THE RANK OF MAZUR'S EISENSTEIN IDEAL

PRESTON WAKE AND CARL WANG-ERICKSON

To Barry Mazur, on his 80th birthday

Abstract. We use pseudodeformation theory to study Mazur's Eisenstein ideal. Given prime numbers N and $p > 3$, we study the Eisenstein part of the p-adic Hecke algebra for $\Gamma_0(N)$. We compute the rank of this Hecke algebra (and, more generally, its Newton polygon) in terms of Massey products in Galois cohomology, answering a question of Mazur and generalizing a result of Calegari–Emerton. We also also give new proofs of Merel's result on this rank and of Mazur's results on the structure of the Hecke algebra.

Contents

Date: July 10, 2019.

1. Introduction

Let N and $p > 3$ be prime numbers. Let $\mathbb{T}$ denote the completion of the Hecke algebra with weight 2 and level $\Gamma_0(N)$ at the Eisenstein maximal ideal with residual characteristic p, and let $\mathbb{T}^0$ denote the cuspidal quotient of $\mathbb{T}$. In his influential paper [Maz77], Mazur studied $\mathbb{T}^0$ and showed that $\mathbb{T}^0 \neq 0$ if and only if $p \mid (N-1)$. In that same paper, he posed the question "Is there anything general that can be said about the Newton polygon of $\mathbb{T}^0$, or even about $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$?" [pg. 140, *loc. cit.*]. In this paper, we give a complete answer to his question, showing that this Newton polygon can be computed exactly in terms of arithmetic invariants present in Galois cohomology.

It remains an interesting avenue of research to systematically compute these new arithmetic invariants. This might be achieved by relating them to more analytic invariants coming from the theory of L-functions. We do this in the case of the lowest-order invariants, by relating our invariant to one studied by Merel [Mer96], thus giving a new proof of Merel's result. The higher-order invariants remain mysterious; however, see Remark 1.5.5 about a recent preprint of Lecouturier that extends Merel's approach. Also, for results along these lines when $p = 2$ or $p = 3$, see [CE05].

1.1. **Galois cohomology.** In order to state the main theorems, we need to establish some notation for certain Galois cohomology groups; full definitions are found in Appendix B. Let $(\mathbb{Z}/p^s\mathbb{Z})_{/\mathbb{Z}_p}$ and $(\mu_{p^s})_{/\mathbb{Z}_p}$ denote the constant and multiplicative group schemes of order p^s over $\mathbb{Z}_p$, respectively. We let

$$\begin{aligned} H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}) &= \mathrm{Ext}^1((\mathbb{Z}/p^s\mathbb{Z})_{/\mathbb{Z}_p}, (\mathbb{Z}/p^s\mathbb{Z})_{/\mathbb{Z}_p}),\\ H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(1)) &= \mathrm{Ext}^1((\mathbb{Z}/p^s\mathbb{Z})_{/\mathbb{Z}_p}, (\mu_{p^s})_{/\mathbb{Z}_p}),\\ \text{and } H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(-1)) &= \mathrm{Ext}^1((\mu_{p^s})_{/\mathbb{Z}_p}, (\mathbb{Z}/p^s\mathbb{Z})_{/\mathbb{Z}_p}),\end{aligned}$$

where the extension groups are taking place in the category of finite flat p^s-torsion group schemes over $\mathbb{Z}_p$.

For each $i = 0, 1, -1$, we have $H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(i)) \subset H^1(\mathbb{Q}_p, \mathbb{Z}/p^s\mathbb{Z}(i))$, an inclusion into local Galois cohomology. Let

$$H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{Z}/p^s\mathbb{Z}(i)) = \ker\left(H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^s\mathbb{Z}(i)) \to \frac{H^1(\mathbb{Q}_p, \mathbb{Z}/p^s\mathbb{Z}(i))}{H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(i))}\right)$$

be the resulting global cohomology groups, which are instances of Selmer groups. We will see that, if $p^s \mid (N-1)$, each of the spaces $H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{Z}/p^s\mathbb{Z}(i))$ is a free $\mathbb{Z}/p^s\mathbb{Z}$-module of rank 1 (Corollary 6.1.5). If $p^t \,||\, (N-1)$, choose generators

$$a \in H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}), \quad b \in H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}(1)),$$
$$c \in H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}(-1)).$$

Below we consider these elements as being in $H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}(i))$.

1.2. **Criterion for rank 1.** We can now state the first main theorem.

Theorem 1.2.1. *Suppose that $p \mid (N-1)$. The following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) \geq 2$

(2) The cup product $b \cup c$ vanishes in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$

(3) The cup product $a \cup c$ vanishes in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$.

Theorem 1.2.1 is the special case $n = s = 1$ of Theorem 14.0.1 below (see also the remarks following that theorem). This theorem can also be interpreted in terms of class groups. We denote the ideal class group of a number field K by $\mathrm{Cl}(K)$.

Corollary 1.2.2. *Suppose that $p \mid (N-1)$. Let $\mathbb{Q}(\zeta_N^{(p)}, \zeta_p)$ denote the degree p subextension of $\mathbb{Q}(\zeta_N, \zeta_p)/\mathbb{Q}(\zeta_p)$. Consider the following conditions:*

(1) The group $\mathrm{Cl}(\mathbb{Q}(N^{1/p}))[p]$ is cyclic.
(2) The group $\mathrm{Cl}(\mathbb{Q}(\zeta_N^{(p)}, \zeta_p))[p]_{(-1)}$ is cyclic. Here the subscript "(-1)" refers to the ω^{-1}-eigenspace for the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.
(3) The rank of the $\mathbb{Z}_p$-algebra $\mathbb{T}^0$ is one.

Then (1) implies (2), and (2) is equivalent to (3).

In this paper, we relate (1) and (2) to the cup products $b \cup c$ and $a \cup c$, respectively, in Proposition 11.1.1. Then it is a corollary of Theorem 1.2.1 that either of (1) and (2) imply (3). The remaining implication that (3) implies (2) is due to Lecouturier [Lec18b].

Remarks 1.2.3. We note the following relations with other works.

- The implication (1) ⇒ (3) of this corollary was first obtained by Calegari–Emerton, and is the main theorem of [CE05] (for $p > 3$).
- The converse implication (3) ⇒ (1) is false in general, but, for regular p, a partial converse is provided by Schaefer–Stubley [SS19, Thm. 1.1.2]. In particular, they prove that the converse is true for $p = 5$.
- The implication (3) ⇒ (2) was proven by Lecouturier [Lec18b, Thm. 1.7] using Merel's theorem (Theorem 1.5.1 below). Also using that theorem, he proves a partial converse of (1) ⇒ (3): he proves that
$$\dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathbb{Q}(N^{1/p}))[p]) = 1 + \sum_{i=1}^{p-2} r_i(\chi_0)$$
for some non-negative integers $r_i(\chi_0)$, and proves that $r_1(\chi_0) = 1$ if and only if $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$ (see the proof of [Lec18b, Thm. 1.1] on pg. 54).
- It would interesting to see if these finer results can be deduced from Sharifi's theory relating class groups of Kummer extensions to cup products and Massey products [Sha07].

1.3. Higher rank and Massey products.

Consider the following matrix of cocycles:
$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \begin{pmatrix} H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}) & H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}(1)) \\ H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}(-1)) & H^1(\mathbb{Z}[1/Np], \mathbb{Z}/p^t\mathbb{Z}) \end{pmatrix}.$$
We have the "matrix cup product" $M \cup M$ given by
$$M \cup M = \begin{pmatrix} a \cup a + b \cup c & a \cup b - b \cup a \\ c \cup a - a \cup c & c \cup b + a \cup a \end{pmatrix}.$$
Using the skew-commutativity of (scalar) cup products, we can see that, if $M \cup M = 0$, then $b \cup c = c \cup a = 0$. In fact, one can show that $M \cup M = 0$ if and only if $b \cup c = c \cup a = 0$. This suggests that, in order to generalize Theorem 1.2.1 to higher rank, one should consider "higher cup powers" of M.

We can formalize this by considering M as an element of
$$H^1(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{Z}/p^t\mathbb{Z}(1) \oplus \mathbb{Z}/p^t\mathbb{Z}))$$

and using the product on $\mathrm{End}(\mathbb{Z}/p^t\mathbb{Z}(1) \oplus \mathbb{Z}/p^t\mathbb{Z})$. Roughly, for $s \le t$, we define Massey product powers $\langle M\rangle^k \in H^2(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$ of M inductively, assuming $\langle M\rangle^{k-1} = 0$. The base case is the cup product $\langle M\rangle^2 = M \cup M$.

Theorem 1.3.1. *Let $k > 1$ and suppose that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) \ge k-1$. The following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) \ge k$

(2) $\langle M\rangle^k = 0$ *in* $H^2(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{F}_p(1) \oplus \mathbb{F}_p))$.

This theorem is morally correct, but not quite precise: we actually need to choose the extra data of a *defining system* for the Massey product $\langle M\rangle^k$ to be defined. See Theorem 14.0.1 for a precise statement, and Remark 14.0.2 for the fact that vanishing behavior does not depend on the choice of defining system. As with Theorem 1.2.1 in the case $k = 2$, for general k the matrix Massey product vanishing $\langle M\rangle^k = 0$ is equivalent to the vanishing of one of its coordinates. See Appendix A for the definition of Massey products and their coordinates, and see Proposition 13.0.1 for the equivalence.

1.4. **Newton polygons.** For this subsection, we let $e = \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ and recall that $t = v_p(N-1)$. As Mazur noted, there is an isomorphism

$$\mathbb{T}^0 \simeq \mathbb{Z}_p[\![y]\!]/(F(y))$$

where $F(y)$ is a polynomial of the form

$$F(y) = \alpha_1 + \alpha_2 y + \dots \alpha_e y^{e-1} + y^e, \ F(y) \equiv y^e \pmod p, \quad v_p(\alpha_1) = t.$$

The polynomial $F(y)$ is not determined canonically, but its Newton polygon is. Mazur's original question addressed this Newton polygon, which influences the factoring behavior of $F(y)$. This is interesting because one can read off partial (but, often, complete) information about the number of Eisenstein-congruent cusp forms and the "depth" of these congruences from the Newton polygon – see [BKK14] for a careful discussion. In particular, one knows that the normalization $\tilde{\mathbb{T}^0}$ of $\mathbb{T}^0$ is of the form

$$\tilde{\mathbb{T}^0} = \prod_{i=1}^m \mathcal{O}_{f_i},$$

where the product is over the normalized eigenforms f_i congruent to the Eisenstein series, and $\mathcal{O}_{f_i}$ is the valuation ring in the p-adic field $\mathbb{Q}_p(f_i)$ generated by the coefficients of f_i. In particular, $\mathrm{rank}_{\mathbb{Z}_p}(\mathcal{O}_{f_i}) = [\mathbb{Q}_p(f_i) : \mathbb{Q}_p]$, and m equals the number of factors of $F(y)$.

Theorem 1.4.1. *The Newton polygon of $\mathbb{T}^0$ is completely and explicitly determined by the list of integers $t = t_1 \ge t_2 \ge \cdots \ge t_e > 0$, where, for $i > 1$, t_i is the maximal integer $s \le t_{i-1}$ such that $\langle M\rangle^i = 0$ in $H^2(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$.*

For the precise result, see Theorem 14.0.1. Here is a precise consequence.

Corollary 1.4.2. *Assume that $\max(e,t) > 2$ and $\min(e,t) > 1$ and that $M \cup M$ is non-zero in $H^2(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{Z}/p^2\mathbb{Z}(1) \oplus \mathbb{Z}/p^2\mathbb{Z}))$.*

Then the vertices of the Newton polygon of $\mathbb{T}^0$ are $\{(0,t), (1,1), (e,0)\}$. In particular, $\mathbb{T}^0$ is not irreducible, and, moreover, there is a cuspidal eigenform f with coefficients in $\mathbb{Z}_p$ that is congruent modulo p to the Eisenstein series of weight 2 and level N.

Note that if $\max(e,t) \le 2$ or $\min(e,t) \le 1$, then there is only one possibility for the Newton polygon. Next, we consider an analytic interpretation of $M \cup M$.

1.5. **Relation to Merel's work.** Mazur give a different criterion for $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$ in terms of the geometry of modular curves [Maz77, Prop. II.19.2, pg. 140], and Merel [Mer96] gave a number-theoretic interpretation of this criterion.

Theorem 1.5.1 (Merel)**.** *Assume that $p \mid (N-1)$. The following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$

(2) The element of $(\mathbb{Z}/N\mathbb{Z})^\times$ given by the formula

$$\prod_{i=1}^{\frac{N-1}{2}} i^i \pmod N$$

is not a p-th power.

There is an alternate formulation, by Calegari and Venkatesh, of this theorem in terms of zeta values, which was explained to us by Venkatesh. Assume that $p^s \mid (N-1)$, and let $G = (\mathbb{Z}/N\mathbb{Z})^\times$ and $I_G = \ker(\mathbb{Z}/p^s\mathbb{Z}[G] \to \mathbb{Z}/p^s\mathbb{Z})$ be the augmentation ideal. Consider the element

$$\zeta = \sum_{i \in (\mathbb{Z}/N\mathbb{Z})^\times} B_2(\lfloor i/N \rfloor)[i] \in \mathbb{Z}/p^s\mathbb{Z}[G],$$

where $B_2(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial and where $\lfloor i/N \rfloor \in [0,1) \cap \frac{1}{N}\mathbb{Z}$ is the fractional part of i/N. This element comes from considering the function

$$\{\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p\} \to \overline{\mathbb{F}}_p, \quad \chi \mapsto L(-1,\chi)$$

where χ is a character and $L(s,\chi)$ is the Dirichlet L-function. One knows that $L(-1,\mathrm{triv}) = \frac{1-N}{12}$, which vanishes in $\mathbb{Z}/p^s\mathbb{Z}$ when $p^s \mid (N-1)$, and that $L(-1,\chi) = -\frac{1}{2}B_{2,\chi}$. We use ζ to give meaning to the "order of vanishing of $L(-1,\chi)$ at $\chi = \mathrm{triv}$."

Following Mazur and Tate [MT87], we let $\mathrm{ord}_s(\zeta) \in \mathbb{Z}$ be the maximal integer r such that $\zeta \in I_G^r$. Then Merel's theorem can be restated as follows.

Theorem 1.5.2 (Merel)**.** *Assume that $p \mid (N-1)$, and take $s = 1$ in the above discussion. Then $\mathrm{ord}_1(\zeta) \ge 1$, and the following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$

(2) $\mathrm{ord}_1(\zeta) = 1$.

We give a new proof of this theorem, combining Theorem 1.2.1 with the following proposition.

Proposition 1.5.3. *Assume that $p^s \mid (N-1)$. Then $\mathrm{ord}_s(\zeta) \ge 1$, and the following are equivalent:*

(1) $M \cup M$ is non-zero in $H^2(\mathbb{Z}[1/Np], \mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$.

(2) $\mathrm{ord}_s(\zeta) = 1$.

(3) Merel's number $\prod_{i=1}^{\frac{N-1}{2}} i^i$ is a not a p^s-th power modulo N.

Combining this result with Corollary 1.4.2, we see that if Merel's number is not a p^2-th power modulo N, then there is only one possibility for the Newton polygon of $\mathbb{T}^0$. The proof is a variant of Stickelberger theory, and is inspired by the work of Lecouturier [Lec18b] and unpublished work of Calegari and Emerton.

In Iwasawa-theoretic parlance, one could see the condition $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$ as an intermediary between the *algebraic side* (the non-vanishing of cup products) and the *analytic side* (ζ vanishes to order 1). Based on this, one might conjecture that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = \mathrm{ord}_1(\zeta)$. This is not quite correct, as the examples below show, but it is true strikingly often. In particular, we optimistically conjecture the following, for which our only evidence is a computation for $N < 10000$.

Conjecture 1.5.4. *Assume that* $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) \geq 2$. *Then the following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 2$
(2) $\mathrm{ord}_1(\zeta) = 2$.

Remark 1.5.5. After posting an earlier version of this paper on arXiv, we learned that Lecouturier was working on an approach to some of the problems considered in this paper using an "analytic side" approach. In particular, he gives another new proof of Merel's Theorem 1.5.1 and proves Conjecture 1.5.4. Lecouturier's work has since appeared as a preprint [Lec18a]. It would be interesting to study the connections between our work and his.

More generally, Theorem 1.3.1 relates $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ to an "algebraic side" (vanishing of Massey products). It is natural to ask whether there is a corresponding object on the analytic side – is there a zeta element $\tilde{\zeta}$ such that $\mathrm{ord}(\tilde{\zeta}) = \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$?

Finally, we remark that, although we give a new proof of Merel's theorem, it is intriguing to consider the possibility of, in a different context, doing the opposite. That is, Theorem 12.5.1 relates an algebraic side (vanishing of cup product) to an analytic side (order of vanishing of zeta element). In a different context where one wants to prove the same type of result (e.g. BSD conjecture, Bloch–Kato conjecture), it is interesting to consider if there is an analog of $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ that can serve as an intermediary: on one hand being related to the algebraic side via deformation theory, and on the other hand being related to the analytic side via geometry.

1.6. **Examples.** We give some explicit examples, computed using the SAGE computer algebra software. See [Maz77, Table, pg. 40] for some relevant computations of $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ (denoted e_p there).

1.6.1. *An example witnessing Corollary 1.2.2(2).* Take $p = 5$ and $N = 31$. In this case we have $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 2$. One can compute that

$$\mathrm{Cl}(\mathbb{Q}(\zeta_N^{(p)}, \zeta_p)) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

We see that the p-torsion subgroup is non-cyclic, as predicted by Corollary 1.2.2 (2).

1.6.2. *An example where the converse to Calegari–Emerton's result is false.* Take $p = 7$ and $N = 337$ and note that $7 \mid 336$. One can compute that $\mathrm{Cl}(\mathbb{Q}(N^{1/p})) \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$. One also checks Merel's number is

$$\prod_{i=1}^{\frac{N-1}{2}} i^i \equiv 227 \pmod{337}$$

which is not a 7th power modulo 337. In particular, we have $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 1$ even though $\mathrm{Cl}(\mathbb{Q}(N^{1/p}))[p]$ is not cyclic. This example was found independently by Lecouturier [Lec18b] and in unpublished work of Calegari–Emerton.

N	p	$\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$	$\mathrm{ord}(\zeta)$
181	5	3	
1321	11	3	
1381	23	3	
1571	5	3	
2621	5	3	
3001	5	6	7
3671	5	5	3
4159	7	4	5
4229	7	3	4
4931	5	3	
4957	7	3	
5381	5	3	
5651	5	4	5
5861	5	4	
6451	5	3	
6761	13	3	4
7673	7	3	4
9001	5	4	
9521	5	3	

Table 1. All examples with rank at least 3, $N < 10000$

1.6.3. *Examples of higher order vanishing.* We computed $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ and $\mathrm{ord}(\zeta)$ for every value of (N, p) with $N < 10000$. In Table 1, we give a list of all the examples with $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) > 2$. In the $\mathrm{ord}(\zeta)$ column, we only list the result if $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) \neq \mathrm{ord}(\zeta)$. Note that for all examples with $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0) = 2$, we found that $\mathrm{ord}(\zeta) = 2$, and vice versa, confirming Conjecture 1.5.4 for $N < 10000$.

1.6.4. *Examples where $\mathbb{T}^0$ is not irreducible.* We also computed the ranks of the irreducible components of $\mathbb{T}^0$ for for every value of (N, p) with $N < 10000$. (See §1.4 for the significance of these ranks.)

In Table 2, we give all examples where $\mathbb{T}^0$ is not irreducible and list the ranks of the components. For each example having either $v_p(N-1) > 2$ or $\mathrm{rank}_{\mathbb{Z}_p} > 2$, except for $(N, p) = (3001, 5)$, we computed that Merel's number is not a p^2-th power modulo N, and so the Newton polygon is given by Theorem 1.4.1. In the case $(N, p) = (3001, 5)$, Merel's number is a p^2-th power modulo N, and the Newton polygon has vertices $\{(0, 3), (1, 2), (3, 1), (6, 0)\}$.

1.7. **Statistics.** In the previous subsection, we gave examples of pairs (N, p) where $\mathbb{T}^0$ exhibits exceptional behavior. In this subsection, we analyze the statistical behavior of the examples we computed. This discussion was influenced by discussions with Ravi Ramakrishna. We will consider the situation for p fixed and N varying. To emphasize the dependence on N, in this subsection we will write $\mathbb{T}^0_N$, instead of $\mathbb{T}^0$, for the Hecke algebra associated to the pair (N, p).

N	p	$\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$	Ranks
751	5	2	(1, 1)
2351	5	2	(1, 1)
3001	5	6	(1, 2, 3)
3251	5	2	(1, 1)
3631	11	2	(1, 1)
3701	5	2	(1, 1)
4001	5	2	(1, 1)
5651	5	4	(1, 3)
6451	5	3	(1, 2)
6761	13	3	(1, 2)
7253	7	2	(1, 1)
9001	5	4	(1, 3)
9901	5	2	(1, 1)

Table 2. Ranks of irreducible components of $\mathbb{T}^0$

For fixed p, let $P(x) = \{N \mid N \text{ is prime}, \ N < x, N \equiv 1 \pmod{p}\}$. Consider the function $r(d,x) : \mathbb{N} \times \mathbb{N} \to [0,1]$ given by

$$r(d,x) = \frac{\#\{N \in P(x) \mid \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0_N) = d\}}{\#P(x)}.$$

Since we computed examples for all $N < 10000$, we let $r(d) = r(d, 10000)$, and give the values of $r(d)$ for various p and d. Before doing this, we explain a heuristic guess for $r(d,x)$ for comparison.

For $N \in P(x)$, we know that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0_N) = \dim_{\mathbb{F}_p}(\mathbb{T}^0_N/p)$, and that

$$\mathbb{T}^0_N/p \cong \mathbb{F}_p\llbracket y \rrbracket/(a_1(N)y + a_2(N)y + \dots),$$

where $a_i(N) \in \mathbb{F}_p$. In particular, $\dim_{\mathbb{F}_p}(\mathbb{T}^0_N/p) = \min\{i \mid a_i(N) \neq 0\}$. Our main Theorem 1.3.1 may be interpreted as saying that the numbers $a_i(N)$ can be extracted from values of certain Massey products. If we make the guess that the values $a_i(N)$ are distributed uniformly randomly in $\mathbb{F}_p$ as N varies, we arrive at the following heuristic guess $g(d)$ for $r(d,x)$,

$$g(d) = \left(\frac{1}{p}\right)^{d-1}\left(\frac{p-1}{p}\right).$$

Indeed, this is the probability that, for a uniformly randomly chosen sequence $b_1, b_2, \dots, b_d, \dots$ of elements of $\mathbb{F}_p$, we have $b_1 = b_2 = \dots = b_{d-1} = 0$ and $b_d \neq 0$.

In Table 2, we give our computed values of $r(d)$ for $p = 5, 7, 11, 13$, and the relevant values of $g(d)$, to three decimals of precision. In each, case, we let $n = \#P(10000)$, the size of the "sample space."

Although the sample size is too small to be convincing, the data seems to align with the heuristic guess. This leads to the question: can one determine the statistical behavior of the Massey products $\langle M \rangle^k$? Are they uniformly random as N varies?

$\mathbf{p=5}$

$n=306$		
d	$r(d)$	$g(d)$
1	0.745	0.800
2	0.216	0.160
3	0.023	0.032
4	0.010	0.006
5	0.003	0.001
6	0.003	0.000

$\mathbf{p=7}$

$n=203$		
d	$r(d)$	$g(d)$
1	0.892	0.857
2	0.089	0.122
3	0.015	0.017
4	0.005	0.002

$\mathbf{p=11}$

$n=125$		
d	$r(d)$	$g(d)$
1	0.912	0.909
2	0.080	0.083
3	0.008	0.008

$\mathbf{p=13}$

$n=99$		
d	$r(d)$	$g(d)$
1	0.929	0.923
2	0.061	0.071
3	0.010	0.005

TABLE 3. Distribution of ranks $r(d)$ versus heuristic distribution $g(d)$

1.8. **Outline of the proof.** The proofs of our main theorems follow the basic strategy of Wiles [Wil95]: Hecke algebras are related to Galois deformation rings, which are related to Galois cohomology. This is also the strategy used by Calegari–Emerton [CE05], but whereas they study "rigidified" deformations of Galois representations, we use deformation theory of pseudorepresentations, as in our previous work [WWE18].

1.8.1. *The definition of R.* Let $G_\mathbb{Q}$ be an absolute Galois group of $\mathbb{Q}$, and let $G_{\mathbb{Q},S}$ be its quotient ramified only at the places S supporting $Np\infty$. Let $\bar{D} = \psi(1 \oplus \omega)$, a $\mathbb{F}_p$-valued 2-dimensional pseudorepresentation of $G_{\mathbb{Q},S}$ – here ω is the mod p cyclotomic character, and ψ means "take the associated pseudorepresentation." This is the residual representation modulo p associated to the Eisenstein series of weight 2 and level N. We consider deformations $D : G_{\mathbb{Q},S} \to A$ of $\bar{D}$ subject to the following constraints:

(1) $\det(D) = \kappa_{\mathrm{cyc}}$
(2) $D|_{I_N} = \psi(1 \oplus 1)$, i.e. D is trivial on an inertia group I_N at N
(3) $D|_{G_p}$ is "finite-flat," where G_p is a decomposition group at p. That is, it arises from the $\overline{\mathbb{Q}}_p$-points of a finite flat group scheme over $\mathbb{Z}_p$.

Condition (1) is related to "weight 2" and condition (2) is related to "level $\Gamma_0(N)$" (note that a pseudorepresentation being trivial is analogous to a representation being unipotent).

Condition (3) is a kind of "geometricity" condition, and is the most delicate to define. There is a well-known finite-flat deformation theory of representations, due to Ramakrishna [Ram93]. The difficulty is transferring the notation of "finite-flat" from representations to pseudorepresentations. We addressed a similar difficulty in our previous work [WWE18] on the *ordinary* condition. In [WWE19], which started as a companion paper to this one, we present an axiomatic approach to go from properties of representations to properties of pseudorepresentations. This allows us to construct pseudodeformation rings satisfying any "deformation condition" (in the sense of Ramakrishna). In §2, we overview the results of [WWE19] as they apply to finite-flat pseudorepresentations.

1.8.2. *Proving $R = \mathbb{T}$.* Once we have defined R, the pseudorepresentation attached to modular forms gives a map $R \to \mathbb{T}$, and a standard argument shows that it is surjective. We use (a variant of) Wiles's numerical criterion [Wil95, Appendix] to prove that the map is an isomorphism. To verify the criterion, we have to compare the η-invariant to the size of a relative tangent space of R. The η-invariant has been computed by Mazur [Maz77] using the constant term of the Eisenstein series.

To study the relative tangent space of R, we first consider reducible deformations. These are the simplest deformations, arising as $D = \psi(\chi_1 \oplus \chi_\omega)$ where χ_1 and χ_ω are characters deforming 1 and ω, respectively. We show that the "size" of the space of reducible deformations is equal to the η-invariant. Next, we use computations in Galois cohomology to show, first, that any square-zero deformation is reducible, and, second, that the space of reducible deformations is cut out by a single equation. This allows us to conclude that the size of the relative tangent space of R is equal to the size of the space of reducible deformations, which we know is the η-invariant. The numerical criterion then lets us conclude that $R = \mathbb{T}$ and that both are complete intersections.

As a consequence of our $R = \mathbb{T}$ theorem, we give new proofs of the results on Mazur on the structure of $\mathbb{T}^0$, including the Gorenstein property, the principality of the Eisenstein ideal, and the classification of generators of the Eisenstein ideal in terms of "good primes."

1.8.3. *Studying deformations.* Having proven $R = \mathbb{T}$, we can reduce questions about $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ to questions about $\mathrm{rank}_{\mathbb{Z}_p}(R)$. As a consequence of the proof, we see that the tangent space of R is 1-dimensional – in other words, there is a unique (up to scaling) mod p first order deformation D_1 of $\bar{D}$. The question of computing $\mathrm{rank}_{\mathbb{Z}_p}(R)$ is reduced to computing to what order D_1 can be further deformed.

Using more detailed Galois cohomology computations, we show that D_1 and each of its further deformations (if they exist) arise as the pseudorepresentation associated to a representation. Then we can relate obstruction theory for representations, which is controlled by cup products (and, more generally, Massey products), to obstructions to deforming D_1. As explained in [WE18b], the formula of Theorem 1.3.1 determines the highest order unrestricted global deformation of a unique first order deformation corresponding to M. Our proofs imply that the local constraints do not contribute additional obstructions.

1.9. **Acknowledgements.** We thank Akshay Venkatesh for suggesting that we study this question. We have benefited greatly from conversations with Kevin Buzzard, Frank Calegari, Matt Emerton, Haruzo Hida, Rob Pollack, Ravi Ramakrishna, Barry Mazur, Romyar Sharifi, and Akshay Venkatesh. We thank Frank Calegari for sharing his unpublished notes and for pointing out the related preprint of Lecouturier [Lec18b]. We thank Rob Pollack for advice on computing examples. We thank Tony Feng and the anonymous referee for their careful reading of an earlier draft.

The intellectual debt owed to the work of Mazur [Maz77] and Calegari–Emerton [CE05] will be obvious to the reader.

P.W. was supported by the National Science Foundation under the Mathematical Sciences Postdoctoral Research Fellowship No. 1606255 and Grant No. DMS-1638352. C.W.E. was supported by the Simons Foundation under an AMS-Simons travel grant and by the Engineering and Physical Sciences Research Council grant EP/L025485/1.

1.10. **Notation and conventions.**

- Rings are commutative and algebras are associative but not necessarily commutative.
- A representation of an R-algebra E is the following data: a commutative R-algebra A, a finitely generated projective A-module V of constant rank, and R-algebra homomorphism $\rho : E \to \mathrm{End}_A(V)$. We sometimes write this data as ρ or as V, when the meaning is clear from context.
- A representation of a group G is a representation of $R[G]$.
- A character is a representation of constant rank 1.
- The symbol $\psi(\rho)$ denotes the pseudorepresentation associated to a representation ρ.
- If G is a profinite group, we let $G^{\text{pro-}p}$ be the maximal pro-p quotient. If G is finite and abelian, we write $G^{p\text{-part}}$ instead of $G^{\text{pro-}p}$.
- We use the symbol "$\smile$" for the multiplication in the differential graded algebra of group cochains valued in an algebra, and "$\cup$" for the cup product of cohomology classes. We sometimes use $[-]$ to denote the cohomology class of a cocycle. If x, y are cocycles, then $[x \smile y] = [x] \cup [y]$, and we often denote this cohomology class by $x \cup y$.
- Throughout the paper, we abbreviate the cohomology groups $H^i(\mathbb{Z}[1/Np], -)$ (resp. $H^i(\mathbb{Q}_\ell, -)$) to $H^i(-)$ (resp. $H^i_\ell(-)$). For further Galois cohomology notation, including the definition of the groups $H^i_{(c)}(-)$, $H^i_{\mathrm{flat}}(-)$, $H^i_{\mathrm{flat},p}(-)$, and $H^i_{(N)}(-)$, see Appendix B.
- For an integer $i \geq 0$ and a ring A, we abbreviate $A[\epsilon]/(\epsilon^{i+1})$ to $A[\epsilon_i]$.
- We write $v_p(x) \in \mathbb{Z} \cup \{\infty\}$ for the p-adic valuation for $x \in \mathbb{Q}_p$.
- We write $\kappa_{\mathrm{cyc}} : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ or $\mathbb{Z}_p(1)$ for the p-adic cyclotomic character. When it cannot cause confusion, we abuse notation and write κ_{cyc} for $\kappa_{\mathrm{cyc}} \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^s\mathbb{Z}$ or $\mathbb{Z}/p^s\mathbb{Z}(1)$.

