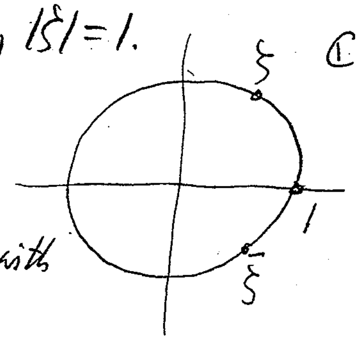
§14. Characters of Finite Abelian Groups: Extensions and Orthogonality

NOTATION. C denotes the set of all $\xi \in \mathbb{C}$ satisfying $|\xi| = 1$. If we identify $\mathbb{C}$ with $\mathbb{R}^2$, then C is the unit circle centered at $O = (0,0)$ in the xy plane



THM A C is a subgroup of $\mathbb{C}^* = \{z \in \mathbb{C} : z \neq 0\}$, with $\xi^{-1} = \bar{\xi}$ (the complex conjugate) for $\xi \in C$.

C is called the <u>circle group</u>.

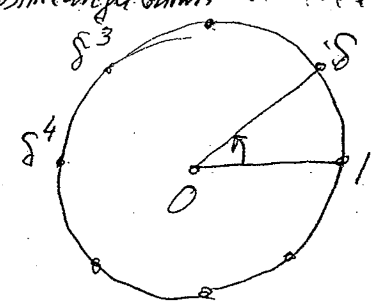
Proof. Clearly $1 \in C$. Also, for z_1 & $z_2 \in \mathbb{C}$, we have $|z_1 z_2| = |z_1||z_2|$, so

$$\xi_1 \,\&\, \xi_2 \in C \implies \xi_1 \xi_2 \in C.$$

Also, for $z \in \mathbb{C}^*$, $z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$. For $\xi \in C$ this gives $\xi^{-1} = \bar{\xi} \in C$. Thus C is a subgroup of $\mathbb{C}^*$.

THM B Each finite subgroup of C is cyclic.

Proof. Let D be a finite subgroup of C. If $D = 1$ then $D = \langle 1 \rangle$, cyclic. If $D \neq 1$, let δ be the element $\neq 1$ in D for which the positive angle shown is minimal.



For $\xi \in D$, either $\xi = \delta^k$ for some $k \in \mathbb{Z}$ or ξ is strictly between δ^k and δ^{k+1} for some $k \in \mathbb{Z}$. In the second case, $\xi\delta^{-k}$ is in D, but has smaller positive angle than δ, a contradiction. Thus $\xi \in \langle \delta \rangle$, showing $D = \langle \delta \rangle$, which is cyclic.

REMARK Not every infinite subgroup of C is cyclic. For example, let θ be an irrational number, eg. $\theta = \sqrt{2}$, and let $D = \langle e^{2\pi i \theta}, -1 \rangle$. If D were cyclic, say generated by $\delta = e^{2\pi i \varphi}$, then there would be $k \,\&\, l \in \mathbb{Z}$ with

$$e^{2\pi i \theta} = e^{2\pi i k\varphi} \quad \& \quad -1 = e^{2\pi i l\varphi}$$

so there would be integers $m \,\&\, n \in \mathbb{Z}$ so that

$$\theta = k\varphi + m, \quad \tfrac{1}{2} = l\varphi + n.$$

Since θ is irrational the first equation implies φ is irrational. Since φ is irrational, the second equation implies $b=0$, $n=\frac{1}{2}$, a contradiction.

DEF. Let G be a finite abelian group. A character of G is a homomorphism $\chi : G \to C$. The set of all characters of G is denoted by $\widehat{G}$.

THM C. Let G be a finite abelian group. If χ & $\chi' \in \widehat{G}$, then the product[*] $\chi\chi' \in \widehat{G}$. This multiplication makes $\widehat{G}$ into a finite abelian group, called the character group of G. In $\widehat{G}$ the identity element is the constant function 1, and the inverse of χ is $\overline{\chi}$.

EXERCISE 1(a) Let X be a set and M a monoid, and let $\mathcal{M}(X,M)$ be the set of all maps $f : X \to M$. With a multiplication defined on $\mathcal{M}(X,M)$ by

$$(fg)(x) = f(x)g(x) \quad \text{for } f \,\&\, g \in \mathcal{M}(X,M) \text{ and } x \in X,$$

prove that $\mathcal{M}(X,M)$ is also a monoid. What is its identity element?

(b) If X is a set and G is a group, prove that $\mathcal{M}(X,G)$ is a group. What is the inverse in $\mathcal{M}(X,G)$ of $f : X \to G$?

