

•  $G \rightarrow GL(V)$      $\dim V = 2$

$V = \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$

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

$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

$V \cong V_1 \oplus V_{-1}$      $\Rightarrow$     all  $V^{\text{IP}} = V_1^{\text{IP}} \oplus V_{-1}^{\text{IP}}$ ,  
 $\det(\dots) = \det(\dots) \det(\dots)$

$\Rightarrow L(V, s) = L(V_1, s) L(V_{-1}, s) = \zeta(s) L(\chi_4, s) = \zeta_{\mathbb{Q}(i)}(s)$ .

In fact any rep. of  $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$  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  $F_p(T) = \det \left( \left( \text{Frob}_p^i \right)_T \mid V^{\text{IP}} \right)$  ?

Write  $G_K = \text{Gal}(K/K)$     ( $K$  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.  
 $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{Z}^{\times}$   
 $\downarrow \sigma \mapsto 1$

② Generally, 1-dim reps of  $G_{\mathbb{Q}} \rightsquigarrow$  Dirichlet L-func.  
 $G_K \rightsquigarrow$  Hecke L-func.

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  $\alpha_1, \dots, \alpha_d$

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

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  $\div$   $L(\mathbb{1}_{G_K}, s) = L(\text{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbb{1}_{G_K}, s)$

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

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

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

§7 Special case:  $L(\chi, s)$

← actually iso. of groups

Thm There is a bijection

$$\left\{ \begin{array}{l} \text{Dirichlet character } \chi \\ \chi \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{1-dim reps } \rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{C}^\times \\ \rho \end{array} \right\}$$

such that

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

Pf Take  $\chi$  of modulus  $m$ , and let

$$\begin{array}{ccccc} \rho_\chi: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\text{can.}} & (\mathbb{Z}/m\mathbb{Z})^\times & \xrightarrow{\chi} & \mathbb{C}^\times \\ \sigma: \zeta_m \mapsto \zeta_m^a & \xrightarrow{\text{Abn. map}} & a^{-1} & \xrightarrow{\chi} & \chi(a)^{-1} \end{array}$$

Note  $\rho \in (\mathbb{Z}/m\mathbb{Z})^\times$  corresponds to  $\zeta_m \mapsto \zeta_m^p$  which is  $\text{Frob}_p$ .  
 $p \leftrightarrow \text{Frob}_p^{-1}$

$\chi$  of modulus  $m \implies (*)$

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

Compare L-functions:

$$\begin{array}{l} \rho_\chi m: L(\chi, s) \text{ has } F_p(T) = 1 - \chi(p)T \\ L(\rho, s) \text{ has } F_p(T) = 1 - \frac{\rho_\chi(\text{Frob}_p)^{-1}}{\chi(p)} T \end{array} \quad \checkmark$$

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

$$\begin{array}{c} \mathbb{Q}(\zeta_m) \\ | \\ \mathbb{Q}(\zeta_m) \\ | \\ \mathbb{Q} \end{array} \quad m = m_0 p^k$$

$\chi$  primitive  $\rho_\chi \implies$  does not factor through  $\text{Gal}(\mathbb{Q}(\zeta_{m_0})/\mathbb{Q}) \implies I_p$  acts non-trivially  $\implies \chi(p) \neq 0 \implies F_p(T) = 1$   $\checkmark$

Rmk Same holds for Hecke characters  $\chi \iff$  1-dim reps  $\text{Gal}(\overline{\mathbb{K}}/\mathbb{K}) \rightarrow \mathbb{C}^\times$

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

# §8 Permutation representations & Dedekind 5

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

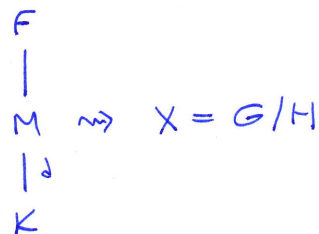
Transitive  $G$ -sets  $\cong$   $\xleftrightarrow{1:1}$  Sgps of  $G$  / conjugacy  $\xleftrightarrow{1:1}$  fields  $K \subseteq M \subseteq F$  up to iso./ $K$

$$X \mapsto \text{Stabiliser}(elt) \quad H \mapsto F^H$$

$$G/H \longleftarrow H \quad \text{Gal}(F/M) \longleftarrow M$$

$\hookrightarrow$   
 left cosets  $g_1H \dots g_dH$   
 $g \cdot (g_iH) = gg_iH$

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



Explicitly, if  $M = K(\alpha)$ ,  $\alpha$  root of  $f(x) \in K[x]$ , irr., deg  $d$   
 $H = \text{Stab}_G(\alpha)$

$$\begin{aligned}
 X = X_{M/K} &= \{\text{roots of } f\} \ni G \quad [\text{or } \ni \text{Gal}(\bar{K}/K)] \\
 &\stackrel{1:1}{=} \{K\text{-embeddings } M \hookrightarrow \bar{K}\} \ni \text{Gal}(\bar{K}/K)
 \end{aligned}$$

Ex  $G = S_3$   
 $K = \mathbb{Q}$ ,  $F = \mathbb{Q}(\zeta_3, \sqrt[3]{m})$

fields $M$	sgps $H$	$G$ -sets $X$
$\mathbb{Q}$	$S_3$	$\bullet$ $G$ acts trivially
$\mathbb{Q}(\zeta_3)$	$C_3$	$\bullet \bullet$ $G$ acts through $S_3/C_3 \cong C_2$
$\mathbb{Q}(\sqrt[3]{m})$	$C_2$	$\bullet \bullet$ $G$ acts as $S_3 \ni \{1, 2, 3\}$
$F$	$\{1\}$	$\bullet \bullet \bullet$ regular action ( $G \ni G$ by left mult.)

