On Constructing Extensions of Residually Isomorphic Characters

Samit Dasgupta*

November 16, 2023

Abstract

This is an exposition of our joint work with Kakde, Silliman, and Wang, in which we prove a version of Ribet's Lemma for GL_2 in the residually indistinguishable case. We suppose we are given a Galois representation taking values in the total ring of fractions of a complete reduced Noetherian local ring $\mathbf{T}$, such that the characteristic polynomial of the representation is reducible modulo some ideal $I \subset \mathbf{T}$. We assume that the two characters that arise are congruent modulo the maximal ideal of $\mathbf{T}$. We construct an associated Galois cohomology class valued in a $\mathbf{T}$-module that is "large" in the sense that its Fitting ideal is contained in I. We make some simplifying assumptions that streamline the exposition—we assume the two characters are actually equal, and we ignore the local conditions needed in arithmetic applications.

Contents

*The author is supported by NSF grant DMS–2200787.

1 Introduction

In 1970, Ribet proved the converse of Herbrand's Theorem [13]. When I learned about this in graduate school, Dick Gross recalled to me that the methods introduced by Ribet "were like a thunderbolt" in the number theory community at the time. Over 50 years later, Ribet's method remains a central force in algebraic number theory, particularly in Iwasawa Theory. Perhaps the seminal work on the topic is the beautiful book of Joel Bellaïche and Gaetan Chenevier [2]. This book presents a very general form of Ribet's approach and also describes deep arithmetic applications. An introduction written for a more general audience is given by Mazur [10].

The goal of Ribet's method is to construct a nontrivial Galois cohomology class from the knowledge that an L-function is appropriately divisible. Typically, we will be given a special value of an L-function, which we denote by L, lying in a ring $\mathbf{T}$ (e.g. $\mathbf{T} = \mathbf{Z}_p$ or $\mathbf{T} = \mathbf{Z}_p[[T]]$), and we assume assume that L lies in some ideal $I \subset \mathbf{T}$. The value L will be associated to two (or more) representations of the Galois group of a number field F over R, say ρ_1 and ρ_2. One then wants to construct a nontrivial class in

$$H^1(G_F, \overline{\rho}_1 \otimes \overline{\rho}_2^*),$$

where ρ_2^* is the dual of ρ_2 and $\overline{\rho}_i$ denotes the reduction of ρ_i modulo I. In Ribet's original setting, he had $\mathbf{T} = \mathbf{Z}_p$, $I = (p)$, and ρ_1, ρ_2 one dimensional characters of $G_{\mathbf{Q}}$. Specifically, ρ_1 was the trivial character and ρ_2 a nontrivial character of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$.

To produce an extension, Ribet constructed a cusp form congruent to the Eisenstein series associated to ρ_1 and ρ_2. In his case, one can show that the cusp form is an eigenform. One therefore obtains a representation

$$\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(K),$$

where K is a finite extension of $\mathbf{Q}_p$, such that

$$\mathrm{tr}(\rho) \equiv \rho_1 + \rho_2, \qquad \det(\rho) \equiv \rho_1\rho_2 \pmod{I}. \tag{1}$$

The representation ρ can be conjugated to land in $\mathrm{GL}_2(\mathcal{O}_K)$, and the Brauer–Nesbitt Theorem implies that one can choose a basis so that the reduction of ρ modulo the maximal ideal $\mathfrak{m}_K \subset \mathcal{O}_K$ has the form

$$\overline{\rho} = \begin{pmatrix} \overline{\rho}_1 & * \\ 0 & \overline{\rho}_2 \end{pmatrix}.$$

Ribet then proves an important lemma which shows that the basis can be chosen so that the image of $*$ in $\mathcal{O}_K/\mathfrak{m}_K$ defines a non-trivial class in $H^1(G_F, \overline{\rho}_1 \otimes \overline{\rho}_2^{-1})$. Furthermore, Ribet proves certain local conditions satisfied by this non-trivial class. It is elementary class field theory to prove that the existence of this class implies the converse to Herbrand's Theorem. We state Ribet's Lemma formally as follows.

Theorem 1.1 (Ribet's Lemma, Version 1)**.** *Let $\mathbf{T}$ be a complete DVR, and let $\mathfrak{m}$ denote its maximal ideal. Let $\mathcal{G}$ be a compact group. Suppose we are given a continuous irreducible representation*

$$\rho\colon \mathcal{G} \longrightarrow \mathrm{GL}_2(K), \qquad K = \mathrm{Frac}(\mathbf{T}),$$

such that

$$\mathit{char}(\rho(g)) \equiv (x - \chi_1(g))(x - \chi_2(g)) \pmod{\mathfrak{m}} \tag{2}$$

for two characters $\chi_1, \chi_2\colon \mathcal{G} \longrightarrow \mathbf{T}^*$. Then there exists a non-zero cohomology class

$$\kappa \in H^1(\mathcal{G}, \mathbf{T}/\mathfrak{m}(\chi_2^{-1}\chi_1)).$$

In more general settings, such as that employed by Mazur–Wiles [11] and Wiles [15] in their study of the Iwasawa Main Conjecture, the ring $\mathbf{T}$ cannot be assumed to be a DVR. It will usually be a complete local Noetherian ring, perhaps reduced. An example of such a ring that is not a DVR is

$$\mathbf{T} = \{(a, b) \in \mathbf{Z}_p \times \mathbf{Z}_p\colon a \equiv b \pmod{p}\}.$$

This example corresponds to two eigenforms with Hecke eigenvalues in $\mathbf{Z}_p$ that are congruent to each other modulo p. The total ring of fractions of $\mathbf{T}$ is $K = \mathrm{Frac}(\mathbf{T}) = \mathbf{Q}_p \times \mathbf{Q}_p$.

In addition, the ideal $I \subset \mathbf{T}$ modulo which the characteristic polynomial of ρ factors will in general not be the maximal ideal of $\mathbf{T}$. One then wants to construct a cohomology class that generates a module that (in a sense we will make precise in a moment) is "as large as" $\mathbf{T}/I$. The first version of Ribet's Lemma that applies in this case was proven by Mazur–Wiles and Wiles. Their work was groundbreaking and had a profound impact, leading to Wiles' theory of pseudorepresentations. In the statement below, a cohomology class κ valued in a $\mathbf{T}$-module M is called *surjective* if the image of every representative cocycle generates M as a $\mathbf{T}$-module.

Theorem 1.2 (Ribet's Lemma, Version 2)**.** *Let* $\mathbf{T}$ *be a complete reduced local Noetherian ring, and let* $\mathfrak{m}$ *denote its maximal ideal. Let* $\mathcal{G}$ *be a compact group. Suppose we are given a continuous representation*

$$\rho\colon \mathcal{G} \longrightarrow \mathrm{GL}_2(K), \qquad K = \mathrm{Frac}(\mathbf{T}),$$

such that for any projection onto a field $K \to k$*, the projection of* ρ *to a representation* $\mathcal{G} \to \mathrm{GL}_2(k)$ *is irreducible. Let* $I \subset \mathbf{T}$ *be a proper ideal. Suppose that*

$$char(\rho(g)) \equiv (x - \chi_1(g))(x - \chi_2(g)) \pmod{I} \tag{3}$$

for two characters $\chi_1, \chi_2\colon \mathcal{G} \longrightarrow \mathbf{T}^*$ *satisfying* $\chi_1 \not\equiv \chi_2 \pmod{\mathfrak{m}}$*. Then there exists a fractional ideal of* $\mathbf{T}$*,* $B \subset K$*, and a surjective cohomology class*

$$\kappa \in H^1(G, B/IB(\chi_2^{-1}\chi_1)).$$

The assumption $\chi_1 \not\equiv \chi_2 \pmod{\mathfrak{m}}$ is essential in Wiles' approach to Theorem 1.2, and it has important consequences. In the Main Conjecture of Iwasawa Theory, one has χ_1 equal to the trivial character and χ_2 equal to a totally odd character of a totally real field. Let c denote complex conjugation. When $p \neq 2$, we have $\chi_1(c) = 1 \not\equiv -1 = \chi_2(c) \pmod{p}$. However when $p = 2$ we may have $\chi_1 \equiv \chi_2 \pmod{p}$, and Theorem 1.2 cannot be applied. This is the main reason that Wiles sets $p \neq 2$ in his proof of the Main Conjecture.

