Thursday, May 12, 2016 12:22 PM

We will explore the main properties of the dual of a finite abelian group G.

Def. $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$.

• Notice that, for any $\alpha \in \hat{G}$, $g \in G$,

$$\alpha(g)^{|G|} = \alpha(g^{|G|}) = 1 \Rightarrow |\alpha(g)| = 1.$$

In fact $\alpha(g)$ is a $|G|^{\text{th}}$ root of unity. So

$$\hat{G} = \mathrm{Hom}(G, S^1).$$

• Pointwise multiplication turns $\hat{G}$ into an abelian group:

$(\alpha_1 \cdot \alpha_2)(g) := \alpha_1(g)\alpha_2(g)$. [Check why $\alpha_1 \cdot \alpha_2 \in \hat{G}$]

$\alpha^{-1}(g) := \alpha(g)^{-1}$ [Check why α^{-1} is the inverse of α under the above multiplication.]

• Suppose H is a subgroup of G. Then the restriction of a group homomorphism of G to H gives us a group homomorphism of H. So we get a map $\hat{G} \xrightarrow{r} \hat{H}$.

Proposition ① r is an onto homomorphism.

② $\ker(r) \simeq \widehat{(G/H)}$.

Proof. ① We have to show any group homomorphism

$$\overline{\alpha} : H \to S^1$$

can be extended to a group homomorphism

$$\alpha : G \to S^1.$$

We prove this by strong induction on $[G : H]$.

Base is clear as $|G:H|=1 \Rightarrow G=H$.

Strong induction step. Let $g \in G \setminus H$ and $d = \mathrm{ord}(gH)$ in G/H,

i.e. d is the smallest positive integer d such that $g^d \in H$.

So the group generated by g and H is

$$H \cup gH \cup \cdots \cup g^{d-1}H.$$

Let $\zeta \in S^1$ be such that $\zeta^d = \alpha(g^d)$.

let $\alpha' : H \cup gH \cup \cdots \cup g^{d-1}H \longrightarrow S^1$,

$$\alpha'(g^i h) := \zeta^i \alpha(h) \qquad \text{for any } i \in \mathbb{Z}.$$

Claim α' is well-defined, i.e.

$$g^{i_1}h_1 = g^{i_2}h_2 \Rightarrow \zeta^{i_1}\alpha(h_1) = \zeta^{i_2}\alpha(h_2).$$

Pf of claim. $g^{i_1}h_1 = g^{i_2}h_2 \Rightarrow g^{i_1-i_2}h_1 = h_2$

$$\Rightarrow \begin{cases} g^{i_1-i_2}H = H \Rightarrow d \mid i_1 - i_2 \\ \alpha(g^{i_1-i_2})\alpha(h_1) = \alpha(h_2) \end{cases}$$

$$\Rightarrow \alpha(g^d)^{\frac{i_1-i_2}{d}}\alpha(h_1) = \alpha(h_2)$$

$$\Rightarrow \left(\zeta^d\right)^{\frac{i_1-i_2}{d}}\alpha(h_1) = \alpha(h_2)$$

$$\Rightarrow \zeta^{i_1}\alpha(h_1) = \zeta^{i_2}\alpha(h_2). \quad \blacksquare$$

Claim. α' is a group homomorphism.

Pf of claim. $\alpha'((g^{i_1}h_1)\cdot(g^{i_2}h_2)) = \alpha'(g^{i_1+i_2}h_1h_2)$

$$= \zeta^{i_1+i_2}\alpha(h_1h_2)$$

$$= \zeta^{i_1}\alpha(h_1)\cdot\zeta^{i_2}\alpha(h_2)$$

$$= \alpha'(g^{i_1}h_1)\,\alpha'(g^{i_2}h_2).$$

$$\alpha'((g^i h)^{-1}) = \alpha'(g^{-i}h^{-1}) = \zeta^{-i}\alpha(h^{-1})$$

$$= \left(\zeta\alpha(h)\right)^{-1}. \quad \blacksquare$$

so α can be extended to a group homomorphism

$$\alpha' : \langle H, g \rangle \longrightarrow S^1.$$

Since $[G : \langle H, g \rangle] < [G : H]$, by the strong induction hypothesis's α' can be extended to $\alpha : G \longrightarrow S^1$.

② $\alpha \in \ker(r) \iff \forall\, h \in H,\ \alpha(h) = 1.$

$$\iff H \subseteq \ker(\alpha)$$

$$\iff \exists\, \bar{\alpha} : G/H \longrightarrow S^1 \text{ s.t. } \alpha(g) = \bar{\alpha}(gH).$$

So we get a bijection between

$$\ker(r) \quad \text{and} \quad \widehat{(G/H)}.$$

And it is easy to see that it is a group homomorphism. ∎

Remark we get a Short Exact Sequence

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

Proposition $|G| = |\hat{G}|$.

