THE UNIVERSITY OF CHICAGO

ON WEIGHT 2 LEVEL N NEWFORMS CONGRUENT TO EISENSTEIN SERIES WHEN N IS FOUR PRIMES

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
BINGJIN LIU

CHICAGO, ILLINOIS
AUGUST 2022

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor Matthew Emerton for his continuous support and patient guidance during my PhD study. I benefited a lot from his immense knowledge and mathematical motivation.

My gratitude extends to Frank Calegari for being my second advisor, and for the valuable comments and suggestions on this thesis.

The inclusive research environment at the math department and especially the number theory group is inspirational. I want to thank the professors and friends here, including Prof. Kazuya Kato, Yiwen Zhou, Gal Porat, Noah Taylor, Shiva Chidambaram, Billy Lee, Chengyang Bao, Sarah Reitzes, Boming Jia and many others, for their help and support.

I would like to express my thanks to my parents and my boyfriend Shuo Pang. Without their love and encouragement I could not complete this PhD journey.

ABSTRACT

Fix a prime $p \geq 5$. In this thesis we study the modularity problem of the Galois representation $\bar{\rho} = \mathbb{1} \oplus \bar{\chi}$, where $\bar{\chi}$ is a cyclotomic character mod p and $\mathbb{1}$ is the trivial one. Assuming N is a product of four distinct primes and $p \nmid N$, we give a sufficient condition on N such that there exists weight 2 level N newforms whose associated mod p representation is isomorphic to $\bar{\rho}$.

Our method is based on level-rising techniques using the geometry of Jacobian varieties of Shimura curves (see e.g. [17]) and pseudodeformation theory (see e.g. [14]).

CHAPTER 1

INTRODUCTION

1.1 background

Fix a prime $p \geq 5$ and f a weight 2 level $\Gamma_0(M)$ newform with $(p, M) = 1$, it is well known that a $p-$adic representation can be associated to f, denoted as $\rho_{f,p}$. The mod p representation $\bar{\rho}_{f,p}$ is unique after semisimplification. If $\bar{\rho}_{f,p}$ is reducible, $\bar{\rho}_{f,p} \cong \mathbb{1} \oplus \bar{\chi}$, where $\mathbb{1}$ is the trivial character and $\bar{\chi}$ is the cyclotomic character mod p [3, Proposition 3.1]. $\bar{\rho}_{f,p}$ being reducible is equivalent to f being congruent to an Eisenstein series mod p.
If M is a single prime, in [9], Mazur proved that $\bar{\rho}_{f,p}$ is reducible if and only if $p|(M-1)$. Later, many cases for squarefree levels were studied. Ribet used level-rising methods [11, 10] to prove some necessary and sufficient conditions. Yoo gave more sufficient conditions in [17]. Wake and Wang-Erickson developed the deformation theory for pseudorepresentations satisfying stable conditions in [12], and used this theory to study the analogue of Mazur's Eisenstein ideal with certain squarefree level in [13] and [14].

If the level M is a product of distinct primes, the eigenvalue of the Hecke operator U_r of f is either -1 or 1 for each prime r with $r|M$. After arranging the order of prime factors, $M = r_1 \cdots r_t$. And fix d such that $1 \leq d \leq t$, we are interested in the existence of a weight 2 newform of level M such that

- there is some prime ideal $\mathfrak{p}$ above p inside the coefficient field K_f of f, and the reduction of f at $\mathfrak{p}$ is Eisenstein.
  I.e $a_s(f) \bmod \mathfrak{p} \equiv s + 1$ for all $s \nmid M$
- $U_{r_i} f = f$ for all $1 \leq i \leq d$ and $U_{r_j} f = -f$ for all $d + 1 \leq j \leq t$

Definition 1.1. A t-tuple $(r_1, \cdots, r_t)$ of distinct primes is called *admissible for d* if such a newform exists.

The following theorem is the necessary condition due to Ribet [14, Theorem 1.2].

Theorem 1.1. *(Necessary condition)*
$p \geq 5$ is a fixed prime, assume $(r_1, \cdots, r_t)$ is admissible for d, then

1. *$d \geq 1$*
2. *p divides $\prod_{i=1}^{t}(r_i - 1)$ if $t = d$*
3. *$r_j \equiv -1 \ mod\ p$ for $d + 1 \leq j \leq t$*

Many sufficient conditions are known, see e.g. [17, Theorem 1.3]. In this thesis, we study particularly some sufficient condition for the case $t = d = 4$.
We assume $M = lr_1r_2q$ with $l \equiv 1 \bmod p$ to meet the necessary condition of (l, r_1, r_2, q) being admissible.

Let D be r_1r_2, N be Dl, and $\mathbb{T}^D(l)^{\text{new}}$ be the $\mathbb{Z}_p$ Hecke algebra generated by T_s with $s \nmid N$ and U_r with $r|N$ acting on the new part of the Jacobian $J^D(l)$ of the Shimura curve $X^D(l)$. Let $I := (U_r - 1 : r|N, T_s - (s+1) : s \nmid N) \subset \mathbb{T}^D(l)^{\text{new}}$, and $\mathfrak{m} := (I, p)$

Theorem 1.2. *[17, Theorem 6.4] Assume $p \geq 5$ and $l \equiv 1 mod\ p$, if $T_q - q - 1$ is not a generator of $I_{\mathfrak{m}}$ in $\mathbb{T}^D(l)^{new}_{\mathfrak{m}}$, then $\{r_1, r_2, l, q\}$ is admissible for $t = d = 4$.*

As in Wake and Wang-Erickson's paper [14], we can study the generators of Eisenstein ideal using pseudodeformation theory.

1.1.1 pseudorepresentation and $R = T$

Recall $N = Dl$, there is a unique weight 2 level $\Gamma_0(N)$ Eisenstein series (up to scalar) such that it is an eigenform for every T_s with $s \nmid N$ and U_r acts by 1 for every $r|N$, denoted by E. And $E \in M_2(\Gamma_0(N), \mathbb{Q}_p)$.
The space $M := \mathbb{Q}_p E \oplus S_2(\Gamma_0(N), \mathbb{Q}_p)^{\text{new}}$.
T is the $\mathbb{Z}_p$ Hecke algebra generated by $\{T_s, U_r\}$ acting on M localized at $\mathfrak{m} = (T_s - s - 1 :$

$s \nmid N, U_r - 1 : r|N, p)$.

$I := (T_s - s - 1, U_r - 1) \subset T$ is the Eisenstein ideal. The cuspidal part of T is denoted by T° which is the localized Hecke algebra acting on $S_2(\Gamma_0(N), \mathbb{Q}_p)^{\text{new}}$, while the ideal $I^\circ := (T_s - s - 1, U_r - 1) \subset T^\circ$ is the image of I.

And from Jacquet-Langlands, T° is isomorphic to $\mathbb{T}^D(l)^{\text{new}}_{\mathfrak{m}}$ mentioned above. $I^\circ \subset T^\circ$ corresponds to $I_{\mathfrak{m}} \subset \mathbb{T}^D(l)^{\text{new}}_{\mathfrak{m}}$.

The question becomes whether $T_q - (q+1)$ generates the Eisenstein ideal I°.

On the other hand, we consider the pseudodeformation functor. We define a functor $\text{PsDef}_{\bar{D},N}$ which sends A to the set of pseudorepresentations $D : G_{\mathbb{Q},S} \to A$ which lifts $\bar{D} := \det(\mathbb{1} \oplus \bar{\chi})$ and is finite-flat at p and Steinberg at $r|N$. This functor is represented by R_N. For detailed definition, check 2.5.

1.2 results

Theorem 1.3. *Assume $l \equiv 1$ mod p, $r_1, r_2 \not\equiv 1$ mod p and r_1 is not a p-th power mod l,*

1. *There is an isomorphism $R_N \xrightarrow{\sim} T$.*
2. *The localized Eisenstein ideal $I^\circ \subset T^\circ$ is principally generated. Thus T° is monogenic.*
3. *Furthermore, we assume $q \equiv 1$ mod p and $R := r_1^a r_2$ for some $0 \leq a \leq p-1$ such that R is a p-th power mod l, if R is also a p-th power mod q then $T_q - (q+1)$ does not generate I°. Thus the $4-$tuple (l, r_1, r_2, q) is admissible for $d = 4$.*

Idea of proof:

$R_N \to \mathbb{Z}_p$ is the map giving rise to the pseudorepresentation induced from the Galois representation associated with the Eisenstein series E. J^{min} is the kernel of the map.

We compute the sizes

$$\#(\frac{J^{min}}{(J^{min})^2}) \leq \#(\frac{\mathbb{Z}_p}{(l-1)\mathbb{Z}_p}) = \#(\frac{\mathbb{Z}_p}{\mathrm{Ann}_T(I)})$$

and apply Wiles' criterion to show $R_N \xrightarrow{\sim} T$.

Then we study in details the tangent space of R_N, which is a 1-dimensional $\mathbb{F}_p$-vector space. We explicitly construct a GMA representation which is finite-flat at p and Steinberg at r with $r|N$.

Then $T_q - (q+1)$ generates I° is equivalent to $\mathrm{tr}(\mathrm{Frob}_q) - (q+1)$ generates J^{min}, the latter can be computed through the explicitly constructed GMA representation.

Example 1.1. Let $(l, r_1, r_2) = (11, 2, 3)$, $N = 66$ and $p = 5$.

R is $r_1^2 r_2 = 12$ in this case, $q = 211, 271, 431$ with $q < 500$ are all the primes such that R is a 5-th power mod q.

There is a unique normalized newform f in $S_2(\Gamma_0(66), \mathbb{Q}_5)^{\mathrm{new}}$ congruent to E. The coefficient field for f is $\mathbb{Q}$.

The localized Hecke algebra $T^\circ \cong \mathbb{Z}_5$, and localized Eisenstein ideal $I^\circ \cong 5\mathbb{Z}_5$. For this toy example, η_q does not generate I° if and only if $a_q(f) \equiv (q+1) \bmod p^2$.

The latter condition holds for $q = 211, 271, 431$.

Example 1.2. Assume $(l, r_1, r_2) = (101, 2, 3)$, $p = 5$, then $N = 606$.

In this case, $T^\circ \cong \mathbb{Z}_5 \times_{\mathbb{F}_5} \mathbb{Z}_5[\sqrt{6}]$. The latter ring is

$$\{(a, b) \in \mathbb{Z}_5 \times \mathbb{Z}_5[\sqrt{6}] | a \bmod 5 \equiv b \bmod (5, \alpha - 1)\}$$

here α is one root of $x^2 - 6 = 0$.

From part 3 of above theorem $R = 6$. Let $q = 31$, then R is p-th power mod q, and $T_{31} - (31+1)$ does not generate T°.

For details of the example, check example 5.2.

CHAPTER 2

DEFORMATION THEORY FOR PSEUDOREPRESENTATIONS

This chapter covers definitions and basic properties of pseudorepresentations. The main references are [6],[2], [15].

2.1 Pseudorepresentation

In the deformation theory of usual Galois representations, if the residue representation is decomposable, its functor of deformations is not representable. It is natural to replace representations by *pseudorepresentations*.

Definition 2.1. Let R be a commutative ring, E an $R-$algebra, and G a group.

1. A *pseudorepresentation*, denoted $D : E \to R$ is a multiplicative polynomial law of degree d, for some $d \geq 1$. To be more precise,
   For each commutative R-algebra B, there is a map P_B

$$P_B : E \otimes_R B \to B$$

   such that

   - $P_B(1_{E\otimes_R B}) = 1_B$
   - P_B is multiplicative.

$$P_B(xy) = P_B(x)P_B(y) \text{for all } x, y \in E \otimes_R B$$

   - All $\{P_B\}_B$ are compatible, i.e for any R algebra map $B \to B'$, the diagram below

commutes:

$$\begin{array}{ccc} E \otimes_R B & \xrightarrow{P_B} & B \\ \downarrow & & \downarrow \\ E \otimes_R B' & \xrightarrow{P_{B'}} & B' \end{array}$$

- *homogeneous of degree d*

  For all $b \in B$ and $x \in E \otimes_R B$

$$P_B(bx) = b^d P_B(x)$$

2. Fix a pseudorepresentation (E, D), for every B and every $a \in E \otimes B$, the corresponding *characteristic polynomial* $\chi_B(a, t) \in B[t]$ is given by

$$\chi_B(a, t) := P_{B[t]}(t - a) : E \otimes B[t] \to B[t]$$

   Notation: use $\chi_B(a)$ to denote $\chi_B(a, a) \in B$.

3. Specially if $E = R[G]$, the R- group algebra , then (D, R) defined as above is also called a *pseudorepresentation of G*.

Example 2.1. Consider the R algebra map $\det(\rho) : R[G] \to R$ induced from the determinant map of a degree d group representation $\rho : G \to GL_d(R)$. It is a pseudorepresentation of degree d. And the characteristic polynomial for each element is the characteristic polynomial for the representation. The induced pseudorepresentation will be the same after semi-simplification of ρ.

Example 2.2. Pseudorepresentations of small degrees:

- **degree 0**

  For any B and any x in $E \otimes_R B$, $P_B(0) = P_B(0 \cdot x) = P_B(x)$ because of homogeneity. $P_B(0) = P_R(0)$. Because of multiplicity, $P_R(0) = P_R(0)^2$.

Fix E and R, there is a bijection between the set of *pseudorepresentation of degree* 0 and the set of *idempotents elements in* R induced by $D \to P(0)$.

In this case, the characteristic polynomial is

$$\chi_B(a,t) = P(0)$$

- **degree 1**

  Being homogeneous of degree 1 implies $P_B(u+v) = P_B(u) + P_B(v)$ [1]. Together with multiplicity, we can conclude P_B is an B-algebra homomorphism. There is a bijection between the set of *pseudorepresentation of degree* 1 *from* E *to* R and the set of R-*algebra homomorphism from* E *to* R given by $D \to P_R$.

  The characteristic polynomial is $\chi_B(a,t) = t - P_B(a)$.

- **degree 2**:

  Similarly as before, P_B is uniquely determined by P_R, which is given as

$$P_B(u+v) = P_B(u) + P_B(v) + f_B(u,v) \quad P_B(bu) = b^2 P_B(u)$$

  Here $f_B(u,v)$ is a B-module homomorphisms : $\mathrm{Sym}^2_B(E \otimes B) \to B$, and it is uniquely determined by f_R.

  The characteristic polynomial $\chi_B(a,t) = t^2 - f_B(a,1)t + P_B(a)$. The proof idea is similar to degree 1 case. [2]

---

1. Consider $B' = B[X,Y]$ and fixed $u, v \in E \otimes B$, $P_B(uX + uY)$ as a polynomial $Q(X,Y)$ satisfying $Q(\lambda X, \lambda Y) = \lambda Q(X,Y)$ for all $\lambda \in B$, thus $Q(X,Y) = a(u,v)X + b(u,v)Y$. Set $(X,Y) = (1,1),(1,0),(0,1)$, we have $P_B(u+v) = P_B(u) + P_B(v)$

2. Interested in $P_B(u+v)$. We can consider $B' = B[X,Y,Z]$, for any fixed u, v, s $P_{B'}(uX + vY + sZ)$ as a polynomial in B' is homogeneous of degree 2. By symmetries,

$$P_{B'}(uX + vY + sZ) = P_B(u)X^2 + P_B(v)Y^2 + P_B(s)Z^2 + f(u,v)XY + f(v,s)YZ + f(s,u)ZX$$

Setting (X,Y,Z) to be $(1,1,0)$ and other special values, we can derive $f(u,v)$ is symmetric and $B-$bilinear.

Lemma 2.1. [6, example 1.8,lemma 1.9]

- The set of degree 2 pseudorepresentations from E to R is bijective to $P : E \to R$ and an $R-$module homomorphism $f : \mathrm{Sym}^2_R E \to R$ satisfying:

  1. $P(1_E) = 1_R$
  2. P is multiplicative and $P(au) = a^2 P(u)$ for $a \in R$ and $u \in E$
  3. $P(u+v) = P(u) + P(v) + f(u,v)$
  4. $f(1,1) = 2$
  5. $f(ru, rv) = P(r)f(u,v)$ and $f(ur, vr) = f(u,v)P(r)$ for all $r, u, v \in E$
  6. $f(u,u')f(v,v') = f(uv, u'v') + f(uv', u'v)$ for all $u, v, u'v' \in E$

- Especially when $E := R[G]$, set $T(g) := f(g,1)$ and $D(g) := P(g)$ for $g \in G$. The bijective set consists of maps (T, D) from G to R satisfying:

  1. $D : G \to R^\times$ is a group homomorphism
  2. $T : G \to R$ is a map with $T(1) = 2$, and for all $g, h \in G$:
     (a) $T(gh) = T(hg)$
     (b) $D(g)T(g^{-1}h) - T(g)T(h) + T(gh) = 0$

- Furthermore, if 2 is invertible in R, we can recover D from T as

$$D(g) = \frac{T(g)^2 - T(g^2)}{2}$$

  . In this case, the bijection becomes an $R-$linear map $T : E \to R$ satisfying

  1. $T(1) = 2$
  2. $T(gh) = T(hg)$
  3. $T(x)T(y)T(z) - T(xy)T(z) - T(xz)T(y) - T(yz)T(x) + T(xyz) + T(xzy) = 0$

Proof. For the details, check [6, example 1.8,lemma 1.9].

The second part of the proof. $f(g,h) = T(h)T(g) - T(hg)$ by setting u', v' as 1. Also $f(g,h) = D(g)T(g^{-1}h)$ □

Remark 2.1. 1. The last equivalence is the definitions of pseudocharacters in many literatures.

2. For usual 2-dimensional group representations, T is the trace map.

2.1.1 Cayley-Hamilton algebra

Definition 2.2. (E, D) is a pseudorepresentation over R, we call (E, D) a *Cayley-Hamilton* R-algebra if E is a finitely generated R algebra and for every commutative $R-$algebra B and every $u \in E \otimes_R B$, u satisfies the characteristic polynomial $\chi_B(u,t) \in B[t]$, i.e $\chi_B(u) = 0$.

Example 2.3. If (E, D) is $(\mathrm{Mat}_d(R), det)$, then it is Cayley-Hamilton algebra because of Cayley-Hamilton Theorem.

More general pseudorepresentations are not necessarily Cayley-Hamilton, but there is a canonical Cayley-Hamilton quotient.

(E, D) is a pseudorepresentation over R of degree d. We use $CH(D) \subset R$ to denote the two-sided ideal of R generated by the coefficients

$$\chi(t_1 r_1 + \cdots + t_n r_n) \in E[t_1, ..., t_n]$$

with any $r_1, ..., r_n \in E$ and any $n \geq 1$.

We can claim (E, D) is Cayley-Hamilton if and only if $CH(D) = 0$. In degree 2 case, it suffices to show that $CH(D)$ is also the ideal generated by $\chi_R(u)$ for all $u \in E$. To see this, we introduce some facts.

Facts 2.1. • [15, definition 1.1.8.4]

The characteristic polynomial $\chi(u)$ for (E, D) over R $\chi(u)$ is a homogeneous degree d R polynomial law.

- [15, definition 1.1.2.14, proposition 1.1.2.16]

  $\chi(t_1 r_1 + \cdots + t_n r_n)$ is a homogeneous degree 2 polynomials in $t_1 \dots t_n$.

For one direction, let $n = 1$ and $t_1 = 1$ we have $\chi_R(u) \in CH(D)$. For other direction, we can plug in special values like$(t_1, t_2 \dots t_n) = (1, 1, 0 \dots 0)$.

Definition 2.3. The *kernel* of a pseudorepresentation (E, D), denoted by $\ker(D)$, is the set

$$\ker(D) = \{r \in E | \text{for any } B \text{ and any } r' \in E \otimes_R B \text{ any } b \in B, D_B(r \otimes b + r') = D_B(r')\}$$

Theorem 2.1. *1. $ker(D)$ is an ideal of E and $CH(D) \subset ker(D)$*

2. $D : E \to R$ factors through $ker(D)$, and $E/ker(D) \to R$ is faithful. $E/CH(D)$ is Cayley-Hamilton.

Proof. For the detailed proofs check [6, section 1.17]. Here we only give proofs in $d = 2$ and $2, 3$ are invertible in R.

In this case, D_B is uniquely determined by D_R, as $D_R \otimes B$. For the equation of the kernel, it suffice to only require $B = R$.

$$r \in \ker(D) \iff D(r + r') = D(r') \iff D(r) + T(r)T(r') - T(rr') = 0 \text{ for all } r'$$

$r' = 1$ implies $D(r) = -T(r)$, $r' = r$ implies $3D(r) = 0$, thus $r \in \ker(D)$ implies $T(r) = 0$ furthermore $T(rr') = 0$ for all r'.

In summary, $\ker(D) \cong \{r \in E | T(rr') = 0 \text{ for all } r'\}$.

Other claims follows. □

Next, we will discuss a special example of Cayley-Hamilton algebra.

Definition 2.4. A *generalized matrix algebra* over R (or $R-GMA$) is the data of

1. An R-algebra E that is finitely generated as an R-module
2. A set of orthogonal idempotents $e_1, ..., e_r \in E$ such that $\sum_i e_i = 1$
3. A set of isomorphisms of R-algebra $\phi_i : e_i E e_i \xrightarrow{\sim} M_{d_i}(R)$ for $i = 1, ..., r$

$\mathcal{E} := (\{e_i\}, \{\phi_i\})$ is called the *GMA structure* of E. And we call $(d_1, ..., d_r)$ the *type* of $(E, \mathcal{E})$.

For example, the matrix algebra $M_n(R)$ can be viewed as a $R-GMA$ of type $(d1, ..., d_r)$ as long as $\sum d_i = d$.

