§ Dirichlet L-functions

Def A Dirichlet character mod $n \in \mathbb{N}$ is a group hom.

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

These form a group $\widehat{(\mathbb{Z}/n\mathbb{Z})}^\times$.

Order of χ = smallest $d \geq 1$ s.t. $\chi^d = 1$ — i.e. $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow \{d^{th} \text{ roots of unity}\}$

order 1 = trivial (or principal) character $\mathbb{1}$

order 2 = quadratic character $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \pm 1$

Modulus of χ = smallest $m \mid n$ s.t. $\exists \chi_0 : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ s.t.

$$\chi(a) = \chi_0(a) \qquad \forall a \in (\mathbb{Z}/n\mathbb{Z})^\times \qquad (*)$$

χ primitive if $m = n$.

We extend χ to $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ by $\chi(a) = 0$ for $(a,n) > 1$.

not a hom. but totally multiplicative.

Ex $n = 1, 2$: only trivial character. $\mathbb{1}$

Ex $n = 3$: $\{\mathbb{1}, \chi_3\}$

$$\chi_3(a) = \begin{cases} 1 & a \equiv 1 \bmod 3 \\ -1 & a \equiv 2 \bmod 3 \\ 0 & a \equiv 0 \bmod 3 \end{cases}$$

order 2
modulus 3

Ex $n = 4$: $\{1, \chi_4\}$

$$\chi_4(a) = \begin{cases} 1 & a \equiv 1 \bmod 4 \\ -1 & a \equiv 3 \bmod 4 \\ 0 & a \equiv 0 \bmod 2 \end{cases}$$

order 2
modulus 4.

Ex $n = 5$ $\quad \{\mathbb{1}, \chi_5, \chi_5^2, \chi_5^3 = \chi_5^{-1} = \overline{\chi_5}\}$

$$(\mathbb{Z}/5\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

$\{2, 2^2, 2^3, 2^4 = 1\}$

$$2 \longmapsto i$$

Ex $n=12$ $\quad (\mathbb{Z}/12\mathbb{Z})^\times \cong C_2 \times C_2 \longrightarrow \mathbb{C}^\times$ $\quad$ 4 characters

$\{1,5,7,11\}$

1	5	7	11		
1	1	1	1	$= \mathbb{1}$	modulus 1
1	−1	1	−1	$= \chi_3$	modulus 3
1	1	−1	−1	$= \chi_4$	modulus 4
1	−1	−1	1	$= \chi_{12}$	modulus 12 (primitive)

Def $\quad \chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ $\quad$ primitive

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

<u>L-function of χ</u>

converges for $\operatorname{Re} s > 1 \quad \chi = \mathbb{1}$

$\operatorname{Re} s > 0 \quad \chi \neq \mathbb{1}$

$\left(\sum_N^M a_n \text{ bounded} \right) \; \forall N, M$

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

degree 1

When χ not primitive, $L(\chi, s) := L(\chi_0, s)$ from $(*)$

Thm $\quad L(\chi, s)$ entire for $\chi \neq \mathbb{1}$, $\quad L^*(\chi, s) = \left(\frac{m}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\lambda}{2}\right) L(\chi, s)$

with $\lambda = \begin{cases} 0 & \chi(-1) = 1 \quad (\chi \text{ even}) \\ 1 & \chi(-1) = -1 \quad (\chi \text{ odd}) \end{cases}$ $\quad$ satisfies fun. eq.

$$L^*(\chi, 1-s) = w \cdot L(\overline{\chi}, s) \qquad w = \frac{1}{\sqrt{m}} \sum_{a=0}^{m-1} \chi(a) \zeta_m^a$$

Gauss sum

Pf $\quad$ Poisson summation for $e^{-\pi n (mx+a)^2}$ (χ even), $e^{-\pi n x^2}$ (χ odd)

§ Cyclotomic fields $\mathbb{Q}(\zeta_m)$ $\qquad \zeta_m = e^{\frac{2\pi i}{m}}$

Major goal of alg. N.T. : understand finite extensions of $\mathbb{Q}$, e.g.

Conj (Inverse Galois Problem) Every finite group is a Galois gp over $\mathbb{Q}$.

Abelian extensions $K/\mathbb{Q}$ are understood:

Galois with $\mathrm{Gal}(K/\mathbb{Q})$ abelian

Thm (Kronecker-Weber) $K/\mathbb{Q}$ abelian $\Longleftrightarrow$ $K \subseteq \mathbb{Q}(\zeta_m)$ for some m,
$\zeta_m = e^{\frac{2\pi i}{m}}$

Max. ab ext. $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ $=$ Max. cyclotomic ext. of $\mathbb{Q}$ $:= \mathbb{Q}(\{\zeta_m\}_{m\geq 1})$
$= \mathbb{Q}(\overline{\mathbb{Q}}^{\times}_{tors})$

there is analogue for imag. quad. fields with $\overline{\mathbb{Q}}^{\times} \rightsquigarrow E(\overline{\mathbb{Q}})$ (CM theory)

§ $\mathbb{Q}(\zeta_{q^k})$

Fix a prime power $m = q^k > 2$ $\quad [\,\mathbb{Q}(\zeta_2) = \mathbb{Q}(\pm 1) = \mathbb{Q}\,]$

$K = \mathbb{Q}(\zeta_m) = \mathbb{Q}(\text{roots of } x^m - 1) = \mathbb{Q}(\text{roots of } \Phi_m(x))$

primitive m^{th} roots of 1.

