KOLYVAGIN

Titolo nota

Funzioni L - parte II

09/02/2023

L. Bertoletti

Review: For $f \in S_k(\Gamma_0(N))$, we have studied the L-function $L(s, f)$ and shown that it enjoys the following properties:

- $L(s, f)$ converges to a holomorphic function for $\mathrm{Re}\, s > k/2 + 1$
- if f is a normalised Hecke eigenform, $L(s, f)$ has an Euler product

$$L(s, f) = \prod_p \left(1 - a_p(f)\, p^{-s} + \mathbb{1}_N(p)\, p^{k-1-2s}\right)^{-1}$$

- if f is an eigenvector for the Fricke involution,

$w_N f = \pm f$, and k is even, the completed L-function

$$\Lambda(s,f) = N^{s/2}(2\pi)^{-s}\,\Gamma(s)\,L(s,f)$$

satisfies $\Lambda(f, k-s) = \pm i^k \Lambda(f,s)$

In our case, f will be a weight-2 newform, so

$$\Lambda(f, 2-s) = -\varepsilon_f \Lambda(f,s)$$

where $w_N f = \varepsilon_f f$

Today: define $L(E,s)$ for E an elliptic curve

We would like it to be an Euler product

$$L(E,s) = \prod_p F_p(p^{-s})^{-1}$$

where F_p, for almost all primes, should be

$$F_p(t) = 1 - a_p(E)\, t + p\, t^2$$

while for $p \mid N$ the polynomial $F_p(t)$ should have degree ≤ 1, $F_p(t) = 1 - a_p(E) \cdot t$ for some $a_p(E)$.

($a_p(E) := p + 1 - \# \tilde{E}(\mathbb{F}_p)$ if E has good red. mod p)

Rmk Taking $N = N(E)$ to be the conductor, $p \nmid N \iff$ E has good reduction at p, in which case the charpoly of Frobenius is $t^2 - a_p(E)\, t + p =: g_p(t)$, and $F_p(t) = \frac{1}{p}\, g_p(pt)$

We would like to make sense of the charpoly of Frob even in the bad reduction case.

Bad reduction $\tilde{E}$ has a unique singular point and geometric genus 0. There is a birational map

$$\tilde{E} \dashrightarrow \mathbb{P}^1$$

Two cases:

- P_{sing} is a node $\Leftrightarrow$ $\tilde{E}^{ns} \simeq \mathbb{G}_m$ over $\overline{\mathbb{F}}_p$
- P_{sing} is a cusp $\Leftrightarrow$ $\tilde{E}^{ns} \simeq \mathbb{G}_a$ over $\overline{\mathbb{F}}_p$ (hence $\mathbb{F}_p$)

In the two cases, we say that E has multiplicative/additive bad reduction.

Moreover: if $\tilde{E}^{ns} \simeq \mathbb{G}_m$ over $\mathbb{F}_p$ (and not just $\overline{\mathbb{F}}_p$), we say that E has SPLIT multiplicative reduction.

Def. The ℓ-adic Tate module of E is

$$T_\ell E := \varprojlim_n E[\ell^n] \simeq \mathbb{Z}_\ell^2$$

$$V_\ell E := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^2$$

The absolute Galois group $G_\mathbb{Q}$ acts on $T_\ell E$, $V_\ell E$

Let now p be a prime, $p \neq \ell$. Fix a place of $\overline{\mathbb{Q}}$ over p.
This gives a decomposition and an inertia subgroup of $G_\mathbb{Q}$ at p.

D_p I_p

Rmk If p is a prime of good reduction, $E[\ell^n] \xrightarrow{\sim} \tilde{E}[\ell^n]$ via reduction. Let $\sigma \in I_p$: one has

$\tilde{O} = \sigma \tilde{P} - \tilde{P} = \widetilde{(\sigma P - P)} \Longrightarrow \sigma P = P$, so I_p acts trivially on $E[\ell^n]$ $\forall n$, hence on $T_\ell E$. One says that $T_\ell E$ is UNRAMIFIED at p.

Teo (Néron - Ogg - Shafarevich) Let $\ell \neq p$ be primes. The prime p is of good reduction iff $T_\ell E$ is unramified.

Rmk $(V_\ell E)^{I_p}$ has dimension ≤ 2, with equality iff p is of good reduction. We will more generally look at char. polys on $V_\ell E$.

Def. $E/\mathbb{Q}$ an elliptic curve, p a prime. We set

$$F_p(t) = \det\left(\mathrm{Id} - \mathrm{Frob}_p^{-1} t \mid (V_\ell E^\vee)^{I_p}\right),$$

where Frob_p is any lift of $(x \mapsto x^p) \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ to the decomposition group D_p. This makes sense since the action of Frob_p on $(V_\ell E)^{I_p}$ (hence on its dual) is independent of the lift chosen.

Fact One can determine $F_p(t)$ in all cases:

- E has split mult. red at p: $F_p(t) = 1 - t$
- " " non-split " " " ": $F_p(t) = 1 + t$
- " " additive " " ": $F_p(t) = 1$

Fricke involution and Heegner points

$Y_0(N)$ parametrizes pairs (E, C), $\mathbb{Z}/N\mathbb{Z} \simeq C \subseteq E$

$$\tau \longmapsto \left(\frac{\mathbb{C}}{\mathbb{Z} \oplus \mathbb{Z}\tau}, \overline{1/N} \right)$$

We had constructed Heegner pts x_n,

$$x_n = \left(\mathbb{C}/\mathcal{O}, \; \mathfrak{n}^{-1}/\mathcal{O} \right) \qquad \mathcal{O} = \mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K \text{ order in } K$$

$$\mathfrak{n} \text{ s.t. } \mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$$

Question: what's $w_N x_n$, where w_N is the Fricke involution?

More generally, given $\mathfrak{a} \in Cl(\mathcal{O})$, we can consider the Heegner point $(\mathcal{O}, \mathfrak{n}^{-1}, \mathfrak{a}) := \left(\mathbb{C}/\mathfrak{a}, \; \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a} \right)$

RmK • We can describe $\ker\left(\mathbb{C}/\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a} \right)$ as

$$\frac{\mathfrak{a}\mathfrak{n}^{-1}}{\mathfrak{a}}$$

• The triples $(\mathcal{O}, \mathfrak{n}, \mathfrak{a})$ parametrise the elliptic curves

E with CM by $\mathcal{O}$, together with a choice of subgroup $C \subseteq E$,
s.t. both E and E/C have CM by $\mathcal{O}$
(Recall that $\mathcal{E}\ell\ell(\mathcal{O}) \longleftrightarrow \mathcal{C}\ell(\mathcal{O})$; so both E and

$$\mathbb{C}/\mathfrak{a} \longleftrightarrow \mathfrak{a}$$

E/C are of the form $\mathbb{C}/\mathfrak{a}$, $\mathbb{C}/\mathfrak{b}$, and then
$\mathfrak{n} := \mathfrak{b}^{-1}\mathfrak{a}$ satisfies $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$, and conversely)

