Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Seminar in Number Theory: L-Functions

Characters and L-Functions

Duri Janett, Sami Fawaz

October 19, 2021

ETH Zurich,
Department of Mathematics

Chapter 1

Characters

Definition 1. — Let G be a finite group. A *character* on G is a group homomorphism

$$\chi : G \to \mathbb{C}^\times,$$

where $\mathbb{C}^\times$ is the group of units $\mathbb{C} \setminus \{0\}$ under multiplication. The set of characters on G form a group under the operations

$$\chi\chi'(g) \coloneqq \chi(g)\chi'(g),\ \chi^{-1}(g) \coloneqq \chi(g)^{-1}$$

which we denote by $\hat{G}$.

Let $m \in \mathbb{N}_{>0}$. For a group $G = (\mathbb{Z}/m\mathbb{Z})^\times = \{n \pmod m \mid (n, m) = 1\}$ we call a character χ on G a *Dirichlet character of modulus m.* Equivalently we may define a Dirichlet character of modulus m as a function $\chi : \mathbb{Z} \to \mathbb{C}$ with

1. $\forall n : \chi(n) = 0 \Leftrightarrow (n, m) \neq 1$
2. $\forall n,\ n' : \chi(nn') = \chi(n)\chi(n')$
3. $\forall n : \chi(n + m) = \chi(n)$.

We will use these definitions interchangeably and denote functions corresponding to each other by the same symbol.

Example 2. — The character χ_0 corresponding to neutral element of $\hat{G}$, that is $\forall g \in G : \chi(g) = 1$, is called *principal character.* For $G = (\mathbb{Z}/m\mathbb{Z})^\times$ using the alternative definition the *principal character of modulus m* is

$$\chi_0(n) : \begin{cases} 1, & (n, m) = 1 \\ 0, & (n, m) \neq 1. \end{cases}$$

Example 3. — The *Legendre symbol* defined for a prime number p by

$$\left(\frac{n}{p}\right) \coloneqq \begin{cases} 0, \text{ if } p | n \\ 1, \text{ if } p \nmid n,\ n \equiv x^2 \pmod p\text{, for some } x \\ -1, \text{ else} \end{cases}$$

is a Dirichlet character of modulus p.

Theorem 4. — *Let G be a finite abelian Group. Then the group of characters $\hat{G}$ on G is isomorphic to G itself. In particular*

$$\varphi(m) = |\widehat{(\mathbb{Z}/m\mathbb{Z})}^{\times}|,$$

that is Euler's phi function

$$\varphi(m) = |\{n \ (mod\ m) \mid (n,m) = 1\}| = m \prod_{p|m} (1 - \frac{1}{p})$$

yields the number of Dirichlet characters of modulus m.

Proof. A finite abelian Group is a product

$$G \cong Z/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Let $g_1, \ldots, g_k$ be generators of G with orders $n_1, \ldots, n_k$. For any character χ on G we have

$$\chi(g_i)^{n_i} = \chi(g_i^{n_i}) = \chi(e) = 1$$

hence $\xi_i \coloneqq \chi(g_i)$ is an n_i-th root of unity. Moreover χ is completely determined by the roots ξ_i through

$$\chi(g) = \chi(g_1^{r_1} \cdots g_k^{r_k}) = \chi(g_1)^{r_1} \cdots \chi(g_k)^{r_k} = \xi_1^{r_1} \cdots \xi_k^{r_k} \tag{4.1}$$

On the other hand any choice of roots $\xi_1, \ldots, \xi_k$ with $\xi_i^{n_i} = 1$ defines a character on G through (4.1). This yields the desired isomorphism $\hat{G} \cong G$. The second part of the statement follows immediately, since $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^{\times}| = |\widehat{(\mathbb{Z}/m\mathbb{Z})}^{\times}|$. □

