Friday, January 13

Montgomery/Vaughan, Section 4.2

Characters on finite abelian groups

Let G be a finite abelian group.

Define $\hat{G} = \{\chi : G \to S^1\}$
(all group homomorphisms into the unit circle in $\mathbb{C}$).

$\hat{G}$ is a group under pointwise multiplication; the identity is the principal character χ_0 whose values are all 1.

- Suppose that G is cyclic: $G = \langle g \rangle$, g has order n.

Then $\chi(g)^n = \chi(g^n) = \chi(e) = 1$, and so $\chi(g)$ is an n^{th} root of unity. Conversely, if we define
$$\chi(g^k) = e^{2\pi i j k/n}$$
for any $j = 0, 1, \ldots, n-1$, then $\chi \in \hat{G}$ (and these are the only possible ones).

Consequences:

(1) $\hat{G} \cong G$

(2) for any $\chi \in \hat{G}$,

$$\sum_{y \in G} \chi(y) = \begin{cases} \#G, & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \neq \chi_0. \end{cases}$$

(3) for any $y \in G$,

$$\sum_{\chi \in \hat{G}} \chi(y) = \begin{cases} \#G, & \text{if } y = e, \\ 0, & \text{if } y \neq e. \end{cases}$$

(2) & (3) are called "orthogonality relations".

<u>Lemma</u>: If G_1 and G_2 are finite abelian groups, then

$$\widehat{G_1 \times G_2} \cong \hat{G}_1 \times \hat{G}_2$$

$$\chi(g_1, g_2) \longmapsto (\chi(g_1, e), \chi(e, g_2))$$

[proof is standard from definitions]

<u>Corollary</u>: If (1), (2), (3) hold for G_1 and G_2, then they hold for $G_1 \times G_2$. [another standard proof]

Consequence (since every finite abelian group is the product of cyclic groups):
(1), (2), (3) hold for <u>every</u> finite abelian group.

Specialize now to $G = (\mathbb{Z}/q\mathbb{Z})^\times$, where $q \in \mathbb{N}$. Then elements of $\hat{G}$ are "Dirichlet characters".

- By (1), $\# \hat{G} = \# G = \phi(q)$.
- (2): For fixed $\chi \in \hat{G}$,

$$\sum_{\substack{1 \le a \le q \\ (a,q)=1}} \chi(a) = \begin{cases} \phi(q), & \text{if } \chi = \chi_0, \\ 0, & \text{if } \chi \ne \chi_0. \end{cases}$$

- (3) For fixed a,

$$\sum_{\chi \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}} \chi(a) = \begin{cases} \phi(q), & \text{if } a \equiv 1 \pmod{q}, \\ 0, & \text{if } a \not\equiv 1 \pmod{q}. \end{cases}$$

Examples for small q:

- $q=1$: only χ_0
- $q=2$: only χ_0 $(\phi(2)=1)$
- $q=3$: χ_0, and χ_1 given by $\chi_1(1 \bmod 3) = 1$, $\chi_1(2 \bmod 3) = -1$
- $q=4$: χ_0, and $\chi_2(1 \bmod 4) = 1$, $\chi_2(3 \bmod 4) = -1$
- $q=5$: $\phi(5)=4$.

  $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic, generated by 2:

a	$\chi_0(a)$	$\chi_3(a)$	$\chi_4(a)$	$\chi_5(a)$
1	1	1	1	1
2	1	i	-1	$-i$
3	1	$-i$	-1	i
$4 \equiv -1$	1	-1	1	-1

(mod 5)

$q=12$: $\phi(12)=4$.

$$(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times$$
$$\cong (\mathbb{Z}/2\mathbb{Z})^+ \oplus (\mathbb{Z}/2\mathbb{Z})^+$$

a	$\chi_0(a)$	$\chi_6(a)$	$\chi_7(a)$	$\chi_8(a)$
1	1	1	1	1
5	1	1	-1	-1
7	1	-1	1	-1
11	1	-1	-1	1

Note:
$$\begin{tikzcd}
(\mathbb{Z}/12\mathbb{Z})^\times \arrow[r, "\pi"] \arrow[dr, "\chi_6"'] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[d, "\chi_2"] \\
& S^1
\end{tikzcd}$$

We say $\chi_2 \pmod 4$ induces $\chi_6 \pmod{12}$.

Similarly,
$$\begin{tikzcd}
(\mathbb{Z}/12\mathbb{Z})^\times \arrow[r, "\pi"] \arrow[dr, "\chi_7"'] & (\mathbb{Z}/3\mathbb{Z})^\times \arrow[d, "\chi_1"] \\
& S^1
\end{tikzcd}$$

and
$$\begin{tikzcd}
(\mathbb{Z}/12\mathbb{Z})^\times \arrow[r] \arrow[dr, "\chi_0"'] & (\mathbb{Z}/1\mathbb{Z})^\times \arrow[d, "\chi_0"] \\
& S^1
\end{tikzcd}$$

Note: χ_8 can't be obtained in this way.

We say χ_8 is a primitive character (mod 12), while χ_0, χ_6, χ_7 are imprimitive.

<u>Definition:</u> A Dirichlet character (mod q), $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to S^1$, is imprimitive if there exists a divisor d of q, $d \neq q$, such that χ factors through $(\mathbb{Z}/d\mathbb{Z})^\times$.

(that is, if there's another character χ_1 (mod d) such that $\chi = \chi_1 \cdot \chi_0$ ← mod q.)

The smallest such d is the <u>conductor</u> of χ.

(Ex: χ_0 always has conductor 1.)

If no such $d < q$ exists, then χ is <u>primitive</u>, and its conductor is q.

<u>Side note:</u> Let $\phi^*(q)$ denote the number of primitive characters (mod q). Then

$$\phi(q) = \sum_{d \mid q} \phi^*(d)$$

(partition χ (mod q) by their conductors)

and thus

$$\phi^*(q) = \sum_{d \mid q} \phi(d) \mu(q/d).$$

↳ ϕ^* is multiplicative.