Characters of Finite Abelian Groups

R. C. Daileda

Let A be an (additive) abelian group. A *character* of A is a homomorphism

$$\chi : A \to \mathbb{C}^\times.$$

Because A is additive and $\mathbb{C}^\times$ is multiplicative, this means that

$$\chi(a + b) = \chi(a)\chi(b)$$

for all $a, b \in A$. If A happens to be multiplicative, we instead have

$$\chi(ab) = \chi(a)\chi(b)$$

for all $a, b \in A$. It should always be clear from context which of these relations defines χ to be a character of A.

Example 1. For any $a \in \mathbb{C}$, define $\chi : \mathbb{R} \to \mathbb{C}^\times$ by

$$\chi(x) = e^{ax}.$$

Then χ is a character of $\mathbb{R}$.

Example 2. Define $\chi : \mathbb{R}^\times \to \mathbb{C}^\times$ by

$$\chi(x) = \frac{x}{|x|}.$$

Then χ is a character of $\mathbb{R}^\times$. The same definition also yields a character of $\mathbb{C}^\times$ if we allow x to be complex.

Example 3. If $f : A \to B$ is a homomorphism of abelian groups and χ is a character of B, then the composition $\chi \circ f$ is a character of A, since the composition of homomorphisms is a homomorphism.

Example 4. Let $n \in \mathbb{N}$ and choose $\zeta \in \mathbb{C}^\times$ satisfying $\zeta^n = 1$ (an nth root of unity). Define $\psi : \mathbb{Z} \to \mathbb{C}^\times$ by $\psi(m) = \zeta^m$. Then ψ is a character of $\mathbb{Z}$. Let $m\mathbb{Z} = \ker \psi$. By the First Isomorphism Theorem ψ yields a character $\overline{\psi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^\times$. If $a \in n\mathbb{Z}$, so that $a = nk$, then

$$\psi(a) = \zeta^a = \zeta^{nk} = (\zeta^n)^k = 1^k = 1,$$

so that $n\mathbb{Z} \subseteq \ker \psi = m\mathbb{Z}$. In general $n\mathbb{Z}$ and $\ker \psi$ need not be the same. However, as we have seen, the Generalized First Isomorphism Theorem provides a homomorphism

$\overline{\pi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $\overline{\pi}(a + n\mathbb{Z}) = a + m\mathbb{Z}$. Example 3 then tells us that $\chi = \overline{\psi} \circ \overline{\pi}$ is a character of $\mathbb{Z}/n\mathbb{Z}$. It is given explicitly by

$$\chi(a + n\mathbb{Z}) = \overline{\psi}(\overline{\pi}(a + n\mathbb{Z})) = \overline{\psi}(a + m\mathbb{Z}) = \psi(a) = \zeta^a.$$

Example 5. Let A be an additive abelian group and let $n \in \mathbb{N}$. The rule $a \mapsto na$ defines a surjective homomorphism $A \to nA$ whose kernel is clearly the n-torsion subgroup $A[n]$. So by the First Isomorphism Theorem we have

$$A/A[n] \cong nA.$$

If A is finite, this implies $|nA| = |A/A[n]| = |A|/|A[n]|$, so that $[A : nA] = |A|/|nA| = |A[n]|$.

If A is multiplicative, then nA becomes the set (subgroup) $A^n = \{a^n \mid a \in A\}$ of nth powers in A, and the preceding computation shows that $[A : A^n] = |A_n|$, where $A_n = \{a \in A \mid a^n = e\}$ is the subgroup of "nth roots of e" in A.

Example 6. Let p be an odd prime and let $A = (\mathbb{Z}/p\mathbb{Z})^\times$. Take $n = 2$ in the preceding example. The square roots of 1 in $(\mathbb{Z}/p\mathbb{Z})^\times$ satisfy $x^2 \equiv 1 \pmod{p}$, which is is equivalent to $x^2 - 1 \equiv 0 \pmod{p}$. Since $x^2 - 1 = (x - 1)(x + 1)$, we find that $x^2 - 1 \equiv 0 \pmod{p}$ if and only if $p|(x-1)(x+1)$. Because p is prime, this happens if and only if $p|x-1$ or $p|x+1$, i.e. $x \equiv \pm 1 \pmod{p}$. Since $1 \not\equiv -1 \pmod{p}$ (why?), this means that ± 1 are the two distinct square roots of 1 in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Example 5 now tells us that the subgroup T of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ has index $|\{\pm 1\}| = 2$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. So $(\mathbb{Z}/p\mathbb{Z})^\times/T = \{T, \epsilon T\} \cong \{\pm 1\}$. Composing this isomorphism with the natural surjection yields a character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ called the *Legendre symbol*. Notice that $\chi(a) = 1$ if and only if aT is the trivial coset T, which is equivalent to $a \in T$. Likewise, $\chi(a) = -1$ if and only if $aT = \epsilon T$ or $a \in \epsilon T$. We conclude that

$$\chi(a) = \begin{cases} 1 & \text{if } a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times, \\ -1 & \text{otherwise.} \end{cases}$$

