$G/H \hookrightarrow G$ USING CHARACTER THEORY

ANURAG SAHAY

1. Introduction

The goal of this note is to prove the following fact:

Theorem 1.1. *Let G be a finite Abelian group, and $H \subseteq G$ a subgroup. Then, G contains an isomorphic copy of G/H.*

In other words, whenever $H \subseteq G$ is a subgroup, then $G/H \hookrightarrow G$. The proof we will provide will use the character (or representation) theory of finite Abelian groups, which is also called Fourier analysis on finite Abelian groups.

The proof uses two facts. The first is that if G is a finite Abelian group then $G \approx \widehat{G}$ where by $\approx$ we mean isomorphism. The second is that in the category of finite Abelian groups, $G \mapsto \widehat{G}$ is an exact contravariant functor. Thus, if $H \subseteq G$, we have the short exact sequence

$$0 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 0$$

and by contravariance and exactness, this gives us a short exact sequence

$$0 \longrightarrow \widehat{G/H} \longrightarrow \widehat{G} \longrightarrow \widehat{H} \longrightarrow 0$$

whose first joint tells us that $\widehat{G/H} \hookrightarrow \widehat{G}$. However, since $\widehat{G} \approx G$ and $\widehat{G/H} \approx G/H$, we conclude that $G/H \hookrightarrow G$ as desired.

In the rest of this note we formalize these statements without using categorical language. For the rest of this note, G and H will always be finite Abelian groups written additively, with the identity always denoted by 0.

In Section 2, we state without proof the group theoretic preliminaries; in Section 3 we describe the basics of character theory and prove the exactness of the functor; and finally, in Section 4 we prove that every finite Abelian group is isomorphic to its dual.

2. Group Theory Preliminaries

Theorem 2.1 (Weak Fundamental Theorem)**.** *Let G be a finite Abelian group. Then, either G is cyclic or $G \approx H \times K$ for non-trivial groups H and K.*

Note that the two possibilities here are not mutually exclusive, since, for example, $\mathbb{Z}/6\mathbb{Z} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We call this the weak fundamental theorem since this is a trivial consequence of either form of the usual fundamental theorem of finite Abelian groups – it's interesting to note that this (and, in fact, the fundamental theorem in its full strength) has a purely character theoretic proof, together with the simple fact that for any $x \in G$, $o(x)$ divides the exponent of the group, $\max_{a \in G} o(a)$. We will not pursue this here, see [Con] for more details.

3. The Exactness of Pontryagin Duality

For G, we define its (Pontryagin) dual group $\widehat{G}$ as $\mathrm{Hom}(G, S^1)$. That is, if $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, then we have the following:

Definition 1. Let G be a finite Abelian group. Then,

$$\widehat{G} = \{\chi : G \to \mathbb{C}^\times : \chi \text{ is a group homomorphism}\}$$

is clearly an Abelian group under point-wise multiplication. This group is called the dual group of G.

The dual group will turn out to be finite since $G \approx \widehat{G}$, as proved in Section 4. The functoriality of $G \mapsto \widehat{G}$ is a consequence of the fact that $\mathrm{Hom}(\cdot, \cdot)$ is contravariant in the first variable. Concretely, it is the following statement:

Proposition 3.1. *Let $\varphi : H \to G$ be a group homomorphism. Then, $\widehat{\varphi} : \widehat{G} \to \widehat{H}$ defined by*

$$\widehat{\varphi}(\chi) = \chi \circ \varphi$$

is also a group homomorphism.

Proof. This is straightforward; $\widehat{\varphi}(\chi)$ is a composition of homomorphisms $H \to G \to S^1$ and hence is in $\mathrm{Hom}(H, S^1)$. Checking that $\widehat{\varphi} : \widehat{H} \to \widehat{G}$ is a homomorphism is routine.

