On singular moduli for higher rank Drinfeld modules

Chien-Hua Chen

National Center for Theoretical Sciences (NCTS), Taiwan

JA 2023

Singular moduli for elliptic curves

Modular j-function:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots$$

, where $q = e^{2\pi i\tau}$.

- A singular modulus is $j(\tau)$ where $\tau \in \mathbb{H}$ an imaginary quadratic irrational number.
- $j(\tau) = j(E_\tau)$, where $E_\tau = \mathbb{C}/ < \tau, 1 >$ is an elliptic curve with CM
- $j(\tau)$ is an algebraic integer.

Question: Is there any description on prime factorization of $j(\tau)$?

Singular moduli for elliptic curves

Theorem (Gross-Zagier, 1985)

Let d_1, d_2 be two fundamental discriminant of imaginary quadratic fields. Asuume further that d_1 and d_2 are coprime to each other. Let w_1, w_2 be the number of roots of unity in the quadratic orders of discriminant d_1, d_2, respectively. Define

$$J(d_1, d_2) := \left(\prod_{[\tau_1],[\tau_2] \text{ with } \operatorname{disc}(\tau_i)=d_i} (j(\tau_1) - j(\tau_2)) \right)^{\frac{4}{w_1 w_2}}.$$

Then we have

$$J(d_1, d_2)^2 = \pm \prod_{x \in \mathbb{Z} \textit{ and } n, n' \in \mathbb{Z}_{>0} \textit{ with } x^2 + 4nn' = d_1 d_2} n^{\epsilon(n')}.$$

Here $\epsilon(n')$ is an explicit map defined in terms of Legendre symbols.

Hilbert class polynomial

- $K := \mathbb{Q}(\sqrt{D})$ imaginary quadratic field
- $E_\tau = \mathbb{C}/ < 1, \tau >:=$ an elliptic curve with CM by $\mathcal{O}_K$
- Hilbert class polynomial is defined to be

$$H_D(x) = \prod_{\frac{\{\tau | E_\tau \text{ has CM by } \mathcal{O}_K\}}{\mathrm{SL}_2(\mathbb{Z})}} (x - j(E_\tau)) \in \mathbb{Z}[x].$$

- Constant term of $H_D(x)$ is a special case of Gross-Zagier formula.

Drinfeld module analogy

- Let $q = p^e$ be a prime power. Consider

$$A = \mathbb{F}_q[T] \subset F = \mathbb{F}_q(T) \subset F_\infty = \mathbb{F}_q((\frac{1}{T})) \subset \mathbb{C}_\infty = \widehat{\overline{F_\infty}}.$$

- $\Lambda :=$ A-lattice of rank r in $\mathbb{C}_\infty$. i.e. a discrete subgroup $\Lambda \subset \mathbb{C}_\infty$ which is finitely generated A-submodule of $\mathbb{C}_\infty$ of rank r.
- Define the exponential map from $\mathbb{C}_\infty$ to $\mathbb{C}_\infty$,

$$e_\Lambda(x) := x \prod_{0 \neq \lambda \in \Lambda} (1 - \frac{x}{\lambda})$$

.

- There is a map $\phi^\Lambda : A \to \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,\mathbb{C}_\infty}) = \mathbb{C}_\infty\{\tau\}$ such that

$$e_\Lambda(ax) = \phi^\Lambda_a(e_\Lambda(x)) \text{ for all } a \in A.$$

- ϕ^Λ is a Drinfeld module over $\mathbb{C}_\infty$ of rank r.

Drinfeld module analogy, rank-2 case

- $q :=$ an odd prime power, $A := \mathbb{F}_q[T]$, and $F := \mathbb{F}_q(T)$.
- $K := F(\sqrt{d})$ imaginary quadratic extension over F. Here d is the discriminant of a quadratic polynomial $ax^2 + bx + c$ over A with a, b, c relatively prime.