Theorem 5. — *Let χ be a Dirichlet character of modulus m. Then*

$$\sum_{n\ (mod\ m)} \chi(n) = \begin{cases} \varphi(n), & if\ \chi = \chi_0 \\ 0, & else \end{cases}$$

holds, where $\sum_{n\ (mod\ m)}$ *is the sum over a representing system of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. The case $\chi = \chi_0$ follows by definition of the Euler φ function. Otherwise let $l \in \mathbb{Z}$ be such that $(l,m) = 1$ and $\chi(l) \neq 1$. It follows:

$$\begin{aligned}(1 - \chi(l)) \sum_{n \pmod m} \chi(n) = \sum_{n \pmod m} \chi(n) - \sum_{n \pmod m} \chi(nl) \\ = \sum_{n \pmod m} \chi(n) - \sum_{n \pmod m} \chi(n) = 0\end{aligned}$$

hence showing $\sum_{n \pmod m} \chi(n) = 0$. □

Theorem 6. — *Let $n \in \mathbb{Z}$. Then*

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m), \text{ if } n \equiv 1 \pmod m \\ 0, \text{ else} \end{cases}$$

holds, where $\sum\limits_{\chi}$ is the sum over all Dirichlet characters of modulus m.

Proof. For $n = 1$ the sum yields:

$$\sum_{\chi} \chi(n) = \sum_{\chi} 1 = |\widehat{(\mathbb{Z}/m\mathbb{Z})^{\times}}| = \varphi(m)$$

by Theorem 4. On the other hand the theorem holds for $(n, m) > 1$ too as $\chi(n)$ vanishes. Let now $n \not\equiv 1 \pmod m$ and $(n, m) = 1$. The quotient group $(\mathbb{Z}/m\mathbb{Z})^{\times}/\langle n \rangle$ containes all characters with $\chi(n) = 1$ and is strictly smaller than $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Hence there is a character χ' with $\chi'(n) \neq 1$. It follows:

$$(1 - \chi'(n)) \sum_{\chi} \chi(n) = \sum_{\chi} \chi(n) - \sum_{\chi} \chi'\chi(n) = \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0$$

with which we conclude $\sum\limits_{\chi} \chi(n) = 0$. □

Definition 7. — Let $m'|m$ be different from m and let χ' be a character of modulus m'. The character resulting from the composition

$$\chi : (\mathbb{Z}/m\mathbb{Z})^{\times} \xrightarrow{(\text{mod } m')} (\mathbb{Z}/m'\mathbb{Z})^{\times} \xrightarrow{\chi'} \mathbb{C}^{\times}$$

is called *imprimitive*. A character that cannot be obtained this way is called *primitive*.

Definition 8. — A *fundamental discriminant* is an integer D with:

$$D \equiv 1 \pmod 4, \text{ and } D \text{ is square-free,}$$

or

$$D = 4m, \text{ with } m \equiv 2 \text{ or } 3 \pmod 4, \text{ and } m \text{ is square-free,}$$

For a fundamental discriminant D we define a function $\chi_D : \mathbb{N} \to \mathbb{Z}$ as follows:

$$\begin{aligned} \chi_D(p) &= \left(\frac{D}{p}\right), \text{ for p odd prime} \\ \chi_D(2) &= \begin{cases} 0, \text{ if } D \equiv 0 \pmod 4 \\ 1, \text{ if } D \equiv 1 \pmod 8 \\ -1, \text{ if } D \equiv 5 \pmod 8 \end{cases} \\ \chi_D(p_1^{r_1} \cdots p_k^{r_k}) &= \chi_D(p_1)^{r_1} \cdots \chi_D(p_k)^{r_k} \end{aligned}$$

Theorem 9. — *Let D be a fundamental discriminant. The map χ_D defines a primitive Dirichlet character of modulus $|D|$ denoted by χ_D as well. In particular*

$$\chi_D(-1) = \mathrm{sign}(D)$$

Moreover every real primitive Dirichlet character is of this type χ_D for some fundamental discriminant D.