□

One of half of showing the exactness of the dual functor is the following:

Proposition 3.2. *Let $\varphi, \widehat{\varphi}$ be as in Proposition 3.1. Then, φ is surjective implies that $\widehat{\varphi}$ is injective.*

Proof. Let $\chi, \nu \in \widehat{G}$ such that $\chi \neq \nu$. Thus, in particular, there is a $g \in G$ such that $\chi(g) \neq \nu(g)$. Since $\varphi : H \to G$ is surjective, $g = \varphi(h)$ for some $h \in H$. However, this implies that $\chi(\varphi(h)) \neq \nu(\varphi(h))$, and hence $\widehat{\varphi}(\chi)(h) \neq \widehat{\varphi}(\nu)(h)$, and hence $\widehat{\varphi}(\chi) \neq \widehat{\varphi}(\nu)$. This shows that $\widehat{\varphi}$ is injective.

□

Note that Proposition 3.2 already reduces Theorem 1.1 to showing that $G \approx \widehat{G}$ for every G. To see this, apply Proposition 3.2 to the canonical surjection $G \twoheadrightarrow G/H$ to get an embedding $\widehat{G/H} \hookrightarrow \widehat{G}$.

The other half of exactness is equivalent to the following lifting property on characters:

Lemma 3.3. *Let $H \subseteq G$, and χ a character on H. Then, there exists an extension χ' of χ to G.*

Proof. We first restate what we want to show. For $\chi \in \widehat{H}$, we want to find $\chi' \in G$ such that $\chi'|_H = \chi$.

Note that $G = \langle H, S \rangle$ for some finite set S. With a simple induction on $|S|$, we can assume without loss of generality that $S = \{g\}$ for some $g \in G$, and hence $G = \langle H, g \rangle$. Let k be the order of g modulo H. That is, let k be the minimal positive integer such that $kg \in H$. Further, define $a = kg$. Since $a \in H$, $\chi(a)$ is well-defined. Let $z \in \mathbb{C}$ be any solution to the equation $z^k - \chi(a) = 0$.

Now, arbitrary $x \in G$ can be written as $x = h + mg$ for $m \in \mathbb{Z}$ and $h \in H$. We define,

$$\chi'(x) = \chi(h) z^m.$$

If χ' is well-defined, it is easily seen to be a homomorphism into S^1.

To show that it is well-defined, suppose that $x = h' + m'g$ is a different representation for x. Then, $(m - m')g = h' - h \in H$, and since k is the order of g in G/H, this implies $k \mid (m - m')$. Writing $m - m' = kq$, and hence $(m - m')g = qa$. We get that

$$\begin{aligned} \chi(h' - h) &= \chi((m - m')g) \\ &= \chi(qa) \\ &= \chi(a)^q \\ &= (z^k)^q \\ &= z^{kq} \\ &= z^{m-m'} \end{aligned}$$

which proves well-definedness.

□

Thus, we get the other half of exactness:

Proposition 3.4. *Let $\varphi, \widehat{\varphi}$ be as in Proposition 3.1. Then, φ is injective implies that $\widehat{\varphi}$ is surjective.*

Proof. If $\varphi(H) \subseteq G$, and so characters on $\varphi(H)$ can be extended to G. Further, since φ is injective, $\varphi(H) \approx H$, and so a character on H can be transported to a character in $\varphi(H)$. Let χ be a character on H, and χ' the character on G obtained by first pulling back the character along φ^{-1} to get a character on $\varphi(H)$, and then extending it using the lifting lemma.

The claim is that $\widehat{\varphi}(\chi') = \chi$. To see this, let $h \in H$. Then, we want to compute $\chi'(\varphi(h))$. However, since $\varphi(h) \in \varphi(H)$, this is $\chi(\varphi^{-1}(\varphi(h)) = \chi(h)$. This completes the proof.

□

4. Self-Duality of Finite Abelian Groups

As remarked earlier, the only missing link in our proof is showing that if G is a finite Abelian group, then it is isomorphic to its Pontryagin dual.

