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

  └ 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 $V^{I_p} = V_1^{I_p} \oplus V_{-1}^{I_p}$,

$\det(\dots) = \det(\dots)\det(\dots)$

$$\Rightarrow \quad L(V, s) = L(V_1, s) L(V_2, s) = \zeta(s) L(\chi_4, s) = \zeta_{\mathbb{Q}(i)}(s).$$

In fact any rep. of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$ is $\cong V_1 \oplus \dots \oplus V_1 \oplus V_{-1} \oplus \dots \oplus V_{-1}$

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

Lecture 4

Why do we define $L(V,s)$ like this, with $F_p(T) = \det((\mathrm{Frob}_p^{-1})T \mid V^{I_p})$?

Write $G_K = \mathrm{Gal}(\bar{K}/K)$ (K number field)

① $L(\mathbb{1}_{G_{\mathbb{Q}}}, s) = \zeta(s)$, $L(\mathbb{1}_{G_K}, s) = \zeta_K(s)$ (by defn.)

└ trivial rep.

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$

$\forall \sigma \longmapsto 1$

② Generally, 1-dim reps of $G_{\mathbb{Q}} \rightsquigarrow$ Dirichlet L-fncs

$G_K \rightsquigarrow$ Hecke L-fncs

③ $[K:\mathbb{Q}] = d \Rightarrow K$ determines a natural d-dim rep. V_K of $G_{\mathbb{Q}}$.

Say $K = \mathbb{Q}[x]/f(x)$ roots $\alpha_1, \dots, \alpha_d$

$$V_K = \mathbb{C}\alpha_1 \oplus \dots \oplus \mathbb{C}\alpha_d \cong \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbb{1}_{G_K}$$

$\circlearrowleft$
$G_{\mathbb{Q}}$

and $\zeta_K(s) = L(V_K, s)$;

decomposition of V_K into irreducibles $\Rightarrow \zeta_K(s) = \prod$ Artin L-functions

④ ①+③ : $L(\mathbb{1}_{G_K}, s) = L(\mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbb{1}_{G_K}, s)$

and same is true for any V in place of $\mathbb{1}$: L-fncs invariant under induction.

⑤ Brauer induction $\Rightarrow$ ①-④ characterise $L(V,s)$ uniquely, (i.e. our defn is the only possible one)

and gives mer. cont. of $L(V,s)$.

⑥ Works in exactly the same way for non-finite order representations (elliptic curves etc.)

§7 Special case : $L(\chi,s)$

Thm There is a bijection ← actually iso. of groups

$$\{\text{Dirichlet characters } \chi\} \longleftrightarrow \{\text{1-dim reps } \rho: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times\}$$
$$\chi \longmapsto \rho_\chi$$

such that

- χ of modulus $m \iff \rho_\chi$ factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and not for smaller $d|m$. (*)
- $L(\chi,s) = L(\rho_\chi,s)$

Pf Take χ of modulus m, and let

$$\rho_\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow[\cong]{\text{can.}} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$$
$$\sigma: \zeta_m \mapsto \zeta_m^a \underset{\text{Artin map}}{\longmapsto} a^{-1} \longmapsto \chi(a)^{-1}$$

Note $p^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$ corresponds to $\zeta_m \to \zeta_m^p$ which is Frob_p.
$p \longleftrightarrow \mathrm{Frob}_p^{-1}$

χ of modulus $m \Rightarrow$ (*)

Kronecker-Weber $\Rightarrow$ every rep. ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that factors through an abelian gp, in particular every 1-dim one factors through some $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$
$\Rightarrow \rho = \rho_\chi$ for some χ.

Compare L-functions:

$p \nmid m$: $L(\chi,s)$ has $F_p(T) = 1 - \chi(p)\,T$ ✓
$L(\rho,s)$ has $F_p(T) = 1 - \underbrace{\rho_\chi(\mathrm{Frob}_p)^{-1}}_{= \overline{\overline{\chi(p)}}}\,T$

$p | m$ $L(\chi,s)$ has $F_p(T) = 1$

$$\begin{tikzcd} \mathbb{Q}(\zeta_m) \arrow[d, dash, "I_p"'] \\ \mathbb{Q}(\zeta_{m_0}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$
$m = m_0 p^k$

χ primitive $\Rightarrow$ ρ_χ does not factor through $\mathrm{Gal}(\mathbb{Q}(\zeta_{m_0})/\mathbb{Q}) \Rightarrow I_p$ acts non-trivially
$\Rightarrow V^{I_p} = 0 \Rightarrow F_p(T) = 1$ ✓. ∎

Rmk Same holds for Hecke characters $/K \xleftrightarrow{1:1}$ 1-dim reps $\mathrm{Gal}(\overline{K}/K) \to \mathbb{C}^\times$

Pf Instead of Kronecker-Weber, full force of global CFT.