So, what's $w_N(\mathcal{O}, \mathfrak{n}, \mathfrak{a})$?
We exploit the bijection $Y_0(N) \longleftrightarrow \{(E, C)\}$.
There exist $\omega_1, \omega_2 \in \mathbb{C}$ s.t.

$$\mathfrak{a} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

$$\mathfrak{n}^{-1}\mathfrak{a} = \mathbb{Z}\,\omega_1 \oplus \mathbb{Z}\,\frac{\omega_2}{N}$$

Since $w_N\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}0 & -1\\ N & 0\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}-\omega_2\\ N\omega_1\end{pmatrix}$, we obtain

$$w_N(\mathcal{O}, \mathfrak{n}, \mathfrak{a}) = \left(\frac{\mathbb{C}}{-\omega_2\mathbb{Z}\oplus N\omega_1\mathbb{Z}},\ \ker\left(\frac{\mathbb{C}}{-\omega_2\mathbb{Z}\oplus N\omega_1\mathbb{Z}} \longrightarrow \frac{\mathbb{C}}{-\omega_2\mathbb{Z}\oplus\omega_1\mathbb{Z}}\right)\right)$$

We make simultaneous changes of bases; using that induced by $\frac{1}{N}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, we obtain

$$= \left(\frac{\mathbb{C}}{\omega_1\mathbb{Z}\oplus\omega_2/N\,\mathbb{Z}},\ \ker\left(\frac{\mathbb{C}}{\omega_1\mathbb{Z}\oplus\frac{\omega_2}{N}\mathbb{Z}} \longrightarrow \frac{\mathbb{C}}{\frac{\omega_1}{N}\mathbb{Z}\oplus\frac{\omega_2}{N}\mathbb{Z}}\right)\right)$$

$$= \left(\frac{\mathbb{C}}{n^{-1}\diamond x}, \left(\frac{\mathbb{C}}{n^{-1}\diamond x} \longrightarrow \frac{\mathbb{C}}{N^{-1}\diamond x} \right) \right)$$

$$= \left(\mathcal{O}, \ \overline{n}, \ n^{-1}\diamond x \right)$$

(Mio seminario)

Local triviality of cohomology classes I

$$D_\ell = \sum_{i=1}^{\ell} i \cdot \sigma_\ell^{\,i} \qquad D_n = \prod_{\ell \mid n} D_\ell \qquad P_n = \sum_{\sigma \in \mathcal{G}_n / G_n} \sigma D_n y_n$$

$$0 \longrightarrow E[p] \longrightarrow E(\overline{K}) \xrightarrow{[p]} E(\overline{K}) \longrightarrow 0$$

$$\begin{tikzcd}
 & & c(n) \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & d(n) \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & \\
0 \arrow[r] & E(K)/pE(K) \arrow[r] \arrow[d] & H^1(K, E[p]) \arrow[r] \arrow[d, "\wr"'] & H^1(K, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \left(E(K_n)/pE(K_n)\right)^{\mathcal{G}_n} \arrow[r] & H^1(K_n, E[p])^{\mathcal{G}_n} \arrow[r] & \left(H^1(K_n, E)[p]\right)^{\mathcal{G}_n} & \\
 & {[P_n]} \arrow[u, phantom, "\rotatebox{90}{$\in$}"] & \delta [P_n] \arrow[u, phantom, "\rotatebox{90}{$\in$}"] & &
\end{tikzcd}$$

Main aim (Prop. 6.2)

(a) For every place v of K, $v \nmid n$, then

$$d(n)_v = 0 \quad \text{in} \quad H^1(K_v, E)$$

(b) v place of K, $v \mid n$: $\quad (n = \ell m, \quad v \mid \ell)$

$d(n)_v$ is trivial in $H^1(K_v, E)[p]$ if and only if

$$P_m \in p E(K_w)$$

where w is a place of K_m lying over v.

Today: Néron models.

Néron models

From now on, $K = \mathrm{Frac}(R)$ where R is a Dedekind domain.

Let E/K be an ell. curve, $E : y^2 = x^3 + ax + b$.

W/log $a, b \in R$ [which we might denote by $\mathcal{O}_K$ in what follows]

Def. Given $E \to \operatorname{Spec} K$, a MODEL for E is $\mathcal{E} \longrightarrow \operatorname{Spec} \mathcal{O}_K$, where $\mathcal{E} \longrightarrow \operatorname{Spec} \mathcal{O}_K$ is an arithmetic surface whose generic fiber is $\mathcal{E} \times_{\mathcal{O}_K} K \cong E$ (the isomorphism is part of the data of the model)

Ex $y^2 = x^3 + 1$ & $y^2 = x^3 + p^6$ are both models for $y^2 = x^3 + 1/K$

One is smooth over $\mathcal{O}_K$ (if the residue char is $\neq 2,3$), the other is not.

Def. A Weierstrass model is given by the subscheme of $\mathbb{P}_{2,\mathcal{O}_K}$ given by a (homogeneous) Weierstrass eqn.

Rmk In particular, a Weierstrass model W satisfies

$$W(\mathcal{O}_K) = W(K)$$

but W is in general not smooth.

Q Can we find a SMOOTH model $\mathcal{E}$ that satisfies

$$\mathcal{E}(\mathcal{O}_K) = \mathcal{E}(K)?$$

Ex $y^2 = x^3 + p^2 \,/\, \operatorname{Spec} \mathcal{O}_K$ is not even regular

($\text{in fact, } y^2 = x^3 + p^n$ regular $\iff n \leq 1$)

Consider the prime $\mathfrak{m} = (x, y, p) \subseteq \mathbb{Z}_p[x, y]$. To show regularity,

want to check if $\mathfrak{m}$ is generated by 2 elements

- for $n=1$, $p = y^2 - x^3$ ok
- for $n>1$, compute $\dim \mathfrak{m}/\mathfrak{m}^2 > 2$

Def. A regular model $\mathcal{C}/\mathcal{O}_K$ of C/K is MINIMAL if

$\forall\, \mathcal{C} \xrightarrow{\pi} \mathcal{C}'$, where $\mathcal{C}'$ is another regular model

and π is dominant, π is an isomorphism.

