§12 Local fields

multiplicative
Δ inq.'s only such except for $|\cdot|_{\mathbb{R}}$

$K = \mathbb{Q}$, p prime $\rightsquigarrow$ p-adic absolute value

$|\cdot|_p$ on $\mathbb{Q}$ $\quad |p^n \frac{a}{b}| = \frac{1}{p^n}$, $|0| = 0$
$p \nmid a, b$

$\rightsquigarrow$ metric $d_p(x,y) = |x-y|_p$

Def p-adic integers $\mathbb{Z}_p$ =

$= \text{top. completion of } \mathbb{Z} \text{ w.r.to } |\cdot|_p \text{ (i.e. } d_p)$

$= \dfrac{\{\text{Cauchy sequences } (x_n)_{n\in\mathbb{Z}}\}}{\{\text{sequences } x_n \to 0\}}$

$= \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{\text{sequences } x_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t. } x_n \equiv x_{n+1} \bmod p^n\}$

$= \{\sum_{n=0}^{\infty} a_n p^n \mid a_n \in \{0,\dots,p-1\}\}$

$\mathbb{Z}_p$ is a DVR, local ring, only one maximal ideal (p), res. field $\mathbb{F}_p$. ; $\supseteq \mathbb{Z}$.

Def p-adic numbers $\mathbb{Q}_p$ =

$= \quad$ —"— $\mathbb{Q}$ —"—

$=$ field of fractions of $\mathbb{Z}_p$

$= \left\{ \sum_{n=n_0}^{\infty} a_n p^n \mid a_n \in \{0, \dots p-1\} \right\}$ field,

$\supseteq \mathbb{Q}$ (char = 0).

Ex In $\mathbb{Q}_2$

$21 = 1+2^2+2^4 \in \mathbb{Z}_2$

$\frac{3}{2} = 2^{-1}+1 \notin \mathbb{Z}_2$

$-1 = 1+2+2^2+2^3+\ldots \in \mathbb{Z}_2$

$[= \frac{1}{1-x}$ geom. series with $x=2$, $|x|_2 < 1 \Rightarrow$ converges.

Similarly $K/\mathbb{Q}$ finite, O, $\mathfrak{p}$, $O/\mathfrak{p} = k$ finite

$\rightsquigarrow$ $\mathfrak{p}$-adic abs. value $|x|_{\mathfrak{p}} = \left(\frac{1}{|k|}\right)^{v_{\mathfrak{p}}(x)}$

$K_{\mathfrak{p}}$ = top. completion of K w.r.to $|\cdot|_{\mathfrak{p}}$

local or p-adic field

fin. ext. of $\mathbb{Q}_p$ ($\mathfrak{p}|p$), and every fin. ext. of $\mathbb{Q}_p$ arises this way.

$$K_{\mathfrak{p}} = \left\{ \sum_{n=n_0}^{\infty} a_n \pi^n \,\middle|\, a_n \in A \right\}$$

π any uniformiser ($v_{\mathfrak{p}}(\pi) = 1$, e.g. $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$).

A any set of representatives of $\mathcal{O}/\mathfrak{p}$.

