1 Characters

For a finite abelian group $G$, a character $\chi$ of $G$ is a homomorphism from $G$ to $\mathbb{C}^*$, the multiplicative group of the nonzero complex numbers.

We have two ways of writing a complex number $z$. The cartesian way is $z = a + bi$, where $a, b \in \mathbb{R}$ are real numbers. The polar way is $z = re^{i\theta}$, where $r, \theta \in \mathbb{R}$ and $r \geq 0$. Finding the polar representation from the cartesian representation is via $r = |z| = (a^2 + b^2)^{1/2}$, and $\theta$ is the radian measure of the angle formed by the vector $(a, b)$ and the vector $(0, 1)$, so it is $\arctan(b/a)$. The argument $\theta$ is only defined up to a multiple of $2\pi$ in that $e^{i\theta} = e^{i(2\pi + \theta)}$, so if you want you might assume that $0 \leq \theta < 2\pi$. Also note that if $z = 0$, then $r = 0$ and $\theta$ can be taken as anything. However, we will be using the polar form of $z$ for nonzero complex numbers.

Going from the polar form to cartesian form is given by the formula of Euler:

$$re^{i\theta} = r \cos \theta + ir \sin \theta.$$ 

The cartesian form of complex numbers is handy for adding them, while the polar form is handy for multiplying them. In particular, if

$$z_1 = r_1 e^{i\theta_1}, \quad z_2 = r_2 e^{i\theta_2},$$

then

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}.$$ 

From this, we see that those complex numbers at distance 1 from the origin are closed under multiplication, and in fact, they form a group, known as the circle group. In the full multiplicative group $\mathbb{C}^*$, we have that any element of finite order must lie in the circle group. In fact, the elements of finite order are of the form $e^{2\pi i \theta}$ where $\theta \in \mathbb{Q}$ is rational. If $\theta = h/k$ with $h, k$ coprime integers and $k > 0$, then $e^{2\pi i \theta}$ has order $k$.

Another neat feature of the circle group is that if $\zeta$ is a member, its inverse $\zeta^{-1}$ is given by $\overline{\zeta}$, the complex conjugate. Indeed, $\zeta \overline{\zeta} = |\zeta|^2 = 1$.

A character $\chi$ of an abelian group $G$ of order $n$ is not only a homomorphism of $G$ into $\mathbb{C}^*$, but the subgroup $\langle e^{2\pi i/n} \rangle$, the cyclic subgroup of the circle group of order $n$. Even more, if the exponent of $G$ is $h$, then $\chi$ sends $G$ into $\langle e^{2\pi i/h} \rangle$.

Some examples are in order. We are primarily concerned with the groups $(\mathbb{Z}/n\mathbb{Z})^*$, so let’s find all the characters for small values of $n$.

$n = 1$: Then $(\mathbb{Z}/1\mathbb{Z})^*$ has order 1 and the only character is the function that takes this single element to 1.

$n = 2$: Again $(\mathbb{Z}/2\mathbb{Z})^*$ has order 1 and the only character is $\chi(1) = 1.$
n = 3: Now we have 2 characters. The group is \{1, 2\} under multiplication modulo 3. One character takes these elements to 1. The second character takes 1 to 1 and it takes 2 to \(-1\).

One thing we are already seeing in the example of \(n = 3\) is that since the group is cyclic, generated by 2, to specify a character \(\chi\) it is sufficient to specify \(\chi\) at the generator 2, and it must be taken to a complex number \(e^{2\pi i h/k}\) where \(k\) is the order of the generator.

\(n = 4\): Again, it is a group of order 2, namely \{1, 3\}. We can send 3 to 1 or we can send 3 to \(e^{2\pi i/2} = -1\).

So far, all of the characters we have looked at are real, in that the values are \(\pm 1\), the real subgroup of the circle group. However, this is because all of the groups we have looked at so far have exponent 1 or 2, in fact order 1 or 2.