- $\Phi_m(x) = \dfrac{x^{q^k} - 1}{x^{q^{k-1}} - 1}$ $\qquad$ ~~degree~~ $(\varphi(m)) = q^k - q^{k-1} = \varphi(m)$
- $\Phi_m(x+1) = x^{\varphi(m)} + \dots + q$ $\qquad$ Eisenstein $\Rightarrow$ irr. $\Rightarrow$ $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$
- $(q) = (1 - \zeta_m)^{\varphi(m)}$ in $\mathcal{O}_K$ $\Rightarrow$ q totally ramified in $K/\mathbb{Q}$.
- All other primes $p \nmid \Delta_{x^m - 1} = \pm m^m$ unramified in $K/\mathbb{Q}$.

  power of q

- $\mathrm{Gal}(\mathbb{Q}(\zeta_{q^k})/\mathbb{Q}) = (\mathbb{Z}/q^k\mathbb{Z})^{\times} \overset{\varprojlim}{\Longrightarrow} \mathrm{Gal}(\bigcup_k \mathbb{Q}(\zeta_{q^k})/\mathbb{Q}) = \mathbb{Z}_q^{\times}$

  $(\zeta_m \mapsto \zeta_m^i) \longleftarrow\!\!\shortmid\ i$

§ $\mathbb{Q}(\zeta_m)$ for general $m = q_1^{k_1} \cdots q_j^{k_j}$

$K = \mathbb{Q}(\zeta_m)$ = compositum of $\underbrace{\mathbb{Q}(\zeta_{q_1^{k_1}}), \ldots,}_{q_j \text{ unramified} \Rightarrow \text{disjoint}} \underbrace{\mathbb{Q}(\zeta_{q_j^{k_j}})}_{q_j \text{ tot. ram.}}$

has degree $\prod_j \varphi(q_j^{k_j}) = \varphi(m)$

- $p \nmid m \Rightarrow p$ <u>unramified</u> in $K/\mathbb{Q}$

  residue degree $f_p = [\mathbb{F}_p(\zeta_m) : \mathbb{F}_p]$ = smallest r s.t. $p^r \equiv 1 \bmod m$

  = order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$

- $p \mid m$, $m = p^k m_0 \Rightarrow p$ <u>ramified</u> in $K/\mathbb{Q}$ $\quad (k \geq 1,\ p \nmid m_0)$

  ram. degree $e_p = \varphi(p^k)$.

  res degree f_p = order of p mod m_0.

- $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$

  $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \prod_q \mathbb{Z}_q^\times = \hat{\mathbb{Z}}^\times$ ← group of finite ideles of $\mathbb{Q}$

§ ζ-function of $\mathbb{Q}(\zeta_m)$

<u>Thm</u> $\displaystyle \zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod_{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times} L(\chi, s).$

<u>Proof</u> Compare local factors $F_p(T)$ at every p.

Say $m = p^k m_0$, $k \geq 0$. Let $f :=$ order of p mod m_0
$e := \varphi(p^k)$
$r := \varphi(m)/ef = \varphi(m_0)/f$

$F_p(T)_{LHS} = (1 - T^f)^r$

degree $= \varphi(m_0)$,
roots = f^{th} roots of 1

$$= \prod_{\chi : (\mathbb{Z}/m_0\mathbb{Z})^\times \to \mathbb{C}^\times} (1 - \chi(p) T)$$

$$= F_p(T)_{RHS}.$$

characters whose modulus $\nmid m_0$ ($\Leftrightarrow p \mid$ modulus) have $\chi(p) = 0$.

Cor $L(\chi, 1) \neq 0$ for $\chi \neq 1$

Proof $\zeta_{\mathbb{Q}(\zeta_m)}(s) = \zeta(s) \cdot \prod_{\chi \neq 1} L(\chi, s)$

at $s=1$: simple pole simple pole no poles at $s=1$ (converges for $\mathrm{Re}\, s > 0$) $\Rightarrow$ all $\neq 0$.

