Dirichlet Characters

Bobby Shen, Shend Zhjeqi

May 9, 2021

This handout is about Dirichlet characters. These are certain functions from the integers mod k to the complex numbers. In doing so, we will also discuss finite abelian groups and practice tricky summations. Good references are wikipedia: Character_(mathematics) and Dirichlet_character. A very advanced reference is this, by Dr. Andrew Sutherland. He is also known for the sum of three cubes project. Making use of supercomputers, he helped to write 3 as the sum of three cubes, each base of which exceeds 10^{17} in absolute value. Uhh anyways the Dirichlet character reference is `https://math.mit.edu/classes/18.785/2015fa/LectureNotes17.pdf` .

Exercise 1. (Also, definition of U_k)

Let $k > 1$ be an integer. Let S be the set of integers $i, 0 < i < k$ such that $\gcd(i,k) = 0$. Consider the set S with the binary operation of multiplication mod k. Prove that S is an abelian group. The axioms are the identity element, inverses, associativity, and commutativity.

We will denote this set U_k. Formally, this group is often called the wordier $(\mathbb{Z}/k\mathbb{Z})^*$ and defined as the set of invertible residue classes mod k, but we will opt for concrete integers in this handout.

Definition 2. A **Dirichlet character with modulus** k ($k > 1$) is a function χ from U_k to complex numbers that satisfies

- $\chi(m) \neq 0$ for all m in U_k.
- $\chi(mn) = \chi(m)\chi(n)$ for all m, n in U_k, where mn is understood to be taken mod k.

Sometimes, an alternative definition is used. χ is a Dirichlet character of modulus k if χ is a function from $\mathbb{Z}$ to $\mathbb{C}$ that satisfies

- $\chi(n) = \chi(n+k)$ for all integers n,
- If $\gcd(n,k) > 1$, then $\chi(n) = 0$,
- If $\gcd(n,k) = 1$, then $\chi(n) \neq 0$,
- $\chi(mn) = \chi(n)\chi(m)$ for all integers m, n.

For now, we will stick with the former.

Exercise 3. Enumerate all characters over U_5. Note that two characters χ_1, χ_2 are the same if $\forall x \in U_5, \chi_1(x) = \chi_2(x)$. The following steps may be useful.

- For convenience, represent U_5 as the 4 elements $\{1, 2, 3, 4\}$.
- Hereafter, let χ be a character over U_5. Prove that $\chi(1) = 1$.
- Prove that χ sends any element to a 4th root of unity.

I consider explicit tables of numbers to be a good way to enumerate characters. We will follow the convention at wikipedia: Dirichlet_character, except that we will only list numbers relatively prime to the modulus k. Their conventions is that we have a 2-D table. Columns are labeled by integers from 1 to $k-1$ which are relatively prime to k. Rows are labeled with functions $\chi_0, \chi_1, \ldots$. Each row is a single Dirichlet character of modulus k.

Exercise 4. Next, try to describe all characters over U_7, U_8, or U_{15}.

The headline of this handout is the **Fundamental theorem of Dirichlet Characters** (probably not an official name)

Theorem 5. Let $k > 1$. Define the group U_k as above. Let n be the number of elements in U_k. Then there exist exactly n Dirichlet characters of modulus k.

Moreover, labeling the characters arbitrarily as $\chi_0, \ldots, \chi_{n-1}$ with χ_0 as the trivial character (mapping all elements to 1) and for any element $x \in U_k$, there exist nonzero complex numbers $z_0, \ldots z_{n-1}$ such that

$$\forall y \in U_k, \sum_{i=0}^{n-1} z_i \chi_i(y) = (1 \text{ if y = x else } 0).$$

Note: This is slightly stronger than linear independence of characters, where characters are interpreted as vectors in $\mathbb{C}^n$ in the natural way.

Lastly, we have

$$\forall \chi_i, \sum_{x \in U_k} \chi_i(x) = (\text{ n if i = 0 else 0 }).$$

The statements of this theorem can be verified for specific examples based on the tables we have constructed. Hereafter, we will try to present the major steps needed to prove this theorem.

1 Finite cyclic groups and Direct Sums

We have been somewhat avoiding abstract groups, but now we will discuss many finite abelian groups. It is useful to define the following finite abelian groups. It can be considered exercises to prove that these are finite abelian groups by checking the four axioms.

Definition 6. Let $n \geq 1$ be an integer. The **Cyclic group of order** n, often denoted C_n, is given by an abstract generator g, and it is a set of n elements,

$$\{1, g, g^2, \ldots, g^{n-1}\},$$

with the operation of multiplication, and the relations $g^n = 1, g^{-}1 = g^{n-1}$.

Some authors might define C_n as the set of residues mod n with the operation of addition. These two definitions are isomorphic. In the main definition, g is known as a generator of C_n, although the generator is not unique. We may also say that C_n is "a cyclic group of order n generated by g."

Definition 7. let $m, n \geq 1$ be integers. Let C_m, C_n be cyclic groups. **The direct sum of** C_m **and** C_n is denoted $C_m \bigoplus C_n$ and is the set of all ordered pairs

$$\{(a_1, a_2) \mid a_1 \in C_m, a_2 \in C_n\}$$

with an operation still informally called multiplication given by

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 a_2, b_1 b_2).$$

The direct product of k cyclic groups $C_{n_1}, \ldots, C_{n_k}$ is similar. It is denoted $\bigoplus_{i=1}^{k} C_{n_i}$. It is the set of k-tuples whose i^{th} coordinate is in C_{n_i} with multiplication defined similarly.

Exercise 8. What cyclic group is U_5 isomorphic to? For any prime p, is U_p cyclic?

Exercise 9. What is U_8 isomorphic to? How about U_{15}?

Dirichlet characters are a special case of "Multiplicative characters," which we now define.

Definition 10. A **character** is a function χ from a group G to the complex numbers satisfying

$$\forall x, y \in G, \chi(xy) = \chi(x)\chi(y),$$

where xy is given by the group operation on G; moreover, χ cannot send any element to 0. Note that the most general definition would be to any field, but we will focus on $\mathbb{C}$.

Note that a character χ is associated with a specific group. χ is said to be a character over G. There can be multiple characters over G.

2 Fundamental results about finite abelian groups and group characters

Now, we are getting into the serious theorems, the full proofs of which are out of scope but concrete examples are tractable.

Theorem 11. (The fundamental theorem of finite abelian groups) Let G be a finite abelian group. Then there exists a finite sequence of prime powers $q_1, q_2, \ldots, q_k$ (not necessarily distinct) such that G is isomorphic to the direct sum of groups

$$\bigoplus_{i=1}^{k} C_{q_i}.$$

Moreover, the sequence of prime powers is unique up to permutation, meaning that if G is isomorphic to the direct sum of such groups in a second way, then the second sequence is a permutation of the first. We will only use the weaker statement that G is isomorphic to a direct sum of cyclic groups.

The fundamental theorem about Dirichlet characters is true for general finite abelian groups, which we restate briefly.

Theorem 12. Let G be a finite abelian group. Let n be the number of elements. Then there exist exactly n characters over G. Next, for all $x \in G$, the function $f(y) = I(x = y)$ is a linear combination of the n characters, all coefficients of which are nonzero. Next, all characters have zero sum except for the trivial character, which has sum $n \neq 0$.

Now, we will work through as many concrete cases of this theorem, using concrete direct sums, as we can.