(c) Let G be a finite abelian group, and let $\mathcal{M}(G,C)$ be the group of all maps $f : G \to C$. Prove that $\widehat{G}$ is a subgroup of $\mathcal{M}(G,C)$.

(d) Complete the proof of THM C, except for the statement that $\widehat{G}$ is finite.

Proof that $\widehat{G}$ is finite. Let G be a finite abelian group of order n. By Lagrange, each subgroup of G has order dividing n, so each element $g \in G$ has order dividing n (since the order of g is the order of the cyclic subgroup $\langle g \rangle$ generated by g). For each character χ of G, we have

$$\chi(g)^n = \chi(g^n) = \chi(1) = 1,$$

*) $(\chi\chi')(g) = \chi(g)\chi'(g)$

so there are only n possibilities for $\chi(g)$ (the n nth roots of unity in $\mathbb{C}$, i.e. elements of C_n).
It follows that G has $\leq n^n$ different characters, i.e. $|\widehat{G}| \leq n^n$ $(< \infty)$.

THM D. If G is a finite cyclic group, then $\widehat{G} \simeq G$

Proof. Let $G = \langle g \rangle$ have order n. Since $g^n = 1$, each $\chi \in \widehat{G}$ satisfies $\chi(g)^n = 1$, i.e. $\chi(g) = \zeta$ for some $\zeta \in C_n$. For each $k \in \mathbb{Z}$,

✓ $\chi(g^k) = \chi(g)^k = \zeta^k$, so χ is determined by ζ.

For each $\zeta \in C_n$, define $\chi_\zeta : G \to \mathbb{C}$ by

✓✓ $\chi_\zeta(g^k) = \zeta^k$ for $k \in \mathbb{Z}$

(This map is well defined since

$$g^{k_1} = g^{k_2} \Rightarrow g^{k_1 - k_2} = 1 \Rightarrow n \mid k_1 - k_2 \Rightarrow \zeta^{k_1 - k_2} = 1 \Rightarrow \zeta^{k_1} = \zeta^{k_2}.)$$

One checks easily that $\chi_\zeta \in \widehat{G}$: complete the check.

$$\chi_\zeta(g^k \cdot g^l) = \chi_\zeta(g^{k+l}) = \zeta^{k+l} = .$$

One checks also that the map $\zeta \mapsto \chi_\zeta$ is a homomorphism from C_n to $\widehat{G}$: In fact, for $\eta, \zeta \in C_n$ and $k \in \mathbb{Z}$ complete the check.

$$\chi_{\eta\zeta}(g^k) = (\eta\zeta)^k = \eta^k \zeta^k =$$

By ✓ and ✓✓ above, each $\chi \in \widehat{G}$ is of the form χ_ζ for some $\zeta \in C_n$, so the map $\zeta \mapsto \chi_\zeta$ is surjective, and since

$$\chi_\zeta = 1 \Rightarrow \zeta^k = 1 \ \forall k \in \mathbb{Z} \Rightarrow \zeta = 1,$$

the map is injective. Thus $\zeta \mapsto \chi_\zeta$ is an isomorphism from C_n to $\widehat{G}$. Since by the exercise below, cyclic groups of equal order are isomorphic, $\widehat{G} \simeq C_n \simeq G$.

EXERCISE 2. Prove that if G_1 and G_2 are cyclic groups of equal order, then $G_1 \simeq G_2$.

THM E (Character Extension Theorem) If H is a subgroup of a finite abelian group G, then each character ψ of H <u>extends</u> to a character χ of G, i.e. some character χ of G <u>restricts</u> to ψ, i.e. $\chi(h) = \psi(h)$ for all $h \in H$.

$\chi \quad G$
$\psi \quad H$

Proof. (By induction on $|G/H|$).

If $|G/H| = 1$, then $H = G$, so each $\psi \in \hat{H}$ <u>is</u> a character of G.

If $|G/H| > 1$, choose $gH \in G/H$ with $gH \neq H$, and put $M/H = \langle gH \rangle$, the cyclic subgroup of G/H generated by the element gH. Thus $H \subsetneqq M \subset G$.

$G - M - H - 1$

If $M \neq G$, then both $|M/H|$ and $|G/M|$ are $< |G/H|$, so by induction ψ extends to a character ξ of M, and ξ extends to a character χ of G.

Thus we may suppose $M = G$, so $G/H = \langle gH \rangle$ is cyclic. Let $n = |G/H|$. Then G is partitioned into the n cosets $g^r H$ with $r = 0, 1, \dots, n-1$.

Since $g^n H = (gH)^n = H$, we have $\boxed{g^n \in H}$.

If ψ <u>does</u> extend to a character χ of G, then $\chi(g)^n = \chi(g^n) = \psi(g^n)$.

