§ Characters of finite abelian groups

(A Course in Arithmetic. Jean-Pierre Serre. Chapetr VI)

Theorem (Arithmetic Progressions)

Let $a, b \in \mathbb{Z}_{>1}$ such that $(a,b) = 1$. There are infinitely many primes in the sequence $a, a+b, a+2b, a+3b, \ldots$

G be a finite abelian group.

Def A character of G is a homomorphism into the multiplicative group $\mathbb{C}^*$. The set of characters is called the dual of G and denoted by $\hat{G}$.

$\chi \in \hat{G}$, $\chi : G \longrightarrow \mathbb{C}^*$

Example 1 Let G be cyclic of order n, say $G = \langle s \rangle$.

For every character $\chi : G \longrightarrow \mathbb{C}^*$ we have that $w = \chi(s)$ is a nth root of unity

$$w^n = (\chi(s))^n = \chi(s^n) = \chi(e) = 1.$$

Conversly, every nth root of crity w defines a character

$$s^a \overset{\varphi_a}{\longmapsto} w^a \qquad a \in \mathbb{Z}$$

Thus, we have tha the map $\chi \mapsto \chi(s)$ is an isomorphism of $\hat{G}$ on the groop μ_n. In particular $\hat{G}$ is a cyclic groop of order n.

Proposition 1 Let $H \leq G$ be a subgroup. Every character of H extends to a character of G.

pf Induction on $[G:H]$. If $[G:H] = 1$, then $G = H$ and we are done. For otherwise let $x \in G$ but not in H. Let $n > 1$ be the smallest integer for which $x^n \in H$. Let $\chi \in \hat{H}$ and define

$$t = \chi(x^n)$$

Notice that we can find $w \in \mathbb{C}^*$ for which $w^n = t$. If we consider the subgroup H' determined by H and x, the every element $h' \in H'$ can be written as $h' = h x^a$ for some $h \in H$ and $a \in \mathbb{Z}$.

Pet

$$\chi'(h') := \chi(h) w^a \quad (\text{a character of } H')$$

In fact χ' does not depend on the decomposition of h'. Moreover, it is extending χ.

Since $[G:H'] < [G:H]$ we can use the induction and thus we can extend χ' to a character of G $\square$

Remark The restriction

$$\rho : \hat{G} \longrightarrow \hat{H} \quad ; \quad \left(G \xrightarrow{\chi} \mathbb{C}^* \right) \longmapsto \left(H \xrightarrow{\chi|_H} \mathbb{C}^* \right)$$

defines a homomorphism. Moreover, the kernel of ρ is the set of characters of G which are trivial on H;

$$\ker(\rho) = \left\{ G \xrightarrow{\chi} \mathbb{C}^* : \begin{array}{ccc} H & \xrightarrow{\chi|_H} & \mathbb{C}^* \\ h & \longmapsto & 1 \end{array} \right\}$$

Thus we have a canonical isomorphism

$$\ker(\rho) \longrightarrow \widehat{G/H}$$

$$\left(G \xrightarrow{\chi} \mathbb{C}^* \right) \longmapsto \left(\begin{array}{ccc} G/H & \xrightarrow{\tilde{\chi}} & \mathbb{C}^* \\ gH & \longmapsto & \chi(g) \end{array} \right)$$

Hence we have the exact sequence

$$\{1\} \longrightarrow (\widehat{G/H}) \longrightarrow \hat{G} \longrightarrow \hat{H} \longrightarrow \{1\}$$

;

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & (\widehat{G/H}) & \longrightarrow & \hat{G} & \longrightarrow & \hat{H} & \longrightarrow & \{1\} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \{1\} & \longrightarrow & G/H & \longrightarrow & G & \longrightarrow & H & \longrightarrow & \{1\} \end{array}$$

Recall from (FSAA) that the order of $\hat{G}$ is the product of the orders of $(\widehat{G/H})$ and $\hat{H}$. We shall use this fact to prove the following result.

<u>Proposition</u> The group $\hat{G}$ is a finite abelian group of the same order as G.

<u>pf</u> Induction on the order n of G. The case $n=1$ is trivial. If $n>2$ we can choose a nontrivial cyclic subgroup $H<G$. Then by the previous remark $|\hat{G}| = |\hat{H}|\,|(\widehat{G/H})|$ but $|\hat{H}| = |H|$, and $|G/H| < n$. By induction we have

$$|\hat{G}| = |H| \cdot |G/H| = |G|$$

Q.E.D

There is a natural homomorphism $\chi \longmapsto \chi(x)$ of G and $\hat{\hat{G}}$.

