# 9. Characters

Def] Let $G$ be a finite abelian group. A character of $G$ is a homomorphism $\chi : G \to \mathbb{C}^*$. The set of characters of $G$ forms a group under

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g).$$

This group is called the dual group of $G$, and is denoted by $\hat{G}$. The identity of $\hat{G}$ is the principal character $\chi_0$, where $\chi_0(g) = 1$ for all $g \in G$. Note that if $|G| = n$, then $g^n = e$ (the identity element) for all $g \in G$. It follows that $(\chi(g))^n = 1$ and thus $\chi(g)$ is an $n^{th}$ root of unity.

Theorem 56: Let $G$ be a finite abelian group. Then:
(1) $|\hat{G}| = |G|$;
(2) $\hat{G} \simeq G$.
(3) We have

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = e, \\ 0 & \text{otherwise}, \end{cases}$$

and

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise}. \end{cases}$$

Proof: (1) Suppose $|G| = n$. Since $G$ is a finite abelian group,

$$G \simeq \mathbb{Z}/h_1\mathbb{Z} \times \cdots \times \mathbb{Z}/h_r\mathbb{Z}$$

Thus there exist $g_1, \ldots, g_r \in G$ such that $g_j^{h_j} = e$ $(1 \le j \le r)$ and every element $g \in G$ has a unique representation in the form

$$g = g_1^{a_1} \cdots g_r^{a_r}$$

with $0 \le a_j \le h_j$ $(1 \le j \le r)$. Note that any character $\chi$ is determined by its action on $g_1, \ldots, g_r$. Since $(\chi(g_j))^{h_j} = 1$, we see that $\chi(g_j)$ is an $h_j^{th}$ root of unity. Thus there are at most $h_1 \cdots h_r$ characters. On the other hand, if $\omega_j$ is a $h_j^{th}$ root of unity, we can define $\chi(g_j) = \omega_j$ $(1 \le j \le r)$ and extend it multiplicatively to all elements of $G$. Thus there are at least $h_1 \cdots h_r$ characters. It follows that $|\hat{G}| = |G|$.

(2) Let $\chi_j$ be the character defined by

$$\chi_j(g_j) = e^{\frac{2\pi i}{h_j}}$$

and $\chi_j(g_k) = 1$ for $j \neq k$. Define $\varphi: G \to \hat{G}$ by

$$\varphi(g_1^{a_1} \cdots g_r^{a_r}) = \chi_1^{a_1} \cdots \chi_r^{a_r}.$$

One can check that $\varphi$ is a homomorphism. Also, since

$$\chi_1^{a_1} \cdots \chi_r^{a_r}(g_j) = e^{\frac{2\pi i a_j}{h_j}},$$

we see that $\chi_1^{a_1} \cdots \chi_r^{a_r} = \chi_0$ if and only if $a_j = h_j$ $(1 \le j \le r)$, and this corresponds to $g_1^{h_1} \cdots g_r^{h_r} = e$, the identity element of $G$. Thus $\varphi$ is injective. Finally, since $G$ is finite and $|\hat{G}| = |G|$, we see that $\varphi$ is surjective. Thus $\hat{G} \simeq G$.

(3) Let 2015 11 13

$$S(g) = \sum_{\chi \in \hat{G}} \chi(g).$$

If $g = e$, then $\chi(e) = 1$ for all $\chi \in \hat{G}$. Thus $S(g) = |\hat{G}| = |G|$. We now assume that $g \neq e$. By (2), there exists a character $\chi_1 \in \hat{G}$ such that $\chi_1(g) \neq 1$. Also, since $\hat{G} \simeq G$, if $\chi \in \hat{G}$ with $\chi \neq \chi_0$, then there exists $\chi^{-1} \in \hat{G}$ such that $\chi\chi^{-1} = \chi_0$. In particular, if $\chi$ runs through all elements of $\hat{G}$ so does $\chi_1\chi$. Thus we have

$$S(g) = \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\chi_1\chi)(g) = \chi_1(g) \sum_{\chi \in \hat{G}} \chi(g) = \chi_1(g) S(g).$$

Since $\chi_1(g) \neq 1$, we have $S(g) = 0$.

Let

$$T(\chi) = \sum_{g \in G} \chi(g).$$

If $\chi = \chi_0$, then $\chi_0(g) = 1$ for all $g \in G$. Thus $T(\chi_0) = |G|$. If $\chi \neq \chi_0$, then there exists $g_1 \in G$ such that $\chi(g_1) \neq 1$. Thus we have

$$T(\chi) = \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_1 g) = \chi(g_1) \sum_{g \in G} \chi(g) = \chi(g_1) T(\chi).$$

Since $\chi(g_1) \neq 1$, we have $T(\chi) = 0$. ■

Let $k \in \mathbb{N}$ with $k \ge 2$. Let $\chi$ be a character on $(\mathbb{Z}/k\mathbb{Z})^*$. We extend the definition of $\chi$ to $\mathbb{Z}$, also denoted by $\chi$, by putting

$$\chi(a) = \begin{cases} \chi(a+k\mathbb{Z}) & \text{if } (a,k)=1, \\ 0 & \text{otherwise.} \end{cases}$$

We call such $\chi$ a character mod $k$.