Thm Let E/K be an elliptic curve. There exists a minimal regular model proper over $\mathcal{O}_K$, and this is unique up to isomorphism

Def. Given E/K, a **Néron model** is $\mathcal{E} \to \operatorname{Spec} \mathcal{O}_K$ which is

- a model
- smooth over $\mathcal{O}_K$
- has the Néron mapping property: $\forall\, \mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ smooth, over $\mathcal{O}_K$, $\forall\, \mathcal{X}_K \to E$,

$$\begin{tikzcd} \mathcal{X}_K \arrow[r, hook] \arrow[d] & \mathcal{X} \arrow[d, dashed, "\exists!"] \\ E \arrow[r, hook] & \mathcal{E} \end{tikzcd}$$

Rmk $\mathcal{X} = \operatorname{Spec} \mathcal{O}_K$. Then the Néron mapping property shows that every K-pt of E lifts to an $\mathcal{O}_K$-pt of $\mathcal{E}$. Uniqueness shows $\mathcal{E}(\mathcal{O}_K) \hookrightarrow E(K)$ is injective, so

$$\boxed{\mathcal{E}(\mathcal{O}_K) = E(K)}$$

Rmk The Néron mapping property also gives uniqueness of the Néron model, up to unique isomorphism:

solleva id $\Rightarrow$ è id.

$$\begin{tikzcd}
\mathcal{E} \arrow[r, dashed] \arrow[d] \arrow[rr, bend left] & \mathcal{E}' \arrow[r, dashed] \arrow[d] & \mathcal{E} \arrow[d] \\
E \arrow[r, "\mathrm{id}"'] & E \arrow[r, "\mathrm{id}"'] & E
\end{tikzcd}$$

Prop. $E \longrightarrow \operatorname{Spec} K$ admits a Néron model.

Proof Take as $\mathcal{E}$ the smooth locus of a minimal regular model. $\square$

Ex • $y^2 = x^3 + 1 / \mathbb{Q}_p$ has Néron model $y^2 = x^3 + 1 / \mathbb{Z}_p$ $(p \neq 2, 3)$; more generally, if E has good red., a Weierstrass model with good reduction gives a Néron model

• $y^2 = x^3 + p / \mathbb{Q}_p$ $(p > 3 ?)$. The curve has bad red. (i.e., no Weierstrass model has good reduction)
However, it's at least regular, so $\tilde{\mathcal{E}} : y^2 = x^3 + p / \mathbb{Z}_p$ is

a minimal reg. model. $\mathcal{E} := \tilde{\mathcal{E}} \setminus (x, y, p)$

$" = " \ \tilde{\mathcal{E}} \setminus (\bar{0}, \bar{0})$

is a Néron model.

- $\tilde{\mathcal{E}} : y^2 = x^3 + p^2$. No Weierstrass eqn is regular.

The integral pt $(0, p)$ reduces to $(\bar{0}, \bar{0})$, which is singular. Hence, removing the singular pts does NOT give a Néron model (the rat pt $(0,p)$ does not extend; more formally, setting $\mathcal{E} = \tilde{\mathcal{E}} \setminus \{(\bar{0}, \bar{0})\}$, one has $\mathcal{E}(\mathcal{O}_K) \subsetneq \tilde{\mathcal{E}}(\mathcal{O}_K) = E(K)$)

Prop. K field, K'/K UNRAMIFIED, E/K an ell. curve

Let $\mathcal{E} \longrightarrow \operatorname{Spec} \mathcal{O}_K$ be the Néron model of E/K.

The base-change $\mathcal{E}' := \mathcal{E} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} \mathcal{O}_{K'}$ is a Néron model for $E_{K'}$

Proof We show that it has the Néron mapping property.

Let $X \longrightarrow \operatorname{Spec} \mathcal{O}_{K'}$ be smooth, fix $X_{K'} \longrightarrow E' := E_{K'}$.

$$X \xrightarrow{\text{smooth}} \operatorname{Spec} \mathcal{O}_{K'} \xrightarrow{\text{smooth}} \operatorname{Spec} \mathcal{O}_K$$

$$\begin{tikzcd}
X_{K'} \arrow[r] \arrow[d] & E' \arrow[r] \arrow[d] & E \arrow[d] \\
\operatorname{Spec} K' \arrow[r, equal] \arrow[d] & \operatorname{Spec} K' \arrow[r] & \operatorname{Spec} K \\
\operatorname{Spec} K & &
\end{tikzcd}$$

$\rightsquigarrow$ get

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & \mathcal{E} \arrow[dl] \\
& \operatorname{Spec} \mathcal{O}_K &
\end{tikzcd}$$

also have

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & \operatorname{Spec} \mathcal{O}_{K'} \arrow[dl] \\
& \operatorname{Spec} \mathcal{O}_K &
\end{tikzcd}$$

Take fibre product:

$$\begin{tikzcd}
X \arrow[dr, dashed] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& \mathcal{E}' \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathcal{E} \arrow[d] \\
& \operatorname{Spec} \mathcal{O}_{K'} \arrow[r] & \operatorname{Spec} \mathcal{O}_K
\end{tikzcd}$$

$\square$

16/03

Andrea Gallese

Setup As usual

Main objective

Prop. 6.2 ① v finite place of K, $v \nmid n$ or $v = \infty$

$$H^1(K, E)[p] \xrightarrow{\text{Res}} H^1(K_v, E)[p]$$
$$d(n) \longmapsto 0$$

② $n = \ell m$, λ l'unico primo di K sopra ℓ

$$H^1(K, E)[p] \xrightarrow{\text{Res}} H^1(K_\lambda, E)[p]$$
$$d(n) \longmapsto 0 \iff P_m \in p\,E(K_\lambda)$$

$$\begin{array}{ccl} K_n & \lambda_n & \\ | & | & \text{tot ramified} \\ K_m & \lambda_m^{(1)} \cdots \lambda_m^{(r)} & \\ | & | & \text{tot split} \\ K & \lambda & \\ | & | & \text{inert} \\ \mathbb{Q} & \ell & \end{array}$$

It suffices to show that $\widetilde{d(n)} \in H^1(K_n/K, E)$ localises to 0

By inf-res,

$$0 \to H^1(K_n/K, E)[p] \longrightarrow H^1(G_\ell, E)[p]$$

Recall that (as a cocycle)

$$\widetilde{d}(n) : G_\ell \longrightarrow E(K_n)$$
$$\sigma \longmapsto \frac{1}{p}(\sigma - 1) P_n$$

Formal groups $\quad y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}_\ell$

$z = -x/y, \quad w = -1/y \quad \rightsquigarrow \quad w = z^3 + w^2 Az + Bw^3$

$\Rightarrow \quad w = w(z) \in \mathbb{Q}_\ell[[z]]$

$x(z) = z/w(z)$

$y(z) = -1/w(z)$

Let Φ_+ be the rat. funct. giving $-x/y$ (sum of pts)

$\rightsquigarrow F(z_1, z_2) = \Phi_+\big((x(z_1), y(z_1)), (x(z_2), y(z_2))\big)$

Fact ① This gives a formal group $\hat{E}$.

max ideal

② $\{P \in E(\mathcal{O}_{K_\lambda}) : \pi(P) = O_{\tilde{E}}\} \simeq \hat{E}(\mathcal{M})$