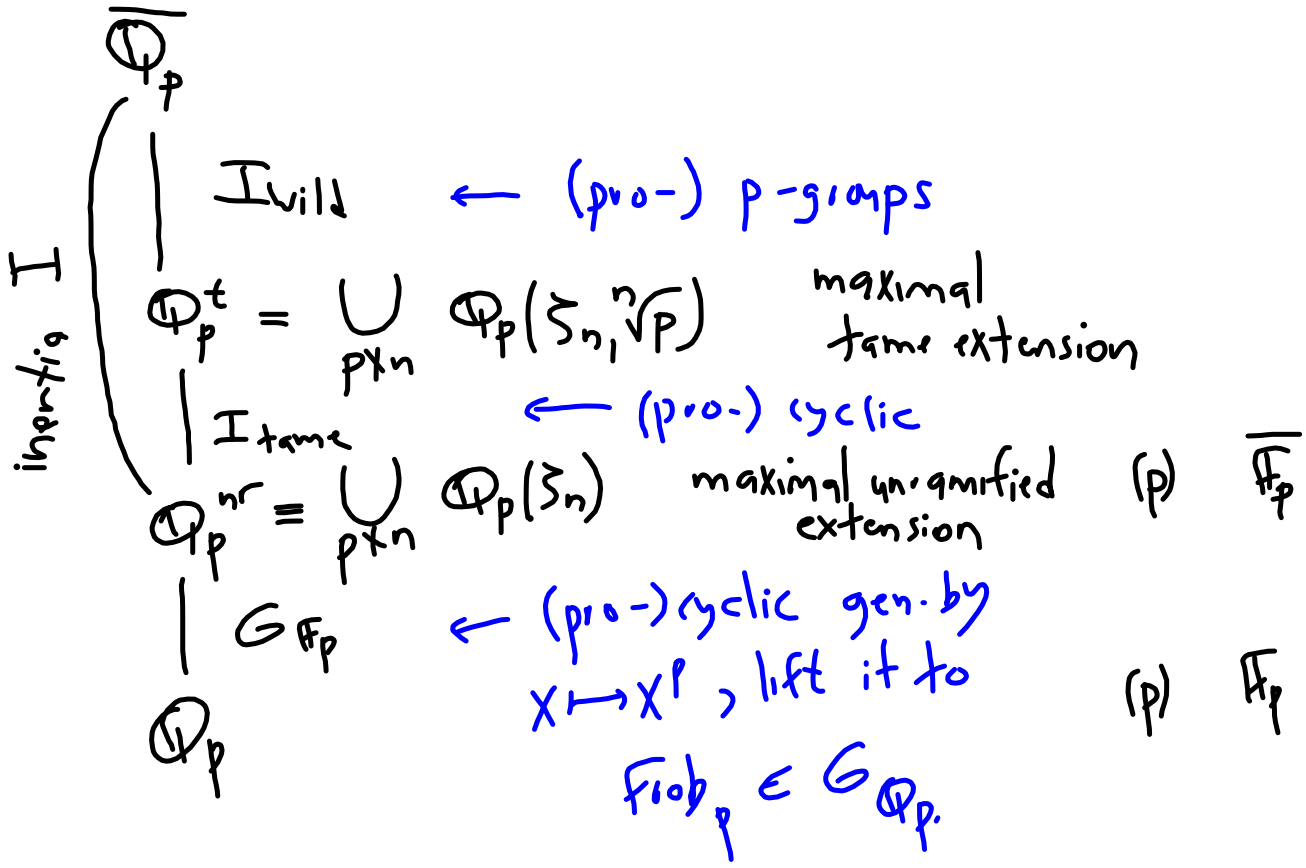
Prop $\begin{array}{ccc} F & & \mathfrak{q} \\ | & \text{Galois} & | \\ K & & \mathfrak{p} \end{array}$ Then $F_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois with $\mathrm{Gal}(F_{\mathfrak{q}}/K_{\mathfrak{p}}) = D_{\mathfrak{q}}$.

(same for all $\mathfrak{q}|\mathfrak{p}$).

Passing to algebraic closure

$\begin{array}{ccc} \overline{\mathbb{Q}} & \text{prime } \mathfrak{q} \text{ above } \mathfrak{p} \text{ in } \overline{\mathbb{Q}} & \overline{\mathbb{Q}_p} \\ | & | & | \; G_{\mathbb{Q}_p} = D_{\mathfrak{q}} < G_{\mathbb{Q}} \\ \mathbb{Q} & p & \mathbb{Q}_p \end{array}$ complete $\rightsquigarrow$