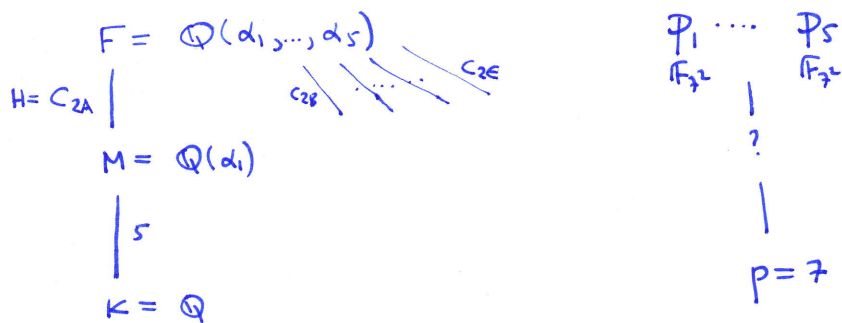
$G$ -set  $X$   $|X| = d \rightsquigarrow$   $d$ -dimensional permutation rep.  $\mathbb{C}[X]$   
 basis = elts of  $X$ ,  $G$  permutes them

$$(X = X_1 \perp X_2 \perp \dots \Rightarrow \mathbb{C}[X] \cong \mathbb{C}[X_1] \oplus \mathbb{C}[X_2] \oplus \dots)$$

so enough to consider transitive ones).

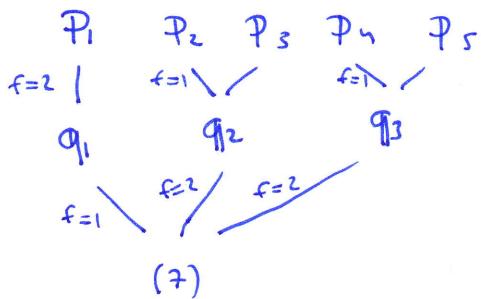
Aside: Prime decomposition in intermediate extensions

Ex  $K = \mathbb{Q}$   
 $F = \mathbb{Q}(\text{roots of } x^5 - 5x^2 - 3)$   
 $G = \text{Gal}(F/K) \cong D_5$



$$D_{P_i}^{F/M} = D_{P_i}^{F/K} \cap H = \begin{cases} C_{2A} & i=1 \quad (\Rightarrow f_{P_i}^{F/M} = 2) \\ 1 & i=2,3,4,5 \quad (\Rightarrow f_{P_i}^{F/M} = 1) \end{cases}$$

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



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

$\Rightarrow (7) = Q_1 Q_2 Q_3$  in  $M/K \Rightarrow D_7^{F/K} = C_2$  [and not  $C_1, C_5, D_5$ ]

Prop  $K$  number field  $\left. \begin{matrix} F \\ H \\ M \\ I \\ K \end{matrix} \right\} \text{Galois with group } G$

$D_i = D_{P_i}^{F/K} < G$   
 $I_i = I_{P_i}^{F/K} < D_i$   
 $I = I_1, D = D_1, \text{Frob}_P \in D$

(i)  $D_{P_i}^{F/M} = D_i \cap H, \quad I_{P_i}^{F/M} = I_i \cap H$

(ii) In  $M/K$  primes  $q_j | p \xleftrightarrow{1:1} \text{double cosets } Dg_i H \in D \backslash G/H \xleftrightarrow{1:1} \text{orbits of } D \text{ on } G/H$   
 with

Each orbit has length  $e_j f_j$  and is a union of  $f_j$   $I$ -orbits of length  $e_j$ , cyclically permuted by  $\text{Frob}_P$ .

Proof (i) clear

(ii)  $H \triangleleft G \setminus \{p_i\}$  orbits  $\xleftrightarrow{1:1} q_i$  stabilisers  $= D_{p_i}^{F/M}$

$H \triangleleft G/D$  orbits  $\xleftrightarrow{1:1}$  double cosets stabilisers  $= D:DH$

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  $\zeta$ -func ( $= \zeta_M$  if  $K=Q$ )

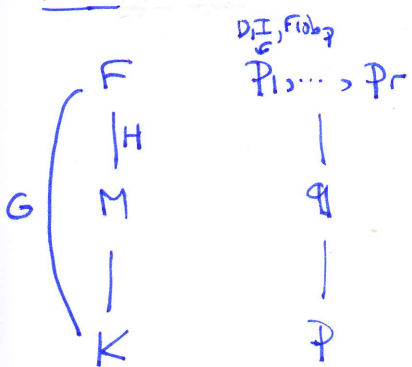
$$\zeta_{M/K}(s) = \prod_{q \subseteq \mathcal{O}_M} \frac{1}{1 - N_{M/K}(q)^{-s}}$$

Alfin L-fnc for the rep  $\mathbb{C}[X_{M/K}] \supset \text{Gal}(K/K)$

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

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

Proof



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

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

As a  $D$ -set,

$$G/H = \coprod_{Dg_iH} D / \underbrace{D \cap g_i H g_i^{-1}}_{\substack{\text{I acts with } f: \text{ orbits} \\ \text{of size } \mathbb{I} \cap g_i H g_i^{-1} \\ \text{cyclically permuted by } \text{Frob}_{\mathfrak{p}}}}$$

$$\Rightarrow \mathbb{C}[G/H]^{\mathbb{I}} \cong \bigoplus_j \mathbb{C}^{f_j}$$

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

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