

Generalizations

Lecture 3

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

"modulus"

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

with $\chi : \begin{cases} \text{fractional ideals} \\ \text{of } F \text{ prime to } \mathfrak{m} \end{cases} \rightarrow \mathbb{C}^\times$ finite order
[other ideals] $\mapsto 0$

s.t. $\chi(\mathfrak{I}) \equiv 1$ on $\mathfrak{P}_{\mathfrak{m}} = \{\text{principal ideals } (\alpha), \alpha \equiv 1 \pmod{\mathfrak{m}}\}$ $\leftarrow [\in \mathbb{I}_{\mathfrak{m}}, \text{finite index}]$

Ex $L(1, s) = \zeta_F(s)$

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

[slight generalisation: Hecke characters or Größencharaktere.

Allow $\chi/p_m : d \mapsto \mathbb{C}^\times$ instead of 1 to agree with

$$F^\times \hookrightarrow (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^{2s} \xrightarrow{\text{some continuous hom. } \psi} \mathbb{C}^\times \quad \leftarrow \psi = \text{"infinity type"}$$

At real places possibilities for ψ are

$$\begin{aligned} \mathbb{R}^\times &\rightarrow \mathbb{C}^\times & x &\mapsto \text{sgn}(x)|x|^{u+iv} & (u \in (0, 1]) \\ \mathbb{C}^\times &\rightarrow \mathbb{C}^\times & x &\mapsto \left(\frac{x}{|x|}\right)^n |x|^{u+iv} & (n \in \mathbb{Z}) \end{aligned}$$

so these are just shifts:

Ex $\zeta(s-1) = \prod_p \frac{1}{1-p^{s-1}} = L(\chi, s)$ with $\chi(p) = p$ "cyclotomic character"

Hecke character with infinity type $\mathbb{R}^\times \xrightarrow{\psi} \mathbb{C}^\times$

Modern formulation:

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

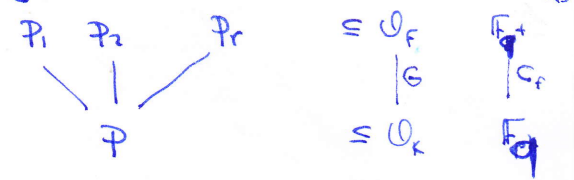
Tate's thesis: alternative proof of meromorphic cont. & fun. eq. for Hecke characters using Fourier analysis on adèles.]

§§ Decomposition, inertia, Frobenius

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

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

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



Fact 1 G permutes the \mathfrak{p}_i transitively.

Def The decomposition group of the prime \mathfrak{p}_i = stabiliser of \mathfrak{p}_i in G

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

It acts on $\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_q^f \Rightarrow$ set

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

Fact 2 This is onto. $\cong C_f$ cyclic, generated by $x \mapsto x^q$

Def The kernel is the inertia group of \mathfrak{p}_i :

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

← elts of G that map $\mathfrak{p}_i \rightarrow \mathfrak{p}_i$
and are inertible on $\mathcal{O}_{\mathfrak{p}_i}$
 $I_{\mathfrak{p}_i} \triangleleft D_{\mathfrak{p}_i}$, $|I_{\mathfrak{p}_i}| = e$.

Def A Frobenius element of \mathfrak{p}_i :

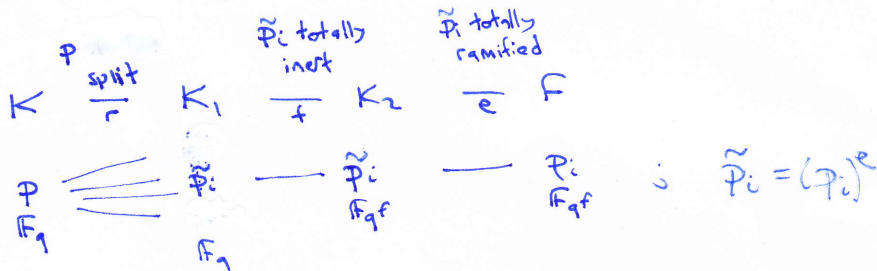
$\text{Frob}_{\mathfrak{p}_i}$ = any elt. of $D_{\mathfrak{p}_i}$ that acts as $x \mapsto x^q$ on $\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{p}_i$

So

$$G \supset D_{\mathfrak{p}_i} \triangleleft I_{\mathfrak{p}_i} \triangleleft \langle 1 \rangle$$

cyclic quo.
gen by $\text{Frob}_{\mathfrak{p}_i}$

By Galois theory corresponds to



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 $\mathfrak{p}_i/\mathfrak{p}$.

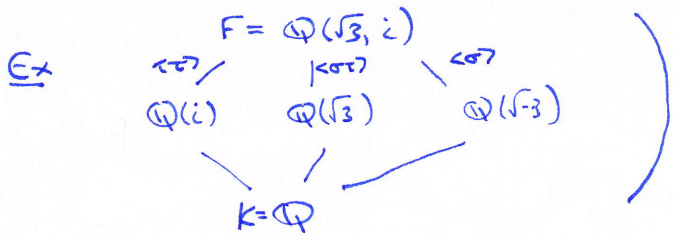
defined up to conjugacy.

$I_{\mathfrak{p}}$:= inertia — " —

— " —

$\text{Frob}_{\mathfrak{p}}$:= Frob. elt. of $D_{\mathfrak{p}}$

— " — and modulo inertia.