Proof. Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of m. By Theorem 4 any Dirichlet character χ factors into a product $\chi_1 \cdots \chi_k$ where χ_i is a Dirichlet character of modulus $p_i^{r_i}$. χ is primitive if and only if every χ_i is primitive. Hence it suffices to consider powers of primes $m = p^r$.

- Case $p =$ odd. From group theory we know $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic. Hence χ is completely determined by its image on a generator x of $(\mathbb{Z}/p^r\mathbb{Z})^\times$ resulting in at most two *real* Dirichlet characters of modulus p^r with $\chi(x) = \pm 1$. The positive value yields the principal character χ_0. The Legendre symbol $(\frac{n}{p})$ defines another Dirichlet character $\chi \neq \chi_0$ of modulus p^r hence $\chi(x) = -1$. It is only primitive for $r = 1$. Therefore $(\frac{n}{p})$ is the only primitive real Dirichlet character of modulus p while there is no such character of modulus p^r for $r > 1$.

For the second case we need the following lemma whose proof is done by induction (exercise).

Lemma 10. — *Let $r \in \mathbb{N}_{>0}$. If $n \equiv 1 \pmod 8$ then $n \equiv x^2 \pmod{2^r}$ for some x.*

- Case $p = 2$. Let χ be a Dirichlet character of modulus 2^r for $r \geq 3$. By the lemma above for any $n \equiv 1 \pmod 8$ it follows

$$\chi(n) = \chi(x^2) = \chi(x)^2 = (\pm 1)^2 = 1.$$

Hence χ can only be primitive for $r \leq 3$. The cases $r = 1, 2, 3$ can be evaluated explicitly: The group $(\mathbb{Z}/2\mathbb{Z})^\times$ is trivial hence χ_0 is the only character. For $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ there are exactly two characters the second of which is primitive

$n \pmod 4$	0	1	2	3
$\chi_0(n)$	0	1	0	1
$\varepsilon_4(n)$	0	1	0	-1

while for $r = 3$ $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ there are 4 characters where the second and third of the following table are primitive.

$n \pmod 8$	0	1	2	3	4	5	6	7
$\chi_0(n)$	0	1	0	1	0	1	0	1
$\varepsilon_8(n)$	0	1	0	1	0	-1	0	-1
$\varepsilon_8'(n)$	0	1	0	-1	0	-1	0	1
$\varepsilon_8''(n)$	0	1	0	-1	0	1	0	-1

We have now categorized all primitive real Dirichlet characters. In summary any such character is a product of Legendre Symbols $(\frac{n}{p})$ for odd primes p and ε_4, $\varepsilon_8(n)$ or $\varepsilon_8'(n)$. Direct calculations show

* $(\frac{n}{p}) = \chi_{\pm p}$ for an odd prime p with the positive value if $p \equiv 1 \pmod 4$ and the negative value if $p \equiv 3 \pmod 4$.
* $\varepsilon_4 = \chi_{-4}$
* $\varepsilon_8(n) = \chi_{-8}$
* $\varepsilon_8'(n) = \chi_8$

For any two coprime fundamental discriminants $D_1,\ D_2$ their product is a fundamental discriminant, hence $\chi_{D_1 D_2} = \chi_{D_1}\chi_{D_2}$. Thus every primitive real Dirichlet character of type χ_D for a fundamental discriminant D. On the other hand all fundamental discriminant are of types $m,\ -4m,\ 8m,\ -8m$ for m squarefree and $m \equiv 1 \pmod 4$ which are exactly the above mentioned characters. Hence for every fundamental discriminant χ_D is a primitive Dirichlet character. It remains to show $\chi_D(-1) = \operatorname{sign}(D)$. Indeed we have

