Images of Galois representations with values in mod p Hecke algebras

Laia Amorós Carafí
Université du Luxembourg
Universitat de Barcelona

Images of Galois representations with values in mod p Hecke algebras

- mod p modular forms, mod p Hecke algebras

Images of Galois representations with values in mod p Hecke algebras

- mod p modular forms, mod p Hecke algebras
- Galois representations with values in these algebras

Images of Galois representations with values in mod p Hecke algebras

- mod p modular forms, mod p Hecke algebras
- Galois representations with values in these algebras
- Computation of the image of these Galois representations

Images of Galois representations with values in mod p Hecke algebras

- mod p modular forms, mod p Hecke algebras
- Galois representations with values in these algebras
- Computation of the image of these Galois representations
- Application

mod p Hecke algebras

mod p Hecke algebras

$S_k(N, \varepsilon; \mathbb{C})$ space of **modular forms** $f(z) = \sum_{n \geq 0} a_n q^n$ ($q = e^{2\pi i z}$) of level $N \geq 1$, weight $k \geq 2$ and Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Moreover assume $a_0 = 0$.

mod p Hecke algebras

$S_k(N, \varepsilon; \mathbb{C})$ space of **cuspidal modular forms** or **cusp forms**

mod p Hecke algebras

$S_k(N; \mathbb{C})$ space of **cusp forms**

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N) := \langle T_p \text{ Hecke operator} : p \text{ prime} \rangle$

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{Z})$

mod p Hecke algebras

$S_k(N; \mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N; \mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N; \mathbb{F}_q) := S_k(N; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

mod p Hecke algebras

$S_k(N; \mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N; \mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N; \mathbb{F}_q) := S_k(N; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $f(z) = \sum_{n\geq 0} a_n q^n \in S_k(N;\mathbb{C})$, $q = e^{2\pi iz}$, simultaneous eigenvector for all Hecke operators, $a_1 = 1$

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $f(z) = \sum_{n\geq 0} a_n q^n \in S_k(N;\mathbb{C})$ **normalised Hecke eigenform**

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $\overline{f}(z) = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N;\mathbb{F}_q)$ **normalised Hecke eigenform mod p**

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $\overline{f}(z) = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N;\mathbb{F}_q)$ **normalised Hecke eigenform mod** p

$\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q,\ \ T_n \mapsto \overline{a}_n = a_n \bmod p \qquad \mathfrak{m}_f := \ker \overline{\lambda}_f$

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $\overline{f}(z) = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N;\mathbb{F}_q)$ **normalised Hecke eigenform mod p**

$\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q,\ T_n \mapsto \overline{a}_n = a_n \bmod p \qquad \mathfrak{m}_f := \ker \overline{\lambda}_f$

$\mathbb{T}_f := \overline{\mathbb{T}}_{\mathfrak{m}_f}$ assume $\mathfrak{m}_f^2 = 0$

mod p Hecke algebras

$S_k(N;\mathbb{C})$ space of **cusp forms**

$\mathrm{End}_{\mathbb{C}}(S_k(N;\mathbb{C})) \supset \mathbb{T}_k(N)$ finite-dimensional commutative $\mathbb{Z}$-algebra

$S_k(N;\mathbb{F}_q) := S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_q$

$\overline{\mathbb{T}} := \mathbb{T}_k(N) \otimes \mathbb{F}_q$ finite-dimensional commutative $\mathbb{F}_q$-algebra

$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}} \overline{\mathbb{T}}_{\mathfrak{m}}$, where $\overline{\mathbb{T}}_{\mathfrak{m}}$ localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$

Let us take $\overline{f}(z) = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N;\mathbb{F}_q)$ **normalised Hecke eigenform mod p**

$\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q,\ T_n \mapsto \overline{a}_n = a_n \bmod p \qquad \mathfrak{m}_f := \ker \overline{\lambda}_f$

$\mathbb{T}_f := \overline{\mathbb{T}}_{\mathfrak{m}_f}$ assume $\mathfrak{m}_f^2 = 0$

$\mathbb{T}_f \simeq \mathbb{F}_q[X_1,\ldots,X_m]/(X_iX_j)_{1\leq i,j\leq m}$ finite-dimensional local commutative algebra, $m = \dim_{\mathbb{F}_q}\mathfrak{m}_f$

Galois representations

Next we want to: attach a Galois representation to $\mathbb{T}_f$.

Galois representations

Next we want to: attach a Galois representation to $\mathbb{T}_f$.

Let $\overline{f} = \sum_{n \geq 0} \overline{a}_n q^n \in S_k(N; \mathbb{F}_q)$ given by $\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q$, $T_n \to \overline{a}_n$

Galois representations

Next we want to: attach a Galois representation to $\mathbb{T}_f$.

Let $\overline{f} = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N; \mathbb{F}_q)$ given by $\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q,\ T_n \to \overline{a}_n$

Deligne, Shimura: We can attach to $\overline{f}$ a **Galois representation**

$$\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

unramified outside Np and, for every $\ell \nmid Np$:

$$\mathbf{tr}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \overline{\lambda}_f(T_\ell) \quad \text{and} \quad \mathbf{det}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$$

Galois representations

Next we want to: attach a Galois representation to $\mathbb{T}_f$.