First, we observe that 3.2 and 3.4 together imply that the dual is an isomorphism invariant:

Corollary 4.1. *If $G \approx H$, then $\widehat{G} \approx \widehat{H}$.*

Proof. It suffices to show that if $\varphi : H \to G$ is isomorphism then $\widehat{\varphi}$ is a bijection. This follows from the fact that φ is a bijection, together with Propositions 3.2 and 3.4.

□

With this we can show the following atomic case:

Proposition 4.2. *If G is a cyclic group then $G \approx \widehat{G}$.*

Proof. By the previous corollary, we can assume without loss of generality that $G = \mathbb{Z}/q\mathbb{Z}$. A character $\chi \in \widehat{G}$ is completely determined by what it does to the generator $1 \in \mathbb{Z}/q\mathbb{Z}$. Further, $\chi(1)^q = 1$ since $\chi(q) = \chi(1)^q$ and $q = 0$ in $\mathbb{Z}/q\mathbb{Z}$.

For the sake of argument, choose a qth root of unity and assign it to $\chi(1)$. If $e(t) = e^{2\pi i t}$, then the qth roots of unity are of the form $e(a/q)$ with $a \in \mathbb{Z}/q\mathbb{Z}$. Define χ_a by,

$$\chi_a(x) = e\left(\frac{ax}{q}\right).$$

It is easily verified that χ_a is a character on $\mathbb{Z}/q\mathbb{Z}$, and that $\chi_a(1) = e(a/q)$, and hence from our previous discussion, the set $\{\chi_a : a \in \mathbb{Z}/q\mathbb{Z}\}$ is all of $\widehat{G}$. Finally, it is easily verified that the map $a \mapsto \chi_a$ is a bijective homomorphism and we are done.

□

To be able to glue together the result for all finite Abelian groups, we need to be able to glue things when taking Cartesian products. In particular, the Pontryagin dual behaves as you would expect with products.

Proposition 4.3. *Suppose that G, H and K are finite Abelian groups such that $G \approx H \times K$. Then $\widehat{G} \approx \widehat{H} \times \widehat{K}$.*

Proof. Without loss of generality, suppose $G = H \times K$.

Let $\chi \in \widehat{G}$. Define $\nu \in H$ and $\eta \in K$ by $\nu(h) = \chi(h, 1)$ and $\eta(k) = \chi(1, k)$.

Finally, let $\nu \in H$ and $\eta \in K$. Define $\chi \in G$ by $\chi(h, k) = \nu(h)\eta(k)$.

It is a straightforward exercise to see that the maps $\chi \mapsto (\nu, \eta)$ and $(\nu, \eta) \mapsto \chi$ defined above are between the sets described, are inverses of each other, and are both homomorphisms.

□

We are now ready to prove the self-duality of finite Abelian groups:

Proposition 4.4. *Let G be a finite Abelian group. Then, $G \approx \widehat{G}$.*

Proof. We induct on the size $|G|$. The case $|G| = 1$ is trivially true.

By Theorem 2.1, we have that either G is cyclic or that $G = H \times K$ for H, K non-trivial. In the first case, we can apply 4.2 to conclude that $G \approx \widehat{G}$.

In the second case, we have that $1 < |H|, |K| < |G|$ and so the strong inductive hypothesis tells us that $H \approx \widehat{H}$ and $K \approx \widehat{K}$. Thus, $H \times K \approx \widehat{H} \times \widehat{K}$. Finally, $G \approx H \times K$ implies $\widehat{G} \approx \widehat{H} \times \widehat{K}$. Putting these together, we get that $G \approx \widehat{G}$, closing the induction, and we are done.

□

References

[Con] Keith Conrad. Characters of finite abelian groups. URL:https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf (version: 2021-01-04). 2

Department of Mathematics, University of Rochester
Rochester, NY 14627, USA

Email address: asahay@ur.rochester.edu