The purpose of this exposition is to describe the main theorem of our paper [6], joint with Mahesh Kakde, Jesse Silliman, and Jiuya Wang, in which we establish a version of Ribet's Lemma that holds even if $\chi_1 \equiv \chi_2 \pmod{\mathfrak{m}}$. Here we describe the proof of the following result, a simplified form of Theorem 2.1 of *loc. cit.*

Theorem 1.3 (Ribet's Lemma, Version 3)**.** *Let* $\mathbf{T}$ *be a complete reduced local Noetherian ring, and let* $\mathfrak{m}$ *denote its maximal ideal. Let* $\mathcal{G}$ *be a compact group. Suppose we are given a continuous representation*

$$\rho\colon \mathcal{G} \longrightarrow \mathrm{GL}_2(K), \qquad K = \mathrm{Frac}(\mathbf{T}),$$

such that for any projection onto a field $K \to k$*, the projection of* ρ *to a representation* $\mathcal{G} \to \mathrm{GL}_2(k)$ *is irreducible. Let* $I \subset \mathbf{T}$ *be a proper ideal. Suppose that*

$$char(\rho(g)) \equiv (x - \chi_1(g))(x - \chi_2(g)) \pmod{I} \tag{4}$$

for two characters $\chi_1, \chi_2\colon \mathcal{G} \longrightarrow \mathbf{T}^*$*. Then there exists a finitely generated* $\mathbf{T}$*-module* M *and a surjective cohomology class*

$$\kappa \in H^1(G, M(\chi_2^{-1}\chi_1))$$

such that

$$\mathrm{Fitt}_{\mathbf{T}}(M) \subset I.$$

The ideal $\mathrm{Fitt}_{\mathbf{T}}(M)$ is the 0th Fitting ideal of the module M, which will be defined in §4.1. Intuitively, the inclusion $\mathrm{Fitt}_{\mathbf{T}}(M) \subset I$ says that M is "large."

In [5], we prove the Brumer–Stark conjecture at $p = 2$ using a suitably generalized version of Theorem 1.3. Previously, we proved the conjecture over $\mathbf{Z}[1/2]$ in [4], with the prime $p = 2$ being avoided for reasons of residual distinguishability. We hope that further strengthenings of Theorem 1.3 (for example, to groups other than GL_2) could have other arithmetic applications.

In this paper, we simplify notation by setting χ_1 and χ_2 to be the trivial character; the case of general χ_1, χ_2 requires no extra ideas, but the notation is heavier. A more significant change in this paper relative to [6] is that all the versions of Ribet's method stated above do not include local conditions on the cohomology classes constructed. In arithmetic applications, ranging from Ribet's original proof of the converse to Herbrand's theorem to our proof of the Brumer–Stark conjecture, local conditions are always necessary. To prove the local properties we need in the Brumer–Stark context, the argument presented here is generalized in [6] using the Buchsbaum–Rim resolution of determinantal ideals; in this paper, the simple Koszul complex suffices. In *loc. cit.* we also give a mild generalization to certain non-reduced Hecke algebras $\mathbf{T}$.

It is an honor to contribute this article to the memorial volume for Joël Bellaïche. Joël was a wonderful collaborator and dear friend. We discussed the residually indistinguishable case of Ribet's Lemma in 2010, at which time both of us felt the problem was intractable. It is a great sadness that I cannot share this result with my colleague who perhaps would have appreciated it the most.

2 The DVR case

In this section we prove Theorem 1.1, Ribet's original setting. Let $\mathbf{T}$ be a complete DVR and let $\mathfrak{m}$ denote its maximal ideal. Let $\mathcal{G}$ be a compact group. We are given a continuous irreducible representation

$$\rho\colon \mathcal{G} \longrightarrow \mathrm{GL}_2(K), \qquad K = \mathrm{Frac}(\mathbf{T}),$$

such that

$$\mathrm{char}(\rho(g)) \equiv (x - \chi_1(g))(x - \chi_2(g)) \pmod{\mathfrak{m}} \tag{5}$$

for two characters $\chi_1, \chi_2\colon \mathcal{G} \longrightarrow \mathbf{T}^*$.

Lemma 2.1. *The representation ρ may be conjugated to have image contained in $\mathrm{GL}_2(\mathbf{T})$, and such that the reduction $\overline{\rho}$ has the shape*

$$\overline{\rho} = \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix}.$$

Proof. The maximal compact subgroups of $\mathrm{GL}_2(K)$ are precisely the conjugates of $\mathrm{GL}_2(\mathbf{T})$. Since $\mathcal{G}$ is compact and ρ is continuous, it follows ρ that may be conjugated to have image contained in $\mathrm{GL}_2(\mathbf{T})$. Now (5) states that

$$\mathrm{char}(\overline{\rho}(g)) = (x - \overline{\chi}_1(g))(x - \overline{\chi}_2(g)) \text{ in } \mathbf{T}/\mathfrak{m}. \tag{6}$$

The Brauer–Nesbitt Theorem [3] states that if two representations over a field have the same characteristic polynomial, then their semisimplifications are isomorphic. Therefore, (6) implies that $\overline{\rho}^{\mathrm{ss}} \cong \overline{\chi}_1 \oplus \overline{\chi}_2$. Hence we have either

$$\overline{\rho} \cong \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix} \qquad \text{or} \qquad \overline{\rho} \cong \begin{pmatrix} \overline{\chi}_2 & * \\ 0 & \overline{\chi}_1 \end{pmatrix}. \tag{7}$$

It is a pleasant exercise to prove (7) directly from (6) without reference to the full strength of the Brauer–Nesbitt Theorem. Now, suppose we are in the second case. Then we can conjugate ρ by the matrix $\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$, where π is a uniformizer of $\mathbf{T}$, to obtain

$$\overline{\rho} \cong \begin{pmatrix} \overline{\chi}_2 & 0 \\ * & \overline{\chi}_1 \end{pmatrix} \cong \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix}$$

as desired. □

Lemma 2.2. *Suppose that the representation ρ has been conjugated so that its image lands in $\mathrm{GL}_2(\mathbf{T})$ and*

$$\overline{\rho} = \begin{pmatrix} \overline{\chi}_1 & \overline{b} \\ 0 & \overline{\chi}_2 \end{pmatrix}.$$

Then the function $\kappa(\sigma) = \overline{\chi}_2^{-1}(\sigma)\overline{b}(\sigma)$ is a 1-cocycle in $Z^1(\mathcal{G}, \mathbf{T}/\mathfrak{m}(\chi_2^{-1}\chi_1))$.

Proof. Since $\overline{\rho}$ is a matrix representation, we have

$$\overline{b}(\sigma\tau) = \overline{\chi_1}(\sigma)\overline{b}(\tau) + \overline{b}(\sigma)\overline{\chi_2}(\tau).$$

Multiplying by $\overline{\chi}_2^{-1}(\sigma\tau)$ gives the desired 1-cocycle formula for $\kappa = \overline{\chi}_2^{-1}\overline{b}$. □

What remains to prove Theorem 1.1 is to show that after conjugating ρ further, we can arrange for the cohomology class represented by κ to be non-trivial.