Example 2.4. [12, Lemma 3.1.5 Example 3.1.7] There is a bijection between $R-$GMA $(E, \mathcal{E})$ of type $(1, 1)$ and triples (B, C, m) where B, C are finitely generated $R-$modules and $m : B \otimes_R C \to R$ is an $R-$module homomorphism such that

$$\begin{array}{ccc} B \otimes_R C \otimes_R B & \xrightarrow{id\otimes(m\circ\iota)} & B \otimes_R R \\ \downarrow{\scriptstyle m\otimes id} & & \downarrow \\ R \otimes_R B & \longrightarrow & B \end{array} \qquad \begin{array}{ccc} C \otimes_R B \otimes_R C & \xrightarrow{id\otimes m} & C \otimes_R R \\ \downarrow{\scriptstyle (m\circ\iota)\otimes id} & & \downarrow \\ R \otimes_R C & \longrightarrow & C \end{array}$$

commute.

Here $\iota : C \otimes_R B \to B \otimes_R B$ is the isomorphism given by $b \otimes c \to c \otimes b$.

The R-GMA associated to a triple (B, C, m) is

$$E = \begin{pmatrix} R & B \\ C & R \end{pmatrix}$$

The idempotents in E is $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

The algebra structure of E is given by the matrix multiplication with $m : B \otimes C \to R$. The commutative diagram guarantees the associativity of the multiplication of E.
For the other direction of the bijection, for an $R-$GMA $(E, \mathcal{E})$, let $B := e_1Ee_2$ and $C := e_2Ee_1$, and $m : B \otimes C \to R$ is given by the multiplication in E as $m(e_1xe_2, e_2ye_1) = \phi_1(e_1xye_1) \in R$.

Example 2.5. a nontrivial-GMA structure
$R = \mathbb{Z}_p$, $B = \mathbb{Z}_p$ and $C = \mathbb{Z}_p \oplus \mathbb{Z}/p\mathbb{Z}$ and $m : B \otimes C \to \mathbb{Z}_p$ defined as $m(b \otimes (c, c')) = pbc$.

For a given R-GMA structure $(E, \mathcal{E})$, there is a canonical CH pseudorepresentation $D_{\mathcal{E}} : E \to R$ such that

$$\mathrm{Tr}_{D_{\mathcal{E}}}(x) = \mathrm{Tr}_{\mathcal{E}}(x) := \sum_{i}^{r} tr(\phi_i(e_ixe_i))$$

2.2 Representations of (E, D)

(E, D) is a d-dim pseudorepresentation over R, A is a commutative R-algebra.

Definition 2.5. A *compatible representation* of (E, D) over A is a pair (V_A, ρ_A), with V_A a projective A-module of rank d and $\rho_A : E \otimes_R A \to \mathrm{End}_A(V_A)$ a A-algebra homomorphism such that $D \otimes_A = \det \circ \rho_A$.

Definition 2.6. A *Cayley-Hamilton representation* (or *CH-representation* for short) (resp. *GMA representation*) of (E, D) over A is a pair $((E', D'), \rho_A)$, with (E', D') a A-CH algebra (resp. A-GMA algebra) and $\rho_A : E \otimes A \to E'$ a A-algebra homomorphism such that $D \otimes_R A = D' \circ \rho_A$.

In particular, for a group G, a *Cayley-Hamilton representation* (or *CH-representation for short*) of dimension d over A is a $((E, D), \rho$ with (R, D) a CH $d-$ dim pseudorepresentation and $\rho : G \to E^*$ is a group homomorphism. Similarly we can define *GMA representation* for a group G.

2.2.1 deformation problems

Notations:

k is a finite field, and $W(k)$ is the ring of Witt vectors.

$\mathrm{Alg}_{W(k)}$ is the category of commutative $W(k)$ algebra

$\hat{\mathcal{C}}_{W(k)} \subset \mathrm{Alg}_{W(k)}$ be the category of complete Noetherian local $W(k)$ algebras $(A, \mathfrak{m}_A)$ with residue field k.

Next, we introduce various deformation functors of pseudorepresentations.

PsR_G^d is a functor from $\mathrm{Alg}_{W(k)}$ to Sets defined as for any algebra A, $\mathrm{PsR}_G(A)$ is the set of all dimension $d$pseudorepresentations of G over A.

To save notation, we may also use PsR_G^d to denote the category with objects being $(A, (A[G], D))$ with A a commutative $W(k)$-algebra, and $D : A[G] \to A$ a dim$-d$ pseudorepresentation; with arrows $(A, (A[G], D)) \to (A', (A'[G], D'))$ $f : A \to A'$ compatible with pseudorepresentations, $f \circ D = D'$.

The category $\mathcal{R}ep_G^d$ is the usual category of dim-d representation of G.

The category $\mathcal{CH}_G^d$ has objects being d-dim CH-representations of G over A, a commutative $W(k)-$ algebra, and arrows $(A_1, (E_1, D_1), \rho_1) \to (A_2, (E_2, D_2), \rho_2)$ pairs (f, g) with a $W(k)-$algebra homomorphism $f : A_1 \to A_2$, $g : E_1 \to E_2$ ring homomorphism compatible with A_1 and A_2 algebra structure, $\rho_2 = g \circ \rho_1$ and $f \circ D_1 = D_2 \circ g$.

Definition 2.7. Fix a pseudorepresentation $\bar{D} : G \to k$. Its deformation functor $\mathrm{PsDef}_{\bar{D}} : \hat{C}_{W(k)} \to \mathrm{Sets}$ is

$$A \to \{D : A[G] \to A \text{ such that } D \otimes_A k \cong \bar{D}\}$$

and elements of $\mathrm{PsDef}_{\bar{D}}(A)$ are called *pseudodeformation*.

$\mathrm{PsDef}_{\bar{D}}$ is a subfunctor of PsR_G^d above. Similarly, $\mathcal{CH}_{G,\bar{D}}^d$ is a subcategory of $\mathcal{CH}_G^d$ having objects $(A, (E, D))$ satisfying $D \otimes k \cong \bar{D}$. Below is a summary of representability of

functors defined above:

Theorem 2.2. *1. [6, Proposition 1.6]*

PsR^d_G is represented by a $W(k)$-algebra, denoted by $W(k)(G,d)$. And the universal pseudorepresentation is $D^u : W(k)(G,d)[G] \to W(k)(G,d)$.

2. [6, Proposition 1.23]

$(W(k)(G,d), (E^u, D^u), \rho^u)$ is the initial object of $\mathcal{CH}^d_G$. Here $E^u := W(k)(G,d)[G]/CH(D^u)$.

3. Above two statements also holds for $PsR^d_{G,\bar{D}}$ and $\mathcal{CH}^d_{G,\bar{D}}$.

[6, Theorem 2.12] claims that for a $d-$ dim pseudorepresentation $D : E \to \bar{k}$ with $\bar{k}$ an algebraically closed field, there exists a unique, up to isomorphism, semi-simple representation $\rho^{ss} : E \to M_d(\bar{k})$ such that $D = \det \circ \rho$ and $\ker\rho^{ss} = \ker(D)$.

Definition 2.8. Fix a field k, a pseudorepresentation $\bar{D} : E \to k$ is *multiplicity-free* if $\rho^{ss}_{\bar{D}\otimes\bar{k}}$, defined as above, has pairwise non-isomorphism simple factors and each of the factors is defined over k.

Theorem 2.3. *[15, Theorem 3.2.2] Let $\bar{D} : G \to k$ be multiplicity-free, and $(d_1, \cdots, d_r)$ be the dimensions of the simple factors of $\rho^{ss}_{\bar{D}}$. Let R be a Noetherian Henselian local ring with residue field k, and let (E, D, ρ) CH representation over R lifting $\bar{D}$, then there is an R-GMA structure $\mathcal{E}$ of type $(d_1, \cdots, d_r)$ on E such that $D = D_{\mathcal{E}}$.*

Remark 2.2. The "multiplicity-free" condition is necessary. Check one counter example below.

Some reasons why CH-representations are introduced:

- $\psi : \mathcal{CH}^d_G \to \mathrm{PsR}^d_G$ extends the functor $det : \mathcal{R}ep^d_G \to \mathrm{PsR}^d_G$.

- The functor ψ defined above is essentially surjective, i.e fix a pseudorepresentation (E, D) over R, it always has a CH representation given by $(E/CH(D), D)$, while *det* is not essentially surjective. One example is given below.

- Restricted to the subcategory of residually multiplicity-free pseudorepresentation over a local Henselian UFD, the functor *det* above is essentially surjective. For details, check [2, Proposition 1.6.1]. One counter example (not satisfying UFD condition) is given below.

2.2.2 Example

Example 2.6. (a CH representation but not a GMA representation)
The representation $\bar{\rho}$ of $G = \mathbb{Z}/3\mathbb{Z}$ over $\mathbb{F}_3$ comes from the standard representation of S_3, and with chosen basis, $\bar{\rho}(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
The pseudorepresentation $(E, D) = (\mathbb{F}_3[\mathbb{Z}/3\mathbb{Z}], \det)$ induced from this representation is characterized by the trace map $T : \mathbb{F}_3[\mathbb{Z}/3\mathbb{Z}] \to \mathbb{F}_3$ with $T([0]) = T([1]) = T([-1]) = 2$. Here we use $[i]$ to denote the element in $\mathbb{Z}/3\mathbb{Z}$.

This pseudorepresentation is not faithful. Because

$$\ker(\bar{D}) = \mathbb{F}_3([0] - [1]) + \mathbb{F}_3([0] - [-1])$$

$E \to E/\ker(\bar{D}) \xrightarrow[\bar{D}]{\sim} \mathbb{F}_3$ is the map $a[0] + b[1] + c[-1] \to a + b + c \to (a + b + c)^2$. The unique ρ^{ss} giving rise to $\bar{D}$ is

$$\rho^{ss} : \mathbb{Z}/3\mathbb{Z} \to GL_2(\mathbb{F}_3) \text{ mapping } [1] \to id$$

Thus $(E, \bar{D})$ is not multiplicity-free. And it is not CH.

$$\mathrm{CH}(\bar{D}) = \mathbb{F}_3([0] + [1] + [-1]) \subset \ker(\bar{D})$$

It maximal CH quotient $(E/\mathrm{CH}(\bar{D}), \bar{D})$ has no GMA-structure.

$E/\mathrm{CH}(\bar{D}) \cong \mathbb{F}_3 \oplus \mathbb{F}_3$ as $\mathbb{F}_3$-module. Only possible GMA-structure is of type $(1,1)$. The algebra homomorphism $\mathbb{F}_3[\rho] : E \to M_2(\mathbb{F}_3)$ factors as $E \to E/\mathrm{CH}(\bar{D}) \hookrightarrow M_2(\mathbb{F}_3)$. The only nontrivial idempotents in $M_2(\mathbb{F}_3)$ are $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ which are not in the image of $\mathbb{F}_3[\rho]$. Thus no GMA-structure on $E/\mathrm{CH}(\bar{D})$.

Example 2.7. (Toy example of a universal pseudodeformation ring) Consider the pseudorepresentation $(\bar{D} : \mathbb{F}_3[\mathbb{Z}/3\mathbb{Z}] \to \mathbb{F}_3)$ defined in above example. We will compute $\mathrm{PsR}^2_{\mathbb{Z}/3\mathbb{Z},\bar{D}}$.

Any dim 2 pseudorepresentation of $\mathbb{Z}/3\mathbb{Z}$ over A is uniquely determined by the trace map T, more specifically determined by $T([1])$ and $T([-1])$ ($T(0)$ automatically is 2).

Thus we can first construct a universal ring R^u representing functor $\mathrm{PsR}^2_{\mathbb{Z}/3\mathbb{Z}}$, and $R^u = \mathbb{Z}_3[X,Y]/J$, where ideal J is generated by $X^3 - 3XY + 4, Y^3 - 3XY + 4, X^2Y - Y^2 - 2X, XY^2 - X^2 - 2Y$. Here X, Y correspond to $T([1]), T([-1])$.

Let $D = (X^2 - Y)/2$, using Grbner basis $R^u \cong \mathbb{Z}_3[X,D]/(X^2 - D^2X - 2D, D^3 - 1)$. Here D corresponds to determinant of $[1]$. The trace map T^u of the universal pseudorepresentation $(R^u[\mathbb{Z}/3\mathbb{Z}], D^u)$ is the R^u-linear map determined by $T^u([1]) = X$ and $T^u([-1]) = X^2 - 2D$.

R^u is not a UFD, because $X^2 - D^2X - 2D = X^2 - D^2X - 2D^4 = (X - 2D^2)(X + D^2)$.

$CH(D^u)$ is the ideal generated by $[-1] - X[1] + D[0]$. And $\ker(D^u) = CH(D^u)$ in this case. The detailed computations are below:

$CH(D^u)$ is the ideal generated by $\chi(r) = r^2 - T(r)r + D(r)[0]$ for every $r \in E^u$. From the

equality of pseudorepresentation $D(a+b) = D(a) + D(b) + T(a)T(b) - T(ab)$, we have

$$\chi(a+b) = \chi(a) + \chi(b) + 2ab - T(a)b - T(b)a + T(a)T(b) - T(ab)$$

By writing general r as linear combinations of $[0], [1], [-1]$, we can show $CH(D^u)$ is generated by $\chi([1])$.

$\ker(D^u)$ is all $r = a[0] + b[1] + c[-1]$ such that $T(rr') = 0$ for all r'. It suffices to show for $r' \in \mathbb{Z}/3\mathbb{Z}$. In the middle of computations, it uses

$$(DX - 2)r = 0 \iff r \in \text{ideal } (DX + 1) \subset R^u$$

Next, we compute $R^u_{\bar{D}}$.

The residue pseudorepresentation $\bar{D}$ corresponds to the maximal ideal $\mathfrak{m} := (3, X+1, D-1)$. $\text{PsDef}_{\bar{D}}$ is represented by $\hat{R}^u_{\mathfrak{m}}$, the completion of R^u at the maximal ideal. The universal pseudorepresentation is $(\hat{E}^u := \hat{R}^u_{\mathfrak{m}}[\mathbb{Z}/3\mathbb{Z}], \hat{D}^u)$, and $\ker(\hat{D}^u) = \text{CH}(\hat{D}^u)$ is the ideal generated by $[-1] - X[1] + D[0]$.

In this case, there is no GMA-structure on $\hat{E}^u/CH(\hat{D}^u)$ (as a $\hat{R}^u_{\mathfrak{m}}$ module, it is free of rank 2). If GMA structure exists, there is an idempotent e corresponding to $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ whose trace is 1. No such element exists.

In this case, there is no adapted representation for $(\hat{E}^u, \hat{D}^u)$ over $\hat{R}^u$. If there is one, consider the pseudorepresentation over $(\mathbb{F}_3[\epsilon]/(\epsilon^2))$ induced by the map $f : \hat{R}^u_{\mathfrak{m}} \to \mathbb{F}[\epsilon]/(\epsilon^2)$ with $f[X] = \epsilon - 1, f[D] = 2\epsilon + 1$. This induced pseudorepresentation will have adapted representation $\rho : \mathbb{F}_3[\epsilon]/(\epsilon^2)[\mathbb{Z}/3\mathbb{Z}] \to M_2(\mathbb{F}_3[\epsilon]/(\epsilon^2))$. Assume $\rho([1]) = A + \epsilon B$, there is no solution for A and B.

Example 2.8. (Toy example where the universal CH algebra has a GMA-structure)

Consider the standard representation of S_3 over $\mathbb{F}_3$. Fix two generators $\sigma = (1, 2, 3)$ and

$\tau = (1,2)$ of S_3, and basis of $\mathbb{F}_3$ vector space $\{e_1, e_2\}$ with $ge_i = e_{g(i)}$, this representation (ρ, V) has an exact sequence

$$0 \to Id \to V \to \bar{\chi} \to 0$$

with nontrivial $\chi : S_3 \to \bar{\mathbb{Z}}/2\mathbb{Z} \to \mathbb{F}_3$.

Its induced pseudorepresentation is multiplicity free.

- Compute $\mathrm{PsR}^2_{G,\bar{D}}$:

  Any pseudo representation of S_3 over R is uniquely determined by $R-$linear trace function T, because of T being central, $T(g) = T(g')$ if g and g' are in the same conjugate class of S_3. Thus T is uniquely determined by $T(\sigma)$ and $T(\tau)$. Similarly as above example, PsR^2_G is represented by $\mathbb{Z}_3[x,y]/I$ with ideal $I = ((x-2)(x+1), y(x-2), y(y-2)(y+2))$. The maximal ideal corresponding to $\bar{D}$ is $\mathfrak{m} = (3, x+1, y)$. Thus $\mathrm{PsR}^2_{G,\bar{D}}$ is represented by $R^u := \mathbb{Z}_3[[x]]/(x-2)(x+1)$.

- Construct the $GMA-$structure:

  $D^u : R^u[S_3] \to R^u$ is not CH, its $CH(D^u)$ is generated by a single element $\sigma + \sigma^2 - x$. And $\mathrm{CH}(D^u) = \mathrm{Ker}(D^u)$. Thus as a $\mathbb{Z}_3$-module, $E^u/\mathrm{CH}(D^u) \cong \mathbb{Z}_3[S_3]$.

  According to the general theorem, there is a $GMA-$structure. For explicit constructions, we need to find idempotents. Consider $E^u/\mathrm{Ker}(\bar{D}) \cong \mathbb{F}_3 \oplus \mathbb{F}_3$, then from general theorem the idempotents in $E^u/\mathrm{Ker}(\bar{D})$ can always be lifted to $E^u/\mathrm{CH}(D)$. $\mathrm{Ker}(\bar{D})$ viewed as an ideal in $E^u/\mathrm{CH}(D)$ is generated by $3, 1-\sigma$. Thus $E^u/\mathrm{Ker}(\bar{D})$ as a $\mathbb{F}_3$ vector space has $1, \tau$ as basis. Its idempotents are $\frac{1}{2}(1+\tau)$ and $\frac{1}{2}(1+\tau)$, which can be lifted to $E^u/\mathrm{CH}(D)$ (they are already in).

  In this case, $B = e_1 E^u/\mathrm{CH}(D) e_2 = \mathbb{Z}_3(\sigma^2 - \sigma)(1+\tau)$ which is a R^u-module with x acting by $\sigma + \sigma^2$. And $C = e_2 E^u/\mathrm{CH}(D) e_1 = \mathbb{Z}_3(\sigma^2 - \sigma)(\tau - 1)$. $m : B \otimes C \to R^u$ is

determined by $m(b \otimes c) = \text{Trace}(bc) = 4(2 - x)$.

2.3 reducible locus of $\mathbf{PsR}^2_{G,\bar{D}}$

In this section we only consider the case where R is in $\hat{\mathcal{C}}_{W(k)}$, (E, D) is a $2-$dim residually multiplicity free pseudorepresentation. Its residual pseudorepresentation is $\bar{D} \cong \det(\bar{\chi_1} \oplus \bar{\chi_2})$. Furthermore assume (E, D) has a $GMA-$structure of type $(1, 1)$, denoted as $E \cong \begin{pmatrix} R & B \\ C & R \end{pmatrix}$.

Definition 2.9. (E, D) is *reducible* if there are two $R-$algebra morphism $\chi_i : E \to R$ $i = 1, 2$ lifting $\bar{\chi_i}$ such that

$$D \cong \det(\chi_1 \oplus \chi_2)$$

Remark 2.3. If (E, D) is has GMA-structure of type $(1, 1)$, then the trace map restricted to e_iEe_i (i.e. $T_{|e_iEe_i}$) is a $R-$algebra homomorphism.
Furthermore, if we assume (E, D) is reducible with $\bar{D} \cong \det(\bar{\chi_1} \oplus \bar{\chi_2})$, then $\{e_1, e_2\}$ can be chosen such that $\chi_1(x) = \chi_1(e_1xe_1) = T(e_1xe_1)$ for all $x \in E$. The reasons are below:
For the first part, because of $D(e_iEe_i) = 0$,

$$0 = D(e_i(x + y)e_i) - D(e_ixe_i) - D(e_iye_i) = T(e_ixe_i)T(e_iye_i) - T(e_ixe_iye_i)$$

For the second part, consider $(\bar{E}, \bar{D})$, $\{\bar{e}_1, \bar{e}_2\}$ are idempotents coming from E. We can label e_i such that $\bar{\chi}_i(e_i) = 1$ because only idempotents in a field are 0 and 1.

$$\chi_1(x) = \chi_1(e_1xe_1) + \chi_1(e_2xe_2) + \chi_1(e_1xe_2) + \chi_1(e_2xe_1) \text{ for any } x \in E$$

The later two are 0 because $e_1e_2 = 0$. After mod maximal ideal $\mathfrak{m}$, $\chi_1(e_2xe_2) \in \mathfrak{m}$.

$$1 = T(e_2) = \chi_1(e_2) + \chi_2(e_2)$$

Thus $\chi_2(e_2)$ is a unit in R, and $\chi_2(e_2)(\chi_2(e_2) - 1) = 0$, thus $\chi_2(e_2) = 1$,. Similarly, $\chi_1(e_1) = 1$. Thus $T(e_1xe_1) = \chi_1(e_1xe_1) + \chi_2(e_1xe_1) = \chi_1(e_1xe_1)$.

Lemma 2.2. There exists an ideal I of R such that for any ideal J of R, $I \subset J$ if and only if $(E, D) \otimes R/J$ is reducible. Moreover,

$$I = \text{image ideal of } m : B \otimes_R C \to R$$

I does not depend on choices of the $GMA-$structure.

Proof. For detailed proof, check [2, Proposition 1.5.1]

□

Fix a ideal J containing I, then there is $\chi_i : E/J \to R/J$ (unique up to isomorphism).