Theorem (Dorman, 1991)

Denote

$$J(d) := \prod_{[\tau] \text{ with } \mathrm{disc}(\tau)=d} (j(\tau) - j(\rho)),$$

where ρ is the Drinfeld module $\rho_T = T + \tau^2$. Let $\mathfrak{p}$ be a nonzero prime ideal of A with monic generator π, then

$$\mathrm{ord}_{\mathfrak{p}} J(d) = \frac{q+1}{2} \sum_{m \in A} \sum_{n \geqslant 1} R\left(\frac{d - um^2}{\pi^{2n-1}}\right).$$

Here $R(a) := \#$ of ideals of $\mathbb{F}_{q^2}[T]$ having norm equal to the ideal $\mathfrak{a} = (a)$ of A.

Drinfeld module analogy, prime rank case

- $q = p^e$ an odd prime power, r be a prime number, and $(p, r) = 1$.
- $A := \mathbb{F}_q[T]$, and $F := \mathbb{F}_q(T)$.
- Consider the A-field L together with the natural embedding $\gamma : A \hookrightarrow L$. Let $\phi : A \to L\{\tau\} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,L})$ be a rank-r Drinfeld module over L. Can characterize ϕ by

$$\phi_T = T + g_1\tau + \cdots + g_r\tau^r, \text{ where } g_i \in L, \text{ and } g_r \neq 0.$$

- Define the ring of homomorphism between two rank-r Drinfeld module ϕ and ψ over L to be

$$\mathrm{Hom}(\phi, \psi) = \mathrm{Hom}_{\bar{L}}(\phi, \psi) := \{u \in \bar{L}\{\tau\} \mid u \circ \phi_a = \psi_a \circ u, \ \forall a \in A\}.$$

Structure of coarse moduli scheme

- $J^{(\delta_1,\cdots,\delta_{r-1})} := \frac{\prod_{1\leqslant i\leqslant r-1} g_i^{\delta_i}}{g_r^{\delta_r}}$ a basic J-invariant. Here δ_i's satisfy

$$(i)\ \ \delta_1(q-1)+\delta_2(q^2-1)+\cdots+\delta_{r-1}(q^{r-1}-1)=\delta_r(q^r-1).$$
$$(ii)\ \ 0\leqslant \delta_i \leqslant \frac{q^r-1}{q^{\mathrm{g.c.d.}(i,r)}-1} \text{ for all } 1\leqslant i\leqslant r-1; \quad \text{g.c.d.}(\delta_1,\cdots,\delta_r)=1.$$

Theorem (Potemine, 1998)

$$M^r(1)=\mathrm{Spec}\ A\left[\left\{J^{(\delta_1,\cdots,\delta_{r-1})}\right\}\right]$$

is the coarse moduli scheme of Drinfeld A-modules of rank r.

Main result

- Let $K := F(s)$ be a degree-r imaginary extension over F, with K/F a normal extension and its ring of integers $\mathcal{O}_K = A[s]$.
- $\mathfrak{p} = (\pi)$ is a finite place of F with degree $\deg_T(\pi)$ prime to r.
- Let ϕ be a rank-r Drinfeld module over $\mathbb{C}_\infty$ with CM by $\mathcal{O}_K$, i.e. $\mathrm{End}(\phi) \cong \mathcal{O}_K$. Fix an isomorphism, then compose with the derivative map ∂, get an embedding $\iota : \mathcal{O}_K \hookrightarrow \mathbb{C}_\infty$.
- $[\phi] :=$ isomorphism class over $\mathbb{C}_\infty$ of "normalizable" rank-r Drinfeld module ϕ of generic characteristic with CM by $\mathcal{O}_K$. Denote $\mathrm{CM}(\mathcal{O}_K, \iota)$ to be the set of $[\phi]'s$
- $$J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})} := \prod_{[\phi]\in \mathrm{CM}(\mathcal{O}_K,\iota)} J^{(\delta_1,\cdots,\delta_{r-1})}(\phi).$$