Theorem 57: Let $\chi$ be a character mod $k$.

(1) If $(n,k)=1$ then $\chi(n)$ is a $\varphi(k)^{th}$ root of unity.

(2) The function $\chi$ is completely multiplicative, i.e.

$$\chi(nm) = \chi(n)\chi(m)$$

for all $m,n \in \mathbb{Z}$

(3) $\chi$ is periodic modulo $k$, i.e. $\chi(n+k) = \chi(n)$ for all $n \in \mathbb{Z}$.

(4) We have

$$\sum_{\substack{\chi \text{ char.} \\ \text{mod } k}} \chi(n) = \begin{cases} \varphi(k) & \text{if } n \equiv 1 \pmod{k}, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \varphi(k) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

(5) Let $\bar{\chi}$ denote the conjugate character to $\chi$, i.e. $\bar{\chi}(n) = \overline{\chi(n)}$ for all $n \in \mathbb{Z}$. Let $\chi'$ be a character mod $k$. Then for $(m,k)=1$, we have

$$\sum_{\substack{\chi \text{ char.} \\ \text{mod } k}} \chi(n)\bar{\chi}(m) = \begin{cases} \varphi(k) & \text{if } n \equiv m \pmod{k}, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{n=1}^{k} \chi(n)\chi'(n) = \begin{cases} \varphi(k) & \text{if } \chi' = \bar{\chi}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: (1)-(4): The results follow either from definition or theorem 56.

(5): Note that $\bar{\chi}(m)\chi(m) = 1 = \chi(m)\chi(m^{-1})$, where $m^{-1}$ is the multiplicative inverse of $m$ modulo $k$. Thus $\bar{\chi}(m) = \chi(m^{-1})$. It follows that

$$\sum_{\substack{\chi \text{ char.} \\ \text{mod } k}} \chi(n)\bar{\chi}(m) = \sum_{\substack{\chi \text{ char.} \\ \text{mod } k}} \chi(n)\chi(m^{-1}) = \sum_{\substack{\chi \text{ char.} \\ \text{mod } k}} \chi(nm^{-1}).$$

By theorem 56(3), the last sum is $\varphi(k)$ if and only if $nm^{-1} \equiv 1 \pmod{k}$ (i.e. $n \equiv m \pmod{k}$) and $0$ otherwise. Thus the $1^{st}$ result in (5) holds.

Also we note that if $\chi' = \overline{\chi}$, then $\chi\chi' = \chi_0$. Otherwise, $\chi\chi'$ is a non-principle character. Thus the $2^{nd}$ result in (5) follows from theorem 56(3). ∎

We now describe the group of characters mod k. By multiplicity, it is enough to discuss the characters mod $p^\ell$ for a prime p.

(1) Assume first that p is an odd prime. Let g be a primitive root mod $p^\ell$. For $n \in \mathbb{Z}$ with $(n,p)=1$, there exists a unique $\nu \in \mathbb{Z}$ with $1 \le \nu \le \varphi(p^\ell)$ such that $n \equiv g^\nu \pmod{p^\ell}$. For $d \in \mathbb{Z}$ with $1 \le d \le \varphi(p^\ell)$, we define the character $\chi^d(n)$ by

$$\chi^d(n) = \exp\left(\frac{2\pi i d\nu}{\varphi(p^\ell)}\right).$$

We get in this way $\varphi(p^\ell)$ different characters mod $p^\ell$, and this gives the complete list of characters mod $p^\ell$.

(2) Consider characters mod $2^\ell$. If $\ell=1$, we only have the principle character. If $\ell=2$, then we have the principle character and the character $\chi_4$, which is defined by

$$\chi_4(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4, \\ -1 & \text{if } n \equiv 3 \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

If $\ell \ge 3$, then $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ is not cyclic. However, we have seen in theorem 51 that for each $n \in \mathbb{Z}$ with $(2,n)=1$, i.e. $n + 2^\ell\mathbb{Z} \in (\mathbb{Z}/2^\ell\mathbb{Z})^*$, there exists a unique integer pair $(a,b)$ with $0 \le a \le 1$ and $0 \le b \le 2^{\ell-2}$ such that $n \equiv (-1)^a 5^b \pmod{2^\ell}$. Thus for $d \in \mathbb{Z}$ with $1 \le d \le \varphi(2^\ell)$

$$\chi^d(n) = \begin{cases} \exp\left(\dfrac{2\pi i d a}{2} + \dfrac{2\pi i d b}{2^{\ell-2}}\right) & \text{if } n \equiv 1 \pmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

We get in this way $\varphi(2^\ell)$ different characters mod $2^\ell$ and this gives the complete list of characters mod $2^\ell$.