Theorem 2.4. *Fix a $GMA-$structure on E, there is a natural bijective map of $R/J-$modules*

$$\iota_B : Hom_R(B, R/J) \xrightarrow{\cong} Ext^1_{E/JE}(\chi_2, \chi_1)$$

$$\iota_C : Hom_R(C, R/J) \xrightarrow{\cong} Ext^1_{E/JE}(\chi_1, \chi_2)$$

Proof. For each $f \in \mathrm{Hom}_R(B, R/J)$, define $\rho_f : E/JE \to M_2(R/J)$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a & f(b) \\ 0 & d \end{pmatrix}$$

We can check that ρ_f is an algebra homomorphism. The construction is injective.

To check the subjectiveness, consider a E/J-module V in the extension class, $\rho : E/J \to M_2(R/J)$ written as $\begin{pmatrix} \chi_1 & f \\ 0 & \chi_2 \end{pmatrix}$ with $f : E/J \to R/J$.

We claim that ρ can be chosen such that $f(x) = f(e_1xe_2)$, thus can be viewed as a R/J-module map $B/J \to R/J$.

To see above claim:

$$f(x) = f(e_1xe_1 + e_2xe_2 + e_1xe_2 + e_2xe_1)$$

Because of the cocycle property of f and $\chi_i(e_i) = 1$, we have $f(e_2xe_1) = 0$ and $f(e_ixe_i) = \chi_i(x)f(e_i)$.

$$f(x) = \chi_1(x)f(e_1) + \chi_2(x)f(e_2) + f(e_1xe_2)$$

By changing new basis, we can choose f such that $f(e_1) = 0$, which implies $f(e_2) = 0 = f(id) - f(e_1)$. □

For the universal pseudodeformation $(R^u[G], D^u)$ over R^u lifting a multiplicity-free $\bar{D} = \det(\bar{\chi}_1 \oplus \bar{\chi}_2)$ of a group G, $R^{\mathrm{red}} := R^u/I$ with I the reducible ideal defined above.

E^u is the initial CH representation. $E^{\mathrm{red}} := E^u \otimes_{R^u} R^{\mathrm{red}} = \begin{pmatrix} R^{\mathrm{red}} & B^{\mathrm{red}} \\ C^{\mathrm{red}} & R^{\mathrm{red}} \end{pmatrix}$.

Remark 2.4. As a R-module homomorphism $m : B^{\mathrm{red}} \otimes_R C^{\mathrm{red}} \to I/I^2$. This is not contradicting with the fact that m^{red}, the R^{red}-module homomorphism map appearing in the GMA-structure of E^{red}, is 0. Here $m^{\mathrm{red}} : B^{\mathrm{red}} \otimes_{R^{\mathrm{red}}} C^{\mathrm{red}} \to R^{\mathrm{red}}$ can be viewed as the above m tensoring with R^{red} over R, which is 0.

Theorem 2.5. *1. R^{red} is the universal deformation ring for the functor sending A to the set of reducible pseudo deformations of G over A.*

There is a canonical isomorphism $R^{red} \cong R_{\bar{\chi}_1} \hat{\otimes} R_{\bar{\chi}_2}$ with $R_{\bar{\chi}_i}$ the universal deformation ring of $\bar{\chi}_i$.

2. *E^{red} is initial among all the reducible GMA-representation. To be more precise, if $\rho : G \to (E, D)$ is a $GMA-$representation of G over R lifting $\bar{D}$, then the resulting GMA map $(E^u, D^u) \to (E, D)$ factors through (E^{red}, D^{red}) if and only if ρ is reducible.*

3. *Furthermore, $A \in \mathcal{C}$ and M is a finitely generated $A-$module, and $\chi_{i,A} : G \to A^\times$ is a character lifting $\bar{\chi}_i$. There is a natural isomorphism*

$$Hom_A(B^{red} \otimes_{R^{red}} A, M) \xrightarrow{\sim} Ext^1_G(\chi_{2,A}, \chi_{1,A} \otimes M)$$

Similar isomorphism is true for C^{red}.

2.4 tangent space of the pseudodeformation functor

In this section, we only consider the dimension 2 case and the residue pseudodeformation is induced by two characters. For more general discussion on tangent space, check [1].

Fix $k[\epsilon]$ with $\epsilon^2 = 0$, and $\bar{D} = \det(\bar{\chi}_1 \otimes \bar{\chi}_2)$, χ_i distinct characters of group G.

The set of pseudorepresentations of G over $k[\epsilon]$ ($\mathrm{Hom}_{W(k)-alg}(R^u, k[\epsilon])$), denoted by $\mathcal{T}$ is naturally k-vector space.

The k-vector space structure is induced by the algebra homomorphism $\alpha : k[\epsilon] \to k[\epsilon]$ sending ϵ to $\alpha\epsilon$ with $\alpha \in k$.

There is a filtration of $\mathcal{T}$, $0 \subset \mathcal{T}_0 \subset \mathcal{T}$. Here $\mathcal{T}_0$ is the set of reducible pseudorepresentations of G over $k[\epsilon]$, i.e. $\mathrm{Hom}(R^{\mathrm{red}}, k[\epsilon])$.

Theorem 2.6. *There is an exact sequence*

$$0 \to \mathcal{T}_0 \to \mathcal{T} \xrightarrow{f} Ext^1_G(\bar{\chi}_2, \bar{\chi}_1) \otimes Ext^1_G(\bar{\chi}_1, \bar{\chi}_2) \xrightarrow{h} Ext^2_G(\bar{\chi}_1, \bar{\chi}_1) \oplus Ext^2_G(\bar{\chi}_2, \bar{\chi}_2)$$

and $\mathcal{T}_0 \cong Ext^1_G(\bar{\chi}_1, \bar{\chi}_1) \oplus Ext^1_G(\bar{\chi}_2, \bar{\chi}_2)$

Remark 2.5. • Recall the basic fact about Ext and cohomology.

$$\mathrm{Ext}^i_G(\chi, \chi\rho) \cong \mathrm{Ext}^i_G(1, \rho) \cong H^i(G, \rho)$$

The explicit definition for Ext^i:

$$Z^1_G(\bar{\chi}_1, \bar{\chi}_2) := \{a : G \to k | a(gg') = \bar{\chi}_2(g)a(g') + a(g)\bar{\chi}_1(g') \forall g, g' \in G\}$$

$$B^1_G(\bar{\chi}_1, \bar{\chi}_2) := \{a : G \to k | a(g) = \bar{\chi}_2(g)A - A\bar{\chi}_1(g)\ \exists A \in k \forall g \in G\}$$

$$Z^2_G(\bar{\chi}_1, \bar{\chi}_2) := \{b : G\times G \to k | \bar{\chi}_2(g)b(g', g'') - b(gg', g'') + b(g, g'g'') - b(g, g')\bar{\chi}_1(g'') = 0 \forall g, g', g'' \in G\}$$

$$B^2_G(\bar{\chi}_1, \bar{\chi}_2) := \{b : G\times G \to k | \exists\, a : G \to k \text{s.t. } b(g, g') = a(gg') - \bar{\chi}_2(g)a(g') - a(g)\bar{\chi}_1(g')\}$$

$\mathrm{Ext}^i_G(\bar{\chi}_1, \bar{\chi}_2)$ is defined as $Z^i_G(\bar{\chi}_1, \bar{\chi}_2)/B^i_G(\bar{\chi}_1, \bar{\chi}_2)$

- h appearing in above theorem is the natural map given by $h(a_1 \otimes a_2) = (b_1, b_2)$ with $b_1(g, g') = a_1(g)a_2(g')$ and $b_2(g, g') = a_2(g)a_1(g')$, here $a_1 \in \mathrm{Ext}^1_G(\bar{\chi}_2, \bar{\chi}_1)$ and $a_2 \in \mathrm{Ext}^1_G(\bar{\chi}_1, \bar{\chi}_2)$.
  The map h corresponds to cup products of cohomology groups.

Proof. Let $D : k[\epsilon][G] \to k[\epsilon]$ be a pseudodeformation in $\mathfrak{T}$, and E be a CH quotient of $k[\epsilon][G]$ having a GMA-structure $\begin{pmatrix} k[\epsilon] & B \\ C & k[\epsilon] \end{pmatrix}$. $\rho : G \to E$ is $\begin{pmatrix} \rho_1 & \rho_B \\ \rho_C & \rho_2 \end{pmatrix}$
First we construct the map f.

$$m : B \otimes_{k[\epsilon]} C \to k[\epsilon]$$

The image ideal of m is denoted as I, then I contained in (ϵ). I can only be either 0 or (ϵ), and is also independent of the choice of E.

m factors through $B/\epsilon B \otimes_k C/\epsilon C$.

We write $m = \phi\epsilon$ then

$$\phi \in \mathrm{Hom}_k(B/\epsilon B \otimes_k C/\epsilon C, k) \cong \mathrm{Hom}_k(B/\epsilon B, k) \otimes \mathrm{Hom}_k(C/\epsilon C, k) \hookrightarrow Ext^1_G(\bar{\chi}_2, \bar{\chi}_1) \otimes Ext^1_G(\bar{\chi}_1, \bar{\chi}_2)$$

The last map comes from Theorem 2.4.

f is defined sending (E, D) to ϕ and the kernel $f \iff I = 0$ corresponding to reducible pseudodeformations. $\mathrm{Ker}(f) \cong \mathfrak{T}_0$.

Next, we can show $h \circ f = 0$.

Unwinding the definitions, $h(f(\phi))(g, g')\epsilon = (m(\rho_B(g), \rho_C(g')), m(\rho_C(g), \rho_B(g')))$.

Because $\rho : G \to E^\times$ is a group homomorphism. Thus

$$m(\rho_B(g), \rho_C(g')) = \rho_1(gg') - \rho_1(g)\rho_1(g')$$

$\rho_1 = \bar{\chi}_1 + a\epsilon$, thus

$$m(\rho_B(g), \rho_C(g')) = a(gg') - \bar{\chi}_1(g)a(g') - \bar{\chi}_1(g')a(g)$$

Similarly, $\rho_2 = \bar{\chi}_2 + d\epsilon$, and $h \circ f = 0$.

Next we will show $\ker(h) = \mathrm{img}(f)$.

We have the following observation:

$k[\epsilon][G]/\ker(D)$ has a GMA-structure $S := \begin{pmatrix} k[\epsilon] & \mathrm{Ext}^1_G(\bar{\chi}_2, \bar{\chi}_1)^* \\ \mathrm{Ext}^1_G(\bar{\chi}_1, \bar{\chi}_2)^* & k[\epsilon] \end{pmatrix}$.

$(\cdot)^*$ means $\mathrm{Hom}_k(\cdot, k)$ and ϵ acts on $\mathrm{Ext}^1_G(\bar{\chi}_i, \bar{\chi}_j)^*$ as 0.

The reasoning: For any CH-representation (E_D, D) of G giving rise to D. (E_D, D) has kernel $\begin{pmatrix} 0 & \epsilon B_D \\ \epsilon C_D & 0 \end{pmatrix}$.

Specially, we pick $E_D := E^u \otimes_{R^u} k[\epsilon]$. And $E_D/\ker(D)$ has GMA-structure as $\begin{pmatrix} k[\epsilon] & B^u \otimes k \\ C^u \otimes k & k[\epsilon] \end{pmatrix}$, the above observation follows from Theorem 2.5 part 3.

For any $\phi \in \mathrm{Ext}^1_G(\bar{\chi}_2, \bar{\chi}_1) \otimes Ext^1_G(\bar{\chi}_1, \bar{\chi}_2)$, $m := \phi\epsilon$ gives a GMA-structure on S. a group homomorphism $\rho : G \to S$. Fix a k-vector space embedding $\mathrm{Ext}^1_G(\bar{\chi}_i, \bar{\chi}_j) \hookrightarrow Z^1_G(\bar{\chi}_i, \bar{\chi}_j)$ with $(i,j) \in \{(1,2),(2,1)\}$, we can define $\rho_B : G \to \mathrm{Ext}^1_G(\bar{\chi}_2, \bar{\chi}_1)$ as $\rho_B(g)(b) = b(g)$. Similarly we can define ρ_C :.

If ϕ is in the kernel of h, there are $(\delta(a), \delta(d)) \in B^2_G(\bar{\chi}_1, \bar{\chi}_1) \oplus B^2_G(\bar{\chi}_2, \bar{\chi}_2)$ such that $h(\phi) = (\delta(a), \delta(d))$. Thus

$$\delta(a)(g,g')\epsilon = m(\rho_B(g), \rho_C(g')) \quad \delta(d)(g,g')\epsilon = m(\rho_C(g), \rho_B(g'))$$

We define $\rho : G \to^{\times}$ as $\begin{pmatrix} \bar{\chi}_1 + a\epsilon & \rho_B \\ \rho_C & \bar{\chi}_2 + d\epsilon \end{pmatrix}$. We can check ρ is a group homomorphism and has residual pseudorepresentation $\bar{D}$.

There are multiple choices of (a,d). We will show these choices correspond to the kernel of f which is $\mathcal{T}_0$.

If (a',b') is another choice. Then $a - a' \in Z^1_G(\bar{\chi}_1, \bar{\chi}_1) = \mathrm{Ext}^1_G(\bar{\chi}_1, \bar{\chi}_1)$. □

2.5 pseudodeformations with conditions

The main reference for this section is [12].

Notations:

$\tilde{\mathbb{Q}}$ is the maximal field extension of $\mathbb{Q}$ unramified outside $S = \{N, p, \infty\}$, its Galois group over $\mathbb{Q}$ is denoted by $G_{\mathbb{Q},S}$.

$\chi : G_{\mathbb{Q},S} \to \mathbb{Z}_p^{\times}$ is the cyclotomic character.

$\bar{\rho} : G_{\mathbb{Q},S} \to GL_2(\mathbb{F}_p)$, $\bar{\rho} := \bar{\chi} \oplus I$. Its induced pseudo-representation is denoted as $\bar{D}$.

$\mathcal{C}$ is the category complete commutative noetherian local $\mathbb{Z}_p$ algebra $(A, \mathfrak{m}_A)$ with residue

field $A/\mathfrak{m}_A = \mathbb{F}_p$. I.e $\hat{\mathcal{C}}_{W(\mathbb{F}_p)}$ defined before.

The deformation functor $PsR^2_{\bar{D}}$ is represented by $(R_{\bar{D}}, \mathfrak{m}_{\bar{D}})$, all pseudodeformations of $G_{\mathbb{Q},S}$ lifting $\bar{D}$.

And $(E_{\bar{D}}, \rho^u : G_{\mathbb{Q},S} \to E^{\times}_{\bar{D}}, D^u_{E_{\bar{D}}} : E_{\bar{D}} \to R_{\bar{D}})$ is the initial object in category of CH algebra.

Because of being residually multiplicity free, there is a $GMA-$structure on $E_{\bar{D}}$.

2.5.1 finite-flat at p condition

$G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the local Galois group.

Let $\mathrm{Mod}^{\mathrm{fin}}_{\mathbb{Z}_p[G_p]}$ be the category of finite $\mathbb{Z}_p[G_p]$-module, an object V is *finite-flat* if there is a finite flat group scheme $\mathcal{G}$ over $\mathbb{Z}_p$ such that $V \cong \mathcal{G}(\bar{\mathbb{Q}}_p)$ as a $\mathbb{Z}_p[G_p]$-module.

$(A, \mathfrak{m}_A)$ is an object in $\mathcal{C}$, then a finite generated $A[G_p]$ module M is *finite-flat* if $M/\mathfrak{m}^i_A M$ is finite-flat as a finite module.

Definition 2.10. Let (E, ρ, D) be a CH representation of G_p over A, it is *finite-flat* if E is finite-flat as a $A[G_p]$-module.

For more details, check [12, section 5.2]

2.5.2 Steinberg at l condition

Definition 2.11. Let (E, ρ, D) be a CH representation of G_l over A, it is called ϵ-*Steinberg* if

$$V_\rho(\sigma, \tau) := (\rho(\sigma) - \lambda(-\epsilon)\chi(\sigma))(\rho(\tau) - \lambda(-\epsilon)) \in E$$

is 0 for every pair (σ, τ) in G_l.

Here $\chi : G_l \to \mathbb{Z}_p^{\times}$ is the cyclotomic character and λ is an unramified character sending Frobenius to $-\epsilon$.

Notice that the order matters. The reason to define this equation:

Assume E is a matrix algebra, $\rho : G_l \to Gl_2(A)$ with $A \in \mathcal{C}$, and $\bar{\rho} \cong \bar{\chi} \oplus Id$, then being Steinberg implies $\rho \cong \begin{pmatrix} \lambda(-\epsilon)\chi & * \\ 0 & \lambda(-\epsilon) \end{pmatrix}$.

To see above claim, consider the basis v_1, v_2 of V such that $\rho(\tau)v_1 \equiv \lambda(-\epsilon)\chi(\tau)v_1 \bmod \mathfrak{m}$ and $\rho(\tau)v_2 \equiv \lambda(-\epsilon)v_2 \bmod \mathfrak{m}$. Pick $\tau_0 \notin$ the inertial group, then $v_1' := (\rho(\tau_0) - \lambda(-\epsilon))v_1$ together with v_2 is a new basis of V. And $(\rho(\sigma) - \lambda(-\epsilon)\chi(\sigma))v_1' = 0$ for all σ because of $V_\rho(\sigma, \tau) = 0$.

Assume $\rho(\tau)v_2 = f(\tau)v_1' + g(\tau)v_2$, then $V_\rho(\sigma, \tau)(v_2) = 0$ implies $(g(\tau) - \lambda(-\epsilon))(g(\sigma) - \lambda(-\epsilon)\chi(\sigma)) = 0$ for all σ, τ. Because $g(\sigma) \equiv \lambda(-\epsilon) \bmod \mathfrak{m}$, $g(\tau) - \lambda(-\epsilon)$ for all τ.

Under this basis v_1', v_2, ρ is of the upper triangular shape.

Remark 2.6. Comparing with the definition *unramified or ϵ_l-Steinberg* [14, Definition 3.4.1].

We modify the condition to consider only *Steinberg* because we only consider Galois representations associated with newforms.

In the following discussion, we will only consider the case where $\epsilon = -1$. To save notation, we will just use *Steinberg* to refer this special case.

2.5.3 Global condition

We define a sub category, denoted as $\mathcal{CH}^{2,N}_{G_{\mathbb{Q},S},\bar{D}}$ of $\mathcal{CH}^{2}_{G_{\mathbb{Q},S},\bar{D}}$ having objects as $(E, \rho : G_{\mathbb{Q},S} \to E^\times, D : E \to R)$ such that it is finite flat viewed as a CH representation of G_p and is Steinberg viewed as a CH representation of G_l for every l dividing N, and arrows are the same.

we can define the functor $\mathrm{PsDef}^N_{G_{\mathbb{Q},S},\bar{D}}$ to be the sub-functor of $\mathrm{PsDef}_{G_{\mathbb{Q},S},\bar{D}}$ such that $\mathrm{PsDef}^N_{G_{\mathbb{Q},S},\bar{D}}(\mathrm{A})$ is the set of all pseudorepresentation $D : A[G_{\mathbb{Q},S}] \to A$ lifting $\bar{D}$ and it has a CH representation being an object of above subcategory $\mathcal{CH}^{2,N}_{G_{\mathbb{Q},S},\bar{D}}$.

Similarly, we can define functor $\mathrm{PsDef}^{\mathrm{flat}}_{G_{\mathbb{Q},S},\bar{D}}$ sending A to the set of all finite-flat at p pseudorepresentations.

The finite-flat condition at p on CH algebras is "stable" condition discussed in [12], and the Steinberg condition is a condition that certain elements vanish. From the discussion from [14, section 3.1.5, section 3.1.6], we have the functor $\mathrm{PsDef}^{N}_{G_{\mathbb{Q},S},\bar{D}}$ is represented by R_N, respectively $\mathrm{PsDef}^{\mathrm{flat}}_{G_{\mathbb{Q},S},\bar{D}}$ by R_{flat}. Furthermore there is a universal CH representation $(E_{\bar{D},N}, \rho^u : G_{\mathbb{Q},S} \to E_{\bar{D},N}, D^u_N : E_{\bar{D},N} \to R_N)$.

The previous description still holds for reducible locus of the pseudodeformation ring satisfying "stable" conditions. Theorem 2.5 holds for universal pseudodeformation ring satisfying "stable" conditions. Below is the precise statement.

Theorem 2.7. *There is an isomorphism $R^{red}_{*,\bar{D}} \to R_{*,\bar{\chi}_1}\hat{\otimes}R_{*,\bar{\chi}_2}$.*
Here $*$ can a stable condition, and $\bar{D} = det(\bar{\chi}_1 \oplus \bar{\chi}_2)$.
Furthermore, $A \in \mathcal{C}$ and M is a finitely generated $A-$module, and $\chi_{i,A} : G \to A^\times$ is a character lifting $\bar{\chi}_i$ satisfying the stable condition $*$. There is a natural isomorphism

$$Hom_A(B^{red}_* \otimes_{R^{red}_*} A, M) \xrightarrow{\sim} Ext^1_{G,*}(\chi_{2,A}, \chi_{1,A} \otimes M)$$

Similar isomorphism is true for C^{red}_*.

Proof. Check [12, Proposition 4.3.4, Theorem 4.3.5] □

Example 2.9. Let $\bar{D} = \det(\bar{\chi} \oplus Id)$ with $\chi : G_{\mathbb{Q},S} \to \mathbb{Z}_p^\times$ cyclotomic character.
Then $R_{\mathrm{flat},Id} \cong \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})^{p-\mathrm{part}}]$.
As we have seen the degree 1 pseudorepresentation is the same as the usual character. And being finite-flat at p implies the character is unramified at p.
$R_{\mathrm{flat},Id} \cong R_{\mathrm{flat},\bar{\chi}} \cong \mathbb{Z}_p[\prod_{r|N} \mathbb{Z}_p/(r-1)\mathbb{Z}_p]$.
The universal character lifting id, denoted by $< - >: G_{\mathbb{Q},S} \to R_{\mathrm{flat},Id} \cong \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})^{p-\mathrm{part}}]$, is given by the natural quotient. And the universal character lifting $\bar{\chi}$ is $\chi < - >$.