Main result

Theorem (Chen, 2023 preprint)

$$\mathrm{ord}_{\mathfrak{p}}(J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})}) \geqslant \frac{(q+1)(q-1)}{q^r-1}\sum_{n\geqslant 1}\#S_n.$$

Here

$$\#S_n = \#\Big\{M_{(x_1,\cdots,x_r)} \in \mathcal{M} \mid x_i \equiv 0 \mod \pi^{n-1} \text{ for } 2\leqslant i\leqslant r, \\ \text{char. poly of } M_{(x_1,\cdots,x_r)} = \text{ min. poly of } s\Big\},$$

$$\mathcal{M} = \left\{\begin{pmatrix} x_0 & x_1 & \cdots & x_{r-1} \\ \pi\sigma(x_{r-1}) & \sigma(x_0) & \cdots & \sigma(x_{r-2}) \\ \vdots & & \ddots & \vdots \\ \pi\sigma^{r-1}(x_1) & \cdots & \pi\sigma^{r-1}(x_{r-1}) & \sigma^{r-1}(x_0)\end{pmatrix} \mid (x_i)\in\mathbb{F}_{q^r}[T]\right\},$$

and $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}(T)/\mathbb{F}_q(T))$ *is the Frobenius map* $\alpha \mapsto \alpha^q$.

Some remarks

- Compare both sides of the inequality

$$\mathrm{ord}_{\mathfrak{p}}(J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})}) \quad \geqslant \frac{(q+1)(q-1)}{q^r-1}\sum_{n\geqslant 1}\#S_n.$$

  LHS depends on the choice of basic J-invariant, while the RHS is independent of the choice of J. Hence RHS can be viewed as an overall lower bound among choices of basic J-invariant.
- There is a criteria on when will the equality happen:

Corollary

The equality in the Theorem happens when the following two conditions are satisfied:

(a) $J^{(\delta_1,\cdots,\delta_{r-1})} = J^{(1,0,\cdots,0,q)} = \frac{g_1\cdot g_{r-1}^q}{\Delta}$.

(b) *For each representative ϕ of $[\phi]\in CM(\mathcal{O}_K,\iota)$ defined over W. If $\phi\not\cong\varphi$* mod μ^i *for some $i\geqslant 1$, then both $g_1\not\equiv 0$ and $g_{r-1}\not\equiv 0$* mod μ^i.

Examples: when K/F is Kummer

- $q = p^e$ odd prime power with $q \equiv 1 \mod 3$. Let
- $K := F(\sqrt[3]{\Delta})$ over $F = \mathbb{F}_q(T)$, where $\Delta \in A := \mathbb{F}_q[T]$ is cubic-free with T-degree prime to 3. Suppose the $\mathcal{O}_K = A[\sqrt[3]{\Delta}]$.
- From our main reuslt, we have

$$\mathrm{ord}_{\mathfrak{p}}(J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})}) \geqslant \frac{(q+1)(q-1)}{q^3-1}\sum_{n\geqslant 1}\#S_n,$$

and $\#S_n = \#$ of $(x_0, x_1', x_2') \in \mathbb{F}_{q^3}[T]^3$ satisfy equations below:

$$\begin{cases} \mathrm{Tr}(x_0) = 0 & (1) \\ \mathrm{Tr}(x_0\sigma(x_0)) = -\frac{1}{2}\mathrm{Tr}(x_0^2) = \pi^{2n+1}\mathrm{Tr}(\mathrm{x}_1'\sigma(\mathrm{x}_2')) & (2) \\ \mathrm{Norm}(x_0) + \pi^{3n-2}\mathrm{Norm}(x_1') + \pi^{3n-1}\mathrm{Norm}(x_2') \\ -\pi^{2n-1}\mathrm{Tr}(x_0\sigma(x_1')\sigma^2(x_2')) = \Delta & (3) \end{cases}.$$

