$  and  $\chi_2$  be characters of a group  $G$ . Then

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g) = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2 \\ 1 & \text{if } \chi_1 = \chi_2 \end{cases}.$$

**Theorem (Second Orthogonality Relation).** For  $g_1, g_2 \in G$ ,

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi(g_1)} \chi(g_2) = \begin{cases} 0 & \text{if } g_1 \neq g_2 \\ 1 & \text{if } g_1 = g_2 \end{cases}.$$

**Definition.** The **Fourier inversion** is a linear map such that  $I : \mathbb{C}^{\widehat{G}} \rightarrow \mathbb{C}^G$  where

$$I(h)(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(-g) h(\chi).$$

**Theorem.** The Fourier transform and the Fourier inversion are inverses of each other, so  $I(F(f)) = f$  if  $f \in \mathbb{C}^G$  and  $F(I(h)) = h$  if  $h \in \mathbb{C}^{\widehat{G}}$ .

**Theorem (Plancherel's Formula).** For  $f_1, f_2 \in \mathbb{C}^G$ , we have that

$$(\widehat{f}_1, \widehat{f}_2) = |G| (f_1, f_2) \quad \text{and therefore} \quad \|\widehat{f}_1\| = \sqrt{|G|} \|f_1\|.$$

**Definition.** For  $A \subset G$  define the **characteristic function**  $f_A : G \rightarrow \mathbb{C}$  by

$$f_A(g) = \begin{cases} 0 & \text{if } g \notin A \\ 1 & \text{if } g \in A \end{cases}.$$

**Theorem.** For  $A \subset G$ , if  $\chi_0$  is the principal character, then  $\widehat{f}_A(\chi_0) = |A|$ .

**Exercise 3.** If  $\chi \neq \chi_0$ , then  $\widehat{f}_A(\chi) = \widehat{f_{G \setminus A}}(\chi)$ .

**Theorem.**  $|\widehat{f}_A(\chi)| \leq |A|$ . (Use the definition of Fourier transform and triangle inequality.)

**Definition.** If  $A \subset G$ , define  $\Phi(A) = \max_{\chi \neq \chi_0} |\widehat{f}_A(\chi)|$ .

**Exercise 4.** If  $A \subset G$  with  $|A| \leq |G|/2$ , then  $\sqrt{|A|/2} \leq \Phi(A)$ .

**Definition.** Let  $\mathbb{F}_q$  be a finite field, then the nonzero elements  $\mathbb{F}_q^*$  are a group and have a character  $\chi_q : \mathbb{F}_q^* \rightarrow \mathbb{T}$  such that

$$\chi_q(x) = \begin{cases} 1 & \text{if } x = y^2 \text{ for } y \in \mathbb{F}_q^* \\ 0 & \text{otherwise} \end{cases}.$$

This is called the **quadratic character**.

**Exercise 5.** Prove that this is indeed a character, i. e.,  $\chi(xy) = \chi(x)\chi(y)$ . (*Hint:* count.)

**Definition.** Let  $\psi : (\mathbb{F}_q, +) \rightarrow \mathbb{T}$  be an additive character and let  $\chi : \mathbb{F}_q^* \rightarrow \mathbb{T}$  be a multiplicative character. Extend  $\chi$  to  $\mathbb{F}_q$  by setting  $\chi(0) = 0$ . Define the **Gaussian sum** to be  $S(\chi, \psi) = \sum_{g \in \mathbb{F}_q} \chi(g)\psi(g)$ .

**Exercise 6.** In the above setting prove that if  $\psi \neq \psi_0$  and  $\chi \neq \chi_0$ , then  $|S(\chi, \psi)| = \sqrt{q}$ .

**Exercise 7.** Let  $G = (\mathbb{F}_q, +)$  where  $q$  is a power of an odd prime and let  $Q$  be the set of squares of  $\mathbb{F}_q$ , so  $Q = \{x^2 \mid x \in \mathbb{F}_q, x \neq 0\}$ . We know that  $|Q| = (q-1)/2$ . Prove that  $\Phi(Q) \leq \sqrt{q}$ .