- "Same" as number fields, but only one prime & much simpler ← cf. $\mathbb{R}, \mathbb{C}$ vs. Φ
- Inertia, Frobenius, tame inertia etc.
  - same definition
- Structure of $G_{\Phi_p} = \mathrm{Gal}(\overline{\Phi}_p / \Phi_p)$:


$\overline{\mathbb{Q}}_p$
I_{wild}
$\leftarrow$ (pro-) p-groups
$\mathbb{Q}_p^t = \bigcup_{p \nmid n} \mathbb{Q}_p(\zeta_n, \sqrt[n]{p})$
maximal tame extension
$\leftarrow$ (pro-) cyclic
I_{tame}
$\mathbb{Q}_p^{nr} = \bigcup_{p \nmid n} \mathbb{Q}_p(\zeta_n)$
maximal unramified extension
(p) $\overline{\mathbb{F}}_p$
$G_{\mathbb{F}_p}$
$\leftarrow$ (pro-)cyclic gen. by $x \mapsto x^p$, lift it to $Frob_p \in G_{\mathbb{Q}_p}$
(p) $\mathbb{F}_p$
$\mathbb{Q}_p$
inertia I

- Local fields have only fin. many extensions of a given degree, e.g.

$$\mathbb{Q}_5(\sqrt{-3}) = \mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\zeta_3) =$$
$$= \mathbb{Q}_5(\zeta_8) = \mathbb{Q}_5(\zeta_{24})$$
$$= \text{unique quad. unramified extension of } \mathbb{Q}_5.$$

§13 ℓ-adic representations

Ex $G_\Phi \curvearrowright \{$ roots of unity in $\overline{\Phi}\}$

$= \{$ torsion points in $G_m(\overline{\Phi})$

$= \overline{\Phi}^\times\}$

[this action does not factor through a finite Galois group]

$\rightsquigarrow$ Galois representation (1-dim) as follows:

ℓ prime

$$
\begin{array}{ccccc}
\cdots & & \cdots & & \text{acts through } (\mathbb{Z}/\ell^3\mathbb{Z})^\times \\
 & & \downarrow & & = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^3})/\mathbb{Q}) \\
\{\ell^3 \text{ roots of unity}\} & \cong & \mathbb{Z}/\ell^3\mathbb{Z} & \circlearrowright & G_{\mathbb{Q}} \\
 & & \downarrow{\scriptstyle (\cdot)^{\ell}} & & \\
\{\ell^2 \text{ roots of unity}\} & \cong & \mathbb{Z}/\ell^2\mathbb{Z} & \circlearrowright & G_{\mathbb{Q}} \\
 & & \downarrow{\scriptstyle (\cdot)^{\ell}} & & \\
\{\ell \text{ th roots of unity}\} & \cong & \mathbb{Z}/\ell\mathbb{Z} & \circlearrowright & G_{\mathbb{Q}}
\end{array}
$$

acts through $(\mathbb{Z}/\ell\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$

Inverse limit

$$G_{\mathbb{Q}} \to \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} \cong \mathbb{Z}_\ell$$

in other words, get

$$\chi_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^\times = GL_1(\mathbb{Z}_\ell)$$

$$= \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q})$$

Embed $\mathbb{Z}_\ell \hookrightarrow \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ may view

$$\chi_\ell : G_{\mathbb{Q}} \longrightarrow GL_1(\mathbb{C})$$

1-dim. Galois representation [one for every ℓ],

ℓ-adic cyclotomic character.

Def K number field, $G_K = Gal(\bar{K}/K)$

An **ℓ-adic representation over K** is (of dimension (or degree) d.)

a continuous hom.

$$\rho_\ell : G_K \longrightarrow GL_d(\mathbb{Q}_\ell)$$

A compatible system of ℓ-adic representations

[or 'a motive'] is a collection $\rho = (\rho_\ell)_{\ell \text{ prime}}$ s.t.