Cor Dirichlet's Thm on Primes in Arith. Progressions

$$\left[\sum_{p \equiv a \bmod m} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi(a)} \log L(\chi, s) + \text{analytic at } s=1 \Rightarrow \text{diverges} \right]$$

diverges for $s = 1$, analytic otherwise

In general, $K/\mathbb{Q}$ abelian $\overset{\text{rep. theory, later.}}{\Longrightarrow}$ $\zeta_K(s) = \prod$ L-fncs of characters.

<u>Ex</u> $m = 12$

$\mathbb{Q}(\zeta_m) = \mathbb{Q}(i, \sqrt{3})$ biquadratic

$\widehat{(\mathbb{Z}/12\mathbb{Z})^\times} = \{ \mathbb{1}, \chi_3, \chi_4, \chi_{12} \}$

	$F_2(T)$	$F_3(T)$	$F_5(T)$	$\cdots$	$F_{13}(T)$	$\cdots$
$L(\mathbb{1}, s) = \zeta(s)$	$1-T$	$1-T$	$1-T$		$1-T$	
$L(\chi_3, s)$	$1+T$	1	$1+T$		$1-T$	
$\times$ $L(\chi_4, s)$	1	$1+T$	$1-T$		$1-T$	
$L(\chi_{12}, s)$	1	1	$1+T$		$1-T$	
$\zeta_{\mathbb{Q}(\zeta_{12})}(s)$	$1-T^2$	$1-T^2$	$(1-T^2)^2$	$\cdots$	$(1-T)^4$	$\cdots$
	$m_0 = 3$	$m_0 = 4$	f = order of 5 mod 12 = 2		f = order of 13 mod 12 = 1	

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(i, \sqrt{3}) \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) \arrow[drr, dash] & & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & & \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

$$\zeta_{\mathbb{Q}(\zeta_{12})} = \zeta \cdot L(\chi_3) \cdot L(\chi_4) \cdot L(\chi_{12})$$
$$\zeta_{\mathbb{Q}(i)} = \zeta \cdot L(\chi_4)$$
$$\zeta_{\mathbb{Q}(\sqrt{-3})} = \zeta \cdot L(\chi_3)$$
$$\zeta_{\mathbb{Q}(\sqrt{3})} = \zeta \cdot L(\chi_{12})$$
$$L = \left(\tfrac{3}{\cdot}\right)$$

<u>Generalisations</u>

$\mathbb{Q} \rightsquigarrow$ number field F

$m \rightsquigarrow \mathfrak{m} \subseteq \mathcal{O}_F$ ideal, $\neq 0$ "modulus".

$\chi : \left\{ \begin{array}{c} \text{fractional ideals} \\ \text{of } F \\ \text{prime to } \mathfrak{m} \end{array} \right\} \longrightarrow \mathbb{C}^\times$ finite order

s.t. $\chi(I) = 1$ for $I = (\alpha)$, $\alpha \equiv 1 \bmod \mathfrak{m}$.

$$\rightsquigarrow \quad L(\chi, s) = \sum_{\substack{I \subseteq \mathcal{O}_F \\ \text{coprime to } \mathfrak{m}}} \frac{\chi(I)}{N I^s} = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}}$$

<u>Ex</u> $L(\mathbb{1}, s) = \zeta_F(s)$

Hecke : analytic cont. & fun. eq.

Further generalisation: Hecke characters or Grössencharacters

Instead of $\chi((\alpha)) = 1$ for $\alpha \equiv 1 \mod \mathfrak{m}$,

$\alpha \longmapsto \chi(\alpha)$

must agree with "infinity type"

$$F^\times \hookrightarrow (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \xrightarrow{\text{some cont. hom. } \varphi} \mathbb{C}^\times$$

Possible cont. homs

$$\mathbb{R}^\times \longrightarrow \mathbb{C}^\times \qquad x \longmapsto \operatorname{sgn}(x)^u |x|^{v+iw} \qquad u \in \{0,1\},\ v,w \in \mathbb{R}$$

$$\mathbb{C}^\times \longrightarrow \mathbb{C}^\times \qquad x \longmapsto \left(\frac{x}{|x|}\right)^u |x|^{v+iw} \qquad u \in \mathbb{Z},\ v,w \in \mathbb{R}.$$

Ex $F = \mathbb{Q}$, $\mathfrak{m} = 1$, $\varphi : \mathbb{R}^\times \xrightarrow{x \mapsto |x|} \mathbb{C}^\times$

$$\chi(a) = a \qquad a \in \mathbb{Q}^\times \qquad \text{"cyclotomic character"}$$

$$L(\chi, s) = \prod_p \frac{1}{1 - p \cdot p^{-s}} = \zeta(s-1)$$

← generally $s \mapsto s-(v+iw)$ is just a shift

Modern formulation:

Hecke characters of F = cont. gp. homs $\mathbb{A}_F^\times \longrightarrow \mathbb{C}^\times$, trivial on $F^\times$

Tate's Thesis:

Alt. proof of anal. cont & fun. eq. for Hecke characters using Fourier analysis on adeles.