\(n = 5\): Now our group is \{1, 2, 3, 4\} under multiplication modulo 5. It is cyclic, generated by 2 (or by 3 if you prefer). A character must send 2 to a complex number \(e^{2\pi i h/4}\) where \(h\) is an integer. We have 4 choices for \(h\), namely 0, 1, 2, 3, corresponding respectively to sending 2 to 1, \(i\), \(-1\), \(-i\). Let’s look at the character \(\chi\) that sends 2 to \(i\):

\[\chi(1) = 1, \ \chi(2) = i, \ \chi(3) = \chi(2^3) = \chi(2)^3 = i^3 = -i, \ \chi(4) = \chi(2^2) = i^2 = -1.\]

Here we have used that \(\chi\) is a homomorphism so that \(\chi(ab) = \chi(a)\chi(b)\).

\(n = 6\): This is just like \(n = 3\), except the group is \{1, 5\} and we can send 5 to 1 or \(-1\).

\(n = 7\): This is \{1, 2, 3, 4, 5, 6\} which is cyclic with generator 3, so we can send 3 to one of the 6th roots of 1: \(e^{2\pi i h/6}\) for \(h = 0, 1, 2, 3, 4, 5\).

\(n = 8\): This is \{1, 3, 5, 7\}, but the group is not cyclic. We have \{1, 3\} a cyclic subgroup of order 2 and we have that the group is generated by 3 and 5, where 5 also has order 2. So we have 4 characters determined by the 4 choices \(\chi(3) = \pm 1\) and \(\chi(5) = \pm 1\).

\(n = 9\): This is the cyclic group \{1, 2, 4, 5, 7, 8\} and is generated by 2. We can send 2 to one of the 6th roots of 1 in \(\mathbb{C}\).

So far, we have exactly the same number of characters as there are elements in the group. Does this always happen?

There is a further observation to make. The characters of a finite abelian group \(G\) themselves form a group, call it \(\hat{G}\). Indeed, the pointwise product of two characters is again a character. The character which sends every element to 1 acts as the identity under pointwise multiplication. And if \(\chi\) is a character, then \(\chi^{-1}\) is a character. This is just the reciprocal of \(\chi\), and as we have seen, it is also the complex conjugate \(\bar{\chi}\) of \(\chi\).

**Proposition 1.** Every finite abelian group \(G\) is isomorphic to its character group \(\hat{G}\).

**Proof.** First suppose that \(G = \langle g \rangle\) is cyclic of order \(n\). Then a character \(\chi\) of \(G\) must send \(g\) to one of the \(n\)th roots of 1 in \(\mathbb{C}\) and this determines the other values of the character. Further each of the \(n\) choices of \(n\)th roots of 1 may be chosen to define a character. And the product of two characters corresponds to the product of the two special \(n\)th roots of 1 which define the character. So, it is clear that \(\hat{G}\) is isomorphic to the group of \(n\)th roots of 1 in \(\mathbb{C}^\ast\), and this group is cyclic of order \(n\). Thus \(G\) is isomorphic to \(\hat{G}\) in this case.
Since every finite abelian group \( G \) is the product of cyclic groups, it suffices to show that if \( G_1, G_2 \) are two finite abelian groups, then \( \hat{G}_1 \times \hat{G}_2 \) is isomorphic to \( \hat{G}_1 \times \hat{G}_2 \). Well, a character of \( G_1 \times G_2 \) can be built in a canonical way from a character \( \psi_1 \) of \( G_1 \) and a character \( \psi_2 \) of \( G_2 \). Namely, \( \psi_1 \) can be identified with the character of \( G_1 \times G_2 \) which is \( \psi_1 \) on \( G_1 \) and the identity (always 1) on \( G_2 \), and \( \psi_2 \) is identified with the character of \( G_1 \times G_2 \) which is the identity on \( G_1 \) and \( \psi_2 \) on \( G_2 \). Thus, it makes sense to consider the character \( \psi_1 \psi_2 \) on \( G_1 \times G_2 \). Further it is easy to check that this procedure gives an isomorphism from \( \hat{G}_1 \times \hat{G}_2 \) onto \( \hat{G}_1 \times \hat{G}_2 \). \( \square \)

2 The orthogonality relations

Let \( G \) be an abelian group of order \( m \) with character group \( \hat{G} \). We will write \( G \) multiplicatively, with the identity element denoted as 1. We will denote the identity character of \( \hat{G} \) as \( \chi_1 \).

