Extra lecture Mon Nov 14
1–3pm

Last time:

$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ Dirichlet character

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

$K = \mathbb{Q}(\zeta_m)$ m^{th} cyclotomic field

$\rightsquigarrow \zeta_K(s) = \prod_{\chi} L(\chi, s)$

Generalisation

Hecke: $\exists$ number field F in place of $\mathbb{Q}$,

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

$$L(\chi, s) = \sum_{\substack{I \subseteq \mathcal{O}_F \\ \text{ideal} \neq 0}} \chi(I) NI^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}}$$

with $\chi : I_{\mathfrak{m}} = \left\{ \begin{array}{l} \text{fractional ideals} \\ \text{of } F \text{ prime to } \mathfrak{m} \end{array} \right\} \xrightarrow[\text{finite order}]{} \mathbb{C}^\times$

[other ideals $\longmapsto 0$].

s.t. $\chi(I) = 1$ on $P_{\mathfrak{m}} = \left\{ \begin{array}{l} \text{principal ideals } (\alpha) \\ \alpha \equiv 1 \bmod \mathfrak{m} \end{array} \right\}$.

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

Hecke $\Rightarrow$ analytic cont. and func. eq. for these L-functions.

Slight generalisation: <u>Hecke characters</u> and <u>Grössencharakters</u>.

Allow $\chi|_{P_m} : \alpha \longmapsto \mathbb{C}^\times$ instead of $\mathbb{1}$

to agree with

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

φ = "infinity type"

At real places possibilities for φ are

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

$\mathbb{C}^\times \to \mathbb{C}^\times \qquad x \mapsto \left(\frac{x}{|x|}\right)^u |x|^{v+iw} \qquad u \in \mathbb{Z}$

so these are just shifts:

<u>Ex</u> $$\zeta(s-1) = \prod_p \frac{1}{1-p\cdot p^{-s}} = L(\chi, s)$$

with $\chi(p) = p$ "cyclotomic character"

Hecke character with infinity type

$$\mathbb{R}^\times \xrightarrow{z \to |z|} \mathbb{C}^\times$$

take generator $\pm n$ of an ideal (n) and map it to n

Modern formulation:

Hecke characters on F = cont. gp. homs

$\mathbb{A}_F^\times \longrightarrow \mathbb{C}^\times$ with $F^\times$ in the kernel.

Tate's thesis : alternative proof of mer. cont. and func. eq. for Hecke characters using Fourier analysis on adeles.

§5 Decomposition, inertia, Frobenius

K number field, $\mathfrak{p} \subseteq \mathcal{O}_K$ prime

[e.g. $\mathbb{Q}$, (p)].

F/K finite Galois, $G = \mathrm{Gal}(F/K)$,
$|G| = [F:K] = d$.

$$\begin{tikzcd}
\mathbb{F}_{q^f} \arrow[d, dash] & \mathcal{O}_F \arrow[d, dash, "G"] & \supseteq & \mathfrak{P}_1 \arrow[dr, dash] & \mathfrak{P}_2 \arrow[d, dash] & \mathfrak{P}_r \arrow[dl, dash] \\
\mathbb{F}_q & \mathcal{O}_K & \supseteq & & \mathfrak{p} &
\end{tikzcd}$$

residue fields

$\mathfrak{P}_1, \dots, \mathfrak{P}_r$ primes above $\mathfrak{p}$ in F,
ramification e , $efr = d$.

<u>Fact 1</u> G permutes the $\mathfrak{p}_i$ transitively.

<u>Def</u> The <u>decomposition group</u> of the prime $\mathfrak{p}_i$
= the stabiliser of $\mathfrak{p}_i$ in G

$$D_{\mathfrak{p}_i} = \{\sigma \in \mathrm{Gal}(F/K) \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\}$$

It acts on $\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_{q^f}$ index r in G. $\Rightarrow$ get

$$D_{\mathfrak{P}_i} \xrightarrow{\text{mod } \mathfrak{P}_i} \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$$

reduction map on automorphisms

$$\sigma \longmapsto \bar{\sigma}$$

$\cong C_f$ cyclic, generated by $x \to x^q$

<u>Fact 2</u> This is onto.

<u>Def</u> The kernel of $\sigma \mapsto \bar{\sigma}$ is the <u>inertia group</u> of $\mathfrak{P}_i$

$$I_{\mathfrak{P}_i} = \{\sigma \in D_{\mathfrak{P}_i} \mid \bar{\sigma} = id\}$$

elts of G that map $\mathfrak{P}_i \to \mathfrak{P}_i$ and are invisible on $\mathcal{O}_F/\mathfrak{P}_i$

$$I_{\mathfrak{p}_i} \overset{f}{\triangleleft} D_{\mathfrak{p}_i}, \quad |I_{\mathfrak{p}_i}| = e$$

<u>Def</u> A <u>Frobenius element</u> of $\mathfrak{p}_i$

$\mathrm{Frob}_{\mathfrak{p}_i}$ = any elt. of $D_{\mathfrak{p}_i}$ that acts as $x \longmapsto x^q$ on $\mathcal{O}_F/\mathfrak{p}_i$.