The traditional notation for the Legendre symbol is

$$\chi(a) = \left(\frac{a}{p}\right).$$

If q is another odd prime, then $\gcd(q, p) = 1$ so that we may view $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $p \in (\mathbb{Z}/q\mathbb{Z})^\times$. There is a remarkable relationship between the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$, discovered by Euler and Legendre and first proven by Gauss in 1801, known as the *Law of Quadratic Reciprocity*, which states that

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

That is, for odd primes $p \neq q$, whether or not p is a square modulo q depends on whether or not q is a square modulo p! Mathematicians have long been fascinated with the Law of Quadratic Reciprocity, and there are literally hundreds of different published proofs.

Example 7. Let G be a finite group of order n. We have seen previously that $a \mapsto \lambda_a$ defines a monomorphism $\lambda : G \to \mathrm{Perm}(G)$. If we fix an isomorphism $f : \mathrm{Perm}(G) \to S_n$, then $f \circ \lambda$ is an embedding of G into S_n. So we may assume $G \leq S_n$. The sign then determines a homomorphism $\epsilon : G \to \{\pm 1\}$. The sign of $a \in G$ tells you whether or not left multiplication by a is an even or odd permutation of G. Since $\{\pm 1\} \leq \mathbb{C}^\times$, when G is abelian ϵ is a character of G.

Let A be an additive abelian group. Let $\widehat{A}$ denote the set of all characters of A. If $\chi, \psi \in \widehat{A}$, then the function $\chi\psi : A \to \mathbb{C}^\times$ defined by $(\chi\psi)(a) = \chi(a)\psi(a)$ for $a \in A$ is easily seen to be another character of A. This yields a binary operation on $\widehat{A}$, which makes $\widehat{A}$ into a group called the *dual* of A. The identity element in $\widehat{A}$ is the *trivial character*, which is just the trivial homomorphism defined by $\chi_0(a) = 1$ for all $a \in A$. The inverse of $\chi \in \widehat{A}$ is given by $\chi^{-1}(a) = 1/\chi(a) = \chi(a)^{-1}$ for all $a \in A$.

The passage from an abelian group to its dual "reverses arrows" (in the language of category theory, $A \mapsto \widehat{A}$ is a *cofunctor*). Suppose that A and B are abelian groups and we have a homomorphism $f : A \to B$. Given $\chi \in \widehat{B}$, the composition $\chi \circ f$ belongs to $\widehat{A}$. If we define $\widehat{f} : \widehat{B} \to \widehat{A}$ by $\widehat{f}(\chi) = \chi \circ f$, then it is easy to see that $\widehat{f}$ is a homomorphism. We will call $\widehat{f}$ the homomorphism *dual* to f.

An important feature of finite abelian groups is that they are *self-dual*. That is, for any finite abelian group A one has

$$A \cong \widehat{A}. \tag{1}$$

We will prove this as an application of the Fundamental Theorem of Finite Abelian Groups. Recall that the Fundamental Theorem states that every finite abelian group is a direct sum of cyclic groups. Our proof, therefore, will consist of two parts. We will show that the operations of direct sum and dualizing commute, so that the dual of a direct sum is the direct sum of the duals of the individual summands. Then we will show that every finite cyclic group is self-dual. The result (1) then follows immediately.

Lemma 1. *Let A and B be abelian groups. Then*

$$\widehat{A \oplus B} \cong \widehat{A} \oplus \widehat{B}.$$

Sketch of Proof. Let $\pi_A : A \oplus B \to A$ be projection onto the first coordinate, $\pi_A(a, b) = a$, and let $i_A : A \to A \oplus B$ be the "inclusion" $i_A(a) = (a, 0)$. Both are homomorphisms. Define π_B and i_B similarly. We then have the dual maps $\widehat{\pi_A} : \widehat{A} \to \widehat{A \oplus B}$, $\widehat{i_A} : \widehat{A \oplus B} \to \widehat{A}$, $\widehat{\pi_B} : \widehat{B} \to \widehat{A \oplus B}$ and $\widehat{i_B} : \widehat{A \oplus B} \to \widehat{B}$. We "add" these to get homomorphisms