$(x,y) \longmapsto -x/y$

③ $\hat{E} \xrightarrow{[p]} \hat{E}$ (formally); $[p](T) = pT + O(T^2)$

has a formal inverse $\rightsquigarrow$ $[p]$ invertible in $\hat{E}(\mathcal{M})$

Let $\mathcal{E}$ be a Néron model for E/K_λ.

$$0 \longrightarrow \hat{E}(\mathcal{M}_\lambda) \longrightarrow \mathcal{E}(\mathcal{O}_{K_\lambda}) \longrightarrow \tilde{\mathcal{E}}(\mathcal{O}/\lambda) \longrightarrow 0$$

Taking cohomology,

$$\begin{tikzcd}
 & & 0 \arrow[d] \\
0 \arrow[r] \arrow[d] & H^1(G_\ell, E(K_{\lambda_m}))[p] \arrow[r] \arrow[d] & H^1(G_\ell, \tilde{\mathcal{E}}(\mathcal{O}/\lambda_m))[p] \arrow[d] \\
H^1(G_\ell, \hat{E}(\mathcal{M}_{\lambda_m})) \arrow[r] \arrow[d, "p"] & H^1(G_\ell, E(K_{\lambda_m})) \arrow[r] \arrow[d, "p"] & H^1(G_\ell, \tilde{E}(\mathcal{O}/\lambda_m)) \arrow[d, "p"] \\
H^1(G_\ell, \hat{E}(\mathcal{M}_{\lambda_m})) \arrow[r] \arrow[d] & H^1(G_\ell, E(K_{\lambda_m})) \arrow[r] & H^1(G_\ell, \tilde{E}(\mathcal{O}/\lambda_m)) \\
0 & &
\end{tikzcd}$$

In partic., it suffices to show that $\tilde{\delta}(n)$ goes to 0 in $H^1(G_\ell, \tilde{\mathcal{E}}(\mathcal{O}_{K_{\lambda_n}}/\lambda_n))$. Let $F_{\lambda_n} = \mathcal{O}_{K_{\lambda_n}}/\lambda_n = \mathcal{O}_K/\lambda$ be the residue field.

Let $Q_n := \dfrac{(\sigma_\ell - 1) P_n}{p} \in \mathcal{E}(\mathcal{O}_{K_n})$, $\quad \tilde{Q}_n \in \mathcal{E}(F_{\lambda_n})$

Recall that $P_n = \sum_{\sigma \in \mathcal{G}_n/G_n} \sigma D_n D_\ell \, y_n$

with $(\sigma_\ell - 1) D_\ell = (\ell+1) - \mathrm{Tr}_\ell$

So

$$(\sigma_\ell - 1) P_n = \sum_\sigma \sigma D_n \left[(\ell+1) - \mathrm{Tr}_\ell \right] y_n$$

$$= \sum_\sigma \sigma D_m \left[(\ell+1)\, y_n - a_\ell\, y_m \right]$$

and $\ell+1 \equiv 0 \equiv a_\ell \pmod{p}$, so

$$\left(\frac{K_{\lambda_m}/\mathbb{Q}}{\lambda_m} \right)$$

$$Q_n = \sum_\sigma \sigma D_m \left[\frac{\ell+1}{p}\, y_n - \frac{a_\ell}{p}\, y_m \right]$$

We also saw (?) $\quad y_n \equiv \mathrm{Frob}(\lambda_m) \cdot y_m \pmod{\lambda_n}$

Reducing mod λ_n,

$$\tilde{Q}_n \equiv \sum_\sigma \sigma D_m \left[\frac{\ell+1}{p} \mathrm{Frob}(\lambda_m) - \frac{a_\ell}{p} \right] \cdot y_m \pmod{\lambda_n}$$

$$\equiv \left[\frac{\ell+1}{p} \mathrm{Frob}(\lambda_m) - \frac{a_\ell}{p} \right] \sum_\sigma \sigma D_m\, y_m \pmod{\lambda_n}$$

$$\equiv \underbrace{\left(\frac{\ell+1}{p} \, \mathrm{Frob}(\lambda_m) - \frac{a_\ell}{p} \right)}_{\alpha,\ \text{non-trivial endom. of } \tilde{E}} \tilde{P}_m \pmod{\lambda_n}$$

Let's work with the $\pm$ - eigenspaces of $\mathrm{Frob}(\lambda_m)$

we don't quite know why

$$\begin{tikzcd}
0 \arrow[r] & \tilde{E}(F_\lambda)[p] \arrow[r] \arrow[d, "?"'] & \tilde{E}(F_\lambda)^+ \arrow[r, "p"] \arrow[d, "\alpha"] \arrow[dr, "0"] & \tilde{E}(F_\lambda)^+ \arrow[d, "\alpha"] \\
0 \arrow[r] & \tilde{E}(F_\lambda)[p] \arrow[r] & \tilde{E}(F_\lambda)^+ \arrow[r, "p"] & \tilde{E}(F_\lambda)^+
\end{tikzcd}$$

$$\alpha \circ [p] \big|_{\tilde{E}^+} = (\ell+1) - a_\ell = [\deg(1 - \mathrm{Frob})]$$

$$= [\# \tilde{E}^+] = [0]$$

$$\tilde{E}^+ = \tilde{E}[1 - \mathrm{Frob}]$$

Look at snake diagram, obtain

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & \ker \alpha \arrow[r] \arrow[d] & \ker \alpha \cap p\tilde{E} \arrow[d, hook] \arrow[dddll, dashed, bend left] \\
\tilde{E}[p]^+ \arrow[r] \arrow[d, "\alpha"] & \tilde{E}^+ \arrow[r] \arrow[d, "\alpha"] & p\tilde{E}^+ \arrow[d, "\alpha"] \\
\tilde{E}[p]^+ \arrow[r] \arrow[d] & \tilde{E}^+ \arrow[r, "p"'] & p\tilde{E}^+ \\
0 & &
\end{tikzcd}$$

Hence $\ker \alpha \big|_{E^\pm} = p\tilde{E}^\pm \Rightarrow \ker \alpha = p\tilde{E}(F_\lambda)$.

So, $d(n)_\nu$ trivial $\Leftrightarrow$ $\tilde{Q}_n$ trivial $\Leftrightarrow$ $\tilde{P}_m \in p\tilde{E}(F_\lambda)$

Now consider again

$$\begin{tikzcd}
\hat{E}(\mathcal{M}_{\lambda_m}) \arrow[r] \arrow[d, "{[p]}"', "2"] & \tilde{E}(\mathcal{O}_{K_{\lambda_m}}) \arrow[r] \arrow[d, "p"] & \tilde{\mathcal{E}}(F_\lambda) \arrow[r] \arrow[d, "{[p]}"] & 0 \\
\hat{E}(\mathcal{M}_{\lambda_m}) \arrow[r] \arrow[d] & \tilde{E}(\mathcal{O}_{K_{\lambda_m}}) \arrow[r] \arrow[d] & \tilde{\mathcal{E}}(F_\lambda) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E/pE \arrow[r] & \tilde{E}/p\tilde{E} \arrow[r] & 0
\end{tikzcd}$$

and therefore $\tilde{P}_m \in p\tilde{E}(F_\lambda) \iff P_m \in pE(F_\lambda)$

Let's now turn to the finite places $\nmid n$, and $\nu = \infty$.