So

$$G \overset{r}{>} \underbrace{D_{\mathfrak{p}_i} \overset{f}{\triangleright} I_{\mathfrak{p}_i}}_{\text{cyclic quo. gen. by } \mathrm{Frob}_{\mathfrak{p}}} \overset{e}{\triangleright} \{1\}$$

By Galois theory corresponds to

$$K \xrightarrow[r]{\mathfrak{p} = \tilde{\mathfrak{p}}_i \cdots} K_1 \xrightarrow[f]{\tilde{\mathfrak{p}}_i \text{ totally inert}} K_2 \xrightarrow[e]{\tilde{\mathfrak{p}}_i \text{ totally ramified},\ \tilde{\mathfrak{p}}_i = (\mathfrak{p}_i)^e} F$$

<u>Rmk</u> For $\tau \in G$

$$D_{\tau(\mathfrak{p}_i)} = \{\sigma \in G \mid \sigma(\tau(\mathfrak{p}_i)) = \tau(\mathfrak{p}_i)\}$$
$$= \{\tau\sigma\tau^{-1} \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\} = \tau D_{\mathfrak{p}_i} \tau^{-1}$$

$$\tau\sigma\cancel{\tau^{-1}} \cdot \cancel{\tau}(\mathfrak{p}_i) = \tau\sigma(\mathfrak{p}_i) = \tau(\mathfrak{p}_i)$$

So $D_{\mathfrak{p}_1}, \dots, D_{\mathfrak{p}_r}$ are conjugate in G

(full conj. class of sgps).

Convenient to descend to K:

<u>Def</u> F/K Galois, $\mathfrak{p}$ prime of K

$D_{\mathfrak{p}}$:= decomposition gp of some $\mathfrak{P}_i | \mathfrak{p}$

$I_{\mathfrak{p}}$:= inertia — " — defined up to conjugacy

$\mathrm{Frob}_{\mathfrak{p}}$:= Frob. elt. of $\mathfrak{P}_i$ — " — and modulo inertia

Ex

$$\begin{tikzcd}
 & F = \mathbb{Q}(\sqrt{3}, i) \arrow[dl, dash, "\langle \tau \rangle"'] \arrow[d, dash, "\langle \sigma \rangle"'] \arrow[dr, dash, "\langle \sigma\tau \rangle"] & \\
\mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-3}) \arrow[dl, dash] \\
 & K = \mathbb{Q} &
\end{tikzcd}$$

$G = C_2 \times C_2$ generated by

$\sigma : i \longmapsto -i$
$\sqrt{3} \longmapsto \sqrt{3}$

$\tau : i \longrightarrow i$
$\sqrt{3} \longrightarrow -\sqrt{3}$

Look at (2) in F/K

(2) inert in $\mathbb{Q}(\sqrt{-3}) \Rightarrow 2 | f$

ramifies in $\mathbb{Q}(i) \Rightarrow 2 | e$

f's and e's multiplicative in towers

So $e = f = 2$, $r = 1$. $\Leftarrow$ $(2) = \mathfrak{p}_2^2$ $N\mathfrak{p}_2 = 4$

$$\mathbb{Q} \overset{\text{no splitting}}{=\!=} \mathbb{Q} \xrightarrow{\text{2 inert}} \mathbb{Q}(\sqrt{-3}) \xrightarrow{\text{2 ramifies}} F.$$

$D_2 = D_{\mathfrak{p}_2} = G$, $I_2 = I_{\mathfrak{p}_2} = \langle \sigma\tau \rangle$

$\mathrm{Frob}_2 = \tau$ or σ.

Explicitly : write $\zeta = \zeta_3 = \frac{-1+\sqrt{-3}}{2}$;

$\zeta^2 = -1-\zeta$

$\mathcal{O}_F = \{ a + bi + c\zeta + di\zeta \mid a,b,c,d \in \mathbb{Z} \}$

$\mathfrak{p}_2 = (1+i) = \{ \text{—}\,\,\text{''}\,\,\text{—} \mid a \equiv b,\ c \equiv d \bmod 2 \}$,

$\mathfrak{p}_2^2 = (2)$.

$\mathcal{O}/\mathfrak{p}_2 = \{ \bar{0}, \bar{1}, \bar{\zeta}, \overline{1+\zeta} \} \cong \mathbb{F}_4$.

$$\sigma\tau(\overset{1+i}{\mathfrak{p}_2}) = (\overset{(1+i)\cdot\text{unit}}{1-i}) = \mathfrak{p}_2$$

$\sigma\tau$ fixes $0, 1, \zeta, 1+\zeta \overset{\text{reduce}}{\Rightarrow}$ trivial on $\mathbb{F}_4$ $\Big)$ $\sigma\tau \in I_{\mathfrak{p}_2}$