Let $\overline{f} = \sum_{n\geq 0} \overline{a}_n q^n \in S_k(N; \mathbb{F}_q)$ given by $\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q, \; T_n \to \overline{a}_n$

Deligne, Shimura: We can attach to $\overline{f}$ a **Galois representation**

$$\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

unramified outside Np and, for every $\ell \nmid Np$:

$$\mathbf{tr}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \overline{\lambda}_f(T_\ell) \quad \text{and} \quad \mathbf{det}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$$

Let $\mathbb{T}_f := \overline{\mathbb{T}}_{\mathfrak{m}_f}$ as before, but without the operators T_ℓ with $\ell \mid Np$.

Galois representations

Next we want to: attach a Galois representation to $\mathbb{T}_f$.

Let $\overline{f} = \sum_{n \geq 0} \overline{a}_n q^n \in S_k(N; \mathbb{F}_q)$ given by $\overline{\lambda}_f : \overline{\mathbb{T}} \to \mathbb{F}_q,\ T_n \to \overline{a}_n$

Deligne, Shimura: We can attach to $\overline{f}$ a **Galois representation**

$$\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

unramified outside Np and, for every $\ell \nmid Np$:

$$\mathbf{tr}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \overline{\lambda}_f(T_\ell) \quad \text{and} \quad \mathbf{det}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$$

Let $\mathbb{T}_f := \overline{\mathbb{T}}_{\mathfrak{m}_f}$ as before, but without the operators T_ℓ with $\ell \mid Np$.

Carayol: If $\overline{\rho}_f$ is absolutely irreducible, then there exists a continuous Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$$

unramified outside Np and, for every $\ell \nmid Np$:

$$\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = \lambda_f(T_\ell) \quad \text{and} \quad \mathbf{det}(\rho_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$$

where $\lambda_f : \overline{\mathbb{T}} \to \mathbb{T}_f$. This representation is unique up to conjugation.

Image of ρ_f

Image of ρ_f

GOAL: Compute the image of $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$.

Image of ρ_f

GOAL: Compute the image of $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$.

Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$

$\mathrm{GL}_2^D(\mathbb{T}_f) := \{g \in \mathrm{GL}_2(\mathbb{T}_f) : \det(g) \in D\}$

$\mathrm{GL}_2^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_2(\mathbb{F}_q) : \det(g) \in D\}$

Image of ρ_f

GOAL: Compute the image of $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$.

Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$

$\mathrm{GL}_2^D(\mathbb{T}_f) := \{g \in \mathrm{GL}_2(\mathbb{T}_f) : \det(g) \in D\}$

$\mathrm{GL}_2^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_2(\mathbb{F}_q) : \det(g) \in D\}$

Assume that $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f)$.

Image of ρ_f

GOAL: Compute the image of $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$.

Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$

$\mathrm{GL}_2^D(\mathbb{T}_f) := \{g \in \mathrm{GL}_2(\mathbb{T}_f) : \det(g) \in D\}$

$\mathrm{GL}_2^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_2(\mathbb{F}_q) : \det(g) \in D\}$

Assume that $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f)$.

We have the following commutative diagram

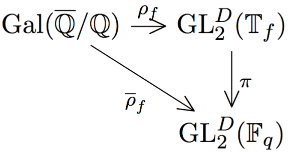

Image of ρ_f

GOAL: Compute the image of $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_f)$.

Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$

$\mathrm{GL}_2^D(\mathbb{T}_f) := \{g \in \mathrm{GL}_2(\mathbb{T}_f) : \det(g) \in D\}$

$\mathrm{GL}_2^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_2(\mathbb{F}_q) : \det(g) \in D\}$

Assume that $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f)$.

We have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_f} & \mathrm{GL}_2^D(\mathbb{T}_f) \\ & \overline{\rho}_f \searrow & \downarrow \pi \\ & & \mathrm{GL}_2^D(\mathbb{F}_q) \end{array}$$

that gives us a short exact sequence:

$$1 \to \ker(\pi) \to \mathrm{GL}_2^D(\mathbb{T}_f) \xrightarrow{\pi} \mathrm{GL}_2^D(\mathbb{F}_q) \to 1$$

Image of ρ_f as a semi-direct product

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$
\begin{array}{ccccccccc}
1 & \to & \ker(\pi) & \to & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\
 & & & & \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} & \mapsto & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & &
\end{array}
$$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$\begin{array}{ccccccccc} 1 & \to & \ker(\pi) & \to & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & & & \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} & \mapsto & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & & \end{array}$$

Take $g = \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} \in \mathrm{GL}_2^D(\mathbb{T}_f)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$.