Proof of Theorem 1.1. In his 2008 lectures from the Clay Summer School in Hawaii, Bellaïche gives a beautiful and conceptual proof of the fact that ρ can be chosen so that the cohomology class represented by κ is non-trivial [1, Proposition 1.4]. He attributes this proof to Serre. Here, we take the more computational approach applied by Ribet.

Since we will be applying a recursive process, let $\rho_1 = \rho$ and write

$$\rho_1(\sigma) = \begin{pmatrix} a_1(\sigma) & b_1(\sigma) \\ c_1(\sigma) & d_1(\sigma \end{pmatrix} \in \mathrm{GL}_2(\mathbf{T}).$$

If π denotes a uniformizer of $K = \mathrm{Frac}(\mathbf{T})$, then we have

$$a_1(\sigma) \equiv \chi_1(\sigma) \pmod{\pi}, \tag{8}$$
$$c_1(\sigma) \equiv 0 \pmod{\pi}, \tag{9}$$
$$d_1(\sigma) \equiv \chi_2(\sigma) \pmod{\pi} \tag{10}$$

for all $\sigma \in \mathcal{G}$. Denote the cocycle constructed in Lemma 2.2 by κ_1.

Suppose that κ_1 represents a trivial cohomology class; then there exists $x_1 \in \mathbf{T}$ such that

$$\kappa_1(\sigma) \equiv (\chi_2^{-1}\chi_1(\sigma) - 1)x_1 \pmod{\pi}$$

for all $\sigma \in \mathcal{G}$, or equivalently,

$$b_1(\sigma) \equiv (\chi_1(\sigma) - \chi_2(\sigma))x_1 \pmod{\pi}. \tag{11}$$

Conjugating the representation ρ_1, we define

$$\rho_2(\sigma) = \begin{pmatrix} a_2(\sigma) & b_2(\sigma) \\ c_2(\sigma) & d_2(\sigma) \end{pmatrix} = \begin{pmatrix} 1 & x_1 \\ 0 & \pi \end{pmatrix} \rho_1(\sigma) \begin{pmatrix} 1 & x_1 \\ 0 & \pi \end{pmatrix}^{-1}.$$

Using the congruences (8)–(11), we find that $\rho_2(\sigma) \in \mathrm{GL}_2(\mathbf{T})$ and furthermore that

$$\begin{aligned} a_2(\sigma) &\equiv \chi_1(\sigma) \pmod{\pi}, \\ c_2(\sigma) &\equiv 0 \pmod{\pi^2}, \\ d_2(\sigma) &\equiv \chi_2(\sigma) \pmod{\pi}. \end{aligned}$$

We are therefore once again in the setting of Lemma 2.2 and obtain a cocycle

$$\kappa_2(\sigma) = \overline{\chi_2}^{-1}(\sigma)\overline{b_2}(\sigma) \in Z^1(\mathcal{G}, \mathbf{T}/\mathfrak{m}(\chi_2^{-1}\chi_1)).$$

If κ_2 represents a nontrivial cohomology class, we are done. If not, we may repeat this process and obtain another representation ρ_3, where now $\pi^3 \mid c_3(\sigma)$. This process continues.

If at any stage, we obtain a cocycle κ_i that represents a non-trivial class, then we are done. If the process continues forever, then one checks that by defining $x = x_1 + \pi x_2 + \pi^2 x_3 + \cdots$, conjugating the original representation ρ_1 by $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ leaves a representation over K with a 0 in the upper right-hand corner. This contradicts the irreducibility of ρ_1. □

3 The Residually Distinguishable Case

In this section, we prove Theorem 1.2. Our complete local ring $\mathbf{T}$ is no longer assumed to be a DVR, but we grant ourselves the assumption $\chi_1 \not\equiv \chi_2 \pmod{\mathfrak{m}}$. Fix $\tau \in \mathcal{G}$ such that

$\chi_1(\tau) \not\equiv \chi_2(\tau) \pmod{\mathfrak{m}}$. By Hensel's Lemma, the congruence (3) implies that $\rho(\tau)$ has two distinct eigenvalues $\lambda_1, \lambda_2 \in \mathbf{T}$ such that

$$\lambda_i \equiv \chi_i(\tau) \pmod{I} \tag{12}$$

for $i = 1, 2$. We choose a basis for ρ over $K = \mathrm{Frac}(\mathbf{T})$ such that

$$\rho(\tau) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

For $\sigma \in \mathcal{G}$, write

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}.$$

Note that unlike the DVR case, we cannot ensure that ρ takes values in $\mathrm{GL}_2(\mathbf{T})$, only $\mathrm{GL}_2(K)$. Nevertheless, we have the following.

Lemma 3.1. *We have $a(\sigma), d(\sigma) \in \mathbf{T}$ for all $\sigma \in \mathcal{G}$, and furthermore*

$$\begin{aligned} a(\sigma) &\equiv \chi_1(\sigma) \pmod{I}, \\ d(\sigma) &\equiv \chi_2(\sigma) \pmod{I}. \end{aligned}$$

Proof. The congruence (3) implies that

$$a(\sigma) + d(\sigma) \equiv \chi_1(\sigma) + \chi_2(\sigma) \pmod{I}. \tag{13}$$

Applying this with σ replaced by $\sigma\tau$, and noting that $a(\sigma\tau) = a(\sigma)\lambda_1$ and $d(\sigma\tau) = d(\sigma)\lambda_2$ by our choice of basis, we obtain

$$a(\sigma)\lambda_1 + d(\sigma)\lambda_2 \equiv \chi_1(\sigma)\chi_1(\tau) + \chi_2(\sigma)\chi_2(\tau). \pmod{I} \tag{14}$$

Solving the congruences (13) and (14) using (12), we find that $a(\sigma), d(\sigma) \in \mathbf{T}$ and furthermore $a(\sigma) \equiv \chi_1(\sigma) \pmod{I}$ and $d(\sigma) \equiv \chi_2(\sigma) \pmod{I}$ as desired. Note that this uses the fact that $\chi_1(\tau) \not\equiv \chi_2(\tau) \pmod{\mathfrak{m}}$ in a crucial way. □

We now let B denote the $\mathbf{T}$-submodule of K spanned by the $b(\sigma)$ for $\sigma \in \mathcal{G}$. Note that the irreducibility assumption on ρ implies that B is a fractional ideal of $\mathbf{T}$. Indeed, if we write K as a product of fields, then the projection of ρ on to each field factor is irreducible, hence the projection of B onto each field factor is nonzero.

In view of the congruences of Lemma 3.1, the equation

$$b(\sigma\sigma') = a(\sigma)b(\sigma') + b(\sigma)d(\sigma')$$

yields

$$\overline{b}(\sigma\sigma') \equiv \chi_1(\sigma)\overline{b}(\sigma') + \chi_2(\sigma')\overline{b}(\sigma) \quad \text{in } B/IB.$$

As in Lemma 2.2, multiplying by $\chi_2^{-1}(\sigma\sigma')$ shows that

$$\kappa(\sigma) = \chi_2^{-1}(\sigma)\bar{b}(\sigma) \in B/IB$$

defines an element of $Z^1(\mathcal{G}, B/IB(\chi_2^{-1}\chi_1))$.