(In fact they are isomorphic.)

Proof. We proceed by strong induction on $|G|$. The base case is trivial.

Let $g_0 \in G \setminus \{1\}$ and $H = \langle g_0 \rangle$. Suppose $o(g_0) = d$. Then

- $\forall\, \bar{\alpha} \in \hat{H}$, $\bar{\alpha}(g_0)^d = \bar{\alpha}(g_0^d) = 1 \Rightarrow \bar{\alpha}(g_0) = \zeta_d^i$ for some $0 \le i < d$ where $\zeta_d = e^{2\pi i/d}$.
- For any $0 \le i < d$, let $\bar{\alpha}_i(g_0^j) := \zeta_d^{ij}$. It is easy to see that $\bar{\alpha}_i \in \hat{H}$.

So $\hat{H}$ is in bijection with $\{1, \zeta_d, \cdots, \zeta_d^{d-1}\}$.

$$\hat{H} \longrightarrow \{1, \zeta_d, \cdots, \zeta_d^{d-1}\}$$

$$\bar{\alpha} \longmapsto \bar{\alpha}(g).$$

$$\overline{\alpha} \longmapsto \overline{\alpha}(g).$$

$$\Longrightarrow |\hat{H}| = d = |H|.$$

. If $H = G$, we are done. Otherwise

$$|\hat{G}| = |\hat{H}|\,|\widehat{(G/H)}| = |H|\,|G/H| = |G|. \quad \blacksquare$$

by strong induction hypothesis

Proposition $f: G \longrightarrow \hat{\hat{G}}$, $f(g): \hat{G} \longrightarrow S^1$,

$$f(g)(\alpha) := \alpha(g)$$

is a group isomorphism.

Proof. Homomorphism: $f(g_1 g_2)(\alpha) = \alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) = \alpha(g_1)\alpha(g_2)$

$$= f(g_1)(\alpha)\ f(g_2)(\alpha)$$

$$= \left(f(g_1)\cdot f(g_2)\right)(\alpha).$$

$$f(g^{-1})(\alpha) = \alpha(g^{-1}) = \alpha(g)^{-1} = f(g)(\alpha)^{-1}$$

$$= \left(f(g)\right)^{-1}(\alpha).$$

Injective. We need to show $g \in \ker(f) \Rightarrow g = 1$.

If $g \neq 1$, then $\exists\, \overline{\alpha} \in \hat{\langle g \rangle}$ s.t. $\overline{\alpha}(g) \neq 1$.

We can extend $\overline{\alpha}$ to $\alpha \in \hat{G}$. So

$$\forall g \neq 1,\ \exists\, \alpha \in \hat{G} \text{ s.t. } \alpha(g) \neq 1.$$

$$\Rightarrow f(g)(\alpha) \neq 1$$

$$\Rightarrow f(g) \neq \text{trivial in } \hat{\hat{G}} = \mathrm{Hom}(\hat{G}, S^1).$$

$$\Rightarrow g \notin \ker(f).$$

Surjective. By the previous Proposition

$$\left.\begin{aligned} |G| &= |\hat{G}| \\ |\hat{G}| &= |\hat{\hat{G}}| \end{aligned}\right\} \Rightarrow |G| = |\hat{\hat{G}}| \Rightarrow \text{so any injection } G \to \hat{\hat{G}} \text{ is a bijection.}$$

$|\hat{G}| = |\hat{\hat{G}}|$ ✓ $\quad G \to \hat{\hat{G}}$ is a bijection. ■

Lemma. For any finite abelian group G we have

$$\forall \alpha \in \hat{G} \setminus \{1\}, \quad \sum_{g \in G} \alpha(g) = 0.$$

Proof. Since $\alpha \neq 1$, $\exists\, g' \in G : \alpha(g') \neq 1$.

$$\Rightarrow \quad \sum_{g \in G} \alpha(gg') = \sum_{g \in G} \alpha(g)$$

$$\Rightarrow \quad \left(\sum_{g \in G} \alpha(g)\right)(\alpha(g') - 1) = 0 \quad \Big\{ \alpha(g') \neq 1 \Rightarrow \sum_{g \in G} \alpha(g) = 0. \quad \blacksquare$$

Corollary For any finite abelian group G we have

$$\forall\, g \in G \setminus \{1\}, \quad \sum_{\alpha \in \hat{G}} \alpha(g) = 0.$$

Proof. By the above Propositions we know that

$$\hat{\hat{G}} = \{\alpha \longmapsto \alpha(g) \mid g \in G\}.$$

So the Lemma applied to $\hat{G}$ gives us the corollary. ■

Theorem. $\hat{G}$ is an orthonormal basis of $\{f : G \to \mathbb{C}\}$

with respect to the dot product $\langle f_1, f_2 \rangle := \frac{1}{|G|} \sum_{g \in G} f_1(g)\, \overline{f_2(g)}$.

