Supplement 1

Characters on Finite Abelian Groups

By a <u>character</u> of a finite abelian group G we mean a homomorphism

$$\chi : G \longrightarrow \mathbb{C} \setminus \{0\}$$

i.e. $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in G$.

Notice that every value which such a χ assomes must be a root of unity.

The characters of G form a group $\hat{G}$ (called the dual group of G) with multiplication given by $\quad \chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$ for all $x \in G$

and identity element the trivial character χ_0 (which is identically 1 on G)

<u>Theorem 1</u>: $\quad |G| = |\hat{G}|$

<u>Theorem 2</u>: (Orthogonality relations)

$$\text{(a)} \quad \frac{1}{|G|} \sum_{x \in G} \chi(x) = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{o/w} \end{cases}$$

$$\text{(b)} \quad \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{o/w} \end{cases}$$

In order to establish Theorem 2 (b) we will also need to following

<u>Theorem 3</u>: If $x \neq 1$, then $\chi(x) \neq 1$ for some $\chi \in \hat{G}$.

The following is key to the proofs of Theorems 1 and 3.

Lemma 1 (Character extension lemma)

Let G be a finite abelian group and $H \leq G$ be a subgroup. Any character of H can be extended to a character of G in $[G:H]$ ways.

(Here $[G:H]$ denotes the index of H in G, which of course equals $|G|/|H|$.)

Proof We induct on the index $[G:H]$ and may assume that $H \neq G$.

Pick $x \in G \setminus H$ and let χ be a character of H. We will extend χ to a character $\tilde{\chi}$ of $\langle x, H \rangle$ and count the number of possible $\tilde{\chi}$. The we use induction to lift the character on $\langle x, H \rangle$ all the way up to G.

Let $k \geq 1$ be minimal such that $x^k \in H$, in other words k is the order of x in G/H and $k = [\langle x, H \rangle : H]$.

If $\tilde{\chi}$ is to be a character, then $\tilde{\chi}(x)$ must satisfy

$$\tilde{\chi}(x)^k = \chi(x^k). \qquad (*)$$

This gives us k possible choices for $\tilde{\chi}(x)$. We will show they all work.

Once we have chosen $\tilde{\chi}$ to satisfy $(*)$, we define $\tilde{\chi}$ on $\langle x, H \rangle$ by

$$\tilde{\chi}(x^i h) := \tilde{\chi}(x)^i \chi(h). \quad (**)$$

Exercise 1: Show that $\tilde{\chi}$ is a well-defined character on $\langle x, H \rangle$ which restricts to χ on H.

The number of choices of $\tilde{\chi}$ extending χ is equal to the number of choices for $\tilde{\chi}(x)$, namely $k = [\langle x, H\rangle : H]$.

Since $[G : \langle x, H\rangle] < [G : H]$, by induction on the index there are $[G : \langle x, H\rangle]$ extensions of each $\tilde{\chi}$ to a character of G, so the number of extensions of a character of H to a character of G is

$$[G : \langle x, H\rangle] \cdot [\langle x, H\rangle : H] = [G : H]. \qquad \square$$

<u>Proof of Theorem 1</u>: Apply Lemma 1 with $H = 1$. $\square$

<u>Proof of Theorem 3</u>: Let $H = \langle x\rangle$. Since H is a nontrivial cyclic group, it follow from Theorem 1 that there exists a non-trivial character $\chi \in \hat{H}$ such that $\chi(x) \neq 1$. Now use Lemma 1 to extend χ to G. $\square$

<u>Proof of Theorem 2</u>:

<u>(a)</u>: Let $S = \sum_{x \in G} \chi(x)$.

If $\chi = \chi_0$, then $S = |G|$. If $\chi \neq \chi_0$, then $\exists\, x_0 \in G$ s.t. $\chi(x_0) \neq 1$.

$$\Rightarrow \chi(x_0) S = \sum_{x \in G} \chi(x x_0) = \sum_{x \in G} \chi(x) = S$$

$$\Rightarrow S = 0.$$

<u>(b)</u>: If $x \neq 1$, then by Theorem 3 we know $\exists\, \chi \in \hat{G}$ such that $\chi(x) \neq 1$. The argument now follows as in part (a) above, but with $S = \sum_{\chi \in \hat{G}} \chi(x)$. $\square$

Dirichlet Characters

Consider the characters χ' on the multiplicative group of residue classes $a \bmod q$ with $(a,q)=1$, $(\mathbb{Z}/q\mathbb{Z})^{\times}$.

We extend these to functions χ on $\mathbb{Z}$ by setting

$$\chi(n) := \begin{cases} \chi'(n+q\mathbb{Z}) & \text{if } (n,q)=1 \\ 0 & \text{if } (n,q)>1. \end{cases}$$

These functions on $\mathbb{Z}$ are what we call <u>Dirichlet characters</u>, note that these functions are periodic mod q & completely multiplicative

The corresponding extension of the trivial character χ_0' mod q is called the principal character modulo q and denoted by χ_0.

Note that
$$\chi_0(n) = \begin{cases} 1 & \text{if } (n,q)=1 \\ 0 & \text{o/w}. \end{cases}$$

$\bar{\chi}(a) = \overline{\chi(a)} = \frac{1}{\chi(a)} = \chi^{-1}(a).$

<u>Corollary 1</u> (of Theorem 2 (b))

If $a, n \in \mathbb{Z}$ with $(a,q)=1$, then $\displaystyle \frac{1}{\varphi(q)} \sum_{\chi} \bar{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \bmod q \\ 0 & \text{o/w} \end{cases}$

where the sum is over all Dirichlet characters modulo q.

<u>Exercise (2)</u>: Deduce Corollary 1 from Theorem 2 (b).