It remains to prove that the cohomology class represented by κ is surjective. Therefore let

$$\kappa'(\sigma) = \kappa(\sigma) + (\chi_2^{-1}\chi_1(\sigma) - 1)x \tag{15}$$

be a cohomologous cocycle, where $x \in B/IB$. Let B' denote the $\mathbf{T}$-submodule of B/IB generated by the values of κ'. Applying (15) to τ and recalling that $\kappa(\tau) = 0$, we see that

$$\kappa'(\tau) = (\chi_2^{-1}\chi_1(\tau) - 1)x \in B'.$$

Since the item in parentheses in a unit in $\mathbf{T}$ by assumption, we find that $x \in B'$. Going back to (15), it follows that $\kappa(\sigma) \in B'$ for all $\sigma \in \mathcal{G}$. But it is clear from the definitions of B and κ that κ generates B/IB, whence $B' = B/IB$ as desired. This completes the proof of Theorem 1.2.

4 The Residually Indistinguishable Case

In the remainder of the paper we describe the proof of Theorem 1.3. Before explaining the definition of the Fitting ideal that appears in the statement of the theorem, we remark that the methods of the previous sections are not directly applicable—in the DVR case, manipulations with the uniformizer π were essential, and in the residually distinguishable case, the basis for ρ afforded by the special element τ was critical. Indeed, in the residually indistinguishable case we do not know how to show that $a(\sigma), d(\sigma) \in \mathbf{T}$ (let alone that the congruences of Lemma 3.1 hold) in *any* basis. A separate construction and proof is required.

As mentioned in the introduction, we will assume for the rest of the paper that χ_1 and χ_2 are trivial; this offers notational simplifications, but no significant changes to the argument.

4.1 Fitting Ideal

Let R be a commutative ring. Let M be a finitely presented R-module. This means that there is a short exact sequence

$$R^n \xrightarrow{f} R^m \longrightarrow M \longrightarrow 0.$$

Definition 4.1. The 0th Fitting ideal of M over R, which we denote $\mathrm{Fitt}_R(M)$, is the ideal of R generated by all $m \times m$ minors of the matrix representing the linear map f. By convention, if $n < m$, then $\mathrm{Fitt}_R(M) = 0$.

We leave the proof of the following basic facts about Fitting ideals as an exercise for the reader (alternatively, she may consult [12]).

Proposition 4.2. *We have the following.*

- *The Fitting ideal* $\mathrm{Fitt}_R(M)$ *depends only on* M *up to* R*-module isomorphism, and not on the particular presentation taken.*
- *If* $I \subset R$ *is a finitely generated ideal, then* $\mathrm{Fitt}_R(R/I) = I$.
- *The Fitting ideal of* M *is contained in the annihilator of* M*:* $\mathrm{Fitt}_R(M) \subset \mathrm{Ann}_R(M)$.
- *If* $R = \mathbf{Z}$ *and* M *is a finitely generated abelian group, then* $\mathrm{Fitt}_{\mathbf{Z}}(M) = 0$ *if* M *is infinite and* $\mathrm{Fitt}_{\mathbf{Z}}(M) = (\#M)$*, the ideal generated by the size of* M*, if* M *is finite.*
- *If* $M \twoheadrightarrow M'$ *is a surjection of finitely presented* R*-modules, then* $\mathrm{Fitt}_R(M') \supset \mathrm{Fitt}_R(M)$.
- *(Base Change) If* S *is an* R*-algebra and* M *is a finitely presented* R*-module, then* $\mathrm{Fitt}_S(M \otimes_R S) = \mathrm{Fitt}_R(M) \cdot S$.

Corollary 4.3. *Let* $\mathbf{T}$ *and* B *be as in Theorem 1.2. Then* $\mathrm{Fitt}_{\mathbf{T}}(B/IB) \subset I$.

Proof. Since B is a fractional ideal of $\mathbf{T}$, it is a faithful $\mathbf{T}$-module, i.e. $\mathrm{Ann}_{\mathbf{T}}(B) = 0$. It follows that $\mathrm{Fitt}_{\mathbf{T}}(B) = 0$. Therefore $\mathrm{Fitt}_{\mathbf{T}/I}(B/IB) = 0$, whence $\mathrm{Fitt}_{\mathbf{T}}(B/IB) \subset I$. □

Motivated by this corollary, one of the insights of Theorem 1.3 is its statement—in the residually indistinguishable case, instead of attempting to necessarily construct a $\mathbf{T}$-module of the form B/IB for a faithful $\mathbf{T}$-module B, one should just attempt to construct some module M such that $\mathrm{Fitt}_{\mathbf{T}}(M) \subset I$.

4.2 Construction of M

To prove Theorem 1.3, we must construct, under the assumptions of the theorem, a finitely generated $\mathbf{T}$-module M such that $\mathrm{Fitt}_{\mathbf{T}}(M) \subset I$ and a surjective cohomology class $\kappa \in H^1(\mathcal{G}, M)$. Since we have specialized to $\chi_1 = \chi_2 = 1$, the $\mathcal{G}$-action on M is trivial, whence $H^1(\mathcal{G}, M)$ is the group of continuous homomorphisms $\mathcal{G} \to M$. Since M is abelian, such a homomorphism necessarily factors through the abelianization $\mathcal{G}^{\mathrm{ab}}$ and thereby induces a $\mathbf{T}$-module map

$$\mathcal{G}^{\mathrm{ab}} \otimes \mathbf{T} \longrightarrow M. \tag{16}$$

The surjectivity of κ is simply the statement that the $\mathbf{T}$-module homomorphism (16) is surjective.

These considerations lead to a very natural construction of the module M. Let Δ denote the augmentation ideal of $\mathcal{G}$ over $\mathbf{T}$, i.e. the kernel of the $\mathbf{T}$-algebra homomorphism

$$\mathbf{T}[\mathcal{G}] \longrightarrow \mathbf{T}, \qquad \sum a_g[g] \mapsto \sum a_g. \tag{17}$$

It is then well-known that we have a $\mathbf{T}$-module isomorphism

$$\Delta/\Delta^2 \cong \mathcal{G}^{\mathrm{ab}} \otimes \mathbf{T}, \qquad \sum a_g[g] \mapsto \sum g \otimes a_g.$$

In order to apply the assumptions of Theorem 1.3, we must invoke the continuous group representation $\rho\colon \mathcal{G} \to \mathrm{GL}_2(K)$. Note that ρ can be extended to a $\mathbf{T}$-algebra homomorphism (also denoted ρ)

$$\mathbf{T}[\mathcal{G}] \longrightarrow M_2(K).$$

We then define

$$M = \rho(\Delta)/\rho(\Delta^2),$$

so there is a canonical surjection

$$\mathcal{G}^{\mathrm{ab}} \otimes \mathbf{T} \cong \Delta/\Delta^2 \xrightarrow{\ \rho\ } M.$$

As explained above, this homomorphism represents a surjective cohomology class

$$\kappa \in H^1(\mathcal{G}, M).$$

It remains to prove that $\mathrm{Fitt}_{\mathbf{T}}(M) \subset I$, and this will take up the remainder of the paper.

4.3 Explication of Fitting Ideal

Since $\mathcal{G}$ is compact and ρ is continuous, the image $\rho(\mathcal{G})$ is a compact subset of $M_2(K)$, and hence $\mathfrak{m}$-adically bounded. The same is therefore true of $\rho(\mathbf{T}[\mathcal{G}])$ and $\rho(\Delta)$. It follows that $\rho(\Delta)$ is a finitely generated $\mathbf{T}$-module, and hence that $M = \rho(\Delta)/\rho(\Delta^2)$ is finitely generated as well.

Let $\rho_1, \ldots, \rho_r$ denote a set of $\mathbf{T}$-module generators for $\rho(\Delta)$, where $\rho_i = \rho(g_i - 1)$ for elements $g_i \in \mathcal{G}$. The images of the ρ_i in M are $\mathbf{T}$-module generators, and there are two types of relations for these generators in M:

- We may have relations
$$\sum_{i=1}^{r} \epsilon_i \rho_i = 0 \text{ in } M_2(K) \tag{18}$$
for constants $\epsilon_i \in \mathbf{T}$. We call these relations of ϵ-type.