1.10.1. *Notation for Galois groups.* Recall that N and p are prime numbers. We fix algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}}_\ell$, and embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, for $\ell = p, N$. This determines decomposition subgroups $G_N \subset G_\mathbb{Q}$ and $G_p \subset G_\mathbb{Q}$. We also have the quotient $G_{\mathbb{Q},S}$ of $G_\mathbb{Q}$ discussed above, the Galois group of the maximal extension of $\mathbb{Q}$ ramified only at the set of places S that support $Np\infty$. The cohomology groups above are the cohomology of continuous cochains on these Galois groups.

Let $I_N \subset G_N$ and $I_p \subset G_p$ denote the inertia subgroups. We let $I_N^{\text{pro-}p}$ denote the maximal pro-p quotient of I_N. We let $I_N^{\text{non-}p}$ denote the kernel of the map $I_N \to I_N^{\text{pro-}p}$.

As is well-known, there is a non-canonical isomorphism $I_N^{\text{pro-}p} \simeq \mathbb{Z}_p$. We fix, once and for all, a topological generator $\bar{\gamma}$ of $I_N^{\text{pro-}p}$, and an element $\gamma \in I_N$ mapping to $\bar{\gamma}$.

Part 1. Pseudo-modularity and the Eisenstein Hecke algebra

We first recall the results of [WWE19] and construct a pseudodeformation ring with the "finite-flat" property at p. We recall some results of Mazur on modular curves and the Eisenstein Hecke algebra $\mathbb{T}$, and construct a map $R \to \mathbb{T}$. We compute Galois cohomology groups to control the structure of R, and use the numerical criterion to prove $R \xrightarrow{\sim} \mathbb{T}$.

2. Finite-flat pseudodeformations

This section is a summary of [WWE19]. In that paper, we develop the deformation theory of pseudorepresentations with a prescribed property. Presently, we only consider the case that is needed in this paper, where the property is the "flat" condition of Ramakrishna [Ram93]. (To avoid confusion with flat modules over a ring, we refer to this condition as "finite-flat" in this paper.)

We only give a brief summary of the parts of the theory that are needed in this paper. We assume that the reader has some familiarity with pseudorepresentations and generalized matrix algebras. For a more detailed treatment, see [WWE19]. Other references for pseudorepresentations and generalized matrix algebras include [BC09, §1], [Che14], and [WE18a, §§2-3]. Proofs or references for all of the results in this section are given in [WWE19]; we only give specific references here to the results that are new to [WWE19].

In this section, we will work in a slightly more general setup than in the rest of the paper. Let $\mathbb{F}$ be a finite field of characteristic p. Let $\chi_1, \chi_2 : G_{\mathbb{Q}} \to \mathbb{F}^\times$ be characters such that $\chi_1|_{G_p} \neq \chi_2|_{G_p}$ and such that $\chi_i|_{G_p}$ are finite-flat representations in the sense defined below. Let $\bar{D} : G_{\mathbb{Q}} \to \mathbb{F}$ be $\psi(\chi_1 \oplus \chi_2)$, the associated pseudorepresentation. Let S be a finite set of places of $\mathbb{Q}$ including p, the infinite places and any primes at which χ_i are ramified, and let $G_{\mathbb{Q},S}$ be the Galois group of the maximal unramified-outside-S extension of $\mathbb{Q}$.

2.1. **Finite-flat representations.** We have $G_p \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let $\mathrm{Mod}^{\mathrm{tor}}_{\mathbb{Z}_p[G_p]}$ denote the category of $\mathbb{Z}_p[G_p]$-modules of finite cardinality. Let $\mathrm{ffgs}_{\mathbb{Z}_p}$ denote the category of finite flat group schemes over $\mathbb{Z}_p$ of p-power rank. Via the generic fiber functor $\mathrm{ffgs}_{\mathbb{Z}_p} \to \mathrm{Mod}^{\mathrm{tor}}_{\mathbb{Z}_p[G_p]}$ given by $\mathcal{G} \mapsto \mathcal{G}(\overline{\mathbb{Q}}_p)$, which is known to be fully faithful, we can consider $\mathrm{ffgs}_{\mathbb{Z}_p}$ as a subcategory of $\mathrm{Mod}^{\mathrm{tor}}_{\mathbb{Z}_p[G_p]}$. We call objects in the essential image of this functor *finite-flat* G_p-modules.

Let $\mathcal{G}_1, \mathcal{G}_2 \in \mathrm{ffgs}_{\mathbb{Z}_p}$ and let $V_i = \mathcal{G}_i(\overline{\mathbb{Q}}_p)$ be the associated finite-flat G_p-modules. The generic fiber functor defines a homomorphism

$$\mathrm{Ext}^1_{\mathrm{ffgs}_{\mathbb{Z}_p}}(\mathcal{G}_2, \mathcal{G}_1) \to \mathrm{Ext}^1_{G_p}(V_2, V_1).$$

We define $\mathrm{Ext}^1_{G_p,\mathrm{flat}}(V_2, V_1)$ to be the image of this homomorphism. If $\tilde{V}_i$ are $G_{\mathbb{Q},S}$-modules such that $\tilde{V}_i|_{G_p} = V_i$, then we define

$$\mathrm{Ext}^1_{G_{\mathbb{Q},S},\mathrm{flat}}(\tilde{V}_2, \tilde{V}_1) = \ker\left(\mathrm{Ext}^1_{G_{\mathbb{Q},S}}(\tilde{V}_2, \tilde{V}_1) \to \frac{\mathrm{Ext}^1_{G_p}(V_2, V_1)}{\mathrm{Ext}^1_{G_p,\mathrm{flat}}(V_2, V_1)}\right).$$

Let $(A, \mathfrak{m}_A)$ be a Noetherian local $\mathbb{Z}_p$-algebra, and let M be a finitely generated A-module with a commuting action of G_p. Then $M/\mathfrak{m}_A^i M \in \mathrm{Mod}^{\mathrm{tor}}_{\mathbb{Z}_p[G_p]}$ for all $i > 0$, and we say M is *finite-flat* if $M/\mathfrak{m}_A^i M$ is a finite-flat G_p-module for all $i > 0$.

2.2. **Generalized matrix algebras.** Let $(A, \mathfrak{m}_A)$ be a Noetherian local $W(\mathbb{F})$-algebra with residue field $\mathbb{F}$.

See [WWE19, §2.1] for the definition of a pseudorepresentation. Let E be an associative A-algebra. As noted in *loc. cit.*, we may and do think of a pseudorepresentation of dimension d on E, written $D : E \to A$ (or, if $E = A[G]$ for a group G, as $D : G \to A$), as a rule that assigns to an element $x \in E$ a degree d polynomial $\chi_D(x)(t) \in A[t]$. These $\chi_D(x)$ satisfy many conditions as if they were characteristic polynomials of a representation $E \to M_d(A)$. The *Cayley–Hamilton property* of a pseudorepresentation (defined in [Che14, §1.17]) implies that $\chi_D(x)(x) = 0$ in E for all $x \in E$.

A *generalized matrix A-algebra* or *A-GMA* (of type $(1,1)$) is an associative A-algebra E equipped with an isomorphism

$$\Phi_{\mathcal{E}} : E \xrightarrow{\sim} \begin{pmatrix} A & B \\ C & A \end{pmatrix}. \tag{2.2.1}$$

This means an isomorphism of A-modules $E \xrightarrow{\sim} A \oplus B \oplus C \oplus A$ for some A-modules B and C, such that the multiplication of E is given by 2×2-matrix multiplication for some A-linear map $B \otimes_A C \to A$. We refer to the isomorphism (2.2.1) as the *matrix coordinates* of E. A morphism of GMAs $(E, \Phi_{\mathcal{E}}) \to (E', \Phi_{\mathcal{E}'})$ is an algebra morphism $\phi : E \to E'$ preserving idempotents; that is, it satisfies $\phi\Phi_{\mathcal{E}}^{-1}(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)) = \Phi_{\mathcal{E}'}^{-1}(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ and $\phi\Phi_{\mathcal{E}}^{-1}(\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \Phi_{\mathcal{E}'}^{-1}(\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right))$. Forming the trace and determinant as functions $E \to A$ in the usual way from these coordinates, we have a Cayley–Hamilton pseudorepresentation denoted $D_{\mathcal{E}} : E \to A$.

An *GMA representation with residual pseudorepresentation* $\bar{D}$ is a homomorphism $\rho : G_{\mathbb{Q}} \to E^{\times}$ such that, in matrix coordinates, ρ is given as

$$\rho : \sigma \mapsto \begin{pmatrix} \rho_{11}(\sigma) & \rho_{12}(\sigma) \\ \rho_{21}(\sigma) & \rho_{22}(\sigma) \end{pmatrix}$$

with $\rho_{ii}(\sigma) \equiv \chi_i(\sigma) \pmod{\mathfrak{m}_A}$. There is an associated pseudorepresentation $\psi_{\mathrm{GMA}}(\rho) : G_{\mathbb{Q}} \to A$ given by $\mathrm{tr}(\psi_{\mathrm{GMA}}(\rho)) = \rho_{11} + \rho_{22}$ and $\det(\psi_{\mathrm{GMA}}(\rho)) = \rho_{11}\rho_{22} - \rho_{12}\rho_{21}$.

A *Cayley–Hamilton representation* of $G_{\mathbb{Q},S}$ over A with residual pseudorepresentation $\bar{D}$ is a triple $(E, \rho : G_{\mathbb{Q},S} \to E^{\times}, D : E \to A)$ where E is an associative A-algebra that is finitely generated as an A-module, D is a Cayley–Hamilton pseudorepresentation, and ρ is a homomorphism such that $D' = D \circ \rho$ is a pseudorepresentation deforming $\bar{D}$.

Proposition 2.2.2.

1. *The functor sending a complete Noetherian local $W(\mathbb{F})$-algebra A with residue field $\mathbb{F}$ to the set of deformations $D : G_{\mathbb{Q},S} \to A$ of $\bar{D}$ is represented by a ring $R_{\bar{D}}$ and universal pseudodeformation $D^u : G_{\mathbb{Q},S} \to R_{\bar{D}}$.*
2. *There is an $R_{\bar{D}}$-GMA representation $\rho^u : G_{\mathbb{Q}} \to E_{\bar{D}}^{\times}$ with residual representation $\bar{D}$ such that $(E_{\bar{D}}, \rho_u, D_{\mathcal{E}})$ is the universal Cayley–Hamilton representation with residual pseudorepresentation $\bar{D}$, and $D^u = D_{\mathcal{E}} \circ \rho^u$.*

Remark 2.2.3. Whenever $\bar{D}$ is multiplicity-free (i.e. $\chi_1 \neq \chi_2$, which we have assumed), any Cayley–Hamilton representation $(E, \rho : G_{\mathbb{Q},S} \to E^{\times}, D : E \to A)$ with residual pseudorepresentation $\bar{D}$ admits an orthogonal lift (e_1, e_2) of the idempotents $(1,0), (0,1)$ over the kernel of $\chi_1 \oplus \chi_2 : E \to \mathbb{F}_p \times \mathbb{F}_p$. See e.g. [WWE18, Lem. 5.6.8]. We always order the idempotents so that e_1 lifts χ_1 and e_2 lifts χ_2. It is these idempotents that specify the coordinate decomposition: for example $B = e_1Ee_2$ and $\rho_{i,j}(\gamma) = e_j\rho(\gamma)e_i$ for $i, j \in \{1, 2\}$. We also refer to a choice of these idempotents by the corresponding choice of matrix coordinates.

2.3. **Finite-flat pseudorepresentations.** We retain the notation of the previous subsection.

Definition 2.3.1. Let (E, ρ, D) be a Cayley–Hamilton representation of $G_{\mathbb{Q},S}$ over A with residual pseudorepresentation $\bar{D}$. Then E is a finitely generated A-module, and it has an action of G_p via $\rho|_{G_p}$ and the left action of E on itself by multiplication. We say that (E, ρ, D) is *finite-flat* if $E/\mathfrak{m}_A^i E$ is a finite-flat G_p-module for all $i \geq 1$.

We say a pseudorepresentation $D' : G_{\mathbb{Q},S} \to A$ is *finite-flat* if $D' = D \circ \rho$ for some finite-flat Cayley–Hamilton representation (E, ρ, D).

We show that there is a universal finite-flat Cayley–Hamilton representation of $G_{\mathbb{Q},S}$ with residual pseudorepresentation $\bar{D}$.

Theorem 2.3.2 ([WWE19, §2.5])**.**

(1) There is a universal finite-flat Cayley–Hamilton representation $(E_{\bar{D},\mathrm{flat}}, \rho_{\mathrm{flat}} : G_{\mathbb{Q},S} \to E^{\times}_{\bar{D},\mathrm{flat}}, D_{\mathrm{flat}} : E_{\bar{D},\mathrm{flat}} \to R_{\bar{D},\mathrm{flat}})$ of $G_{\mathbb{Q},S}$ over $R_{\bar{D},\mathrm{flat}}$ with residual pseudorepresentation $\bar{D}$. The algebra $E_{\bar{D},\mathrm{flat}}$ is a quotient of $E_{\bar{D}}$.

(2) The algebra $R_{\bar{D},\mathrm{flat}}$ is the quotient of $R_{\bar{D}}$ such that, for any deformation $D : G_{\mathbb{Q},S} \to A$ of $\bar{D}$, the corresponding map $R_{\bar{D}} \to A$ factors through $R_{\bar{D},\mathrm{flat}}$ if and only if D is a finite-flat pseudorepresentation.

We let

$$E_{\bar{D},\mathrm{flat}} = \begin{pmatrix} R_{\bar{D},\mathrm{flat}} & B_{\bar{D},\mathrm{flat}} \\ C_{\bar{D},\mathrm{flat}} & R_{\bar{D},\mathrm{flat}} \end{pmatrix}$$

represent a choice of matrix coordinates of $E_{\bar{D},\mathrm{flat}}$ induced by those of $E_{\bar{D}}$.

Finite-flat Cayley–Hamilton representations can arise from endomorphism algebras of modules. The following theorem shows that the notion of finite-flat Cayley–Hamilton representation behaves as expected in this case.

Theorem 2.3.3 ([WWE19, §2.6])**.** *Let $(E, \rho, D : E \to A)$ be a Cayley–Hamilton representation of G_p, and let M be a faithful E-module that is finitely generated as an A-module. Consider M as a $A[G_p]$-module via the map $\rho : A[G_p] \to E$. Then M is a finite-flat G_p-module if and only if (E, ρ, D) is a finite-flat Cayley–Hamilton representation.*

The following example illustrates the utility of this theorem. It is exactly the situation coming from the Jacobian $J_0(N)$, as encountered by Mazur in [Maz77, §§II.7-8], which we apply in §3.3.

Example 2.3.4. Let $\mathcal{G} = \{\mathcal{G}_i\}$ be a p-divisible group with good reduction outside S. Then the Tate module $V = T_p\mathcal{G} = \varprojlim \mathcal{G}_i(\overline{\mathbb{Q}})$ is a finitely generated, free $\mathbb{Z}_p$-module with an action of $G_{\mathbb{Q},S}$. In particular, V is a finite-flat representation.

Now assume that V has a commuting action of A, where A is a finite flat $\mathbb{Z}_p$-algebra, and that there is an isomorphism of A-modules

$$V \cong X_1 \oplus X_2$$

where X_i are A-modules satisfying $\mathrm{End}_A(X_i) = A$ (but X_i may not be free as A-modules). This decomposition induces a decomposition

$$\mathrm{End}_A(V) \cong \begin{pmatrix} A & \mathrm{Hom}_A(X_1, X_2) \\ \mathrm{Hom}_A(X_2, X_1) & A \end{pmatrix}$$

giving $\mathrm{End}_A(V)$ the structure of an A-GMA, where the idempotents arise from projection onto each summand. Let $\rho_V : G_{\mathbb{Q},S} \to \mathrm{Aut}_A(V)$ be the action map, and let $D_V : \mathrm{End}_A(V) \to A$ be the GMA-pseudorepresentation. Then the theorem implies that $(\mathrm{End}_A(V), \rho_V, D_V)$ is a finite-flat Cayley–Hamilton representation.

2.4. **Reducibility.** We say that a pseudorepresentation D is *reducible* if $D = \psi(\nu_1 \oplus \nu_2)$ for characters ν_i.

Proposition 2.4.1. *Let $D : G_{\mathbb{Q},S} \to R$ be a pseudorepresentation deforming $\bar{D}$.*

(1) There is a quotient R^{red} of R characterized as follows. For any homomorphism $\phi : R \to R'$, the map ϕ factors through R^{red} if and only if the composite pseudorepresentation $D' = \phi \circ D : G_{\mathbb{Q},S} \to R'$ is reducible.

(2) Let

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

be a choice of matrix coordinates of $E = E_{\bar{D}} \otimes_{R_{\bar{D}}} R$. Then the image of the R-linear map $B \otimes_A C \to R$ equals the kernel of $R \to R^{\mathrm{red}}$.

We call the ideal $\ker(R \to R^{\mathrm{red}})$ the *reducibility ideal* of D. For the finite-flat pseudodeformation ring, we can describe the reducible quotient.

Proposition 2.4.2 ([WWE19, §4.3])**.** *For $i = 1, 2$, let R_i denote Ramakrishna's finite-flat deformation ring of the character χ_i, and let $\nu_i : G_{\mathbb{Q},S} \to R_i^{\times}$ denote the universal character. Then there is an isomorphism $R^{\mathrm{red}}_{\bar{D},\mathrm{flat}} \xrightarrow{\sim} R_1 \hat{\otimes}_{W(\mathbb{F})} R_2$ identifying $\psi(\nu_1 \oplus \nu_2)$ as the universal reducible finite-flat deformation of $\bar{D}$.*

2.5. **Reducible GMAs and extensions.** For this section, we fix a surjective homomorphism $R^{\mathrm{red}}_{\bar{D},\mathrm{flat}} \twoheadrightarrow R'$. By Proposition 2.4.2, this homomorphism determines finite-flat characters $\nu'_i : G_{\mathbb{Q},S} \to R'^{\times}$ deforming χ_i for $i = 1, 2$. We can determine the structure of $B_{\bar{D},\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R'$ and $C_{\bar{D},\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R'$ in terms of Galois cohomology.

Proposition 2.5.1 ([WWE19, §4.3])**.** *Let M be a finitely generated R'-module. Then there are canonical isomorphisms*

$$\mathrm{Hom}_{R'}(B_{\bar{D},\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R', M) \xrightarrow{\sim} \mathrm{Ext}^1_{G_{\mathbb{Q},S},\mathrm{flat}}(\nu'_2, \nu'_1 \otimes_{R'} M)$$

and

$$\mathrm{Hom}_{R'}(C_{\bar{D},\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R', M) \xrightarrow{\sim} \mathrm{Ext}^1_{G_{\mathbb{Q},S},\mathrm{flat}}(\nu'_1, \nu'_2 \otimes_{R'} M).$$

3. The modular pseudorepresentation

In this section, we recall some results of Mazur [Maz77] on modular curves and Hecke algebras.

3.1. Modular curves, modular forms, and Hecke algebras.

The statements given here are all well-known. We review them here to fix notations. Our reference is the paper of Ohta [Oht14].

3.1.1. *Modular curves.* Let $Y_0(N)_{/\mathbb{Z}_p}$ be the $\mathbb{Z}_p$-scheme representing the functor taking a $\mathbb{Z}_p$-scheme S to the set of pairs (E, C), where E is an elliptic curve over S and $C \subset E[N]$ is a finite-flat subgroup scheme of rank N. Let $X_0(N)_{/\mathbb{Z}_p}$ be the usual compactification of $Y_0(N)_{/\mathbb{Z}_p}$, and let cusps denote the complement of $Y_0(N)_{/\mathbb{Z}_p}$ in $X_0(N)_{/\mathbb{Z}_p}$, considered as an effective Cartier divisor on $X_0(N)_{/\mathbb{Z}_p}$. Finally, let

$$X_0(N) = X_0(N)_{/\mathbb{Z}_p} \otimes \mathbb{Q}_p.$$

3.1.2. *Modular forms.* The map $X_0(N)_{/\mathbb{Z}_p} \to \mathrm{Spec}(\mathbb{Z}_p)$ is known to be LCI, and we let Ω be the sheaf of regular differentials. Let

$$S_2(N;\mathbb{Z}_p) = H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega), \quad M_2(N;\mathbb{Z}_p) = H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$$

There is an element $E \in M_2(N;\mathbb{Z}_p)$ with q-expansion

$$E = \frac{N-1}{24} + \sum_{n=1}^{\infty} \left(\sum_{0<d|n,\ N\nmid d} d \right) q^n. \tag{3.1.1}$$

3.1.3. *Hecke algebras.* Let $\mathbb{T}'$ and $\mathbb{T}'^0$ be the subalgebras of

$$\mathrm{End}_{\mathbb{Z}_p}(M_2(N;\mathbb{Z}_p)), \quad \mathrm{End}_{\mathbb{Z}_p}(S_2(N;\mathbb{Z}_p)),$$

respectively, generated by all Hecke operators T_n with $(N,n) = 1$. These are commutative $\mathbb{Z}_p$-algebras.

Let $I' = \mathrm{Ann}_{\mathbb{T}'}(E)$, and let $\mathbb{T}$ be the completion of $\mathbb{T}'$ at the maximal ideal (I', p), and let $\mathbb{T}^0 = \mathbb{T}'^0 \otimes_{\mathbb{T}'} \mathbb{T}$. Let $I = I'\mathbb{T}$ and let I^0 be the image of I in $\mathbb{T}^0$. Let $U_p \in \mathbb{T}$ be the unique unit root of the polynomial

$$X^2 - T_p X + p = 0,$$

which exists by Hensel's lemma. Since $T_p - (p+1) \in I$, we see that $U_p - 1 \in I$. For a $\mathbb{T}'$-module M, let $M_{\mathrm{Eis}} = M \otimes_{\mathbb{T}'} \mathbb{T}$.

There are perfect pairings of free $\mathbb{Z}_p$-modules

$$M_2(N;\mathbb{Z}_p)_{\mathrm{Eis}} \times \mathbb{T} \to \mathbb{Z}_p, \quad S_2(N;\mathbb{Z}_p)_{\mathrm{Eis}} \times \mathbb{T}^0 \to \mathbb{Z}_p$$

given by $(f,t) \mapsto a_1(t \cdot f)$, where $a_1(-)$ refers to the coefficient of q in the q-expansion. In particular, $M_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}$ (resp. $S_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}$) is a dualizing (and hence faithful) $\mathbb{T}$-module (resp. $\mathbb{T}^0$-module). The map $\mathbb{T} \to \mathbb{Z}_p$ so induced by E is a surjective ring homomorphism with kernel I. We refer to this as the augmentation map for $\mathbb{T}$.

3.2. **Congruence number.** We recall the following theorem of Mazur, and related results.

Theorem 3.2.1 (Mazur)**.** *There is an isomorphism $\mathbb{T}^0/I^0 \simeq \mathbb{Z}_p/(N-1)\mathbb{Z}_p$.*

This is [Maz77, Prop. II.9.7, pg. 96]. We give a slightly different proof of this theorem using ideas of Ohta and Emerton [Eme99]. This should help clarify the proof of [WWE18, Prop. 3.2.5], which uses the same idea but is needlessly complicated; we thank the referee for pointing this out.

We recall that if $A \to C$ and $B \to C$ are commutative ring homomorphisms, the pullback ring $A \times_C B$ is defined and the underlying set is the same as the pullback in the category of sets.

Lemma 3.2.2. *The composition of the augmentation map $\mathbb{T} \to \mathbb{Z}_p$ with the quotient map $\mathbb{Z}_p \to \mathbb{Z}_p/(N-1)\mathbb{Z}_p$ factors through $\mathbb{T}^0$ and induces an isomorphism*

$$\mathbb{T} \simeq \mathbb{T}^0 \times_{\mathbb{Z}_p/(N-1)\mathbb{Z}_p} \mathbb{Z}_p.$$

In particular, $\ker(\mathbb{T} \to \mathbb{T}^0) = \mathrm{Ann}_{\mathbb{T}}(I)$.

Proof. By [Oht14, Lem. 3.2.3] there is an exact sequence

$$(*) \qquad 0 \to S_2(N,\mathbb{Z}_p)_{\mathrm{Eis}} \to M_2(N,\mathbb{Z}_p)_{\mathrm{Eis}} \xrightarrow{a_0} \mathbb{Z}_p \to 0,$$

where the first map is the inclusion and where $a_0(f)$ denotes the constant term in the q-expansion of f. By duality, we see that $\ker(\mathbb{T} \to \mathbb{T}^0) = \mathrm{Ann}_{\mathbb{T}}(S_2(N,\mathbb{Z}_p)_{\mathrm{Eis}})$ is the free $\mathbb{Z}_p$-module generated by the element $T_0 \in \mathbb{T}$ that satisfies $a_1(T_0 f) = a_0(f)$ for all $f \in M_2(N,\mathbb{Z}_p)_{\mathrm{Eis}}$.

Since $a_0(E) = \frac{N-1}{24}$ maps to 0 in $\mathbb{Z}_p/(N-1)\mathbb{Z}_p$, we see that the composite $\mathbb{T} \to \mathbb{Z}_p/(N-1)\mathbb{Z}_p$ factors through $\mathbb{T}^0$. We have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & T_0\mathbb{Z}_p \arrow[r] \arrow[d] & \mathbb{T} \arrow[r] \arrow[d] & \mathbb{T}^0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (N-1)\mathbb{Z}_p \arrow[r] & \mathbb{Z}_p \arrow[r] & \mathbb{Z}_p/(N-1)\mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

where the center vertical map is the augmentation $t \mapsto a_1(tE)$. Since $a_1(T_0 E) = \frac{N-1}{24}$, the leftmost vertical map is surjective and hence an isomorphism since the domain and codomain are both free of rank 1. An easy diagram chase then shows that the map $\mathbb{T} \to \mathbb{T}^0 \times_{\mathbb{Z}_p/(N-1)\mathbb{Z}_p} \mathbb{Z}_p$ is an isomorphism. The fact that $\ker(\mathbb{T} \to \mathbb{T}^0) = \mathrm{Ann}_{\mathbb{T}}(I)$ follows formally from this and the fact that I^0 is a faithful $\mathbb{T}^0$-module. □

3.3. **Trace and determinant.** Let $J_0(N)$ be the Jacobian of $X_0(N)$. The p-adic Tate module $\mathrm{Ta}_p(J_0(N)(\overline{\mathbb{Q}}))$ is a $\mathbb{T}'^0[G_{\mathbb{Q},S}]$-module. Let $\mathcal{T} = \mathrm{Ta}_p(J_0(N)(\overline{\mathbb{Q}}))_{\mathrm{Eis}}$.

Lemma 3.3.1. *The $\mathbb{T}^0[1/p]$-module $\mathcal{T}[1/p]$ is free of rank 2.*

Proof. See [Maz77, Lem. II.7.7, pg. 92], for example. □

Let $\rho_{\mathcal{T}[1/p]} : G_{\mathbb{Q},S} \to \mathrm{Aut}_{\mathbb{T}^0[1/p]}(\mathcal{T}[1/p]) \simeq \mathrm{GL}_2(\mathbb{T}^0[1/p])$ be the corresponding Galois representation.

Lemma 3.3.2. *The representation $\rho_{\mathcal{T}[1/p]}|_{I_N}$ is unipotent.*

Proof. This is proven in the course of the proof of [Maz77, Prop. II.14.1, pg. 113], and we recall the argument here. By the theorem of Mazur and Rapoport [Maz77, Thm. A.1, pg. 173] (attributed there to Deligne), $J_0(N)$ has semi-stable reduction at N. By the critère Galoisien de réduction semi-stable [GRR72, Exposé IX, Prop. 3.5, pg. 350], this implies the result. □

Lemma 3.3.3. *Let $\ell \nmid Np$ be a prime, and let $\mathrm{Fr}_\ell \in G_{\mathbb{Q},S}$ be a Frobenius element. Then the characteristic polynomial $\mathrm{char}(\rho_{\mathcal{T}[1/p]})(\mathrm{Fr}_\ell) \in \mathbb{T}^0[1/p][X]$ is given by*

$$\mathrm{char}(\rho_{\mathcal{T}[1/p]})(\mathrm{Fr}_\ell) = X^2 - T_\ell X + \ell.$$

In particular, we have $\det(\rho_{\mathcal{T}[1/p]}) = \kappa_{\mathrm{cyc}}$ and, for any $\sigma \in G_{\mathbb{Q},S}$, $\mathrm{tr}(\rho_{\mathcal{T}[1/p]}(\sigma)) \in \mathbb{T}^0$.

Proof. The formula for the characteristic polynomial follow from the Eichler–Shimura relation (see e.g. [Maz77, §II.6, pg. 89]). The remaining parts follow by Chebotaryov density. □

From this lemma, we see that there is a pseudorepresentation $D_{\mathcal{T}} : G_{\mathbb{Q},S} \to \mathbb{T}^0$ determined by $\det(D_{\mathcal{T}}) = \kappa_{\mathrm{cyc}}$ and $\mathrm{tr}(D_{\mathcal{T}})(\mathrm{Fr}_\ell) = T_\ell$ for all $\ell \nmid Np$, and that $D_{\mathcal{T}} \otimes_{\mathbb{T}^0} \mathbb{T}^0[1/p] = \psi(\rho_{\mathcal{T}[1/p]})$.

Proposition 3.3.4. *Assume that $p \mid (N-1)$. There is a short exact sequence of $\mathbb{T}^0[G_p]$-modules*

$$0 \to \mathcal{T}^{mul} \to \mathcal{T} \to \mathcal{T}^{ét} \to 0$$

where $\mathcal{T}^{mul}$ is free of rank 1 as a $\mathbb{T}^0$-module and $\mathcal{T}^{ét}$ is a dualizing $\mathbb{T}^0$-module. The G_p-action on $\mathcal{T}^{ét}$ is unramified, and the sequence splits as $\mathbb{T}^0$-modules.

Proof. The sequence is constructed in [Maz77, §II.8, pg. 93], using the connected-étale exact sequence for the Néron model of $J_0(N)$. It follows by construction that the G_p-action on $\mathcal{T}^{\text{ét}}$ is unramified. As remarked in *loc. cit.*, the sequence is self-$\mathbb{Z}_p$-dual by Cartier duality. Then [Maz77, Cor. II.14.11, pg. 120] implies that $\mathcal{T}^{mul}$ is a free $\mathbb{T}^0$-module of rank 1. By duality, $\mathcal{T}^{\text{ét}}$ is a dualizing $\mathbb{T}^0$-module.

Finally, to see that the sequence splits as $\mathbb{T}^0$-modules, we note that (either by Lemma 3.3.3 or by construction) G_p acts on $\mathcal{T}^{mul}$ by the character κ_{cyc}. Let $\tau \in I_p$ be an element such that $\kappa_{\mathrm{cyc}}(\tau) = -1$. Then we see that $\mathcal{T} = (\tau - 1)\mathcal{T} \oplus (\tau + 1)\mathcal{T}$ as $\mathbb{T}^0$-modules. □

Remark 3.3.5. Note that this proposition does not use the the fact that $\mathbb{T}^0$ is a Gorenstein ring. See, for example, [Oht14, Thm. 3.5.10], where a similar statement is proven in a more general setting where the Hecke algebra need not be Gorenstein.