- $\nu = \infty$ is trivial, b/c $H^1(\mathbb{C}, E) = (0)$

- $v \nmid n$, of good reduction (i.e. $v \nmid N$)

It suffices to look at $H^1(\mathrm{Gal}(K_v^{nr}/K_v), E)[p]$
(inflation)

$$0 \longrightarrow H^1(\mathrm{Gal}(K_v^{nr}/K_v), E)[p] \xrightarrow{\sim} H^1(\mathrm{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v), \tilde{E})[p]$$

$$\| \\ (0)$$

Lang's isogeny thm
or
homog. spaces w/ a rat'l pt

30/03/2023
L. Speciale

Tate pairing

$K/\mathbb{Q}_\ell$ finite, $F = \mathcal{O}_K/(\pi_K)$, $G_K = Gal(\overline{K}/K)$

$\mathfrak{g} = Gal(K^{nr}/K) = Gal(\overline{F}/F)$, $p \neq \ell$ prime

E/K an ell. curve with good reduction

<u>Aim</u> Construct $H^i(G_K, E_p) \otimes H^{2-i}(G_K, E_p) \to \mathbb{Z}/p\mathbb{Z}$ $\quad i = 0, 1$

$$\begin{array}{ccccc} \cup\!\! \mid & & \| & & \\ E(K)/pE(K) & \times & H^1(G_K, E_p) & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \quad (i=1) \end{array}$$

Lemma Let A be a topological $\mathfrak{g}$-mod. Suppose one of the following holds:

1) A is torsion

2) A is divisible and $A^{\mathfrak{g}}$ is torsion

Then

$$H^r(\mathfrak{g}, A) = \begin{cases} A^{\mathfrak{g}} & \text{for } r = 0 \\ A/(\mathrm{Frob}-1)A & \text{for } r = 1 \\ 0 & \text{for } r \geq 2 \end{cases}$$

if time permits...

Pf Later; based on the 2-periodicity of cohomology for cyclic groups. $\square$

Starting from $0 \to \tilde{E}_p(\bar{F}) \longrightarrow \tilde{E}(\bar{F}) \longrightarrow \tilde{E}(\bar{F}) \longrightarrow 0$

and taking cohomology,

$$0 \to \tilde{E}(F)/p\,\tilde{E}(F) \xrightarrow{\sim} H^1(\mathfrak{g}, E_p(\bar{F})) \to \overset{\overset{(0)}{\parallel\ \star}}{H^1(\mathfrak{g}, E(\bar{F}))}$$

$\circledast$ holds by Lang's thm or by the lemma.

Thm (Tate pairing) For $i=0,1,2$ $H^i(G_k, E_p(\bar{k}))$ is finite and $H^i(G_k, E_p) \otimes H^{2-i}(G_k, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$ (induced by the cup-product) is a perfect pairing.
(+ Weil pairing & CFT)

Cup product $H^1(G_k, E_p) \otimes H^1(G_k, E_p) \xrightarrow{\cup} H^1(G_k, E_p \otimes E_p)$

Weil pairing $E_p \times E_p \longrightarrow \mu_p$ G_k-equivariant

$\rightsquigarrow$ $w: E_p \otimes E_p \longrightarrow \mu_p$ $\rightsquigarrow$ $w_* : H^2(G_k, E_p^{\otimes 2}) \to H^2(G_k, \mu_p)$

CFT The Kummer sequence

$$0 \to \mu_p(\bar{k}) \longrightarrow \mathbb{G}_m(\bar{k}) \xrightarrow{\wedge p} \mathbb{G}_m(\bar{k}) \longrightarrow 1$$

gives $\quad 0 = H^1(K, \overline{K}) \longrightarrow H^2(K, \mu_p) \longrightarrow H^2(K, \mathbb{G}_m) \xrightarrow{[p]} H^2(K, \mathbb{G}_m)$

$$\Rightarrow \quad H^2(K, \mu_p) \simeq H^2(K, \mathbb{G}_m)[p] = Br(K)[p] \simeq \mathbb{Z}/p\mathbb{Z}$$

Prop. $H^1(\mathfrak{g}, E_p)$ is naturally a submodule of $H^1(G_K, E_p)$ and is isotropic wrt the Weil pairing.

Pf $\quad$ Inf gives an injection

$$H^1(\mathfrak{g}, E_p) = H^1(\mathfrak{g}, E_p^{I}) \xhookrightarrow{\text{Inf}} H^1(G_K, E_p)$$

inertia

by Néron - Ogg - Shafarevich

$$\begin{tikzcd}
H^1(\mathfrak{g}, E_p)^{\otimes 2} \arrow[r, "\mathrm{Inf}"] \arrow[d, "\cup"] & H^1(G_k, E_p)^{\otimes 2} \arrow[d, "\cup"] \\
H^2(\mathfrak{g}, E_p) \arrow[r, "\mathrm{Inf}"] \arrow[d, "w_*"] \arrow[dr, phantom, "\circlearrowright"] & H^2(G_k, E_p) \arrow[d, "w_*"] \\
H^2(\mathfrak{g}, \mu_p) \arrow[r] \arrow[d, equal] & H^2(G_k, \mu_p) \\
0 &
\end{tikzcd}$$

by the lemma, or since $Br(\text{finite field}) = 0$ ◻

Thm 2 (Restricted Tate pairing) The Tate pairing induces a non-degenerate pairing of $\mathbb{F}_p$-vector spaces (of dim ≤ 2)

$$\frac{E(k)}{pE(k)} \times H^1(G, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

Pf. $\quad \dfrac{E(K)}{pE(K)} \simeq H^1(\mathfrak{g}, E_p) \subseteq H^1(G_K, E_p)$

$$\begin{tikzcd}
\overline{K} \arrow[dash, dr, "\mathcal{L}"] \arrow[dash, dd, "I"'] & \\
 & K^{tame} \arrow[dash, dl, "\Delta"] \\
K^{nr} \arrow[dash, d, "\mathfrak{g} = \hat{\mathbb{Z}}"] & \\
K &
\end{tikzcd}$$