$$\chi_{-4}(-1) = \varepsilon_4(-1) = -1$$

$$\chi_{-8}(-1) = \varepsilon_8(n)(-1) = -1$$

$$\chi_8(-1) = \varepsilon_8'(n)(-1) = 1$$

$$\chi_p(-1) = (\frac{-1}{p}) = 1, \text{ for } p \equiv 1 \pmod 4$$

$$\chi_{-p}(-1) = (\frac{-1}{-p}) = -1, \text{ for } p \equiv 3 \pmod 4$$

which completes the proof. □

Proof of lemma. The cases $r = 1,\ 2,\ 3$ are trivial. We proceed by induction. Assume $r \geq 4$ and $n \equiv x^2 \pmod{2^{r-1}}$. If $n \equiv x^2 \pmod{2^r}$ we are done. Otherwise

$$n \equiv x^2 + 2^{r-1} \pmod{2^r}.$$

Obviously x is odd, since $x^2 \equiv 1 \pmod 8$. Hence we conclude

$$n \equiv x^2 + 2^{r-1} \equiv x^2 + x2^{r-1} + 2^{2r-4} \equiv (x + 2^{r-2})^2 \pmod{2^r},$$

since $2r - 4 \geq r$, hence proving the claim. □

Chapter 2

L-series

We will introduce *Dirichlet L-series* and see an important theorem about them. From said theorem, *Dirichlet's theorem on arithmetic progressions* will follow. This script closely follows the exposition in Chapter 6 of [1].

Definition 1. — Let χ be a Dirichlet character of modulus m. The *Dirichlet L-series* corresponding to χ is given by

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

Remark 2. For $\sigma > 1$, the Dirichlet L-series can be written as an Euler product as follows,

$$\prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}, \tag{2.1}$$

where the product runs over all primes p.

This remark follows by applying Theorem 2.1 from [1] (pp. 11), and from the fact that χ is completely multiplicative.

Example 3. — We have

$$\begin{aligned} L(s,\chi_0) &= \prod_p \frac{1}{1 - \frac{\chi_0(p)}{p^s}} = \prod_{p \nmid m} \left(1 - p^{-s}\right)^{-1} \\ &= \prod_{p|m} \left(1 - p^{-s}\right) \cdot \prod_p \left(1 - p^{-s}\right)^{-1} = \prod_{p|m} (1 - p^{-s}) \zeta(s). \end{aligned}$$

As $L(s,\chi_0)$ differs from the Riemann zeta function $\zeta(s)$ only by a simple multiplicative factor, it follows that $L(s,\chi_0)$ can be meromorphically extended to all of $\mathbb{C}$. It has only one singularity, namely a simple pole at $s = 1$ with residue $\prod_{p|m}(1 - p^{-s})$.

Remark 4. If χ is a Dirichlet character different from χ_0, then the abscissa of convergence of $L(s,\chi)$ is 0.

Proof. For $\chi \neq \chi_0$, we have as $x \to \infty$

$$\begin{aligned}
\left|\sum_{n=1}^{x} \chi(n)\right| &= \left|\sum_{n=1}^{m\cdot\lfloor\frac{x}{m}\rfloor} \chi(n) + \sum_{n=m\cdot\lfloor\frac{x}{m}\rfloor}^{x} \chi(n)\right| \\
&= \left|\left\lfloor\frac{x}{m}\right\rfloor \sum_{n \pmod m} \chi(n) + \sum_{n=m\cdot\lfloor\frac{x}{m}\rfloor}^{x} \chi(n)\right| \qquad (4.1)\\
&= \left|\sum_{n=m\cdot\lfloor\frac{x}{m}\rfloor}^{x} \chi(n)\right| \qquad (4.2)\\
&\leq \left|x - m\cdot\lfloor\frac{x}{m}\rfloor\right| \leq m = O(1). \qquad (4.3)
\end{aligned}$$