$G = C_2 \times C_2$ generated by

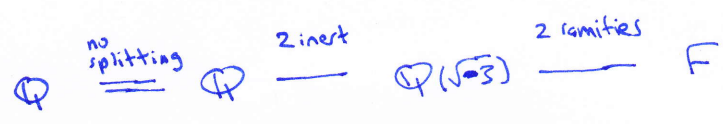
$$\begin{array}{l}
 \sigma: i \mapsto -i \\
 \quad \sqrt{3} \mapsto \sqrt{3} \\
 \tau: i \mapsto i \\
 \quad \sqrt{3} \mapsto -\sqrt{3}
 \end{array}$$

(complex conj.)

Look at (2) in F/K .

(2) inert in $\mathbb{Q}(\sqrt{3}) \Rightarrow 2|f$ \leftarrow f's and e's multiplicative in Galois towers
 ramifies in $\mathbb{Q}(i) \Rightarrow 2|e$

So $e=f=2, r=1 \Leftrightarrow (2) = \mathfrak{P}_2^2 \quad N_{\mathfrak{P}_2} = 4.$



$D_2 = D_{\mathfrak{P}_2} = G$
 $I_2 = I_{\mathfrak{P}_2} = \langle \sigma \rangle$
 $\text{Frob}_2 = \tau$ or $\sigma\tau$

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

$\mathcal{O}_F = \{a + bi + c\zeta + d\zeta^2 \mid a, b, c, d \in \mathbb{Z}\}$
 $\mathfrak{P}_2 = (1+i) = \{ \text{---} \mid a \equiv b, c \equiv d \pmod{2} \}, \quad \mathfrak{P}_2^2 = (2).$

$\mathcal{O}/\mathfrak{P}_2 = \langle \bar{0}, \bar{1}, \bar{\zeta}, 1 + \bar{\zeta} \rangle \cong \mathbb{F}_4$
 $\bar{i} = i \times \text{unit}$

$\sigma(\mathfrak{P}_2) = (1-i) = \mathfrak{P}_2$
 σ fixes $0, 1, \zeta, \zeta^2 \Rightarrow$ trivial on \mathbb{F}_4 $\left. \begin{array}{l} \sigma \in I_{\mathfrak{P}_2} \\ \tau = \text{Frob}_2 \end{array} \right\} D = \langle I, \text{Frob} \rangle = G.$

$\tau(\mathfrak{P}_2) = \mathfrak{P}_2$ as τ fixes $1+i$
 τ fixes $0, 1, \zeta \leftrightarrow \zeta^2 \equiv 1 + \zeta \pmod{2}$

i.e. $\tau: \mathbb{F}_4 \rightarrow \mathbb{F}_4$
 $x \mapsto x^2$

§6 Galois representations

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

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

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

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

$\rho: G \rightarrow GL_d(\mathbb{C})$
 $g \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
 Rot. by 90°

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

$$\rho: \text{Gal}(F/K) \rightarrow \text{GL}_d(\mathbb{C})$$

or $\rho: \text{Gal}(\bar{K}/K) \rightarrow \text{Gal}(F/K) \rightarrow \text{GL}_d(\mathbb{C})$

a Galois representation [with finite image]; when F, K number fields

an Artin representation [over K]

Def $\rho: \text{Gal}(F/K) \rightarrow \text{GL}(V)$ Artin representation. The L-function

$$L(\rho, s) = L(V, s) = \prod_{p \text{ prime of } K} F_p(N_p^{-s}); \quad F_p(T) = \det(1 - \rho(\text{Frob}_p^{-1})T \mid V^{\text{I}_p})$$

\uparrow degree d for all p unramified in F/K , $\leq d$ for ramified
 \uparrow inertia invariants $\{v \in V \mid \sigma(v) = v \ \forall \sigma \in \text{I}_p\}$

Exc This is well-defined [do it!]

$\begin{matrix} F = \mathbb{Q}(i) \\ \\ K = \mathbb{Q} \end{matrix} \right) G = \langle 1, \sigma \rangle \cong C_2$	$p=2$	$I_2 = G$		
	$p \equiv 1 \pmod{4}$	$I_p = \{1\}$	$D_p = \{1\}$	$\text{Frob}_p = 1$
	$p \equiv 3 \pmod{4}$	$I_p = \{1\}$	$D_p = G$	$\text{Frob}_p = \sigma$

• $G \rightarrow \mathbb{C}^\times = \text{GL}(V_1) \quad \dim V_1 = 1$
 $1, \sigma \mapsto \text{Id}$

$V_1^{\text{I}_p} = V_1 \ \forall p \quad \dim 1$
 $\rho(\text{Frob}_p) = \text{Id} \ \forall p \Rightarrow F_p(T) = \det(1 - \text{Id} \cdot T) = 1 - T$ } $L(V_1, s) = \zeta(s)$.

• $G \rightarrow \mathbb{C}^\times = \text{GL}(V_{-1}) \quad \dim V_{-1} = 1$
 $1 \mapsto \text{Id}$
 $\sigma \mapsto -\text{Id}$

$$V_{-1}^{\text{I}_p} = \begin{cases} 0 & p=2 \\ V_{-1} & p>2 \end{cases}$$

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

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

[Dirichlet character of conductor 4].