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$1 \to \ker(\pi) \to \begin{array}{c}\mathrm{GL}_2^D(\mathbb{T}_f) \\ \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix}\end{array} \begin{array}{c}\xrightarrow{\pi} \\ \mapsto\end{array} \begin{array}{c}\mathrm{GL}_2^D(\mathbb{F}_q) \\ \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\end{array} \to 1$$

Take $g = \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} \in \mathrm{GL}_2^D(\mathbb{T}_f)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$. Then

$$g \in \ker(\pi) \Leftrightarrow g = \begin{pmatrix} 1+a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & 1+d_2\mathfrak{m}_f \end{pmatrix} \text{ and } \det(g) = 1+(a_2+d_2)\mathfrak{m}_f \in D \subseteq \mathbb{F}_q^\times.$$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$\begin{array}{ccccccccc} 1 & \to & \ker(\pi) & \to & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & & & \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} & \mapsto & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & & \end{array}$$

Take $g = \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} \in \mathrm{GL}_2^D(\mathbb{T}_f)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$. Then

$$g \in \ker(\pi) \Leftrightarrow g = \begin{pmatrix} 1+a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & 1+d_2\mathfrak{m}_f \end{pmatrix} \text{ and } \det(g) = 1+(a_2+d_2)\mathfrak{m}_f \in D \subseteq \mathbb{F}_q^\times.$$

$$\Leftrightarrow g = 1 + \begin{pmatrix} a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & d_2\mathfrak{m}_f \end{pmatrix} \text{ and } a_2 = -d_2$$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$\begin{array}{ccccccccc} 1 & \to & \ker(\pi) & \to & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & & & \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} & \mapsto & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & & \end{array}$$

Take $g = \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} \in \mathrm{GL}_2^D(\mathbb{T}_f)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$. Then

$$g \in \ker(\pi) \Leftrightarrow g = \begin{pmatrix} 1+a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & 1+d_2\mathfrak{m}_f \end{pmatrix} \text{ and } \det(g) = 1+(a_2+d_2)\mathfrak{m}_f \in D \subseteq \mathbb{F}_q^\times.$$

$$\Leftrightarrow g = 1 + \begin{pmatrix} a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & d_2\mathfrak{m}_f \end{pmatrix} \text{ and } a_2 = -d_2 \Leftrightarrow \ker(\pi) = 1 + \mathrm{M}_2^0(\mathfrak{m}_f)$$

Image of ρ_f as a semi-direct product

Assumptions:

- $\mathfrak{m}_f^2 = 0$
- $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$ The residual representation has **big image**

$$\begin{array}{ccccccccc} 1 & \to & \ker(\pi) & \to & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & & & \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} & \mapsto & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & & \end{array}$$

Take $g = \begin{pmatrix} a_1+a_2\mathfrak{m}_f & b_1+b_2\mathfrak{m}_f \\ c_1+c_2\mathfrak{m}_f & d_1+d_2\mathfrak{m}_f \end{pmatrix} \in \mathrm{GL}_2^D(\mathbb{T}_f)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$. Then

$$g \in \ker(\pi) \Leftrightarrow g = \begin{pmatrix} 1+a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & 1+d_2\mathfrak{m}_f \end{pmatrix} \text{ and } \det(g) = 1+(a_2+d_2)\mathfrak{m}_f \in D \subseteq \mathbb{F}_q^\times.$$

$$\Leftrightarrow g = 1 + \begin{pmatrix} a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & d_2\mathfrak{m}_f \end{pmatrix} \text{ and } a_2 = -d_2 \Leftrightarrow \ker(\pi) = 1 + \mathrm{M}_2^0(\mathfrak{m}_f)$$

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \begin{pmatrix} a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & -a_2\mathfrak{m}_f \end{pmatrix} & \mapsto & 1 + \begin{pmatrix} a_2\mathfrak{m}_f & b_2\mathfrak{m}_f \\ c_2\mathfrak{m}_f & -a_2\mathfrak{m}_f \end{pmatrix} & & & & \end{array}$$

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \stackrel{\iota}{\to} & \mathrm{GL}_2^D(\mathbb{T}_f) & \stackrel{\pi}{\to} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & H & \to & G & \to & \overline{G} & \to & 1 \end{array}$$

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & H & \to & G & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \end{array}$$

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & H & \to & G & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \end{array}$$

The first exact sequence splits, so $\mathrm{GL}_2^D(\mathbb{T}_f) \simeq \mathrm{M}_2^0(\mathfrak{m}_f) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$.

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \stackrel{\iota}{\to} & \mathrm{GL}_2^D(\mathbb{T}_f) & \stackrel{\pi}{\to} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & H & \to & G & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \end{array}$$

The first exact sequence splits, so $\mathrm{GL}_2^D(\mathbb{T}_f) \simeq \mathrm{M}_2^0(\mathfrak{m}_f) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$.

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & H & \to & G & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \end{array}$$

The first exact sequence splits, so $\mathrm{GL}_2^D(\mathbb{T}_f) \simeq \mathrm{M}_2^0(\mathfrak{m}_f) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$.

Theorem 1. (A.) Assume $q \neq 2, 3, 5$. The second exact sequence is also (**non-trivially**) split, so

$$G = \mathrm{Im}(\rho_f) \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q).$$

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}_f) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}_f) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & H & \to & G & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \end{array}$$

The first exact sequence splits, so $\mathrm{GL}_2^D(\mathbb{T}_f) \simeq \mathrm{M}_2^0(\mathfrak{m}_f) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$.