$\mathcal{L}$ — wild inertia, pro-ℓ

$$\Delta \simeq \prod_{p \neq \ell} \mathbb{Z}_p$$

Inf-Res for $I \trianglelefteq G_K$ gives

$$0 \to H^1(\mathfrak{g}, E_p) \to H^1(G_K, E_p) \to H^1(I, E_p)^{\mathfrak{g}} \to H^2(\mathfrak{g}, E_p) = (0)$$

$$\begin{tikzcd}
0 \arrow[r] & \frac{E(k)}{pE(k)} \arrow[r] \arrow[d, "\wr"] & H^1(G_k, E_p) \arrow[r] \arrow[d, "="] & H^1(G_k, E)[p] \arrow[r] \arrow[d, dotted, "\wr"] & 0 \\
0 \arrow[r] & H^1(\mathfrak{g}, E_p) \arrow[r] & H^1(G_k, E_p) \arrow[r] & H^1(I, E_p)^{\mathfrak{g}} \arrow[r] & 0
\end{tikzcd}$$

both are the cokernel of the same map

On the other hand, from

$$1 \longrightarrow \mathcal{L} \longrightarrow I \longrightarrow \Delta \longrightarrow 1$$

we get

$$0 \to H^1(\Delta, E_p^{\mathcal{L}}) \xrightarrow{\text{Inf}} H^1(I, E_p) \xrightarrow{\text{Res}} H^1(\mathcal{L}, E_p)^{\Delta}$$

Now $H^1(\mathcal{L}, E_p) = \mathrm{Hom}_{\mathrm{cont}}(\underset{\text{pro-}\ell}{\mathcal{L}}, \underset{p\text{-torsion}}{E_p}) = (0)$, so $H^1(I, E_p)^{\mathfrak{g}}$

$$\downarrow \wr$$

$$H^1(\Delta, E_p^{\mathcal{L}})^{\mathfrak{g}}$$

On the other hand,

- $$H^1(\Delta, E_p^{\mathcal{L}})^{\mathcal{G}} = \mathrm{Hom}(\Delta, E_p)^{\mathcal{G}} = \mathrm{Hom}\Big(\prod_{q \neq \ell} \mathbb{Z}_q, E_p\Big)^{\mathcal{G}}$$
$$= \mathrm{Hom}(\mathbb{Z}_p, E_p)^{\mathcal{G}}$$
has $\mathbb{F}_p$-dim ≤ 2.

- $$H^1(\mathcal{G}, E_p) \simeq \frac{E_p(\bar{k})}{(\mathrm{Frob}-1)\, E_p(\bar{k})}.$$

$$\dim_{\mathbb{F}_p}\big((\mathrm{Frob}-1)\, E_p(\bar{k})\big) = \dim \mathrm{Imm}(\mathrm{Frob}-1)$$
$$= 2 - \dim \ker(\mathrm{Frob}-1)$$
$$= 2 - \dim E_p(\mathbb{F}_\ell) \leq 2.$$

Finally, has Tate-dual

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{E(K)}{pE(K)} \arrow[r] \arrow[d, hook, "\circledast"'] & H^1(G_K, E_p) \arrow[r] \arrow[d, "\wr", "\circledast_2"'] & H^1(G_K, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \left(H^1(G_K, E)[p]\right)^T \arrow[r] & \left(H^1(G_K, E_p)\right)^T \arrow[r] & \left(\dfrac{E(K)}{pE(K)}\right)^T \arrow[r] & 0
\end{tikzcd}$$

$\circledast$ is defined by isotropy. For dimensional reasons, it's an isomorphism

$\circledast_2$ is the unrestricted Weil pairing

We will relate the Tate pairing to the Weil pairing more explicitly next time. (Se Giulio e' d'accordo...)

Lemma Let A be a topological $\mathfrak{g}$-mod. Suppose one of the following holds:

1) A is torsion

2) A is divisible and $A^{\mathfrak{g}}$ is torsion

Then
$$H^r(\mathfrak{g}, A) = \begin{cases} A^{\mathfrak{g}} & \text{for } r=0 \\ A/(\mathrm{Frob}-1)A & \text{for } r=1 \\ 0 & \text{for } r\geq 2 \end{cases}$$

Pf Let $D = \mathrm{Frob}-1$, $N_n = \sum_{j=1}^{n} \mathrm{Frob}^j : A \longrightarrow A$

Let $\mathfrak{g}_n = \mathfrak{g} / \overline{\langle \mathrm{Frob}^n \rangle}$. We have $H^i(\mathfrak{g}, A) = \varinjlim H^i(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n})$

The cohomology of the cyclic group $\mathfrak{g}/\mathfrak{g}_n$ is computed by

$$\begin{tikzcd}
0 \arrow[r] & A^{\mathfrak{g}_n} \arrow[r, "D"] \arrow[d, "1"'] \arrow[dr, phantom, "\circlearrowleft"] & A^{\mathfrak{g}_n} \arrow[r, "N_n"] \arrow[d, "1"'] \arrow[dr, phantom, "\circlearrowleft"] & A^{\mathfrak{g}_n} \arrow[r, "D"] \arrow[d, "m"'] \arrow[dr, phantom, "\circlearrowleft"] & A^{\mathfrak{g}_n} \arrow[r] \arrow[d, "m"'] \arrow[dr, phantom, "\circlearrowleft"] & A^{\mathfrak{g}_n} \arrow[d, "m^2"'] \\
0 \arrow[r] & A^{\mathfrak{g}_{nm}} \arrow[r, "D"'] & A^{\mathfrak{g}_{nm}} \arrow[r, "N_{nm}"'] & A^{\mathfrak{g}_{nm}} \arrow[r, "D"'] & A^{\mathfrak{g}_{nm}} \arrow[r, "N_{nm}"'] & A^{\mathfrak{g}_{nm}}
\end{tikzcd}$$

$$N_{nm} \circ 1 \underset{\substack{\cap \\ A^{\mathfrak{g}_n}}}{(a)} = \sum_{i=1}^{mn} \mathrm{Frob}^i a = m \sum_{i=1}^{n} \mathrm{Frob}^i a = m N_n (a)$$

* $r=0$: the claim is Trivial

* $r \geq 2$: if A is finite, $m = \# A$, the transition map induced by $\begin{array}{ccc} A^{\mathfrak{g}_n} & \xrightarrow{[m]} & A^{\mathfrak{g}_{nm}} \\ a & \longmapsto & 0 \end{array}$ is 0, so $H^r(G,A)=(0)$

if A is torsion: write it as $A = \varinjlim_{\alpha} A_\alpha$ w/ A_α finite & $\mathfrak{g}$-invariant, pass to the limit.

if A is divisible: $\quad 0 \to A_n \to A \xrightarrow{[n]} A \to 0$

and for $r \geq 2$ $\quad H^r(A_n) = 0 \to H^r(A) \xrightarrow{[n]} H^r(A) \to H^{r+1}(A_n) = 0$