$R^{\text{red}}_{\text{flat}} \cong R_{\text{flat},\bar{\chi}} \hat{\otimes} R_{\text{flat},Id}$ is the universal reducible finite-flat pseudodeformation ring. Let $\chi_1^u : G_{\mathbb{Q},S} \to R^{\text{red}}_{\text{flat}}$ be $\chi < - > \otimes Id$, and $\chi_2^u := Id \otimes < - >$, then the universal reducible finite-flat pseudodeformation is $\det(\chi_1^u \oplus \chi_2^u)$.

Lemma 2.3. Let (E, D) be a pseudorepresentation of $G_{\mathbb{Q},S}$ lifting $\bar{D} = \det(\bar{\chi} \oplus Id)$ over A and is finite-flat at p and *Steinberg* for $l|N$, then $D(\tau) = \chi(\tau)$ for $\tau \in G_{\mathbb{Q},S}$.

Proof. D restricted to $G_{\mathbb{Q},S}$ is a character, it is the determinant map. It suffices to show $D\chi^{-1} : G_{\mathbb{Q},S} \to A$ is unramified at every place.

At place p, check [14, Corollary 3.7.6].

For place $r|N$, it follows from [14, Lemma 3.4.4]. Here we replicate the proof because the proof uses many basic properties of pseudorepresentations.

It suffices to show $D(\gamma) = 1$ for any $\gamma \in I_r$. From Steinberg condition at r, we have

$$V(\gamma, \gamma) = (\rho(\gamma) - 1)^2 = 0$$

Thus $D(\rho(\gamma) - 1) = 0$. $D(g) = \frac{Tr(g)^2 - Tr(g^2)}{2}$ implies $Tr(\rho(\gamma) - 1) = 0$, thus $Tr(\gamma) = Tr(1) = 2$.

$D(\gamma - 1) = D(\gamma) + 1 + Tr(\gamma) * Tr(-1) - Tr(-\gamma) = 0$, thus $D(\gamma) = 1$.

□

Remark 2.7. Above lemma corresponds to the claim that the p-adic Galois representations associated to weight 2 level $\Gamma_0(N)$ newforms have determinant χ.

Lemma 2.4. Assume the universal reducible finite-flat pseudodeformation is $\det(\chi_1^u \oplus \chi_2^u)$ with $\chi_i^u : G_{\mathbb{Q},S} \to R^{\text{red}}_{\text{flat}}$. Then there is an ideal I in $R^{\text{red}}_{\text{flat}}$ such that every finite-flat reducible $D : R[G_{\mathbb{Q},S}] \to R$, D is Steinberg if and only if $R^{\text{red}}_{\text{flat}} \to R$ factors through I.

Ideal I is generated by $(\chi_1^u(\tau) - \chi(\tau))(\chi_1^u(\sigma) - Id), (\chi_2^u(\tau) - \chi(\tau))(\chi_2^u(\sigma) - Id)$ for τ, σ in G_r with $r|N$.

Proof. $(E^u, \rho^u, R^{\text{red}}_{\text{flat}})$ is the universal GMA structure. D is a finite-flat reducible pseudorepresentation, it induces $\phi : R^{\text{red}}_{\text{flat}} \to R$.

If D is Steinberg, there is a CH representation $D : E \to R$ and $\rho : E^u = \begin{pmatrix} \chi_1^u & * \\ * & \chi_2^u \end{pmatrix} \to E$ satisfying $\rho(V_{\rho^u}(\tau, \sigma)) = 0$ for any $\tau, \sigma \in G_r$ with $r|N$.

In particularly, the trace of $\rho(V_{\rho^u}(\tau, \sigma) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix})$ is $\phi((\chi_1^u(\tau) - \chi(\tau))(\chi_1^u(\sigma) - Id))$ is 0 in R, similarly $\phi((\chi_2^u(\tau) - \chi(\tau))(\chi_2^u(\sigma) - Id)) = 0$. Thus ϕ factors through I.

For the other direction, given a map $\phi : R^{\text{red}}_{\text{flat}} \to R^{\text{red}}_{\text{flat}}/I \to R$, we can construct $(\phi \circ \chi_1 \oplus \phi \circ \chi_2)$ that is a Steinberg CH representation inducing D. □

Example 2.10. Compute R^{red}_N :

From lemma2.3, the ideal generated by $\{D(\tau) - \chi(\tau)\}$ is contained in the ideal from 2.4. To compute R^{red}_N, we first quotient the former ideal. Here $D(\tau) = \chi(\tau) < \tau > \otimes < \tau >$.

$$R_{\text{flat},Id} \hookrightarrow \frac{R_{\text{flat},\bar{\chi}} \otimes R_{\text{flat},Id}}{\text{ideal generated by} \{< \tau > \otimes < \tau > -1\}}$$

The above map is given as $x \to 1 \otimes x$. It turns out to be an isomorphism.

The universal pseudodeformation is given by $\det(\chi < - >^{-1} \oplus < - >)$.

From lemma2.4, $R^{\text{red}}_N \cong R_{\text{flat},Id}/I$ with I being generated by $(< \tau > -\chi(\tau))(< \sigma > -1)$ for every σ, τ in G_r with $r|N$.

Notations: for a prime r with $r|N$, fix a decomposition group $G_r \subset G_{\mathbb{Q},S}$, I_r is the inertia subgroup. The maximal pro-p quotient of I_r is denoted by $I_r^{\text{pro}-p}$, which is isomorphic to $\mathbb{Z}_p$. Pick $\gamma_r \in G_r$ which is a topological generator of $I_r^{\text{pro}-p}$ and $\sigma_r \in G_r$ which lifts the Frobenius element.

Lemma 2.5. $N = r_1 r_2 l$ with $l \equiv 1 \bmod p$ and $r_1, r_2 \not\equiv 1 \bmod p$, furthermore assume r_1 is not a p-th power mod l, then $R^{\text{red}}_N \cong \mathbb{Z}_p$.

Proof. $R_{\text{flat},Id} \cong \mathbb{Z}_p[\mathbb{Z}_p/(l-1)\mathbb{Z}_p] \cong \mathbb{Z}_p[y_l]/(y_l^{p^{v_l}}-1)$, use y_l to denote the image of γ_l under $\langle\ \rangle$ and $v_l = \text{order}_p(l-1)$.

$< \gamma_{r_i} >= 1$ and assume $\langle \sigma_{r_i} \rangle = y_l^{\alpha_i}$, I is generated by $(y_l-1)^2, (y_l-1)(l-1), (y_l^{\alpha_i}-r_i)(y_l^{\alpha_i}-1)$ with $i = 1, 2$.

Let $Y_l := y_l - 1$, then R_N^{red} is the ring

$$\mathbb{Z}_p[Y_l]/(Y_l^2, (l-1)Y_l, (1-r_1)\alpha_1 Y_l, (1-r_2)\alpha_2 Y_l)$$

When one of α_i satisfying $(\alpha_i, p) = 1$, then the above ring is $\mathbb{Z}_p$. Thus $R_N^{red} \cong \mathbb{Z}_p$. The condition $(\alpha_i, p) = 1$ is equivalent to the inert degree f_i of r_i inside the field extension $\mathbb{Q}(\xi_l)/\mathbb{Q}$ has the same p-order as $l-1$. It is equivalent to r_1 is not a p-th power mod l. $\square$

CHAPTER 3

HECKE ALGEBRA

3.1 congruence module

The main reference for congruence module is [8].

K is a finite field extension of $\mathbb{Q}_p$. M is K-subspace of $M^2(\Gamma_0(N), K)$ (space of weight 2, level $\Gamma_0(N)$ modular forms) stable under all Hecke action T_n for all n. Use $M(\mathcal{O}_K)$ to denote the intersection of $M^2(\Gamma_0(N), K)$ and $M(K)$. Assume $M = X \oplus Y$ with X, Y $K-$sub space stable under all T_n, and

$$\text{rank}(X \cap M(\mathcal{O}_K)) + \text{rank}(Y \cap M(\mathcal{O}_K)) = \text{rank}(M(\mathcal{O}_K))$$

Similarly, we can define $X(\mathcal{O}_K)$ and $Y(\mathcal{O}_K)$.

Congruence module $C_{X,Y}$ is defined to capture the congruences of modular forms between X and Y. Below is the detailed definition.

$$C_{X,Y} := \frac{M(\mathcal{O}_K)}{X(\mathcal{O}_K) \oplus Y(\mathcal{O}_K)}$$

is called *congruence module*.

From the definition, $C_{X,Y} \neq 0$ if and only if there exists a nontrivial element annihilated by π if and only if there exists $f \in X(\mathcal{O}_K)$ and $g \in Y(\mathcal{O}_K)$ such that

$$f \equiv g \bmod \pi \quad \text{and} f \not\equiv 0 \bmod \pi$$

$M_X := \text{Proj}_X(M(\mathcal{O}_K))$ is the projection of $M(\mathcal{O}_K)$ to X. M_Y is similarly defined.

Then $M(\mathcal{O}_K) \hookrightarrow M_X \oplus M_Y$. There is a similar $\mathcal{O}_K-$module $C'_{X,Y}$

$$C'_{X,Y} := M_X \oplus M_Y \Big/ M(\mathcal{O}_K)$$

Lemma 3.1. $C'_{X,Y} \neq 0$ if and only if $C_{X,Y} \neq 0$

Proof. The proof comes from unwinding the definition.

$C'_{X,Y} \neq 0$ if and only if there is a nontrivial element annihilated by π, which is equivalent to that there exists $u, v, w \in M(\mathcal{O}_K)$ such that $(w_X, w_Y) = \pi(u_X, v_Y)$ and $\frac{w}{\pi} = u_X + v_Y \notin M(\mathcal{O}_K)$.

Assume $C'_{X,Y} \neq 0$, then consider $w - \pi u, w - \pi v \in M(\mathcal{O}_K)$. $(w - pu)_X = 0$ implies $w - pu \in Y(\mathcal{O}_K)$, similarly $w - pv \in X(\mathcal{O}_K)$. Furthermore, $w - pu \equiv w - pv$and $w \not\equiv 0 \bmod \pi$. Thus one direction is clear.

For the other direction, we assume $f - g = \pi h$ with $h \in M(\mathcal{O}_K)$, $f \in X(\mathcal{O}_K)$ and $g \in Y(\mathcal{O}_K)$. $(h_X = \frac{f}{\pi} - \frac{g}{\pi})_X = \frac{f}{\pi} \in M_X$, thus $(h_X, 0) \in C'_{X,Y}$ is an element in $C'_{X,Y}$ annihilated by π. It is non-trivial because $f \not\equiv 0 \bmod \pi$. □

We can also describe congruence module using Hecke operators, which follows from the perfect pairing between modular forms and Hecke algebra.

Notations:

T is the $\mathcal{O}_K$ algebra generated by all T_n inside End(M).

T_X is the $\mathcal{O}_K$ algebra generated by all T_n inside End(X). T_Y is defined similarly. Then

$$T \twoheadrightarrow T_X \quad T \twoheadrightarrow T_Y \quad T \hookrightarrow T_X \oplus T_Y$$

Consider the finite $T-$module $T_X \oplus T_Y \,/_T$, the following theorem claims

Theorem 3.1.

$$\frac{M(\mathcal{O}_K)}{X(\mathcal{O}_K) \oplus Y(\mathcal{O}_K)} \times \frac{T_X \oplus T_Y}{T} \to K \Big/ \mathcal{O}_K$$

induces an $\mathcal{O}_K-$ module isomorphism

$$C_{X,Y} \to Hom_{\mathcal{O}_K}(T_X \oplus T_Y \,/_T, K \Big/ \mathcal{O}_K)$$

$M(\mathcal{O}_K) \hookrightarrow M = X \oplus Y$, the pairing from the theorem is induced from the classical pairing in the following lemmas.

We introduce two classical results before stating the proof of the theorem.

Lemma 3.2. The pairing of $K-$module

$$M \times T(K) \longrightarrow K$$
$$(f, T) \longrightarrow a_1(Tf)$$

is perfect.

Lemma 3.3. The pairing of $\mathcal{O}_K-$module

$$M(\mathcal{O}_K) \times T \longrightarrow \mathcal{O}_K$$
$$(f, T) \longrightarrow a_1(Tf)$$

is perfect.

The key point of the proofs is $a_1(T_n f) = a_n(f)$ for all n.

Proof. proof of the theorem:
notation: $\hat{T} := \mathrm{Hom}_{\mathcal{O}_K}(T, \mathcal{O}_K)$, $\tilde{T} := T_X \oplus T_Y$ and $T(K) := T \otimes_{\mathcal{O}_K} K$
There is a commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X(\mathcal{O}_K) \oplus Y(\mathcal{O}_K) & \longrightarrow & M(\mathcal{O}_K) & \longrightarrow & C_{X,Y} & \longrightarrow & 0 \\
 & & \downarrow \sim & & \downarrow \sim & & \downarrow \phi_{X,Y} & & \\
0 & \longrightarrow & \widehat{T_X} \oplus \widehat{T_Y} & \xrightarrow{\alpha} & \widehat{T} & \xrightarrow{\beta} & \mathrm{Hom}_{\mathcal{O}_K}(\tilde{T}/T, K/\mathcal{O}_K) & \longrightarrow & 0
\end{array}$$

The first two vertical maps are induced from the perfect pairings in above propositions.

β is defined as following: $T(K) \cong T_X(K) \oplus T_Y(K) \cong \tilde{T}(K)$, then

$$\mathrm{Hom}_{\mathcal{O}_K}(T, \mathcal{O}_K) \hookrightarrow \mathrm{Hom}_K(T(K), K) \cong \mathrm{Hom}_K(\tilde{T}(K), K) \cong \mathrm{Hom}_{\mathcal{O}_K}(\tilde{T}, K)$$

The definition for β follows and it is surjective and $\ker(\beta) = \mathrm{img}(\alpha)$.
The maps in the second square commute, thus the theorem is proved. □

There are several equivalent statements that ${}^{T_X \oplus T_Y}/_{T}$ (to save notation, denoted as ${}^{\tilde{T}}/_{T}$) is nontrivial.

- We denote the kernel of $T \twoheadrightarrow T_X$ as I_X. Similarly, I_Y is defined. Then as a T- module

$$ {}^{\tilde{T}}/_{T} \cong {}^{T_X}\Big/ ({}^{I_X + I_Y}\Big/_{I_X}) \cong {}^{T}\Big/_{I_X + I_Y}$$

  thus ${}^{\tilde{T}}/_{T}$ is nontrivial if ans only if there is a maximal ideal $\mathfrak{m}$ of T such that $I_X + I_Y \subset \mathfrak{m}$.
  Furthermore, assume $\mathfrak{m} \subset T$ is a maximal ideal, then $({}^{\tilde{T}}/_{T})_{\mathfrak{m}} = 0$ if and only if $I_X + I_Y \subset \mathfrak{m}$. Furthermore, if $I_X + I_Y \subset \mathfrak{m}$, then ${}^{\tilde{T}}/_{T} \twoheadrightarrow ({}^{\tilde{T}}/_{T})_{\mathfrak{m}}$.
  To see above claim, $I_X + I_Y \not\subset \mathfrak{m}$ implies $({}^{T}\Big/_{I_X + I_Y})_{\mathfrak{m}} = 0$. For the other direction, if $I_X + I_Y \subset \mathfrak{m}$, thus $\mathfrak{m}$ can be viewed as a maximal ideal of ${}^{T}\Big/_{I_X + I_Y}$. $({}^{T}\Big/_{I_X + I_Y})_{\mathfrak{m}}$ is a local ring whose quotient is ${}^{T}/_{\mathfrak{m}}$. Thus $({}^{T}\Big/_{I_X + I_Y})_{\mathfrak{m}} \neq 0$. Furthermore ${}^{T}\Big/_{I_X + I_Y} \to ({}^{T}\Big/_{I_X + I_Y})_{\mathfrak{m}}$ is surjective. This is true for general finite ring R and its maximal ideal $\mathfrak{m}$, because for any $s \notin \mathfrak{m}$, there is some $\alpha \in R$ and $m \in \mathfrak{m}$ such that $\alpha s + m = 1$, thus αs is a unit (because of R being finite), thus for any $\frac{a}{s} \in R_{\mathfrak{m}}$ there is $b := \alpha a(\alpha s)^{-1} \in R$ such that $\frac{b}{1} = \frac{a}{s}$. In our case $R = {}^{T}\Big/_{I_X + I_Y}$.
  Naturally, ${}^{\tilde{T}}/_{T} \neq 0$ if and only if there is a nontrivial T-module V such that V can be viewed both as T_X and T_Y module. I.e the annihilator of V, $\mathrm{Ann}_T(V)$, is a nontrivial ideal containing $I_X + I_Y$.

- Consider the special element $e : M \overset{\mathrm{Proj}_X}{\to} X \hookrightarrow M$ in $\mathrm{End}_K(M)$, we have $e|_X = \mathrm{id}$ and $e|_Y = 0$. Thus $e \in T_X \oplus T_Y = \tilde{T}$. $\tilde{T}/T$ nontrivial if and only if $e \notin T$. The claim follows from $T_X = T \cdot e$ as a T-module and $T_Y = T \cdot (1 - e)$.

- From the perfect pairing, we have seen $T(K)$ is a finite commutative $K-$algebra. From the structure theorem,

$$T(K) \cong \prod_{\mathfrak{m}} T(K)/\mathfrak{m}^n \qquad \text{the product is over all maximal ideals of } T(K)$$

Furthermore we assume $T(K)$ is reduced, then $T(K) \cong \prod_i K_i$ with K_i be a finite field over K.

Example 3.1. 1. If $M = S_2(\Gamma_0(N), K)^{\mathrm{new}}$, the full Hecke algebra is reduced. This claim follows from the strong multiplicity one result.
In this case, $M \otimes \bar{K} \cong \prod_{\mathrm{newform}} \bar{K}$.

2. The Hecke algebra T^{red} generated by T_n with $(n, N) = 1$ on $M = S_2(\Gamma_0(N), K)$ is reduced. And $T^{\mathrm{red}} \otimes \bar{K} \cong \prod_{\mathrm{newform}} \bar{K}$.
3. The full Hecke algebra acting on $S_2(\Gamma_0(N), K)$ is not necessarily reduced, because of the existence of cuspforms of level M which is non-ordinary at prime q with $Mq = N$.
But if we consider the Hecke algebra T_w generated by $T_n, (n, N) = 1$ and $w_r, r|N$, then T_w is reduced. For details, check [14, Lemma 2.3.1].

The maximal ideals of $T(K)$ are in bijection with the minimal prime ideals of T.
Because T is finite flat over O_K and $T(K)$ is flat over T, the going-down property

holds.

Extend to $\bar{K}$ (or a large enough field L), a maximal ideal of $T(\bar{K})$ corresponds to an algebra homomorphism $T(\bar{K}) \to \bar{K}$, equivalent to a normalized eigenform of T.

If we assume T is reduced and $T \otimes \bar{K} \cong \prod_f \bar{K}$ with $f's$ normalized eigenvectors of T.

Lemma 3.4. ${}^{\tilde{T}}/_{T}$ is nontrivial if and only if there is an eigenform f in $X \otimes L$ and an eigenform g in $Y \otimes L$ such that $f \equiv g \bmod \pi'$, here L is a large field.

Proof. It suffices to prove the lemma in the case when T is over $\mathcal{O}_L$ for a large finite extension over K.

${}^{\tilde{T}}/_{T}$ is nontrivial if and only if there is a maximal ideal $\mathfrak{m}$ containing $I_X + I_Y$ whose residue field is p.

$\mathcal{O}_L \to T_X$ is a finite flat extension, $\mathfrak{m}$ pulls back to (π), thus there is a prime ideal $\mathfrak{p}_f$ pulling back to (0). $\mathfrak{p}_f$ is a minimal prime ideal of T. Similarly, there is a minimal prime ideal $\mathfrak{p}_g$ of T containing I_Y. And $\mathfrak{p}_f$ and $\mathfrak{p}_g$ corresponds to maximal ideals of $T(L)$, thus eigenforms. Also they are congruent to each other. □

We use $C^*_{X,Y}$ to denote $\mathrm{Hom}_{\mathcal{O}_K}(C_{X,Y}, {}^{K}\big/_{\mathcal{O}_K}) \cong {}^{T_X \oplus T_Y}/_{T}$, then T has the following structure.

Lemma 3.5.

$$T \cong T_X \times_{C^*_{X,Y}} T_Y$$

Proof. The proof is totally algebraic.

First the map $T_X \to C^*_{X,Y}$ is defined as follows:

$$T_X \to {}^{T_X}\Big/_{I_X + I_Y}\Big/_{I_X} \xrightarrow{\sim} {}^{T_X \oplus T_Y}/_{T} \cong C^*_{X,Y}$$

Consider the map $\alpha : T \to T_X \times T_Y$ sending $t \in T$ to $(t_X, -t_Y)$, here t_X is the image of t under the usual quotient $T \to T_X$. In ${}^{T_X \oplus T_Y}/_{T}$, $t_X \to (t_X, 0) \bmod T$ while $-t_Y \to$

$(0, -t_Y) \bmod T$. The difference is 0 in $C^*_{X,Y}$. Thus α has image in $T_X \times_{C^*_{X,Y}} T_Y$.