- For each pair $1 \leq i, j \leq r$, we may write
$$\rho_i \rho_j = \sum_{k=1}^{r} \delta_{ijk} \rho_k \tag{19}$$
for constants $\delta_{ijk} \in \mathbf{T}$. These expressions vanish in M; we call these relations of δ-type.

The Fitting ideal of M is the ideal generated by all determinants $\det(D)$ where D is an $r \times r$ matrix whose rows have the form $(\epsilon_1, \ldots, \epsilon_r)$ for relations of ϵ-type or $(\delta_{ij1}, \delta_{ij2}, \ldots, \delta_{ijr})$ for relations of δ-type. We need to show that $\det(D) \in I$ for each such matrix D.

4.4 Traces and Determinants

In order to prove that $\det(D) \in I$, we need to generate expressions involving the ρ_i that are known to lie in I. This is given by the following.

Lemma 4.4. *For each $A \in \rho(\Delta)$, we have $\mathrm{tr}(A) \in I$ and $\det(A) \in I$.*

Proof. Let $\chi\colon \mathbf{T}[\mathcal{G}] \longrightarrow \mathbf{T}$ denote the augmentation map defined in (17), i.e. the trivial character of $\mathcal{G}$ extended to a $\mathbf{T}$-algebra homomorphism on $\mathbf{T}[\mathcal{G}]$. The congruence (4) implies that

$$\mathrm{tr}(\rho(g)) \equiv 2\chi(g) \pmod{I}, \qquad \det(\rho(g)) \equiv \chi(g) \pmod{I}$$

for $g \in \mathcal{G}$. A simple argument shows that these congruences extend to all $g \in \mathbf{T}[\mathcal{G}]$ (see [14, Lemma 3.1]). By definition, $\chi(g) = 0$ for $g \in \Delta$. The result follows. □

4.5 An Altered Matrix

Write

$$\rho_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

Given an $r \times r$ matrix D of ϵ-type and δ-type relations as in §4.3, we define an associated matrix D' obtained by altering the rows of D as follows.

- No change for ϵ-type rows.
- For rows of δ-type, replace δ_{ijj} by $\delta_{ijj} - a_i$, replace δ_{iji} by $\delta_{iji} - d_j$, and leave the other δ_{ijk} unchanged.

Lemma 4.5. *We have $\det(D') = 0$.*

Proof. Let

$$w = (b_1, b_2, \ldots, b_r)^T \qquad \text{(column vector)}.$$

We claim that $D'w = 0$. For a row of ϵ-type, the corresponding component of $D'w$ is $\sum_{i=1}^{r} \epsilon_i b_i$. This is the upper right coefficient of the matrix $\sum_{i=1}^{r} \epsilon_i \rho_i$, and hence vanishes by the definition of the ϵ_i (see (18)). Similarly for a row of δ-type, the corresponding component of $D'w$ is

$$\left(\sum_{k=1}^{r} \delta_{ijk} b_k \right) - (a_i b_j + b_i d_j) = 0. \tag{20}$$

The quantity (20) vanishes because each expression in parentheses equals the upper right coefficient of $\rho_i \rho_j$; this follows on the left by the definition (19) of the δ_{ijk}, and on the right by the definition of matrix multiplication.

The ring $K = \mathrm{Frac}(\mathbf{T})$ is a product of fields. To prove $\det(D') = 0$, it suffices to prove this on each field factor of K. Now, in each field factor of K, the projection of some b_i must be

nonzero; otherwise the projection of ρ to that field factor would be lower triangular and hence reducible, contrary to assumption. Therefore the equation $D'w = 0$ implies $\det(D') = 0$ as desired. $\square$

Our goal is to show that $\det(D) \in I$, and we have shown that $\det(D') = 0$. It therefore suffices to show that $\det(D') - \det(D) \in I$. In other words, the alterations used to go from D to D' are small enough to leave the determinant unchanged modulo I. Let us motivate our strategy to prove this with an example.

4.6 An Example

Suppose $r = 2$. We consider a matrix with only rows of δ-type, namely

$$D = \begin{pmatrix} \delta_{121} & \delta_{122} \\ \delta_{211} & \delta_{212} \end{pmatrix}, \qquad \text{whence} \qquad D' = \begin{pmatrix} \delta_{121} - d_2 & \delta_{122} - a_1 \\ \delta_{211} - a_2 & \delta_{212} - d_1 \end{pmatrix}.$$

As shorthand, write $t_i = a_i + d_i$ for the trace of ρ_i. We write $d_{12} = c_1b_2 + d_1d_2$ for the "d"-component of $\rho_1\rho_2$, and $t_{12} = a_{12} + d_{12}$ for the trace of $\rho_1\rho_2$. By multilinearity of the determinant, we have

$$\det(D') - \det(D) = -\det \begin{pmatrix} d_2 & a_1 \\ \delta_{211} & \delta_{212} \end{pmatrix} - \det \begin{pmatrix} \delta_{121} & \delta_{122} \\ a_2 & d_1 \end{pmatrix} + \det \begin{pmatrix} d_2 & a_1 \\ a_2 & d_1 \end{pmatrix}. \tag{21}$$

We evaluate the determinants on the right using the substitution $t_i = a_i + d_i$ where convenient. Then

$$\begin{aligned} \det \begin{pmatrix} d_2 & a_1 \\ \delta_{211} & \delta_{212} \end{pmatrix} &= -t_1\delta_{211} + (d_1\delta_{211} + d_2\delta_{212}) \\ &= -t_1\delta_{211} + d_{21} \qquad (22) \\ &= -t_1\delta_{211} + (c_2b_1 + d_1d_2). \qquad (23) \end{aligned}$$

Note that equation (22) uses the definition of the δ_{ijk}. Similarly

$$\begin{aligned} \det \begin{pmatrix} \delta_{121} & \delta_{122} \\ a_2 & d_1 \end{pmatrix} &= -t_2\delta_{122} + (d_1\delta_{121} + d_2\delta_{122}) \\ &= -t_2\delta_{122} + d_{12} \\ &= -t_2\delta_{122} + (c_1b_2 + d_1d_2). \qquad (24) \end{aligned}$$

Combining (21), (23), and (24), we obtain

$$\begin{aligned} \det(D') - \det(D) &= t_1\delta_{211} - (c_2b_1 + d_2d_1) + \\ &\quad + t_2\delta_{122} - (c_1b_2 + d_1d_2) + \\ &\quad + (d_1d_2 - a_1a_2) \\ &= t_1\delta_{211} + t_2\delta_{122} - t_{12}. \qquad (25) \end{aligned}$$

By Lemma 4.4, the expression (25) lies in I as desired.

5 Formal Variables

We do not know how to establish *explicit* formulae such as (25) to prove that

$$\det(D') - \det(D) \in I$$

in general. Instead, we will prove *abstractly* the existence of polynomial identities such as (25) that express the difference $\det(D') - \det(D)$ in terms of traces and determinants of elements of $\rho(\Delta)$.

For this, it is convenient to shift our perspective from working with the ring $\mathbf{T}$ to working with formal polynomial rings. We will define a polynomial algebra R and a specialization homomorphism $\pi\colon R \longrightarrow K = \mathrm{Frac}(\mathbf{T})$. We will show that the identities we need hold in $R/\ker\pi$, so they apply in $\mathbf{T}$ as well by applying π. The advantage of working in R is that we can identify the subring generated by traces and determinants of matrices mapping to $\rho(\Delta)$ under π as the subspace of invariants under a certain group action, and use cohomological considerations to show that our element of interest lies in this subspace. We now describe this in greater detail.