§8 Permutation representations & Dedekind ζ

F/K finite Galois, $G = \mathrm{Gal}(F/K)$

$$\begin{tikzcd} \text{Transitive } G\text{-sets}/\cong \arrow[r, leftrightarrow, "1:1"] & \text{Sgps of } G/\text{conjugacy} \arrow[r, leftrightarrow, "1:1"] & \text{fields } K \subseteq M \subseteq F \text{ up to iso.}/K \end{tikzcd}$$

$X \longmapsto \text{Stabiliser}(\text{elt}) \qquad H \longmapsto F^H$

$G/H \longleftarrow\!\shortmid\ H \qquad \mathrm{Gal}(F/M) \longleftarrow\!\shortmid\ M$

$\circlearrowright$

$\{\text{left cosets } g_1H \ldots g_dH$

$g\cdot(g_iH) = gg_i \cdot H$

So $[M:K]=d \rightsquigarrow$ transitive G-set X of size d
[or $\mathrm{Gal}(\bar{K}/K)$-set, does not depend on F]

$$\begin{tikzcd} F \arrow[d, dash] & \\ M \arrow[d, dash, "d"] \arrow[r, squiggly] & X = G/H \\ K & \end{tikzcd}$$

Explicitly, if $M = K(\alpha)$, α root of $f(x) \in K[x]$, irr., deg d

$H = \mathrm{Stab}_G(\alpha)$

$X = X_{M/K} = \{\text{roots of } f\} \circlearrowleft G \quad [\text{or } \circlearrowleft \mathrm{Gal}(\bar{K}/K)]$

$\overset{1:1}{=} \{K\text{-embeddings } M \hookrightarrow \bar{K}\} \quad \circlearrowleft \mathrm{Gal}(\bar{K}/K)$

Ex $G = S_3$

$K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_3, \sqrt[3]{m})$

fields M	sgps H	G-sets X	
$\mathbb{Q}$	S_3	•	G acts trivially
$\mathbb{Q}(\zeta_3)$	C_3	• •	G acts though $S_3/C_3 \cong C_2$
$\mathbb{Q}(\sqrt[3]{m})$	C_2	⁖	G acts as $S_3 \circlearrowleft \{1,2,3\}$
F	$\{1\}$	⠿	reglular action ($G \circlearrowleft G$ by left mult.)

G-set X, $|X| = d$ $\rightsquigarrow$ d-dimensional permutation rep. $\mathbb{C}[X]$
basis = elts of X, G permutes them

$(X = X_1 \amalg X_2 \amalg \cdots \Rightarrow \mathbb{C}[X] \cong \mathbb{C}[X_1] \oplus \mathbb{C}[X_2] \oplus \ldots$

so enough to consider transitive ones).

Aside: Prime decomposition in intermediate extensions

Ex $K = \mathbb{Q}$

$F = \mathbb{Q}(\text{roots of } x^5 - 5x^2 - 3)$

$G = \mathrm{Gal}(F|K) \cong D_5$

$$\begin{tikzcd}
F = \mathbb{Q}(\alpha_1, \dots, \alpha_5) \arrow[d, dash, "H = C_{2A}"'] \arrow[dr, dash, "C_{2B}"'] \arrow[drr, phantom, "\cdots"] \arrow[drrr, dash, "C_{2E}"] & & & \\
M = \mathbb{Q}(\alpha_1) \arrow[d, dash, "5"] & & & \\
K = \mathbb{Q} & & &
\end{tikzcd}
\qquad
\begin{tikzcd}
\underset{\mathbb{F}_{7^2}}{\mathfrak{p}_1} \cdots \underset{\mathbb{F}_{7^2}}{\mathfrak{p}_5} \arrow[d, dash, "?"] \\
p = 7
\end{tikzcd}$$

$$D^{F/M}_{\mathfrak{p}_i} = \underset{C_{2A} \cdots C_{2E}}{D^{F/K}_{\mathfrak{p}_i}} \cap \underset{C_{2A}}{H} = \begin{cases} C_{2A} & i=1 \quad (\Rightarrow f^{F/M}_{\mathfrak{p}_1} = 2) \\ 1 & i=2,3,4,5 \quad (\Rightarrow f^{F/M}_{\mathfrak{p}_i} = 1) \end{cases}$$

f's multiplicative (cf. Problem 3) $\Rightarrow$

$$\begin{tikzcd}
\mathfrak{p}_1 \arrow[d, dash, "f=2"'] & \mathfrak{p}_2 \arrow[d, dash, "f=1"'] & \mathfrak{p}_3 \arrow[dl, dash] & \mathfrak{p}_4 \arrow[d, dash, "f=1"'] & \mathfrak{p}_5 \arrow[dl, dash] \\
\mathfrak{q}_1 \arrow[dr, dash, "f=1"'] & \mathfrak{q}_2 \arrow[d, dash, "f=2"] & & \mathfrak{q}_3 \arrow[dll, dash, "f=2"'] & \\
& (7) & & &
\end{tikzcd}$$