Last, we show α is surjective to $T_X \times_{C^*_{X,Y}} T_Y$. For any $(f_X, g_Y) \in T_X \times_{C^*_{X,Y}} T_Y$, we have $(f_X, -g_Y) = 0$ in ${}^{T_X \oplus T_Y}\big/_{T}$. So α induces an isomorphism $T \cong T_X \times_{C^*_{X,Y}} T_Y$. □

Lemma 3.6.

$$C^*_{X,Y} \cong {}^{T_Y}\Big/_{\mathrm{Ann}_T(I_Y)}$$

Here, we quotient the image of $\mathrm{Ann}_T(I_Y)$ in T_Y.

Proof. We have the claim $\mathrm{Ann}_T(I_Y) = \ker(T \to T_X) = I_X$, and the lemma follows.

To see the claim, we use the structure lemma above.

$T \cong T_X \times_C T_Y \to T_Y$, thus $I_Y \subset T$ is identified as ${}^{I_Y + I_X}\big/_{I_X} \times 0$. Since ${}^{T}\big/_{I_X + I_Y}$ is finite, thus ${}^{I_Y + I_X}\big/_{I_X}$ is a faithful T_X-module. Thus $\mathrm{Ann}_T(I_Y) = 0 \times {}^{I_Y + I_X}\big/_{I_Y}$, is exactly $\ker(T \to T_X) = I_X$. □

Remark 3.1. Assume $\mathfrak{m} \subset T$ is a maximal ideal containing $I_X + I_Y$, then above two lemmas work for the localized Hecke algebra. Because $T_{\mathfrak{m}}$ is flat over T, pull-back and quotient commute with localization.

3.2 special case

Let $N = r_1 \cdots r_d$ be an square free integer, then the dimension of Eisenstein subspace of $M_2(\Gamma_0(N))$ is $2^d - 1$.

Let E_2 be the power series

$$E_2 = -\frac{B_2}{4} + \sum_{n \geq 1} \sigma(n) q^n$$

Here $B_2 = \frac{1}{6}$ and $\sigma(n) = \sum_{d|n} d$.

Lemma 3.7. There is a unique normalized Eisenstein series E in $M_2(\Gamma_0(N))$ such that it is an eigenform with U_r acts as 1 for all $r|N$.

Proof. $E_2^{(1)} := E_2(\tau) - r_1 E_2(r_1\tau)$ then $E_2^{(1)}$ is of level $\Gamma_0(r_1)$ with U_{r_1} acting as 1.
$E_2^{(2)} := E_2^{(1)}(\tau) - r_2 E_2^{(1)}(r_2\tau)$ then $E_2^{(2)}$ is of level $\Gamma_0(r_1 r_2)$ with U_{r_1} and U_{r_2}acting as 1.
We keep lifting the level, then $E = \prod_i (Id - r_i V_{r_i}) E_2$ is the desired Eisenstein series. Here V_{r_i} is the operator sending modular form $f(\tau)$ to $f(r_i\tau)$.
$a_1(E) = 1$, thus E is normalized. □

The space $M := \mathbb{Q}_p E \oplus S_2(\Gamma_0(N), \mathbb{Q}_p)^{new}$. $S := S_2(\Gamma_0(N), \mathbb{Q}_p)^{new}$.
$\widetilde{T}$ (resp. $\widetilde{T}^\circ$) is the $\mathbb{Z}_p$ Hecke algebra on M (resp. S).
The Eisenstein ideal $I = (T_s - s - 1 : s \nmid N, U_r - 1 : r|N)$ inside $\widetilde{T}$ is also the kernel of the map $\widetilde{T} \twoheadrightarrow \mathbb{Z}_p$ sending T_n to $a_1(T_n(E))$.
$\mathfrak{m} := (I, p) \subset \widetilde{T}$ is a maximal ideal. And T denotes the localization of $\widetilde{T}$ at $\mathfrak{m}$.
Similarly, $T^\circ := \widetilde{T}^\circ_{\mathfrak{m}}$.

The upper $\circ$ means the cuspidal part, and upper $\sim$ means the algebra before localization. To save notation, we always use I to denote the ideal generated by T_s and U_r inside a given ring.

From previous section, the congruence module between S and $\mathbb{Q}_p E$ is denoted as

$$C := \frac{M(\mathbb{Z}_p)}{S(\mathbb{Z}_p) \oplus \mathbb{Z}_p E}$$

3.2.1 the size of C

$a_0 : M \to \mathbb{Q}_p$ is the map sending a modular form to the constant term of its q-expansion.
Then $C = \frac{M(\mathbb{Z}_p)}{S(\mathbb{Z}_p) \oplus \mathbb{Z}_p E} = \frac{a_0(M(\mathbb{Z}_p))}{a_0(E)\mathbb{Z}_p}$ is a subgroup of $\frac{\mathbb{Z}_p}{a_0(E)\mathbb{Z}_p}$.
From lemma 3.5 above, $a_0(E) = -\frac{1}{24}\prod_{r|N}(1-r)$.
Thus the size of C is $\leq |\frac{\mathbb{Z}_p}{\prod_{r|N}(r-1)\mathbb{Z}_p}|$.

Next, we want give a lower bound of the size of C, before that we introduce some

background knowledge on Shimura curve

Because of the perfect pairing in Theorem 3.1,

$$\frac{\widetilde{T}^\circ}{I} = \frac{\widetilde{T}^\circ \oplus \mathbb{Z}_p}{\widetilde{T}} \cong C^*$$

with C^* the Pontryagin dual of C.

And we have $C^*_{\mathfrak{m}} \cong {}^{T^\circ}/_{I}$.

3.3 Shimura curve

Assume $N = Dl$ with $l \equiv 1 \bmod p$ and D being $r_1 \cdots r_d$, a product of even number of primes.

Consider $X_0^D(l)/\mathbb{Q}$, the Shimura curve attached to the unique quaternion algebra over $\mathbb{Q}$ with discriminant D. $\mathcal{O}_D$ is a fixed maximal order.

Define a moduli problem over $\mathbb{Z}$ which associates to any scheme S over $\mathbb{Z}$ the set of isomorphism classes of structure (A, ι, Q_l), where ${A}/_{S}$ is an abelian surface over S, $\iota : \mathcal{O}_D \to \mathrm{End}_S(A)$, $Q_l \subset A[l]$ is a rank l^2 subgroup scheme which is, fppf locally on S, cyclic as an $\mathcal{O}_D$-module.

There is a canonical model $X_0^D(l)_{\mathbb{Z}_l}$ and its special fiber ${X_0^D(l)}/_{\mathbb{F}_l}$ has two irreducible components, each isomorphic to the smooth curve ${X_0^D(1)}/_{\mathbb{F}_l}$. And the two components intersect transitively at supersingular points on $X_0^D(1)_{\mathbb{F}_l}$, and the collection of these supersingular points are denoted by $\mathcal{S}$. For details, check [4, Theorem 4.7] or [7] theorem 4 and theorem 12.

There are natural Hecke correspondence on $X_0^D(l)_{\mathbb{Z}_l}$ and $J := Pic^0(X^D(l)_{\mathbb{Q}})$ given in terms of the moduli interpretation:

$$\text{for } s \not| D, T_s(A, Q_l) = \sum_{Q_s} (A/Q_s, Q_l/Q_s)$$

here Q_s is an order s^2, $\mathcal{O}$ stable subgroup of $A[s]$ which intersects with Q_l trivially.
And for $s = l$, use U_l to denote T_l:

$$U_l(A, Q_l) = (A/Q_l, Q_l')$$

There is the Weil pairing on $A[l]$, and $\widetilde{Q_l'}$ is a $\mathcal{O}$ stable subgroup of order l^2 such that its pairing with Q_l has full image μ_l, Q_l' is the reduction of $\widetilde{Q_l'}$ mod Q_l. For $r|D$, U_r is defined as w_r:

$$w_r(A, Q_l) = (A/A[I_r], Q_l/A[I_r])$$

here I_r is the unique prime ideal of norm r in $\mathcal{O}_D$.
Let $T^D(l)^{\text{new}}$ be the algebra generated by $\{T_s : s \nmid Dl, U_r : r|Dl\}$ acting on the new part of the Jacobian J of the Shimura curve $X^D(\Gamma_0(l))$.
$\mathcal{S}$ is the collection of these supersingular points in $X^D(\Gamma_0(1))$. Let X be the $\mathbb{Z}$ module formally generated by elements in $\mathcal{S}$, and X° be the degree 0 part. And X° is isomorphic to the character group of the torus part of $J/\mathbb{F}_l$. There are naturally Hecke actions on X induced from the moduli description.
There is a pairing given by

$$X \times X \xrightarrow{<\ ,\ >} \mathbb{Z} \quad < A_i, A_j >= \frac{\#\text{Aut}(A_i)}{2}$$

Here A_i is one isomorphism class of supersingular points in $\mathcal{S}$.
Above pairing induces a map $\iota : X^\circ \to (X^\circ)^*$. Let $\Phi_l(J_0^D(l))$ be the component group of $J_0^D(l)_{/\mathbb{F}_l}$, then

Theorem 3.2. *X is a $T^D(l)^{new}$-module.*
$\Phi_l(J_0^D(l)) \cong (X^\circ)^* \Big/ \iota(X^\circ)$, *thus also a $T^D(l)^{new}$-module. And $T_s - (s+1)$ annihilates $\Phi_l(J_0^D(l))$ for $s \nmid Dl$.*

Proof. Check section 4 of [10]. □

The lemma below is well-known, cf. [11, Proposition 3.8].

Lemma 3.8. The action of U_l on the character group X° is induced by the Frobenius automorphism on the set supersingular points $\mathcal{S}$.

Lemma 3.9. [17, proposition A.2, A.3]
There is cyclic subgroup $\Phi \subset \Phi_l(J_0^D(l)) \otimes \mathbb{Z}_p$ and the ideal $I^\circ = (T_s - s - 1, U_r - 1)$ with $r|N$ annihilates Φ. The order of Φ is $\#(\frac{\mathbb{Z}_p}{\prod_{r|N}(r-1)\mathbb{Z}_p})$.

Proof. For the proof details, check Yoo's paper[17]. □

The lemma above implies $\#(\frac{\widetilde{T}^\circ}{I^\circ}) \geq \#(\mathbb{Z}_p/\prod_{r|N}(r-1)\mathbb{Z}_p)$.
Thus $\#C = \#(\mathbb{Z}_p/\prod_{r|N}(r-1)\mathbb{Z}_p)$.

Lemma 3.10. Assume $l \equiv 1$ mod p, and $r_1, r_2 \not\equiv 1$ mod p, then

$$\#C = \#(\mathbb{Z}_p/(l-1)\mathbb{Z}_p)$$

CHAPTER 4

FLAT GALOIS COHOMOLOGY

4.1 local flat cohomology

Notation: $H^1_{p,flat}(V) := \mathrm{Ext}^1_{G_p,flat}(\mathbb{Z}/p^n\mathbb{Z}, V)$ with V a $\mathbb{Z}/p^n\mathbb{Z}[G_p]-$module.
$\mathbb{Q}_p^{\mathrm{ur}}$ denotes the maximal unramified extension of $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$

Lemma 4.1. [13, Lemma 6.2.1] For any $n > 0$,

1. $H^1_{p,flat}(\mathbb{Z}/p^n\mathbb{Z}) = \ker(H^1_p(\mathbb{Z}/p^n\mathbb{Z}) \to H^1(\mathbb{Q}_p^{ur}, \mathbb{Z}/p^n\mathbb{Z})$
2. $H^1_{p,flat}(\mathbb{Z}/p^n\mathbb{Z}(-1)) = 0$
3. Under the identification $H^1_p(\mathbb{Z}/p^n\mathbb{Z}(1)) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{p^n}$, $H^1_{p,flat}$ corresponds to the subgroup $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^{p^n}$.

4.2 global flat cohomology

For details, check the finite flat cohomology computations in [13, Section 6.3].
$H^1_{flat}(G_{\mathbb{Q},S}, V) := \ker(H^1(G_{\mathbb{Q},S}, V) \to H^1_p(V)/H^1_{p,flat}(V))$ with V a $G_{\mathbb{Q},S}-$module.

Lemma 4.2. For $n > 0$,

1. $$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z} \otimes \mathbb{Z}/p^n\mathbb{Z}, \quad H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}_p) = 0$$
2. $$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(1)) \cong (\mathbb{Z}[1/N])^\times \otimes \mathbb{Z}/p^n\mathbb{Z}$$
3. $$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(-1)) \cong \prod_{l|N} \mathbb{Z}_p \Big/ (p^n, l^2 - 1)\mathbb{Z}_p$$

Proof. 1. $H^1(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}) = \mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}) = \mathrm{Hom}(\prod_{l|Np} \mathbb{Z}_l^\times/\{\pm 1\}, \mathbb{Z}/p^n\mathbb{Z})$ from class field theory. From lemma above, $H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}/N\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/N\mathbb{Z} \otimes \mathbb{Z}/p^n\mathbb{Z}$.

2. The result comes from Kummer theory.

   $H^1(\mathrm{Gal}(\bar{\mathbb{Q}})/\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z}(1)) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n}$. When restricted to local cohomology at s outside Np, the desired unramified cohomological class corresponds to unramified extension over $\mathbb{Q}_s$ and are in the subspace $\mathbb{Z}_s^\times \otimes \mathbb{Z}/p^n\mathbb{Z} \subset \mathbb{Q}_s^\times \otimes \mathbb{Z}/p^n\mathbb{Z} \cong H^1_s(\mathbb{Z}/p^n\mathbb{Z}(1))$. Being flat at p implies the local cohomology class is also in $\mathbb{Z}_p^\times \otimes \mathbb{Z}/p^n\mathbb{Z}$.

   Thus $H^1(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(1)) \cong \mathbb{Z}[\frac{1}{N}]^\times \otimes \mathbb{Z}/p^n\mathbb{Z}$.

3. For detailed proofs, check [13, lemma 6.3.6].

   In this paragraph we recast the proof following [5, lemma 3.9], which will be later used.

   K_n is the field $\mathbb{Q}(\xi_{p^n})$, the field extension of $\mathbb{Q}$ adding p^n-th root of unity.

   $\tilde{K}$ is the maximal Galois extension over K_n, unramified outside pN.

   $G_{\mathbb{Q},S} \cong \mathrm{Gal}(\tilde{K}/\mathbb{Q}),\ H := \mathrm{Gal}(\tilde{K}/K_n),\ \Delta := \mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$.

   Since $H^1_{p,flat}(\mathbb{Z}/p^n\mathbb{Z}(-1)) = 0$, we have that

$$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(-1)) = ker(H^1(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(-1)) \to H^1_p(\mathbb{Z}/p^n\mathbb{Z}(-1)).$$

   From the inflation-restriction sequence of $H \trianglelefteq G_{\mathbb{Q},S}$, we have the following commutative diagram, where V stands for $\mathbb{Z}/p^n\mathbb{Z}(-1)$.

$$\begin{array}{ccccccc}
0 \longrightarrow & H^1(\Delta, V^H) & \longrightarrow & H^1(G_{\mathbb{Q},S}, V) & \longrightarrow & H^1(H, V)^\Delta & \longrightarrow H^2(G_{\mathbb{Q},S}, V^H) \\
& \downarrow & & \downarrow \mathrm{Res}_p & & \downarrow \mathrm{Res}_{\mathfrak{p}} & \downarrow \\
0 \longrightarrow & H^1(D_{\mathfrak{p}/p}, V^H) & \longrightarrow & H^1(D_p, V) & \longrightarrow & H^1(D_{\mathfrak{p}}, V)^{D_{\mathfrak{p}/p}} & \longrightarrow H^2(D_{\mathfrak{p}/p}, V^H)
\end{array}$$

Because $K_n/\mathbb{Q}$ is totally ramified at p and $\mathfrak{p}$ is the unique prime over p, then $D_{\mathfrak{p}/p} \xrightarrow{\sim} \Delta$. So the first and the last vertical maps are isomorphism, and

$$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{Z}/p^n\mathbb{Z}(-1)) = \ker(\mathrm{Res}_p) \cong \ker(\mathrm{Res}_{\mathfrak{p}})$$

$\mathbb{Z}/p^n\mathbb{Z}(-1)$ is a trivial H module, thus

$$H^1(H, \mathbb{Z}/p^n\mathbb{Z}(-1))^{\Delta} = \mathrm{Hom}(H^{\Delta=\chi^{-1}}, \mathbb{Z}/p^n\mathbb{Z}) = \mathrm{Hom}(\left(H^{\mathrm{ab}}/\{p^n\}\right)^{\chi^{-1}}, \mathbb{Z}/p^n\mathbb{Z})$$

Notation: for a group G, $\{p^n\} \subset G$ is the subgroup generated by g^{p^n} for all g.
Let the number field L_n be the maximal abelian extension of K_n being unramified outside N, splitting completely at places over p, whose Galois group over K_n is of exponent dividing p^n with Δ acting by χ^{-1}. Thus

$$\ker(\mathrm{Res}_{\mathfrak{p}}) \cong \mathrm{Hom}(\left(H^{\mathrm{ab}}/(D_{\mathfrak{p}}, \{p^n\})\right)^{\chi^{-1}}, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(L_n/K_n), \mathbb{Z}/p^n\mathbb{Z})$$

From class field theory of field K_n, here U denotes the global units of K_n and $\mathrm{RCl}_N := K^{\times} \backslash \mathbb{A}_f^{\times} / \prod_{v \nmid N} \mathcal{O}_v^{\times}$, we have

$$U \Big\backslash \prod_{r|N} \mathcal{O}_r^{\times} \to \mathrm{RCl}_N \to \mathrm{Cl}_K \to 0$$

We will quotient $\{p^n\}$ and take $\Delta = \chi^{-1}$ subspace.
From Herbrand's criterion, $\mathrm{Cl}_K \Big/ \{p^n\}^{\chi^{-1}} = \{0\}$ when $p \geq 5$, thus

$$\left(\prod_{r|N} \mathcal{O}_r^{\times} \Big/ \{p^n\}\right)^{\chi^{-1}} \longrightarrow\!\!\!\!\!\rightarrow \left(\prod_{r|N} \mathcal{O}_r^{\times} \Big/ (U, \{p^n\})\right)^{\chi^{-1}} \xrightarrow{\sim}\!\!\!\!\!\rightarrow \left(\mathrm{RCl}_N \Big/ \{p^n\}\right)^{\chi^{-1}}$$
$$\Big\downarrow q$$
$$\mathrm{Gal}(L_n/K_n) \qquad (*)$$

Here, the action of Δ on the ideles is induced from the action on K. The map q is quotient by the subgroup generated by $1-\xi_{p^r} \in K_{n,\pi} \hookrightarrow \mathrm{RCl}_N$ with π the unique place over p and $1-\xi_{p^r}$ a uniformizer.

First, we will study $\left(\prod_{r|N} \mathcal{O}_r^\times \Big/ \{p^n\}\right)^{\chi^{-1}}$.

For each $r|N$, $r\mathcal{O}_{K_n} = \mathfrak{r}_1 \cdots \mathfrak{r}_s$ and for each prime ideal $\mathfrak{r}_i$, $\mathcal{O}/\mathfrak{r}_i \cong \mathbb{F}_{r^f}$, the degree f extension of $\mathbb{F}_r$ with f the smallest integer such that $p^n | r^f - 1$. And $D_{\mathfrak{r}} \subset \Delta$ is the subgroup stabilizing $\mathfrak{r}_1$, with $D_{\mathfrak{r}} \cong \mathbb{Z}/f\mathbb{Z}$ generated by $\mathrm{Frob}_{\mathfrak{r}}$. Then as a $\Delta-$module,

$$\mathcal{O}_r^\times \Big/ \{p^n\} \cong \mathrm{Ind}_{D_{\mathfrak{r}}}^{\Delta} (\mathcal{O}/\mathfrak{r}_1)^\times \Big/ \{p^n\} \text{ and } \left(\mathcal{O}_r^\times \Big/ \{p^n\}\right)^{\chi^{-1}} \cong \left((\mathcal{O}/\mathfrak{r}_1)^\times \Big/ \{p^n\}\right)^{D_{\mathfrak{r}}=\chi^{-1}}$$

We compute the latter space now, x_0 is a generator in $\mathcal{O}/\mathfrak{r}_1$, then

$$\mathrm{Frob}_{\mathfrak{r}}(x_0^a) = x_0^{ar} = \chi^{-1}(\mathrm{Frob}_{\mathfrak{r}}) x_0^a = x_0^{ar^{-1}}$$

$x_0^{a(r^2-1)} = 1$ in $(\mathcal{O}/\mathfrak{r}_1)^\times \Big/ \{p^n\}$ if and only if $p^n | a(r^2-1)$. Thus the latter space $\cong \mathbb{Z}_p/(p^n, r^2-1)\mathbb{Z}_p$.

Next, we need to consider the quotient map q, corresponding to the requirement that L_n splits completely at places over p. The diagonal embedding of $1-\xi_{p^n}$ of $\prod_{r|N} \mathcal{O}_r^\times \Big/ \{p^n\}$ gives $((1-\xi_{p^n})^{-1})_\pi$ in $\mathrm{RCl}_N \Big/ \{p^n\}$. We will show that this element when projected to χ^{-1} quotient is 0, thus the quotient map q has trivial kernel.

$$X := \prod_{a \in \Delta} \chi(a) a (1-\xi_{p^n}) = \prod_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} (1-\xi_{p^n}^a)^a \in \left(\prod_{r|N} \mathcal{O}_r^\times \Big/ \{p^n\}\right)^{\chi^{-1}}$$

It suffices to show $X^2 = 0$, because 2 does not divide the order of χ^{-1} space.

$$X^2 = \prod_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} (1-\xi_{p^n}^a)^a \prod_{a \in (X := \mathbb{Z}/p^n\mathbb{Z})^\times} (1-\xi_{p^n}^{-a})^{-a} = \xi_{p^n}^{\sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} a^2}$$

From elementary computation $\sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} a^2 \equiv 0 \bmod p^n$, thus $X = 0$.