Theorem 1. (A.) Assume $q \neq 2, 3, 5$. The second exact sequence is also (**non-trivially**) split, so

$$G = \mathrm{Im}(\rho_f) \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q).$$

It is consequence of:

- $H^1(\mathrm{GL}_n^D(W_m), \mathbb{F}_q) = 0$
- there is an injection $H^2(\mathrm{GL}_n^D(W_m), N) \hookrightarrow H^2(\mathrm{GL}_n^D(W_m), M)$

Image of ρ_f as a semi-direct product

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$, and $G := \mathrm{Im}(\rho_f)$. They fit in a short exact sequence:

$$\begin{array}{ccccccccc} 0 & \rightarrow & \mathrm{M}_2^0(\mathfrak{m}_f) & \stackrel{\iota}{\rightarrow} & \mathrm{GL}_2^D(\mathbb{T}_f) & \stackrel{\pi}{\rightarrow} & \mathrm{GL}_2^D(\mathbb{F}_q) & \rightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \rightarrow & H & \rightarrow & G & \rightarrow & \mathrm{GL}_2^D(\mathbb{F}_q) & \rightarrow & 1 \end{array}$$

The first exact sequence splits, so $\mathrm{GL}_2^D(\mathbb{T}_f) \simeq \mathrm{M}_2^0(\mathfrak{m}_f) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$.

Theorem 1. (A.) Assume $q \neq 2, 3, 5$. The second exact sequence is also (**non-trivially**) split, so

$$G = \mathrm{Im}(\rho_f) \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q).$$

It is consequence of:

- $H^1(\mathrm{GL}_n^D(W_m), \mathbb{F}_q) = 0$
- there is an injection $H^2(\mathrm{GL}_n^D(W_m), N) \hookrightarrow H^2(\mathrm{GL}_n^D(W_m), M)$

$N \subseteq M \subseteq M_2^0(\mathfrak{m}_f)$ are $\mathbb{F}_p[\mathrm{GL}_n^D(\mathbb{F}_q)]$-submodules
$W(\mathbb{F}_q)$ ring of Witt vectors of $\mathbb{F}_q$ and $W_m := W(\mathbb{F}_q)/p^m$

Explicit determination of $\mathrm{Im}(\rho_f)$

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_iX_j)_{1 \leq i,j \leq m}$ and $\mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$ and $\mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$

$\mathrm{M}_2^0(\mathfrak{m}_f) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}$

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m} \quad \text{and} \quad \mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$$

$$\mathrm{M}_2^0(\mathfrak{m}_f) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} = \underbrace{M^0 \oplus \ldots \oplus M^0}_{m}$$

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_iX_j)_{1 \leq i,j \leq m}$ and $\mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$

$\mathrm{M}_2^0(\mathfrak{m}_f) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} = \underbrace{M^0 \oplus \ldots \oplus M^0}_{m}$

Lemma 1 (one copy): If $p \neq 2$, M^0 is a simple module.

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \le i,j \le m} \quad \text{and} \quad \mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$$

$$\mathrm{M}_2^0(\mathfrak{m}_f) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} = \underbrace{M^0 \oplus \ldots \oplus M^0}_{m}$$

Lemma 1 (one copy): If $p \neq 2$, M^0 is a simple module.

So the only possible submodules of M^0 are (0) and M^0.

Explicit determination of $\mathrm{Im}(\rho_f)$

We have

$$G \simeq H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

with $H \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ a submodule over $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$.

Question: Which are the possible submodules H of $\mathrm{M}_2^0(\mathfrak{m}_f)$ **?**

$$\mathbb{T}_f \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \le i,j \le m} \quad \text{and} \quad \mathfrak{m}_f \simeq \underbrace{\mathbb{F}_q \oplus \ldots \oplus \mathbb{F}_q}_{m}$$

$$\mathrm{M}_2^0(\mathfrak{m}_f) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} = \underbrace{M^0 \oplus \ldots \oplus M^0}_{m}$$

Lemma 1 (one copy): If $p \neq 2$, M^0 is a simple module.

So the only possible submodules of M^0 are (0) and M^0.

Lemma 2 (several copies): If M is a simple module, any submodule $N \subseteq M \oplus \ldots \oplus M$ is isomorphic to some copies of M.

Explicit determination of $\mathrm{Im}(\rho_f)$

$\Rightarrow$ If $p \neq 2$: $H \simeq \underbrace{M^0 \oplus \ldots \oplus M^0}_{\alpha}$ with $0 \leq \alpha \leq m$.

Explicit determination of $\mathrm{Im}(\rho_f)$

$\Rightarrow$ If $p \neq 2$: $H \simeq \underbrace{M^0 \oplus \ldots \oplus M^0}_{\alpha}$ with $0 \leq \alpha \leq m$.

Lemma 3 (one copy): If $p = 2$, M^0 has $\mathcal{S} = \{\lambda \mathrm{Id}_2 : \lambda \in \mathbb{F}_q\}$ as a submodule.

Let $N \subseteq M^0$. Then either $N \subseteq \mathcal{S}$ subgroup or $N = M^0$.

Explicit determination of $\mathrm{Im}(\rho_f)$

$\Rightarrow$ If $p \neq 2$: $H \simeq \underbrace{M^0 \oplus \ldots \oplus M^0}_{\alpha}$ with $0 \leq \alpha \leq m$.

Lemma 3 (one copy): If $p = 2$, M^0 has $\mathcal{S} = \{\lambda \mathrm{Id}_2 : \lambda \in \mathbb{F}_q\}$ as a submodule.
Let $N \subseteq M^0$. Then either $N \subseteq \mathcal{S}$ subgroup or $N = M^0$.

Lemma 4 (several copies): Let $N \subseteq \overbrace{M^0 \oplus \ldots \oplus M^0}^{m}$. Then $N \simeq N_1 \oplus \ldots \oplus N_n$, with $N_i \subseteq M^0$ submodule.