Lemma 3.3.6. *Let $\mathrm{Fr}_p \in G_p$ be a Frobenius element. Then Fr_p acts on $\mathcal{T}^{ét}$ by the scalar $U_p \in \mathbb{T}^0$.*

Proof. By the previous proposition, we know that Fr_p acts on $\mathcal{T}^{\text{ét}}$ by a well-defined unit in $\mathbb{T}^0$. To determine the unit, we extend scalars to $\mathbb{T}^0[1/p]$. We know that $\mathcal{T}^{\text{ét}} = \mathcal{T}_{I_p}$ (the inertia coinvariants), so it suffices to determine the action of Fr_p on $(\rho_{\mathcal{T}[1/p]})_{I_p}$. The fact that Fr_p acts on $(\rho_{\mathcal{T}[1/p]})_{I_p}$ as U_p follows from local-global compatibility for modular forms [Sch90, Thm. 1.2.4(ii)]. □

We let $E_{\mathcal{T}} = \mathrm{End}_{\mathbb{T}^0}(\mathcal{T})$, and let $\rho_{\mathcal{T}} : G_{\mathbb{Q},S} \to E_{\mathcal{T}}^\times$.

Corollary 3.3.7. *The $\mathbb{T}^0$-algebra $E_{\mathcal{T}}$ admits a $\mathbb{T}^0$-GMA structure $\mathcal{E}_{\mathcal{T}}$ such that $D_{\mathcal{T}} = D_{\mathcal{E}_{\mathcal{T}}} \circ \rho_{\mathcal{T}}$, and $D_{\mathcal{T}}$ is a finite-flat pseudorepresentation.*

Proof. Following Example 2.3.4, a choice of $\mathbb{T}^0$-module isomorphism $\mathcal{T} \xrightarrow{\sim} \mathbb{T}^0 \oplus (\mathbb{T}^0)^\vee$ arising from Proposition 3.3.4 produces a GMA structure $\mathcal{E}_{\mathcal{T}}$ on $E_{\mathcal{T}}$. As in that example, it follows from Theorem 2.3.3 that $(E_{\mathcal{T}}, \rho_{\mathcal{T}}, D_{\mathcal{E}_{\mathcal{T}}})$ is a finite-flat Cayley–Hamilton representation (since $\mathcal{T}|_p$ is a finite-flat $\mathbb{Z}_p[G_p]$-module). It is easy to check that $D_{\mathcal{T}} = D_{\mathcal{E}_{\mathcal{T}}} \circ \rho_{\mathcal{T}}$, so $D_{\mathcal{T}}$ is a finite-flat pseudorepresentation by Definition 2.3.1. □

4. The pseudodeformation ring

Let $\bar{D} = \psi(\omega \oplus 1)$. In this section, we construct R, the universal pseudodeformation ring for $\bar{D}$ satisfying the following additional conditions:

(1) D is finite-flat at p
(2) $D|_{I_N} = \psi(1 \oplus 1)$
(3) $\det(D) = \kappa_{\mathrm{cyc}}$

Let $D_{\mathrm{Eis}} : G_{\mathbb{Q},S} \to \mathbb{Z}_p$ be the reducible pseudorepresentation $\psi(\mathbb{Z}_p(1) \oplus \mathbb{Z}_p)$. We will show that D_{Eis} and the pseudorepresentation $D_{\mathcal{T}} : G_{\mathbb{Q},S} \to \mathbb{T}^0$ both satisfy conditions (1)-(3), and we use this fact to produce a surjection $R \twoheadrightarrow \mathbb{T}$.

4.1. **Construction of R.** Let $R_{\bar{D},\mathrm{flat}}$ be the universal finite-flat pseudodeformation ring, and let $E_{\bar{D},\mathrm{flat}} = E_{\bar{D}} \otimes_{R_{\bar{D}}} R_{\bar{D},\mathrm{flat}}$ be the universal finite-flat Cayley–Hamilton algebra (see Theorem 2.3.2).

Let $I_{\det} \subset R_{\bar{D},\mathrm{flat}}$ denote the ideal generated by the set

$$\{\det(D)(\sigma) - \kappa_{\mathrm{cyc}}(\sigma) \mid \sigma \in G_{\mathbb{Q},S}\}$$

and let $I_{ss} \subset R_{\bar{D},\mathrm{flat}}$ denote the ideal generated by the set

$$\{\mathrm{tr}(D)(\tau) - 2 \mid \tau \in I_N\}.$$

(The notation I_{ss} comes from "semi-stable at N" (cf. Lemma 3.3.2).) Define

$$R = R_{\bar{D},\mathrm{flat}}/(I_{\det} + I_{ss}).$$

Proposition 4.1.1. *The ring R pro-represents the functor sending an Artinian local $\mathbb{Z}_p$-algebra A with residue field $\mathbb{F}_p$ to the set of pseudorepresentations $D : G_{\mathbb{Q},S} \to A$ satisfying*

(1) $D \otimes_A \mathbb{F}_p = \bar{D}$
(2) *D is finite-flat at p*
(3) $D|_{I_N} = \psi(1 \oplus 1)$
(4) $\det(D) = \kappa_{\mathrm{cyc}}$.

Proof. We already know by Theorem 2.3.2 that $R_{\bar{D},\mathrm{flat}}$ is the deformation ring for pseudorepresentations satisfying (1) and (2). We have to show that, for any A as in the proposition, and any homomorphism $\phi : R_{\bar{D},\mathrm{flat}} \to A$, the corresponding pseudorepresentation D satisfies (3) and (4) if and only if ϕ factors through R.

We note that, since κ_{cyc} is unramified at N, a pseudorepresentation D satisfying (4) will also satisfy (3) if and only if $\mathrm{tr}(D)|_{I_N} = 2$. We see that D satisfies (4) if and only if $\ker(\phi) \supset I_{\det}$, and so D satisfies (3) and (4) if and only if $\ker(\phi) \supset I_{\det} + I_{ss}$. This completes the proof. □

Let $E = E_{\bar{D},\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R$ and let $\rho = \rho_{\mathrm{flat}} \otimes_{R_{\bar{D},\mathrm{flat}}} R$. We fix an arbitrary choice of matrix coordinates on E, so that we can write ρ as

$$\rho : G_{\mathbb{Q},S} \to E^\times, \quad \sigma \mapsto \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}. \tag{4.1.2}$$

Let $D = \psi(\rho) : G_{\mathbb{Q},S} \to R$ be the universal pseudorepresentation for the functor of Proposition 4.1.1.

4.2. **The map $R \to \mathbb{T}$.** First we construct a homomorphism $R \to \mathbb{T}^0$.

Lemma 4.2.1. *The pseudorepresentation $D_{\mathcal{T}} : G_{\mathbb{Q},S} \to \mathbb{T}^0$ induces a homomorphism $R \to \mathbb{T}^0$. Moreover, we have $\mathrm{tr}(D_{\mathcal{T}})(\mathrm{Fr}_\ell) = T_\ell$ and*

$$\mathrm{tr}(D_{\mathcal{T}})(\mathrm{Fr}_\ell) \equiv 1 + \ell \pmod{I^0}$$

for any $\ell \nmid Np$.

Proof. To show the first statement, we have to check that $D_{\mathcal{T}}$ satisfies conditions (1)-(4) of Proposition 4.1.1. Note that the second statement implies (1), so we prove the second statement first. The fact that $\mathrm{tr}(D_{\mathcal{T}})(\mathrm{Fr}_\ell) = T_\ell$ follows from Lemma 3.3.3. It follows from the formula (3.1.1) that $T_\ell - (1+\ell) \in I^0$, and so the second statement follows.

Condition (2) follows from Corollary 3.3.7, condition (3) follows from Lemma 3.3.2, and condition (4) follows from Lemma 3.3.3. □

Lemma 4.2.2. *The pseudorepresentation $D_{\mathrm{Eis}} = \psi(\mathbb{Z}_p \oplus \mathbb{Z}_p(1))$ induces a homomorphism $R \to \mathbb{Z}_p$. Moreover, we have $\mathrm{tr}(D_{\mathrm{Eis}})(\mathrm{Fr}_\ell) = 1 + \ell$ for all $\ell \nmid Np$.*

Proof. The second statement is clear, and implies that D_{Eis} satisfies condition (1) of Proposition 4.1.1. Conditions (3) and (4) are clear, and condition (2) follows from Theorem 2.3.3 and the fact that $\mathbb{Z}_p \oplus \mathbb{Z}_p(1)$ is the Tate module of the generic fiber of the p-divisible group

$$(\mathbb{Q}_p/\mathbb{Z}_p \oplus \mu_{p^\infty})_{/\mathbb{Z}_p}. \qquad \square$$

This map $R \to \mathbb{Z}_p$ gives R the structure of an augmented $\mathbb{Z}_p$-algebra. We let $J^{\min} = \ker(R \to \mathbb{Z}_p)$, and refer to $J^{\min}$ as the augmentation ideal of R. We see that $J^{\min} \subset R$ is the ideal generated by the reducibility ideal J of R (since D_{Eis} is obviously reducible) along with lifts over $R \twoheadrightarrow R/J$ of the image under $R^{\mathrm{red}}_{\bar{D},\mathrm{flat}} \twoheadrightarrow R/J$ of the set

$$\{\nu_1(\sigma) - \kappa_{\mathrm{cyc}}(\sigma), \nu_2(\sigma) - 1 \mid \sigma \in G_{\mathbb{Q},S}\} \subset R^{\mathrm{red}}_{\bar{D},\mathrm{flat}}, \tag{4.2.3}$$

where ν_1, ν_2 (the universal finite-flat deformations of ω and $\mathbb{F}_p$, respectively) arise from Proposition 2.4.2.

Using the two maps $R \to \mathbb{T}^0$ and $R \to \mathbb{Z}_p$, we can produce a map $R \to \mathbb{T}$, as in [WWE18, Cor. 7.1.3].

Proposition 4.2.4. *There is a surjective homomorphism $R \twoheadrightarrow \mathbb{T}$ of augmented $\mathbb{Z}_p$-algebras. Moreover $\mathbb{T}$ and $\mathbb{T}^0$ are generated as $\mathbb{Z}_p$-algebras by the Hecke operators T_n with $(n, Np) = 1$. In particular, $\mathbb{T}$ and $\mathbb{T}^0$ are reduced.*

Proof. We already have $R \to \mathbb{T}^0$ via $D_{\mathcal{T}}$, and $R \to \mathbb{Z}_p$ via D_{Eis}. By Lemma 3.2.2, to construct a homomorphism $R \to \mathbb{T}$, is suffices to show that the composite maps

$$R \to \mathbb{T}^0 \to \mathbb{T}^0/I^0 \to \mathbb{Z}_p/(N-1)\mathbb{Z}_p$$

and

$$R \to \mathbb{Z}_p \to \mathbb{Z}_p/(N-1)\mathbb{Z}_p$$

coincide. Equivalently, we have to show that

$$D_{\mathcal{T}} \otimes_{\mathbb{T}^0} \mathbb{Z}_p/(N-1)\mathbb{Z}_p = D_{\mathrm{Eis}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/(N-1)\mathbb{Z}_p$$

as pseudorepresentations $G_{\mathbb{Q},S} \to \mathbb{Z}_p/(N-1)\mathbb{Z}_p$. However, we have already shown in Lemma 4.2.1 and Lemma 4.2.2 that these two pseudorepresentations agree at Fr_ℓ for all $\ell \nmid Np$, hence they agree by continuity. This defines a map $R \to \mathbb{T}$. By construction, we see that the composite map

$$R \to \mathbb{T} \to \mathbb{T}/I \cong \mathbb{Z}_p$$

coincides with the augmentation $R \to \mathbb{Z}_p$, and so $R \to \mathbb{T}$ is a map of augmented $\mathbb{Z}_p$-algebras.

Under the isomorphism $\mathbb{T} \cong \mathbb{T}^0 \times_{\mathbb{Z}_p/(N-1)\mathbb{Z}_p} \mathbb{Z}_p$, we can think of an element of $\mathbb{T}$ as a pair $(t, a) \in \mathbb{T}^0 \times \mathbb{Z}_p$. Then the pseudorepresentation $D_\mathbb{T} : G_{\mathbb{Q},S} \to \mathbb{T}$ corresponding to the map $R \to \mathbb{T}$ constructed above is given by $D_\mathbb{T}(\sigma) = (D_\mathcal{T}(\sigma), D_{\mathrm{Eis}}(\sigma))$. In this notation, for any prime $\ell \nmid Np$, the element $T_\ell \in \mathbb{T}$ for $\ell \nmid N$ corresponds to the pair $(T_\ell, \ell + 1)$, and we see that $\mathrm{tr}(D_\mathbb{T})(\mathrm{Fr}_\ell) = (T_\ell, \ell + 1)$ for any prime $\ell \nmid Np$. By Chebotaryov density, R is generated as a $\mathbb{Z}_p$-algebra by the elements $\mathrm{tr}(D_\mathbb{T})(\mathrm{Fr}_\ell)$ for $\ell \nmid Np$; indeed, by [Che14, Cor. 2.39], $R_{\bar{D}}$ is generated by the values of the characteristic polynomial on Frobenius elements, and its quotient R has determinants valued in $\mathbb{Z}_p$. Then we see that the image of $R \to \mathbb{T}$ is generated, as a $\mathbb{Z}_p$-algebra, by the elements T_ℓ.

It remains to show that the image of $R \to \mathbb{T}$ contains T_p. Since $U_p^2 - T_pU_p + p = 0$, we see that the it is enough to show that the image contains U_p and U_p^{-1}. In the notation above, the element $U_p \in \mathbb{T}$ corresponds to the pair $(U_p, 1) \in \mathbb{T}^0 \times \mathbb{Z}_p$. Choose a Frobenius element $\mathrm{Fr}_p \in G_p$ and let $z = \kappa_{\mathrm{cyc}}(\mathrm{Fr}_p)$. By Proposition 3.3.4 and Lemma 3.3.6, we have

$$\rho_\mathcal{T}(\mathrm{Fr}_p) = \begin{pmatrix} zU_p^{-1} & * \\ 0 & U_p \end{pmatrix}.$$

Choose an element $\sigma \in I_p$ such that $\omega(\sigma) \neq 1$, and let $x = \kappa_{\mathrm{cyc}}(\sigma)$. Then we have

$$\rho_\mathcal{T}(\mathrm{Fr}_p\sigma) = \begin{pmatrix} xzU_p^{-1} & * \\ 0 & U_p \end{pmatrix}.$$

We see that $\mathrm{tr}(D_\mathcal{T})(\mathrm{Fr}_p\sigma) - x\mathrm{tr}(D_\mathcal{T})(\mathrm{Fr}_p) = (1-x)U_p$. We also see easily that $\mathrm{tr}(D_{\mathrm{Eis}})(\mathrm{Fr}_p\sigma) - x\mathrm{tr}(D_{\mathrm{Eis}})(\mathrm{Fr}_p) = 1 - x$. Hence we see that $((1-x)U_p, 1-x) \in \mathbb{T}$ is in the image of $R \to \mathbb{T}$. Since

$$x \equiv \omega(\sigma) \not\equiv 1 \pmod{p}$$

we see that $1 - x \in \mathbb{Z}_p^\times$, and so we have that U_p is in the image of $R \to \mathbb{T}$. A similar argument shows that U_p^{-1} is also in the image, completing the proof.

The operators T_n for $(n, N) = 1$ are well-known to act semi-simply on the modules of modular forms and cusp forms. Since $\mathbb{T}$ and $\mathbb{T}^0$ are generated by these operators, we see that they are reduced. □

Remark 4.2.5. In [CE05], the authors present a proof of a related result. However, the proof of [CE05, Lem. 3.16] contains a subtle error about the difference between T_p and U_p. To correct that error, one would have to argue as above. Similarly, the proof of [CE05, Prop. 3.18] is flawed and must be corrected as in the proof of Corollary 9.1.2 below.

5. Computation of R^{red}

Let R^{red} denote the quotient of R representing the pseudodeformations of $\bar{D}$ that satisfy the conditions of Proposition 4.1.1 and are also reducible. Such a quotient exists in light of the theory of reducibility for pseudorepresentations reviewed in §2.4. In this section we give a presentation of R^{red}.

5.1. **Presentation of R^{red}.** For this section, we let $R' = R_{\bar{D},\mathrm{flat}}/I_{\det}$ (recall the notation of §4.1).

Lemma 5.1.1. *We have* $R'^{\mathrm{red}} \simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}]$.

Proof. By Proposition 2.4.2, we have $R^{\mathrm{red}}_{\bar{D},\mathrm{flat}} = R_{1,\mathrm{flat}} \hat{\otimes}_{\mathbb{Z}_p} R_{\omega,\mathrm{flat}}$, where $R_{1,\mathrm{flat}}$ and $R_{\omega,\mathrm{flat}}$ are the finite-flat deformation rings of 1 and ω, respectively, and the universal deformation is $\psi(\nu_\omega \oplus \nu_1)$, where ν_ω and ν_1 are the universal deformation characters. Using the well-known description of the universal deformation ring of a character, and the fact that finite-flat deformations of 1 (resp. ω) are trivial (resp. trivial after a twist by $\kappa_{\mathrm{cyc}}^{-1}$) on I_p, we have

$$R_{\omega,\mathrm{flat}} \cong R_{1,\mathrm{flat}} \cong \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}]$$

and that $\nu_\omega = \kappa_{\mathrm{cyc}}\langle - \rangle$ and $\nu_1 = \langle - \rangle$, where $\langle - \rangle$ is the character given by

$$G_{\mathbb{Q},S} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}} \subset \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}]^\times$$

(the quotient map, followed by map sending group element to the corresponding group-like element).

By the definition of I_{det} we see that

$$R'^{\mathrm{red}} \cong \frac{R_{\omega,\mathrm{flat}} \hat{\otimes}_{\mathbb{Z}_p} R_{1,\mathrm{flat}}}{(\nu_\omega(\sigma) \otimes \nu_1(\sigma) - \kappa_{\mathrm{cyc}}(\sigma) : \sigma \in G_{\mathbb{Q},S})} \simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}]. \qquad \square$$

We fix this isomorphism so that the universal pseudodeformation $D'^{\mathrm{red}} : G_{\mathbb{Q},S} \to R'^{\mathrm{red}}$ can be written as $D'^{\mathrm{red}} = \psi(\langle - \rangle \kappa_{\mathrm{cyc}} \oplus \langle - \rangle^{-1})$.

Recall from §1.10.1 that we have chosen an element $\gamma \in I_N$ such that γ topologically generates $I_N^{\text{pro-}p}$. Let $g \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$ be the image of γ in the quotient. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$ is the Galois group of a finite p-extension of $\mathbb{Q}$ that is totally ramified at N, we see that g generates $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$.

Proposition 5.1.2. *There is a presentation*

$$R^{\mathrm{red}} \simeq \mathbb{Z}_p[X]/(X^2, (N-1)X)$$

where the universal deformation $D^{\mathrm{red}} : G_{\mathbb{Q},S} \to \mathbb{Z}_p[X]/(X^2, (N-1)X)$ *is given by* $D^{\mathrm{red}} = \psi(\langle \bar{-} \rangle \kappa_{\mathrm{cyc}} \oplus \langle \bar{-} \rangle^{-1})$. *Here* $\langle \bar{-} \rangle$ *is the character* $\sigma \mapsto (1+X)^{m_\sigma}$, *where* $m_\sigma \in \mathbb{Z}/p^n\mathbb{Z}$ *is defined so that* σ *maps to* g^{m_σ} *in* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$.

Proof. Let $t = v_p(N-1)$, so that $\#\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}} = p^t$. There are isomorphisms

$$\mathbb{Z}_p[x]/(x^{p^t} - 1) \xrightarrow{\sim} \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}] \cong R'^{\mathrm{red}},$$

where the first sends x to the group-like element g. We use these isomorphisms as identifications in the rest of the proof.

The quotient R^{red} of R'^{red} corresponds to the condition that D'^{red} satisfy $D'^{\mathrm{red}}|_{I_N} = \psi(1 \oplus 1)$. We know that $\det(D'^{\mathrm{red}}) = \kappa_{\mathrm{cyc}}$, which satisfies $\kappa_{\mathrm{cyc}}|_{I_N} = 1$. Then the only condition is that $\mathrm{tr}(D'^{\mathrm{red}})|_{I_N} = 2$. We know that $\mathrm{tr}(D'^{\mathrm{red}})|_{I_N} = \langle - \rangle + \langle - \rangle^{-1}$. For $\sigma \in I_N$, we have

$$\langle \sigma \rangle + \langle \sigma \rangle^{-1} = \langle g^{m_\sigma} \rangle + \langle g^{m_\sigma} \rangle^{-1} = x^{m_\sigma} + x^{-m_\sigma}.$$

Since $m_\gamma = 1$ by our choice of g, we see that the condition $\mathrm{tr}(D'^{\mathrm{red}})|_{I_N} = 2$ is equivalent to the conditions

$$x^m + x^{-m} = 2$$

for all $m = 1, \dots, p^n$. This proves that R^{red} is the quotient of $\mathbb{Z}_p[x]$ by the ideal $\mathfrak{a}$ generated by the set

$$\{x^{p^n} - 1\} \cup \{x^m + x^{-m} - 2 \ : \ m = 1, \dots, p^n\}.$$

It only remains to simplify the presentation. Notice that x is a unit, and that

$$x^m(x^m + x^{-m} - 2) = x^{2m} - 2x^m + 1 = (x^m - 1)^2.$$

Since this is a multiple of $(x-1)^2$, we see that $\mathfrak{a}$ is generated by $\{x^{p^t} - 1, (x-1)^2\}$.

Letting $X = x - 1$, notice that

$$x^{p^t} - 1 = (X+1)^{p^t} - 1 \equiv p^t X \pmod{X^2}.$$

We see that $\mathfrak{a}$ is generated by $\{p^t X, X^2\}$, so $\mathfrak{a} = ((N-1)X, X^2)$. □

5.2. **Structure of $J^{\min}/J$.** Recall that $J^{\min} = \ker(R \to \mathbb{Z}_p)$, where $R \to \mathbb{Z}_p$ is the augmentation defined in Lemma 4.2.2. Let $J \subset R$ be the reducibility ideal, so that $R^{\mathrm{red}} = R/J$. Note that $J \subset J^{\min}$.

Corollary 5.2.1. *We have $J^{\min}/J \simeq \mathbb{Z}_p/(N-1)\mathbb{Z}_p$.*

Proof. By Proposition 5.1.2, we have a presentation

$$R^{\mathrm{red}} \cong \mathbb{Z}_p[X]/(X^2, (N-1)X),$$

which we will use as an identification. Then the image of $J^{\min}$ in R^{red} is XR^{red} and we have

$$J^{\min}/J \cong XR^{\mathrm{red}} \simeq R^{\mathrm{red}}/(\mathrm{Ann}_{R^{\mathrm{red}}}(X)) = R^{\mathrm{red}}/(X, N-1) \cong \mathbb{Z}_p/(N-1)\mathbb{Z}_p. \quad \square$$

Proposition 5.2.2. *Let $Y = 1 - d_\gamma$ (here $\gamma \in I_N$ is as in §1.10.1 and $d_\gamma \in R$ is as in (4.1.2)). Then $Y \in J^{\min}$ and the image of Y in $J^{\min}/J$ is a generator of that cyclic group. Moreover, $Y^2 = -b_\gamma c_\gamma \in J$ and there is an inclusion $(J^{\min})^2 \subset J$.*

Proof. The fact that $Y \in J^{\min}$ is immediate from the description of $J^{\min}$ in (4.2.3). By Proposition 5.1.2, we have a presentation

$$R^{\mathrm{red}} = \mathbb{Z}_p[X]/(X^2, (N-1)X).$$

From the proof of that proposition, we see that Y maps to X, which generates $J^{\min}/J$.

To see that $Y^2 = -b_\gamma c_\gamma$, note that, in R, we have the equation $a_\gamma + d_\gamma = 2$ and so $a_\gamma = 1 + Y$. Then we have

$$\rho(\gamma) = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} = \begin{pmatrix} 1+Y & b_\gamma \\ c_\gamma & 1-Y \end{pmatrix}.$$

The equation $\det(\rho)(\gamma) = \kappa_{\mathrm{cyc}}(\gamma) = 1$ forces

$$(1-Y)(1+Y) - b_\gamma c_\gamma = 1.$$

This implies $Y^2 = -b_\gamma c_\gamma$.

Finally, the fact that the image of Y in $J^{\min}/J$ is a generator implies that $J^{\min} = YR + J$. Since $Y^2 \in J$, we see that $(J^{\min})^2 \subset J$. □

We will use Galois cohomology to see that J is a principal ideal and that $b_\gamma c_\gamma$ is a generator (Theorem 6.1.2). This will imply that $J = (J^{\min})^2$ and that $J^{\min} = YR$ (Corollary 7.1.2).

6. Calculations in Galois cohomology

In this section, our goal is to determine the structure of $E/J^{\min}E$. We have already determined this structure in terms of Galois cohomology. This was done in Proposition 2.4.1, which we will recall shortly. Therefore, we must calculate various Galois cohomology groups. Namely, certain *global finite-flat cohomology* groups $H^\bullet_{\mathrm{flat}}(-)$ must be determined. This cohomology theory and other cohomological tools are defined in Appendix B. The reader will find it necessary to review Appendix B before following this section's arguments in detail. We use the notation and definitions introduced in Appendix B freely here.

The calculations of H^1_{flat} are crucial to our proof of $R = \mathbb{T}$ and to our computation of ranks. The calculations of H^2_{flat}, on the other hand, are not logically necessary for the proofs. We include them as a guide to understand this work in the general context of deformation theory: the groups H^2_{flat} are the "correct H^2 groups," in that they are the right place to compute the obstructions to lifting a global finite-flat deformation. However, we prove an injectivity result in Proposition 6.1.6 that implies that it is sufficient to calculate these obstructions in the usual global cohomology H^2. Therefore, we can limit the amount of new technology we have to introduce, at the cost of, in places, doing ad hoc work to make a deformation finite-flat. See Remark 10.6.3 for more on this.

6.1. Main results.

Recall the notations of §4.1. Let

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

be the GMA form of E as in (4.1.2), i.e. B and C are R-modules, and the multiplication in E induces an R-module homomorphism $B \otimes_R C \to R$. We know from Proposition 2.4.1 that the image of this homomorphism is the reducibility ideal J.

Let $B^{\min} = B/J^{\min}B$ and $C^{\min} = C/J^{\min}C$. Since $I_{\det} + I_{ss} \subset J^{\min}$, the natural maps $B_{\bar{D},\mathrm{flat}}/J^{\min}B_{\bar{D},\mathrm{flat}} \to B^{\min}$ and $C_{\bar{D},\mathrm{flat}}/J^{\min}C_{\bar{D},\mathrm{flat}} \to C^{\min}$ are isomorphisms. By Proposition 2.5.1, for any $\mathbb{Z}_p$-module M we have

$$\mathrm{Hom}(B^{\min}, M) \cong \mathrm{Ext}^1_{G_{\mathbb{Q},S},\mathrm{flat}}(\mathbb{Z}_p, M(1)),\ \mathrm{Hom}(C^{\min}, M) \cong \mathrm{Ext}^1_{G_{\mathbb{Q},S},\mathrm{flat}}(\mathbb{Z}_p(1), M).$$

In the notation of Appendix B, this is

$$\mathrm{Hom}(B^{\min}, M) = H^1_{\mathrm{flat}}(M(1)), \quad \mathrm{Hom}(C^{\min}, M) = H^1_{\mathrm{flat}}(M(-1)). \tag{6.1.1}$$

In this section we compute these cohomology groups to reach our goal, the following characterizations of $B^{\min}$ and $C^{\min}$.

Theorem 6.1.2. *Let $\gamma \in I_N$ be the element chosen in §1.10.1. Recall the notation of (4.1.2).*

(1) There are isomorphisms

$$B^{\min} \simeq \mathbb{Z}_p, \quad C^{\min} \simeq \mathbb{Z}_p/(N-1)\mathbb{Z}_p.$$

(2) The R-modules B and C are cyclic and $b_\gamma \in B$ and $c_\gamma \in C$ are generators.

(3) The ideal $J \subset R$ is principal and $b_\gamma c_\gamma \in J$ is a generator.

Remark 6.1.3. While the $\mathbb{Z}_p$-module structures of $B^{\min}$ and $C^{\min}$ suffice for the sequel, the interested reader may find it useful to know that there are canonical isomorphisms

$$B^{\min} \cong H^2_{\mathrm{flat}^\perp}(\mathbb{Z}_p), \qquad C^{\min} \cong H^2_{(N)}(\mathbb{Z}_p(2)),$$

where "flat$^\perp$" refers to the dual condition to the flat condition on the cohomology of $\mathbb{Z}_p(1)$, in the standard sense (see e.g. [GV18, App. B]), but will not be used in our computations. The latter isomorphism is proved in Proposition 6.3.3.

Remark 6.1.4. We note that (2) implies (3) and (2) follows easily from (the proof of) (1). For the proof of $R = \mathbb{T}$ (Corollary 7.1.3 below), it is only necessary to prove part (3). To prove (3) directly, one could work exclusively with cohomology with $\mathbb{F}_p$-coefficients, rather than the more cumbersome $\mathbb{Z}/p^r\mathbb{Z}$-coefficients we use below. However, the methods are essentially the same, and the payoff of using $\mathbb{Z}/p^r\mathbb{Z}$-coefficients is the result (1), which is crucial to our study of the finer structure of R and $\mathbb{T}$ (see §7.2 and §10.2).

The following "dual" result to Theorem 6.1.2 specifies the cohomology groups generated by the cohomology classes a, b, c of the introduction.

Corollary 6.1.5. *Let s be an integer such that $p^s \mid (N-1)$. Then $H^1_{\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(i)) \simeq \mathbb{Z}/p^s\mathbb{Z}$ for $i = -1, 0, 1$. Moreover,*

1. *$H^1_{\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z})$ is generated by the class of the cocycle*
$$G_{\mathbb{Q},S} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z},$$
for any choice of surjective homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$.
2. *$H^1_{\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(1))$ is generated by the Kummer class of N.*
3. *$H^1_{\mathrm{flat}}(\mathbb{Z}/p^s\mathbb{Z}(-1))$ is equal to $H^1_{(p)}(\mathbb{Z}/p^s\mathbb{Z}(-1))$.*

Along the way, we also prove the following result, which will be used in our study of obstruction theory for R.

Proposition 6.1.6. *For any $r > 0$ and $i \in \{0, 1, -1\}$, the natural map*
$$H^1(\mathbb{Z}/p^r\mathbb{Z}(i)) \longrightarrow H^1_p(\mathbb{Z}/p^r\mathbb{Z}(i))/H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}(i))$$
is surjective. Equivalently, the natural map
$$H^2_{\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}(i)) \longrightarrow H^2(\mathbb{Z}/p^r\mathbb{Z}(i))$$
is injective.

Remark 6.1.7. The equivalence is clear from the cone construction of H^i_{flat}. See further comments in Remark 10.6.3.

6.2. **Calculation of certain $H^1_{p,\mathrm{flat}}(V)$.** For this section and §6.3, we drop the convention that N is prime and $p \mid (N-1)$, allowing it to be a squarefree integer N such that $p \nmid N$.

In order to begin computing, we first need to compute some extension groups in the category of finite flat group schemes. Here $\mathbb{Q}_p^{\mathrm{nr}}$ denotes the maximal unramified subextension of $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$.