We have the following two theorems known as the orthogonality relations for characters. Note that they are much akin to the concept of an orthonormal basis in linear algebra.

Theorem 1. For each \( \chi \in \hat{G} \) we have

\[
\sum_{a \in G} \chi(a) = \begin{cases} 
m, & \chi = \chi_1, \\
0, & \chi \neq \chi_1. 
\end{cases}
\]

Theorem 2. For each \( a \in G \) we have

\[
\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} 
m, & a = 1, \\
0, & a \neq 1. 
\end{cases}
\]

We begin with the proof of Theorem 1. If \( \chi = \chi_1 \), then each \( \chi(a) \) in the sum is 1, so the sum is \( m \). Now suppose that \( \chi \neq \chi_1 \). Since \( \chi \) is not identically 1 on \( G \), there is some \( b \in G \) with \( \chi(b) \neq 1 \). Let

\[
S = \sum_{a \in G} \chi(a),
\]

so that we are trying to show that \( S = 0 \). But note that

\[
\chi(b)S = \sum_{a \in G} \chi(b)\chi(a) = \sum_{a \in G} \chi(ba).
\]

But as \( a \) runs through all of \( G \), so do the products \( ba \), just in a different order. Thus, \( \chi(b)S = S \). Since \( \chi(b) \neq 1 \) this forces \( S = 0 \).

Theorem 2 can be viewed as really saying nothing new that Theorem 1 doesn’t already say. The idea is to consider \( G \) as \( \hat{\hat{G}} \). And the way to do this is to look at the complex number \( \chi(a) \) not with \( a \) as the independent variable, but \( \chi \) as the independent variable. For \( a \in G \), let \( f_a \) be the function that sends \( \chi \in \hat{G} \) to the complex number \( \chi(a) \). This is a homomorphism from
\( \hat{G} \) to \( \mathbb{C}^* \) so is a character of \( \hat{G} \). Moreover, the product of two of these, say \( f_a f_b \) is the same function as \( f_{ab} \). This gives us then the view of \( G \) embedded isomorphically as a subgroup of \( \hat{G} \). But both groups are isomorphic to each other (and finite) so this embedding must be an isomorphism onto \( \hat{G} \). Theorem 2 is then Theorem 1 applied to the character group \( \hat{G} \).

3 Dirichlet characters

Now that we understand characters, we try to unite the idea of a character \( \chi \) of the unit group \( (\mathbb{Z}/k\mathbb{Z})^* \) with the idea of an arithmetic function. For \( m \in \mathbb{Z} \), if \( \text{gcd}(m, k) = 1 \), we can view \( m \) as a member of \( (\mathbb{Z}/k\mathbb{Z})^* \) and thus map \( m \) to \( \chi(m) \). This is fine if \( \text{gcd}(m, k) = 1 \), but what do we do if \( m \) is not coprime to \( k \)? The answer: send it to 0. Note that 0 \( \notin \mathbb{C}^* \) so this will clearly brand the new elements when we try to expand the domain of \( \chi \).

This is not so mysterious. Let’s take the nontrivial character \( \chi \) of \( (\mathbb{Z}/3\mathbb{Z})^* \), so that \( \chi(1) = 1 \) and \( \chi(2) = -1 \). Using the exact same notation \( \chi \), we have now a function on \( \mathbb{Z} \) given by

\[
\chi(a) = \begin{cases} 
1, & a \equiv 1 \pmod{3}, \\
-1, & a \equiv 2 \pmod{3}, \\
0, & a \equiv 0 \pmod{3}.
\end{cases}
\]

This \( \chi \) is an arithmetic function with the following properties:

- It is defined on all of \( \mathbb{Z} \).
- It is completely multiplicative.
- It is periodic with period 3.
- Its values are \( \pm 1, 0 \) and it is 0 precisely when the argument is not coprime to 3.