Explicit determination of $\mathrm{Im}(\rho_f)$

$\Rightarrow$ If $p \neq 2$: $H \simeq \underbrace{M^0 \oplus \ldots \oplus M^0}_{\alpha}$ with $0 \leq \alpha \leq m$.

Lemma 3 (one copy): If $p = 2$, M^0 has $\mathcal{S} = \{\lambda \mathrm{Id}_2 : \lambda \in \mathbb{F}_q\}$ as a submodule.
Let $N \subseteq M^0$. Then either $N \subseteq \mathcal{S}$ subgroup or $N = M^0$.

Lemma 4 (several copies): Let $N \subseteq \overbrace{M^0 \oplus \ldots \oplus M^0}^{m}$. Then $N \simeq N_1 \oplus \ldots \oplus N_n$, with $N_i \subseteq M^0$ submodule.

$\Rightarrow$ If $p = 2$: $H \simeq \underbrace{M^0 \oplus \ldots \oplus M^0}_{\alpha} \oplus \underbrace{C_2 \oplus \ldots \oplus C_2}_{\beta}$, with $C_2 \subset \mathcal{S}$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

(a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

(*a*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$

(*b*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (*a*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (*b*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (*c*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (*a*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (*b*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (*c*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and t = number of different traces in $\mathrm{Im}(\rho)$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (*a*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (*b*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (*c*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and t = number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (c) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and $t =$ number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ and $t = q^{m+1}$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

(a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$

(b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$

(c) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and $t =$ number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ and $t = q^{m+1}$.

If $p = 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (c) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and t = number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ and $t = q^{m+1}$.

If $p = 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$

$t = q^\alpha \cdot ((q-1)2^\beta + 1)$,

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

(a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
(b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
(c) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and t = number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ and $t = q^{m+1}$.

If $p = 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$

$t = q^\alpha \cdot ((q-1)2^\beta + 1)$, for $0 \leq \alpha \leq m$, $0 \leq \beta \leq d(m - \alpha)$.

Explicit determination of $\mathrm{Im}(\rho_f)$

Theorem 1. (A.) $\mathbb{F}_q$ with $q \neq 2, 3, 5$.
$(\mathbb{T}, \mathfrak{m})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$.
Suppose that $\mathfrak{m}^2 = 0$.
$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ continuous representation such that

- (a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} = \rho \bmod \mathfrak{m}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$
- (b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$
- (c) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$, and $t =$ number of different traces in $\mathrm{Im}(\rho)$.

If $p \neq 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ and $t = q^{m+1}$.

If $p = 2$: $\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$

$t = q^\alpha \cdot ((q-1)2^\beta + 1)$, for $0 \leq \alpha \leq m$, $0 \leq \beta \leq d(m - \alpha)$. Moreover $\mathrm{Im}(\rho)$ is determined uniquely by t up to isomorphism.

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$.

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function HeckeAlgebras [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$.

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound}, \ \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$. If $\mathfrak{m}_f^2 \neq 0$, we take $\mathbb{T}_f/\mathfrak{m}_f^2$.

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound}, \ \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$. If $\mathfrak{m}_f^2 \neq 0$, we take $\mathbb{T}_f/\mathfrak{m}_f^2$.

From the 3 Hecke algebras, only one satisfies $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$.

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$. If $\mathfrak{m}_f^2 \neq 0$, we take $\mathbb{T}_f/\mathfrak{m}_f^2$.

From the 3 Hecke algebras, only one satisfies $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$.

− The field is $\mathbb{F}_4$

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound, } \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$. If $\mathfrak{m}_f^2 \neq 0$, we take $\mathbb{T}_f/\mathfrak{m}_f^2$.

From the 3 Hecke algebras, only one satisfies $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$.

– The field is $\mathbb{F}_4$
– $D = 1$, so actually $\mathrm{Im}(\overline{\rho}_f) = \mathrm{SL}_2(\mathbb{F}_q)$, and $\mathrm{Im}(\rho_f) \subseteq \mathrm{SL}_2(\mathbb{T}_f)$

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

Fix a prime p, a level $N \geq 1$ coprime to p, and a weight $k \geq 2$.

With the function $\mathrm{HeckeAlgebras}$ [1] implemented in *Magma* we obtain every local mod p Hecke algebra $\mathbb{T}_f$ (up to Galois conjugacy) of level N and weight k

$$\mathbb{T}_f = \langle T_\ell \text{ Hecke operator } \mid \ell \leq \text{ Sturm bound}, \ \ell \nmid Np \rangle.$$

Example: $p = 2$, $N = 133$ and $k = 2$. There are 3 such Hecke algebras.

For every $\mathbb{T}_f$, let $\mathbb{F}_q := \mathbb{T}_f/\mathfrak{m}_f$ be its residue field. We check if the residual image is $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$. If $\mathfrak{m}_f^2 \neq 0$, we take $\mathbb{T}_f/\mathfrak{m}_f^2$.

From the 3 Hecke algebras, only one satisfies $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$.