Lemma 6.2.1. *For any $r > 0$, we have:*

1. *$H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}(-1)) = 0$.*
2. *Under the identification $H^1_p(\mathbb{Z}/p^r\mathbb{Z}(1)) \cong \mathbb{Q}_p^\times \otimes \mathbb{Z}/p^r\mathbb{Z}$ of Kummer theory, $H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}(1))$ corresponds to the subgroup $\mathbb{Z}_p^\times \otimes \mathbb{Z}/p^r\mathbb{Z}$.*
3. *$H^1_{p,\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}) = \ker(H^1_p(\mathbb{Z}/p^r\mathbb{Z}) \to H^1(\mathbb{Q}_p^{\mathrm{nr}}, \mathbb{Z}/p^r\mathbb{Z}))$.*

Proof. (1) Indeed, this group corresponds to extensions
$$0 \longrightarrow \mathbb{Z}/p^r\mathbb{Z} \longrightarrow ? \longrightarrow \mu_{p^r} \longrightarrow 0$$
in the category of group schemes of exponent p^r over $\mathbb{Z}_p$, and no such non-trivial extensions exist (see e.g. the proof of [Con97, Thm. 1.8]).

(2) This can be proven by Kummer theory as in [CE05, Lem. 2.6], working over the $fppf$-site of $\mathrm{Spec}(\mathbb{Z}_p)$ (of which the category of finite flat group schemes is an exact subcategory).

(3) Indeed, this group corresponds to extensions
$$0 \longrightarrow \mathbb{Z}/p^r\mathbb{Z} \longrightarrow ? \longrightarrow \mathbb{Z}/p^r\mathbb{Z} \longrightarrow 0$$
in the category of group schemes of exponent p^r over $\mathbb{Z}_p$. In such an exact sequence, all the terms must be étale, and the category of finite étale groups schemes over $\mathbb{Z}_p$ is equivalent to the category of finite abelian groups with $\pi_1^{\text{ét}}(\mathbb{Z}_p) \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p)$-action. □

6.3. **Cohomology computations.** In this section, we state the results of our computations, continuing to allow N to be squarefree where $p \nmid N$. In many cases, when the computation is particularly straightforward and standard, we leave the proofs to the reader.

Proposition 6.3.1. *We have $H^0_{\text{flat}}(\mathbb{Z}_p) = \mathbb{Z}_p$, $H^i_{\text{flat}}(\mathbb{Z}_p) = 0$ for $i \notin \{0,2\}$, and*
$$H^2_{\text{flat}}(\mathbb{Z}_p) \simeq \prod_{\ell \mid N \text{prime}} \mathbb{Z}_p/(\ell-1)\mathbb{Z}_p.$$

Proof. Exercise in class field theory. □

Proposition 6.3.2. *There are isomorphisms*
$$H^1_{\text{flat}}(\mathbb{Z}/p^r\mathbb{Z}(1)) \cong \mathbb{Z}[1/N]^\times \otimes \mathbb{Z}/p^r\mathbb{Z} \simeq \mathbb{Z}/p^r\mathbb{Z}^{\#\{\ell \mid N \text{prime}\}}$$
and
$$H^2_{\text{flat}}(\mathbb{Z}/p^r\mathbb{Z}(1)) \cong \ker\left(\bigoplus_{\ell \mid N\text{prime}} \mathbb{Z}/p^r\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Z}/p^r\mathbb{Z}\right) \simeq \mathbb{Z}/p^r\mathbb{Z}^{\#\{\ell \mid N\text{prime}\}-1}.$$

Proof. Exercise in Kummer theory. □

By Lemma 6.2.1, we have $H^1_{p,\text{flat}}(\mathbb{Z}/p^r\mathbb{Z}(-1)) = 0$. Using the notation of §B.3, we have $H^1_{\text{flat}}(\mathbb{Z}/p^r\mathbb{Z}(-1)) = H^1_{(p)}(\mathbb{Z}/p^r\mathbb{Z}(-1))$.

Proposition 6.3.3. *We have*
$$C^{\min} \cong H^2_{(N)}(\mathbb{Z}_p(2)) \cong H^1_N(\mathbb{Z}_p(2)) \simeq \bigoplus_{\ell \mid N\text{prime}} \mathbb{Z}_p/(\ell^2-1)\mathbb{Z}_p.$$

Proposition 6.3.3 will follow from the duality Theorem B.3.2, together with the following two lemmas.

Lemma 6.3.4. *Let ℓ be a prime different from p. Then $H^0(\mathbb{Q}_\ell, \mathbb{Z}_p(2)) = 0$,*
$$H^1(\mathbb{Q}_\ell, \mathbb{Z}_p(2)) \simeq \mathbb{Z}_p/(\ell^2-1)\mathbb{Z}_p, \quad \textit{and} \quad H^2(\mathbb{Q}_\ell, \mathbb{Z}_p(2)) \simeq \mathbb{Z}_p/(\ell-1)\mathbb{Z}_p.$$
Also, $H^2(\mathbb{Q}_p, \mathbb{Z}_p(2)) = 0$.

Proof. This follows from [NSW08, Thm. 7.3.10, pg. 400]. □

Lemma 6.3.5. *For any $p > 3$, there are isomorphisms*

$$H^2(\mathbb{Z}_p(2)) \cong \bigoplus_{\ell \mid N \text{prime}} \mathbb{F}_\ell^\times \otimes \mathbb{Z}_p \simeq \bigoplus_{\ell \mid N \text{prime}} \mathbb{Z}_p/(\ell-1)\mathbb{Z}_p.$$

For $i \neq 2$, $H^i(\mathbb{Z}_p(2)) = 0$.

Proof. This follows from combining the excision spectral sequence associated to $\mathrm{Spec}(\mathbb{Z}[1/Np]) \subset \mathrm{Spec}(\mathbb{Z}[1/p])$ (cf. [Sou79, Prop. 1 of III.1.3, pg. 18]) with the fact that $H^i(\mathbb{Z}[1/p], \mathbb{Z}_p(2)) = 0$ for $i > 0$ if $p > 3$. (The Chern class map

$$c_{i,n} : K_{2n-i}(\mathbb{Z}) \otimes \mathbb{Z}_p \longrightarrow H^i(\mathbb{Z}[1/p], \mathbb{Z}_p(n))$$

is known to be isomorphism, where $K_3(\mathbb{Z}) \simeq \mathbb{Z}/48\mathbb{Z}$ and $K_2(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.) □

Proof of Proposition 6.3.3. By the isomorphism (6.1.1) along with Lemma 6.2.1, we have

$$C^{\min} \cong H^1_{(p)}(\mathbb{Q}_p/\mathbb{Z}_p(-1))^*.$$

By duality Theorem B.3.2, we have

$$C^{\min} \cong H^2_{(N)}(\mathbb{Z}_p(2)).$$

By Lemma 6.3.5, $H^1(\mathbb{Z}_p(2)) = 0$. By the duality theorem, $H^3_{(N)}(\mathbb{Z}_p(2)) = H^0_{(p)}(\mathbb{Q}_p/\mathbb{Z}_p(-1))^* = 0$. Then the cone construction of $H^\bullet_{(N)}$ gives an exact sequence

$$0 \to H^1_N(\mathbb{Z}_p(2)) \to H^2_{(N)}(\mathbb{Z}_p(2)) \to H^2(\mathbb{Z}_p(2)) \to H^2_N(\mathbb{Z}_p(2)) \to 0.$$

By Lemmas 6.3.4 and 6.3.5, we see that $H^2(\mathbb{Z}_p(2))$ and $H^2_N(\mathbb{Z}_p(2))$ are both finite groups of the same order (which is the p-part of $\prod_{\ell \mid N \text{prime}}(\ell-1)$). Therefore the rightmost surjection in the exact sequence is an isomorphism. Hence we have a canonical isomorphism

$$H^1_N(\mathbb{Z}_p(2)) \xrightarrow{\sim} H^2_{(N)}(\mathbb{Z}_p(2)).$$

Finally, Lemma 6.3.4 gives the computation of $H^1_N(\mathbb{Z}_p(2))$. □

Finally, we complete the proof of Proposition 6.1.6. We leave the case of $i = 0, 1$ to the reader, and sketch the proof of $i = -1$ in the next lemma.

Lemma 6.3.6. *For any $r > 0$, there are isomorphisms*

$$H^1_p(\mathbb{Z}/p^r\mathbb{Z}(-1)) \simeq \mathbb{Z}/p^r\mathbb{Z}, \quad H^1_{(p)}(\mathbb{Z}/p^r\mathbb{Z}(-1)) \simeq \bigoplus_{\ell \mid N \text{prime}} \mathbb{Z}_p/(\ell^2-1, p^r)\mathbb{Z}_p$$

and there is an exact sequence

$$0 \to H^1_{(p)}(\mathbb{Z}/p^r\mathbb{Z}(-1)) \to H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) \to H^1_p(\mathbb{Z}/p^r\mathbb{Z}(-1)) \to 0.$$

In particular,

$$\#H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) = p^r \cdot \prod_{\ell \mid N \text{prime}} \#\mathbb{Z}_p/(\ell^2-1, p^r)\mathbb{Z}_p.$$

Proof. The isomorphism $H^1_p(\mathbb{Z}/p^r\mathbb{Z}(-1)) \simeq \mathbb{Z}/p^r\mathbb{Z}$ follows from $H^0_p(\mathbb{Q}_p/\mathbb{Z}_p(-1)) = 0$ and $H^1_p(\mathbb{Q}_p/\mathbb{Z}_p(-1)) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ (see [NSW08, Thm. 7.3.10, pg. 400]). Since $H^3_{(N)}(\mathbb{Z}_p(2)) = 0$, we have $H^2_{(N)}(\mathbb{Z}/p^r\mathbb{Z}(2)) = H^2_{(N)}(\mathbb{Z}_p(2)) \otimes \mathbb{Z}/p^r\mathbb{Z}$, so the description of $H^1_{(p)}(\mathbb{Z}/p^r\mathbb{Z}(-1))$ follows from Proposition 6.3.3 and the duality Theorem B.3.2.

The proof is completed by considering the exact sequence

$$0 \to H^1_{(p)}(\mathbb{Z}/p^r\mathbb{Z}(-1)) \to H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) \to H^1_p(\mathbb{Z}/p^r\mathbb{Z}(-1)) \tag{6.3.7}$$

and the inequality

$$\#H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) \geq p^r \cdot \prod_{\ell \mid N \text{prime}} \#\mathbb{Z}_p/(\ell^2-1, p^r)\mathbb{Z}_p.$$

This inequality follows from the instance $H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) \cong H^2_{(c)}(p^{-r}\mathbb{Z}/\mathbb{Z}(2))^*$ of Poitou–Tate duality, along with the three consecutive terms

$$0 = H^1(\mathbb{Z}_p(2)) \to H^1_p(\mathbb{Z}_p(2)) \oplus \bigoplus_{\text{prime } \ell \mid N} H^1_\ell(\mathbb{Z}_p(2)) \to H^2_{(c)}(\mathbb{Z}_p(2))$$

of the standard long exact sequence in Galois cohomology. Here the leftmost vanishing is recorded in Lemma 6.3.5, $H^1_\ell(\mathbb{Z}_p(2))$ is calculated in Lemma 6.3.4, and it is well-known that $H^1_p(\mathbb{Z}_p(2)) \simeq \mathbb{Z}_p$. □

6.4. **Proof of Theorem 6.1.2 and Corollary 6.1.5.** We now return to the convention that N is prime and $p \mid (N-1)$.

Propositions 6.3.2 and 6.3.3 give us part (1) of the theorem. Part (3) follows from part (2) and the fact that $J = B \cdot C$. It remains to show (2). We give the proof for B, the proof for C being almost identical. The strategy will be to use the following version of Nakayama's lemma.

Lemma 6.4.1. *Let $(A, \mathfrak{m}, k)$ be a local ring and M be a finitely generated A-module. Then M is cyclic if and only if the k-vector space $\mathrm{Hom}_A(M,k)$ is one-dimensional. If M is cyclic, then an element $m \in M$ is a generator if and only if $\phi(m) \neq 0$ for some non-zero $\phi \in \mathrm{Hom}_A(M,k)$.*

Now we let $\mathfrak{m} \subset R$ be the maximal ideal (so $\mathfrak{m} = J^{\min} + pR$). Using (6.1.1) we calculate

$$\mathrm{Hom}_R(B, R/\mathfrak{m}) = \mathrm{Hom}_R(B^{\min}, R/\mathfrak{m}) \cong H^1_{\text{flat}}(\mathbb{F}_p(1)). \tag{6.4.2}$$

Proposition 6.3.2 shows that this is a 1-dimensional $\mathbb{F}_p$-vector space. Hence B is a cyclic R-module. Moreover, Proposition 6.3.2 implies that any cocycle generating $H^1_{\text{flat}}(\mathbb{F}_p(1))$ is ramified at N.

Now, the maps in (6.4.2) are given as follows. Let $\phi \in \mathrm{Hom}_R(B, R/\mathfrak{m})$ be non-zero (and hence a generator). Then the corresponding extension of 1 by $\mathbb{F}_p(1)$ is

$$\sigma \mapsto \begin{pmatrix} \omega(\sigma) & \phi(b_\sigma) \\ 0 & 1 \end{pmatrix}$$

If $\phi(b_\gamma)$ were zero, then this extension would be trivial at I_N and hence unramified at N. Since we know, by (6.4.2), that this extension generates $H^1_{\text{flat}}(\mathbb{F}_p(1))$ and that any such generator is ramified at N, we must have $\phi(b_\gamma) \neq 0$. The lemma then implies that b_γ generates B. This completes the proof of the theorem.

To prove Corollary 6.1.5, first we see that its main statement for $i = \pm 1$ follows directly from Theorem 6.1.2 in light of (6.1.1). The main statement for $i = 0$, along with statements (1) and (2), are basic class field theory. Statement (3) follows immediately from Lemma 6.2.1.

7. $R = \mathbb{T}$ and Applications

In this section, we use the numerical criterion to prove that the map $R \to \mathbb{T}$ constructed in Proposition 4.2.4 is an isomorphism. We also give further information about the structure of R and the R-modules B and C.

7.1. Numerical criterion.

We will use the strengthening of Wiles's numerical criterion [Wil95, Appendix] due to Lenstra (see [dSRS97, Criterion I, pg. 343]).

Theorem 7.1.1 (Wiles–Lenstra numerical criterion). *Let $\mathcal{O}$ be a DVR and let R and T be augmented $\mathcal{O}$-algebras with augmentation ideals I_R and I_T and assume that T is finite and flat over $\mathcal{O}$. Let $\pi : R \to T$ be a surjective homomorphism of augmented $\mathcal{O}$-algebras. Let η_T be the image of $\mathrm{Ann}_T(I_T)$ in $\mathcal{O}$.*

Then $\mathrm{length}(I_R/I_R^2) \geq \mathrm{length}(\mathcal{O}/\eta_T)$ with equality if and only if π is an isomorphism of complete intersection rings.

We apply this to the map $R \to \mathbb{T}$ constructed in §4.2. In this case, the DVR $\mathcal{O}$ is $\mathbb{Z}_p$ and the augmentation ideals are $J^{\min} \subset R$ and $I \subset \mathbb{T}$. Let $\eta \subset \mathbb{Z}_p$ be the image of $\mathrm{Ann}_{\mathbb{T}}(I)$ under the augmentation $\mathbb{T} \to \mathbb{Z}_p$, so that

$$\mathbb{Z}_p/\eta = \mathbb{T}/(I + \mathrm{Ann}_{\mathbb{T}}(I)).$$

By Theorem 3.2.1 and Lemma 3.2.2 we have

$$\mathbb{Z}_p/\eta = \mathbb{T}/(I + \mathrm{Ann}_{\mathbb{T}}(I)) \cong \mathbb{T}^0/I^0 \cong \mathbb{Z}_p/(N-1)\mathbb{Z}_p.$$

On the other hand, we have this consequence of Proposition 5.2.2 and Theorem 6.1.2.

Corollary 7.1.2. *We have $J^{\min} = YR$, $J = (J^{\min})^2$ and $J^{\min}/(J^{\min})^2 \cong \mathbb{Z}_p/(N-1)\mathbb{Z}_p$.*

Proof. We already know by Proposition 5.2.2 that $J^{\min} = YR + J$, and by Theorem 6.1.2 that J is generated by $b_\gamma c_\gamma$. Since $b_\gamma c_\gamma = -Y^2$, we see that $J \subset YR$ and so $J^{\min} = YR$. It also follows that $J = (J^{\min})^2$, and, since we know by Corollary 5.2.1 that $J^{\min}/J \cong \mathbb{Z}_p/(N-1)\mathbb{Z}_p$, the last part follows as well. □

We can now apply the numerical criterion.

Corollary 7.1.3. *The surjection $R \twoheadrightarrow \mathbb{T}$ from Proposition 4.2.4 is an isomorphism and both rings are complete intersections.*

Proof. This is immediate from the numerical criterion: we know that $\mathbb{T}$ is a finite flat $\mathbb{Z}_p$-algebra and we have the calculations of $\mathbb{Z}_p/\eta$ and $J^{\min}/(J^{\min})^2$. □

Corollary 7.1.4. *The ideals $I \subset \mathbb{T}$ and $I^0 \subset \mathbb{T}^0$ are principal. In particular, $\mathbb{T}^0$ is a complete intersection.*

Proof. It follows from Corollary 7.1.2 that $J^{\min}$ is principal. Since $R \to \mathbb{T}$ is an isomorphism of augmented algebras, it follows that $J^{\min} \cong I$ and so I is also principal. Then I^0 must also be principal. Since $\mathbb{T}^0$ is a flat $\mathbb{Z}_p$-algebra and $\mathbb{T}^0/I^0$ is finite, I^0 must be generated by a non-zero divisor. Since $\mathbb{T}^0/I^0 = \mathbb{Z}_p/(N-1)\mathbb{Z}_p$ is complete intersection, $\mathbb{T}^0$ is also complete intersection. □

We can also reprove Mazur's results regarding generators of I (see Corollary 9.1.2 below).

7.2. **Structure of R, B and C.** We have this immediate corollary.

Corollary 7.2.1. *The ring R is reduced, and it is finite and flat as a $\mathbb{Z}_p$-algebra.*

Proof. This follows from the isomorphism $R \xrightarrow{\sim} \mathbb{T}$ and the corresponding properties for $\mathbb{T}$ (§3.1.2, Proposition 4.2.4). □

In particular, it follows that any generator of $J^{\min}$ as an ideal is a generator for R as a $\mathbb{Z}_p$-algebra. Similarly, any generator of I will generate $\mathbb{T}$ as a $\mathbb{Z}_p$-algebra, as well as its quotient $\mathbb{T}^0$.

Corollary 7.2.2. *Let $Y \in R$ be the element described in Proposition 5.2.2, so that Y is a generator of $J^{\min}$. Let $g(y) \in \mathbb{Z}_p[y]$ be the monic minimal polynomial of Y, so that there is an isomorphism*

$$\mathbb{Z}_p[y]/(g(y)) \xrightarrow{\sim} R$$

given by $y \mapsto Y$. Then $g(y) = yf(y)$ for some $f(y) \in \mathbb{Z}_p[y]$ with $f(y) \equiv y^{\deg f} \pmod p$ and $f(0)\mathbb{Z}_p = (N-1)\mathbb{Z}_p$, and $\mathrm{Ann}_R(J^{\min})$ is the image of the ideal $(f(y))$.

Proof. The fact that the map is an isomorphism is a standard exercise. The image of (y) is the augmentation ideal $YR = J^{\min}$, so reducing modulo (y) we obtain a $\mathbb{Z}_p$-algebra homomorphism $\mathbb{Z}_p/(g(0)) \to \mathbb{Z}_p$, which implies that $g(0) = 0$, and so $g(y) = yf(y)$. The annihilator of (y) is $(f(y))$, so the annihilator of $J^{\min}$ is the image of $(f(y))$. Since R is local and $Y \in J^{\min}$, g is distinguished and the congruence $f(y) \equiv y^{\deg f} \pmod p$ follows. Finally, under the isomorphism $R \xrightarrow{\sim} \mathbb{T}$, we see that $\mathbb{Z}_p/(f(0))$ corresponds to $\mathbb{Z}_p/\eta = \mathbb{Z}_p/(N-1)\mathbb{Z}_p$, so the valuation of $f(0)$ must equal that of $N-1$. □

We see that $\deg f = \mathrm{rank}_{\mathbb{Z}_p}(R) - 1 = \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$. We write $R^0 = R/\mathrm{Ann}_R(J^{\min})$, so that the isomorphism $R \xrightarrow{\sim} \mathbb{T}$ induces $R^0 \xrightarrow{\sim} \mathbb{T}^0$.

Lemma 7.2.3.

1. *There are isomorphisms $J \simeq J^{\min} \simeq R^0$ of R-modules.*
2. *Any non-zero ideal $\mathfrak{a} \subset \mathrm{Ann}_R(J^{\min})$ is of the form $p^i \mathrm{Ann}_R(J^{\min})$ for some $i \geq 0$.*

Proof. (1) Since both ideals are principal, it suffices to show $\mathrm{Ann}_R(J) = \mathrm{Ann}_R(J^{\min})$. But we know that $J^{\min} = YR$ and $J = Y^2R$, so this follows from the fact that R is reduced (Corollary 7.2.1).

(2) By Corollary 7.2.2, we may study subideals of $(f(y))$ in $\mathbb{Z}_p[y]/(yf(y))$. As $\mathbb{Z}_p$-modules, the ideal $(f(y))$ is a free direct summand of $\mathbb{Z}_p[y]/(yf(y))$ of rank 1. Since any subideal must also by a sub-$\mathbb{Z}_p$-module, the lemma follows. □

Corollary 7.2.4. *The module B is free of rank 1 as an R module and there is an isomorphism $C \simeq J$ of cyclic R-modules. In particular, the map $B \otimes_R C \to J$ is an isomorphism.*

Proof. The second sentence follows from the first, since we already have a surjection $B \otimes_R C \twoheadrightarrow J$ and the first sentence implies that $B \otimes_R C \simeq J$ as R-modules.

By Theorem 6.1.2, B and C are cyclic R-modules, so it suffices to show that B is faithful as an R-module and that $\mathrm{Ann}_R(C) = \mathrm{Ann}_R(J)$. Since we have a surjection $B \otimes_R C \twoheadrightarrow J$, we know that $\mathrm{Ann}_R(B)$ and $\mathrm{Ann}_R(C)$ are subideals of $\mathrm{Ann}_R(J)$. By the previous lemma, we have $\mathrm{Ann}_R(B)$ and $\mathrm{Ann}_R(C)$ are either zero or of the form $p^i \mathrm{Ann}_R(J^{\min})$ for some $i \geq 0$.

Now, by Corollary 7.2.2, we have isomorphisms

$$R/(p^i \mathrm{Ann}_R(J^{\min}))\otimes_R R/J^{\min} \simeq \mathbb{Z}_p[y]/(y, p^i f(y)) \simeq \mathbb{Z}_p/(p^i f(0)) = \mathbb{Z}_p/p^i(N-1)\mathbb{Z}_p.$$

On the other hand, we know by Theorem 6.1.2 that

$$B \otimes_R R/J^{\min} \simeq \mathbb{Z}_p, \quad C \otimes_R R/J^{\min} \simeq \mathbb{Z}_p/(N-1)\mathbb{Z}_p.$$

It follows that $\mathrm{Ann}_R(B) = 0$ and that $\mathrm{Ann}_R(C) = \mathrm{Ann}_R(J^{\min}) = \mathrm{Ann}_R(J)$. □

We have the following immediate consequence of foregoing statements.

Corollary 7.2.5. *Let $e = \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$. Using the isomorphism $R \xrightarrow{\sim} \mathbb{Z}_p[y]/(yf(y))$ of Corollary 7.2.2, the R-modules J, $J^{\min}$, R^0, and C are isomorphic to $\mathbb{Z}_p[y]/(f(y))$. In particular, we have that $C/pC \simeq \mathbb{F}_p[y]/(y^e)$ as a module for $R/pR \xrightarrow{\sim} \mathbb{F}_p[y]/(y^{e+1})$.*

Remark 7.2.6. These results on the R-module structures of B and C are proven for an arbitrary choice of GMA structure on E, and so they hold for any choice of GMA structure. This is not surprising because the modules obtained for a different choice of GMA structure will be a priori isomorphic.

Remark 7.2.7. Using Proposition 3.3.4 and Corollary 7.2.4, one can prove that (E, ρ, D) is *ordinary* in the sense of [WWE18, Defn. 5.9.1].

8. The Newton polygon of $\mathbb{T}$ and a finer invariant

By the results of the previous section, there are isomorphisms

$$\mathbb{T} \simeq \mathbb{Z}_p[y]/(yf(y)), \quad \mathbb{T}^0 \simeq \mathbb{Z}_p[y]/(f(y)).$$

These presentations are not canonical, but, as is well-known, the Newton polygon of $f(y)$ is a canonical invariant of $\mathbb{T}^0$ (and, of course, it can be determined from the Newton polygon of $\mathbb{T}$). Mazur [Maz77, §II.19, pg. 140] asked what can be said about this Newton polygon. In this section, we introduce a finer invariant than the Newton polygon and prepare some lemmas to relate it to deformation theory.

8.1. Newton polygons.

For this subsection, we fix $g(x) = \sum_{i=0}^m \alpha_i x^i \in \mathbb{Z}_p[x]$ a monic, distinguished polynomial (i.e. $v_p(\alpha_i) > 1$ for $i < m$ and $\alpha_m = 1$). Note that a coefficient may be zero, so it is possible that $v_p(\alpha_i) = \infty$ in what follows. We slightly abuse terminology by calling these valuations "integers" nonetheless.

Definition 8.1.1. The *Newton polygon* of $g(x)$ is the lower convex hull of the points $\{(i, v_p(\alpha_i)) : i = 0, \dots, m\}$ in $\mathbb{R}^2$, where a point is omitted when $v_p(\alpha_i) = \infty$. We denote it by $\mathrm{NP}(g)$.

Define a sequence $z_0, \dots, z_m$ inductively by

$$z_0 = v_p(\alpha_0), \qquad z_i = \min\{z_{i-1}, v_p(\alpha_i)\} \text{ for } i = 1, \dots, m.$$

Then it is an easy exercise to see that $\mathrm{NP}(g)$ is the lower convex hull of the points $\{(i, z_i) : i = 0, \dots, m\}$.

Let $T = \mathbb{Z}_p[x]/(g(x))$. We will call an element $y \in T$ a *generator* if $(x) = (y)$ as ideals of T. Such an element will also generate T as a $\mathbb{Z}_p$-algebra. Since T is local, we can see that $y = ux$ for some unit $u \in T^\times$. Recall from §1.10 that $(\mathbb{Z}/p^r\mathbb{Z})[\epsilon_i] := (\mathbb{Z}/p^r\mathbb{Z})[\epsilon]/(\epsilon^{i+1})$.

Lemma 8.1.2. *For $i = 0, \dots, m$, define t_i (resp. r_i) to be the maximal integer r such that there exists a surjective ring homomorphism*

$$\varphi : T \twoheadrightarrow (\mathbb{Z}/p^r\mathbb{Z})[\epsilon_i]$$

such that $\varphi(y) = \epsilon$ for some generator $y \in T$ (resp. such that $\varphi(x) = \epsilon$). Then $t_i = r_i = z_i$ for $i = 0, \dots, m$.

Proof. For $i = 0$, a homomorphism φ as in the statement must factor through $T/yT = T/xT = \mathbb{Z}_p/\alpha_0\mathbb{Z}_p$, and so we see $t_0 = r_0 = v_p(\alpha_0) = z_0$. By induction, we can assume the result for $i < n$ for some $1 \le n \le m$, and prove that $t_n = r_n = z_n$. Since the sequence t_i is decreasing and since $r_{n-1} \le t_{n-1}$, we have $v_p(\alpha_i) \ge t_{n-1} \ge r_{n-1}$ for $i = 0, \dots, n-1$.

For $r \le t_{n-1}$, a homomorphism $\varphi : T \twoheadrightarrow (\mathbb{Z}/p^r\mathbb{Z})[\epsilon_n]$ with $\varphi(y) = \epsilon$ for a generator $y \in xT$ must factor through

$$T/(p^rT + y^{n+1}T) = T/(p^rT + x^{n+1}T) = \mathbb{Z}/p^r\mathbb{Z}[x]/(\alpha_n x^n, x^{n+1}).$$

For any generator y, there exists $u(x) = u_0 + u_1x + \cdots + u_{m-1}x^{m-1}$ with $u_0 \in \mathbb{Z}_p^\times$ such that $x = u(x)y$ in T. We see that there is a such a homomorphism φ if and only if there is a homomorphism

$$\mathbb{Z}/p^r\mathbb{Z}[x]/(\alpha_n x^n, x^{n+1}) \to (\mathbb{Z}/p^r\mathbb{Z})[\epsilon_n]$$

sending x to $\epsilon u(\epsilon)$. Such a homomorphism exists if and only if $\alpha_n\epsilon^n u(\epsilon) = u_0\alpha_n\epsilon^n$ is 0 in $(\mathbb{Z}/p^r\mathbb{Z})[\epsilon_n]$. Similarly, a homomorphism φ such that $\varphi(x) = \epsilon$ exists if and only if $\alpha_n\epsilon^n$ is 0 in $(\mathbb{Z}/p^r\mathbb{Z})[\epsilon_n]$. Both of these happen if and only if $v_p(\alpha_n) \ge r$, so we see that $t_n = r_n = \min\{t_{n-1}, v_p(\alpha_n)\} = \min\{z_{n-1}, v_p(\alpha_n)\} = z_n$. □

Note that the integers t_i are an invariant of the pair $(T, (x))$ of T and the ideal $(x) \subset T$ generated by x. That is, we emphasize that $\{t_i\}$ do not depend on the particular choice of generator x of T. The lemma implies that $\mathrm{NP}(g)$ is the lower convex hull of the points $\{(i, t_i) : i = 0, \dots, m\}$, and hence is also an invariant of $(T, (x))$. In applications, T will be $\mathbb{T}$ or $\mathbb{T}^0$ and (x) will be the Eisenstein ideal.

The following example witnesses the fact that the set $\{t_i\}$ is a strictly finer invariant than $\mathrm{NP}(g)$.

Example 8.1.3. Suppose that $g(x) = x^2 + \alpha_1x + \alpha_0$, with $v_p(\alpha_0) = 2$ and $v_p(\alpha_1) > 0$. Then $\mathrm{NP}(g)$ must be the line segment from $(0, 2)$ to $(2, 0)$, but there are two possible values of (t_0, t_1, t_2): either $(2, 1, 0)$ or $(2, 2, 0)$. Moreover, the two different possible values of t_1 encode information about $g(x)$. For example, if $g(x)$ is reducible and $t_1 = 2$, then the two roots of $g(x)$ can be additive inverses of each other, but not if $t_1 = 1$. This applies to the generators of $\mathbb{T}$ given in Corollary 9.1.2.

8.2. **The Newton polygon of $\mathbb{T}$.** For the remainder of the paper, we will be interested in studying the integers t_i associated by Lemma 8.1.2 to $\mathbb{T}$. Combining Lemma 8.1.2 with the results of §7.2, we have the following.