$$\widehat{\pi_A} \oplus \widehat{\pi_B} : \widehat{A} \oplus \widehat{B} \to \widehat{A \oplus B},$$

given by $(\widehat{\pi_A} \oplus \widehat{\pi_B})(\chi, \psi) = \widehat{\pi_A}(\chi)\widehat{\pi_B}(\psi)$, and

$$\widehat{i_A} \oplus \widehat{i_B} : \widehat{A \oplus B} \to \widehat{A} \oplus \widehat{B},$$

given by $(\widehat{i_A} \oplus \widehat{i_B})(\chi) = (\widehat{i_A}(\chi), \widehat{i_B}(\chi))$. It is straightforward to check that these maps are inverse isomorphisms, proving the lemma. The details are left to the reader. □

Lemma 2. *If C is a finite cyclic group, then $C \cong \widehat{C}$.*

Sketch of Proof. We may assume $C = \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. Let $\boldsymbol{\mu}_n \leq \mathbb{C}^\times$ denote the group of nth roots of unity. Given $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$, we have $\chi(1)^n = \chi(n \cdot 1) = \chi(n) = \chi(0) = 1$, so that $\chi(1) \in \boldsymbol{\mu}_n$. It is then easy to see that $\chi \mapsto \chi(1)$ defines a homomorphism $f : \widehat{\mathbb{Z}/n\mathbb{Z}} \to \boldsymbol{\mu}_n$. Because 1 generates $\mathbb{Z}/n\mathbb{Z}$, χ is trivial if and only if $\chi(1) = 1$. This means that $\ker f$ is trivial. Given $\zeta \in \boldsymbol{\mu}_n$, the character χ of Example 4 satisfies $\chi(1) = \zeta$. This shows that f is surjective, and is therefore an isomorphism. Because $\boldsymbol{\mu}_n \cong \mathbb{Z}/n\mathbb{Z}$ we have

$$\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \boldsymbol{\mu}_n \cong \mathbb{Z}/n\mathbb{Z}.$$

This finishes the proof. □

Theorem 1. *Let A be a finite abelian group. Then $A \cong \widehat{A}$.*

Proof. Use the Fundamental Theorem to write

$$A = \bigoplus_{i=1}^{k} C_i,$$

where each C_i is a finite cyclic group. Lemma 1, Lemma 2 and a quick induction then imply

$$\widehat{A} = \widehat{\bigoplus_{i=1}^{k} C_i} \cong \bigoplus_{i=1}^{k} \widehat{C_i} \cong \bigoplus_{i=1}^{k} C_i = A.$$

□

Example 8. As an application, we return to Examples 6 and 7. Let p be an odd prime. The Legendre symbol χ from Example 6 and the sign ϵ from Example 7 both belong to $\widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$. Because exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are perfect squares, χ is nontrivial, i.e. $\operatorname{im}\chi = \{\pm 1\}$. We claim that ϵ is also nontrivial.

To prove this, we need a nontrivial result from number theory. Specifically, for any odd prime p the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is *cyclic*. Specific generators are not easy to identify in general, but all we need to know is that one exists. Write $(\mathbb{Z}/p\mathbb{Z})^\times = \langle r \rangle$. Then $|r| = |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. By homework exercise 10.1.3 we then have

$$\epsilon(r) = (-1)^{(p-1+1)(p-1)/(p-1)} = (-1)^p = -1,$$

since p is odd. In particular, this shows that $-1 \in \operatorname{im}$, which proves that ϵ is nontrivial.

Now let $a \in \widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$. Then by the definition of character multiplication

$$\chi^2(a) = (\chi(a))^2 = (\pm 1)^2 = 1 = \chi_0(a) \;\; \Rightarrow \;\; \chi^2 = \chi_0.$$

Since χ is nontrivial, this shows that $|\chi| = 2$. An identical computation with ϵ shows that $|\epsilon| = 2$. Because $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, Lemma 2 implies that $\widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ is also cyclic of order $p-1$. Recall that a finite cyclic group has a unique subgroup of any allowable size (dividing the order of the group). Since $p-1$ is even, this tells us that $\widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ has a unique subgroup of order 2. But both χ and ϵ generate such a subgroup, by the computations above. Hence

$$\chi = \epsilon.$$

That is, the Legendre symbol, which is essentially the indicator function for the subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$, is the same as the permutation sign character on $(\mathbb{Z}/p\mathbb{Z})^\times$. So the way in which $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ permutes the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ determines whether or not the congruence $x^2 \equiv a \pmod{p}$ has a solution!