§ 12 Local fields

$K = \mathbb{Q}$, p prime $\rightsquigarrow$ <u>p-adic absolute value</u> $|\cdot|_p$ on $\mathbb{Q}$ ← multiplicative; triangle inequality; only such on $\mathbb{Q}$ except $|\cdot|_{\mathbb{R}}$.

$$\left|p^n \tfrac{a}{b}\right|_p = \frac{1}{p^n}, \quad |0| = 0 \qquad (p \nmid a,b)$$

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

Def <u>p-adic integers</u>

$$\begin{aligned} \mathbb{Z}_p &= \text{(top.) completion of } \mathbb{Z} \text{ w.r.to } d_p \\ &= \{\text{Cauchy sequences } (x_n) \text{ in } \mathbb{Z}\} / \{\text{sequences } x_n \to 0\} \\ &= \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}. \quad \leftarrow \left\{\begin{array}{l}\text{sequences } (x_n \in \mathbb{Z}/p^n\mathbb{Z}) \\ \text{s.t. } x_n \equiv x_{n+1} \bmod p^n\end{array}\right\} \\ &= \left\{ \sum_{n=0}^{\infty} a_n p^n \;\middle|\; a_n \in \{0, \dots, p-1\} \right\} \end{aligned}$$

← DVR, $\supseteq \mathbb{Z}$, <u>local ring</u>: only one max. ideal (p), res. field $\mathbb{F}_p$.

<u>p-adic numbers</u>

$$\begin{aligned} \mathbb{Q}_p &= \text{——— " ———} \quad \mathbb{Q} \\ &= \text{field of fractions of } \mathbb{Z}_p \\ &= \left\{ \sum_{n=n_0}^{\infty} a_n p^n \right\} \end{aligned}$$

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

Ex In $\mathbb{Q}_2$

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

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

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

[$= \frac{1}{1-x}$ geom. series with $|x|_p < 1$ $\Rightarrow$ converges].

Similarly $K/\mathbb{Q}$ finite, $\mathcal{O}, \mathfrak{p}$, $\mathcal{O}/\mathfrak{p} = k$ $\rightsquigarrow$ $\mathfrak{p}$-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 $|x|_{\mathfrak{p}}$ — <u>local</u> or <u>p-adic field</u>

↪ 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 <u>uniformiser</u> ($v_{\mathfrak{p}}(\pi) = 1$, e.g. $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$)

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

Prop

$$\begin{array}{ccc} F & & \mathfrak{q} \\ \big| \text{ Galois} & & \big| \\ K & & \mathfrak{p} \end{array}$$

Then $F_{\mathfrak{q}}/K_{\mathfrak{p}}$ Galois with

$$\mathrm{Gal}(F_{\mathfrak{q}}/K_{\mathfrak{p}}) = D_{\mathfrak{q}}.$$

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

Passing to alg. closure

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

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

$$\begin{array}{lll}
\overline{\mathbb{Q}}_p & & \\
\quad | \; I_{\text{wild}} & & \leftarrow \text{(pro-) } p\text{-group} \\
\mathbb{Q}_p^t = \bigcup_{p \nmid n} \mathbb{Q}_p(\zeta_n, \sqrt[n]{p}) & & \\
\quad | \; I_{\text{tame}} & & \leftarrow \text{(pro) cyclic} \\
\mathbb{Q}_p^{nr} = \bigcup_{p \nmid n} \mathbb{Q}_p(\zeta_n) & \text{max. unr. ext.} & \\
\quad | \; G_{\mathbb{F}_p} & & \leftarrow \text{(pro)-cyclic gen. by } x \mapsto x^p, \text{ lift to } \mathrm{Frob}_p \in G_{\mathbb{Q}_p} \\
\mathbb{Q}_p & &
\end{array}$$

I inertia $= \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$

$$\begin{array}{cc} (p) & \overline{\mathbb{F}}_p \\ | & | \\ (p) & \mathbb{F}_p \end{array}$$

- local fields have only fin. many exts of a given degree, e.g.

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

§13 ℓ-adic representations

Ex

$G_{\mathbb{Q}} \circlearrowright \{\text{roots of unity in } \overline{\mathbb{Q}}\}$ $= \{\text{torsion points of } \mathbb{G}_m(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}^{\times}\}$

[not through a finite gp]

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

ℓ prime

$$\begin{array}{ccccccc}
\cdots & & \vdots & & & & \vdots \\
\{\ell^3 \text{ roots of } 1\} & \cong & \mathbb{Z}/\ell^3\mathbb{Z} & \circlearrowleft & G_{\mathbb{Q}} & & \mathbb{Q}(\zeta_{\ell^3}) \\
\downarrow x \mapsto x^{\ell} & & \downarrow [\ell] & & & (\mathbb{Z}/\ell^3\mathbb{Z})^{\times} & | \\
\{\ell^2 \text{ roots of } 1\} & \cong & \mathbb{Z}/\ell^2\mathbb{Z} & \circlearrowleft & G_{\mathbb{Q}} & & \mathbb{Q}(\zeta_{\ell^2}) \\
\downarrow x \mapsto x^{\ell} & & \downarrow [\ell] & & & (\mathbb{Z}/\ell^2\mathbb{Z})^{\times} & | \\
\{\ell^{th} \text{ roots of } 1\} & \cong & \mathbb{Z}/\ell\mathbb{Z} & \circlearrowleft & G_{\mathbb{Q}} \text{ through} & (\mathbb{Z}/\ell\mathbb{Z})^{\times} & \mathbb{Q}(\zeta_{\ell}) \\
& & & & & & | \\
& & & & & & \mathbb{Q}
\end{array}$$

Inverse limit $\Rightarrow$ $\quad G_{\mathbb{Q}} \circlearrowleft \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} \cong \mathbb{Z}_\ell$,

in other words set

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

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 rep, for every ℓ, <u>ℓ-adic cyclotomic character</u>

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

An <u>ℓ-adic representation over K</u> is a continuous hom.