Example: under the condition $\Delta = \pi = T$

- $\{(0,\beta,0) \mid \beta \in \mathbb{F}_{q^3}[T] \text{ with } \mathrm{Norm}(\beta) = 1)\}$ satisfy equation (1) to (3) when $n = 1$.
- $$\#S_1 \geqslant \#\{(0,\beta,0) \mid \beta \in \mathbb{F}_{q^3}[T] \text{ with } \mathrm{Norm}(\beta) = 1)\} = q^2 + q + 1.$$

  The equality on the right hand side comes from the fact that $\mathrm{Norm} : \mathbb{F}_{q^3}^* \to \mathbb{F}_q^*$ is surjective.
- get

$$\begin{aligned} \nu_{\mathfrak{p}}(J_{\mathcal{O}_K}^{(\delta_1,\delta_2)}) &\geqslant \tfrac{(q+1)(q-1)}{q^3-1} \textstyle\sum_{n\geqslant 1} \#S_n \\ &\geqslant \tfrac{(q+1)(q-1)(q^2+q+1)}{(q^3-1)} \\ &= q+1 \end{aligned}$$

Example: under the condition $\Delta = T(T+1)$ and $\pi = T$

- Then the set

  $$\mathcal{B} := \{(0,\beta,\gamma) \mid \beta,\gamma \in \mathbb{F}_{q^3}[T], \mathrm{Nm}(\beta) = \mathrm{Nm}(\gamma) = 1 \text{ and } \mathrm{Tr}(\beta\sigma(\gamma)) = 0\}$$

  satisfy equation (1) to (3) when $n = 1$.
- We have that $\mathcal{B}$ contains

  $$\{(0,\beta,1) \mid \mathrm{Norm}(\beta) = 1, \mathrm{Tr}(\beta) = 0\} \sqcup \{(0,1,\gamma) \mid \mathrm{Norm}(\gamma) = 1, \mathrm{Tr}(\gamma) = 0\}$$

- Katz's estimation on Soto-Andrade sum:
  The number $N_3(0,1)$ of elements in $\mathbb{F}_{q^3}$ with norm equal to 1 and trace equal to 0 is bounded by

  $$|N_3(0,1) - \frac{q^2-1}{q-1}| \leqslant g.c.d.(3, q-1)\sqrt{q}.$$

  Thus $\#\mathcal{B} \geqslant 2(q+1 - g.c.d(3,q-1)\sqrt{q})$
- Get

  $$\nu_{\mathfrak{p}}(J_{\mathcal{O}_K}^{(\delta_1,\delta_2)}) \geqslant \frac{(q+1)(q-1)}{q^3-1} \sum_{n \geqslant 1} \#S_n \geqslant \frac{(q+1)(q-1)}{q^3-1} \cdot \#\mathcal{B}$$

Strategy for proof of the main result

Reduce to counting isomorphisms:

$$\nu(J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})}) \geqslant \frac{q+1}{q^r-1} \sum_{[\phi]\in \mathrm{CM}(\mathcal{O}_K,\iota)} \sum_{n\geqslant 1} \#\mathrm{Iso}_{W/\mu^n W}(\phi,\varphi).$$

$$\Big\downarrow (1)$$

Reduce to counting endomorphisms on $\varphi_T = T + \tau^r$:

$$\nu(J_{\mathcal{O}_K}^{(\delta_1,\cdots,\delta_{r-1})}) \geqslant \frac{(q+1)(q-1)}{q^r-1} \sum_{n\geqslant 1} \#S_n.$$

$$S_n := \left\{ \begin{array}{c} \alpha_0 \in \mathrm{End}_{W/\mu^n W}(\varphi) : \text{char. poly. of } \alpha_0 \in A[\alpha_0] = \text{min. poly. of } s, \\ \text{and } \partial(\alpha_0) \equiv \iota(s) \mod \mu^n \end{array} \right\}$$

$$\Big\downarrow (2)$$

Matrix realization reduce to counting certain type of $r \times r$ matrices over $\mathbb{F}_{q^r}[T]$ with specified characteristic polynomial.

