TALK 9 :- OBSTRUCTIONS TO GLOBAL POINTS ON X^D

§0 RECAP OF LAST TALK

D be a division algebra over $F = \mathbb{F}_q(t)$, $p \in R = \mathrm{Bad}(D)$ s.t. $\mathrm{inv}(D_p) = \frac{1}{d}$. K/F be a deg. d ext'n.

$\underline{\mathcal{E}}$ be a sound D-elliptic sheaf over K of generic characteristic

$$\rho_{\underline{\mathcal{E}},p} : \Gamma_K^{ab} \longrightarrow \mathbb{F}_p^{(d)}$$

be the associated canonical isogeny character. Upon choosing a uniformizer of $\mathcal{O}_v$ (v a place of K), we have

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_v^\times \arrow[r] \arrow[d, "\wr", "\omega_v|\mathcal{O}_v^\times"'] & K_v^\times \arrow[r, "\deg_v"] \arrow[d, "\omega_v"] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & I_v \arrow[r] & G(K_v^{ab}|K_v) \arrow[r] & G(K_v^{ur}|K_v) \arrow[r] & 1
\end{tikzcd}$$

where ω_v is the local Artin map.

Let $\widetilde{r}_{\underline{\varepsilon},P}(v) := \rho_{\underline{\varepsilon},P} \circ \omega_v$,

$$r_{\underline{\varepsilon},P}(v) := \widetilde{r}_{\underline{\varepsilon},P} \big|_{\mathcal{O}_v^\times}.$$

Also set $n := l_q(d) \left(\dfrac{d^2}{\text{g.c.d}(d^2, q^d - 1)} \right)$

THEOREM (Talk 8) (a) If $v \nmid P\infty$, then $r_{\underline{\varepsilon},P}(v)^n = \underline{1}$.

(b) If $v \mid \infty$, then $\widetilde{r}_{\underline{\varepsilon},P}(v)^n = \underline{1}$.

(c) If $v \mid P$ and q is a monic irreducible polynomial of A co-prime to P, then

$$r_{\underline{\varepsilon},P}(q^{-1})^n \equiv q^{n \frac{[K_v : F_P]}{d}} \pmod{P}$$

---

§1. A global property of $\rho_{\underline{\varepsilon},P}$

Assume further that K splits

D, i.e. $D \otimes_{\mathbb{P}} K \simeq M_d(K)$ and that there exists a place $\mathfrak{m} \in |X| \setminus (R \cup \{\infty\})$ which totally ramifies in K. $\tilde{\mathfrak{m}} | \mathfrak{m}$ be the unique place of K. Then by the theorem above, $\rho^n_{\underline{\mathcal{E}}, \mathbb{P}}$ is unramified at $\tilde{\mathfrak{m}}$, hence $\rho^n_{\underline{\mathcal{E}}, \mathbb{P}}(\mathrm{Fr}^d_{\tilde{\mathfrak{m}}})$ is independent of the choice of the Frobenius at $\tilde{\mathfrak{m}}$.

<u>Proposition</u>: $\rho^n_{\underline{\mathcal{E}}, \mathbb{P}}(\mathrm{Fr}^d_{\tilde{\mathfrak{m}}}) \equiv \mathfrak{m}^n \pmod{\mathfrak{p}}$

Pf: Compatibility of GCFT and LCFT is expressed as the commutative diagram

$$\begin{tikzcd}
K_{\tilde{\mathfrak{m}}}^{\times} \arrow[r] \arrow[d] & \Gamma_{K_{\tilde{\mathfrak{m}}}}^{ab} \arrow[d] \\
\mathbb{A}_K^{\times}/K^{\times} \arrow[r] & \Gamma_K^{ab}
\end{tikzcd}$$

where $\varpi_{\tilde{\mathfrak{m}}} \in K_{\tilde{\mathfrak{m}}}^{\times}$ maps to a Frobenius lift at $\tilde{\mathfrak{m}}$ in Γ_K^{ab} and to $(\dots, 1, \varpi_{\tilde{\mathfrak{m}}}, 1, \dots)$ in $\mathbb{A}_K^{\times}/K^{\times}$. Consequently, since $\varpi_{\tilde{\mathfrak{m}}}^d = u\mathfrak{m}$ for some $u \in \mathcal{O}_{\tilde{\mathfrak{m}}}^{\times}$, we have

$$\rho_{\underline{\varepsilon},p}^n(\mathrm{Fr}_{\tilde{\mathfrak{m}}}^d) = \rho_{\underline{\varepsilon},p}^n(\dots, 1, \varpi_{\tilde{\mathfrak{m}}}^d, 1, \dots)$$

$$= \rho_{\underline{\varepsilon},p}^n(\dots, \mathfrak{m}^{-1}, u, \mathfrak{m}^{-1}, \dots) = r_{\underline{\varepsilon},p}(\tilde{\mathfrak{m}})(u)^n \prod_{v \nmid \mathfrak{m}} \tilde{r}_{\underline{\varepsilon},p}(v)(\mathfrak{m}^{-1})^n$$