Proof. $\forall g \in G$, let $\delta_g : G \to \mathbb{C}$, $\delta_g(g') = \begin{cases} 0 & g \neq g', \\ 1 & g = g'. \end{cases}$

$$\forall f : G \to \mathbb{C}, \quad f = \sum_{g \in G} f(g)\, \delta_g \Rightarrow f \in \sum_{g \in G} \mathbb{C}\, \delta_g. \Big\}$$

$$\langle \delta_{g_1}, \delta_{g_2} \rangle = \begin{cases} 0 & \text{if } g_1 \neq g_2 \\ 1/|G| & \text{if } g_1 = g_2 \end{cases} \Rightarrow \{\delta_g\}_{g \in G} \text{ is linearly indep.}$$

$$\Rightarrow \dim \{f : G \to \mathbb{C}\} = |G|.$$

Since $|G| = |\hat{G}|$, it is enough to prove that $\hat{G}$ consists of orthonormal functions, i.e. $\langle \alpha_1, \alpha_2 \rangle = \begin{cases} 0 & \text{if } \alpha_1 \neq \alpha_2 \end{cases}$

orthonormal functions, i.e. $\langle \alpha_1, \alpha_2 \rangle = \begin{cases} \\ 1 \end{cases}$ otherwise.

$$\langle \alpha_1, \alpha_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha_1(g)\, \overline{\alpha_2(g)}$$

$$= \frac{1}{|G|} \sum_{g \in G} \alpha_1(g)\, \alpha_2(g)^{-1}$$

$|z|=1 \Rightarrow z \cdot \bar{z} = 1.$

$$= \frac{1}{|G|} \sum_{g \in G} (\alpha_1 \cdot \alpha_2^{-1})(g) = \begin{cases} \frac{1}{|G|} \sum_{g \in G} 1 & \text{if } \alpha_1 = \alpha_2 \\ 0 & \text{if } \alpha_1 \neq \alpha_2 \end{cases}$$

above corollary applied to $\alpha_1 \cdot \alpha_2^{-1}$

$$= \begin{cases} 1 & \text{if } \alpha_1 = \alpha_2 \\ 0 & \text{if } \alpha_1 \neq \alpha_2. \end{cases}$$

■

Theorem. For any finite abelian group G we have

$$\prod_{\alpha \in \hat{G}} (T - \hat{\alpha}(g_0)) = (T^{o(g_0)} - 1)^{|G|/o(g_0)}.$$

Proof. Let $R_{g_0} : \{f : G \to \mathbb{C}\} \to \{f : G \to \mathbb{C}\}$,

$$R_{g_0} f(g) := f(g g_0).$$

- R_{g_0} is a linear function:

$$R_{g_0}(c_1 f_1 + c_2 f_2) = c_1 R_{g_0} f_1 + c_2 R_{g_0} f_2.$$

- $\forall \alpha \in \hat{G}$, $(R_{g_0} \alpha)(g) = \alpha(g_0 g) = \alpha(g_0)\alpha(g)$

$\Rightarrow R_{g_0} \alpha = \alpha(g_0)\, \alpha$

$\Rightarrow R_{g_0}$ is diagonal in the basis $\hat{G}$, and its diagonal entries are $\alpha(g_0)$'s.

$\Rightarrow$ The characteristic polynomial of R_{g_0} is

$$\prod_{\alpha \in \hat{G}} (T - \alpha(g_0)).$$

On the other hand $(R_{g_0} \delta_g)(g') = \delta_g(g' g_0) = \delta_{g g_0^{-1}}(g')$

Q δ

$\Rightarrow$ R_{g_0} just permutes δ_g's

$\Rightarrow$ In the basis $\{\delta_g\}_{g\in G}$, R_{g_0} is a permutation matrix. In each coset of $\langle g_0\rangle$, R_{g_0} induces a cycle of length $o(g_0)$. So its matrix is

$$\begin{bmatrix} C & & \\ & C & \\ & & \ddots \\ & & & C \end{bmatrix} \quad \text{where} \quad C = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{bmatrix}$$

$|G|/o(g_0)$-many; C is $o(g_0) \times o(g_0)$

$\Rightarrow$ Its characteristic polynomial is

$$(\text{Char. poly. of } C)^{|G|/o(g_0)} \overset{?}{=} (T^{o(g_0)} - 1)^{|G|/o(g_0)}.$$

■