Proposition 8.2.1. *Let $y \in \mathbb{T}$ be a generator of I, so that $\mathbb{Z}_p[x]/(g(x)) \xrightarrow{\sim} \mathbb{T}$ via $x \mapsto y$, where $g(x) = \sum_{i=0}^{e+1} \alpha_i x^i \in \mathbb{Z}_p[x]$ is the monic minimal polynomial of y. Define t_i inductively by $t_0 = v_p(\alpha_0)$ and $t_i = \min\{t_{i-1}, v_p(\alpha_i)\}$ for $i = 1, \dots, e+1$. Then the sequence $\{t_i\}$ is independent of the choice of y, and $NP(g)$ is the lower convex hull of the set $\{(i, t_i)\}$.*

Moreover, for any $0 \le n \le e+1$ and any positive integer s, the following are equivalent:

(1) $s \le t_n$,
(2) *For any generator* $z \in J^{\min}$, *there is a homomorphism* $\varphi : R \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ *such that* $\varphi(z) = \epsilon$.

Note that $t_0 = \infty$, $t_1 = v_p(N-1)$, $t_i > 0$ for $i \le e$, and $t_{e+1} = 0$.

Part 2. Massey products and deformations

In this part, we use the results of the previous part to show that the tangent space of R is 1-dimensional and choose an explicit basis D_1 of this space. We consider three representations ρ_0, ρ_0^c and ρ_0^b that all have the same pseudorepresentation and relate the existence of deformations of these three representations to the structure of R and to different Massey products.

For this whole part, we fix the integer $t = v_p(N-1) \ge 1$.

9. The tangent space and cocycles

In this section, we study the tangent space of R. Recall from §1.10 the notation that $\mathbb{Z}/p^s\mathbb{Z}[\epsilon_i] := \mathbb{Z}/p^s\mathbb{Z}[\epsilon]/(\epsilon^{i+1})$. The numbering makes $\mathrm{Hom}(R, \mathbb{Z}/p^s\mathbb{Z}[\epsilon_i])$ the space of i-th order deformations modulo p^s. The tangent space (modulo p^s) is the space of first order deformations modulo p^s.

Recall the other notations introduced in §1.10, including the cyclotomic character κ_{cyc} and the element $\gamma \in I_N$.

9.1. The tangent space of R and generators of $\mathbb{T}$.

We can describe the tangent space of R using our explicit presentation of R in Corollary 7.2.2.

Proposition 9.1.1. *Let* $t = v_p(N-1)$.

(1) *The* $\mathbb{F}_p$*-vector space* $\mathrm{Hom}(R, \mathbb{F}_p[\epsilon_1])$ *is* 1*-dimensional. Any non-zero element of this space sends* $J^{\min}$ *to* (ϵ) *and* J *to* 0.
(2) *There exists a local surjection* $R \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}[\epsilon_1]$ *if and only if* $s \le t$. *Any such surjection sends* $J^{\min}$ *to* (ϵ) *and* J *to* 0.
(3) *Let* $Y = 1 - d_\gamma$. *Let* $\varphi_1 : R \to \mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]$ *be the unique homomorphism sending* Y *to* ϵ. *Let* $a : G_{\mathbb{Q},S} \to \mathbb{Z}/p^t\mathbb{Z}$ *be the unique homomorphism factoring through* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ *and sending* γ *to* 1.

Then the pseudorepresentation $D_1 : G_{\mathbb{Q},S} \to \mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]$ *associated to* φ_1 *is given by* $\det(D_1) = \kappa_{\mathrm{cyc}}$ *and*

$$\mathrm{tr}(D_1) = (\kappa_{\mathrm{cyc}} + 1) + \epsilon a(\kappa_{\mathrm{cyc}} - 1).$$

Proof. Parts (1) and (2) are clear from the structure of R computed in Corollary 7.2.2. Since $J \subset \ker(\varphi_1)$, we see that φ_1 factors through R^{red}, so part (3) follows from Proposition 5.1.2. □

The following corollary was first proven by Mazur [Maz77, Prop. II.16.1, pg. 125]. Recall that Mazur calls a prime number $\ell \neq N$ a *good prime (for* N *and* p*)* if both of the following are true: (i) $\ell \not\equiv 1 \pmod p$ and, (ii) ℓ is not a p-th power modulo N.

Corollary 9.1.2. *Let* $\ell \neq N$ *be a prime number. Then* $T_\ell - (\ell + 1) \in I$ *is a generator of the principal ideal* I *if and only if* ℓ *is a good prime.*

Note that any generator of I is also a generator of $\mathbb{T}$ (and $\mathbb{T}^0$) as a $\mathbb{Z}_p$-algebra.

Proof. In this proof, for $x \in \mathbb{Z}_p$, we write $\bar{x}$ for the reduction modulo p of x, and we define $\bar{D}_1 = D_1 \otimes_{\mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]} \mathbb{F}_p[\epsilon_1]$.

First, assume $\ell \neq p$. As in the proof of Proposition 4.2.4, we have $\mathrm{tr}(D_{\mathbb{T}})(\mathrm{Fr}_\ell) = T_\ell$, so we see that $T_\ell - 1 - \ell$ is a generator of I if and only if $\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_\ell) - 1 - \bar{\ell}$ is non-zero. Since

$$\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_\ell) - (1+\bar{\ell}) = (\bar{\ell}-1)\bar{a}(\mathrm{Fr}_\ell)\epsilon$$

we see that $T_\ell - (1+\ell)$ is a generator of I if and only if $(\bar{\ell}-1)\bar{a}(\mathrm{Fr}_\ell) \neq 0$, which happens if and only if $\ell \not\equiv 1 \pmod{p}$ and $\bar{a}(\mathrm{Fr}_\ell) \neq 0$. It follows from class field theory that $\bar{a}(\mathrm{Fr}_\ell) \neq 0$ if and only if ℓ is not a p-th power modulo N.

Now let $\ell = p$. Since $T_p = U_p + pU_p^{-1}$ we see that the images of $T_p - (p+1)$ and $U_p - 1$ in $\mathbb{F}_p[\epsilon_1]$ are the same. In particular, $T_p - (p+1)$ generates I if and only if $U_p - 1$ generates I. Now let $\mathrm{Fr}_p \in G_p$ be a Frobenius element, choose $\sigma \in I_p$ such that $\omega(\sigma) \neq 1$, and let $x = \kappa_{\mathrm{cyc}}(\sigma)$. Then, as in the proof of Proposition 4.2.4, we have

$$U_p = \frac{1}{1-x}(\mathrm{tr}(D_{\mathbb{T}})(\mathrm{Fr}_p\sigma) - x\mathrm{tr}(D_{\mathbb{T}})(\mathrm{Fr}_p))$$

so $U_p - 1$ generates I if and only if

$$\frac{1}{1-\bar{x}}\left(\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_p\sigma) - \bar{x}\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_p)\right) \neq 1.$$

Using the fact that a is unramified at p, we see that

$$\frac{1}{1-\bar{x}}\left(\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_p\sigma) - \bar{x}\mathrm{tr}(\bar{D}_1)(\mathrm{Fr}_p)\right) = 1 + \bar{a}(\mathrm{Fr}_p)\epsilon.$$

Hence we see that $U_p - 1$ generates I if and only if $\bar{a}(\mathrm{Fr}_p) \neq 0$ and the proof continues as above. □

9.2. **A normalization for certain cocycles.** We now depart from the notation of §1.1 where a, b and c were cohomology classes chosen up to multiplication by $(\mathbb{Z}/p^t\mathbb{Z})^\times$. We let $a \in Z^1_{\mathrm{flat}}(\mathbb{Z}/p^t\mathbb{Z})$ be the cocycle defined in Proposition 9.1.1, let $b \in Z^1_{\mathrm{flat}}(\mathbb{Z}/p^t\mathbb{Z}(1))$ be a Kummer cocycle associated to a choice of p^t-th root of N, and let $c \in Z^1_{\mathrm{flat}}(\mathbb{Z}/p^t\mathbb{Z}(-1))$ be an element such that $c|_p = 0$ and whose image in $H^1_{\mathrm{flat}}(\mathbb{Z}/p^t\mathbb{Z}(-1))$ is a generator. Recall from Corollary 6.1.5 that $H^1_{\mathrm{flat}}(\mathbb{Z}/p^t\mathbb{Z}(i)) \simeq \mathbb{Z}/p^t\mathbb{Z}$, and that the classes of a, b and c are generators. We have specified a completely, and b and c up to a multiple of $(\mathbb{Z}/p^t\mathbb{Z})^\times$.

Next, as with a, we want to normalize b and c with respect to our choice of $\gamma \in I_N$ from §1.10.1. Since $b(\gamma), c(\gamma) \not\equiv 0 \pmod{p}$, we can and do normalize so that $b(\gamma) = -1$ and $c(\gamma) = 1$. Because of this choice we have

$$a(\gamma)^2 + b(\gamma)c(\gamma) = 0.$$

Since a, b, c are continuous homomorphisms on I_N, this implies that

$$(a^2 + bc)|_{I_N} = 0. \tag{9.2.1}$$

Remark 9.2.2. Note that these cocycles a, b, c are not related to the elements $a_\sigma, b_\sigma, c_\sigma$ introduced in (4.1.2). We write cochains in function notation (i.e. $a(\sigma)$), so hopefully this does not cause confusion.

10. Matrix-valued deformations

Let $\rho_0 : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^t\mathbb{Z})$ be the representation $\mathbb{Z}/p^t\mathbb{Z}(1) \oplus \mathbb{Z}/p^t\mathbb{Z}$. From the choice of the cocycles a, b, c in §9.2, we have a first order deformation of ρ_0. Namely, let

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in Z^1(\mathrm{End}(\mathbb{Z}/p^t\mathbb{Z}(1) \oplus \mathbb{Z}/p^t\mathbb{Z}))$$

and define

$$\rho_1 = (1 + M\epsilon)\rho_0 : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]).$$

This is a finite-flat representation such that $\psi(\rho_1) = D_1$.

We specify two more representations $\rho_0^b, \rho_0^c : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^t\mathbb{Z})$ satisfying $\psi(\rho_0) = \psi(\rho_0^b) = \psi(\rho_0^c)$, namely

$$\rho_0^b = \begin{pmatrix} \kappa_{\mathrm{cyc}} & b \\ 0 & 1 \end{pmatrix}, \quad \rho_0^c = \begin{pmatrix} \kappa_{\mathrm{cyc}} & 0 \\ \kappa_{\mathrm{cyc}} c & 1 \end{pmatrix}$$

In this section, we will consider deformations of ρ_0, ρ_0^b and ρ_0^c, and how they are related to R.

10.1. Notation for deformations and Massey products.

We define the notions of *good*, *very good*, and *adapted* deformations.

Definition 10.1.1. Let $1 \le r \le s$ and $0 \le n \le m$ be integers. Let $\nu : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n])$ be a representation. A representation $\nu' : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_m])$ is called an *m-th order deformation of ν modulo p^r* if there is an isomorphism

$$\nu' \otimes_{\mathbb{Z}/p^r\mathbb{Z}[\epsilon_m]} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n] \cong \nu \otimes_{\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n].$$

Definition 10.1.2. Let $r \le t$, and let $\rho_n : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n])$ be a representation. We call ρ_n *good* if the following conditions are satisfied:

1. $\psi(\rho_n) \otimes_{\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]} \mathbb{Z}/p^r\mathbb{Z} = \psi(\rho_0) \otimes_{\mathbb{Z}/p^t\mathbb{Z}} \mathbb{Z}/p^r\mathbb{Z}$.
2. $\det(\rho_n) = \kappa_{\mathrm{cyc}}$.
3. $\rho_n|_p$ is finite-flat and upper-triangular.
4. $\mathrm{tr}(\rho_n)|_{I_N} = 2$.

When ρ_n is a good n-th order deformation of ρ_1 modulo p^s, we define $\chi_a(\rho_n), \chi_d(\rho_n) : G_{\mathbb{Q}_p} \to (\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n])^\times$ to be the diagonal characters of $\rho_n|_p$.

Note that after assuming (2), (4) is equivalent to $\psi(\rho_n)|_{I_N}$ being trivial, cf. §1.8.1 and Proposition 4.1.1. Thus a good representation induces a surjective homomorphism $R \twoheadrightarrow \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ corresponding to $\psi(\rho_n)$.

Definition 10.1.3. Suppose that ρ_n is an n-th order deformation of ρ_1 modulo p^s with $s \le t$. We call ρ_n *mildly ramified at N* if it satisfies

$$\rho_n|_{I_N} = \begin{pmatrix} 1 + a\epsilon & b\epsilon \\ c\epsilon & 1 - a\epsilon \end{pmatrix}\Bigg|_{I_N}.$$

We call ρ_n *very good* if it is good and mildly ramified at N.

Definition 10.1.4. Let $1 \le s \le t$ and let ρ_n be an n-th order deformation of ρ_1 modulo p^s, and write ρ_n as

$$\rho_n = \left(1 + \sum_{i=1}^{n} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \epsilon^i\right) \rho_0.$$

We say that an n-th order deformation ρ_n^c of ρ_0^c modulo p^s is *adapted to* ρ_n if

$$\rho_n^c = \rho_0^c + \sum_{i=1}^{n} \begin{pmatrix} \kappa_{\mathrm{cyc}} a_i & b_{i-1} \\ \kappa_{\mathrm{cyc}} c_{i+1} & d_i \end{pmatrix} \epsilon^i$$

for some $c_{n+1} \in C^1(\mathbb{Z}/p^s\mathbb{Z}(-1))$, where $b_0 := 0$. In this situation, we call c_{n+1} the *cochain associated to* ρ_n^c, and we note that $\rho_n^c \mapsto c_{n+1}$ is a bijective correspondence between the set of n-th order deformations ρ_n^c of ρ_0^c modulo p^s that are adapted to ρ_n and the set of cochains c_{n+1} satisfying

$$dc_{n+1} = \sum_{i=1}^{n} c_i \smile a_{n+1-i} + d_i \smile c_{n+1-i}.$$

Similarly, we say that an n-th order deformation ρ_n^b of ρ_0^b modulo p^s is *adapted to* ρ_n if

$$\rho_n^b = \rho_0^b + \sum_{i=1}^{n} \begin{pmatrix} \kappa_{\mathrm{cyc}} a_i & b_{i+1} \\ \kappa_{\mathrm{cyc}} c_{i-1} & d_i \end{pmatrix} \epsilon^i$$

for some $b_{n+1} \in C^1(\mathbb{Z}/p^s\mathbb{Z}(1))$, where $c_0 := 0$. We also call b_{n+1} the *cochain associated to* ρ_n^b, and note that there is a similar bijection $\rho_n^b \mapsto b_{n+1}$.

One readily calculates that when ρ_n^c and ρ_n^b are adapted to ρ_n as above, then there is an equality of pseudorepresentations

$$\psi(\rho_n) = \psi(\rho_n^c) = \psi(\rho_n^b) : G_{\mathbb{Q},S} \longrightarrow \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]. \tag{10.1.5}$$

We introduce some notation for Massey products, Massey powers, and their connection with deformations; see Appendix A for full details. For $s \le t$, let M_s denote the image of M in $Z^1(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$. If ρ_n is an n-th order deformation of ρ_1 modulo p^s, it provides a defining system D for the Massey power $\langle M_s\rangle^{n+1}$. We will abuse notation and say $\langle M\rangle_D^{n+1}$ *vanishes in* $H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$ if $\langle M_s\rangle_D^{n+1} = 0$, and refer to the Massey relations for $\langle M_s\rangle_D^{n+1}$ as the *Massey relations for* $\langle M\rangle_D^{n+1}$ *modulo* p^s.

Remark 10.1.6. In the notation of the previous paragraph, if $r \le s$, then $\rho_n \otimes_{\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ is a deformation of ρ_1 modulo p^r, which provides a defining system D_r for the Massey power $\langle M_r\rangle^{n+1}$. Examining the definition, one sees that $\langle M_r\rangle_{D_r}^{n+1}$ is the image of $\langle M_s\rangle_D^{n+1}$ under the natural map

$$H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z})) \to H^2(\mathrm{End}(\mathbb{Z}/p^r\mathbb{Z}(1) \oplus \mathbb{Z}/p^r\mathbb{Z}))$$

and similarly for the coordinate Massey relations. In particular, one sees that the following are equivalent:

(1) $\langle M_r\rangle_{D_r}^{n+1}$ is 0 in $H^2(\mathrm{End}(\mathbb{Z}/p^r\mathbb{Z}(1) \oplus \mathbb{Z}/p^r\mathbb{Z}))$.

(2) $\langle M_s\rangle_D^{n+1}$ is in the kernel of the natural map
$$H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z})) \to H^2(\mathrm{End}(\mathbb{Z}/p^r\mathbb{Z}(1) \oplus \mathbb{Z}/p^r\mathbb{Z})).$$

(3) $\langle M_s\rangle_D^{n+1}$ is in the image of the map
$$H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z})) \to H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$$
induced by multiplication by p^r.

This perhaps justifies the abuse of notation.

10.2. **GMA lemmas.** In this subsection, we consider homomorphisms from generalized matrix algebras to matrix algebras. This will be used to relate the existence of certain matrix-valued deformations to properties of R.

Lemma 10.2.1. *Let A be a commutative ring, let*

$$E_A = \begin{pmatrix} A & B_A \\ C_A & A \end{pmatrix}$$

be an A-GMA, and let $\Phi : B_A \times C_A \to A$ be the A-bilinear map that induces the multiplication in E_A. Then there is a bijection between the set of A-GMA homomorphisms $E_A \to M_2(A)$ and the set of pairs $(\varphi_b : B_A \to A, \varphi_c : C_A \to A)$ of A-module homomorphisms satisfying $\Phi(b,c) = \varphi_b(b)\varphi_c(c)$ for all $b \in B_A$ and $c \in C_A$.

Proof. The map sends an A-GMA homomorphism $\Psi : E_A \to M_2(A)$ to $(\Psi|_{B_A}, \Psi|_{C_A})$. The fact that Ψ is an A-GMA homomorphism implies that $\Phi(b,c) = \Psi(b)\Psi(c)$ for all $b \in B_A$ and $c \in C_A$. Conversely, given a pair (φ_b, φ_c), we can define a map of A-modules by

$$E_A \xrightarrow{\left(\begin{smallmatrix} 1 & \varphi_b \\ \varphi_c & 1 \end{smallmatrix}\right)} M_2(A),$$

and we see that it is a homomorphism of A-GMAs if and only if $\Phi(b,c) = \varphi_b(b)\varphi_c(c)$ for all $b \in B_A$ and $c \in C_A$. □

For the universal Cayley–Hamilton R-algebra E defined in §4.1, the following lemma shows that deformations of ρ_0 give rise to GMA homomorphisms from E to a matrix algebra.

Lemma 10.2.2. *Let $\rho_n : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n])$ be a good deformation of ρ_0 modulo p^r. Then there exists a GMA structure on the Cayley–Hamilton R-algebra E such that the Cayley–Hamilton representation $\rho_n : E \to M_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n])$ induced by ρ_n is a homomorphism of GMAs.*

Proof. The Cayley–Hamilton representation ρ_n exists by virtue of the universal property of E: ρ_n is finite-flat and induces a pseudorepresentation with the properties enumerated in Proposition 4.1.1. For the rest, see [WWE19, Thm. 3.2.2], for example. □

10.3. **Criteria for goodness and very goodness.** Let $1 \le s \le t$, and let $n \ge 1$ be an integer. Fix an n-th order *good* deformation ρ_n of ρ_1 modulo p^s.

Lemma 10.3.1. *Let ρ_n^c and ρ_n^b be n-th order deformations of ρ_1^c and ρ_n^b modulo p^s, respectively, that are adapted to ρ_n. Let $c_{n+1} \in C^1(\mathbb{Z}/p^s\mathbb{Z}(-1))$ and $b_{n+1} \in C^1(\mathbb{Z}/p^s\mathbb{Z}(1))$ be the associated cochains. Then*

1. *ρ_n^c is good if and only if $c_{n+1}|_p = 0$.*
2. *ρ_n^b is good if and only if b_{n+1} makes $\sum_{i=0}^n b_{i+1}|_p\epsilon^i$ define a finite-flat extension of $\chi_d(\rho_n)$ by $\chi_a(\rho_n)$.*

Proof. By (10.1.5), we see that ρ_n^c and ρ_n^b are good if and only if $\rho_n^c|_p$ and $\rho_n^b|_p$, respectively, are finite-flat and upper-triangular. This shows the "only if" part of (1), and, since $\rho_n^b|_p$ is automatically upper-triangular, (2) is immediate. It remains to show that $\rho_n^c|_p$ is finite-flat if $c_{n+1}|_p = 0$.

If $c_{n+1}|_p = 0$, then $\rho_n^c|_p$ is the extension of $\chi_d(\rho_n)$ by $\chi_a(\rho_n)$ defined by $\sum_{i=1}^{n-1} b_i\epsilon^{i+1}$. Its class in $\mathrm{Ext}_{\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n][G_p]}(\chi_d(\rho_n), \chi_a(\rho_n))$ is the scalar multiple by ϵ of the class of $\rho_n|_p$ (which is finite-flat). Since scalar multiplication on extensions preserves finite-flatness (see Remark C.3.2), $\rho_n^c|_p$ is finite-flat. □

Lemma 10.3.2. *Let $1 \le s \le t$, and let $n \ge 1$ be an integer. Suppose that ρ_{n+1} is an $(n+1)$-st order deformation of ρ_1 modulo p^s. Write ρ_{n+1} as*

$$\rho_{n+1} = \left(1 + \sum_{i=1}^{n+1} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \epsilon^i \right) \rho_0,$$

so $a_1 = a$, $b_1 = b$, $c_1 = c$ and $d_1 = -a$, and $a_i, d_i \in C^1(\mathbb{Z}/p^s\mathbb{Z})$, $b_i \in C^1(\mathbb{Z}/p^s\mathbb{Z}(1))$, $c_i \in C^1(\mathbb{Z}/p^s\mathbb{Z}(-1))$. Suppose also that $\rho_n := \rho_{n+1} \otimes_{\mathbb{Z}/p^s\mathbb{Z}[\epsilon_{n+1}]} \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ is very good. Then ρ_{n+1} is very good if and only if these three conditions hold:

- *(i)* $c_{n+1}|_p = 0$ *and* $a_{n+1}|_{I_p} = d_{n+1}|_{I_p} = 0$,
- *(ii)* $\sum_{i=1}^{n+1} b_i|_p \epsilon^i$ *defines a finite-flat extension of* $\chi_d(\rho_{n+1})$ *by* $\chi_a(\rho_{n+1})$,
- *(iii)* $a_{n+1}|_{I_N} = b_{n+1}|_{I_N} = c_{n+1}|_{I_N} = d_{n+1}|_{I_N} = 0$.

Proof. First assume that ρ_{n+1} is very good. Then (iii) is clear from the definition of very good. Since ρ_{n+1} is good, we have that $\rho_{n+1}|_p$ is finite-flat and upper-triangular. This implies that $c_{n+1}|_p = 0$. Because $\chi_a(\rho_{n+1})$ (resp. $\chi_d(\rho_{n+1})$) is a finite-flat deformation of $\mathbb{Z}/p^s\mathbb{Z}(1)$ (resp. $\mathbb{Z}/p^s\mathbb{Z}$), which is equivalent to being an unramified deformation, we have (i). Then (ii) follows from $\rho_{n+1}|_p$ being finite-flat.

Conversely, suppose that ρ_{n+1} satisfies (i), (ii), and (iii). We have just explained why $\rho_{n+1}|_p$ is finite-flat and upper-triangular. Also ρ_{n+1} is clearly mildly ramified at N and $\mathrm{tr}(\rho_{n+1}|_{I_N}) = 2$. Because ρ_n is good, $\det(\rho_{n+1}) = \kappa_{\mathrm{cyc}}(1 + \epsilon^{n+1}\delta)$ for some $\delta \in Z^1(\mathbb{Z}/p^s\mathbb{Z})$. We observe that (i) implies $\delta|_{I_p} = 0$. Since ρ_{n+1} is mildly ramified at N, we see that $\det(\rho_{n+1})|_{I_N}$ has the form $1 - (a^2 + bc)|_{I_N}\epsilon^2 = 1$ by the normalizations of (9.2.1). Thus δ is unramified everywhere and consequently equals 0. □

10.4. **Residually lower-triangular deformations.** We study deformations of ρ_0^c.

Lemma 10.4.1. *Let $1 \le r \le s \le t$, and let $n \ge 1$ be an integer. Suppose that ρ_n is an n-th order deformation of ρ_1 modulo p^s, and suppose that ρ_n is very good. Let $\varphi : R \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ be the corresponding homomorphism, and let D be the corresponding defining system for the Massey power $\langle M \rangle^{n+1}$. Write $\rho_{n,r} = \rho_n \otimes_{\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$. Then the following are equivalent:*

1. *There is a surjective homomorphism $\varphi' : R \twoheadrightarrow \mathbb{Z}/p^r\mathbb{Z}[\epsilon_{n+1}]$ such that the following diagram commutes*

$$\begin{tikzcd} R \arrow[r, "\varphi'"] \arrow[d, "\varphi"'] & \mathbb{Z}/p^r\mathbb{Z}[\epsilon_{n+1}] \arrow[d] \\ \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n] \arrow[r] & \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n], \end{tikzcd}$$

where the unlabeled arrows are the quotient maps.

2. *The $\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$-module $C \otimes_{R,\varphi} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ is free of rank* 1.
3. *There is an n-th order deformation of ρ_0^c modulo p^r that is adapted to $\rho_{n,r}$.*

(4) *There is an n-th order deformation of ρ_0^c modulo p^r that is adapted to $\rho_{n,r}$ and is good.*

(5) *The Massey relation for $\langle M\rangle_D^{n+1}$ holds in the $(2,1)$-coordinate modulo p^r.*

Remark 10.4.2. For $n = 1$, we can take $\rho_n = \rho_1 \otimes_{\mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]} \mathbb{Z}/p^s\mathbb{Z}[\epsilon_1]$, and the Massey relation for $\langle M\rangle_D^2 = M \cup M$ in the $(2,1)$-coordinate is simply $c \cup a - a \cup c = 0$. Using the skew-commutativity of the cup product, we see that this relation holds if and only if $a \cup c = 0$.

Proof. In the proof, it will be helpful to induce an alternate characterization of (2). First note that (2) only depends on the R-module structure of C, which is independent of the choice of GMA-structure on E. We apply Lemma 10.2.2 to $\rho_{n,r}$, which defines a GMA structure on E, and we will write $E \xrightarrow{\sim} \left(\begin{smallmatrix} R & B \\ C & R \end{smallmatrix}\right)$ for this choice of GMA structure. We write $\Phi : B \times C \to R$ for the R-bilinear map coming from the multiplication in E. Write $C_{n,r} := C \otimes_{R,\varphi} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ and $B_{n,r} := B \otimes_{R,\varphi} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$.

By Lemmas 10.2.1 and 10.2.2, the deformation $\rho_{n,r}$ defines $\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$-module homomorphisms $\varphi_b : B_{n,r} \to \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ and $\varphi_c : C_{n,r} \to \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$, both having image $\epsilon\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$, and satisfying $\Phi(b, c) = \varphi_b(b)\varphi_c(c)$ for all $b \in B_{n,r}$ and $c \in C_{n,r}$.

With this notation, we can see that (2) is equivalent to the following condition:

(2') There is a homomorphism $\tilde{\varphi}_c : C_{n,r} \to \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ of $\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$-modules such that $\epsilon \cdot \tilde{\varphi}_c = \varphi_c$.

Indeed, if $C_{n,r}$ is free, then it has a generator z such that $\varphi_c(z) = \epsilon$, and we can define $\tilde{\varphi}_c$ by $\tilde{\varphi}_c(z) = 1$. Conversely, any such $\tilde{\varphi}_c$ must be surjective, so the fact that $C_{n,r}$ is cyclic implies that it must be free.

(1) $\iff$ (2): Choose a generator $x \in R$ such that $\varphi(x) = \epsilon$. By Corollaries 7.2.2 and 7.2.5, there is an isomorphism

$$\mathbb{Z}_p[x]/(xg(x)) \xrightarrow{\sim} R$$

for some distinguished monic polynomial $g(x) = \sum_{i=0}^{e} \beta_i x^i$, and an isomorphism of R-modules $C \simeq \mathbb{Z}_p[x]/(g(x))$. The existence of φ implies that $v_p(\beta_i) \geq s$ for $i < n$. We see that

$$C \otimes_{R,\varphi} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n] \simeq \frac{\mathbb{Z}/p^r\mathbb{Z}[\epsilon]}{(g(\epsilon), \epsilon^{n+1})} = \frac{\mathbb{Z}/p^r\mathbb{Z}[\epsilon]}{(\beta_n\epsilon^n, \epsilon^{n+1})}$$

as an $\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$-module. Hence (2) is equivalent to $v_p(\beta_n) \geq r$, which is equivalent to (1) by Lemma 8.1.2.

$(2') \implies (3)$: Let $\tilde{\varphi}_c$ be as in (2'). Then we see that $\Phi(b, c) = (\epsilon \cdot \varphi_b)(b)\tilde{\varphi}_c(c)$ for all $b \in B_{n,r}$ and $c \in C_{n,r}$, so Lemma 10.2.1 implies that the pair $(\epsilon \cdot \varphi_b, \tilde{\varphi}_c)$ induces a GMA homomorphism $E \to M_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n])$. Pre-composing with $\rho^u : G_{\mathbb{Q},S} \to E^\times$, we obtain a representation $\rho_n^c : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n])$ satisfying the conditions in (3).

$(3) \implies (4)$: Let ρ_n^c be a deformation of ρ_0^c adapted to $\rho_{n,r}$, and let $c_{n+1} \in C^1(\mathbb{Z}/p^r\mathbb{Z}(-1))$ be the associated cochain. We have

$$dc_{n+1} = \sum_{i=1}^{n} c_i \smile a_{n+1-i} + d_i \smile c_{n+1-i}.$$

Since ρ_n is very good, we have $c_i|_p = 0$ for $i \leq n$, and so $c_{n+1} \in Z_p^1(\mathbb{Z}/p^r\mathbb{Z}(-1))$. By Proposition 6.1.6, the map

$$H^1(\mathbb{Z}/p^r\mathbb{Z}(-1)) \twoheadrightarrow H_p^1(\mathbb{Z}/p^r\mathbb{Z}(-1))$$

is surjective. Then we can subtract an element of $Z^1(\mathbb{Z}/p^r\mathbb{Z}(-1))$ from c_{n+1} to obtain an element c'_{n+1} such that $dc_{n+1} = dc'_{n+1}$ and such that $c'_{n+1}|_p = 0$. We let $\rho_n^{c\,\prime}$ be the deformation of ρ_0^c that is adapted to $\rho_{n,r}$ associated to c'_{n+1}. By Lemma 10.3.1, $\rho_n^{c\,\prime}$ is good.

(4) $\implies$ (2$'$): Let ρ_n^c be a good deformation of ρ_0^c that is adapted to $\rho_{n,r}$. This induces an $\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$-algebra homomorphism

$$E \otimes_{R,\varphi} \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n] \to M_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]).$$

By Lemma 10.2.1, this defines a homomorphism $\tilde{\varphi}_c : C_{n,r} \to \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ that, from the definition of adapted, satisfies the condition of (2').

(5) $\iff$ (3): This is Lemma A.3.4. □

10.5. **Residually upper-triangular deformations.** We consider deformations of ρ_0^b.