We used $\chi(n) = \chi(n+m)$ to get (4.1). Using Theorem 5 from the previous chapter, we get (4.2). The first inequality in (4.3) follows with $|\chi(n)| \leq 1$ and the triangle-inequality.
Applying Theorem 1.2. from [1] (pp. 4) yields

$$\sigma_0 = \limsup_{t\to\infty} \frac{\log|\sum_{n=m}^{\infty} \chi(n)|}{\log t} \leq \limsup_{t\to\infty} \frac{m}{\log t} = 0.$$

□

Theorem 5. — *If χ is a Dirichlet character different from χ_0, then*

$$L(1,\chi) \neq 0.$$

Proof. Consider

$$f(s) = \prod_{\chi} L(s,\chi), \qquad (5.1)$$

where the product runs over all Dirichlet characters of modulus m.
By (2.1), it holds for $\sigma > 1$:

$$\log f(s) = \sum_{\chi}\sum_{p} \log \frac{1}{1-\frac{\chi(p)}{p^s}} =$$

$$\sum_{\chi}\sum_{p}\sum_{r=1}^{\infty} \frac{\chi(p)^r}{rp^{rs}} = \varphi(m) \sum_{p \text{ prime}} \sum_{\substack{r\geq 1,\\ p^r\equiv 1 \pmod m}} \frac{1}{rp^{rs}}.$$

For the last equality, we used Theorem 6 from the Chapter 1. We observe for $s \in \mathbb{R}, s > 1$:

- $\log f(s) \geq 0$,
- $\lim_{s\to 1, s\in\mathbb{R}} f(s) \geq 1$.

By Remark 4, the product (5.1) contains only one factor with a pole at $s = 1$, namely $L(s, \chi_0)$. It follows from Example 3 that this pole is simple.
Consider now the case where $L(1, \chi) = 0$ for more that one Dirichlet character χ different from χ_0. Then $f(s)$ would be holomorphic at $s = 1$, and $f(1) = 0$. This contradicts our second observation. Hence, there can only be at most character $\chi \neq \chi_0$ with $L(1, \chi) = 0$.
Assume that χ is such a character. As $L(1, \chi) = 0 = \overline{L(1, \chi)} = L(1, \overline{\chi})$, χ is a real character. Let

$$\psi(s) = \frac{L(s, \chi)L(s, \chi_0)}{L(2s, \chi_0)}.$$

For $\sigma > \frac{1}{2}$, ψ is holomorphic: Firstly, the pole of $L(s, \chi_0)$ at $s = 1$ is removed by the zero of $L(s, \chi)$, and secondly, $L(2s, \chi) \neq 0$, by Example 3.
For $\sigma > 1$, we have

$$\psi(s) = \prod_p \frac{1 - \chi_0(p)p^{-2s}}{(1 - \chi_0(p)p^{-s})(1 - \chi(p)p^{-s})} =$$

$$\prod_{p \nmid m} \frac{1 - p^{-2s}}{(1 - p^{-s})(1 - \chi(p)p^{-s})} = \tag{5.2}$$

$$\prod_{p \nmid m} \frac{1 + p^{-s}}{1 - \chi(p)p^{-s}} = \tag{5.3}$$

$$\prod_{\chi(p)=1} \frac{1 + p^{-s}}{1 - p^{-s}} = \prod_{\chi(p)=1} \Big(1 + \sum_{k=1}^{\infty} 2p^{-ks}\Big). \tag{5.4}$$

We applied the third binomial formula to the numerator of (5.2) to get (5.3). The LHS of (5.4) follows as χ only takes the values ± 1.
It follows that for $\sigma > 1$,

$$\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

for some coefficients $a_n \geq 0$. The coefficients are non-negative, as on the RHS of (5.4), $2p^k$ is always non-negative.
As ψ is holomorphic for $\sigma > \frac{1}{2}$, it admits a Taylor series expansion on the open disk of radius $\frac{3}{2}$ around 2. That is, for s with $|s - 2| < \frac{3}{2}$,

$$\begin{aligned} \psi(s) &= \sum_{k=0}^{\infty} \frac{(s-2)^k}{k!} \psi^{(k)}(2) \\ &= \sum_{k=0}^{\infty} \frac{(2-s)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n (\log n)^k}{n^2}. \end{aligned} \tag{5.5}$$

As $a_n \geq 0$, the expression (5.5) is monotonically decreasing for $s \in \mathbb{R}$, $\frac{1}{2} < s < 2$. So for s as before, $\psi(s) \geq \psi(2) \geq 1$.