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

$\leftarrow$ of <u>degree</u> or <u>dimension</u> d

or "<u>motive</u>"

<u>A compatible system of ℓ-adic reps</u> is a collection $\rho = (\rho_\ell)_{\ell \text{ prime}}$ s.t.

(1) There is a finite set S of 'bad' 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 $\mathfrak{p}$, the local polynomial

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

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

$\leftarrow$ poor man's version of a global representation $G_K \to GL_d(\mathbb{Q})$

We define

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

Have standard constructions $\oplus, \otimes$, Ind, Res for compatible systems, L-fncs satisfy Artin formalism.

<u>Ex</u> $\rho : G \to GL_n(\mathbb{Q})$ Artin rep. (finite image, factors through $\mathrm{Gal}(\underset{\text{finite}}{F/K})$)

$$\rho_\ell : G \to GL_n(\mathbb{Q}) \hookrightarrow GL_n(\mathbb{Q}_\ell) \quad \text{obviously compatible system;}$$

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

<u>Rmk</u> 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 $G_K \to GL_n(\mathbb{C})$ not just $\to GL_n(\mathbb{Q})$, e.g. Dirichlet characters.

<u>Ex</u> $\chi = (\chi_\ell)_\ell$ cyclotomic character

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

unramified at all $p \neq \ell$

$I_p \longmapsto 1 \quad \forall p \neq \ell$ can take $S = \emptyset$, $S_\ell = \{\ell\}$ ①

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

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

$F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid \chi_\ell^{I_p}) = 1 - pT \in \mathbb{Q}[T]$, ②

$\circlearrowleft$ the $G_{\mathbb{Q}}$ — independent of ℓ

compatible system with

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

In modern language, χ_ℓ are ℓ-adic realizations of the "Tate motive $\mathbb{Q}(1)$",
also denoted $\mathbb{Q}_\ell(1)$

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

Étale cohomology (Grothendieck, Deligne, Verdier)

$V/\mathbb{Q}$ [or number field] nonsing. proj. variety of dim d, $0 \leq i \leq 2d$

$\rightsquigarrow H^i(V) = H^i_{et}(V_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ étale coh. gp., $\mathbb{Q}_\ell$-vector space of dim $b_i(V(\mathbb{C}))$ (ith Betti number)

with $G_{\mathbb{Q}}$-action (continuous)

① Unramified outside $S = \{$places of bad red. of $V\}$ $\cup \{\ell\}$.

② Known to be compatible at $p \notin S$, often (H^0, H^1, curves, ab. varieties) for $p \in S$ as well.

Ex $H^0(V) = \mathbb{Q}_\ell[$connected components of $V/\bar{\mathbb{Q}}]$ $\circlearrowleft G_{\mathbb{Q}}$

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

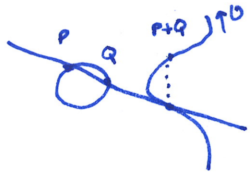
$V: f(x) = 0 \subseteq \mathbb{A}^1$

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

If $f = f_1 \cdots f_n$, f_i irr. $/\mathbb{Q}$, $K_i = \mathbb{Q}[x]/f_i$

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

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



E/K ell. curve

$$y^2 = x^3 + ax + b$$

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

<u>Def</u> $m \geq 1$ integer.

$$E[m] = \{ P \in E(\bar{K}) \mid mP = 0 \} \qquad \underline{m\text{-torsion}}$$

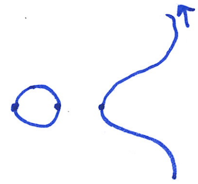
$$\cong (\mathbb{Z}/m\mathbb{Z})^2 \quad \circlearrowleft G_K \text{ acts linearly}$$

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

Gives a representation ["mod m" rep.]

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

<u>Ex</u> $m = 2$



$$E[2] = \{0, (\alpha,0), (\beta,0), (\gamma,0)\} \qquad \begin{array}{c} G_K \\ \circlearrowleft \end{array} \quad \alpha, \beta, \gamma \text{ roots of } x^3+ax+b$$

$$\cong (\mathbb{Z}/2\mathbb{Z})^2$$

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

Take $m = \ell^n$, ℓ prime.

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

$$\to (\mathbb{Z}/\ell^n\mathbb{Z})^2 \to (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 \to \cdots \to (\mathbb{Z}/\ell\mathbb{Z})^2 \qquad \leftarrow \text{inverse system.}$$

<u>Def</u> The <u>ℓ-adic Tate module</u>

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

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

Embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, get 2-dim rep., <u>$\ell$-adic rep. for E/K</u>.

$$H^1_{et}(E_{\bar{K}}, \mathbb{Q}_\ell) = V_\ell E^* \qquad \circlearrowleft G_K \qquad \text{[not finite image]}$$

We will see these form a compatible system, so

<u>Def</u> The <u>L-function of E/K</u>

$$L(E/K, s) = \prod_p F_p(p^{-s}) \quad ; \quad F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid \rho_\ell^{I_p})$$

for any ℓ s.t. $p \nmid \ell$

degree 2 L-function.