Strategy: Reduce to counting isomorphism

- $H_K :=$ Hilbert class field of K.
- Fix a place $\mathfrak{P}$ of H_K above $\mathfrak{p}$.
- $\widehat{H}^{nr}_{K,\mathfrak{P}} :=$ the completion of $H^{nr}_{K,\mathfrak{P}}$, the maximal unramified extension over the local field of H_K at $\mathfrak{P}$.
- $W :=$ the discrete valuation ring of $\widehat{H}^{nr}_{K,\mathfrak{P}}$
- fix a uniformizer μ of W, with normalized valuation ν

Write $\phi_T = T + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \tau^r \in W\{\tau\}$, and ϕ' in tems of $g_i'\tau^i$.
Assume that $\phi \cong \phi'$ after reduction modulo μ^k for some $k \in \mathbb{Z}_{\geqslant 1}$, but not isomorphic after reduction modulo μ^{k+1}.
If $g_1^{\delta_1} \cdot \cdots \cdot g_{r-1}^{\delta_{r-1}} = 0$ in W. We separate $\{1, 2, \cdots, r-1\}$ into

$$\mathcal{A} := \{1 \leqslant i_\ell \leqslant r-1 \mid g_{i_\ell} = 0\} \text{ and } \mathcal{B} := \{1, \cdots, r-1\} - \mathcal{A}.$$

Then

$$\nu(J^{(\delta_1,\cdots,\delta_{r-1})}(\phi) - J^{(\delta_1,\cdots,\delta_{r-1})}(\phi')) = \nu\left(\prod_{1\leqslant i\leqslant r-1} g_i^{\delta_i} - \prod_{1\leqslant i\leqslant r-1} g_i'^{\delta_i}\right)$$

$$= \nu[(c^{q-1}g_1 + \mu^k u_1)^{\delta_1} \cdot \cdots \cdot (c^{q^{r-1}-1}g_{r-1} + \mu^k u_{r-1})^{\delta_{r-1}}]$$

$$\geqslant k \cdot \left(\textstyle\sum_{j\in\mathcal{A}} \delta_j\right)$$

Strategy: Reduce to counting isomorphism

- Since $\phi \cong \phi' \mod \mu^i$ for $1 \leqslant i \leqslant k$ and $\phi \ncong \phi' \mod \mu^{k+1}$, get

$$\begin{aligned} & \#\mathrm{Iso}_{W/\mu^i W}(\phi, \phi') = \#\mathrm{Aut}_{W/\mu^i W}(\phi) \\ = \quad & \#\{\mathbb{F}_{q^r}^* \bigcap_{1 \leqslant j \leqslant r-1} \mathbb{F}_{q^j}^* \mid g_j \not\equiv 0 \mod \mu^i\} \text{ for } 1 \leqslant i \leqslant k \end{aligned}.$$

Therefore,

$$\begin{aligned} & \textstyle\sum_{n \geqslant 1} \#\mathrm{Iso}_{W/\mu^n W}(\phi, \phi') \\ = \quad & \textstyle\sum_{i=1}^{k} g.c.d.(q^r - 1, q^j - 1 \mid g_j \not\equiv 0 \mod \mu^i \text{ for } 1 \leqslant j \leqslant r-1) \\ \leqslant \quad & k \cdot (q^r - 1) \end{aligned}$$

Lemma

Restrict to our case where ϕ has CM by $\mathcal{O}_K$, and $\phi' = \varphi_T := T + \tau^r$. Get

$$\nu(J^{(\delta_1, \cdots, \delta_{r-1})}(\phi) - J^{(\delta_1, \cdots, \delta_{r-1})}(\varphi)) \geqslant \frac{q+1}{q^r - 1} \sum_{n \geqslant 1} \#\mathrm{Iso}_{W/\mu^n W}(\phi, \varphi)$$