Proposition The homomomorphism

$$\begin{array}{ccc} G & \xrightarrow{\varepsilon} & \hat{\hat{G}} \\ x & \longmapsto & \left(\hat{G} \xrightarrow{\phi_x} \mathbb{C}^*,\ \chi \longmapsto \chi(x)\right) \end{array}$$

is an isomorphism of G onto its bidual $\hat{\hat{G}}$.

pf Since G and $\hat{\hat{G}}$ have the same order, we just need to prove that ε is injective. That is, if $x \in G$ is $\neq 1$, there is a character χ of G such that $\chi(x) \neq 1$.

Let $H = \langle x \rangle$ (cyclic group) since we have that $\hat{H} \cong \mu_{|H|}$ we can find $\chi \in \hat{H}$ such that $\chi(x) \neq 1$. ~~the rest~~

we can extend χ to a character of G. Q.E.D.

We have the following orthogonality relations

Prop Let $n = |G|$ and let $\chi \in \hat{G}$. Then

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$$

pf The first equation is obvious. To prove the other equation let $y \in G$ s.t $\chi(y) \neq 1$. We then have

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(yx) = \sum_{x \in G} \chi(x)$$

$$\Rightarrow (\chi(y) - 1) \sum_{x \in G} \chi(x) = 0$$

Therefore, since $\chi(y) \neq 1$, we conclude the desired result ∎

Corollary Let $x \in G$. Then

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & \text{if } x = 1 \\ 0 & \text{if } x \neq 1 \end{cases}$$

Now that we have a better understanding about the characters of finite abelian groups, we can discuss about modular characters.

Denote by $G(m)$ the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$, $m \in \mathbb{Z}_{\geq 1}$.
$G(m)$ is an abelian group of finite order $\phi(m)$, the Euler ϕ-function. A character of $G(m)$ is called a character modulo m; we can think of $\chi \in \widehat{G(m)}$ as a function, defined on the set of integers prime to m, with values in $\mathbb{C}^*$, and such that $\chi(ab) = \chi(a)\chi(b)$. We can extend this characters to a function of $\mathbb{Z}$ by setting $\chi(c) = 0$ if $(c, m) \neq 1$.

Ex: $m = 4$; $G(4) = \{1, 3\}$

$\Rightarrow \widehat{G}(4) = \{\tilde{1}, \chi\}$

$\tilde{1}(1) + \chi(3) = 0 \Rightarrow \chi(3) = -1$

$\Rightarrow \chi(x) = (-1)^{\varepsilon(x)}$ is the only nontrivial character.

where

$$\varepsilon(n) \equiv \frac{n-1}{2} \pmod 2.$$

Example $m = p > 2$ prime number. The group $G(p)$ is cyclic of order $p-1$, hence has a unique character of order 2, the Legendre character $x \longmapsto \left(\frac{x}{p}\right)$

The following result shows that the characters of order 2 are closely related to the Legendre characters.

Proposition Let a be a non-zero square-free integer and let $m = 4|a|$. Then there exists a unique character χ_a modulo m such that $\chi_a(p) = \left(\frac{a}{p}\right)$ for all prime numbers p not dividing m.

pf The uniqueness follows by that fact that all prime numbers to m are products of prime numbers not dividing m. Thus, if there would be another character χ modulo m such that $\chi(p) = \left(\frac{q}{p}\right)$ for every prime number $p \nmid m$, the previous observation and the multiplicity of characters i.e. $\chi(a \cdot b) = \chi(a)\chi(b)$ would imply that χ and χ_a agree in all the integers. These observations also implies that $\chi_a^2 = 1$.

To prove the existance, we first assume that $a = l_1 \dots l_k$ where the l_i's are distinct prime numbers, different from 2.

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{l_1}\right) \cdots \left(\frac{x}{l_k}\right)$$

Recall the quadratic reciprocity lame due to Gauss

Theorem Let p and ℓ be two distinct odd prime numbers. We have

$$\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\varepsilon(p)\,\varepsilon(\ell)}$$

Applying this result we get

$$\chi_a(p) = (-1)^{\frac{p-1}{2}\varepsilon(a)} \left(\frac{p}{\ell_1}\right)\cdots\left(\frac{p}{\ell_K}\right)$$

$$= (-1)^{\frac{p-1}{2}K} \left(\frac{\ell_1}{p}\right)\cdots\left(\frac{\ell_1}{p}\right), \text{ for some constant } K$$

$$= \left(\frac{\ell_1}{p}\right)\cdots\left(\frac{\ell_1}{p}\right) = \left(\frac{a}{p}\right)$$

and χ_a has the required property.

When a is of the form $-b$ (or $2b$ or $-2b$) where $b = \ell_1 \cdots \ell_K$ as above, we take we take

$$\chi_a(x) = \chi_b(x)(-1)^{\varepsilon(x)} \quad \left(\text{or } \chi_b(x)(-1)^{\omega(x)} \text{ or } \chi_b(x)(-1)^{\varepsilon(x)+\omega(x)}\right)$$

where

$$w(x) \equiv \frac{n^2-1}{8} \pmod 2$$

and proceed as before Q.E.D