However, we also have

$$\lim_{s\to\frac{1}{2}} \psi(s) = \frac{L(\frac{1}{2},\chi)L(\frac{1}{2},\chi_0)}{\lim_{s\to\frac{1}{2}} L(2s,\chi_0)} = 0,$$

as $L(2s,\chi_0)$ has a pole at $s=\frac{1}{2}$ by Example 3. This contradiction shows that there cannot be such a χ, which concludes the proof of the theorem. □

Corollary 6 (Dirichlet's theorem on arithmetic progressions). — *Let $a, m \in \mathbb{Z}_{>0}$, such that a and m are mutually prime. Then the arithmetic progression $(mk+a)_{k\in\mathbb{Z}_{\geq 0}}$ contains infinitely many primes. Furthermore, we have*

$$\sum_{\substack{p \text{ prime},\\ p\equiv a \pmod m}} \frac{1}{p} = \infty. \tag{6.1}$$

To prove this, we need the following remark, which follows from Theorem 5 of Chapter 1 by choosing some n with $nb \equiv a \pmod m$.

Remark 7. Let $a, b \in \mathbb{Z}$ such that b, m are mutually prime. Then

$$\frac{1}{\varphi(m)} \sum_{\chi} \chi(a)\overline{\chi}(b) = \begin{cases} 1, \text{ if } a \equiv b \pmod m \\ 0, \text{ if } a \not\equiv b \pmod m. \end{cases}$$

We proceed with the proof of Corollary 6.

Proof. It is enough to show (6.1). By Remark 7, it holds for $\sigma > 1$

$$\sum_{p \text{ prime}} \sum_{\substack{r\geq 1,\\ p^r\equiv a \pmod m}} \frac{1}{rp^{rs}} = \sum_{p}\sum_{r\geq 1} \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a)\chi(p^r)\frac{1}{rp^{rs}} \tag{7.1}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \sum_{p}\sum_{r=1}^{\infty} \frac{\chi(p)^r}{rp^{rs}} \tag{7.2}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) \tag{7.3}$$

$$= \frac{1}{\varphi(m)} \left(\log L(s,\chi_0) + \sum_{\chi\neq\chi_0} \overline{\chi}(a) \log L(s,\chi) \right),$$

where $\sum_p$ and $\sum_\chi$ sum over all primes and all Dirichlet characters of modulus m, respectively. We can interchange the order of summation as in (7.2) due to absolute convergence. The third equality (7.3) follows form —. We note that $\log L(s,\chi_0)$ diverges as $s \to 1$. In contrast, $\log L(s,\chi)$ is bounded for $s = 1$ and $\chi \neq \chi_0$ because of Theorem 5. Hence, the above expression diverges for $s = 1$.

Consider

$$\begin{aligned}
\sum_{p \text{ prime}} \sum_{\substack{r>1, \\ p^r \equiv a \pmod m}} \frac{1}{rp^r} &\leq \sum_p \sum_{r>1} \frac{1}{rp^r} \\
&= \sum_p \sum_{r=2}^{\infty} \frac{1}{rp^r} \leq \sum_p \sum_{r=2}^{\infty} \frac{1}{2p^r} \\
&= \sum_p \frac{1}{2p(p-1)} = \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2}.
\end{aligned}$$

We see that the sum with terms $r = 1$ on the LHS of (7.1) must diverge, which yields (6.1). □

Bibliography

[1] D.B. Zagier. *Zetafunktionen und quadratische Körper*. Springer, 1981.