Lemma 10.5.1. *Let $1 \le r \le s \le t$, and let $n \ge 1$ be an integer. Suppose that ρ_n is an n-th order deformation of ρ_1 modulo p^s, and suppose that ρ_n is very good. Let $\varphi : R \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ be the corresponding homomorphism, and let D be the corresponding defining system for the Massey power $\langle M\rangle^{n+1}$. Then the following are* ***true****:*

1. *The $\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$-module $B \otimes_{R,\varphi} \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ is free of rank 1.*
2. *There is a n-th order deformation of ρ_0^b modulo p^s that is adapted to $\rho_{n,r}$ and is good.*
3. *The Massey relation for $\langle M\rangle_D^{n+1}$ holds in the $(1,2)$-coordinate modulo p^s.*

Remark 10.5.2. For $n = 1$ and $r = s = t$, we can take $\rho_n = \rho_1$, and the Massey relation for $\langle M\rangle_D^2 = M \cup M$ in the $(1,2)$-coordinate is simply $b \cup a - a \cup b = 0$. Using the skew-commutativity of the cup product, the lemma implies that $a \cup b = 0$.

Proof. By Lemma 7.2.4, B is a free R-module of rank 1. Then (1) is clear, and (2) implies (3) by Lemma A.3.4. To show (2), we follow the proof of Lemma 10.4.1, and will use the same notation of φ_b and φ_c introduced there. As in that proof, (1) implies that there is a homomorphism $\tilde{\varphi}_b : B \to \mathbb{Z}/p^r\mathbb{Z}[\epsilon_n]$ such that $\epsilon \cdot \tilde{\varphi}_b = \varphi_b$. The data $(\tilde{\varphi}_b, \epsilon \cdot \varphi_c)$ give a GMA homomorphism $E \otimes_{R,\varphi} \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n] \to M_2(\mathbb{Z}/p^s\mathbb{Z}[\epsilon_n])$, and this gives a finite-flat representation ρ_n^b that is adapted to $\rho_{n,r}$. By Lemma 10.3.1, ρ_n^b is good. □

10.6. **Residually diagonal deformations.** We consider deformations of ρ_1.

Lemma 10.6.1. *Let $1 \le r \le s \le t$, and let $n \ge 1$ be an integer. Suppose that ρ_n is a very good n-th order deformation of ρ_1 modulo p^s. Let D be the corresponding defining system for the Massey power $\langle M\rangle^{n+1}$. Then the following are equivalent:*

1. *There is an $(n+1)$-st order deformation of ρ_n modulo p^r.*
2. *There is an $(n+1)$-st order deformation of ρ_n modulo p^r that is very good.*
3. *The Massey power $\langle M\rangle_D^{n+1}$ vanishes in $H^2(\mathrm{End}(\mathbb{Z}/p^r\mathbb{Z}(1) \oplus \mathbb{Z}/p^r\mathbb{Z}))$.*

Remark 10.6.2. For $n = 1$, we can take $\rho_n = \rho_1 \otimes_{\mathbb{Z}/p^t\mathbb{Z}[\epsilon_1]} \mathbb{Z}/p^s\mathbb{Z}[\epsilon_1]$, and the Massey power $\langle M\rangle_D^{n+1} = \langle M\rangle_D^2$ is just the cup product

$$M \cup M = \begin{pmatrix} a \cup a + b \cup c & a \cup b - b \cup a \\ c \cup a - a \cup c & a \cup a + c \cup b \end{pmatrix}.$$

Using the skew-commutativity of the cup product and the fact that $a \cup b = 0$ (Remark 10.5.2), we see that $\langle M \rangle_D^2 = 0$ if and only if $a \cup c$ and $b \cup c$ are both zero.

Proof. First note that (1) is equivalent to (3) by Lemma A.2.2, and clearly (2) implies (1). It remains to show that (1) implies (2). Fix a deformation $\rho_{n+1} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}[\epsilon_{n+1}])$ of ρ_n and write

$$\rho_{n+1} = \left(1 + \sum_{i=1}^{n+1} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \epsilon^i \right) \rho_0$$

with $a_1 = a$, $b_1 = b$, $c_1 = c$ and $d_1 = -a$, and $a_i, d_i \in C^1(\mathbb{Z}/p^r\mathbb{Z})$, $b_i \in C^1(\mathbb{Z}/p^r\mathbb{Z}(1))$, $c_i \in C^1(\mathbb{Z}/p^r\mathbb{Z}(-1))$. We will construct another deformation ρ'_{n+1} of ρ_n such that ρ'_{n+1} satisfies the conditions (i), (ii), (iii) of Lemma 10.3.2.

Since ρ_{n+1} is a representation, we have

$$(*) \qquad da_{n+1} = \sum_{i=1}^{n} (a_i \smile a_{n+1-i} + b_i \smile c_{n+1-i})$$

in $C^2(\mathbb{Z}/p^r\mathbb{Z})$. Since ρ_n is very good, we have $a_i|_{I_p} = c_i|_{I_p} = 0$ for $i = 1, \dots, n$, so we see that $a_{n+1}|_{I_p}$ is a cocycle. Similarly, we can see that $d_{n+1}|_{I_p}$ and $c_{n+1}|_p$ are cocycles. As in the proof of (3) ⇒ (4) in Lemma 10.4.1, we can use Proposition 6.1.6 to show that, by subtracting a global cocycle, we can obtain elements a'_{n+1}, d'_{n+1} and c'_{n+1} satisfying $a'_{n+1}|_{I_p} = d'_{n+1}|_{I_p} = c'_{n+1}|_p = 0$.

Define $\chi'_a := \kappa_{\mathrm{cyc}}(1 + \sum_{i=1}^n a_i|_p \epsilon^i + a'_{n+1}|_p \epsilon^{n+1})$ and $\chi'_d := 1 + \sum_{i=1}^n d_i|_p \epsilon^i + d'_{n+1}|_p \epsilon^{n+1})$, and note that they are unramified deformations of $\kappa_{\mathrm{cyc}}|_p$ and $1|_p$, respectively.

Now, applying Lemma 10.5.1, we can find an n-th order deformation ρ_n^b of ρ_0^b modulo p^s that is adapted to $\rho_{n,r}$ and is good. Let $b'_{n+1} \in C^1(\mathbb{Z}/p^r\mathbb{Z}(1))$ be the cochain associated to ρ_n^b, and note that $db'_{n+1} = db_{n+1}$. Since ρ_n^b is good, $\rho_n^b|_p$ is a finite-flat extension of $\chi_d(\rho_n)$ by $\chi_a(\rho_n)$. Following Appendix C, we see that $\sum_{i=1}^n b_i|_p \epsilon^i + b'_{n+1}|_p \epsilon^{n+1}$ is a finite-flat extension of χ'_d by χ'_a, since it is obtained from $\rho_n^b|_p$ by first pulling back by $\chi'_d \twoheadrightarrow \chi_d(\rho_n)$ and then pushing out along $\chi_a(\rho_n) \cong \epsilon \chi'_a \hookrightarrow \chi'_a$.

We have now constructed cochains $a'_{n+1}, b'_{n+1}, c'_{n+1}$ and d'_{n+1} such that $da'_{n+1} = da_{n+1}$, $db'_{n+1} = db_{n+1}$, $dc'_{n+1} = dc_{n+1}$, and $dd'_{n+1} = dd_{n+1}$, and satisfying conditions (i) and (ii) of Lemma 10.3.2. To show (iii), we use:

Claim. *$a'_{n+1}|_{I_N}, b'_{n+1}|_{I_N}, c'_{n+1}|_{I_N}, d'_{n+1}|_{I_N}$ are cocycles.*

Proof. Indeed, this is clear from (the analog of) $(*)$ if $n > 1$, using the fact that ρ_n is very good. For $n = 1$, let $\sigma = x\gamma^i$ and $\tau = y\gamma^j$ with $x, y \in I_N^{\text{non-}p}$ and $i, j \in \mathbb{Z}$. By our normalizations (see (9.2.1)) we have $a(\sigma) = c(\sigma) = \bar{i}$ and $b(\sigma) = -\bar{i}$ (where $\bar{i} \in \mathbb{Z}/p^r\mathbb{Z}$ is the reduction of i). Then, by $(*)$, we have

$$da'_2(\sigma, \tau) = a(\sigma)a(\tau) + b(\sigma)c(\tau) = \bar{i}\bar{j} - \bar{i}\bar{j} = 0.$$

Since pairs (σ, τ) of this type form a dense subset of $I_N \times I_N$, and since da'_2 is continuous, we see that we see that $a'_2|_{I_N}$ is a cocycle. The proof for b, c and d is similar. □

Subtracting a multiple of a from a'_{n+1}, we can arrange so that $a'_{n+1}(\gamma) = 0$ while maintaining the properties that $da'_{n+1} = da_{n+1}$, that $a'_{n+1}|_{I_p} = 0$, and that $a'_{n+1}|_{I_N}$

is a cocycle. This implies that $a'_{n+1}|_{I_N} = 0$, since γ is a generator of the pro-p part of I_N.

Similarly, we can alter b'_{n+1}, c'_{n+1}, and d'_{n+1} so that they vanish on restriction to I_N, without changing their properties on restriction to $G_{\mathbb{Q}_p}$.

Now we define ρ'_{n+1} to be

$$\rho'_{n+1} = \left(1 + \sum_{i=1}^{n} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \epsilon^i + \begin{pmatrix} a'_{n+1} & b'_{n+1} \\ c'_{n+1} & d'_{n+1} \end{pmatrix} \epsilon^{n+1}\right) \rho_0.$$

Since $da'_{n+1} = da_{n+1}$, $db'_{n+1} = db_{n+1}$, $dc'_{n+1} = dc_{n+1}$, and $dd'_{n+1} = dd_{n+1}$, we see that ρ'_{n+1} is a deformation of ρ_n. By construction, we see that ρ'_{n+1} satisfies the conditions (i), (ii), (iii) of Lemma 10.3.2, and so ρ'_{n+1} is very good. □

Remark 10.6.3. Another way to think of this proposition is that, morally speaking, the cup products and Massey products in this paper "should be" valued in the global finite-flat cohomology group H^2_{flat} explained in §B.4.2. Then, for example, the unconditional vanishing of the Massey relation in the $(1,2)$-coordinate would follow from the fact that $H^2_{\text{flat}}(\mathbb{Z}/p^t\mathbb{Z}(1)) = 0$ (see Proposition 6.3.2).

More generally, the pattern of the arguments that relate Massey product vanishing to the existence of a global finite-flat representation has been

(1) Choose a global cochain whose coboundary is the Massey product
(2) Modify it by a global cocycle (so that its coboundary does not change) so that it is a finite-flat cocycle upon restriction to G_p.

We have developed a theory of cup products and Massey products in global finite-flat cohomology that would simplify such arguments. The same simplification can be achieved using a formulation in terms of A_∞-operations, which induces a choice of Massey products compatible with this theory; for this, see [WE18b, Thm. 3.4.1 and §12].

Since the relevant H^1_{flat} groups are 1-dimensional in each coordinate (spanned by a, b, c, and a, respectively), the resulting Massey products are unambiguously defined (i.e. various choices of defining systems result in the same Massey product) and we would not need to consider specific defining systems. However, this theory would take several pages to properly develop. More importantly, it is not necessary for our arguments because Proposition 6.1.6 implies that it suffices to test a global finite-flat Massey condition (in H^2_{flat}) as a global Massey condition (in H^2). An inductive procedure produces appropriate defining systems.

Part 3. Massey products and arithmetic

In this part, we study some analytic and algebraic number-theoretic interpretations of the vanishing of cup products and Massey products. We prove that some of the coordinate Massey relations considered in the previous part are equivalent to each other. Combining these equivalence with the results of the previous part, we prove our main result, interpreting the rank and Newton polygon of $\mathbb{T}$ in terms of Massey products. The results of this part also explain how to deduce the main results of Calegari–Emerton [CE05] (for $p > 3$) and Merel [Mer96] from our Theorem 1.2.1.

For the entirety of Part 3, we continue to fix $t = v_p(N-1) \geq 1$, and also fix an integer s with $1 \leq s \leq t$. We also let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^s})/\mathbb{Q}) \cong (\mathbb{Z}/p^s\mathbb{Z})^\times$.

11. Cup products and arithmetic

In this section, we deduce a generalization of the main result of Calegari–Emerton [CE05], relating $e = \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$ to certain class groups.

11.1. Cup products and Galois theory.

We let $\zeta_N^{(p^s)} \in \mathbb{Q}(\zeta_N)$ denote an element such that $[\mathbb{Q}(\zeta_N^{(p^s)}) : \mathbb{Q}] = p^s$. Note that $\mathbb{Q}(\zeta_N^{(p^s)})$ is the fixed field of the kernel of the homomorphism $a : G_{\mathbb{Q},S} \to \mathbb{Z}/p^t\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$.

Proposition 11.1.1.

1. *If $b \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z})$, then $\mathrm{Cl}(\mathbb{Q}(N^{1/p^s}))[p^\infty]$ admits $\mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}$ as a quotient.*
2. *If $a \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z}(-1))$, then $(\mathrm{Cl}(\mathbb{Q}(\zeta_N^{(p^s)}, \zeta_{p^s}))[p^\infty] \otimes \mathbb{Z}_p(1))^\Delta$ admits $\mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}$ as a quotient.*

Proof. Replace a, b, c with their reductions modulo p^s.

(1) Let $F \in C^1(\mathbb{Z}/p^s\mathbb{Z})$ be a cochain satisfying $dF = b \smile c$. Since $c|_p = 0$, we have that $F|_{I_p}$ is a cocycle. Just as in the proof of Lemma 10.4.1, we can subtract an element of $Z^1(\mathbb{Z}/p^s\mathbb{Z})$ from F to ensure that $F|_{I_p} = 0$. Moreover, since $dF \neq 0$, we have $F \notin Z^1(\mathbb{Z}/p^s\mathbb{Z})$.

Consider the function $\nu : G_{\mathbb{Q},S} \to \mathrm{GL}_3(\mathbb{Z}/p^s\mathbb{Z})$ given by

$$\sigma \mapsto \begin{pmatrix} 1 & c & F \\ 0 & \kappa_{\mathrm{cyc}} & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $dF = b \smile c$, we see that ν is a homomorphism. Since κ_{cyc} is unramified at N, the image of $\nu|_{I_N}$ is unipotent. Since the unipotent radical of the upper-triangular Borel in $\mathrm{GL}_3(\mathbb{Z}/p^s\mathbb{Z})$ has exponent p^s, and since $I_N^{\text{pro-}p}$ is pro-cyclic, we see that the image of $\nu|_{I_N}$ is a cyclic group. Because $b|_{I_N}, c|_{I_N}$ induce surjective homomorphisms $I_N \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$, this cyclic group has order p^s. Since $\mathbb{Q}(N^{1/p^s})/\mathbb{Q}$ is totally ramified at N, this implies that the restriction of ν to $G_{\mathbb{Q}(N^{1/p^s})}$ is unramified at N.

At the start of §9.2, we chose b to be a constant multiple of the Kummer cocycle corresponding to the chosen root N^{1/p^t} of N. Since we have now reduced b modulo p^s, $b : G_{\mathbb{Q},S} \to \mathbb{Z}/p^s\mathbb{Z}(1)$ is given by

$$\sigma \mapsto \frac{\sigma(N^{1/p^s})}{N^{1/p^s}}.$$

In particular, $b|_{G_{\mathbb{Q}(N^{1/p^s})}} = 0$. This implies that $F|_{G_{\mathbb{Q}(N^{1/p^s})}} \in Z^1(\mathbb{Q}(N^{1/p^s}), \mathbb{Z}/p^s\mathbb{Z})$, and so it corresponds to a cyclic degree p^s extension $K_F/\mathbb{Q}(N^{1/p})$ that is unramified outside Np. Since F is chosen to be unramified at p and $\nu|_{G_{\mathbb{Q}(N^{1/p^s})}}$ is unramified at N, we see that K_F is actually unramified everywhere. By class field theory, K_F is cut out by a surjection $\mathrm{Cl}(\mathbb{Q}(N^{1/p^s})) \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$.

Finally, since the image of F in $C^1(\mathbb{Z}/p^r\mathbb{Z})$ is not a cocycle for any $1 \leq r \leq s$, we see that K_F is linearly disjoint from the genus field of $\mathbb{Q}(N^{1/p^s})$, which is $\mathbb{Q}(\zeta_N^{(p^s)}, N^{1/p^s})$. Hence the two unramified degree p^s extensions of $\mathbb{Q}(N^{1/p^s})$ given by K_F and $\mathbb{Q}(\zeta_N^{(p^s)}, N^{1/p^s})$ correspond to linearly independent elements of $\mathrm{Cl}(\mathbb{Q}(N^{1/p^s}))[p^s]$ of order p^s.

(2) Similar. □

12. Cup products and Merel's number

Let $G = (\mathbb{Z}/N\mathbb{Z})^\times$, recall $1 \le s \le t = v_p(N-1)$, and let I_G be the augmentation ideal in $(\mathbb{Z}/p^s\mathbb{Z})[G]$. This section concerns Merel's number $\prod_{i=1}^{\frac{N-1}{2}} i^i$ that appears in Merel's Theorem 1.5.1, and its relation to cup products and to the "zeta element"

$$\zeta := \sum_{i \in (\mathbb{Z}/N\mathbb{Z})^\times} B_2(\lfloor i/N \rfloor)[i] \in (\mathbb{Z}/p^s\mathbb{Z})[G],$$

where $B_2(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial and where $\lfloor i/N \rfloor \in [0,1) \cap \frac{1}{N}\mathbb{Z}$ is the fractional part of i/N. We give a direct proof (not using deformation theory or modular forms) that the following four statements are equivalent:

1. $a \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z}(-1))$
2. $b \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z})$
3. Merel's number is a p^s-th power modulo N
4. $\zeta \in I_G^2$, i.e. $\mathrm{ord}_s \zeta \ge 2$.

Combining this equivalence for $s = 1$ with Theorem 1.2.1, which we will prove in §14, we have a new proof of Merel's Theorem 1.5.1 without considering the geometry of modular Jacobians. For $s = 1$, Theorem 12.5.1 (without the equivalent condition (1)) was known to Calegari and Emerton in unpublished work, but they did not know Theorem 1.2.1. We thank them for sharing their unpublished note with us.

The proof of Theorem 12.5.1 is in two steps: first to relate the vanishing of cup products to the non-vanishing of a certain Selmer group, and second to use Stickelberger theory to relate the element ζ to the Selmer group, as in the proof of Herbrand's theorem. The second step has already been carried out beautifully in the paper [Lec18b] of Lecouturier, which we use as a reference.

12.1. **Cup products and Selmer groups.** In this section, we give a simple proof that $a \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z}(-1))$ if and only if $b \cup c = 0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z})$, and relate this vanishing to the non-vanishing of certain Selmer groups. The proof relies on considering the cohomology of G_N, so we start with some remarks about it. We note that since $p^s \mid (N-1)$, there is a primitive p^s-th root of unity ζ_{p^s} in $\mathbb{Q}_N$; we fix a choice of $\zeta_{p^s} \in \mathbb{Q}_N$, and this determines isomorphisms $\mathbb{Z}/p^s\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p^s\mathbb{Z}(i)$ of G_N-modules for all i, which we will use as identifications.

By Tate duality, we have a canonical isomorphism $H^2_N(\mathbb{Z}/p^s(1)) \cong \mathbb{Z}/p^s\mathbb{Z}$, which we use as an identification. By Kummer theory, we have $H^1_N(\mathbb{Z}/p^s(1)) \cong \mathbb{Q}_N^\times \otimes \mathbb{Z}/p^s\mathbb{Z}$, and we let $\mathcal{L}_N \subset H^1_N(\mathbb{Z}/p^s\mathbb{Z}(1))$ be the free rank-1 $\mathbb{Z}/p^s\mathbb{Z}$-summand spanned by the image of N under this isomorphism. Using our identification of $H^1_N(\mathbb{Z}/p^s\mathbb{Z}(1))$ and $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$, and the canonical basis of $H^2_N(\mathbb{Z}/p^s(1))$, we can think of Tate duality as providing a symplectic pairing on the free rank-2 $\mathbb{Z}/p^s\mathbb{Z}$-module $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$.

Finally, note that since $B^1_N(\mathbb{Z}/p^t\mathbb{Z}) = 0$, we have $Z^1_N(\mathbb{Z}/p^s\mathbb{Z}) = H^1_N(\mathbb{Z}/p^s\mathbb{Z})$ and we can (and will) safely conflate cocycles with their cohomology classes.

Lemma 12.1.1. *For $i = 0, -1$, the map $H^2(\mathbb{Z}/p^s\mathbb{Z}(i)) \to H^2_N(\mathbb{Z}/p^s\mathbb{Z}(i))$ is an isomorphism.*

Proof. The map $H^2(\mathbb{Z}/p^s\mathbb{Z}(i)) \to H^2_{Np}(\mathbb{Z}/p^s\mathbb{Z}(i))$ is surjective because

$$H^3_{(c)}(\mathbb{Z}/p^s\mathbb{Z}(i)) \cong H^0(\mathbb{Z}/p^s\mathbb{Z}(1-i))^* = 0.$$

Hence the map in question is surjective, so it is enough to show that the two groups have the same cardinality. We are reduced to showing that $\#H^2(\mathbb{Z}/p^s\mathbb{Z}(i)) = p^s$.

Write $h^j(\mathbb{Z}/p^s\mathbb{Z}(i)) = \#H^j(\mathbb{Z}/p^s\mathbb{Z}(i))$. By the global Euler characteristic formula (see, for example, [NSW08, Corollary 8.7.5, pg. 509]), we have

$$h^2(\mathbb{Z}/p^s\mathbb{Z}) = \frac{h^1(\mathbb{Z}/p^s\mathbb{Z})}{h^0(\mathbb{Z}/p^s\mathbb{Z})}, \quad h^2(\mathbb{Z}/p^s\mathbb{Z}(-1)) = \frac{h^1(\mathbb{Z}/p^s\mathbb{Z}(-1))}{h^0(\mathbb{Z}/p^s\mathbb{Z}(-1)) \cdot p^s}.$$

One sees easily that $h^1(\mathbb{Z}/p^s\mathbb{Z}) = p^{2s}$ and $h^0(\mathbb{Z}/p^s\mathbb{Z}) = p^s$, so $h^2(\mathbb{Z}/p^s\mathbb{Z}) = p^s$. We also have $h^0(\mathbb{Z}/p^s\mathbb{Z}(-1)) = 1$, and, by Lemma 6.3.6, $h^1(\mathbb{Z}/p^s\mathbb{Z}(-1)) = p^{2s}$, so $h^2(\mathbb{Z}/p^s\mathbb{Z}(-1)) = p^s$. □

Proposition 12.1.2. *For $i = 0, 1$, there is a commutative diagram*

$$\begin{tikzcd}
H^1(\mathbb{Z}/p^s\mathbb{Z}(i)) \times H^1(\mathbb{Z}/p^s\mathbb{Z}(-1)) \arrow[r, "\cup"] \arrow[d, "|_N"] & H^2(\mathbb{Z}/p^s\mathbb{Z}(i-1)) \arrow[d, "\wr"] \\
H^1_N(\mathbb{Z}/p^s\mathbb{Z}(i)) \times H^1_N(\mathbb{Z}/p^s\mathbb{Z}(-1)) \arrow[r, "\cup"] & H^2_N(\mathbb{Z}/p^s\mathbb{Z}(i-1)).
\end{tikzcd}$$

In particular, for $x \in H^1(\mathbb{Z}/p^s\mathbb{Z}(i))$ and $y \in H^1(\mathbb{Z}/p^s\mathbb{Z}(-1))$, we have $x \cup y = 0$ if and only if $x|_N \cup y|_N = 0$.

Proof. The commutativity is clear, so this follows from the previous lemma. □

Lemma 12.1.3. *Under our identification $H^1_N(\mathbb{Z}/p^s\mathbb{Z}) = H^1_N(\mathbb{Z}/p^s\mathbb{Z}(1))$, both of the elements $a|_N$ and $b|_N$ are generators of $\mathcal{L}_N \subset H^1_N(\mathbb{Z}/p^s\mathbb{Z})$.*

Proof. We know that neither $a|_N$ nor $b|_N$ is divisible by p because their value on γ is ±1. So it will suffice to show that $a|_N, b|_N \in \mathcal{L}_N$.

We have $b|_N \in \mathcal{L}_N$ by Proposition 6.3.2. Since the Tate pairing is symplectic, to show that $a|_N \in \mathcal{L}_N$, it is enough to show that $a|_N \cup b|_N = 0$. But we know that $a \cup b = 0$ by Lemma 10.5.1, so we are done by the previous proposition. □

Let $H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1))$ denote the Selmer group

$$H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1)) := \ker\left(H^1(\mathbb{Z}/p^s\mathbb{Z}(-1)) \to H^1_p(\mathbb{Z}/p^s\mathbb{Z}(-1)) \oplus H^1_N(\mathbb{Z}/p^s\mathbb{Z})/\mathcal{L}_N\right).$$

Let $H^1_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2))$ denote the "dual" Selmer group

$$H^1_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) := \ker\left(H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \to H^1_N(\mathbb{Z}/p^s\mathbb{Z})/\mathcal{L}_N\right).$$

Proposition 12.1.4. *The following are equivalent:*

(1) $a \cup c = 0$ *in* $H^2(\mathbb{Z}/p^s\mathbb{Z}(-1))$
(2) $b \cup c = 0$ *in* $H^2(\mathbb{Z}/p^s\mathbb{Z})$
(3) *The image of* $c|_N$ *in* $H^1_N(\mathbb{Z}/p^s\mathbb{Z}(-1))$ *is in the subgroup* $\mathcal{L}_N$
(4) $H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1)) \simeq \mathbb{Z}/p^s\mathbb{Z}$
(5) $H^1_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \simeq \mathbb{Z}/p^s\mathbb{Z}$
(6) *There is an element* $x \in H^1(\mathbb{Z}/p^s\mathbb{Z}(2))$ *with non-zero image in* $H^1(\mathbb{Z}/p\mathbb{Z}(2))$ *such that* $x|_N \in \mathcal{L}_N$.

Remark 12.1.5. By Remark 10.6.2, and using the notation from there, we see that all these items are also equivalent to $\langle M\rangle^2_D$ being zero in $H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$.

Proof. The equivalence of (1)-(3) follows from Proposition 12.1.2, Lemma 12.1.3, and the fact that the Tate pairing is symplectic.

By the definition of $H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1))$, we have

$$H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1)) = \{x \in H^1_{(p)}(\mathbb{Z}/p^s\mathbb{Z}(-1)) \mid x|_N \in \mathcal{L}_N\}.$$

Since $H^1_{(p)}(\mathbb{Z}/p^s\mathbb{Z}(-1)) \simeq \mathbb{Z}/p^s\mathbb{Z}$ is generated by c, we see that (3) and (4) are equivalent.

By duality (Theorem B.3.2), we have $H^1_\Sigma(\mathbb{Z}/p^s\mathbb{Z}(-1)) = H^2_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2))^*$, so (4) is equivalent to $H^2_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \simeq \mathbb{Z}/p^s\mathbb{Z}$. Here $H^2_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2))$ fits into an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow H^1_N(\mathbb{Z}/p^s\mathbb{Z}(2))/\mathcal{L}_N \\ \longrightarrow H^2_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow H^2(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow H^2_{Np}(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow 0. \end{aligned}$$

As in the proof of Proposition 6.3.3, the last map $H^2(\mathbb{Z}/p^s\mathbb{Z}(2)) \to H^2_{Np}(\mathbb{Z}/p^s\mathbb{Z}(2))$ is an isomorphism, so we have an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow \\ H^1_N(\mathbb{Z}/p^s\mathbb{Z}(2))/\mathcal{L}_N \longrightarrow H^2_{\Sigma^\perp}(\mathbb{Z}/p^s\mathbb{Z}(2)) \longrightarrow 0. \end{aligned}$$

By Lemma 6.3.5, we have $H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \cong H^2(\mathbb{Z}_p(2))[p^s] \simeq \mathbb{Z}/p^s\mathbb{Z}$, and we see that $x \in H^1(\mathbb{Z}/p^s\mathbb{Z}(2))$ is a generator if and only if its image in $H^1(\mathbb{Z}/p\mathbb{Z}(2))$ is non-zero. Since $H^1_N(\mathbb{Z}/p^s\mathbb{Z}(2))/\mathcal{L}_N$ is also free $\mathbb{Z}/p^s\mathbb{Z}$-module of rank 1 (see Lemma 6.3.4), this gives the equivalence of (4)-(6). □

In the end, we use condition (6) to relate cup products to Merel's number.

12.2. **Results of Lecouturier.** We follow [Lec18b]. Choose a surjective homomorphism $\log : \mathbb{Z}_N^\times \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$; it factors through a map $\mathbb{F}_N^\times \twoheadrightarrow \mathbb{Z}/p^s\mathbb{Z}$, which we also denote by log. Note that Merel's number is a p^s-th power modulo N if and only if $\sum_{i=1}^{\frac{N-1}{2}} i\log(i) = 0$ in $\mathbb{Z}/p^s\mathbb{Z}$.

Lemma 12.2.1. *We have the equality*

$$\sum_{i=1}^{N-1} i^2 \log(i) = -\frac{4}{3}\sum_{i=1}^{\frac{N-1}{2}} i\log(i)$$

in $\mathbb{Z}/p^s\mathbb{Z}$.

Proof. This is [Lec18b, Prop. 1.2]. □

Let $\Lambda : \mathbb{Q}_N^\times \otimes_\mathbb{Z} \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^s\mathbb{Z}$ be defined by $\Lambda(N^k x \otimes \alpha) = \alpha\log(x)$ for $k \in \mathbb{Z}$, $x \in \mathbb{Z}_N^\times$ and $\alpha \in \mathbb{Z}/p^s\mathbb{Z}$.

Choose a prime ideal $\mathfrak{n} \subset \mathbb{Z}[\zeta_p]$ lying over N, so that the completion of $\mathbb{Q}(\zeta_p)$ at $\mathfrak{n}$ is $\mathbb{Q}_N$. For $x \in \mathbb{Q}(\zeta_p)$, let $x_\mathfrak{n} \in \mathbb{Q}_N$ denote the image in this completion. Finally, for a $\mathbb{Z}[\frac{1}{p-1}][\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$-module M and a character $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$, let M_χ denote the χ-eigenspace.

Proposition 12.2.2. *There is an element $\mathcal{G} \in (\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{Z}_p)_{\omega^{-1}}$ such that*

$$\Lambda(\mathcal{G}_\mathfrak{n}) = -\frac{2}{3}\sum_{i=1}^{\frac{N-1}{2}} i\log(i).$$

and whose natural image in $(\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{F}_p)_{\omega^{-1}}$ is non-trivial.

Proof. Let $e_{\omega^{-1}} \cdot \mathcal{G} \in (\mathbb{Z}[1/N, \zeta_{Np}]^\times \otimes \mathbb{Z}_p)_{\omega^{-1}}$ be the element defined in [Lec18b, §3.3]; it is a product of conjugates of Gauss sums. By [Lec18b, Prop. 3.4], we actually have $e_{\omega^{-1}} \cdot \mathcal{G} \in (\mathbb{Z}[1/N, \zeta_p]^\times \otimes \mathbb{Z}_p)_{\omega^{-1}}$.