In general, if \( \chi \in (\mathbb{Z}/k\mathbb{Z})^* \), we can view \( \chi \) as a completely multiplicative function on \( \mathbb{Z} \) that is periodic modulo \( k \) and with values being \( \varphi(k) \)th roots of 1 in \( \mathbb{C} \) or 0, where it has the value 0 precisely when the argument is not coprime with \( k \). These functions on \( \mathbb{Z} \) are called Dirichlet characters. Each function on \( \mathbb{Z} \) with these properties arises from a character of \( (\mathbb{Z}/k\mathbb{Z})^* \).

Note that it is possible for two such characters to come from different moduli yet be the same function on \( \mathbb{Z} \). For example, the character above with modulus 3 can also be viewed as a character in \( (\mathbb{Z}/9\mathbb{Z})^* \) and it gives exactly the same function on \( \mathbb{Z} \). We will look into this phenomenon and a related phenomenon a bit later in the course: some characters are primitive and some are induced by a character with a smaller modulus.

If the Dirichlet character \( \chi \) arises from a character of \( (\mathbb{Z}/k\mathbb{Z})^* \), we say that \( \chi \) has modulus \( k \). As we have just noted, the modulus of a Dirichlet character is not necessarily unique.
The orthogonality relations when dealing with \((\mathbb{Z}/k\mathbb{Z})^*\) now read as follows: For \(\chi\) a Dirichlet character with modulus \(k\),

\[
\sum_{a \pmod{k}} \chi(a) = \begin{cases} \varphi(k), & \chi = \chi_1, \\ 0, & \chi \neq \chi_1. \end{cases}
\]

For \(a\) an integer,

\[
\sum_{\chi \pmod{k}} \chi(a) = \begin{cases} \varphi(k), & a \equiv 1 \pmod{k}, \\ 0, & a \not\equiv 1 \pmod{k}. \end{cases}
\]

The notation under the summation signs needs a word of explanation. In the first sum, \(a\) is the dummy variable and is running over a complete residue system modulo \(k\). It also could be written as \(\sum_{a=1}^{k}\), since here too \(a\) is running over a complete residue system. In the second sum, \(\chi\) is the dummy variable and it is running over the \(\varphi(k)\) Dirichlet characters corresponding to the \(\varphi(k)\) characters in \((\mathbb{Z}/k\mathbb{Z})^*\).

These orthogonality relations are important to us because we can use them to pick out a particular residue class modulo \(k\). For example, note that

\[
\frac{1}{\varphi(k)} \sum_{\chi \pmod{k}} \chi(a)
\]

is a function of the integer variable \(a\) that sends \(a\) to 1 if \(a \equiv 1 \pmod{k}\) and to 0 otherwise. It is the characteristic function of the numbers that are 1 mod \(k\).

We can also pick out other coprime residue classes mod \(k\).

**Proposition 2.** Let \(k\) be a positive integer and let \(b\) be an integer coprime to \(k\). The function that sends an integer \(a\) to

\[
\frac{1}{\varphi(k)} \sum_{\chi \pmod{k}} \overline{\chi(b)} \chi(a)
\]

is the characteristic function of the set of integers \(a\) for which \(a \equiv b \pmod{k}\).

**Proof.** Recall that the complex conjugate \(\overline{\chi(b)}\) is the same as the reciprocal \(\chi(b)^{-1}\). Let \(\bar{b}\) be the multiplicative inverse of \(b \in (\mathbb{Z}/k\mathbb{Z})^*\). Also \(\overline{\chi(b)} = \chi(b)^{-1}\), so that the summand in the proposition is \(\chi(\bar{b})\chi(a) = \chi(\bar{ba})\). Thus, the sum is 1 when \(\bar{ba} \equiv 1 \pmod{k}\) and is 0 otherwise, which translates to being 1 when \(b \equiv a \pmod{k}\) and 0 otherwise.

This result is sort of the main point about Dirichlet characters, at least for our development here.
4 Dirichlet $L$-functions

We have seen that if $f$ is an arithmetic function, we may consider the function

$$L(f, s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$ 

When we do this with $f$ being a Dirichlet character $\chi$, we have the Dirichlet $L$-function $L(s, \chi)$.

