Generalizations

Lecture 3

Hecke : / number fields F in place of $\mathbb{Q}$, $\quad \mathfrak{m} \subseteq \mathcal{O}_F$ ideal $\neq 0$ "modulus"

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

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

[other ideals $\longmapsto 0$]

s.t. $\chi(I) \equiv 1$ on $P_{\mathfrak{m}} = \{\text{principal ideals } (\alpha),\ \alpha \equiv 1 \bmod \mathfrak{m}\}$ [$\subseteq I_{\mathfrak{m}}$, finite index]

Ex $L(\mathbb{1}, s) = \zeta_F(s)$.

Hecke $\Rightarrow$ analytic continuation & fun. eq. for these L-fncs.

[slight generalisation: <u>Hecke characters</u> or <u>Grössencharakters.</u>

Allow $\chi|_{P_m} : \alpha \mapsto \mathbb{C}^\times$ instead of 1 to agree with

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

At real places possibilities ~~for~~ φ are

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

$$\mathbb{C}^\times \longrightarrow \mathbb{C}^\times \qquad x \longmapsto \left(\frac{x}{|x|}\right)^n |x|^{v+iw} \qquad (n \in \mathbb{Z})$$

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

Modern formulation:

Hecke characters on F = continuous gp. homs $\mathbb{A}_F^\times \to \mathbb{C}^\times$ with $F^\times$ in the kernel.

Tate's thesis: alternative proof of meromorphic cont. & fun. eq. for Hecke characters using Fourier analysis on adeles.]

<u>§5 Decomposition, inertia, Frobenius</u>

K number field, $\mathfrak{p} \subseteq \mathcal{O}_K$ prime [e.g. $\mathbb{Q}, (p)$]

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

$\mathfrak{p}_1 \dots \mathfrak{p}_r$ primes above $\mathfrak{p}$ in F.

ramification e, residue deg f, $efr = d$.

$$\begin{array}{ccccc} \mathfrak{p}_1 & \mathfrak{p}_2 & \cdots & \mathfrak{p}_r & \subseteq \mathcal{O}_F \\ & & \mathfrak{p} & & \subseteq \mathcal{O}_K \end{array} \qquad \begin{array}{c} \mathcal{O}_F \\ |\,G \\ \mathcal{O}_K \end{array} \qquad \text{residue fields} \quad \begin{array}{c} \mathbb{F}_{q^f} \\ |\,C_f \\ \mathbb{F}_q \end{array}$$

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

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

$$D_{\mathfrak{p}_i} = \{ \sigma \in \operatorname{Gal}(F/K) \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i \}. \qquad \text{index } r \text{ in } G.$$

It acts on $\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_{q^f} \implies$ get

$$D_{\mathfrak{p}_i} \xrightarrow{\text{mod } \mathfrak{p}_i} \operatorname{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) \qquad \text{reduction map on automorphisms}$$

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

<u>Fact 2</u> This is onto. $\qquad \cong C_f$ cyclic, generated by $x \to x^q$

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

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

← elts of G that map $\mathfrak{P}_i \mapsto \mathfrak{P}_i$ and are invisible on $\mathcal{O}_F/\mathfrak{P}_i$;
$I_{\mathfrak{P}_i} \overset{f}{\triangleleft} D_{\mathfrak{P}_i}$, $|I_{\mathfrak{P}_i}| = e$.

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

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

So

$$G \overset{r}{>} D_{\mathfrak{P}_i} \overset{f}{\triangleright} I_{\mathfrak{P}_i} \overset{e}{\triangleright} \{1\}$$

cyclic quo. gen by $\mathrm{Frob}_{\mathfrak{P}_i}$

By Galois theory corresponds to

$$\begin{array}{ccccccc}
K & \xrightarrow[r]{\mathfrak{p}\ \text{split}} & K_1 & \xrightarrow[f]{\tilde{\mathfrak{P}}_i\ \text{totally inert}} & K_2 & \xrightarrow[e]{\tilde{\mathfrak{P}}_i\ \text{totally ramified}} & F \\
\mathfrak{p} & \equiv & \tilde{\tilde{\mathfrak{P}}}_i & - & \tilde{\mathfrak{P}}_i & - & \mathfrak{P}_i \\
\mathbb{F}_q & & \mathbb{F}_q & & \mathbb{F}_{q^f} & & \mathbb{F}_{q^f}
\end{array}$$

; $\tilde{\mathfrak{P}}_i = (\mathfrak{P}_i)^e$

Rmk For $\tau \in G$

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

So $D_{\mathfrak{P}_1}, \dots, D_{\mathfrak{P}_i}$ are conjugate (full conj. class of sgps).