- The field is $\mathbb{F}_4$
- $D = 1$, so actually $\mathrm{Im}(\overline{\rho}_f) = \mathrm{SL}_2(\mathbb{F}_q)$, and $\mathrm{Im}(\rho_f) \subseteq \mathrm{SL}_2(\mathbb{T}_f)$
- $\mathbb{T}_f/\mathfrak{m}_f^2 \simeq \mathbb{F}_4[X, Y]/(X^2, Y^2, XY)$

[1] It can be found in G. Wiese webpage http://math.uni.lu/ wiese/

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G.

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

bound $= 1000$. We find $\widetilde{t} = 13$

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

bound $= 1000$. We find $\widetilde{t} = 13$

$t = q^\alpha \cdot ((q-1)2^\beta + 1)$, for some $0 \leq \alpha \leq 2$ and $0 \leq \beta \leq 2(2-\alpha)$,

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

bound = 1000. We find $\widetilde{t} = 13$

$t = 4^0 \cdot ((4-1)2^2 + 1) = 13$

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

bound $= 1000$. We find $\widetilde{t} = 13$

$t = 4^0 \cdot ((4-1)2^2 + 1) = 13$

0×38,			
1×12,	$(Y + a) \times 12$	$(X + Y + a^2) \times 10$	$(aX + aY + 1) \times 13$
$a \times 10$,	$(aY + a^2) \times 10$	$(X + a^2Y + a^2) \times 7$	$(a^2X + aY + a) \times 6$
$a^2 \times 7$,	$(a^2Y + 1) \times 13$	$(aX + Y + 1) \times 16$	$(a^2X + a^2Y + a) \times 11$

where $\mathbb{F}_4 = \{0, 1, a, a^2\}$.

How can we compute $\mathrm{Im}(\rho_f)$ in concrete examples?

By Theorem 1: the number t of traces in $G := \mathrm{Im}(\rho_f)$ determines G.

$\widetilde{t} = \#$ different operators T_ℓ, with $\ell < b$ bound

Since $\mathbf{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell$, $\widetilde{t} = \#$ different traces in G. We have $\widetilde{t} \leq t$.

bound $= 1000$. We find $\widetilde{t} = 13$

$t = 4^0 \cdot ((4-1)2^2 + 1) = 13$

0×38,			
1×12,	$(Y + a) \times 12$	$(X + Y + a^2) \times 10$	$(aX + aY + 1) \times 13$
$a \times 10$,	$(aY + a^2) \times 10$	$(X + a^2 Y + a^2) \times 7$	$(a^2 X + aY + a) \times 6$
$a^2 \times 7$,	$(a^2 Y + 1) \times 13$	$(aX + Y + 1) \times 16$	$(a^2 X + a^2 Y + a) \times 11$

where $\mathbb{F}_4 = \{0, 1, a, a^2\}$.

It seems likely that $t = \widetilde{t} = 13$. So, according to Theorem 1:

$$\mathrm{Im}(\rho_f) \simeq (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_4) \simeq \mathrm{SL}_2(\mathbb{F}_4[X, Y]/(X^2, Y^2, XY)).$$

More examples in characteristic 2: $m = 1$

More examples in characteristic 2: $m = 1$

$1 \leq N \leq 1500, \quad k = 2, 3$
$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 1$
$t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1), \quad 0 \leq \alpha \leq 1$ and $0 \leq \beta \leq d(1-\alpha)$

More examples in characteristic 2: $m = 1$

$1 \leq N \leq 1500, \quad k = 2, 3$
$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 1$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \leq \alpha \leq 1$ and $0 \leq \beta \leq d(1-\alpha)$

$\mathbb{F}_{2^2}$		β		
		0	1	2
α	0	**4**	**7**	**13**
	1	**16**	-	-

$\mathbb{F}_{2^3}$		β			
		0	1	2	3
α	0	**8**	**15**	**29**	**57**
	1	**64**	-	-	-

$\mathbb{F}_{2^4}$		β				
		0	1	2	3	4
α	0	**16**	**31**	**61**	**121**	**241**
	1	**256**	-	-	-	-

Table : Possible number of traces when $m = 1$.

More examples in characteristic 2: $m = 1$

$1 \leq N \leq 1500, \quad k = 2, 3$
$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 1$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \leq \alpha \leq 1$ and $0 \leq \beta \leq d(1-\alpha)$

$\mathbb{F}_{2^2}$		β = 0	1	2
α	0	**4**	**7**	**13**
	1	**16**	-	-

$\mathbb{F}_{2^3}$		β = 0	1	2	3
α	0	**8**	**15**	**29**	**57**
	1	**64**	-	-	-

$\mathbb{F}_{2^4}$		β = 0	1	2	3	4
α	0	**16**	**31**	**61**	**121**	**241**
	1	**256**	-	-	-	-

Table : Possible number of traces when $m = 1$.

More examples in characteristic 2: $m = 1$

$1 \leq N \leq 1500, \quad k = 2, 3$
$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 1$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \leq \alpha \leq 1$ and $0 \leq \beta \leq d(1-\alpha)$

$\mathbb{F}_{2^2}$		$\beta = 0$	$\beta = 1$	$\beta = 2$
α	0	**4**	**7**	**13**
	1	**16**	-	-

$\mathbb{F}_{2^3}$		$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$
α	0	**8**	**15**	**29**	**57**
	1	**64**	-	-	-

$\mathbb{F}_{2^4}$		$\beta = 0$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
α	0	**16**	**31**	**61**	**121**	**241**
	1	**256**	-	-	-	-

Table : Possible number of traces when $m = 1$.