By the theorem above,

$$r_{\underline{\varepsilon},P}(\tilde{m})(u)^n = 1 \quad \&$$

$$r_{\underline{\varepsilon},P}(v)(m^{-1})^n = 1 \quad \forall v \nmid P$$

For any place $v \mid P$, we have

$$\begin{tikzcd}
D_P \arrow[d] & \mathrm{Br}(F_P) \arrow[r] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[K_v:F_P]}"] \\
D_P \otimes K_v & \mathrm{Br}(K_v) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Since K splits D, so does K_v split D_P, hence $d \mid [K_v : F_P]$ or $[K_v : F_P] = d$. In particular, $\exists!\ \mathfrak{P} \mid P$ in K. By theorem above,

$$r_{\underline{\varepsilon},P}(\mathfrak{P})(m^{-1})^n \equiv m^n \pmod{P}$$

$\blacksquare$

§2. Non-existence of $X^{P}(K)$-criteria

Def'n (a) Let $W(m)$ be the set of $\pi \in \bar{F}$ s.t.

(i) $[F(\pi) : F] = d$;

(ii) π is integral over A;

(iii) $N_{F(\pi)|F}(\pi) \in \mathbb{F}_q^{\times} m$;

(iv) there is a unique place $\tilde{\infty}$ over ∞ in $F(\pi)$.

(b) $P(m)$ be the set of primes in A dividing $N_{F(\pi)|F}(\pi^{dn} - m^{n})$ for some $\pi \in W(m)$.

Remark. (i) If $X^d + a_1 X^{d-1} + \cdots + a_d$ is the minimal polynomial of π, then $a_d = \mu m$ for some $\mu \in \mathbb{F}_q^{\times}$ and a Newton polygon argument shows that $\deg(a_i) \leq \dfrac{i}{d} \deg(a_d)$

$\forall\, 1 \le i \le d$.

(ii) When $d=2$, $m=t$, the above condition is also a sufficient condition to determine $W(t)$.

(iii) $P(m) = \phi \iff \pi^{dn} = m^n$ $\forall\, \pi \in W(m)$.

Due to (ii) & (iii), the authors could produce $p \notin P(t)$ via a PARI/GP code. For example

$$t^3+t^2+t+2,\ t^3+t^2+2t+1,\ t^5+2t+1 \notin P(t) \quad (q=3).$$

THEOREM 8.5 If we further assume that $\exists\, p \in R \setminus P(m)$ and that $F(\sqrt[d]{\mu m})$ does not split D, for all $\mu \in \mathbb{F}_q^\times$. Then

$$X_D(K) = \phi.$$

Pf. Suppose $X^D(K) \neq \phi \xrightarrow[\text{Talk 5}]{\text{Talk 4}}$

$\exists$ a $\mathcal{D}$-elliptic sheaf $\underline{\mathcal{E}}$ over K, of generic characteristic, and a totally ramified extension $L|K_{\tilde{m}}$ s.t. $\underline{\mathcal{E}}_{|L}$ admits a model $\underline{\mathcal{E}}_{\mathcal{O}_L}$. Denote by $\bar{\underline{\mathcal{E}}}$ its reduction to $\kappa_L = \mathbb{F}_m$.

In Talk 6, we had the map

$$i_p : G_{\mathbb{F}_m} \longrightarrow \mathrm{Aut}(T_p(\bar{\underline{\mathcal{E}}}))$$

and $P_{\bar{\underline{\mathcal{E}}}, \mathbb{F}_m}(X) = \mathrm{Nrd}(X - i_p(Fr_{\mathbb{F}_m}))$

Write its decomposition over $\bar{F}$ as $\prod_{i=1}^{d} (X - \pi_i)$. If $\pi \in \mathrm{End}(\bar{\underline{\mathcal{E}}})$ is the $|m|^{th}$-power Frobenius on $\bar{\underline{\mathcal{E}}}$, then by Cor. 5.7,

$P_{\underline{\bar{\mathcal{E}}}, \mathbb{F}_{\mathfrak{m}}}(X)$ is the minimal polynomial of π and consequently π as well as all the other π_i's lie in $W(\mathfrak{m})$.