Let $\beta = \sum_{i=1}^{p-1} \omega(i)i \in \mathbb{Z}_p$; as is well-known, $\beta = py$ for some $y \in \mathbb{Z}_p^\times$. Using the Gross–Koblitz formula, Lecouturier computes that

$$(e_{\omega^{-1}} \cdot \mathcal{G})_{\mathfrak{n}} = (-N \otimes y) \cdot \left(\prod_{i=1}^{p-1} \Gamma_N \left(\frac{i}{p} \right) \otimes \omega(i) \right) \in \mathbb{Q}_N^\times \otimes \mathbb{Z}_p \tag{12.2.3}$$

where Γ_N is the N-adic Gamma function. In particular, $(e_{\omega^{-1}} \cdot \mathcal{G})_{\mathfrak{n}}$ is not in the image of $\mathbb{Z}_N^\times \otimes \mathbb{Z}_p \to \mathbb{Q}_N^\times \otimes \mathbb{Z}_p$, so its image in $(\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{F}_p)_{\omega^{-1}}$ is non-trivial.

Finally, the formula for $\Lambda((e_{\omega^{-1}} \cdot \mathcal{G})_{\mathfrak{n}})$ follows by (12.2.3) and the formula

$$\sum_{j=1}^{p-1} j \log \left(\Gamma_N \left(\frac{j}{p} \right) \right) = -\frac{2}{3} \sum_{i=1}^{\frac{N-1}{2}} i \log(i)$$

obtained by combining [Lec18b, Lem. 4.3] (with $\chi = \omega^{-1}$) with Lemma 12.2.1. □

12.3. **Merel's number and the zeta element.** Recall the zeta element $\zeta \in \mathbb{Z}/p^s\mathbb{Z}[G]$ defined at the start of this section. Let $\mathrm{ord}_s\zeta$ denoted the greatest integer r such that $\zeta \in I_G^r$, where $I_G \subset \mathbb{Z}/p^s\mathbb{Z}[G]$ is the augmentation ideal. We now show, following Lecouturier, how Theorem 1.5.2 follows from Merel's result (Theorem 1.5.1).

Lemma 12.3.1. *The following are equivalent:*

1. *Merel's number is a p^s-th power modulo N*
2. $\mathrm{ord}_s\zeta \geq 2$.

Proof. We first note that $\zeta \in I_G$ because $s \leq t = v_p(N-1)$. Furthermore, we recall that there is an isomorphism

$$I_G/I_G^2 \xrightarrow{\sim} G \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} \xrightarrow{\log} \mathbb{Z}/p^s\mathbb{Z}$$

sending $[g] - 1 \in I_G$ to $\log(g)$ for $g \in G$. Under this isomorphism, $\zeta \pmod{I_G^2}$ is sent to

$$\sum_{i=1}^{N-1} (i^2 - i + 1/6) \log(i).$$

One sees easily that $\sum_{i=1}^{N-1} \log(i)$ and $\sum_{i=1}^{N-1} i \log(i)$ are both 0 in $\mathbb{Z}/p^s\mathbb{Z}$. Then $\mathrm{ord}_2\zeta \geq 2$ if and only if $\sum_{i=1}^{N-1} i^2 \log(i) = 0$. The lemma now follows from Lemma 12.2.1. □

12.4. **Hochschild–Serre arguments.** Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^s})/\mathbb{Q}) \cong (\mathbb{Z}/p^s\mathbb{Z})^\times$ and let $\Delta^0 \cong (\mathbb{Z}/p\mathbb{Z})^\times$ denote the prime-to-p subgroup, so $\Delta \cong \Delta^0 \times \Delta_p$, where $\Delta_p \simeq \mathbb{Z}/p^{s-1}\mathbb{Z}$.

Lemma 12.4.1. *Let n be an integer such that $(p-1) \nmid n$. Then, for all $i \geq 0$, we have*

$$H^i(\Delta, \mathbb{Z}/p^s\mathbb{Z}(n)) = 0.$$

Proof. Since $\Delta^0 \subset \Delta$ is prime-to-p, we have

$$H^i(\Delta, \mathbb{Z}/p^s\mathbb{Z}(n)) = H^i(\Delta_p, H^0(\Delta^0, \mathbb{Z}/p^s\mathbb{Z}(n))).$$

Let $\zeta_{p-1} \in (\mathbb{Z}/p^s\mathbb{Z})^\times$ be a primitive $(p-1)$-st root of unity. Then

$$H^0(\Delta^0, \mathbb{Z}/p^s\mathbb{Z}(n)) = \{x \in \mathbb{Z}/p^s\mathbb{Z} \mid \zeta_{p-1}^n x = x\}.$$

Since $(p-1) \nmid n$, we see that $\zeta_{p-1}^n \not\equiv 1 \pmod{p}$. Hence $H^0(\Delta^0, \mathbb{Z}/p^s\mathbb{Z}(n)) = 0$. □

Lemma 12.4.2. *Let n be an integer such that $(p-1) \nmid n$. Then*

$$H^1(\mathbb{Z}/p^s\mathbb{Z}(n)) = H^1(\mathbb{Z}[1/Np, \zeta_{p^s}], \mathbb{Z}/p^s\mathbb{Z}(n))^\Delta.$$

Proof. Note that $H^0(\mathbb{Z}[1/Np, \zeta_{p^s}], \mathbb{Z}/p^s\mathbb{Z}(n)) \cong \mathbb{Z}/p^s\mathbb{Z}(n)$ as Δ-modules. Then, by the Hochschild–Serre spectral sequence, there is an exact sequence

$$H^1(\Delta, \mathbb{Z}/p^s\mathbb{Z}(n)) \longrightarrow H^1(\mathbb{Z}/p^s\mathbb{Z}(n)) \longrightarrow H^1(\mathbb{Z}[1/Np, \zeta_{p^s}], \mathbb{Z}/p^s\mathbb{Z}(n))^\Delta \\ \longrightarrow H^2(\Delta, \mathbb{Z}/p^s\mathbb{Z}(n)),$$

so this follows from the previous lemma. □

12.5. Merel's number and cup products.

We can now complete the proof of the following theorem.

Theorem 12.5.1. *The following are equivalent:*

1. $a \cup c = 0$ *in* $H^2(\mathbb{Z}/p^s\mathbb{Z}(-1))$
2. $b \cup c = 0$ *in* $H^2(\mathbb{Z}/p^s\mathbb{Z})$
3. *Merel's number is a p^s-th power modulo N*
4. $\mathrm{ord}_s(\zeta) \geq 2$.

Proof. By Proposition 12.1.4 and Lemma 12.3.1, we are reduced to showing that Merel's number is a p^s-th power modulo N if and only if there exists some $x \in H^1(\mathbb{Z}/p^s\mathbb{Z}(2))$ with non-zero image in $H^1(\mathbb{Z}/p\mathbb{Z}(2))$ such that $x|_N \in \mathcal{L}_N$.

By Lemma 12.4.2 (and with the notation there), we have

$$H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) = H^1(\mathbb{Z}[1/Np, \zeta_{p^s}], \mathbb{Z}/p^s\mathbb{Z}(2))^\Delta = (H^1(\mathbb{Z}[1/Np, \zeta_{p^s}], \mathbb{Z}/p^s\mathbb{Z}(1))(1)^\Delta.$$

Then, by Kummer theory, we have an isomorphism

$$\iota : H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \cong (\mathbb{Z}[1/Np, \zeta_{p^s}]^\times \otimes \mathbb{Z}/p^s\mathbb{Z}(1))^\Delta.$$

There is a commutative diagram

$$\begin{tikzcd}
(\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{Z}_p)_{\omega^{-1}} \arrow[r, "j"] \arrow[d] & (\mathbb{Z}[1/Np, \zeta_{p^s}]^\times \otimes \mathbb{Z}/p^s\mathbb{Z}(1))^\Delta \arrow[r, "\sim"] \arrow[d] & H^1(\mathbb{Z}/p^s\mathbb{Z}(2)) \arrow[d] \\
(\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{F}_p)_{\omega^{-1}} \arrow[r, equal] & (\mathbb{Z}[1/Np, \zeta_p]^\times \otimes \mathbb{Z}/p\mathbb{Z}(1))^\Delta \arrow[r, "\sim"] & H^1(\mathbb{Z}/p\mathbb{Z}(2)),
\end{tikzcd}$$

where j is induced by the inclusion $\mathbb{Z}[1/Np, \zeta_p]^\times \subset \mathbb{Z}[1/Np, \zeta_{p^s}]^\times$. Letting $x = \iota^{-1}(j(\mathcal{G}))$, where $\mathcal{G}$ is as in Proposition 12.2.2, we see that the image of x in $H^1(\mathbb{Z}/p\mathbb{Z}(2))$ is non-zero. We have $x|_N \in \mathcal{L}_N$ if and only if $\Lambda(\mathcal{G}_\mathfrak{n}) = 0$, and by Proposition 12.2.2, this happens if and only if Merel's number is a p^s-th power modulo N. □

Taking $s = 1$ in the theorem gives Proposition 1.5.3 from the introduction.

13. Equivalence of Massey products

In the previous section, we gave a direct algebraic proof that $a \cup c = 0$ if and only if $b \cup c = 0$. In this section, we prove the analogous result for higher Massey powers – namely, that the Massey relations in the $(1,1)$, $(2,1)$ and $(2,2)$ coordinates are all equivalent.

To state the result, we fix $n \geq 2$ and $s \leq t$ and assume that we have a very good deformation $\rho_n : G_{\mathbb{Q},S} \to \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n]$ of $\rho_1 \otimes_{\mathbb{Z}/p^t\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}$, which we write as

$$\rho_n = \begin{pmatrix} \kappa_{\mathrm{cyc}} & 0 \\ 0 & 1 \end{pmatrix} + \sum_{i=1}^{n} \begin{pmatrix} \kappa_{\mathrm{cyc}} a_i & b_i \\ \kappa_{\mathrm{cyc}} c_i & d_i \end{pmatrix} \epsilon^i$$

with $a_1 = a \pmod{p^s}$, etc. Let D be the associated defining system for the Massey power $\langle M \rangle^{n+1}$.

Proposition 13.0.1. *The $\mathbb{Z}/p^s\mathbb{Z}$-valued 1-cochains $a_n|_N, b_n|_N, c_n|_N, d_n|_N$ are 1-cocycles, i.e. they lie in $Z^1_N(\mathbb{Z}/p^s\mathbb{Z})$. In addition,*

(1) $a_n|_N = -d_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$,
(2) $a_n|_N = -b_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$,
(3) The Massey relation for $\langle M \rangle^{n+1}_D$ in the $(1,1)$-coordinate holds modulo p^s if and only if $c_n|_N \equiv -b_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$,
(4) The Massey relation for $\langle M \rangle^{n+1}_D$ in the $(2,1)$-coordinate holds modulo p^s if and only if $c_n|_N \equiv a_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$
(5) The Massey relation for $\langle M \rangle^{n+1}_D$ in the $(2,2)$-coordinate holds modulo p^s if and only if $c_n|_N \equiv -b_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})$.

In particular, the Massey relation for $\langle M \rangle^{n+1}_D$ modulo p^s in the $(1,1)$, $(2,1)$ and $(2,2)$-coordinates are all equivalent to $\langle M \rangle^{n+1}_D$ vanishing in $H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1) \oplus \mathbb{Z}/p^s\mathbb{Z}))$.

Proof. The final statement of the proposition follows from Lemmas 10.5.1 and A.3.2.

As in the previous section, since $H^1_N(\mathbb{Z}/p^s\mathbb{Z}) = Z^1_N(\mathbb{Z}/p^s\mathbb{Z})$, we conflate 1-cocycles with their cohomology classes. Since $n \geq 2$, by Lemma 10.6.1, we have $M \cup M = 0$, which implies that $a \cup c = 0$. By Proposition 12.1.4, this implies that $c|_N \in \mathcal{L}_N \subset H^1_N(\mathbb{Z}/p^s\mathbb{Z})$. Then, by Lemma 12.1.3, we have $a|_N, b|_N, c|_N, d|_N \in \mathcal{L}_N$, where $d = -a$. We may write them as multiples of $[N]$, the Kummer class of N. Write $b|_N = x[N]$ with $x \in (\mathbb{Z}/p^t\mathbb{Z})^\times$. By our normalizations (9.2.1), we have $a|_N = c|_N = -x[N]$ and $d|_N = x[N]$, as elements of $Z^1_N(\mathbb{Z}/p^s\mathbb{Z})$.

By induction, we may assume that $a_i|_N = c_i|_N = -b_i|_N = -d_i|_N$ for $i = 1, \dots, n-1$. We first prove that $a_n|_N$ is a cocycle. Note that

$$da_n = \sum_{i=1}^{n-1} a_i \smile a_{n-i} + b_i \smile c_{n-i}.$$

Restricting to G_N, we have by induction

$$\begin{aligned} da_n|_N &= \sum_{i=1}^{n-1} a_i|_N \smile a_{n-i}|_N + b_i|_N \smile c_{n-i}|_N \\ &= \sum_{i=1}^{n-1} c_i|_N \smile c_{n-i}|_N + (-c_i|_N) \smile c_{n-i}|_N = 0. \end{aligned}$$

Hence $a_n|_N \in Z^1_N(\mathbb{Z}/p^s\mathbb{Z})$. Similarly for b_n, c_n, d_n.

(1) Since $\det(\rho_n) = \kappa_{\mathrm{cyc}}$, we have

$$a_n + d_n = \sum_{i=1}^{n-1} b_i c_{n-i} - a_i d_{n-i}.$$

Using the induction hypotheses, this implies that

$$\begin{aligned} a_n|_N + d_n|_N &= \sum_{i=1}^{n-1} b_i|_N c_{n-i}|_N - a_i|_N d_{n-i}|_N \\ &= \sum_{i=1}^{n-1} (-c_i|_N) c_{n-i}|_N - (c_i|_N)(-c_{n-i}|_N) = 0. \end{aligned}$$

(2) By Lemma 10.5.1, the Massey relation for $\langle M \rangle_D^{n+1}$ in the $(1,2)$-coordinate holds. In other words, the class of the cocycle

$$\sum_{i=1}^{n} a_i \smile b_{n-i+1} + b_i \smile d_{n-i+1}$$

is 0 in $H^2(\mathbb{Z}/p^s\mathbb{Z}(1))$. Restricting to $H^2_N(\mathbb{Z}/p^s\mathbb{Z}(1))$ and applying (1) and the induction hypotheses, we find

$$\begin{aligned} 0 &= \sum_{i=1}^{n} a_i|_N \smile b_{n-i+1}|_N + b_i|_N \smile d_{n-i+1}|_N \\ &= \sum_{i=2}^{n-1} (c_i|_N \smile (-c_{n-i+1}|_N) + (-c_i|_N) \smile (-c_{n-i+1}|_N)) \\ &\qquad + x(-[N] \smile b_n|_N + [N] \smile (-a_n|_N) + a_n|_N \smile [N] + b_n|_N \smile [N]) \\ &= x(-[N] \smile b_n|_N + [N] \smile (-a_n|_N) + a_n|_N \smile [N] + b_n|_N \smile [N]) \\ &= x(-[N] \smile (a_n|_N + b_n|_N) + (a_n|_N + b_n|_N) \smile [N]) \\ &= 2x(a_n|_N + b_n|_N) \smile [N]. \end{aligned}$$

Since $2x \in (\mathbb{Z}/p^s\mathbb{Z})^\times$, the fact that the Tate pairing is symplectic implies that the class of $a_n|_N + b_n|_N$ in $H^1_N(\mathbb{Z}/p^s\mathbb{Z})/\mathcal{L}_N$ is zero. Since ρ_n is very good, both a_n and b_n are unramified at N, so this implies that $a_n|_N = -b_n|_N$.

(3) Let $\alpha \in Z^2(\mathbb{Z}/p^s\mathbb{Z})$ denote the cocycle

$$\alpha = \sum_{i=1}^{n} a_i \smile a_{n+1-i} + b_i \smile c_{n+1-i}.$$

The Massey relation for $\langle M\rangle^{n+1}$ in the $(1,1)$-coordinate holds modulo p^s if and only if $[\alpha]=0$ in $H^2(\mathbb{Z}/p^s\mathbb{Z})$. By Lemma 12.1.1, this is equivalent to the equation $[\alpha|_N]=0$ in $H^2_N(\mathbb{Z}/p^s\mathbb{Z})$. Using (2), this equation can be simplified to $2x[N]\smile(b_n|_N+c_n|_N)=0$. Then we apply the same kind of final argument as in the proof of (2).

The remaining parts are similar. □

14. Main result

Let $e=\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}^0)$. Recall the sequence $t=t_1\geq\cdots\geq t_e>t_{e+1}=0$, defined in Proposition 8.2.1. This sequence is invariant of $\mathbb{T}$ that determines its Newton polygon, but may even be finer than it. In this section, we complete the proof of our main theorem, which is an inductive procedure: assuming we know $t_1,\dots,t_n$, we describe t_{n+1} in terms of Massey products.

Theorem 14.0.1. *Let n and s be integers such that $1\leq n\leq e$ and $1\leq s\leq t_n$. Then there is a very good n-th order deformation ρ_n of ρ_1 modulo p^{t_n}.*

Fix such an ρ_n, and let D be the corresponding defining system for the Massey power $\langle M\rangle^{n+1}$ modulo p^{t_n}. Then the following are equivalent:

(1) We have $s\leq t_{n+1}$.

(2) The Massey power $\langle M\rangle^{n+1}_D$ vanishes in $H^2(\mathrm{End}(\mathbb{Z}/p^s\mathbb{Z}(1)\oplus\mathbb{Z}/p^s\mathbb{Z}))$.

Proof. We first prove that (1) and (2) are equivalent, assuming the existence of ρ_n. Let $\varphi:R\twoheadrightarrow\mathbb{Z}/p^{t_n}\mathbb{Z}[\epsilon_n]$ be the corresponding surjective homomorphism. Let $z\in J^{\min}$ be a generator such that $\varphi(z)=\epsilon$. Then (1) is equivalent to

(1)' There is a surjective homomorphism $\varphi':R\twoheadrightarrow\mathbb{Z}/p^s\mathbb{Z}[\epsilon_{n+1}]$ such that the following diagram commutes

$$\begin{tikzcd}
R \arrow[r, "\varphi'"] \arrow[d, "\varphi"'] & \mathbb{Z}/p^s\mathbb{Z}[\epsilon_{n+1}] \arrow[d] \\
\mathbb{Z}/p^{t_n}\mathbb{Z}[\epsilon_n] \arrow[r] & \mathbb{Z}/p^s\mathbb{Z}[\epsilon_n],
\end{tikzcd}$$

where the unlabeled arrows are the quotient maps.

Indeed, by Proposition 8.2.1, (1) implies the existence of a homomorphism φ' such that $\varphi'(z)=\epsilon$, and such a homomorphism makes the diagram commute. Conversely, any φ' as in (1)' must satisfy $\varphi(z')=\epsilon$ for some generator $z'\in J^{\min}$, which, by Proposition 8.2.1, implies (1).

By Lemma 10.4.1, (1)' is equivalent to the Massey relation for $\langle M\rangle^{n+1}_D$ in the $(2,1)$-coordinate modulo p^s. This is equivalent to (2) by Proposition 13.0.1 (and by Remark 12.1.5 for $n=1$).

Now we prove that ρ_n exists by induction on n, the base case $n=1$ being vacuous. Assume that ρ_{n-1} exists modulo $p^{t_{n-1}}$, and let D' be the corresponding corresponding defining system for the Massey power $\langle M\rangle^n$ modulo $p^{t_{n-1}}$. By the equivalence of (1) and (2) already proven, we see that the Massey power $\langle M\rangle^n_{D'}$ vanishes in $H^2(\mathrm{End}(\mathbb{Z}/p^{t_n}\mathbb{Z}(1)\oplus\mathbb{Z}/p^{t_n}\mathbb{Z}))$. By Lemma 10.6.1, there is a very good n-th order deformation of ρ_{n-1} modulo p^{t_n}, which we can take as ρ_n. □

Remark 14.0.2. Note that since (1) in the theorem does not depend on the choice of defining system D, the vanishing behavior of the Massey power $\langle M\rangle^{n+1}_D$ does not depend on the choice of D (as long as it is associated to a very good n-th order deformation).

We now explain how to deduce the results stated in the introduction from this main theorem. For $n = 1$ in the theorem, we let $\rho_n = \rho_1$ and observe that $e \geq 2$ if and only if $t_2 > 0$ if and only if $\langle M \rangle_D^2 = M \cup M$ vanishes in $H^2(\mathrm{End}(\mathbb{F}_p(1) \oplus \mathbb{F}_p))$. This is equivalent to $b \cup c = 0$ and to $a \cup c = 0$ (see Remark 12.1.5). This proves Theorem 1.2.1. Corollary 1.2.2 follows from this and Proposition 11.1.1.

Finally, to prove Theorem 1.4.1, we note that if Merel's number is not a p^2-th power, then Theorem 12.5.1 implies that $b \cup c$ is non-zero in $H^2(\mathbb{Z}/p^2\mathbb{Z})$, which implies that $M \cup M$ is non-zero in $H^2(\mathrm{End}(\mathbb{Z}/p^2\mathbb{Z}(1) \oplus \mathbb{Z}/p^2\mathbb{Z}))$. By the main theorem, this implies that $t_2 \leq 1$, which implies Theorem 1.4.1 by standard properties of Newton polygons.

Part 4. Appendices

In the appendices, we collect some formal results. With the possible exception of §A.3 and §B.4, the contents are standard and will be known to experts. We include them here for completeness and to fix notation.

Appendix A. Massey products

Massey products are a generalization of cup products. They were first introduced in topology by Massey and Uehara–Massey [Mas58, UM57]. For an introduction to the subject, see Kraines [Kra66] and May [May69]. Massey products are closely related to A_∞-operations; see e.g. [WE18b, Part 2] for this relation, and the connection with deformation theory. For applications of Massey products in Galois cohomology, see Sharifi [Sha07].

In this section, we collect some statements that we will need and define "Massey powers." We do not give proofs, as all the results either follow immediately from the definitions or by a purely formal computation.

In this section, we let G be a group, A be a ring, and V a $A[G]$-module equipped with a pairing $V \otimes V \to V$. Given $a \in C^i(G,V)$, $b \in C^j(G,V)$ we let $a \smile b \in C^{i+j}(G,V)$ denote the composite of the usual cup product with the pairing $V \otimes V \to V$:

$$C^i(G,V) \times C^j(G,V) \to C^{i+j}(G, V \otimes V) \to C^{i+j}(G,V).$$

A.1. Massey products.

Definition A.1.1. Let $a_1, \dots, a_n \in C^1(G,V)$ be cochains. We say that a set $D = \{a(i,j) : 1 \leq i \leq j \leq n, (i,j) \neq (1,n)\} \subset C^1(G,V)$ is a *defining system for the Massey product* $\langle a_1, \dots, a_n \rangle$ if

(1) $a(i,i) = a_i$ for all $i = 1, \dots n$, and

(2) $da(i,j) = \displaystyle\sum_{k=i}^{j-1} a(i,k) \smile a(k+1,j)$ for all i,j.

In particular, (1) and (2) for $i = j$ imply that $da(i,i) = da_i = 0$ for all i.

If D is a defining system for the Massey product $\langle a_1, \dots, a_n \rangle$, then we note that

$$c(D) = \sum_{k=1}^{n-1} a(1,k) \smile a(k+1,n)$$

is an element of $Z^2(G,V)$ and we let $\langle a_1,\dots,a_n\rangle_D \in H^2(G,V)$ be the class of $c(D)$. We let

$$\langle a_1,\dots,a_n\rangle = \{\langle a_1,\dots,a_n\rangle_D\} \subset H^2(G,V)$$

where D ranges over all defining systems.

We say that $\langle a_1,\dots,a_n\rangle$ is *defined* if it is non-empty (i.e. if there exists a defining system). We say that $\langle a_1,\dots,a_n\rangle$ *vanishes* if $0 \in \langle a_1,\dots,a_n\rangle$.

It is known that the set $\langle a_1,\dots,a_n\rangle$ only depends on the cohomology classes of $a_1,\dots,a_n$ [Kra66, Thm. 3].

Example A.1.2. If $n = 2$, then the Massey product is defined if and only if $a_1, a_2 \in Z^1(G,V)$. If they are, then $D = \{a(1,1) = a_1, a(2,2) = a_2\}$ is the only defining system, and $\langle a_1,a_2\rangle_D = [a_1 \smile a_2]$.

Example A.1.3. Take $V = A$ with trivial G-action. Suppose that $D = \{a(i,j) : 1 \le i \le j \le n, (i,j) \neq (1,n)\} \subset C^1(G,A)$ is a defining system. Condition (2) implies that the the cochains $\nu_1,\nu_2 \in C^1(G,M_n(A))$ given by

$$\nu_1 = \begin{pmatrix} 1 & a(1,1) & a(1,2) & \cdots & a(1,n-1) \\ 0 & 1 & a(2,2) & \cdots & a(2,n-1) \\ \cdots & & & & \\ 0 & \cdots & & 1 & a(n-1,n-1) \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$$

and

$$\nu_2 = \begin{pmatrix} 1 & a(2,2) & a(2,3) & \cdots & a(2,n) \\ 0 & 1 & a(3,3) & \cdots & a(3,n) \\ \cdots & & & & \\ 0 & \cdots & & 1 & a(n,n) \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$$

are cocycles (i.e. ν_1 and ν_2 are homomorphisms). Notice that ν_1 and ν_2 have a $n-1 \times n-1$-submatrix in common. The class $\langle a_1,\dots,a_n\rangle_D \in H^2(G,A)$ measures the obstruction to concatenating ν_1 and ν_2, in the following sense. If $\langle a_1,\dots,a_n\rangle_D = 0$, then there exists $a \in C^1(G,A)$ such that $da = c(D)$ and the cochain $\nu \in C^1(G,M_{n+1}(A))$ given by

$$\nu = \begin{pmatrix} 1 & a(1,1) & a(1,2) & \cdots & a(1,n-1) & a \\ 0 & 1 & a(2,2) & \cdots & a(2,n-1) & a(2,n) \\ \cdots & & & & & \\ 0 & \cdots & & 1 & a(n-1,n-1) & a(n-1,n) \\ 0 & \cdots & & & 1 & a(n,n) \\ 0 & \cdots & & & 0 & 1 \end{pmatrix}$$

is a cocycle. Moreover, if $\langle a_1,\dots,a_n\rangle_D \neq 0$, then no such ν exists.

A.2. **Massey powers.** We remark that "Massey power" is not standard terminology; we use it to refer to certain Massey products. More precisely, a Massey power is not merely a Massey product of a set of identical 1-cochains, but also requires a symmetry in the defining system that is not required by the definition of a Massey product. These symmetries naturally occur in the defining systems induced by deformations, as discussed in §10.

Definition A.2.1. Let $a \in C^1(G,V)$ be a cochain, and let $m_1, \dots, m_{k-1} \in C^1(G,V)$. We say that $D := \{m_1, \dots, m_{k-1}\}$ is a *defining system for the Massey power* $\langle a \rangle^k$ if the set

$$\tilde{D} = \{a(i,j) = m_{j-i+1} : 1 \le i \le j \le k, (i,j) \neq (1,k)\}$$

is a defining system for the Massey product $\langle a, \dots, a \rangle$ (with a repeated k times). If D is a defining system for the Massey power $\langle a \rangle^k$, then we let $\langle a \rangle^k_D = \langle a, \dots, a \rangle_D$, and we let $c(D) := c(\tilde{D})$. We let

$$\langle a \rangle^k = \{\langle a \rangle^k_D\} \subset H^2(G,V)$$

where D ranges over defining systems for the Massey powers. Note that $\langle a \rangle^k \subset \langle a, \dots, a \rangle$.

Note that, for $D = \{m_1, \dots, m_{k-1}\} \subset C^1(G,V)$, D is a defining system for the Massey power $\langle a \rangle^k$ if and only if $m_1 = a$ and, for all $i = 1, \dots, k-1$, we have

$$dm_i = \sum_{j=1}^{i-1} m_j \smile m_{i-j}.$$

We also note that, for such D, we have

$$c(D) = \sum_{j=1}^{k-1} m_j \smile m_{k-j}.$$

Lemma A.2.2. *Let $\nu : G \to \mathrm{GL}_n(A)$ be a representation, and let $V = \mathrm{End}(\nu)$. Let $M_1, \dots, M_r \in C^1(G,V)$ and let $M = M_1$, and, for $i = 1, \dots, r$, define $\nu_i : G \to \mathrm{GL}_n(A[\epsilon_i])$ by*

$$\nu_i = \nu + \sum_{j=1}^{i} M_j \epsilon^j.$$

Assume that ν_{r-1} is a homomorphism. Then $D = \{M_1, \dots, M_{r-1}\}$ is a defining system for $\langle M \rangle^r$, and ν_r is a homomorphism if and only if $dM_r = c(D)$ (in which case $\langle M \rangle^r_D = 0$).

A.3. **Coordinates of matrix Massey products.** In the situation of the previous lemma, if ν is a reducible representation, it is interesting to consider the matrix coordinates of the Massey power, as we now explain. For the rest of this section, we fix two characters $\chi_1, \chi_2 : G \to A^\times$, and let $\nu = \chi_1 \oplus \chi_2$. We also fix $M \in Z^1(G, \mathrm{End}(\nu))$.

Definition A.3.1. Let $M \in Z^1(G, \mathrm{End}(\nu))$ and let $D = \{M_1, \dots, M_{r-1}\}$ be a defining system for the Massey power $\langle M \rangle^r$ in $H^2(G, \mathrm{End}(\nu))$. Write M_i as

$$M_i = \begin{pmatrix} \chi_1 a_{11}^{(i)} & \chi_2 a_{12}^{(i)} \\ \chi_1 a_{21}^{(i)} & \chi_2 a_{22}^{(i)} \end{pmatrix}.$$

where we think of $a_{11}^{(i)}$ and $a_{22}^{(i)}$ as elements of $C^1(G,A)$ and $a_{12}^{(i)}$ and $a_{21}^{(i)}$ as elements of $C^1(G, \chi_1^{-1}\chi_2)$ and $C^1(G, \chi_1\chi_2^{-1})$, respectively.

Consider the matrix

$$(*) \qquad \sum_{j=1}^{r-1} \begin{pmatrix} a_{11}^{(j)} \smile a_{11}^{(r-j)} + a_{12}^{(j)} \smile a_{21}^{(r-j)} & a_{11}^{(j)} \smile a_{12}^{(r-j)} + a_{12}^{(j)} \smile a_{22}^{(r-j)} \\ a_{21}^{(j)} \smile a_{11}^{(r-j)} + a_{22}^{(j)} \smile a_{21}^{(r-j)} & a_{21}^{(j)} \smile a_{12}^{(r-j)} + a_{22}^{(j)} \smile a_{22}^{(r-j)} \end{pmatrix}$$

as an element in

$$\left(\begin{array}{cc} Z^2(G,A) & Z^2(G,\chi_1^{-1}\chi_2) \\ Z^2(G,\chi_1\chi_2^{-1}) & Z^2(G,A) \end{array} \right).$$

For $s,t \in \{1,2\}$, we say that *the Massey relation for* $\langle M\rangle_D^r$ *holds in the* (s,t)*-coordinate* if the (s,t)-coordinate of the matrix $(*)$ vanishes in cohomology.

For example, the Massey relation for $\langle M\rangle_D^r$ holds in the $(2,1)$-coordinate if and only if

$$\sum_{j=1}^{r-1} a_{21}^{(j)} \smile a_{11}^{(r-j)} + a_{22}^{(j)} \smile a_{21}^{(r-j)} \in B^2(G,\chi_1\chi_2^{-1}).$$

Lemma A.3.2. *Let $D=\{M_1,\dots,M_{r-1}\}$ be a defining system for the Massey power $\langle M\rangle^r$ in $H^2(G,\mathrm{End}(\nu))$. The Massey relation for $\langle M\rangle_D^r$ holds in the (s,t)-coordinate for all $s,t\in\{1,2\}$ if and only if $\langle M\rangle_D^r=0$.*

The purpose of the (s,t)-Massey relations is that they are useful for comparing Massey products for different representations with the same semi-simplification.