Next we need to show that $U^{\Delta=\chi^{-1}}$ is trivial. Use U^+ to denote the real units, i.e all the units such that $c(u) = u$ here $c \in \Delta$ is the complex conjugate. Thus U^+ has trivial $\Delta = \chi^{-1}$ subspace. So is the the torsion-free part of U^+, denoted as U^+_{tf}. There is the exact sequence

$$0 \to \mu_{2p^n} \to U \to U^+_{tf} \to 0$$

Taking the $\Delta = \chi^{-1}$ invariant space, we have $U^{\Delta=\chi^{-1}}$ is trivial.

□

CHAPTER 5

MAIN PROOF

5.1 $R = T$

Recall R_N is the universal pseudodeformation ring of finite-flat at p and Steinberg at $r|N$ pseudorepresentations lifting $\bar{D}$.

The definition for T, we can refer section3.2. Consider the minimal primes of T, (i.e the minimal primes of $\widetilde{T}$ contained in $\mathfrak{m}$). The set of these prime ideals is bijection with Galois conjugacy classes of normalized eigenforms in $M = \mathbb{Q}_p E \oplus S_2(\Gamma_0(N), \mathbb{Q}_p)^{\text{new}}$.

$$\Sigma := \{f \in S_2(\Gamma_0(N), \overline{\mathbb{Q}_p})^{\text{new}} \text{ normalized eigenforms } | f \bmod \mathfrak{p} \equiv E \bmod p\}/\sim$$

The equivalence relation $\sim$ is Galois conjugation. And there is natural injection

$$v : T \hookrightarrow \mathbb{Z}_p \times \prod_{f\in\Sigma} O_f \text{ defined as: } t \to (a_1(tE), (a_1(tf))_f)$$

Furthermore, we have

Lemma 5.1. The local algebra T is complete with respect to its unique maximal ideal $\mathfrak{m}$.

Proof. T is complete with respect to ideal (p), because T is a finite free $\mathbb{Z}_p$-module. To show this lemma, it suffices to show the topology induced by powers of $\mathfrak{m}$ and ideal $(p) \subset T$ are the same. We have $(p) \subset \mathfrak{m}$.

For other direction, the push forward of $\mathfrak{m}^n$ along the map $T \hookrightarrow \mathbb{Z}_p \times \prod_{f\in\Sigma} O_f$ is the ideal $p^n \times (\mathfrak{p}_f^{n_f})_f$ with $n_f \geq 1$, thus if n is larger enough, then the push-forward ideal is contained in $(p)^{n_s}$, thus $\mathfrak{m}^n \subset (p)^{n_s}$ after pulling-back to T.

□

Lemma 5.2. There is a surjection $\iota : R_N \to T$ of augmented $\mathbb{Z}_p$ algebra. And ι maps $\mathrm{tr}(\rho(Frob_q))$ to T_q for $q \not| Np$.

Proof. check [14, proposition 4.1.1]

For each $f \in \Sigma$, there is a $G_{\mathbb{Q},S}$ representation $\rho_f : G_{\mathbb{Q},S} \to GL_2(O_f)$ such that

- for $s \nmid Np$, the characteristic polynomial of $\rho_f(\mathrm{Frob}_s)$ is $X^2 - a_s(f)X + s$.
- $\rho_f|_{G_p}$ is finite-flat.
- for $r|N$, there is an isomorphism

$$\rho_f|_{G_r} \cong \begin{pmatrix} \chi cyc & * \\ 0 & Id \end{pmatrix}$$

From the universality of R_N, for each $f \in \Sigma$, there is an algebra homomorphism $R_N \to O_f$, together with E. We have a map $\iota : R_N \to \mathbb{Z} \times \prod_{f \in \Sigma} O_f$. R_N is a quotient of $\mathbb{Z}_p[G_{\mathbb{Q},S}]$, thus ι sends $\mathrm{Tr}(\mathrm{Frob}_s)$ to $(s+1, (a_s(f))_f)$ for all $s \nmid Np$. Here Tr is the trace map of the universal pseudorepresentation. Because of Chebotarev's density theorem, the map is well-defined. Combined with v defined above, ι factor through T by sending $\mathrm{Tr}(\mathrm{Frob}_s)$ to T_s for all $s \nmid Np$. Next, we need to show ι is surjective. It suffices to show T is generated by all T_s with $s \nmid Np$ over $\mathbb{Z}_p$.

For $r|N$, $U_r \in T$ acting by 1 on E and $f \in \Sigma$, thus $U_r = 1$ in T.

We then consider T_p. The argument is the same as [14, proposition 4.1.1]. □

There is a canonical map $R_N \to \mathbb{Z}_p$ corresponding to the pseudorep $\chi_p \oplus 1$, which is the Galois rep attached to the Eisenstein series E. The kernel of the map is denoted by J^{min}. The argumentation ideal for T is the Eisenstein ideal I.

We can use the strengthening of Wiles' numerical criterion [16, Appendix]. The detailed statement can be found as [13, Theorem 7.1.1]. In our case, it suffices to show length of

$(J^{min}/J^{min}{}^2) \leq$ length $(\mathbb{Z}_p/\mathrm{Ann}_T(I))$.

And both of these two $\mathbb{Z}_p$ module, which is of the form of $\prod_s \mathbb{Z}_p/p^s\mathbb{Z}_p$. Then its length is $\log_p$(its size). Thus it suffices to show the size of $(J^{min}/J^{min}{}^2) \leq$ the size of $(\mathbb{Z}_p/\mathrm{Ann}_T(I))$ to prove ι is an isomorphism.

5.1.1 size of $J^{min}/J^{min}{}^2$

From this section, we add assumptions in Lemma 2.5. i.e

$N = r_1 r_2 l$ with $l \equiv 1 \bmod p$, $r_1, r_2 \not\equiv 1 \bmod p$ and r_1 is not a p-th power mod l.

Recall R_N^{red} is reducible locus of R_N. There is the canonical map $R_N \to R_N^{red} \to \mathbb{Z}_p$.

J^{red} is defined to be the kernel of $R_N \to R_N^{red}$. Then $J^{red} \subset J^{min}$.

Under the assumptions in Lemma 2.5, $R_N^{red} \cong \mathbb{Z}_p$. Then $J^{red} = J^{min}$.

We will compute $J^{red}/J^{min}J^{red}$ instead of computing the size of $J^{min}/J^{min}{}^2$.

Also from lemma 3.6, the size of $(\mathbb{Z}_p/\mathrm{Ann}_T(I))$ is size of $\mathbb{Z}_p \Big/ (l-1)\mathbb{Z}_p$.

Now the question boils down to proving the size of $J^{red}/J^{min}J^{red} \leq$ the size of $\mathbb{Z}_p \Big/ (l-1)\mathbb{Z}_p$.

5.1.2 size of $J^{red}/J^{min}J^{red}$

Recall the notations:

R_{flat}^{red} is the universal ring whose space parametrize all the pseudorepresentation lifting $\bar{D}$, being finite flat at p and reducible. And R_N^{red} is a quotient of R_{flat}^{red}.

$(R_N, E_N, \rho_N : G_{\mathbb{Q},S} \to E_N, D_N : E_N \to R_N)$ is the universal pseudodef ring and its universal Caley-Hamilton algebra satisfying being finite flat at p and Steinberg condition at $r|N$.

$$E_N = \begin{pmatrix} R_N & B_N \\ C_N & R_N \end{pmatrix} \quad \rho_N(\tau) = \begin{pmatrix} a_{N,\tau} & b_{N,\tau} \\ c_{N,\tau} & d_{N,\tau} \end{pmatrix} \quad \text{for } \tau \in G_{\mathbb{Q},S}$$

If the lower index N is changed to $flat$, it represents the universal pseudodef ring and its universal Cayley-Hamilton algebra satisfying only being finite flat at p.

The lower index may be dropped to save notations if there is no confusion.

B_N^{min} denotes $B_N/J^{min}B_N$, and C_N^{min} is similarly defined. $B_N^{min}\otimes C_N^{min} \to J^{red}/J^{min}J^{red}$ is surjective because J^{red} is the image of the map $B_N \otimes C_N \to R_N$.

Lemma 5.3. [14, Lemma 3.9.4] There are isomorphisms

$$\oplus_{r|N}\mathbb{Z}_p \cong B_{flat}^{min} \qquad \oplus_{r|N}\mathbb{Z}_p/(r^2-1)\mathbb{Z}_p \cong C_{flat}^{min}$$

The generators of B_{flat}^{min} are given by $b_{\gamma_{r_1}}, b_{\gamma_{r_2}}, b_{\gamma_l}$. Here $b_{\gamma_{r_1}}$ is the image of γ_{r_1} under the map $G_{\mathbb{Q},S} \to B_{flat}^{min}$. Similarly the generators of C_{flat}^{min} are given by c_{γ_r} with r satisfying $p|r^2-1$.

Proof. Theorem 2.5 (3) claims that for any finitely generated $\mathbb{Z}_p$-module M,

$$\mathrm{Hom}_{\mathbb{Z}_p}(B_{flat}^{min}, M) \cong H_{flat}^1(M(1))$$

From the structure of finitely generated $\mathbb{Z}_p$- module and the flat cohomology computations, $B_{flat}^{min} \cong \prod_{r|N}\mathbb{Z}_p$.

From Nakayama's lemma, the generators of B_{flat}^{min} are the elements which are nonzero under the basis of $\mathrm{Hom}_{\mathbb{Z}_p}(B_{flat}^{min}, \mathbb{F}_p) \cong H_{flat}^1(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$. Kummer theory implies the $\mathbb{F}_p$ basis of $H_{flat}^1(G_{\mathbb{Q},S},)$ have representatives as $f_r : G_{\mathbb{Q},S} \to \mathbb{F}(1)$ with $f_r(\sigma) = \frac{\sigma(\sqrt[p]{r})}{\sqrt[p]{r}}$ for each $r|N$. The field cutting out by f_r is $\mathbb{Q}(\xi_p, \sqrt[p]{r})$ that only ramifies at r and p, and $f_r(\gamma_r) \neq 0$. Unwinding the proofs of Theorem 2.5, f_r can be chosen satisfying $b_{\gamma_r}(f_s) = f_s(\gamma_r)$, and it is nonzero if and only if $r \neq s$. Thus b_{γ_r} with $r|N$ is a set of generators of B_{flat}^{min}.

Similarly, we can have $C_{flat}^{min} \cong \oplus_{r|N}\mathbb{Z}_p/(r^2-1)\mathbb{Z}_p$. To check the generators, we analyze $H_{flat}^1(\mathbb{F}_p(-1))$ in details.

From the argument of lemma 4.2 (3) in flat cohomology computations,

$$H^1_{flat}(\mathbb{F}_p(-1)) \cong \mathrm{Hom}(\mathrm{Gal}(L/\mathbb{Q}(\xi_p)), \mathbb{F}_p)$$

If $p|r^2-1$, then there is a unique subfield K_r of L, degree p over $\mathbb{Q}(\xi_p)$ which is ramified only at places above r. Then the representative $f_r : G_{\mathbb{Q},S} \to \mathbb{F}_p(-1)$ of cohomology class, whose restriction to $\mathrm{Gal}_{\mathbb{Q}(\xi_p)}$ factor through K_r, is a set of basis for $H^1_{flat}(\mathbb{F}_p(-1))$. Then $f_r(\gamma_s)$ nonzero if and only if $s \neq r$. Similar reasoning applies for the generators of C^{min}_{flat}. $\square$

Lemma 5.4. There are surjections

$$\oplus_{r|N}\mathbb{Z}_p \to B^{min}_N \qquad \mathbb{Z}_p/(l-1)\mathbb{Z}_p \to C^{min}_N$$

And the generators of B^{min}_N are given by $b_{\gamma_{r_1}}, b_{\gamma_{r_2}}, b_{\gamma_l}$, and the generators of C^{min}_N are given by c_{γ_l}.

Proof. There is a surjective map $E^{\min}_{\mathrm{flat}} = \begin{pmatrix} \mathbb{Z}_p & B^{\min}_{\mathrm{flat}} \\ C^{\min}_{\mathrm{flat}} & \mathbb{Z}_p \end{pmatrix} \twoheadrightarrow \begin{pmatrix} \mathbb{Z}_p & B^{\min}_N \\ C^{\min}_N & \mathbb{Z}_p \end{pmatrix}$.
The $V(\sigma,\tau)$ for σ and τ in G_r for $r|N$ are 0 in the image. This condition is equivalent to $(\chi(\tau_r)-1)c(\sigma_r) + (\chi(\sigma_r)-1)c(\tau_r)$ for any $\sigma_r, \tau_r \in G_r$, which implies $(r-1)c(\gamma_r) = 0$ with γ_r the generator of pro$-p$ part of inertial subgroup I_r.
Under the assumption that $r_1, r_2 \not\equiv 1 \bmod p$, the generator for C^{min}_N can only be c_{γ_l}. $\square$

Remark 5.1. To save notations, later we will use b_{γ_r} to denote both the generator of B^{min}_{flat} or its image in B^{min}_N or the generator in $H^1_{flat}(\mathbb{F}_p(1))$ that corresponding to the field $\mathbb{Q}(\xi_p, \sqrt[p]{r})$ in above proof. Similarly, c_{γ_r} to denote multiple roles when no confusion is caused.

Lemma 5.5. $b_{\gamma_l} c_{\gamma_l} \in {J^{min}}^2$

Proof. We use $\begin{pmatrix} a_{\gamma_l} & b_{\gamma_l} \\ c_{\gamma_l} & d_{\gamma_l} \end{pmatrix}$ to denote the image of γ_l under $G_{\mathbb{Q},S} \to E_N$. Then $a_{\gamma_l} \equiv \chi(\gamma_l)$ mod $J^{\min}_N$, thus $a_{\gamma_l} - 1 \in J^{\min}_N$.

$V(\gamma_l, \gamma_l) = (\rho(\gamma_l) - 1)^2 = 0$ implies $(a_{\gamma_l} - 1)^2 + b_{\gamma_l} c_{\gamma_l} = 0$, thus $b_{\gamma_l} c_{\gamma_l} \in J_N^{\min 2}$.

□

Lemma 5.6. If r_1 is not a $p-th$ power mod l, then $b_{\sigma_l}, b_{\gamma_l}, b_{\gamma_{r_2}}$ are basis of B_{flat}^{min}.

Proof. It suffices to show that the cohomology class's image in $H^1(G_l, \mathbb{F}_p(-1))$ is nonzero. It suffices to require the decomposition group D_l is nontrivial for the field extension $\mathbb{Q}(\xi_p, \sqrt[p]{r_1})/\mathbb{Q}(\xi_p)$, and it is true if and only if r_1 is not a $p-th$ power mod l. □

Lemma 5.7.

$$b_{\sigma_l} c_{\gamma_l} \in (J^{min})^2$$

Proof. This follows from $V(\sigma_l, \gamma_l) = 0$, $V(\gamma_l, \sigma_l) = 0$.
In more details, $V(\sigma_l, \gamma_l) = 0$ gives

$$(a_{\sigma_l} - 1)(a_{\gamma_l} - 1) + b_{\sigma_l} c_{\gamma_l} = 0$$

and $V(\gamma_l, \sigma_l) = 0$ gives

$$(d_{\sigma_l} - 1)(d_{\gamma_l} - 1) + b_{\sigma_l} c_{\gamma_l} = 0$$

$d_{\gamma_l} - 1$ and $a_{\gamma_l} - 1$ are both in J^{min}. And at least one of $a_{\sigma_l} - 1$ and $d_{\sigma_l} - 1$ is in J^{min}.
Thus $b_{\sigma_l} c_{\gamma_l} \in J^{min 2}$. □

In summary,

Theorem 5.1. *Under the following assumptions*

- $r_1, r_2 \not\equiv 1 \ mod\ p$ *and* $l \equiv 1 \ mod\ p$.
- r_1 *is not a p-th power mod l.*

$B_N^{min} \otimes C_N^{min} \twoheadrightarrow J^{red}/J^{red} J^{min} \cong J^{min}/(J^{min})^2$ *is generated by* $b_{\gamma_{r_2}} \otimes c_{\gamma_l}$. *Then the size of* $J^{min}/(J^{min})^2$ *is less than* $|\mathbb{Z}_p/(l-1)\mathbb{Z}_p|$.

Furthermore, $\iota : R_N \to T$ *is an isomorphism.*

5.2 generators of I

Notation: From this section, we will use c_l to denote c_{γ_l} to save notations.

We are interested in when $T_q - (q+1)$ generates I. Because of $R_N \xrightarrow{\sim} T$, we can study the generators of J^{min}.

$(R_N, \mathfrak{m})$ is a local ring, J^{min} is an R_N module and $\mathfrak{m} = (J^{min}, p)$. It suffices to find out the generators of $J^{min}/\mathfrak{m}J^{min}$.

The surjection $J^{min}/(J^{min})^2 \to J^{min}/\mathfrak{m}J^{min}$ implies $\dim_{\mathbb{F}_p}(J^{min}/\mathfrak{m}J^{min}) \leq 1$. Actually, its dimension is 1. It can been seen as below:

Assume $\dim_{\mathbb{F}_p}(J^{min}/\mathfrak{m}J^{min}) = 0$, then from Nakayama's lemma, $J^{min} = 0$, thus $R_N \cong \mathbb{Z}_p$. But [17, Theorem 1.2, 1.3] claims that there is some new cuspform of level $N = r_1 r_2 l$ which is congruent to E mod p, which implies $R_N \ncong \mathbb{Z}_p$. This leads contradiction, thus $\dim_{\mathbb{F}_p}(J^{min}/\mathfrak{m}J^{min}) = 1$, and J^{min} is a principally generated ideal.

$$\mathrm{Hom}_{\mathbb{F}_p}(J^{min}/\mathfrak{m}J^{min}, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{m}/(\mathfrak{m}^2, p), \mathbb{F}_p) \cong \mathrm{Hom}(R_N, \mathbb{F}_p[\epsilon])$$

The first isomorphism is because $J^{min} \cap (p) = pJ^{min}$ as ideals in $R_N \cong T$, thus

$$J^{min} \cap (\mathfrak{m}^2, p) = J^{min} \cap (p, \mathfrak{m}J^{min}) = \mathfrak{m}J^{min}$$

This implies $J^{min}/\mathfrak{m}J^{min} \xhookrightarrow{\sim} \mathfrak{m}/(\mathfrak{m}^2, p)$. Thus the tangent space of the pseudo deformation space, denoted by $\mathfrak{T}_N$ is of dimensional 1.

We would like to explicitly construct a GMA structure giving rise to the nontrivial pseudo-deformation in the tangent space.

5.2.1 tangent space of R_N

There is no explicit description of $\mathcal{T}_N$. But we have

$$0 \to \mathcal{T}_{flat} \to \mathrm{Ext}^1_{flat}(\mathbb{F}_p(1), \mathbb{F}_p) \otimes \mathrm{Ext}^1_{flat}(\mathbb{F}_p, \mathbb{F}_p(1)) \to \mathrm{Ext}^2(\mathbb{F}_p, \mathbb{F}_p) \oplus \mathrm{Ext}^2(\mathbb{F}_p(1), \mathbb{F}_p(1)))$$

And $\mathcal{T}_N \hookrightarrow \mathcal{T}_{flat}$.

Following the proof of Theorem 2.6, for a pseudorepresentation D in $\mathcal{T}_N$, $E = \begin{pmatrix} \mathbb{F}_p[\epsilon] & B \\ C & \mathbb{F}_p[\epsilon] \end{pmatrix}$ is one $GMA-$structure satisfying finite flat at p and Steinberg at $r|N$ with $m : B \otimes C \to {}^{B}/_{\epsilon B} \otimes {}^{C}/_{\epsilon C} \to \mathbb{F}_p\epsilon$.

There are surjections $B_N^{min} \to {}^{B}/_{\epsilon B}$ and $C_N^{min} \to {}^{C}/_{\epsilon C}$, thus $m \in \mathrm{Hom}(B_N^{min} \otimes C_N^{min}, \mathbb{F}_p)$, and the latter space is a subspace of $H^1_{flat}(\mathbb{F}_p(1)) \otimes \mathbb{F}_p\{c_l\}$.

Also, m is in the kernel of the cup product maps.

Lemma 5.8. Assume $r \not\equiv 1 \bmod p$, then the image of c_l under the restriction map

$$H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{F}_p(-1)) \to H^1_{flat}(G_r, \mathbb{F}_p(-1))$$

is trivial.

Proof. The set-up for the proof is the same as . There is a diagram

$$\begin{array}{ccccc} \left(\prod_{r|N} ({}^{\mathcal{O}}/_{r\mathcal{O}})^\times \Big/ \{p\}\right)^{\Delta=\chi^{-1}} & \twoheadrightarrow & \left(\mathbb{Q}(\xi_p)^\times \backslash \mathbb{A}_f^\times / \prod_{v\nmid N} \mathcal{O}_v^\times\right) \Big/ \{p\}^{\Delta=\chi^{-1}} & & \\ \downarrow & \searrow^{\sim} & \downarrow & & \\ \mathbb{F}_p \cong \left(({}^{\mathcal{O}}/_{l\mathcal{O}})^\times \Big/ \{p\}\right)^{\Delta=\chi^{-1}} & \twoheadleftarrow & \mathrm{Gal}(L/\mathbb{Q}(\xi_p)) & & \end{array}$$

K_c is the unique subfield of L only ramifying at places above l over $\mathbb{Q}(\xi_p)$, its degree over $\mathbb{Q}(\xi_p)$ is p and it corresponds to the $\mathbb{F}_p$ quotient above. And c_l is a nontrivial homomorphism

$\mathrm{Gal}(K_c/\mathbb{Q}(\xi_p)) \to \mathbb{F}_p$.