Strategy: Reduce to counting endomorphisms

Theorem

There is a $(q-1)$-to-1 correspondence between $\mathrm{Iso}_{W/\mu^n W}(\phi, \varphi)$ and the set $S_n :=$

$$\left\{ \begin{array}{c} \alpha_0 \in \mathrm{End}_{W/\mu^n W}(\varphi) : \textit{char. poly. of } \alpha_0 \in A[\alpha_0] = \textit{min. poly. of } s, \\ \textit{and } \partial(\alpha_0) \equiv \iota(s) \mod \mu^n \end{array} \right\}.$$

Here the charateristic polynomial of α_0 is obtained by viewing $\alpha_0 \in A[\alpha_0]$ as "left multiplication by α_0". And minimal polynomial of s is obtained from the field extension $k = F(s)$ over F.

Sketch of proof

$(\Rightarrow)$ Since ϕ over W has CM by $\mathcal{O}_K = A[s]$. We may view ϕ as a Drinfeld $\mathcal{O}_K$-module of rank 1 over W. Thus $\phi_s \in \mathrm{End}_W(\phi)$ is well-defined. Taking reduction modulo μ^n, we get $\bar{\phi}_s \in \mathrm{End}_{W/\mu^n W}(\phi)$.
Now for any $w \in \mathrm{Iso}_{W/\mu^n W}(\varphi, \phi)$, we consider the composition of maps:

$$s_w := w^{-1} \circ \bar{\phi}_s \circ w \in \mathrm{End}_{W/\mu^n W}(\varphi)$$

The map s_w lies in S_n

Sketch of proof

Claim

$(\bar{\varphi} \equiv \varphi \mod \mu^n, \alpha_0)$ over $W/\mu^n W$ can be lifted to (ψ, α) over W, where

$(\Leftarrow)$ (a) $\psi \in \mathrm{CM}(\mathcal{O}_K, \iota)$.

(b) $\psi \equiv \varphi \mod \mu^n$.

(c) $\alpha \in \mathrm{End}_W(\psi)$, *and* $\alpha \equiv \alpha_0 \mod \mu^n$.

See for instance the case $n = 1$.

- Set $\underline{\varphi}|_A \equiv \varphi \mod \mu$, and $\underline{\varphi}_s \equiv \alpha_0 \mod \mu$. This makes (φ, α_0) over $W/\mu W$ a rank-1 Drinfeld $\overline{\mathcal{O}}_K$-module $\underline{\varphi}$ over $W/\mu W$.
- Drinfeld module analogue of Serre-Tate lifting theorem $\Rightarrow$ Let $\mathfrak{q} := \mu \cap \mathcal{O}_K$. It is enough to construct a lifting of $\underline{\varphi}[\mathfrak{q}^\infty]$, the $\mathcal{O}_\mathfrak{q}$-divisible group of $\underline{\varphi}$, to W.
- There is a one-to-one correspondence between "$\mathcal{O}_\mathfrak{q}$-divisible group of rank-1" and "Formal $\mathcal{O}_\mathfrak{q}$-module of height-1".
- For height-1 formal $\mathcal{O}_\mathfrak{q}$-modules. There is a lifting, unique up to W-isomorphism, to W.

Note: The above process work when viewing (φ, α_0) as rank-1 Drinfeld $\mathcal{O}$-module, the $\mathcal{O}$ is a maximal order.

Matrix realization

At here, we further assume

(a) $r \geqslant 3$ is a prime number

(b) $\varphi_T = T + \tau^r$ has good supersingular reduction at $\mathfrak{p}$. This is equivalent to say that the monic generator π of $\mathfrak{p}$ has degree $\deg_T(\pi)$ prime to r.