$\Rightarrow H^r(A)$ doesn't have nontrivial torsion elements,

but is torsion $\quad \Rightarrow H^r(A) = (0)$

* $r=1$: $\quad H^1(\mathfrak{g}, A) = \varinjlim H^1(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) \simeq \dfrac{\ker N_n}{I_{\mathfrak{g}_n} A^{\mathfrak{g}_n}}$

with $I_{\mathfrak{g}_n} = (\mathrm{Frob} - 1) \subseteq \mathbb{Z}[G]$

It suffices to show that $\forall a \in A \ \exists n$ st $a \in \ker N_n$, which is easy: if $N_{n_k}(a) = a$, $a \in A^{\Gamma_k} \subset A^{\Gamma}$,

which " torsion. Hence $m_0 N_n a = N_{m_0 n}(a) = 0$,

of order m_0

so $\varinjlim A^{\Gamma_n} = A$

13/04/2023
G. Grammatica

Recap

$$\langle\ ,\ \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow H^2(K_\lambda, \mu_\ell) \xrightarrow[\text{inv}]{\sim} \mathbb{Z}/p\mathbb{Z}$$

$$[f] \qquad [g] \longmapsto \big((\sigma,\tau) \mapsto \{f(\sigma), \sigma(g(\tau))\}\big)$$

$$0 \to \underbrace{E(K_\lambda)/pE(K_\lambda)}_{\text{isotropic for } \langle\ ,\ \rangle} \longrightarrow H^1(K_\lambda, E_p) \longrightarrow H^1(K_\lambda, E)_p \longrightarrow 0$$

Abststractly, given ① $\langle\ ,\ \rangle : B \times B \longrightarrow \mathbb{Z}/p\mathbb{Z}$, $A \subset B$ isotropic

$$\rightsquigarrow \quad ② \ \langle\ ,\ \rangle : A \times B/A \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

② non-degenerate $\Leftrightarrow$ ① non-deg. (Tate) + $\dim A = \dim B/A$.

In our world, $A = E(K_\lambda)/pE(K_\lambda)$

$B = H^1(K_\lambda, E)_p$

Now $H^1(K_\lambda, E)_p \simeq H^1(I, E_p)^{\mathrm{Frob}} \simeq \mathrm{Hom}(I, E_p)^{\mathrm{Frob}}$

$\simeq \mathrm{Hom}(\Delta, E_p)^{\mathrm{Frob}}$

where $1 \to P \longrightarrow I \longrightarrow \Delta \longrightarrow 0$

P ↳ wild subgp, Δ ↳ tame quot

Moreover, $\Delta \simeq \prod_{q \neq \ell} \mathbb{Z}_q(1)$, so

$$\mathrm{Hom}(\Delta, E_p)^{\mathrm{Frob}} = \mathrm{Hom}(\mu_p, E_p)^{\mathrm{Frob}}.$$

where $\mu_p = \mathrm{Gal}\left(K_\lambda^{nr}(\pi^{1/p}) / K_\lambda^{nr}\right)$

Let $K_p := K_\lambda(\pi^{1/p}, \zeta^{1/p})$. Then, an element in $\mathrm{Hom}(\mu_p, E_p)^{\mathrm{Frob}}$

comes from an element in $\mathrm{Hom}\left(\mathrm{Gal}(K_p/K_\lambda), E_p\right)^{\mathrm{Frob}}$

[Since $\mathrm{Gal}\left(K_\lambda^{nr}(\pi^{1/p}) / K_\lambda^{nr}\right) \hookrightarrow \mathrm{Gal}(K_p/K_\lambda)$, we get a surjective map on Homs]

ASSUME $E_p(\overline{K_\lambda}) = E_p(K_\lambda)$

We now compute the restricted Tate pairing explicitly.

$$\langle\ ,\ \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow H^2(K_\lambda, \mu_p) \xrightarrow{\text{inv}} \mathbb{Z}/p\mathbb{Z}$$

$$\underset{\substack{\cup\\ c_1}}{E(K_\lambda)/pE(K_\lambda)} \times \underset{\substack{\cup\\ c_2}}{H^1(K_\lambda, E)_p} \longrightarrow H^2(K, \mu_p) \simeq \mathbb{Z}/p\mathbb{Z}$$

$$c_1 \overset{\text{lifts to}}{\rightsquigarrow} \varphi_1 : \sigma \longmapsto \sigma\left(\frac{1}{p}c_1\right) - \frac{1}{p}c_1$$

$$c_2 \rightsquigarrow \varphi_2 : \mathrm{Gal}(K_p/K_\lambda) = G_p \longrightarrow E_p$$

Then, $\langle c_1, c_2 \rangle = \mathrm{inv}(B)$, where B is the 2-cocycle

$$B(\sigma, \tau) = \{ \varphi_1(\sigma), \varphi_2(\tau) \}$$

We will make this explicit.

Notation K ℓ-adic field, $\mathbb{F}$ residue field, $p \mid \#\mathbb{F} - 1$,

ξ a $(\#\mathbb{F}-1)$-th root of unity, $\zeta = \xi^{\left(\frac{\#\mathbb{F}-1}{p}\right)}$

Thm (local class field, Artin reciprocity form)

$\exists\ \theta : K^\times \hookrightarrow \mathrm{Gal}(K^{ab}/K)$ s.t.

1. $\forall L/K$ unramified, $\forall \pi$ uniformiser, $\vartheta(\pi)|_L = \mathrm{Frob}_{L/K}$
2. $\forall L/K$ finite abelian, ϑ induces an isomorphism

$$\vartheta : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

Rmk $K^\times \simeq \mathbb{Z} \times \mathcal{O}_K^\times$

Recall $K_p = K(\pi^{1/p}, \xi^{1/p})$

$$\vartheta : K^\times / N_{K_p/K}(K_p^\times) \xrightarrow{\sim} \mathrm{Gal}(K_p/K) =: G_p$$

One can check that the norm group is $(K^\times)^p$. In fact,

$$F : \quad K^\times / K^{\times p} \simeq H^1(K, \mu_p) \simeq \mathrm{Hom}(G_K, \mu_p) = \mathrm{Hom}(G_p, \mu_p)$$

$$a \qquad\qquad f_a(\sigma) = \frac{\sigma(a^{1/p})}{a^{1/p}}$$

Def (Hilbert symbol)

$$(\ , \ ) : K^\times / K^{\times p} \times K^\times / K^{\times p} \longrightarrow \mu_p$$

$$(a, b) \longmapsto \frac{\vartheta(a)(b^{1/p})}{b^{1/p}}$$

It's bilinear (easy), non-degenerate (it's the natural pairing between G_p and its dual), and alternating (admitted).