(1) There is a finite set S of primes of K s.t. each ρ_ℓ is unramified outside $S_\ell = S \cup \{\text{primes} \mid \ell\}$, i.e.

$$\mathfrak{p} \notin S_\ell \Rightarrow \rho_\ell(I_\mathfrak{p}) = 1.$$

(2) For every prime $\mathfrak{p}$, the local polynomial

$$F_{\mathfrak{p}}(T) = \det(1 - \mathrm{Frob}_{\mathfrak{p}}^{-1} T \mid \rho_\ell^{I_{\mathfrak{p}}}) \in \mathbb{Q}_\ell[T]$$

is in $\mathbb{Q}[T]$ and is independent of ℓ, $\mathfrak{p} \nmid \ell$.

We define

$$L(\rho, s) = \prod_{\mathfrak{p}} F_{\mathfrak{p}}(N\mathfrak{p}^{-s})$$ L-function of ρ

poor man's version of

one global representation

$G_{\mathbb{Q}} \longrightarrow GL_d(\mathbb{Q})$

Have standard constructions

$\oplus$, $\otimes$, Ind, Res, ... for

compatible systems, L-fncs satisfy

Artin formalism.

Ex $\rho : G_K \longrightarrow GL_n(\mathbb{Q})$ Artin rep.

{finite image, factors through some finite $Gal(F/K)$}

$\rho_\ell : G_K \to GL_n(\mathbb{Q}) \hookrightarrow GL_n(\mathbb{Q}_\ell)$

obviously a compatible system;

$S = \{$ primes ramified in $F/K\}$

Rmk Can also replace $(\mathbb{Q}_\ell)_{\ell \text{ prime of } \mathbb{Q}}$ to $(M_\lambda)_{\lambda \text{ primes of } M}$, M number field to include all Artin representations $G_K \to GL_n(\mathbb{C})$, e.g. Dirichlet characters.

Ex $\chi = (\chi_\ell)_\ell$ cyclotomic character

$$\chi_\ell : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}) = \mathbb{Z}_\ell^\times \hookrightarrow GL_1(\mathbb{Q}_\ell)$$

$I_p \longmapsto 1 \quad \forall p \neq \ell$

$\mathrm{Frob}_p \longmapsto p^{-1}$

$\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^p$

can take
$\zeta = \phi$
$\zeta_\ell = 1\ell$

$$F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid \mathbb{Z}_\ell^{I_p})$$

$$\mathbb{Z}_\ell \text{ a } G_{\mathbb{Q}}\text{-module}$$

$$= 1 - pT \in \mathbb{Q}[T]$$

and is independent of ℓ.

$\Rightarrow$ Form a compatible system with

$$L(\chi, s) = \prod_p \frac{1}{1 - p \cdot p^{-s}} = \zeta(s-1)$$

In modern language, χ_ℓ are ℓ-adic realisations of the "Tate motive $\mathbb{Q}(1)$"

[and the χ_ℓ denoted $\mathbb{Q}_\ell(1)$],

which has associated L-function $\zeta(s-1)$.

Étale cohomology (Grothendieck, Deligne, Verdier).

$V/\mathbb{Q}$ [or /number field K]

non-singular proj. variety of dim d,

$0 \leq i \leq 2d$

$\rightsquigarrow H^i(V) = H^i_{ét}(V_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ étale coh. gp.

$\mathbb{Q}_\ell$-vector space of dim $= b_i(V(\mathbb{C}))$ (ith Betti number)

with a (continuous) action of $G_{\mathbb{Q}}$.

$\rightsquigarrow$ ℓ-adic representation of $G_{\mathbb{Q}}$ for every ℓ.

(1) Unramified outside

$S = \{$ primes of bad reduction for $V\} \cup \{\ell\}$

(2) Known to be compatible at $p \notin S$,

often (H^0, H^1, curves, abelian varieties)

for $p \in S$ as well.