Convenient to descend to K:

Def F/K Galois, $\mathfrak{p}$ prime of K.

$D_\mathfrak{p}$:= dec. gp. of some $\mathfrak{P}_i \mid \mathfrak{p}$. — defined up to conjugacy.

$I_\mathfrak{p}$:= inertia —"— — —"—

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

Ex

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

$G = C_2 \times C_2$ generated by

$\sigma : \begin{matrix} i \mapsto -i \\ \sqrt{3} \mapsto \sqrt{3} \end{matrix}$ $\qquad$ $\tau : \begin{matrix} i \mapsto i \\ \sqrt{3} \mapsto -\sqrt{3} \end{matrix}$

(complex conj.)

Look at (2) in F/K.

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

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

f's and e's multiplicative in Galois towers

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

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

$D_2 = D_{\mathfrak{p}_2} = G$

$I_2 = I_{\mathfrak{p}_2} = \langle \sigma \rangle$

$\mathrm{Frob}_2 = \tau$ or $\sigma\tau$

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

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

$\mathfrak{p}_2 = (1+i) = \{ \quad \text{''} \quad \mid a \equiv b,\ c \equiv d \mod 2 \}$, $\mathfrak{p}_2^2 = (2)$.

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

$\sigma(\mathfrak{p}_2) = (\underset{}{\overset{1+i \,\times\, \text{unit}}{1-i}}) = \mathfrak{p}_2$

σ fixes $0, 1, \zeta, \zeta^2 \Rightarrow$ trivial on $\mathbb{F}_4$

$\Big\}\ \sigma \in I_{\mathfrak{p}_2}$

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

τ fixes $0, 1$, $\zeta \leftrightarrow \zeta^2 \equiv 1+\zeta \mod (2)$

i.e. $\tau : \mathbb{F}_4 \longrightarrow \mathbb{F}_4$
$\qquad x \longmapsto x^2$

$\Big\}\ \tau = \mathrm{Frob}_2$

$\Big\}\ D = \langle I, \mathrm{Frob} \rangle = G.$

§6 Galois representations

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

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

Ex $G = C_4 = \langle g \mid g^4 = 1 \rangle$

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

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

$\quad g \longmapsto \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\text{rot. by } 90^\circ}$

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

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

or

$$\rho: \mathrm{Gal}(\bar{K}|K) \twoheadrightarrow \mathrm{Gal}(F|K) \twoheadrightarrow GL_d(\mathbb{C})$$

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 representation. The <u>L-function</u>

$$L(\rho, s) = L(V, s) = \prod_{\substack{\mathfrak{p} \text{ prime} \\ \text{of } K}} F_{\mathfrak{p}}(N\mathfrak{p}^{-s}) \;; \quad F_{\mathfrak{p}}(T) = \det(1 - \rho(\mathrm{Frob}_{\mathfrak{p}}^{-1}) T \mid V^{I_{\mathfrak{p}}})$$

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

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

<u>Exc</u> This is well-defined [do it!]

<u>Ex</u> $F = \mathbb{Q}(i)$, $K = \mathbb{Q}$ $\Big\}$ $G = \langle 1, \sigma \rangle \cong C_2$

$p = 2$	$I_2 = G$		
$p \equiv 1 \bmod 4$	$I_p = \{1\}$	$D_p = \{1\}$	$\mathrm{Frob}_p = 1$
$p \equiv 3 \bmod 4$	$I_p = \{1\}$	$D_p = G$	$\mathrm{Frob}_p = \sigma$

• $G \longrightarrow \mathbb{C}^\times = GL(V_1)$ $\quad \dim V_1 = 1$

$1, \sigma \longmapsto \mathrm{Id}$

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

$\rho(\mathrm{Frob}_p) = \mathrm{Id} \ \ \forall p \Rightarrow F_p(T) = \det(1 - \mathrm{Id} \cdot T) = 1 - T$

$\Big\}$ $L(V_1, s) = \zeta(s)$.

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

$1 \longmapsto \mathrm{Id}$

$\sigma \longmapsto -\mathrm{Id}$

$$V_{-1}^{I_p} = \begin{cases} 0 & p = 2 \\ V_{-1} & p > 2 \end{cases} \qquad F_p(T) = \begin{cases} 1 & = 1 \quad p = 2 \\ \det(1 - \mathrm{Id} \cdot T) & = 1 - T \quad p \equiv 1 \bmod 4 \\ \det(1 + \mathrm{Id} \cdot T) & = 1 + T \quad p \equiv 3 \bmod 4 \end{cases}$$

$$\Rightarrow L(V_{-1}, s) = L(\chi_4, s)$$

[Dirichlet character of conductor 4].