This lemma is equivalent to K_c over $\mathbb{Q}(\xi_p)$ splits completely over places above r, if $r \not\equiv 1 \mod p$.

Places above r in $\mathbb{Q}(\xi_p)$ are denoted by $\mathfrak{r}_1, \cdots \mathfrak{r}_g$ with $fg = p-1$ and f being the inertia degree. $r \not\equiv 1 \mathrm{mod} p$ implies $f > 1$. Use $\pi_{\mathfrak{r}_1}$ to denote a uniformizer for place $\mathfrak{r}_1$.

From class field theory, $\mathfrak{r}_i$ splits completely in K_c over $\mathbb{Q}(\xi)$ is equivalent to $(1, \cdots, \pi_{\mathfrak{r}_i}, \cdots, 1)$ (the only non 1 place is $\mathfrak{r}_\mathfrak{i}$) under the projection to the $\mathbb{F}_p$ quotient is trivial.

$(1, \cdots, \pi_{\mathfrak{r}_i}, \cdots, 1)$ projected to $\Delta = \chi^{-1}$ subspace:

$$\sum_{g \in \Delta} \chi(g) g.(1, \cdots, \pi_{\mathfrak{r}_i}, \cdots, 1) = \sum_{g \in \Delta/D_r} \chi(g) g. \sum_{h \in D_r} \chi(h) h.(1, \cdots, \pi_{\mathfrak{r}_i}, \cdots, 1)$$

here D_r is the decomposition group for place $\mathfrak{r}_i$.

Pick one generator h_0 of D_r and $\chi(h_0) = a$, and $a \neq 1$ then

$$\sum_{h \in D_r} \chi(h) h.(1, \cdots, \pi_{\mathfrak{r}_i}, \cdots, 1) = (1, \cdots, \pi_{\mathfrak{r}_i}^{\frac{1-a^f}{1-a}}, \cdots, 1) \quad \text{up to units in } \mathcal{O}_{\mathfrak{r}_i}$$

Because $a^f = 1$ in $\mathbb{Z}/p\mathbb{Z}$, then the above element is in $\prod_{i=1}^{g} \mathcal{O}_{\mathfrak{r}_i}^{\times}$ which has trivial image under the projection to the $\mathbb{F}_p$ quotient.

□

Example 5.1. Assume $(l, r_1, r_2) = (101, 2, 3)$, $p = 5$. Then K_c is the unique degree p field over $\mathbb{Q}(\xi_p)$ only ramified at $l = 101$, and $\mathrm{Gal}(K_c/\mathbb{Q})$ sits inside the exact sequence below

$$0 \to \mathrm{Gal}(K_c/\mathbb{Q}(\xi_p)) = \mathbb{Z}/p\mathbb{Z} \to \mathrm{Gal}(K_c/\mathbb{Q}) \to \mathbb{Z}/p\mathbb{Z}^{\times} \to 0$$

with $\mathbb{Z}/p\mathbb{Z}^{\times}$ acting on the sub by χ^{-1} and places above p splits completely for the field extension $K_c/\mathbb{Q}(\xi_p)$.

More information about this field, checkLMFDB

Lemma 5.9. $H \subset H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ is defined to the subset

$$\{b | b \cup c_l = 0 \in H^2(G_{\mathbb{Q},S}, \mathbb{F}_p) \text{ and } b|_{I_l} = 0 \in H^1(I_l, \mathbb{F}_p(1))\}$$

then under the assumption above (at the end of last section), H is of dimension 1.

And $b \in H$ satisfies its restriction to G_l in trivial. i.e $b|_{G_l} = 0$.

Proof. $H^1_{flat}(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ is generated by Kummer classes b_{r_1}, b_{r_2} and b_l as a vector space. The restriction to inertia group I_l being trivial implies $b = a_1 b_{r_1} + a_2 b_{r_2}$, the field cutting out by b is $\mathbb{Q}\big(\xi_p, \sqrt[p]{r_1^{a_1} r_2^{a_2}}\big)$.

Check Appendix B in [14]. We apply lemma B 1.2 and lemma B 1.3. $H^2(G_{\mathbb{Q},S}, \mathbb{F}_p) \xrightarrow{\sim} H^2_l(\mathbb{F}_p)$. In $H^2_l(\mathbb{F}_p)$, the cup product of a nontrivial cohomology class unramified at l with c_l does not vanish. Because b_{r_1} restricted to D_l is nontrivial, this follows from r_1 is not a p-th power mod l and $\mathbb{Q}(\xi_p, \sqrt[p]{r_1})$ is inert at l over $\mathbb{Q}(\xi_p)$, thus

$b_{r_1} \cup c_l \neq 0$.

The global Euler characteristic formula implies $H^2(G_{\mathbb{Q},S}, \mathbb{F}_P)$ is of dimension 1 (since $H^1(G_{\mathbb{Q},S}, \mathbb{F}_p)$ is of dimension 2), thus $b_{r_1} \cup c_l$ is a $\mathbb{F}_p$ space generator.

$$b \cup c_l = (a_1 b_{r_1} + a_2 b_{r_2}) \cup c_l = 0 \quad \Longrightarrow \; a_1 = -a_2 \frac{b_{r_2} \cup c_l}{b_{r_1} \cup c_l}$$

Thus H is of dimension 1. □

5.2.2 Explicit constructions of GMA-structure

Next, we will explicitly construct a generalized matrix algebra structure satisfying being finite flat at p and Steinberg at $r|N$.

The ideal follows from the proof of Theorem 2.6.

We can a lift $\tilde{c}_l \in Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p(-1))$ of c_l in $H^1(G_{\mathbb{Q},S}, \mathbb{F}_p(-1))$ such that $\tilde{c}_l|_{G_p} = 0$. The

existence of such lifting is guaranteed from $c_l|_{G_p} = 0 \in H^1(G_p, \mathbb{F}_p(-1))$.

In details, $\tilde{c}_l$ is a map $\mathrm{Gal}(K_c/\mathbb{Q}) \to \mathbb{F}_p$ satisfying cocycle condition, where K_c is the degree p extension over $\mathbb{Q}(\xi_p)$ that ramifies only at l, splits completely over places above p and Δ acts $\mathrm{Gal}(K_c/\mathbb{Q}(\xi_p))$ by χ^{-1}.

Furthermore, because of lemma 5.3 c_l restricted to G_{r_i} is trivial, we can choose places $\mathfrak{R}_1, \mathfrak{R}_2, \mathfrak{P}$ of K_c above r_1, r_2, p respectively such that $\tilde{c}_l$ restricted to $D_{\mathfrak{R}_1/r_1}, D_{\mathfrak{R}_2/r_2}, D_{\mathfrak{P}/p}$ respectively is 0.

To see this, there is an exact sequence for $\mathrm{Gal}(K_c/\mathbb{Q})$,

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathrm{Gal}(K_c/\mathbb{Q}) \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \to 0$$

The subgroup is $\mathrm{Gal}(K_c/\mathbb{Q}(\xi_p))$, and $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ acts on $\mathbb{Z}/p\mathbb{Z}$ by χ^{-1}.

Thus there are p many order $p-1$ cyclic subgroup inside $\mathrm{Gal}(K_c/\mathbb{Q})$ and they are conjugate to each other by elements in $\mathbb{Z}/p\mathbb{Z}$. There are p many places in K_c above p, these decomposition groups are also of order $p-1$ and conjugate to each other by elements in $\mathrm{Gal}(K_c/\mathbb{Q}(\xi_p))$. Thus those order $p-1$ subgroups are decomposition groups for places above p.

For place $\mathfrak{R}_1$ of K_c above r_1, $D_{\mathfrak{R}_1/r_1}$ is a cyclic group of order f_1 and is contained in some order $p-1$ subgroup. Similar claims are true for any place $\mathfrak{R}_2$ of K_c above r_2. Thus we can choose $\mathfrak{R}_1$ and $\mathfrak{R}_2$ such that the decomposition groups are in the same order $p-1$ subgroup, which corresponds to some place $\mathfrak{P}$ above p.

$b \in H$ is a nonzero element, and $b|_{G_l} \in H^1(G_l, \mathbb{F}_p(1)) = 0$. Thus we can pick a lift $\tilde{b} \in Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ of b such that $\tilde{b}|_{G_l} = 0$. Similarly, we use K_b to denote the smallest field such that $\tilde{b}|_{\mathrm{Gal}_{K_b}} = 0$.

- Construction of E

Both B and C are one dimension $\mathbb{F}_p$ vector space and as an $\mathbb{F}_p[\epsilon]-$ module, ϵ acts by 0.

Precise definition of B and C:

$\tilde{b} \in Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ generates a one-dimensional subspace, denoted by B^*, then B is defined, as a $\mathbb{F}_p[G_{\mathbb{Q},S}]$ module, to be $\mathrm{Hom}(B^*, \mathbb{F}_p(1))$. And B can be identified with $\mathbb{F}_p(1)$ via $f \to f(\tilde{b})$.

Similarly, C^* is the $\mathbb{F}_p$ vector subspace generated by $\tilde{c}_l$, and $C := \mathrm{Hom}(C^*, \mathbb{F}_p(-1))$.

$B \otimes C \to \mathbb{F}_p \to \mathbb{F}_p[\epsilon]$ is defined to be

$$f \otimes g \to f(\tilde{b})g(\tilde{c}_l) \in \mathbb{F}_p \to f(\tilde{b})g(\tilde{c}_l)\epsilon \in \mathbb{F}_p[\epsilon]$$

- Galois action on E

  Next we need to define the homomorphism $\rho : G_{\mathbb{Q},S} \to E^\times$.

  Write $\rho(g) = \begin{pmatrix} \rho_A(g) & \rho_B(g) \\ \rho_C(g) & \rho_D(g) \end{pmatrix}$.

  Define $\rho_B \in Z^1(G_{\mathbb{Q},S}, B) \cong Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ given by $\tilde{b}$.

  Define $\rho_C(g) = \chi(g)\tilde{c}_l(g)$ with $\tilde{c}_l \in Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p(-1)) \cong Z^1(G_{\mathbb{Q},S}, C)$ with χ being the mod p cyclotomic character.

  Because $b \cup c_l = 0 \in H^2(G_{\mathbb{Q},S}, \mathbb{F}_p)$, thus there is some $A : G_{\mathbb{Q},S} \to \mathbb{F}_p$ satisfying

  $$\tilde{b} \cup \tilde{c}_l = dA \qquad \text{i.e} \quad \tilde{b} \cup \tilde{c}_l(g_1, g_2) = A(g_1 g_2) - A(g_1) - A(g_2)$$

  The choice of A is not unique, different choices differ by elements in $Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p) = \mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{F}_p)$. Actually we can pick A such that $A|_{I_p} = 0$ and $A|_{G_{r_1}} = 0$ (Actually here I_p need to be chosen such that the prime over K_b above p with respect to I_p is $\mathfrak{P}$, similarly G_{r_1} is nicely chosen.)

  Why? Because $\tilde{c}_l|_{I_p} = 0$ and $\tilde{c}_{G_{r_1}} = 0$, then A is a homomorphism on I_p and on G_{r_1}.

From class field theory,

$$H^1(G_{\mathbb{Q},S}, \mathbb{F}_p) = \mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{F}_p) \cong \mathrm{Hom}((\mathbb{Z}/l\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p), \mathbb{F}_p)$$

and $H^1(I_p, \mathbb{F}_p) \cong \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{F}_p)$. For $i = 1, 2$, $H^1(G_{r_i}, \mathbb{F}_p)$ is a one dimensional space (because of the assumption that $p \not| r_i - 1$), and is given by the unique unramified degree p extension of $\mathbb{Q}_{r_i}$. There is a surjection $Z^1(G_{\mathbb{Q},S}, \mathbb{F}_p) = H^1(G_{\mathbb{Q},S}, \mathbb{F}_p) \to H^1(G_{r_1}, \mathbb{F}_p)$. Because r_1 is not a p-th power mod l.

Once A is fixed, define $\rho_A(g) = \chi(g)(1 + A(g)\epsilon)$.

To make sure the determinant of $\rho : G_{\mathbb{Q},S} \to E^\times$ is χ, $\rho_D(g)$ is defined to be $1 + D(g)\epsilon$ with $D(g) = \tilde{b}(g)\tilde{c}_l(g) - A(g)$.

It is easy to check that ρ defined above is indeed a group homomorphism.

- Check finite-flat at p and Steinberg condition

  Next we will adjust A such that The ρ is

  - finite flat at p
  - Steinberg at l
  - Steinberg at r_1 and r_2

  1. Check being finite flat at p, similar to lemma 7.1.9 in [14]. The key point is $\tilde{c}_l|_{G_p} = 0$ and $A|_{I_p} = 0$.
  2. Check it is Steinberg at l, similar to lemma 7.1.9 in [14], the key point is $\tilde{b}|_{D_l} = 0$ and $l \equiv 1 \bmod p$.
  3. Check it is Steinberg at r_1 and r_2.

     We have seen that $\tilde{c}_l|_{G_{r_1}} = \tilde{c}_l|_{G_{r_2}} = 0$ for some choice of decomposition group

G_{r_1} and G_{r_2}. Thus

$$\rho|_{G_{r_i}} = \begin{pmatrix} \chi(1+A\epsilon) & \tilde{b} \\ 0 & 1+D\epsilon \end{pmatrix}$$

We want ρ to satisfy Steinberg condition at r_i, which is

$$V_\rho(\sigma,\tau) = (\rho(\sigma)-\chi(\sigma))(\rho(\tau)-1) = 0 \text{ for every } \sigma,\tau \text{ in } G_{r_i}$$

which is equivalent to

$$\begin{cases} (\chi(\tau)-1)\chi(\sigma)A(\sigma) = 0 \\ (1-\chi(\sigma))A(\tau) = 0 \end{cases} \quad \text{for all } \sigma \text{ and } \tau \text{ in } G_{r_i}$$

The above condition is equivalent to $A(\sigma) = 0$ for all $\sigma \in G_{r_i}$.

Consider the map

$$H^1(G_{\mathbb{Q},S}, \mathbb{F}_p) \to H^1(G_{r_1}, \mathbb{F}_p) \times H^1(G_{r_2}, \mathbb{F}_p)$$

Thus we need to when A is chosen to satisfying $A|_{I_p} = 0 = A|_{G_{r_1}}$, A restricted to $A|_{G_{r_2}}$ is also trivial.

$A|_{G_{r_1}} = 0$

We first recall the set-up and notations.

$\tilde{b} \in Z^1_{flat}(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$ satisfying $\tilde{b}|_{G_l} = 0$ and lifting b is unique. Similarly $\tilde{c}_l \in Z^1_{flat}(G_{\mathbb{Q},S}, \mathbb{F}_p(-1))$ satisfying $\tilde{c}_l|_{G_p} = 0$ (then $\tilde{c}_l|_{G_{r_1}} = \tilde{c}_l|_{G_{r_2}} = 0$) and lifting c_l is unique.

$$\tilde{b} \cup \tilde{c}_l(g_1, g_2) = A(g_1 g_2) - A(g_1) - A(g_2)$$

$A : G_{\mathbb{Q},S} \to \mathbb{F}_p$ satisfies $A|_{I_p} = 0$ and $A|_{G_{r_1}} = 0$. Such A is also unique. Then we want to show

$$A|_{G_{r_2}} = 0$$

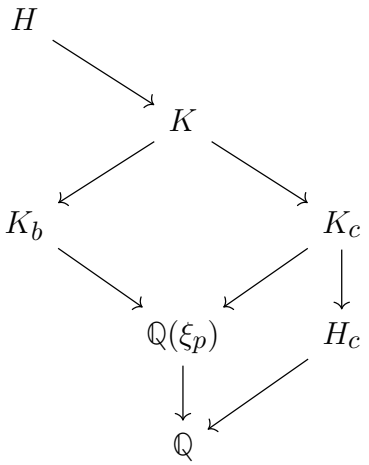
K_b is the field cutting out by b. To be more precise, any cocycle lifting b is a homomorphism when restricted to $Gal(\tilde{\mathbb{Q}}/\mathbb{Q}(\xi_p))$, K_b is the field corresponding to the kernel. K_b is of the form $\mathbb{Q}(\xi_p, \sqrt[p]{r_1^{a_1} r_2^{a_2}})$, and places above l split completely over $\mathbb{Q}(\xi_p)$.
Similarly, K_c is defined as before, the field cutting out by c_l. And places over p, r_1, r_2 in K_c split completely over $\mathbb{Q}(\xi_p)$ and places over l are totally ramified.

properties of A

Notation:

- For $i = 1, 2$, $\mathfrak{r}_j^i$ with $j = 1, \cdots, g_i$ to denote places in $\mathbb{Q}(\xi_p)$ over r_i.
  $\mathfrak{r}_1^i$ is the place such that $\tilde{c}_l|_{D_{\mathfrak{R}^i/\mathfrak{r}_1^i}}$ is 0 for some place of K_c over $\mathfrak{r}_1^i$.
- l splits completely in K_b over $\mathbb{Q}$, and $\mathfrak{l}_1, \cdots, \mathfrak{l}_{p(p-1)}$ are primes over l in K_b.

A is a homomorphism on $Gal(\tilde{\mathbb{Q}}/K_b)$, it follows from $\tilde{b}|_{Gal(\tilde{\mathbb{Q}}/K_b)} = 0$. Also $A|_{G_{r_2}}$ is a homomorphism because $\tilde{c}_i|_{G_{r_2}} = 0$. When $r_2 \not\equiv 1 \mathrm{mod} p$, $\mathrm{Hom}(G_{r_2}, \mathbb{F}_p)$ is given by the unique degree p unramified extension. Thus $A|_{I_{r_2}} = 0$.
Furthermore, we assume $A_{I_p} = 0$ and $A_{G_{r_1}} = 0$. Thus A is in $\mathrm{Hom}(Gal(H/K_b), \mathbb{F}_p)$, where H is the maximal abelian extension over K_b unramified outside places above l, r_1, r_2, and $\mathrm{Gal}(H/K_b)$ is of exponent p. H is Galois over $\mathbb{Q}$.
Let K denote the composition of K_b and K_c inside $\tilde{\mathbb{Q}}$, because places over p, r_1, r_2 split completely in K_c over $\mathbb{Q}(\xi_p)$, so do these places over K/K_b. Thus K is a subfield of H.



A can be viewed as a function on $\mathrm{Gal}(H/\mathbb{Q})$ satisfying the property

$$\tilde{b}(g_1)\chi^{-1}(g_1)\tilde{c}_l(g_2) = A(g_1g_2) - A(g_1) - A(g_2) \quad \text{for all } g_1 \text{ and } g_2 \text{ in } \mathrm{Gal}(H/\mathbb{Q}) \qquad ((*))$$

Also $A|_{I_{r_2}} = A|_{I_p} = 0$ for some I_{r_2}, I_p.

There is $\alpha \in I_{r_2} \subset \mathrm{Gal}(H/\mathbb{Q}(\xi_p))$ such that its projection to $\mathrm{Gal}(K_b/\mathbb{Q}(\xi_p))$ is a generator of $\mathrm{Gal}(K_b/\mathbb{Q}(\xi_p))$ and there is $\beta \in I_p \subset \mathrm{Gal}(H/\mathbb{Q})$ whose projection to $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is a generator of $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$.

Consider the subgroup generated by α and β inside $\mathrm{Gal}(H/\mathbb{Q})$, denoted by $<\alpha, \beta>$. Then $<\alpha, \beta>$ mod $\mathrm{Gal}(H/K_b)$ is isomorphic to $\mathrm{Gal}(K_b/\mathbb{Q})$.

$$\mathrm{Gal}(H/\mathbb{Q}) = \cup_{\gamma \in <\alpha,\beta>} \mathrm{Gal}(H/K_b)\gamma$$

And $A(\gamma) = 0$ for any γ in $<\alpha, \beta>$. This follows from

$$A(g_1g_2) = A(g_1) + A(g_2) \quad \text{for any } g_2 \in I_p \cup I_{r_2} \text{ and } A|_{I_{r_2}} = A|_{I_p} = 0$$

Every element in $\mathrm{Gal}(H/\mathbb{Q})$ can be written as $\sigma\gamma$ with $\sigma \in \mathrm{Gal}(H/K_b)$ and $\gamma \in< \alpha, \beta >$,

then

$$A(\sigma\gamma) = A(\sigma) \qquad \text{(property } \heartsuit\text{)}$$

Condition $(*)$ above now is that for every $\sigma, \sigma' \in \mathrm{Gal}(H/K_b)$ and for every $\gamma, \gamma' \in <\alpha, \beta>$

$$\begin{aligned}\tilde{b}(\sigma\gamma)\chi^{-1}(\sigma\gamma)\tilde{c}_l(\sigma'\gamma') &= A(\sigma\gamma\sigma'\gamma') - A(\sigma\gamma) - A(\sigma'\gamma') = A(\sigma\gamma\sigma'\gamma^{-1}\gamma\gamma') - A(\sigma) - A(\sigma') \\ &= A(\sigma\gamma\sigma'\gamma^{-1}) - A(\sigma) - A(\sigma') = A(\sigma) + A(\gamma\sigma'\gamma^{-1}) - A(\sigma) - A(\sigma') \\ &= A(\gamma\sigma'\gamma^{-1}) - A(\sigma')\end{aligned}$$

The left hand side is

$$\tilde{b}(\sigma\gamma)\chi^{-1}(\sigma\gamma)\tilde{c}_l(\sigma'\gamma') = (\tilde{b}(\sigma) + \tilde{b}(\gamma))\chi^{-1}(\sigma)\chi^{-1}(\gamma)\tilde{c}_l(\sigma'\gamma') = \tilde{b}(\gamma)\chi^{-1}(\gamma)\tilde{c}_l(\sigma')$$

Thus

$$\tilde{b}(\gamma)\chi^{-1}(\gamma)\tilde{c}_l(\sigma') = A(\gamma\sigma'\gamma^{-1}) - A(\sigma')$$

The above equality is true for special case $\sigma' \in \mathrm{Gal}(H/K)$, and $\tilde{c}|_{\mathrm{Gal}(H/K)} = 0$, thus for every $\sigma \in \mathrm{Gal}(H/K)$

$$A(\gamma\sigma\gamma^{-1}) = A(\sigma) \tag{5.1}$$

proof of $A|_{G_{r_2}} = 0$

To show $A|_{G_{r_2}} = 0$, by property$\heartsuit$, it suffices to show $A|_{G_{r_2} \cap \mathrm{Gal}(H/K_b)} = 0$.
There are two cases for K_b:

- If r_2 is some p-th power mod l, then $K_b = \mathbb{Q}(\xi_p)(\sqrt[p]{r_2})$.
  For the field extension $K_b/\mathbb{Q}(\xi_p)$, $\mathfrak{r}_j^{(1)}$ splits completely, and $\mathfrak{r}_j^{(2)}$ is totally ramified. (check the beginning of 5.4.2 for notations) Use $\pi_{\mathfrak{r}_j^{(2)}}$ to denote the unique prime in K_b above $\mathfrak{r}_j^{(2)}$.