Ex $H^0(V) = \mathbb{Q}_\ell\left[\begin{array}{l}\text{connected components}\\ \text{of } V/\bar{\mathbb{Q}}\end{array}\right]$

$\circlearrowright$

$G_{\mathbb{Q}}$

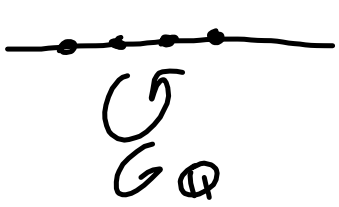
permutation rep. on connected components.

(factors through some finite $Gal(F/\mathbb{Q})$)

Ex $\dim V = 0$. $\rightsquigarrow$ only H^0.

$V: f(x) = 0 \subseteq \mathbb{A}^1_x$

$f \in \mathbb{Q}[x]$



$\circlearrowright$

$G_{\mathbb{Q}}$

$$H^0(V) = \mathbb{Q}_\ell[\text{roots of } f]$$

If $f(x) = f_1(x) \cdots f_n(x)$ $f_i \in \mathbb{Q}(x)$ irr.

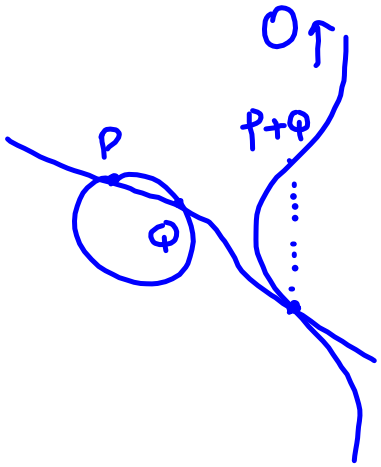
$$K_i = \mathbb{Q}[x]/(f_i)$$

$$L(H^0(V), s) = \zeta_{K_1}(s) \cdots \zeta_{K_n}(s).$$

§14 Torsion points on elliptic curves & $H^1(E)$

E/K ell. curve, K number field

$$y^2 = x^3 + ax + b;\ a, b \in K$$



$E(\bar{K})$ abelian group

Def $m \geq 1$ integer.

$$E[m] = \{ P \in E(\bar{K}) \mid mP = O \}$$ m-torsion

$$\cong (\mathbb{Z}/m\mathbb{Z})^2 \circlearrowright G_K$$ acts linearly

$(P+Q)^\sigma = P^\sigma + Q^\sigma$

Gives a representation ("mod m" representation)

$$\rho_{E,m} : G_K \longrightarrow GL_2(\mathbb{Z}/m\mathbb{Z})$$

Ex $m = 2$. $\quad y^2 = f(x)$

$E[2] = \{0, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$

α, β, γ roots of f. $\quad \circlearrowright G_K$

$\cong (\mathbb{Z}/2\mathbb{Z})^2 \quad \circlearrowright G_K$.

Get

$$\rho_{E,2} : G_K \longrightarrow GL_2(\mathbb{F}_2) \cong S_3.$$

Take $m = \ell^n$, ℓ prime.

$$\longrightarrow E[\ell^n] \xrightarrow{[\ell]} E[\ell^{n-1}] \longrightarrow \cdots \longrightarrow E[1]$$

$$\longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 \longrightarrow \cdots \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^2$$

Def The ℓ-adic Tate module

$$T_\ell E = \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^2 \circlearrowright G_K$$

$$V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^2 \circlearrowright G_K$$

Get a 2-dim. ℓ-adic representation for E/K,

$$H^1_{\text{ét}}(E_{\bar{K}}, \mathbb{Q}_\ell) = V_\ell E^* \text{ as a } G_K\text{-representation.}$$

We will see that these form a compatible system, so

Def The L-function of ϵ

$$L(\epsilon, s) = \prod_p F_p(N_p^{-s})$$

$$F_p(T) = \det\left(1 - \mathrm{Frob}_p^{-1} T \,\middle|\, (V_\epsilon \epsilon^*)^{I_p}\right).$$

degree 2 L-function.