This corresponds always to the group $G \simeq C_2 \times \mathrm{SL}_2(\mathbb{F}_q)$.

More examples in characteristic 2: $m = 2$

More examples in characteristic 2: $m = 2$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 2$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 2$ and $0 \le \beta \le d(2-\alpha)$

More examples in characteristic 2: $m = 2$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 2$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 2$ and $0 \le \beta \le d(2-\alpha)$

$\mathbb{F}_{2^2}$		β				
		0	1	2	3	4
α	0	**4**	**7**	**13**	**25**	**49**
	1	**16**	**28**	**52**	**100**	-
	2	**64**	-	-	-	-

$\mathbb{F}_{2^3}$		β						
		0	1	2	3	4	5	6
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**
	1	**64**	**120**	**232**	**456**	-	-	-
	2	**512**	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**916**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	-	-	-	-
	2	**4096**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 2$.

More examples in characteristic 2: $m = 2$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 2$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \leq \alpha \leq 2$ and $0 \leq \beta \leq d(2-\alpha)$

$\mathbb{F}_{2^2}$		β				
		0	1	2	3	4
α	0	**4**	**7**	**13**	**25**	**49**
	1	**16**	**28**	**52**	**100**	-
	2	**64**	-	-	-	-

$\mathbb{F}_{2^3}$		β						
		0	1	2	3	4	5	6
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**
	1	**64**	**120**	**232**	**456**	-	-	-
	2	**512**	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**916**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	-	-	-	-
	2	**4096**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 2$.

More examples in characteristic 2: $m = 2$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 2$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 2$ and $0 \le \beta \le d(2-\alpha)$

$\mathbb{F}_{2^2}$		β: 0	1	2	3	4
α	0	**4**	**7**	**13**	**25**	**49**
	1	**16**	**28**	**52**	**100**	-
	2	**64**	-	-	-	-

$\mathbb{F}_{2^3}$		β: 0	1	2	3	4	5	6
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**
	1	**64**	**120**	**232**	**456**	-	-	-
	2	**512**	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β: 0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**916**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	-	-	-	-
	2	**4096**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 2$.

More examples in characteristic 2: $m = 3$

More examples in characteristic 2: $m = 3$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 3$
$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 3$ and $0 \le \beta \le d(3-\alpha)$

More examples in characteristic 2: $m = 3$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 3$

$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 3$ and $0 \le \beta \le d(3-\alpha)$

$\mathbb{F}_{2^2}$		β						
		0	1	2	3	4	5	6
α	0	**4**	**7**	**13**	**25**	**49**	**97**	**193**
	1	**16**	**28**	**52**	**100**	**196**	-	-
	2	**64**	**112**	**208**	-	-	-	-
	3	**256**	-	-	-	-	-	-

$\mathbb{F}_{2^3}$		β									
		0	1	2	3	4	5	6	7	8	9
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**	**897**	**1793**	**3585**
	1	**64**	**120**	**232**	**456**	**904**	**1800**	**3592**	-	-	-
	2	**512**	**960**	**1856**	**3648**	-	-	-	-	-	-
	3	**4096**	-	-	-	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**961**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	**7969**	**15376**	**30736**	**61456**
	2	**4096**	**7936**	**15616**	**30976**	**61696**	-	-	-	-
	3	**65536**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 3$.

More examples in characteristic 2: $m = 3$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 3$

$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 3$ and $0 \le \beta \le d(3-\alpha)$

$\mathbb{F}_{2^2}$		β						
		0	1	2	3	4	5	6
α	0	**4**	**7**	**13**	**25**	**49**	**97**	**193**
	1	**16**	**28**	**52**	**100**	**196**	-	-
	2	**64**	**112**	**208**	-	-	-	-
	3	**256**	-	-	-	-	-	-

$\mathbb{F}_{2^3}$		β									
		0	1	2	3	4	5	6	7	8	9
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**	**897**	**1793**	**3585**
	1	**64**	**120**	**232**	**456**	**904**	**1800**	**3592**	-	-	-
	2	**512**	**960**	**1856**	**3648**	-	-	-	-	-	-
	3	**4096**	-	-	-	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**961**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	**7969**	**15376**	**30736**	**61456**
	2	**4096**	**7936**	**15616**	**30976**	**61696**	-	-	-	-
	3	**65536**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 3$.

More examples in characteristic 2: $m = 3$

$m = \dim_{\mathbb{F}_q} \mathfrak{m}_f / \mathfrak{m}_f^2 = 3$

$t = q^\alpha \cdot ((q-1)2^\beta + 1), \quad 0 \le \alpha \le 3$ and $0 \le \beta \le d(3-\alpha)$

$\mathbb{F}_{2^2}$		β						
		0	1	2	3	4	5	6
α	0	**4**	**7**	**13**	**25**	**49**	**97**	**193**
	1	**16**	**28**	**52**	**100**	**196**	-	-
	2	**64**	**112**	**208**	-	-	-	-
	3	**256**	-	-	-	-	-	-

$\mathbb{F}_{2^3}$		β									
		0	1	2	3	4	5	6	7	8	9
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**	**897**	**1793**	**3585**
	1	**64**	**120**	**232**	**456**	**904**	**1800**	**3592**	-	-	-
	2	**512**	**960**	**1856**	**3648**	-	-	-	-	-	-
	3	**4096**	-	-	-	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**961**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	**7969**	**15376**	**30736**	**61456**
	2	**4096**	**7936**	**15616**	**30976**	**61696**	-	-	-	-
	3	**65536**	-	-	-	-	-	-	-	-

Table : Possible number of traces when $m = 3$.