By [Rei, Thm. 9.5], we have

$$P_{\underline{\bar{\mathcal{E}}}, \mathbb{F}_{\mathfrak{m}}^{(dn)}}(X) = \prod_{i=1}^{d} (X - \pi_i^{dn})$$

On the other hand, by Talk 8

$$P_{\underline{\bar{\mathcal{E}}}, \mathbb{F}_{\mathfrak{m}}^{(dn)}}(X) \equiv \prod_{j=0}^{d-1} \left(X - \rho_{\underline{\bar{\mathcal{E}}}, P}(\mathrm{Fr}_{\mathbb{F}_{\mathfrak{m}}}^{dn})^{|P|^j}\right) \pmod{P}$$

Since, there is $\mathcal{O}_D / P\mathcal{O}_D$-compatibility of isomorphisms

$$\begin{aligned} \underline{\mathcal{E}}_L[P](L^{sep}) &\simeq \underline{\mathcal{E}}_{\mathcal{O}_L}[P](\mathcal{O}_{L^{sep}}) \\ &\simeq \underline{\bar{\mathcal{E}}}[P](\bar{\mathbb{F}}_{\mathfrak{m}}), \end{aligned}$$

we have $\rho_{\underline{\mathcal{E}},p}(Fr_{\mathbb{F}_{\mathfrak{m}}}^{dn}) = \rho_{\underline{\mathcal{E}},p}(Fr_{\widetilde{\mathfrak{m}}}^{dn})$

In particular, using Prop. 8.1,

$$P_{\underline{\mathcal{E}},\mathbb{F}_{\mathfrak{m}}}^{dn}(X) \equiv \prod_{j=0}^{d-1}(X - \mathfrak{m}^n) \pmod{\mathfrak{p}}$$

$$\|$$

$\prod(X - \pi_i^{dn})$. So for each $1 \leq i \leq d$, there is a place $\mathfrak{P}_i \mid \mathfrak{p}$ in $F(\pi_i)$ s.t. $\pi_i^{dn} \equiv \mathfrak{m}^n \pmod{\mathfrak{P}_i}$, or

$\mathfrak{p} \mid N_{F(\pi_i)|F}(\pi_i^{dn} - \mathfrak{m}^n)$.

Since $\mathfrak{p} \notin P(\mathfrak{m})$, we have

$$\pi_i^{dn} = \mathfrak{m}^n.$$

If $P_{\underline{\mathcal{E}},\mathbb{F}_{\mathfrak{m}}}(X) = X^d + a_1 X^{d-1} + \cdots + a_d$,

then by Cor. 5.7, $\deg(a_i) \leq \frac{i}{d}\deg(a_d)$

and the $\mathfrak{m}$-adic Newton

polygon of the same polynomial gives $v_m(a_i) \geq 1 \quad \forall 1 \leq i < d$.

Since $N(\pi) \in \mathbb{F}_q^\times m$, $a_d = -\mu m$ for some $\mu \in \mathbb{F}_q^\times$. Hence $m \mid a_i$

$\Rightarrow \deg(a_i) \geq \deg(m)$. So for $0 < i < d$, $a_i = 0$.

So $P_{\underline{\xi}, \mathbb{F}_m}(X) = X^d - \mu m$

and $F(\pi) = F(\sqrt[d]{\mu m})$. By Thm. 4.13, $F(\sqrt[d]{\mu m}) = F(\pi) \hookrightarrow D$, contradicting that $F(\sqrt[d]{\mu m})$ doesn't split D $\blacksquare$

Example: $d = 2, q = 3, m = t$

Let D be the division algebra over F with $Bad(D) = \{p, q\}$, where p, q are co-prime monic irreducible polynomials chosen as follows :

(i) $P \notin P(t)$;

(ii) $\left(\left(\frac{t}{P}\right) \vee \left(\frac{t}{q}\right) = 1\right) \wedge \left(\left(\frac{-t}{P}\right) \vee \left(\frac{-t}{q}\right) = 1\right)$

where $\left(\frac{a}{h}\right)$ is the unique element in $\mathbb{F}_q^\times$ s.t. $a^{\frac{|h|-1}{2}} \equiv \left(\frac{a}{h}\right) \pmod{h}$ for $h \in A$ monic, irreducible.

Consequently, $F(\sqrt{\pm t})$ does not split D.

If H is a square free polynomial in A which is coprime to tPq, then choose

$$K = F(\sqrt{tPqH}).$$ Then the pair (D,K) satisfy conditions of Theorem 8.5, giving $X^D(K) = \phi$.

As pointed out in the remark earlier, by a PARI/GP program, one can choose

$$(P,Q)=(t^3+t^2+t+2,\ t+1).$$

With this choice of (P,Q), the pair (D,K) also satisfy the conditions of the Prop. 9.9, the which is a consequence of the paper "Local Diophantine properties of modular curves of $\mathcal{D}$-elliptic sheaves" by Papikian. In particular, $X^D(K_v)\neq\phi$ for any place v of K. This provides a counterexample to Hasse principle. For other such counterexamples, see Theorem 9.11 of the paper.