$$(\pi, \pi) = 1 \qquad (\pi, \xi) = \frac{\vartheta(\pi)(\xi^{1/p})}{\xi^{1/p}} = \xi^{\frac{\#\mathbb{F}-1}{p}} = \zeta$$

$$(\xi, \xi) = 1 \qquad (\xi, \pi) = (\pi, \xi)^{-1}$$

We give another interpretation, which makes it easier to see that it is alternating

$$\begin{array}{ccccccc}
K^\times/K^{\times p} & \times & K^\times/K^{\times p} & & & & \\
\| & & \| & & & & \\
H^1(K,\mu_p) & \times & H^1(K,\mu_p) & \longrightarrow & H^2(K,\mu_p\otimes\mu_p) & \overset{\mathrm{inv}\otimes\mathrm{id}}{\simeq} & \mu_p
\end{array}$$

$$\begin{array}{ccccc}
H^2(K,\mu_p) & \otimes & H^0(K,\mu_p) & \xrightarrow{\sim} & H^2(K,\mu_p\otimes\mu_p) \\
\wr\| \, \mathrm{inv} & & \| & & \\
\mathbb{Z}/p\mathbb{Z} & \otimes & \mu_p & \simeq & \mu_p
\end{array}$$

Thm This second pairing is also the Hilbert symbol.

Comparing the two descriptions, we get an explicit formula for the invariant of (certain) 2-cocycles

Let's make this explicit.

$$a, b \in K^\times/K^{\times p} \times K^\times/K^{\times p} \longrightarrow H^2(K, \mu_p \otimes \mu_p) \simeq \mu_p$$

$$\begin{tikzcd}
K^\times/K^{\times p} \times K^\times/K^{\times p} \arrow[r] \arrow[d, "F \times F"] & H^2(K, \mu_p \otimes \mu_p) \simeq \mu_p \\
H^1(K, \mu_p) \otimes H^1(K, \mu_p) \arrow[d, phantom, "\wr"] & \\
H^1(G_p, \mu_p) \otimes H^1(G_p, \mu_p) \arrow[r] & H^2(G_p, \mu_p \otimes \mu_p) \arrow[uu] \underset{\text{non-can.}}{\simeq} H^2(G_p, \mu_p)
\end{tikzcd}$$

$\delta_a, \delta_b \in H^1(K, \mu_p) \otimes H^1(K, \mu_p)$

[since G_p is the largest p-group quotient of $\mathrm{Gal}(\bar{K}/K)$]

Write $\delta_a = \zeta^{\phi_a}$, $\delta_b = \zeta^{\phi_b}$

Using ζ as generator of μ_p, we get a commutative diagram

$$
\begin{tikzcd}
H^2(K, \mu_p \otimes \mu_p) \arrow[d, "\mathrm{id} \otimes \mathrm{inv}"'] \arrow[dr, phantom, "\circlearrowright"] & H^2(K, \mu_p \otimes \mathbb{Z}/p\mathbb{Z}) \arrow[l, "\sim"'] \arrow[d, "\mathrm{inv}"] \\
\mu_p & \mathbb{Z}/p\mathbb{Z} \arrow[l, "\sim"']
\end{tikzcd}
\tag{$\star$}
$$

Now $\delta_a \cup \delta_b$ is the 2-cocycle

$$\delta_a(\sigma) \otimes \delta_b(\tau) = \zeta^{\phi_a(\sigma)} \otimes \zeta^{\phi_b(\tau)}$$

Via the non-canonical iso $\mu_p \otimes \mu_p \xrightarrow{\sim} \mu_p$, this yields the 2-cocycle $(\sigma, \tau) \longmapsto \zeta^{\phi_a(\sigma)\phi_b(\tau)}$

Commutativity of $\circledast$ then gives

$$\boxed{\zeta^{\mathrm{Inv}(B_{a,b})} = (a,b)}$$

where $B_{a,b}$ is $(\sigma,\tau) \longmapsto \zeta^{\phi_a(\sigma)\phi_b(\tau)}$

We now compute a specific $B_{a,b}$: $a = \xi$, $b = \pi$

$$B_{\xi,\pi}\big(\theta(\pi), \theta(\pi)\big) = 1 \qquad B_{\xi,\pi}\big(\theta(\xi), \theta(\pi)\big) = 1$$

$$B_{\xi,\pi}\big(\theta(\pi), \theta(\xi)\big) \qquad B_{\xi,\pi}\big(\theta(\xi), \theta(\xi)\big) = 1$$

Now $\zeta^{\phi_b(\theta(a))} = f_b(\theta(a)) = (a,b)$

Hence $\xi^{\phi_\pi(\theta(\pi))} = (\pi,\pi) = 1$, and similarly $\xi^{\phi_\xi(\theta(\xi))} = 1$, which gives the three trivial results.

The remaining one is

$$\left(\xi^{\phi_\pi(\theta(\xi))}\right)^{\phi_\xi(\theta(\pi))} = (\xi,\pi)^{\phi_\xi(\theta(\pi))}$$
$$= \left(\xi^{\phi_\xi(\theta(\pi))}\right)^{-1} = (\pi,\xi)^{-1} = \xi^{-1}$$

Conclusion: $\mathrm{inv}(B_{\xi,\pi}) = -1$

$$\left(\text{since } \xi^{\mathrm{inv}(B_{a,b})} = (a,b)\right)$$

We can finally compute the invariant of the cocycle $B(\sigma, \tau)$ which appears in the restricted Weil pairing.

Recall: we have $\varphi_1, \varphi_2 \in H^1(K_\lambda, E_p) = \mathrm{Hom}(G_p, E_p)$

Here • $\varphi_2(\theta(\pi)) = 0$, $\varphi_2(\theta(\xi)) =$ something, let's call it e_2

• $\varphi_1(\theta(\pi)) = e_1$, $\varphi_2(\theta(\xi)) = 0$ (inertia acts trivially)

Finally, $\langle C_1, C_2 \rangle = \mathrm{Inv}\, B(\sigma, \tau)$, $B(\sigma, \tau) = \{\varphi_1(\sigma), \varphi_2(\tau)\}$

As before, $B(\theta(\pi), \theta(\pi)) = 1$ $\quad B(\theta(\pi), \theta(\xi)) = \{e_1, e_2\} = \zeta^x$

$B(\theta(\xi), \theta(\pi)) = 1$ $\quad B(\theta(\xi), \theta(\xi)) = 1$

Hence $B(\sigma, \tau) = B_{\xi, \pi}^{-x}$

$$\zeta^{\langle c_1, c_2 \rangle} = \zeta^{\mathrm{inv}\, B} = \left(\zeta^{\mathrm{inv}\, B_{\xi,\pi}} \right)^{-x} = \zeta^{x} = \{e_1, e_2\}$$

(Note that e_2 depends on the choice of ξ !)

From here, it's not hard to show that $\langle\, ,\, \rangle$ is non-degenerate: if we let c_1, c_2 vary, e_1, e_2 vary among all p-torsion pts.