Conclusions

Conjecture. If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 2$, then

$$\mathrm{Im}(\rho_f) \simeq \begin{cases} (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q). \end{cases}$$

Conclusions

Conjecture. If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 2$, then

$$\mathrm{Im}(\rho_f) \simeq \begin{cases} (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q). \end{cases}$$

Conjecture. If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 3$, then

$$\mathrm{Im}(\rho_f) \simeq \begin{cases} (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (C_2 \oplus C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2 \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q). \end{cases}$$

Application: existence of p-elementary abelian extensions

Application: existence of p-elementary abelian extensions

Proposition. $\mathbb{F}_q$ finite field of characteristic $p \neq 2$ with $q \geq 7$.
$(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$ and $\mathfrak{m}_{\mathbb{T}}^2 = 0$.
$m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}}$ and $t = \#$different traces in $\mathrm{Im}(\rho)$.
$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ Galois representation unramified outside Np such that

(*i*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ is the residual representation and $D = \mathrm{Im}(\det \circ \overline{\rho})$.
(*ii*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.
(*iii*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.

Application: existence of p-elementary abelian extensions

Proposition. $\mathbb{F}_q$ finite field of characteristic $p \neq 2$ with $q \geq 7$.
$(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$ and $\mathfrak{m}_{\mathbb{T}}^2 = 0$.
$m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}}$ and $t = \#$different traces in $\mathrm{Im}(\rho)$.
$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ Galois representation unramified outside Np such that

- (*i*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ is the residual representation and $D = \mathrm{Im}(\det \circ \overline{\rho})$.
- (*ii*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.
- (*iii*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.

Then there are number fields $L/K/\mathbb{Q}$ with $G_L = \ker(\rho)$ and $G_K = \ker(\overline{\rho})$ such that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$

Application: existence of p-elementary abelian extensions

Proposition. $\mathbb{F}_q$ finite field of characteristic $p \neq 2$ with $q \geq 7$.
$(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$ and $\mathfrak{m}_{\mathbb{T}}^2 = 0$.
$m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}}$ and $t = \#$different traces in $\mathrm{Im}(\rho)$.
$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ Galois representation unramified outside Np such that

- *(i)* $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ is the residual representation and $D = \mathrm{Im}(\det \circ \overline{\rho})$.
- *(ii)* $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.
- *(iii)* $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.

Then there are number fields $L/K/\mathbb{Q}$ with $G_L = \ker(\rho)$ and $G_K = \ker(\overline{\rho})$ such that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$ and

$$\mathrm{Gal}(L/\mathbb{Q}) = \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

Application: existence of p-elementary abelian extensions

Proposition. $\mathbb{F}_q$ finite field of characteristic $p \neq 2$ with $q \geq 7$.
$(\mathbb{T}, \mathfrak{m}_\mathbb{T})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_\mathbb{T} \simeq \mathbb{F}_q$ and $\mathfrak{m}_\mathbb{T}^2 = 0$.
$m := \dim_{\mathbb{F}_q} \mathfrak{m}_\mathbb{T}$ and $t = \#$different traces in $\mathrm{Im}(\rho)$.
$\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{T})$ Galois representation unramified outside Np such that

- (*i*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} := G_\mathbb{Q} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ is the residual representation and $D = \mathrm{Im}(\det \circ \overline{\rho})$.
- (*ii*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.
- (*iii*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.

Then there are number fields $L/K/\mathbb{Q}$ with $G_L = \ker(\rho)$ and $G_K = \ker(\overline{\rho})$ such that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$ and

$$\mathrm{Gal}(L/\mathbb{Q}) = \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

with $\mathrm{Gal}(K/\mathbb{Q})$ acting on $\mathrm{Gal}(L/K)$ by conjugation.

Application: existence of p-elementary abelian extensions

Proposition. $\mathbb{F}_q$ finite field of characteristic $p \neq 2$ with $q \geq 7$.
$(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ finite-dimensional local commutative $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$ and $\mathfrak{m}_{\mathbb{T}}^2 = 0$.
$m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}}$ and $t = \#$different traces in $\mathrm{Im}(\rho)$.
$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ Galois representation unramified outside Np such that

- (*i*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ is the residual representation and $D = \mathrm{Im}(\det \circ \overline{\rho})$.
- (*ii*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.
- (*iii*) $\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.

Then there are number fields $L/K/\mathbb{Q}$ with $G_L = \ker(\rho)$ and $G_K = \ker(\overline{\rho})$ such that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$ and

$$\mathrm{Gal}(L/\mathbb{Q}) = \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

with $\mathrm{Gal}(K/\mathbb{Q})$ acting on $\mathrm{Gal}(L/K)$ by conjugation.
L/K is abelian of degree p^{3dm} unramified at all primes $\ell \nmid pN$, and cannot be defined over $\mathbb{Q}$.

Gràcies!