With the notation as above, define a function ν' by

$$\nu' = \left(\begin{array}{cc} \chi_1 & 0 \\ \chi_1 a_{21}^{(1)} & \chi_2 \end{array} \right).$$

Since M_1 is a cocycle, ν' is a homomorphism.

Proposition A.3.3. *Let $r>1$ and let $D=\{M_1,\dots,M_{r-1}\}$ be a defining system for the Massey power $\langle M\rangle^r$ in $H^2(G,\mathrm{End}(\nu))$. Define $a_{st}^{(i)}$ as in Definition A.3.1. For $1\le i<r-1$, define M_i' by the formula*

$$M_i' = \left(\begin{array}{cc} \chi_1 a_{11}^{(i)} & \chi_2 a_{12}^{(i-1)} \\ \chi_1 a_{21}^{(i+1)} & \chi_2 a_{22}^{(i)} \end{array} \right).$$

with $a_{12}^{(0)}=0$ and let $M'=M_1'$. Then

1. *$D'=\{M_1',\dots,M_{r-2}'\}$ is a defining system for $\langle M'\rangle^{r-1}$ in $H^2(G,\mathrm{End}(\nu'))$, and*
2. *$\langle M'\rangle_{D'}^{r-1}=0$ in $H^2(G,\mathrm{End}(\nu'))$ if and only if Massey relation for $\langle M\rangle_D^r$ holds in the $(2,1)$-coordinate.*

Lemma A.3.4. *Let $\{M_1,\dots,M_{r-1}\}\subset C^1(G,V)$, and suppose that $\nu_{r-1}:G\to \mathrm{GL}_2(A[\epsilon_{r-1}])$ is a homomorphism, where*

$$\nu_{r-1} = \nu + \sum_{j=1}^{r-1} M_j\epsilon^j.$$

Define M_i' as in Proposition A.3.3. Choose an element $a\in C^1(G,\chi_1^{-1}\chi_2)$ and define

$$M_{r-1}' = \left(\begin{array}{cc} \chi_1 a_{11}^{(r-1)} & \chi_2 a_{12}^{(r-2)} \\ \chi_1 a & \chi_2 a_{22}^{(r-1)} \end{array} \right).$$

For $i=1,\dots,r-1$, define $\nu_i':G\to\mathrm{GL}_2(A[\epsilon_i])$ by

$$\nu_i' = \nu' + \sum_{j=1}^{i} M_j'\epsilon^j.$$

Then ν'_i is a homomorphism for $i < r-1$, and ν'_{r-1} is a homomorphism if and only if

$$da = \sum_{j=1}^{r-1} a_{21}^{(j)} \smile a_{11}^{(r-j)} + a_{22}^{(j)} \smile a_{21}^{(r-j)}.$$

Appendix B. Galois cohomology - generalities

In this section, we use cone constructions to define cochain complexes that compute Galois cohomology with various local conditions. In particular, we discuss the compactly supported, partially compactly supported, and finite-flat variants. The idea to consider derived versions of Selmer groups is due to Nekovář [Nek06]. For a more down-to-earth treatment (and all that will be needed here), see [GV18, App. B], where they use the notation of fundamental groups $\pi_1^{\text{ét}}(\mathbb{Z}[1/Np])$ (resp. $\pi_1^{\text{ét}}(\mathbb{Q}_\ell)$) in place of our $G_{\mathbb{Q},S}$ (resp. G_ℓ).

While N usually denotes a prime in the main text, here we allow it to be a squarefree integer prime to p, as in §§6.2-6.3.

B.1. **Notation from homological algebra.** If $(C^\bullet, d)$ is a cochain complex, we let $Z^i(C^\bullet) = \ker(d : C^i \to C^{i+1})$ and $B^i(C^\bullet) = \operatorname{im}(d : C^{i-1} \to C^i)$. Let $(C[i]^\bullet, d[i])$ be the complex $C[i]^j = C^{j-i}$ with differential $d[i] = (-1)^i d$. If $f : A^\bullet \to B^\bullet$ is a map of cochain complexes, we let $\operatorname{Cone}(f)^\bullet$ be the complex $\operatorname{Cone}(f)^i = B^i \oplus A^{i+1}$ and $d(b,a) = (db - f(a), -da)$. Then there is an exact sequence

$$0 \longrightarrow B^\bullet \xrightarrow{b\mapsto(b,0)} \operatorname{Cone}(f)^\bullet \xrightarrow{(a,b)\mapsto a} A[-1]^\bullet \longrightarrow 0.$$

B.2. **Notation for group cochains and cohomology groups.** Let G be a topological group, and let M be a continuous G-module. Let $C^\bullet(G, M)$ denote the complex of continuous inhomogeneous cochains.

For $N' \mid Np$, we define

$$C^\bullet(-) := C^\bullet(\mathbb{Z}[1/Np], -) := C^\bullet(G_{\mathbb{Q},S}, -), \quad C^\bullet_\ell(-) := C^\bullet(\mathbb{Q}_\ell, -) := C^\bullet(G_\ell, -),$$
$$C^\bullet_{\mathrm{loc}}(-) := \bigoplus_{\ell|Np \text{ prime}} C^\bullet_\ell(-), \quad C^\bullet_{N'}(-) := \bigoplus_{\ell|N' \text{ prime}} C^\bullet_\ell(-)$$

We let $x \mapsto x|_{N'}$ denote the restriction map $C^\bullet(-) \to C^\bullet_{N'}(-)$. We let

$$C^\bullet_{(c)}(M) = \operatorname{Cone}(C^\bullet(M) \to C^\bullet_{\mathrm{loc}}(M))[1], \; C^\bullet_{(N')}(M) = \operatorname{Cone}(C^\bullet(M) \to C^\bullet_{N'}(M))[1]$$

The associated cohomology groups are $H^i_\star(-) := H^i(C^\bullet_\star(-))$, where $\star$ is one of the symbols $\{-, \ell, N', \mathrm{loc}, (c), (\ell), (N')\}$. We call $H^i_{(c)}(-)$ compactly supported Galois cohomology, in analogy with the geometric situation.

B.3. **Duality theories.** Let M denote a p-power torsion $G_{\mathbb{Q},S}$-module, and let M^* denote the Pontryagin dual of M. We have the the following duality theorem of Poitou–Tate, which resembles Poincaré duality.

Theorem B.3.1. *For $i = 0, \dots, 3$, the cup product induces a perfect paring*

$$H^i(M) \times H^{3-i}_{(c)}(M^*(1)) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Then duality theory with "local constraints" gives the following generalization of Theorem B.3.1.

Theorem B.3.2. *For any divisor $N' \mid Np$ and $i = 0, \dots, 3$, the cup product induces a perfect paring*

$$H^i_{(N')}(M) \times H^{3-i}_{(Np/N')}(M^*(1)) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Proof. This is a special case of the duality theorem of [GV18, App. B]. In the notation of that theorem, we take the set of primes S to be the primes dividing Np, and, for any divisor n of Np, we define a condition $\mathcal{L}_n$ by

$$C_{\mathcal{L}_n}(\mathbb{Q}_\ell, M) = \begin{cases} 0 & \text{if } \ell \mid n \\ C(\mathbb{Q}_\ell, M) & \text{if } \ell \nmid n \end{cases}$$

for all primes ℓ dividing Np. Then we see that $H^*_{\mathcal{L}_{N'}}(M) = H^*_{(N')}(M)$, and that the dual condition $\mathcal{L}^\perp_{N'}$ is given by $\mathcal{L}_{Np/N'}$. The theorem follows from [GV18, Thm. B.1]. □

B.4. **Extensions of finite flat group schemes and cohomology.** Let $\mathcal{G}/\mathbb{Z}_p$ be a finite flat group scheme such that $\nu_\mathcal{G} := \mathcal{G}(\overline{\mathbb{Q}}_p)$ is free of finite rank as a $\mathbb{Z}/p^r$-module. Then there is a subgroup

$$\mathrm{Ext}^1_{\mathrm{flat}}(\nu_\mathcal{G}, \nu_\mathcal{G}) \subset \mathrm{Ext}^1_{\mathbb{Z}/p^r\mathbb{Z}[G_p]}(\nu_\mathcal{G}, \nu_\mathcal{G}) \cong H^1_p(\mathrm{End}(\nu_\mathcal{G}))$$

coming from extensions in the category of finite flat group schemes over $\mathbb{Z}_p$ that are killed by p^r. We denote

$$H^1_{p,\mathrm{flat}}(\mathrm{End}(\nu_\mathcal{G})) := \mathrm{Ext}^1_{\mathrm{flat}}(\nu_\mathcal{G}, \nu_\mathcal{G}).$$

We also want to define $H^1_{p,\mathrm{flat}}(-)$ in two other specific cases. If $\mathcal{G} \simeq \mu_{p^r} \otimes_{\mathbb{Z}/p^r\mathbb{Z}} A$ for some $\mathbb{Z}/p^r\mathbb{Z}$-module A, then $\nu_\mathcal{G} \simeq A(1)$. We write $H^1_{p,\mathrm{flat}}(A(1))$ for the subgroup

$$\mathrm{Ext}^1_{\mathrm{flat}}(\mathbb{Z}/p^r\mathbb{Z}, A(1)) \subset \mathrm{Ext}^1_{\mathbb{Z}/p^r\mathbb{Z}[G_p]}(\mathbb{Z}/p^r\mathbb{Z}, A(1)) \cong H^1_p(A(1))$$

and $H^1_{p,\mathrm{flat}}(A(-1))$ for the subgroup

$$\mathrm{Ext}^1_{\mathrm{flat}}(A(1), \mathbb{Z}/p^r\mathbb{Z}) \subset \mathrm{Ext}^1_{\mathbb{Z}/p^r\mathbb{Z}[G_p]}(A(1), \mathbb{Z}/p^r\mathbb{Z}) \cong H^1_p(A(-1)).$$

Now suppose V is a $G_{\mathbb{Q},S}$-module such that $V|_{G_p}$ is isomorphic to either $\nu_\mathcal{G}$, $A(1)$, or $A(-1)$, as above. We wish to define cochain complexes $C^\bullet_{p,\mathrm{flat}}(V)$ and $C^\bullet_{\mathrm{flat}}(V)$ such that

(1) $H^1(C^\bullet_{p,\mathrm{flat}}(V)) = H^1_{p,\mathrm{flat}}(V)$
(2) $H^1(C^\bullet_{\mathrm{flat}}(V)) = \ker(H^1(V) \to H^1_p(V)/H^1_{p,\mathrm{flat}}(V))$
(3) $H^2(C^\bullet_{\mathrm{flat}}(V))$ controls obstructions to global finite-flat deformations.

B.4.1. *The flat and non-flat local cochain complexes.* We define $C^\bullet_{p,\mathrm{flat}}(V)$ by

$$C^i_{p,\mathrm{flat}}(V) = \begin{cases} C^0_p(V) & \text{if } i = 0 \\ Z^1_{p,\mathrm{flat}}(V) & \text{if } i = 1 \\ 0 & \text{if } i \geq 2 \end{cases}$$

where

$$Z^1_{p,\mathrm{flat}}(V) := \ker(Z^1_p(V) \to H^1_p(V)/H^1_{p,\mathrm{flat}}(V)).$$

Then it is clear that $C^\bullet_{p,\mathrm{flat}}(V) \subset C^\bullet_p(V)$ is a subcomplex, and that $H^1(C^\bullet_{p,\mathrm{flat}}(V)) = H^1_{p,\mathrm{flat}}(V)$. We define $H^i_{p,\mathrm{flat}}(V) := H^i(C^\bullet_{p,\mathrm{flat}}(V))$.

We define

$$C^\bullet_{p,\text{non-flat}}(V) = \mathrm{Cone}(C^\bullet_{p,\mathrm{flat}}(V) \to C^\bullet_p(V))$$

and $H^i_{p,\text{non-flat}}(V) := H^i(C^\bullet_{p,\text{non-flat}}(V))$. Then we have

$$H^0_{p,\text{non-flat}}(V) = 0, \qquad H^2_{p,\text{non-flat}}(V) = H^2_p(V),$$

and an exact sequence

$$0 \longrightarrow H^1_{p,\text{flat}}(V) \longrightarrow H^1_p(V) \longrightarrow H^1_{p,\text{non-flat}}(V) \longrightarrow 0.$$

B.4.2. *The global finite-flat cochain complex.* Let $(-)|_{p,\text{flat}} : C^\bullet(V) \to C^\bullet_{p,\text{non-flat}}(V)$ denote the composition

$$C^\bullet(V) \xrightarrow{|_p} C^\bullet_p(V) \longrightarrow C^\bullet_{p,\text{non-flat}}(V).$$

Let

$$C^\bullet_{\text{flat}}(V) := \mathrm{Cone}(C^\bullet(V) \xrightarrow{|_{p,\text{flat}}} C^\bullet_{p,\text{non-flat}}(V))[1].$$

We call the resulting cohomology $H^\bullet_{\text{flat}}(V) := H^\bullet(C^\bullet_{\text{flat}}(V))$ *global flat cohomology.* The long exact sequence of the cone is

$$\begin{aligned} 0 = H^0_{p,\text{non-flat}}(V) &\longrightarrow H^1_{\text{flat}}(V) \longrightarrow H^1(V) \longrightarrow H^1_{p,\text{non-flat}}(V) \\ &\longrightarrow H^2_{\text{flat}}(V) \longrightarrow H^2(V) \longrightarrow H^2_{p,\text{non-flat}}(V) \longrightarrow H^3_{\text{flat}}(V) \longrightarrow 0. \end{aligned}$$

Take note of the isomorphisms

$$H^1_{p,\text{non-flat}}(V) \cong \frac{H^1_p(V)}{H^1_{p,\text{flat}}(V)}, \quad H^2_{p,\text{non-flat}}(V) \cong H^2_p(V), \text{ and } H^3_{\text{flat}}(V) \cong H^3_{(p)}(V),$$

which are useful interpretations of terms of the sequence.

We will often refer to $Z^1_{\text{flat}}(V)$, which we will take to be the kernel of $Z^1(V) \to H^1_p(V)/H^1_{p,\text{flat}}$. (This is part of the data of a cocycle in the cone defining $H^1_{\text{flat}}(V)$.)

Appendix C. Operations in homological algebra in terms of cocycles

In this section, we show that some standard operations on representations, described in terms of matrices and cocycles, behave nicely with finite-flat cohomology. The reason is that these operations correspond to operations on extensions in a general exact category, and so can be done equally well in the category of finite flat group schemes of fixed exponent over a scheme, which is an full additive subcategory of the category of abelian category of *fppf*-sheaves of abelian groups of that exponent, and is closed under extensions (see [Oor66, Prop. III.17.4, pg. 110]).

Below $\mathcal{C}$ will denote any exact category. This means $\mathcal{C}$ is an additive category equipped with a class of pairs of composable morphisms $A \to X \to B$ that should be thought of as exact sequences, and satisfy certain axioms – for a precise definition, see [Büh10], for example. For our purposes, it suffices to assume that $\mathcal{C}$ is a full additive subcategory of an abelian category that is closed under extensions.

C.1. **Pushout.** Suppose we have short exact sequences

$$\mathcal{E}' : 0 \longrightarrow C \longrightarrow X \xrightarrow{j} B \longrightarrow 0$$

$$\mathcal{E} : 0 \longrightarrow X \xrightarrow{i} X' \longrightarrow A \longrightarrow 0.$$

in the exact category $\mathcal{C}$. Then, by the axioms of an exact category, the pushout X'' of i and j sits in an exact sequence

$$0 \longrightarrow B \longrightarrow X'' \longrightarrow A \longrightarrow 0$$

where $X'' \to A$ is induced by the composite $X' \times B \to X' \to A$. We called this extension the pushout of $\mathcal{E}$ by $\mathcal{E}'$.

Example C.1.1. Let $\mathcal{C}$ be the exact category of representations of a group G in projective R-modules of constant finite rank, where R is a commutative ring. We explain how to interpret the pushout construction in terms of matrices. Write an object A of $\mathcal{C}$ as a pair (V_A, ρ_A) with V_A a finite constant rank projective R-module and $\rho_A : G \to \mathrm{GL}(V_A)$ a homomorphism.

Suppose we have A, B, C, X, X' as above in this category. Then we may write X in block matrix form as

$$\rho_X = \begin{pmatrix} \rho_C & \rho_{\mathcal{E}'} \\ 0 & \rho_B \end{pmatrix}$$

and X' as

$$\rho_{X'} = \begin{pmatrix} \rho_A & 0 & 0 \\ \rho_{\mathcal{E},1} & \rho_C & \rho_{\mathcal{E}'} \\ \rho_{\mathcal{E},2} & 0 & \rho_B \end{pmatrix}.$$

Direct computation as in Example C.3.1 below shows that the pushout of $\mathcal{E}$ by $\mathcal{E}'$ is given by the block matrix

$$\begin{pmatrix} \rho_A & 0 \\ \rho_{\mathcal{E},2} & \rho_B \end{pmatrix}.$$

C.2. **Pullback.** Suppose we have short exact sequences

$$\mathcal{E}' : 0 \longrightarrow B \longrightarrow X \xrightarrow{j} A \longrightarrow 0$$

$$\mathcal{E} : 0 \longrightarrow C \xrightarrow{i} Y \longrightarrow A \longrightarrow 0.$$

in the exact category $\mathcal{C}$. Then, by the axioms of an exact category, the pullback $Z = X \times_A Y$ sits in an exact sequence

$$0 \longrightarrow B \longrightarrow Z \longrightarrow Y \longrightarrow 0.$$

We call this the pullback of $\mathcal{E}$ along $\mathcal{E}'$.

Suppose Y gives an extension $\mathcal{E}$ of A by C and X gives an extension $\mathcal{E}'$ of A by B. Then we can construct the pullback extension of Y by B as follows. Let $Z = X \times_A Y$. The map $Z \to Y$ is an epimorphism with kernel isomorphic to B. We call the resulting extension of Y by B the pullback of $\mathcal{E}$ along $\mathcal{E}'$.

Example C.2.1. We return to the category of finite rank representations from the previous example, and retain the notation there. Suppose we have A, B, C, X, Y as above in this category. Then we may write Y in block matrix form as

$$\rho_Y = \begin{pmatrix} \rho_A & 0 \\ \rho_{\mathcal{E}} & \rho_C \end{pmatrix}$$

and X as

$$\rho_X = \begin{pmatrix} \rho_A & 0 \\ \rho_{\mathcal{E}'} & \rho_B \end{pmatrix}$$

By direct computation as in Example C.3.1 below, we see that the pullback of $\mathcal{E}$ along $\mathcal{E}'$ is given by the block matrix

$$\begin{pmatrix} \rho_A & 0 & 0 \\ \rho_{\mathcal{E}} & \rho_C & 0 \\ \rho_{\mathcal{E}'} & 0 & \rho_B \end{pmatrix}.$$

C.3. **Baer sum.** Suppose we have short exact sequences

$$\mathcal{E}: \ 0 \longrightarrow B \xrightarrow{i} X \xrightarrow{j} A \longrightarrow 0$$

$$\mathcal{E}': \ 0 \longrightarrow B \xrightarrow{i'} X' \xrightarrow{j'} A \longrightarrow 0$$

in $\mathcal{C}$. Then, by the axioms of an exact category, the direct sum $\mathcal{E} \oplus \mathcal{E}'$ is an extension of $A \oplus A$ by $B \oplus B$. The Baer sum $\mathcal{E} + \mathcal{E}'$ is the extension of A by B obtained by pulling back $\mathcal{E} \oplus \mathcal{E}'$ by the diagonal $A \to A \oplus A$ and then pushing out the result by the sum map $B \oplus B \to B$.

In an abelian category, there is an alternate construction of $\mathcal{E} + \mathcal{E}'$ given as follows. There is a skew diagonal map $\Delta^s : B \to X \times_A X'$ given by $\Delta^s = i \times (-i')$. Let $Y = \mathrm{coker}(\Delta^s)$. The composite $X \times_A X' \to X' \xrightarrow{j'} A$ induces an epimorphism $Y \to A$ whose kernel is isomorphic to B. The resulting extension of A by B is defined to be $\mathcal{E} + \mathcal{E}'$.

Example C.3.1. We return to the category $\mathcal{C}$ of the previous examples. We explain how to interpret the Baer sum construction in terms of matrices.

Recall that we write an object A of $\mathcal{C}$ as a pair (V_A, ρ_A). For an extension $\mathcal{E}$ of A by B as above, we can choose a decomposition $V_X = V_A \oplus V_B$, and write ρ_X in block matrix form as

$$\rho_X = \begin{pmatrix} \rho_A & 0 \\ \rho_{\mathcal{E}} & \rho_B \end{pmatrix}$$

with $\rho_{\mathcal{E}} \in Z^1(G, \mathrm{Hom}(V_A, V_B))$; the extension $\mathcal{E}$ is determined by this cocycle.

Now, given two extensions $\mathcal{E}$ and $\mathcal{E}'$ of A by B, to describe the extension $\mathcal{E} + \mathcal{E}'$, we need only describe the cocycle $\rho_{\mathcal{E}+\mathcal{E}'}$. We claim that it is given by $\rho_{\mathcal{E}+\mathcal{E}'} = \rho_{\mathcal{E}} + \rho_{\mathcal{E}'}$. Indeed, for $Y = \mathrm{coker}(\Delta^s)$ as above, we can write a V_Y as a direct sum $V_Y = \{(b, 0) | b \in V_B\} \oplus \{(a, a) | a \in V_A\}$. Then for $\sigma \in G$ and $a \in V_A$, the cocycle $\rho_{\mathcal{E}+\mathcal{E}'}$ is defined by the formula

$$\rho_Y(\sigma)(a, a) = (\rho_A(\sigma)a, \rho_A(\sigma)a) + (\rho_{\mathcal{E}+\mathcal{E}'}(\sigma)a, 0).$$

On the other hand, we compute that

$$\begin{aligned} \rho_Y(\sigma)(a, a) &= (\rho_A(\sigma)a + \rho_{\mathcal{E}}(\sigma)a, \rho_A(\sigma)a + \rho_{\mathcal{E}'}(\sigma)a) \\ &= (\rho_A(\sigma)a, \rho_A(\sigma)a) + (\rho_{\mathcal{E}}(\sigma)a, \rho_{\mathcal{E}'}(\sigma)a) \\ &= (\rho_A(\sigma)a, \rho_A(\sigma)a) + (\rho_{\mathcal{E}}(\sigma)a + \rho_{\mathcal{E}'}(\sigma)a, 0), \end{aligned}$$

using the fact that $(-\rho_{\mathcal{E}'}(\sigma)a, \rho_{\mathcal{E}'}(\sigma)a) = 0$ in V_Y.

Remark C.3.2. In this situation, there is also a "Baer scalar product" defining an R-module structure on $\mathrm{Ext}^1_{\mathcal{C}}(B, A)$. For $r \in R$ and $\mathcal{E} \in \mathrm{Ext}^1_{\mathcal{C}}(B, A)$ as above, the extension $r \cdot \mathcal{E}$ is obtained as a quotient of the direct sum $X \oplus A$.

C.4. **Application to finite-flat representations.** We apply the above examples to the case of finite-flat deformations. Let R be a commutative ring of finite cardinality.

Lemma C.4.1. *Let $\nu : G_p \to \mathrm{GL}_n(R)$ be a finite-flat representation, and let $\nu_r : G_p \to \mathrm{GL}_n(R[\epsilon_r])$ be a finite-flat deformation of ν for some $r \geq 1$. Let $x \in C^1(G_p, \mathrm{End}(\nu))$, and let $\nu'_r = \nu_r + x\epsilon^r$. Then ν'_r is a finite-flat representation if and only if $x \in Z^1_{\mathrm{flat}}(G_p, \mathrm{End}(\nu))$.*

Proof. We can think of a free $R[\epsilon_r]$-module of rank n as being an R-module of rank $n(r+1)$ with additional structure. In this way, we can apply the two examples above to this situation. We write $\nu_r = \nu + \sum_{i=1}^{r} x_i \epsilon^i$ with $x_i \in C^1(G_p, \mathrm{End}(\nu))$. Let $\nu_{r-1} = \nu_r/\epsilon^r \nu_r$, and $\nu_{r-2} = \nu_r/\epsilon^{r-1}\nu_r$ (so $\nu_{r-2} = 0$ if $r = 1$).

First suppose that ν_r' is a finite-flat representation, and let $x_r' = x_r + x$. Then since $\epsilon^r \nu_r \cong \epsilon^r \nu_r' \cong \nu$, and $\nu_r'/\epsilon^r \nu_r \cong \nu_{r-1}$, we can consider ν_r and ν_r' as being extensions of ν_{r-1} by ν. In block matrix form, they look like

$$\nu_r = \left(\begin{array}{cccc|c} \multicolumn{4}{c|}{\nu_{r-1}} & 0 \\ \hline x_r & x_{r-1} & \cdots & x_1 & \nu \end{array}\right), \ \nu_r' = \left(\begin{array}{cccc|c} \multicolumn{4}{c|}{\nu_{r-1}} & 0 \\ \hline x_r' & x_{r-1} & \cdots & x_1 & \nu \end{array}\right).$$

By Example C.3.1, the Baer difference extension is given by

$$\left(\begin{array}{cccc|c} \multicolumn{4}{c|}{\nu_r} & 0 \\ \hline x & 0 & \cdots & 0 & \nu \end{array}\right) = \left(\begin{array}{c|ccc|c} \nu & 0 & \cdots & 0 & 0 \\ \hline x_1 & \nu & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{r-1} & x_{r-2} & \cdots & \nu & 0 \\ \hline x & 0 & \cdots & 0 & \nu \end{array}\right).$$

As in Example C.1.1, we can pushout to obtain an extension of ν by ν whose cocycle is given by x. Since the Baer sum and pushout can be done in any exact category, we could equally well do these operations to the finite-flat groups schemes giving rise to ν_r and ν_r', and obtain an extension of finite flat group schemes whose cocycle is x. This implies that x is a finite-flat cocycle.

Conversely, suppose that $x \in Z^1_{\mathrm{flat}}(G_p, \mathrm{End}(\nu))$. Then x gives rise to an extension $\mathcal{E}_x$ of ν by ν. As above, we can consider ν_r as an extension of ν_{r-1} by ν. We can also think of ν_{r-1} as an extension $\mathcal{E}_{r-1}$ of ν by ν_{r-2}. By Example C.1.1, the pullback extension $\mathcal{E}$ of $\mathcal{E}_{r-1}$ along $\mathcal{E}_x$ can be written in block matrix form as

$$\left(\begin{array}{cccc|c} \multicolumn{4}{c|}{\nu_{r-1}} & 0 \\ \hline x & 0 & \cdots & 0 & \nu \end{array}\right)$$

Then, by Example C.3.1, we see that the Baer sum of $\mathcal{E}$ with ν_r is given by the same matrix as ν_r'. As above, we see that the representation obtained from pullback and Baer sum is finite-flat, so this implies that ν_r' is finite-flat. □

References

[BC09] Joël Bellaïche and Gaëtan Chenevier. Families of Galois representations and Selmer groups. *Astérisque*, (324):xii+314, 2009.

[BKK14] Tobias Berger, Krzysztof Klosin, and Kenneth Kramer. On higher congruences between automorphic forms. *Math. Res. Lett.*, 21(1):71–82, 2014.

[Büh10] Theo Bühler. Exact categories. *Expo. Math.*, 28(1):1–69, 2010.

[CE05] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[Che14] Gaëtan Chenevier. The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings. In *Automorphic Forms and Galois Representations: Vol. I*, volume 414 of *London Mathematical Society Lecture Note Series*, pages 221–285. Cambridge Univ. Press, Cambridge, 2014. We follow the numbering of the online version https://arxiv.org/abs/0809.0415v2, which differs from the print version.

[Con97] Brian Conrad. The flat deformation functor. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 373–420. Springer, New York, 1997.

[dSRS97] Bart de Smit, Karl Rubin, and René Schoof. Criteria for complete intersections. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 343–356. Springer, New York, 1997.

[Eme99] Matthew Emerton. The Eisenstein ideal in Hida's ordinary Hecke algebra. *Internat. Math. Res. Notices*, (15):793–802, 1999.

[GRR72] Alexander Grothendieck, Michel Raynaud, and Dock Sang Rim. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I).

[GV18] S. Galatius and A. Venkatesh. Derived Galois deformation rings. *Adv. Math.*, 327:470–623, 2018.

[Kra66] David Kraines. Massey higher products. *Trans. Amer. Math. Soc.*, 124:431–449, 1966.

[Lec18a] Emmanuel Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. arXiv:1709.09114v2 [math.NT], 2018.

[Lec18b] Emmanuel Lecouturier. On the Galois structure of the class group of certain Kummer extensions. *J. Lond. Math. Soc. (2)*, 98(1):35–58, 2018.

[Mas58] W. S. Massey. Some higher order cohomology operations. In *Symposium internacional de topología algebraica International symposium on algebraic topology*, pages 145–154. Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958.

[May69] J. Peter May. Matric Massey products. *J. Algebra*, 12:533–568, 1969.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Mer96] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.

[MT87] B. Mazur and J. Tate. Refined conjectures of the "Birch and Swinnerton-Dyer type". *Duke Math. J.*, 54(2):711–750, 1987.

[Nek06] Jan Nekovář. Selmer complexes. *Astérisque*, (310):viii+559, 2006.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Oht14] Masami Ohta. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II. *Tokyo J. Math.*, 37(2):273–318, 2014.

[Oor66] F. Oort. *Commutative group schemes*, volume 15 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1966.

[Ram93] Ravi Ramakrishna. On a variation of Mazur's deformation functor. *Compositio Math.*, 87(3):269–286, 1993.

[Sch90] A. J. Scholl. Motives for modular forms. *Invent. Math.*, 100(2):419–430, 1990.

[Sha07] Romyar T. Sharifi. Massey products and ideal class groups. *J. Reine Angew. Math.*, 603:1–33, 2007.

[Sou79] C. Soulé. K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale. *Invent. Math.*, 55(3):251–295, 1979.

[SS19] Karl Schaefer and Eric Stubley. Class groups of Kummer extensions via cup products in Galois cohomology. To appear in *Trans. Amer. Math. Soc.* https://doi.org/10.1090/tran/7746, 2019.

[UM57] Hiroshi Uehara and W. S. Massey. The Jacobi identity for Whitehead products. In *Algebraic geometry and topology. A symposium in honor of S. Lefschetz*, pages 361–377. Princeton University Press, Princeton, N. J., 1957.

[WE18a] Carl Wang-Erickson. Algebraic families of Galois representations and potentially semi-stable pseudodeformation rings. *Math. Ann.*, 371(3-4):1615–1681, 2018.

[WE18b] Carl Wang-Erickson. Deformations of residually reducible Galois representations via A_∞-algebra structure on Galois cohomology. arXiv:1809.02484v1 [math.NT], 2018.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[WWE18] Preston Wake and Carl Wang-Erickson. Pseudo-modularity and Iwasawa theory. *Amer. J. Math.*, 140(4):977–1040, 2018.

[WWE19] Preston Wake and Carl Wang-Erickson. Deformation conditions for pseudorepresentations. arXiv:1707.01896v3 [math.NT]. To appear in *Forum Math. Sigma*, 2019.

Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540
Email address: pwake@ias.edu

Department of Mathematics, Imperial College London, London SW7 2AZ, UK
Email address: c.wang-erickson@imperial.ac.uk