5.1 The ring R

Define

$$R_0 = \mathbf{Z}[\boldsymbol{\epsilon}_i, \boldsymbol{\delta}_{ijk}],$$

the commutative polynomial ring in r^2 free variables enumerated by the entries of the matrix D. Define

$$R = R_0[\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i, \boldsymbol{d}_i]_{i=1}^r,$$

a commutative polynomial ring in $r^2 + 4r$ free variables. Define a ring homomorphism $R \longrightarrow K$ in the natural way indicated by our variable names, i.e.

$$\pi(\boldsymbol{\epsilon}_i) = \epsilon_i, \quad \pi(\boldsymbol{\delta}_{ijk}) = \delta_{ijk}, \quad \pi(\boldsymbol{a}_i) = a_i, \ldots, \quad \pi(\boldsymbol{d}_i) = d_i.$$

Note that $\pi(R_0) \subset \mathbf{T}$.

Finally, let $\boldsymbol{D}, \boldsymbol{D}' \in M_r(R)$ denote the natural matrices whose images under π are equal D, D', respectively, i.e. they are defined by making each entry bold. Our goal is to prove that

$$\pi(\det(\boldsymbol{D}') - \det(\boldsymbol{D})) = \det(D') - \det(D) \in I.$$

5.2 Relation Ideal

We now define the polynomial relations that allow us to reduce $\det(\boldsymbol{D}') - \det(\boldsymbol{D})$ to an expression involving traces and determinants, as in the example of §4.6. Define

$$\boldsymbol{\rho_i} = \begin{pmatrix} \boldsymbol{a}_i & \boldsymbol{b}_i \\ \boldsymbol{c}_i & \boldsymbol{d}_i \end{pmatrix} \in M_2(R).$$

Let $J \subset R$ be the ideal generated by the following:

- The 4 coefficients of
$$\sum_{i=1}^{r} \boldsymbol{\epsilon}_i \boldsymbol{\rho}_i \tag{26}$$
for each row of ϵ-type in D.

- The 4 coefficients of
$$\boldsymbol{\rho}_i \boldsymbol{\rho}_j - \sum_{k=1}^{r} \boldsymbol{\delta}_{ijk} \boldsymbol{\rho}_k \tag{27}$$
for each row of δ-type in D.

It is clear that $J \subset \ker(\pi)$.

5.3 Subring of traces and determinants

Let $A \subset R$ denote the R_0-subalgebra generated by the traces and determinants of all matrices in the noncommutative $\mathbf{Z}$-algebra generated by the matrices $\boldsymbol{\rho}_i$. Denote by $\overline{A}$ the image of A in R/J. We will show that in order to deduce our desired result $\pi(\det(\boldsymbol{D}') - \det(\boldsymbol{D})) \in I$, it suffices to prove that the image of $\det(\boldsymbol{D}') - \det(\boldsymbol{D})$ in R/J lies in $\overline{A}$. For this, it is important that $\det(\boldsymbol{D}') - \det(\boldsymbol{D})$ lies in the following ideal of R:

$$I_R = \langle \boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i, \boldsymbol{d}_i \rangle.$$

Lemma 5.1. *We have* $\det(\boldsymbol{D}') - \det(\boldsymbol{D}) \in I_R$.

Proof. This follows immediately from multilinearity of the determinant since every entry of $\boldsymbol{D}' - \boldsymbol{D}$ lies in I_R. □

Lemma 5.2. *We have* $\pi(A \cap I_R) \subset I$.

Proof. Let $f \in \mathbf{Z}\langle X_1, \ldots, X_r \rangle$ be an element of the free polynomial algebra in r noncommuting variables. If f has no constant term, then

$$\pi(f(\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_r)) = f(\rho_1, \ldots, \rho_r) \in \rho(\Delta),$$

and hence the trace and determinant of this element lies in I by Lemma 4.4. The element $f(\boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_r)$ clearly has coefficients lying in I_R. From these considerations, to prove the lemma it suffices to prove that $\pi(R_0 \cap I_R) \subset I$. In fact, it is clear that $R_0 \cap I_R = 0$, as

$$R/I_R \cong R_0,$$

with $\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i, \boldsymbol{d}_i \mapsto 0$. This concludes the proof. □

We summarize the result of this section: in order to prove the desired result

$$\det(D') - \det(D) \in I, \tag{28}$$

it suffices to prove that the image of $\det(\boldsymbol{D}') - \det(\boldsymbol{D})$ in R/J lies in the subring $\overline{A}$, the image of A in R/J. Indeed, if this condition holds, then then

$$\det(\boldsymbol{D}') - \det(\boldsymbol{D}) = a + j \tag{29}$$

for some $a \in A, j \in J$. Since $J \subset I_R$, we have $a \in I_R$ by Lemma 5.1 and hence $\pi(a) \in I$ by Lemma 5.2. Since $\pi(j) = 0$, the desired result (28) follows from applying π to (29).

6 Matrix Invariant Theory and Rational Cohomology

The advantage of passing to the ring of formal variables R (rather than working directly with $\mathbf{T}$ and K) is that we may identify the subring $A \subset R$ as the subspace invariant under a group action, rather than needing to write down explicit formulae. To this end, we have the following important classical result, called the fundamental theorem of matrix invariant theory.

Theorem 6.1. *Endow the ring $\mathbf{Z}[\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i, \boldsymbol{d}_i]_{i=1}^r$, with an action of $\mathrm{GL}_2(\mathbf{Z})$ defined by simultaneous conjugation on the matrices $\boldsymbol{\rho}_i = \begin{pmatrix} \boldsymbol{a}_i & \boldsymbol{b}_i \\ \boldsymbol{c}_i & \boldsymbol{d}_i \end{pmatrix}$. The subring of invariant elements is generated over $\mathbf{Z}$ by the traces and determinants of all matrices in the noncommutative algebra generated by the $\boldsymbol{\rho}_i$.*

With notation as in §5.1, we have the following corollary.

Corollary 6.2. *Endow the ring R with an action of $\mathrm{GL}_2(\mathbf{Z})$ defined by simultaneous conjugation on the matrices $\rho_i = \begin{pmatrix} \boldsymbol{a}_i & \boldsymbol{b}_i \\ \boldsymbol{c}_i & \boldsymbol{d}_i \end{pmatrix}$. The subring of invariant elements is equal to A.*

Proof. We may write $R = \mathbf{Z}[\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i, \boldsymbol{d}_i]_{i=1}^r \otimes R_0$, where $\mathrm{GL}_2(\mathbf{Z})$ acts trivially on R_0. Since R_0 is $\mathbf{Z}$-flat, the result follows immediately from Theorem 6.1. □

In our computations, it will be convenient to work with the Borel subgroup of GL_2 consisting of lower triangular matrices. We would like restriction to the Borel to induce an isomorphism on cohomology. This is not true in general for ordinary group cohomology, so for this reason, we must work with the cohomology of algebraic groups called *rational cohomology*. Here "rational" refers to actions defined by rational functions, rather than the rational numbers; throughout, we work integrally over $\mathbf{Z}$.

6.1 Rational cohomology

For simplicity, we will describe algebraic groups and their cohomology through their "functor of points" rather than via group schemes. We therefore view the algebraic group $\mathbf{G} = \mathrm{GL}_2$ as the functor that associates to any commutative ring S the group $\mathrm{GL}_2(S)$.

Definition 6.3. A *rational* $\mathbf{G}$*-module* is a $\mathbf{Z}$-module V endowed with a functorial action, for every ring S, of the group $\mathrm{GL}_2(S)$ on $V \otimes S$, such that the action of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by rational functions in the variables a, b, c, d. We say that V is a rational $\mathbf{G}$-module over a commutative ring R_0 if V has a structure of R_0-module that commutes with the $\mathbf{G}$-action.