To finish the proof we will show that for each $\xi \in \mathbb{C}$ satisfying $\xi^n = \psi(g^n)$, the map $\chi : G \to \mathbb{C}$ defined by

$$\checkmark \qquad \chi(g^r h) = \xi^r \psi(h) \quad \text{for } 0 \le r < n \text{ and } h \in H.$$

is a character of G, and χ <u>does</u> restrict to ψ.

Since each element of G is uniquely of the form $g^r h$ with $0 \le r < n$ and $h \in H$, the map χ is well defined. For $0 \le r, r' < n$ and $h, h' \in H$, we have

$$\checkmark\checkmark \quad g^r h g^{r'} h' = g^{r+r'} \cdot h h' \quad (\text{which we write } g^{r+r'-n} \cdot g^n h h' \text{ if } r + r' \ge n).$$

By $\checkmark$ and $\checkmark\checkmark$,

$$\chi(g^r h \cdot g^{r'} h') = \chi(g^{r+r'} \cdot h h') = \begin{cases} \xi^{r+r'} \psi(h h') & \text{if } r + r' < n \\ \xi^{r+r'-n} \psi(g^n h h') & \text{if } r + r' \ge n \end{cases}$$

$$\overset{(=)}{=} \xi^r \psi(h) \xi^{r'} \psi(h') = \chi(g^r h) \chi(g^{r'} h') \text{ in both cases,}$$

so $\chi \in \hat{G}$, the $(=)$ by (iii) above. The case $r = 0$ of $\checkmark$ shows that χ restricts to ψ.

COR. For each finite abelian group G and each $h \in G$ with $h \neq 1$, we have $\chi(h) \neq 1$ for some $\chi \in \widehat{G}$.

Proof. Let $H = \langle h \rangle$, the cyclic subgroup generated by h. Since $H \neq 1$, we have $\widehat{H} \neq 1$ so there is a $\psi \in \widehat{H}$ with $\psi \neq 1$, so $\psi(h) \neq 1$. Let $\chi \in \widehat{G}$ extend ψ. Then $\chi(h) \neq 1$.

THM F (Orthogonality Relations) For each finite abelian group G,

(1) if $\chi, \chi' \in \widehat{G}$, then $\displaystyle\sum_{g \in G} \bar{\chi}(g)\chi'(g) = \begin{cases} |G|, & \text{if } \chi = \chi' \\ 0, & \text{if } \chi \neq \chi' \end{cases}$;

(2) if $g, g' \in G$, then $\displaystyle\sum_{\chi \in \widehat{G}} \bar{\chi}(g)\chi(g') = \begin{cases} |\widehat{G}|, & \text{if } g = g' \\ 0 & \text{if } g \neq g' \end{cases}$.

Proof. (1) Put $\xi = \bar{\chi}\chi'$. To show:

$$\checkmark \quad \sum_{g \in G} \xi(g) = \begin{cases} |G| & \text{if } \xi = 1 \\ 0 & \text{if } \xi \neq 1. \end{cases}$$

If $\xi = 1$, the sum is clearly $|G|$. If $\xi \neq 1$ then some $\xi(g_1) \neq 1$, so

$$\xi(g_1) \sum_{g \in G} \xi(g) = \sum_{g \in G} \xi(g_1)\xi(g) = \sum_{g \in G} \xi(g_1 g) = \sum_{g \in G} \xi(g),$$

so, since $\xi(g_1) \neq 1$, the sum in $\checkmark$ is 0.

(2) Put $h = g^{-1}g'$. To show

$$\checkmark\checkmark \quad \sum_{\chi \in \widehat{G}} \chi(h) = \begin{cases} |\widehat{G}| & \text{if } h = 1 \\ 0 & \text{if } h \neq 1. \end{cases}$$

If $h = 1$, the sum is clearly $|\widehat{G}|$. If $h \neq 1$, then some $\chi_1(h) \neq 1$ (by COR), so

$$\chi_1(h) \sum_{\chi \in \widehat{G}} \chi(h) = \sum_{\chi \in \widehat{G}} \chi_1(h)\chi(h) = \sum_{\chi \in \widehat{G}} (\chi_1\chi)(h) = \sum_{\chi \in \widehat{G}} \chi(h),$$

so, since $\chi_1(h) \neq 1$, the sum in $\checkmark\checkmark$ is 0.

THM G For each finite abelian group G, we have $\boxed{|\widehat{G}| = |G|}$

Proof. $|\widehat{G}| = |\widehat{G}| + 0 + \cdots + 0 = \displaystyle\sum_{g \in G}\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}}\sum_{g \in G} \chi(g) = |G| + 0 + \cdots + 0 = |G|.$