We have been taking $s$ as a real variable, and we will continue to do so at this point. But notice that $\chi(n)$ takes complex values, so the function $L(s, \chi)$ maps the real variable $s$ into the complex numbers. By taking the real part of $L(s, \chi)$ and the complex part, we can view it as two separate series, but it is indeed very helpful to view it holistically as one series.

The first issue for us is for which $s$ does $L(s, \chi)$ converge? The answer to this depends very strongly on $\chi$. If $\chi$ is the Dirichlet character modulo $k$ which sends numbers coprime to $k$ to 1, then the series $L(s, \chi)$ converges when $s > 1$, and it diverges at $s = 1$. If $\chi$ is any other Dirichlet character modulo $k$, then the series $L(s, \chi)$ converges when $s > 0$ and it diverges when $s = 0$.

We essentially saw these facts for homework, but let’s quickly review. Suppose that $\chi$ is the character mod $k$ corresponding to the identity in the character group, so that $\chi = \chi_1$, the character which takes numbers coprime to $k$ to 1 and other numbers to 0. Note that

$$\sum_{n=1}^{\infty} \frac{\chi_1(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{n} \geq \sum_{m=0}^{\infty} \frac{1}{mk+1},$$

which diverges to $+\infty$. Thus $L(1, \chi_1)$ diverges, and in comparison with $\zeta(s)$, it converges for $s > 1$. Note that we have an Euler product for $L(s, \chi_1)$ when $s > 1$, it is

$$L(s, \chi_1) = \zeta(s) \prod_{p|k} (1 - p^{-s}) = \prod_{p|k} (1 - p^{-s})^{-1},$$

that is, it differs from $\zeta(s)$ by only finitely many Euler factors.

For $\chi$ a character modulo $k$ with $\chi \neq \chi_1$ the situation is more interesting. We have, by the orthogonality relations, that the sum over any $k$ consecutive integers of $\chi(n)$ is 0. So by blocking off the interval $[1, x]$ into disjoint blocks of $k$ consecutive integers, with perhaps a few stragglers left over, we see that

$$\sum_{n \leq x} \chi(n) = \sum_{k|x/k<n \leq x} \chi(n),$$

and so

$$\left| \sum_{n \leq x} \chi(n) \right| < \varphi(k).$$
That is, $| \sum_{n \leq x} \chi(n) | = O(1)$, so as we learned from homework, the series for $L(s, \chi)$ converges when $s > 0$.

It is clear that the series for $L(0, \chi)$ diverges since the terms do not approach 0 in the limit.

Let’s work out the Euler product expansion for $L(s, \chi)$. We learned that we can do this for $L(s, f)$ if $f$ is multiplicative and the series converges absolutely. This gives

$$L(s, \chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}, \quad s > 1. \quad (1)$$

The region is $s > 1$ since this is where the series converges absolutely. However, the series converges as we have seen for $s > 0$. Let’s see how we can expand the domain of truth for (1). Note that if we restrict to integers $n$ with $P(n) \leq x$, then

$$\sum_{P(n) \leq x} \frac{1}{n^s} \quad (2)$$

converges for $s > 0$. To see this, let $\psi(X, x)$ denote the number of integers $n \leq X$ with $P(n) \leq x$. Since $P(n) \leq x$ implies that $n$ has the prime factorization $p_1^{a_1}p_2^{a_2}\ldots p_m^{a_m}$, where $p_1, p_2, \ldots, p_m$ are all of the primes in $[1, x]$ and exponents $a_j$ satisfy $0 \leq a_j \leq \log X / \log p_j$, we have that

$$\psi(X, x) \leq \prod_{j=1}^m (1 + \log X / \log p_j) \leq (1 + \log X / \log 2)^m = O(x^\epsilon)$$

for any fixed $\epsilon > 0$. Thus, by partial summation we have that $\sum_{P(n) \leq x} 1/n^s$ converges when $s > \epsilon$, which proves our assertion (2). It follows that

$$\sum_{P(n) \leq x} \frac{\chi(n)}{n^s}$$

converges absolutely when $s > 0$ and is equal to

$$\prod_{p \leq x} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

The trick is to now let $x \to \infty$. The sum converges to $L(s, \chi)$. Thus, the products converge to the same thing. We conclude that (1) holds.