Example 6.4. We denote by $\mathcal{A} = \mathbf{Z}A \oplus \mathbf{Z}B \oplus \mathbf{Z}C \oplus \mathbf{Z}D$ the $\mathbf{G}$-module given by the adjoint representation, i.e. if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$\begin{pmatrix} g \cdot A & g \cdot B \\ g \cdot C & g \cdot D \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let $\mathbf{B} \subset \mathbf{G}$ denote the algebraic subgroup of lower triangular matrices. Note that for $g = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$ in $\mathbf{B}$, we have

$$g \cdot A = A + \frac{y}{x}B, \qquad g \cdot B = \frac{z}{x}B, \qquad g \cdot D = D - \frac{y}{x}B.$$

In particular, $\mathbf{Z}B$ is a $\mathbf{B}$-submodule of $\mathcal{A}$.

Definition 6.5 ([9] Ch. 4)**.** If V is a $\mathbf{G}$-module, define the invariants

$$H^0(\mathbf{G}, V) = V^{\mathbf{G}} = \{v \in V : \text{for all commutative rings } A \text{ and } g \in \mathbf{G}(A),\ g \cdot v = v\}.$$

The rational cohomology groups $H^i(\mathbf{G}, -)$ are the right derived functors of $H^0(\mathbf{G}, -)$.

The same definitions hold with $\mathbf{G}$ replaced by $\mathbf{B}$. The following is our motivation for using rational cohomology.

Theorem 6.6. *Let V be a $\mathbf{G}$-module. The restriction map*

$$H^i(\mathbf{G}, V) \to H^i(\mathbf{B}, V)$$

is an isomorphism for all $i \geq 0$.

Proof. See [6, Theorem 4.4] for the general case. In this paper we only need the case that $i = 0$ and V is a finitely generated $\mathbf{Z}$-module, so we describe the proof in this case. Injectivity is clear, so we need only prove surjectivity. Let $\boldsymbol{V}$ denote the spectrum of the tensor algebra of $V^* = \mathrm{Hom}(V, \mathbf{Z})$. This is the affine scheme whose points over a ring S are $\boldsymbol{V}(S) = V \otimes S$.

Let $x \in H^0(\mathbf{B}, V)$. If S is any ring, we can define a map $\mathbf{G}(S) \longrightarrow \boldsymbol{V}(S) = V \otimes S$ by $g \mapsto g \cdot x$. Since $x \in H^0(\mathbf{B}, V)$, this map factors through $G(S)/B(S) = \mathbf{P}^1(S)$. This yields a morphism of schemes $\mathbf{P}^1 \longrightarrow \boldsymbol{V}$. Since $\boldsymbol{V}$ is affine, this morphism must be constant, i.e. $x \in H^0(\mathbf{G}, V)$. □

Corollary 6.7. *We have* $H^0(\mathbf{B}, R) = A$.

Proof. First note that $H^0(\mathbf{G}, R) = A$. Indeed, the inclusion $H^0(\mathbf{G}, R) \supset A$ is clear. Meanwhile the inclusion $H^0(\mathbf{G}, R) \subset A$ follows from Corollary 6.2 and the observation that invariance under $\mathbf{G}$ is stronger than invariance under its group of points $\mathbf{G}(\mathbf{Z})$. The corollary then follows from Theorem 6.6. □

We conclude this section by stating a key input we will need from the cohomology theory of algebraic groups. See [6, §4.2] for a proof.

Theorem 6.8. *Let* $\mathcal{A}$ *be the adjoint representation defined in Example 6.4. For any non-negative integer* k*, the* $\mathbf{B}$*-module* $\mathcal{A}^{\otimes k} \otimes R$ *is acyclic, i.e.* $H^i(\mathbf{B}, \mathcal{A}^{\otimes k} \otimes R) = 0$ *for* $i \geq 1$.

6.2 Roadmap

Let $\boldsymbol{e} = \det(\boldsymbol{D}') - \det(\boldsymbol{D})$ and denote by $\overline{\boldsymbol{e}}$ its image in R/J. Our strategy to prove that $\overline{\boldsymbol{e}}$ lies in $\overline{A}$ is as follows. We will first prove that the ideal J is stable under the action of $\mathbf{B}$. We will then show that

$$\overline{\boldsymbol{e}} \in H^0(\mathbf{B}, R/J).$$

The long exact sequence in rational cohomology associated to

$$0 \longrightarrow J \longrightarrow R \longrightarrow R/J \longrightarrow 0$$

yields an exact sequence

$$H^0(\mathbf{B}, R) = A \longrightarrow H^0(\mathbf{B}, R/J) \xrightarrow{c_J} H^1(\mathbf{B}, J). \tag{30}$$

The equality on the left is Corollary 6.7. Let $\beta \in H^1(\mathbf{B}, J)$ denote the image of $\overline{\boldsymbol{e}}$ under the connecting homomorphism c_J. In view of (30), the desired result $\overline{\boldsymbol{e}} \in \overline{A}$ will follow if we can show that $\beta = 0$.

For this, we will define a certain $\mathbf{B}$-stable subideal $J' \subset J$ and show that in fact

$$\overline{\boldsymbol{e}} \in H^0(\mathbf{B}, R/J').$$

(This is a slight abuse of notation, as here $\overline{\boldsymbol{e}}$ denotes the reduction of $\boldsymbol{e}$ modulo J'.)

We let $\alpha = c_{J'}(\overline{\boldsymbol{e}}) \in H^1(\mathbf{B}, J')$ defined as above. Then $\beta = \iota_*(\alpha)$ where $\iota\colon J' \to J$ is the inclusion and ι_* is the induced map on rational cohomology. To conclude, we will prove that the map

$$\iota_*\colon H^1(\mathbf{B}, J') \longrightarrow H^1(\mathbf{B}, J)$$

vanishes. Therefore $\beta = 0$, and our result follows.

6.3 Invariance

Let $J' \subset J$ denote the subideal generated by the "b" coefficients of the matrices in (26)–(27). To be precise, J' is generated by:

- The elements $\sum_{i=1}^{r} \boldsymbol{\epsilon}_i \boldsymbol{b}_i$ for each row of ϵ-type in D.
- The elements $\boldsymbol{a}_i \boldsymbol{b}_j + \boldsymbol{b}_i \boldsymbol{d}_j - \sum_{k=1}^{r} \boldsymbol{\delta}_{ijk} \boldsymbol{b}_k$ for each row of δ-type in D.

Lemma 6.9. *The ideals J' and J are stable under the action of $\mathbf{B}$. More precisely, the $\mathbf{Z}$-module spanned by each set of 4 relations in (26)–(27) is isomorphic as a $\mathbf{B}$-module to a copy of the adjoint representation $\mathcal{A}$ (see Example 6.4).*

Proof. The relations defining J are linear combinations of products of the $\boldsymbol{\rho}_i$, with coefficients in R_0 (on which $\mathbf{B}$ acts trivially), and the definition of our action is by simultaneous conjugation on $\boldsymbol{\rho}_i$. The second sentence of the Lemma follows. The stability of J' under $\mathbf{B}$ follows since the module of upper right entries $\mathbf{Z}B \subset \mathcal{A}$ is stable under $\mathbf{B}$ (see Example 6.4). □

The goal of the rest of this subsection is to prove the following.

Lemma 6.10. *We have $\overline{\boldsymbol{e}} \in H^0(\mathbf{B}, R/J')$.*

Proof. The matrix $\boldsymbol{D}$ has coefficients in R_0, on which $\mathbf{B}$ acts trivially, so we must show that

$$\overline{\det(\boldsymbol{D}')} \in H^0(\mathbf{B}, R/J').$$

The group $\mathbf{B}$ is generated by elements of the form $\sigma_{x,y} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ and $\tau_x = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$. The matrix $\boldsymbol{D}'$ has coefficients in $R_0[\boldsymbol{a}_i, \boldsymbol{d}_i]$ on which $\sigma_{x,y}$ acts trivially. Therefore we must only consider the action of τ_x.