In practice, go the other way: $x^5 - 5x^2 - 3 = (x-1)(x^2+3x-2)(x^2-2x+2) \bmod 7$

$\Rightarrow (7) = \overset{f=1}{\mathfrak{q}_1} \overset{f=2}{\mathfrak{q}_2} \overset{f=2}{\mathfrak{q}_3}$ in $M|K$ $\Rightarrow D^{F/K}_7 = C_2$ [and not C_1, C_5, D_5]

Prop K number field

$$\begin{tikzcd}
F \arrow[d, dash, "H"'] \arrow[dd, bend left, dash, "\text{Galois with group } G"] \\
M \arrow[d, dash] \\
K
\end{tikzcd}
\qquad
\begin{tikzcd}
\overset{D,I}{\mathfrak{p}_1 \cdots \mathfrak{p}_r} \arrow[d, dash] \\
\{\mathfrak{q}_j\} \arrow[d, dash] \\
p
\end{tikzcd}$$

$D_i = D^{F/K}_{\mathfrak{p}_i} < G$

$I_i = I^{F/K}_{\mathfrak{p}_i} \trianglelefteq D_i$

$I = I_1$, $D = D_1$, $\mathrm{Frob}_p \in D$

(i) $D^{F/M}_{\mathfrak{p}_i} = D_i \cap H$, $I^{F/M}_{\mathfrak{p}_i} = I_i \cap H$

(ii) In $M|K$ with primes $\mathfrak{q}_j | p \xleftrightarrow{1:1}$ double cosets $Dg_iH \in D\backslash G/H$ $\xleftrightarrow{1:1}$ orbits of D on G/H.

Each orbit has length e_jf_j and is a union of f_j I-orbits of length e_j, cyclically permuted by Frob_p.

Proof (i) clear

(ii) $H \circlearrowright \{\mathfrak{p}_i\}$ orbits $\overset{1:1}{\leftrightarrow}$ $\mathfrak{q}_j$. stabilisers $= D^{F/M}_{\mathfrak{p}_i}$

$H \circlearrowright G/D$ orbits $\overset{1:1}{\longleftrightarrow}$ double cosets stabilisers $= D_i \cap H$

Same stabilisers $\Rightarrow$ same orbits,

Rest also easy. ∎

Thm $M|K$ finite. Then

$$\zeta_{M|K}(s) = L(\mathbb{C}[X_{M|K}], s)$$

relative ζ-fnc ($= \zeta_M$ if $K = \mathbb{Q}$)

$$\zeta_{M|K}(s) = \prod_{\mathfrak{q} \subseteq \mathcal{O}_M} \frac{1}{1 - N_{M|K}(\mathfrak{q})^{-s}}$$

Artin L-fnc for the rep $\mathbb{C}[X_{M|K}] \circlearrowleft \mathrm{Gal}(\bar{K}/K)$

On the level of local polys: for every prime $\mathfrak{p}$ of K

$$\prod_{\mathfrak{q}|\mathfrak{p}} (1 - T^{f_\mathfrak{q}}) \overset{\text{Thm}}{=} \det(1 - \mathrm{Frob}_\mathfrak{p}^{-1} T \mid \mathbb{C}[X_{M/K}]^{I_\mathfrak{p}})$$

Proof

$$\begin{tikzcd}
F \arrow[d, dash, "H"] \arrow[dd, dash, bend right=60, "G"'] & \overset{D, I, \mathrm{Frob}_\mathfrak{p}}{\circlearrowright} \mathfrak{P}_1, \dots, \mathfrak{P}_r \arrow[d, dash] \\
M \arrow[d, dash] & \mathfrak{q} \arrow[d, dash] \\
K & \mathfrak{p}
\end{tikzcd}$$

Recall: X G-set $\Rightarrow$ $\mathbb{C}[X]^G \cong \mathbb{C}^{\#\text{orbits}}$

(e.g. $x_1 \circlearrowright x_2 \quad x_3 \circlearrowright x_4 \circlearrowright x_5$ $\quad \mathbb{C}[X]^G = \langle x_1 + x_2, x_3 + x_4 + x_5 \rangle$)

As a D-set,

$$G/H = \coprod_{D g_i H} \underbrace{D / D \cap g_i H g_i^{-1}}_{\substack{I \text{ acts with } f_i \text{ orbits} \\ \text{of size } I \cap g_i H g_i^{-1} \\ \text{cyclically permuted by } \mathrm{Frob}_\mathfrak{p}}} \Rightarrow \mathbb{C}[G/H]^I \cong \bigoplus_j \mathbb{C}^{f_j}$$

$\circlearrowleft$ $\mathrm{Frob}_\mathfrak{p}$ acts cyclically (and $\mathrm{Frob}_\mathfrak{p}^{-1}$ as well)

$$\Rightarrow \det(1 - \mathrm{Frob}_\mathfrak{p}^{-1} T \mid \mathbb{C}[G/H]^I) = \prod_j (1 - T^{f_j}). \quad ∎$$