For instance we look at the set $S_1 \subset \mathrm{End}_{W/\mu W}(\varphi)$

- The endomorphism algebra $D := \mathrm{End}(\underline{\varphi}) \otimes_A F$ has Hasse invariant

$$\mathrm{Inv}_\nu(D) = \begin{cases} \frac{1}{r}, & \nu = \mathfrak{p} \\ \frac{-1}{r}, & \nu = \infty \\ 0, & \text{otherwise} \end{cases}.$$

- $\mathrm{End}_{W/\mu W}(\varphi) \otimes_A \mathcal{O}_H = \mathrm{End}(\underline{\varphi}) \otimes_A \mathcal{O}_H \hookrightarrow D \otimes_F H \simeq M_r(H)$.
- Compare with matrix realization of the cyclic algebra

$$(H/F, \sigma, \pi) := H[\tau, \tau^{-1}]/(\tau^r - \pi)H[\tau, \tau^{-1}].$$

Here $H := \mathbb{F}_{q^r}(T)$, and $\sigma \in \mathrm{Gal}(H/F)$ is the Frobenius element. The multiplication in $H[\tau, \tau^{-1}]$ is defined by

$$\alpha\tau^n \cdot \beta\tau^m = \alpha\sigma^n(\beta)\tau^{n+m}.$$

Matrix realization

- The matrix realization of $(H/F, \sigma, \pi)$ in $M_r(H)$ is the following

$$\left\{ \begin{pmatrix} x_0 & x_1 & \cdots & x_{r-1} \\ \pi\sigma(x_{r-1}) & \sigma(x_0) & \cdots & \sigma(x_{r-2}) \\ \vdots & & \ddots & \vdots \\ \pi\sigma^{r-1}(x_1) & \cdots & \pi\sigma^{r-1}(x_{r-1}) & \sigma^{r-1}(x_0) \end{pmatrix} \mid (x_0, \cdots, x_{r-1}) \in H \right\}$$

- The embedding $\mathrm{End}_{W/\mu W}(\varphi) \hookrightarrow M_r(H)$ is optimal. i.e. $\mathrm{End}_{W/\mu W}(\varphi)$ is equal to $\mathcal{M}$ up to conjugation in $M_r(\mathcal{O}_H)$, where $\mathcal{M}$ is the set

$$\left\{ \begin{pmatrix} x_0 & x_1 & \cdots & x_{r-1} \\ \pi\sigma(x_{r-1}) & \sigma(x_0) & \cdots & \sigma(x_{r-2}) \\ \vdots & & \ddots & \vdots \\ \pi\sigma^{r-1}(x_1) & \cdots & \pi\sigma^{r-1}(x_{r-1}) & \sigma^{r-1}(x_0) \end{pmatrix} \mid (x_i)_{0\leqslant i\leqslant r-1} \in \mathcal{O}_H \right\}.$$

- From definition of S_1 and the matrix realization

$$S_1 = \left\{ M_{(x_0,\cdots,x_{r-1})} \in \mathcal{M} \mid \text{ char. poly of } M = \text{ min. poly of } s \right\} .$$

Matrix realization

Matrix realization for S_n when $n \geqslant 2$:

*Case*1. When $\mathfrak{p}$ is unramified in K/F

Proposition

As $\mathcal{O}_H$-modules we have

$$\mathrm{End}_{W/\mu^n W}(\varphi) = \mathcal{O}_H + \pi^{n-1}\mathrm{End}(\underline{\varphi})$$

Thus we get

$$\mathrm{End}_{W/\mu^n W}(\varphi) = \left\{ M_{(x_0,\cdots,x_{r-1})} \in \mathcal{M} \mid x_i \equiv 0 \mod \pi^{n-1} \ \textit{for}\ 1 \leqslant i \leqslant r-1 \right\}.$$

*Case*2. When $\mathfrak{p}$ is ramified in K/F

Proposition

$$\mathrm{End}_{W/\mu^n W}(\varphi) = \left\{ M_{(x_0,\cdots,x_{r-1})} \in \mathcal{M} \mid x_i \equiv 0 \mod \pi^{z-1} \ \textit{for}\ 1 \leqslant i \leqslant r-1 \right\},$$

where $z := \lfloor \frac{n+r-1}{r} \rfloor$.

Thank you.