- If r_2 is not pth power mod l, then $K_b = \mathbb{Q}(\xi_p)(\sqrt[p]{r_1^{a_1} r_2^{a_2}})$ for some a_1 and a_2 nonzero. In this case, for $K_b/\mathbb{Q}(\xi_p)$, $\mathfrak{r}_j^{(1)}$ and $\mathfrak{r}_j^{(2)}$, as places in $\mathbb{Q}(\xi_p)$, are totally ramified. Use $\pi_{\mathfrak{r}_j^{(i)}}$ with $i = 1, 2$ to denote the unique prime in K_b above $\mathfrak{r}_j^{(i)}$.

Class field theory give some description of $\mathrm{Gal}(H/K_b)$:

$$\left(K_b^{\times} \backslash \mathbb{A}_{K_b,f}^{\times} \Big/ \prod_{v \nmid l r_1 r_2} \mathcal{O}_{K_b,v}^{\times}\right) \Big/ \{p\} \xrightarrow{\sim} \mathrm{Gal}(H/K_b) \tag{5.2}$$

$$\frac{\oplus_{v|lr_1r_2} \left(\mathcal{O}_{K_b} / \pi_v\right)^{\times}}{\text{global units}} \Big/ \{p\} \to \mathrm{Gal}(H/K_b) \to Cl_{K_b}/(\{p\} \to 0$$

Lemma 5.10.

$$A|_{G_{r_2}} = 0$$

Proof. It suffice to show that $A([1, \cdots, \pi_{\mathfrak{r}_1^{(2)}}, \cdots, 1]) = 0$, because $A_{I_{r_2}} = 0$.
$[1, \cdots, \pi_{\mathfrak{r}_1^{(2)}}, \cdots, 1] \in \mathbb{A}_{K_b,f}^{\times}$ has only nontrivial entry appearing at place $\pi_{\mathfrak{r}_1^{(2)}}$.

For each $\pi_{\mathfrak{r}_j^{(2)}}$, there is some $\gamma_{2,j}$ such that $\gamma_{2,j} \pi_{\mathfrak{r}_1^{(2)}} = \pi_{\mathfrak{r}_j^{(2)}}$.
Because places over r_2 for K over K_b split completely, element $[1, \cdots, \pi_{\mathfrak{r}_j^{(2)}}, \cdots, 1]$ in $\mathrm{Gal}(H/K_b)$ is actually in the subgroup $\mathrm{Gal}(H/K)$, thus we have

$$A([1, \cdots, \pi_{\mathfrak{r}_j^{(2)}}, \cdots, 1]) = A(\gamma_{2,j}.[1, \cdots, \pi_{\mathfrak{r}_1^{(2)}}, \cdots, 1]) = A([1, \cdots, \pi_{\mathfrak{r}_1^{(2)}}, \cdots, 1])$$

The last equality above follows from the property (5.1) of A and the above isomorphism (5.2) is equivariant under the action $\mathrm{Gal}(K_b/\mathbb{Q})$.

- When $K_b = \mathbb{Q}(\xi_p, \sqrt[p]{r_2})$, Because A is a homomorphism restricted to $\mathrm{Gal}(H/K_b)$,

$$\sum_j A([1, \cdots, \pi_{\mathfrak{r}_j^{(2)}}, \cdots, 1]) = A(\prod_j [1, \cdots, \pi_{\mathfrak{r}_j^{(2)}}, \cdots, 1])$$

As ideals in K_b,

$$(\sqrt[p]{r_2}) = \pi_{\mathfrak{r}_1^{(2)}}\pi_{\mathfrak{r}_2^{(2)}}\cdots\pi_{\mathfrak{r}_{g_2}^{(2)}},$$

Thus

$$\prod_j [1,\cdots,\pi_{\mathfrak{r}_j^{(2)}},\cdots,1] \in \left(K_b^\times \backslash \mathbb{A}_{K_b,f}^\times \big/ \prod_{v\nmid lr_1r_2} \mathcal{O}_{K_b,v}^\times\right) \to Cl_{K_b} \text{ has trivial image.}$$

Actually

$$\prod_j [1,\cdots,\pi_{\mathfrak{r}_j^{(2)}},\cdots,1] = \frac{1}{\sqrt[p]{r_2}}\prod_j [1,\cdots,\pi_{\mathfrak{r}_j^{(2)}},\cdots,1] = [y_v]_v \quad \in K_b^\times\backslash\mathbb{A}_{K_b,f}^\times/\prod_{v\nmid lr_1r_2}\mathcal{O}_{v,K_b}^\times$$

here for $v\nmid lr_1r_2$ $y_v=1$; for $v|lr_1$ $y_v=\frac{1}{\sqrt[p]{r_2}}$; for $v=\pi_{\mathfrak{r}_j^{(2)}}$, $y_v=\frac{1}{\sqrt[p]{r_2}}\pi_{\mathfrak{r}_j^{(2)}}$.
Break $[y_v]_v$ into three parts: places over l, over r_1, and over r_2, and we will show for each piece $*$, $A(*)=0$.

- places over r_1:

  Places over r_1 splits completely for K_b over $\mathbb{Q}(\xi_p)$:

  Use $[1,\cdots,\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_j^{(1)},k}$ to denote the idele with only nontrivial element at k-th place above $\mathfrak{r}_j^{(1)}$ with $j=1,\cdots,g_1$ and $k=1,\cdots,p$.

  $$A([1,\cdots,\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_j^{(1)},k}) = A(\gamma_{j,k}.[1,\cdots,\gamma_{j,k}^{-1}\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_1^{(1)},1})$$

  here $\gamma_{j,k}$ ranges over the order pf_1 subgroup G_1 of $\mathrm{Gal}(K_b/\mathbb{Q})$.

  Here $[1,\cdots,\gamma_{j,k}^{-1}\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_1^{(1)},1}$ viewed as an element in $\mathrm{Gal}(H/K_b)$ is actually in the subgroup $\mathrm{Gal}(H/K)$. Thus

  $$A([1,\cdots,\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_j^{(1)},k}) = A([1,\cdots,\gamma_{j,k}^{-1}\sqrt[p]{r_2},\cdots 1]_{\mathfrak{r}_1^{(1)},1}) = 0$$

The first equality follows from the property (5.1) and the second equality is because $A|_{I_{r_1}} = 0$.

– places over r_2:

It is almost the same as above: $[1, \cdots, \sqrt[p]{r_2}^{-1}\pi_{\mathfrak{r}_j^2}, \cdots, 1]$ can be viewed as an element in $\mathrm{Gal}(H/K)$, because of property (5.1) and $A_{I_{r_2}} = 0$, thus

$$A([1, \cdots, \cdots, \sqrt[p]{r_2}^{-1}\pi_{\mathfrak{r}_1^2}, \cdots, \cdots, \sqrt[p]{r_2}^{-1}\pi_{\mathfrak{r}_{g_2}^2}, \cdots, 1]) = 0$$

– places over l: Want to show the statement below

$$A([1, \cdots, \sqrt[p]{r_2}, \cdots, \sqrt[p]{r_2}, \cdots, 1]) = 0$$

here $[1, \cdots, \sqrt[p]{r_2}, \cdots \sqrt[p]{r_2}, \cdots, 1]$ has only nontrivial element at places over l.

There are $p(p-1)$ places over l, denoted by $\mathfrak{l}_j$ with $j = 1, \cdots, p(p-1)$, and $\mathrm{Gal}(K_b/\mathbb{Q})$ acts transitively on these places. Assume $\mathfrak{l}_j = \gamma_j\mathfrak{l}_1$, then

$$A([1, \cdots, \sqrt[p]{r_2}, \cdots, 1]_{l,j}) = A(\gamma_j.[1, \cdots, \gamma_j^{-1}\sqrt[p]{r_2}, \cdots, 1]_{l,1})$$

Notice that $[1, \cdots, \gamma_j^{-1}\sqrt[p]{r_2}, \cdots, 1]_{l,1}$ is not necessarily in $\mathrm{Gal}(H/K)$, property (5.1) does not apply. We need to use the assumption $A_{G_{r_1}} = 0$, i.e

$$A([1, \cdots, \pi_{\mathfrak{r}_1^{(1)},1}, \cdots, 1]) = 0$$

here $\pi_{\mathfrak{r}_1^{(1)},k}$ is a uniformizer of place $\mathfrak{r}_1^{(1)}, 1$, because of the property (5.1), for every j and k

$$A([1, \cdots, \pi_{\mathfrak{r}_{j^{(1)},k}}, \cdots, 1]) = 0$$

Similar as above, we can consider the products of above ideles, then conclude

$A([z_v]_v) = 0$ here $z_v = 1$ if $v \nmid lr_1r_2$; $z_v = r_1^{-1}$ if $v|lr_2$; and $z_{\mathfrak{r}_j^{(1)},k} = r_1^{-1}\pi_{\mathfrak{r}_{j^{(1)}},k}$.
Similarly, we break $[z_v]_v$ into three parts, places over l, r_1, r_2, for places over r_1 and r_2, we can show $A([z_v]_{v|r_1r_2}) = 0$. Thus $A([z_v]_{v|l}) = 0$, i.e

$A([1, \cdots, r_1, \cdots, r_1, \cdots 1]_l) = 0$ lower index l means $r_1's$ are only at places over l

Because r_1 is not a pth power mod l, then r_1 is a generator of $\left(\mathbb{Z}/l\mathbb{Z}\right)^\times \Big/ \{p\}$, thus either $[1, \cdots, \sqrt[p]{r_2}, \cdots, \sqrt[p]{r_2}, \cdots 1]$ is trivial in $\left(\mathcal{O}_{K_b,v}/l\mathcal{O}_{K_b,v}\right)^\times \Big/ \{p\}$
or $[1, \cdots, \sqrt[p]{r_2}, \cdots, \sqrt[p]{r_2}, \cdots 1]_l$ generates the same subgroup as $[1, \cdots, r_1, \cdots, r_1, \cdots 1]_l$ inside $\left(\mathcal{O}_{K_b,v}/l\mathcal{O}_{K_b,v}\right)^\times \Big/ \{p\}$, in both cases,

$$A([1, \cdots, \sqrt[p]{r_2}, \cdots, \sqrt[p]{r_2}, \cdots 1]) = 0$$

- When $K_b = \mathbb{Q}(\xi_p, \sqrt[p]{r_1^a r_2^b})$, the proof is similar, instead we take the sum

$$\sum_j A([1, \cdots, \pi_{\mathfrak{r}_j^{(1)}}]) + \sum_k A([1, \cdots, \pi_{\mathfrak{r}_k^{(2)}}, \cdots, 1]) = g_2 A([1, \cdots, \pi_{\mathfrak{r}_k^{(2)}}, \cdots, 1])$$

The second equality follows from the assumption $A|_{G_{r_1}} = 0$.
We have instead as ideals $\prod_j \pi_{\mathfrak{r}_j^{(1)}} \prod_k \pi_{\mathfrak{r}_k^{(2)}} = (\sqrt[p]{r_1^{a_1} r_2^{a_2}})$. The rest arguments are basically the same.

□

5.3 admissible (l, r_1, r_2, q)

From last section, given $\tilde{b}$ and $\tilde{c}$ fixed, then there is a unique choice of A such that the GMA structure over $\mathbb{F}_p[\epsilon]$ defined above satisfies the desired properties. This GMA structure induces a nontrivial homomorphism $\phi_0 : R_N \to \mathbb{F}[\epsilon]$. And ϕ_0 is a $\mathbb{F}_p$ generator for $\mathrm{Hom}(J/\mathfrak{m}J, \mathbb{F}_p) \cong \mathrm{Hom}(R_N, \mathbb{F}_p[\epsilon])$.

As we have seen before, because of the Galois reps attached to modular forms, there is a natural isomorphism $\iota : R_N \to T$. And the map ι is uniquely determined by mapping $\mathrm{tr}(\rho(Frob_q))$ to T_q.

Thus $T_q-(q+1)$ does not generate I if and only if $\mathrm{tr}(\rho(Frob_q))-(q+1)$ does not generate J, if and only if for the homomorphism ϕ_0 in $\mathrm{Hom}(J/\mathfrak{m}J, \mathbb{F}_p)$, $\phi_0\big(\mathrm{tr}(\rho(Frob_q)) - (q+1)\big) = 0$.

Lemma 5.11. $D_R : R[G] \to R$ is a pseudorepresentation of dimension d, $f : R \to A$ is an algebra homomorphism. D_A is the pseudorepresentation given by $D_R \otimes_f A$. For every $g \in G$, $tr_{D_R}(g) \in R$ is the trace of D_R and $tr_{D_A}(g)$ is the trace of D_A, then $tr_{D_A}(g) = f(tr_{D_R}(g))$.

From the lemma above, it suffices to show $\mathrm{tr}(\rho_{\mathbb{F}_p[\epsilon]}(Frob_q)) = q+1$.

$$\mathrm{tr}(\rho_{\mathbb{F}_p[\epsilon]}(Frob_q))-(q+1) = \rho_A(\sigma_q)+\rho_D(\sigma_q)-(q+1) = [(\chi(\sigma_q)-1)A(\sigma_q)+\tilde{b}(\sigma_q)\tilde{c}(\sigma_q)]\epsilon = 0$$

here σ_q is a Frobenius element over q.

Lemma 5.12. $T_q - (q+1)$ generates I if and only if $T_q - (q+1)$ generates I°.

Proof. One direction is easy, it suffices to prove that if $T_q-(q+1)$ generates I°, then it also generates I.

Projection to cuspidal part $T \twoheadrightarrow T^\circ$ induces $\mathbb{F}_p$ space isomorphism

$$I/\mathfrak{m}I \xrightarrow{\sim} I^\circ/\mathfrak{m}^\circ I^\circ$$

From Nakayama's lemma, $T_q-(q+1)$ generates I if $T_q-(q+1) \to I/\mathfrak{m}I$ is surjective. The assumption is saying $T_q-(q+1)$ maps onto $I^\circ/\mathfrak{m}^\circ I^\circ$.

Thus this proves the lemma. □

In summary, $T_q-(q+1)$ does not generate I° if and only if

$$(\chi(\sigma_q)-1)A(\sigma_q)+\tilde{b}(\sigma_q)\tilde{c}(\sigma_q) = 0$$

Depending on whether $\chi(\sigma_q) = 0$, there are two cases:

1. If q splits completely in $\mathbb{Q}(\xi_p)$, i.e $q \equiv 1 \mathrm{mod} p$. Then $\chi(\sigma_q) = 1$, in this case, $T_q - (q+1)$ does not generate I if and only if $\tilde{b}(\sigma_q)\tilde{c}(\sigma_q) = 0$.
   $K_b = \mathbb{Q}(\xi_p, \sqrt[p]{R})$, with $R = r_2$ or $R = r_1^a r_2^b$ depending on whether r_2 is a $p-th$ power mod l. Then $\tilde{b}(\sigma_q) = 0$ if and only if R is a $p-th$ power mod q.

2. If q does not split completely in $\mathbb{Q}(\xi_p)$. As we have seen before, any place above q splits completely in $K_c/\mathbb{Q}(\xi_p)$. Thus $\tilde{c}(\sigma_q) = 0$. Thus in this case, $T_q - (q+1)$ does not generate I if and only if $A(\sigma_q) = 0$.

Case 1 gives the following theorem:

Theorem 5.2. *Assume $l \equiv 1$ mod p, $r_1, r_2 \not\equiv 1$ mod p and r_1 is not a p-th power mod l. Furthermore, we assume $q \equiv 1$ mod p and $R := r_1^a r_2$ for some $0 \leq a \leq p-1$ such that R is a $p-th$ power mod l, if R is also a p-th power mod q then $T_q - (q+1)$ does not generate I°. Thus the $4-$tuple (l, r_1, r_2, q) is admissible for $d = 4$.*

Example 5.2. This example is from case 1 above.

Let $(l, r_1, r_2) = (101, 2, 3)$, $N = 606$ and $p = 5$. There are two newform classes f_1 and f_2 in $S_2(\Gamma_0(606), \bar{\mathbb{Q}})^{\mathrm{new}}$ that are congruent to E.

The coefficient ring for f_1 (respectively f_2) is $\mathbb{Z}$(resp. $\mathbb{Z}[\sqrt{6}] \cong \mathbb{Z}[\alpha]/(\alpha^2 - 6)$).

In this case, $R = 6$, and it is a p-th power mod 31, the argument above implies $T_{31} - 31 - 1$ does not generate the Eisenstein ideal. While $T_{11} - 11 - 1$ does, and this claim is from explicitly computing K_c.

Next, we will verify the above claims. Let $\eta_s := T_s - (s+1)$, $R_s(y)$ is the minimal polynomial of η_s.

$$\mathbb{Z}_5[\eta_s] \cong \mathbb{Z}_5[y]/R_s(y) \hookrightarrow T^\circ \hookrightarrow \mathbb{Z}_5 \times_{\mathbb{F}_5} \mathbb{Z}_5[\sqrt{6}]$$

$$\mathbb{Z}_5 \times_{\mathbb{F}_5} \mathbb{Z}_5[\sqrt{6}] := \{(a, b) \in \mathbb{Z}_5 \times \mathbb{Z}_5[\alpha]/(\alpha^2 - 6) | a \bmod 5 \equiv b \bmod (5, \alpha - 1)\}$$

$$T_{11}f_1 = 2f_1 \quad T_{31}f_1 = 7f_1$$

$$T_{11}f_2 = (-\alpha - 2)f_2 \quad T_{31}f_2 = (-2 - \alpha)f_2$$

Thus $R_s(y)$ for η_{11} (respectively, η_{31}) is

$$R_{11}(y) = (y+10)((y+14)^2 - 6) \quad \text{resp. } R_{31}(t) = (y+25)((y+34)^2 - 6)$$

We can show $\mathbb{Z}_5[\eta_{11}]$ is isomorphic to $\mathbb{Z}_p \times_{\mathbb{F}_5} \mathbb{Z}_p[\sqrt{6}]$. Thus $T^\circ \cong \mathbb{Z}_5[y]/R_{11}(y)$, which is monogenic.

But $\mathbb{Z}_5[\eta_{31}]$ is strictly smaller than T°. The key part is that $y+10$ and $(y+14)^2-6$ generate the maximal ideal $(y, 5)$, while when $q = 31$, the ideal generated by $y + 25$ and $(y + 34)^2 - 6$ is $(y, 25)$.

REFERENCES

[1] Joël Bellaïche. Pseudodeformations. *Mathematische Zeitschrift*, 270(3):1163–1180, 2012.

[2] Joël Bellaıche and Gaëtan Chenevier. Families of galois representations and selmer groups. *Astérisque*, 324:1–314, 2009.

[3] Nicolas Billerey and Ricardo Menares. On the modularity of reducible mod l galois representations. *Mathematical Research Letters*, 23(1):15–41, 2016.

[4] Kevin Buzzard. Integral models of certain shimura curves. *Duke Mathematical Journal*, 87(3):591–612, 1997.

[5] Frank Calegari and Matthew Emerton. On the ramification of hecke algebras at eisenstein primes. *arXiv preprint math/0311368*, 2003.

[6] Gaëtan Chenevier. The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings. *Automorphic forms and Galois representations*, 1:221–285, 2014.

[7] Pete Clark. Shimura curves lecture notes 11: Integral structures, genera and class numbers.

[8] Fred Diamond. Congruence primes for cusp forms of weight k ≥ 2. *Astérisque*, (196-97):205–213, 1991.

[9] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[10] Kenneth A Ribet. On modular representations of $\mathrm{Gal}(\bar{\mathbb{q}}/\mathbb{Q})$ arising from modular forms. *Invent. math*, 100(2):431–476, 1990.

[11] Kenneth A Ribet. Raising the levels of modular representations. In *Séminaire de Théorie des Nombres, Paris 1987–88*, pages 259–271. Springer, 1990.

[12] Preston Wake and Carl Wang-Erickson. Deformation conditions for pseudorepresentations. In *Forum of Mathematics, Sigma*, volume 7. Cambridge University Press, 2019.

[13] Preston Wake and Carl Wang-Erickson. The rank of mazurs eisenstein ideal. *Duke Mathematical Journal*, 169(1):31–115, 2020.

[14] Preston Wake and Carl Wang-Erickson. The eisenstein ideal with squarefree level. *Advances in Mathematics*, 380:107543, 2021.

[15] Carl William Wang Erickson. *Moduli of Galois Representations*. PhD thesis, 2013.

[16] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

[17] Hwajong Yoo. Non-optimal levels of a reducible mod l modular representation. *Transactions of the American Mathematical Society*, 371(6):3805–3830, 2019.