$\tau(\mathfrak{p}_2) = \mathfrak{p}_2$ as τ fixes $1+i$

τ fixes $0, 1$, $\zeta \leftrightarrow \zeta^2 \equiv 1+\zeta$ mod (2), mod $(\mathfrak{p}_2)$

i.e. $\bar{\tau} : \mathbb{F}_4 \to \mathbb{F}_4$, $x \mapsto x^2$ $\Big)$ $\tau = \mathrm{Frob}_2$

$D_2 = \langle I_2, \mathrm{Frob}_2 \rangle = G.$

§6 Galois representations

Def G finite group. A d-dimensional (complex) representation of G is a gp. hom.

$$\rho : G \longrightarrow GL_d(\mathbb{C}) = GL(V)$$

$$V \cong \mathbb{C}^d$$

$\underline{\text{Ex}}$ $G = C_4 = \langle g \mid g^4 = 1 \rangle$

$$\rho : G \longrightarrow GL_2(\mathbb{C})$$

$$g \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$\llcorner$ rot. by $90°$

i.e. we "represent G as a group of matrices".

When $G = \mathrm{Gal}(F/K)$ we call
finite Galois

$$\rho: \mathrm{Gal}(F/K) \longrightarrow GL_d(\mathbb{C})$$

or

$$\rho: \mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(F/K) \longrightarrow GL_d(\mathbb{C})$$

a <u>Galois representation</u> [with finite image];
when F, K number fields an <u>Artin representation</u> [over K].

<u>Def</u> $\rho: \mathrm{Gal}(F/K) \longrightarrow GL(V)$ Artin rep.

The (Artin) <u>L-function</u>

inertia invariants
$\{v \in V \mid \sigma(v) = v \ \forall \sigma \in I_{\mathfrak{p}}\}$

$$L(\rho, s) = L(V, s) := \prod_{\substack{\mathfrak{p} \text{ prime} \\ \text{of } K}} F_{\mathfrak{p}}(N\mathfrak{p}^{-s})$$

with $F_{\mathfrak{p}}(T) = \det\left(1 - \rho(\mathrm{Frob}_{\mathfrak{p}}^{-1})T \mid V^{I_{\mathfrak{p}}}\right).$

degree d for all $\mathfrak{p}$ unramified in F/K
$\leq d$ for ramified ones

Exc This is well-defined (do it!)

Ex $F = \mathbb{Q}(i)$

$\Big|$ $\Big)$ $G = \langle 1, \sigma \rangle \cong C_2$

$K = \mathbb{Q}$

$p = 2$ $I_2 = G$

$p \equiv 1 \bmod 4$ $I_p = \{1\}$ $D_p = \{1\}$ $\mathrm{Frob}_p = 1$

$p \equiv 3 \bmod 4$ $I_p = \{1\}$ $D_p = G$ $\mathrm{Frob}_p = \sigma$.

- $G \xrightarrow{\rho} \mathbb{C}^\times = GL(V_1)$ $\dim V_1 = 1$

$1, \sigma \longmapsto Id$

$V_1^{I_p} = V_1 \quad \forall p \quad \dim 1$

$\rho(Frob_p) = Id \ \forall p, \quad f_p(T) = det(1 - Id \cdot T)$
$= 1 - T.$

$\rightsquigarrow L(V_1, s) = \zeta(s).$

- $G \xrightarrow{\rho} \mathbb{C}^\times = GL(V_{-1}) \quad \dim V_{-1} = 1$

$1 \longmapsto Id$

$\sigma \longmapsto -Id \qquad V_{-1}^{I_p} = \begin{cases} 0 & p=2 \\ V_{-1} & p>2 \end{cases}$

$$F_p(T) = \begin{cases} 1 & p=2 \\ \det(1 - Id \cdot T) = 1-T & p \equiv 1 \bmod 4 \\ \det(1 + Id \cdot T) = 1+T & p \equiv 3 \bmod 4 \end{cases}$$

$\Rightarrow L(V_{-1}, s) = L(\chi_4, s)$. Dirichlet char. of conductor 4

• $G \longrightarrow GL(V)$ $\dim V = 2$ $V = \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$

look at G acting on $\mathbb{Q}(i) = \mathbb{Q}\cdot 1 + \mathbb{Q}\cdot i$ $\mathbb{Q}$-linearly, and take same matrices / $\mathbb{C}$.

$1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\sigma \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$V \cong V_1 \oplus V_{-1}$, all $V^{I_p} = V_1^{I_p} \oplus V_{-1}^{I_p}$,
$\det(\cdots) = \det(\cdots) \cdot \det(\cdots)$

$$\Rightarrow L(V, s) = L(V_1, s) \cdot L(V_{-1}, s)$$

$$= \zeta(s) L(\chi_4, s) = \zeta_{\mathbb{Q}(i)}(s)$$

In fact any rep. of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}_2) \cong C_2$

is $\cong V_1 \oplus \dots \oplus V_1 \oplus V_{-1} \oplus \dots \oplus V_{-1} \rightsquigarrow$

$\rightsquigarrow \zeta(s)^a L(\chi_4, s)^b$.