The difference $\det(\tau_x(\boldsymbol{D}')) - \det(\boldsymbol{D}')$ is a linear combination (with coefficients ± 1) of determinants of all matrices M obtained by starting with $\boldsymbol{D}'$ and replacing some nonempty subset of the rows w with $\tau_x(w) - w$. We will show $\det(M) \in J'$ for each such matrix M.

Rows of ϵ-type in $\boldsymbol{D}'$ contain only the elements $\boldsymbol{\epsilon}_i \in R_0$ that are fixed by the action of $\mathbf{B}$. So any matrix M that contains a row $\tau_x(w) - w = 0$ for a row w of ϵ-type will have determinant 0. Therefore we need only consider matrices M that contain a row $\tau_x(w) - w$ for a row w of δ-type. Conjugation by τ_x sends $\boldsymbol{a}_i \mapsto \boldsymbol{a}_i + \boldsymbol{b}_i x$ and $\boldsymbol{d}_i \mapsto \boldsymbol{d}_i - \boldsymbol{b}_i x$. Say w is associated to a pair (i, j). Then

$$\tau_x(w) - w = (0, 0, \ldots, \boldsymbol{b}_j x, 0, \ldots, -\boldsymbol{b}_i x, 0, \ldots, 0),$$

where there is $\boldsymbol{b}_j x$ in the ith slot and $-\boldsymbol{b}_i x$ in the jth slot. Note that if $i = j$ then $\tau_x(w) - w = 0$ and hence $\det(M) = 0$. So we assume $i \neq j$. We make the following alterations to M which do not change the determinant:

- We replace $\tau_x(w) - w$ by

$$(0, 0, \ldots, x, 0, \ldots, -x, 0, \ldots, 0).$$

  At the same time, in every row other than w we multiply the jth coordinate by $\boldsymbol{b}_j$ and the ith coordinate by $\boldsymbol{b}_i$.

- We then add the new jth column to the new ith column.

- For each $1 \leq k \leq r, k \neq i, j$, we add $\boldsymbol{b}_k$ times the kth column to the new ith column.

In the matrix M that results from these changes, the ith coordinate is precisely the generator of J' associated to the row. Therefore M has an entire column with elements lying in J', so its determinant lies in J' as well. □

6.4 Koszul complex

For simplicity, denote the r elements of J' corresponding to the rows of $\boldsymbol{D'}$ by $B_1, \ldots, B_r$, i.e.

$$\boldsymbol{D'} \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_r \end{pmatrix} = \begin{pmatrix} B_1 \\ \vdots \\ B_r \end{pmatrix}.$$

The rank 1 modules $\mathbf{Z}B_i$ are rational $\mathbf{B}$-representations isomorphic to $\mathbf{Z}B \subset \mathcal{A}$ as in Example 6.4. Let $V = \oplus_{i=1}^r \mathbf{Z}B_i$. Consider the following complex of rational $\mathbf{B}$-representations over R:

$$0 \longrightarrow \left(\bigwedge^r V\right) \otimes R \xrightarrow{f_r} \left(\bigwedge^{r-1} V\right) \otimes R \xrightarrow{f_{r-1}} \cdots \left(\bigwedge^2 V\right) \otimes R \xrightarrow{f_2} V \otimes R \xrightarrow{f_1} R. \tag{31}$$

Here all wedge products and tensor products are over $\mathbf{Z}$. The maps

$$f_i \colon \left(\bigwedge^i V\right) \otimes R \to \left(\bigwedge^{i-1} V\right) \otimes R$$

are given by

$$B_{k_1} \wedge B_{k_2} \wedge \cdots \wedge B_{k_i} \otimes r \mapsto \sum_{j=1}^{i} (-1)^j B_{k_1} \wedge B_{k_2} \wedge \cdots \wedge \hat{B}_{k_j} \wedge \cdots B_{k_i} \otimes B_{k_j} r.$$

Noting that each term $\left(\bigwedge^r V\right) \otimes R$ in (31) is isomorphic to $\bigwedge_R^r (V \otimes R)$, the sequence (31) is precisely the Koszul complex for the free R-module $V \otimes R$. It is therefore exact if we can prove that the elements $B_1, \ldots, B_r$ form a regular sequence in R.

Lemma 6.11. *The elements $B_1, \ldots, B_r$ form a regular sequence in R.*

After enacting the change of variables for rows of δ-type:

$$\delta'_{ijk} = \begin{cases} \delta_{iji} - d_j & k = i \\ \delta_{ijj} - a_i & k = j \\ \delta_{ijk} & k \neq i, j, \end{cases}$$

we see the lemma follows from the following.

Lemma 6.12. *Let S be a commutative ring and let $T = S[x_{ij}]_{i,j=1}^r$. The elements $L_i = \sum_{j=1}^r x_{ij} y_j$ form a regular sequence in $T[y_1, \ldots, y_r]$.*

We leave the proof of Lemma 6.12 as an exercise, referring the reader to [6, Proposition 5.13].

6.5 Embedding into an acyclic complex

Theorem 6.13. *There is a commutative diagram of complexes of rational* **B***-modules*

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & (\bigwedge^r V) \otimes R & \xrightarrow{f_r} & \left(\bigwedge^{r-1} V\right) \otimes R & \xrightarrow{f_{r-1}} & \cdots \left(\bigwedge^2 V\right) \otimes R & \xrightarrow{f_2} & V \otimes R & \xrightarrow{f_1} & J' \\ \downarrow & & \downarrow{\scriptstyle \iota_r} & & \downarrow{\scriptstyle \iota_{r-1}} & & \downarrow{\scriptstyle \iota_2} & & \downarrow{\scriptstyle \iota_1} & & \downarrow{\scriptstyle \iota_0} \\ 0 & \longrightarrow & W_r \otimes R & \xrightarrow{g_r} & W_{r-2} \otimes R & \xrightarrow{g_{r-1}} & \cdots W_2 \otimes R & \xrightarrow{g_2} & W_1 \otimes R & \xrightarrow{g_1} & J, \end{array} \tag{32}$$

where the $W_i \otimes R$ are acyclic **B***-modules for $i \geq 1$.*

Proof. We have already constructed the complex in the top row (see (31)), noting that the image of f_1 is the ideal generated by the B_i, namely J'. Next we define the bottom row. Fix an index $i = 1, \ldots, r$, and suppose that the ith row of D corresponds to a pair (m, n), i.e. we have $B_i = B_{mn}$ where

$$\boldsymbol{\rho}_m \boldsymbol{\rho}_n - \sum_{k=1}^r \boldsymbol{\delta}_{mnk} \boldsymbol{\rho}_k = \begin{pmatrix} A_{mn} & B_{mn} \\ C_{mn} & D_{mn} \end{pmatrix}.$$

We then let

$$\mathcal{A}_i = \mathbf{Z} A_{mn} \oplus \mathbf{Z} B_{mn} \oplus \mathbf{Z} C_{mn} \oplus \mathbf{Z} D_{mn}$$

denote the corresponding copy of the adjoint. Define

$$W_i = \bigoplus_{\{k_1, k_2, \ldots, k_i\} \subset \{1, \ldots, r\}} \mathcal{A}_{k_1} \otimes \cdots \otimes \mathcal{A}_{k_i}.$$

The vertical maps ι_i are given by, for $k_1 < k_2 < \cdots < k_i$,

$$B_{k_1} \wedge \cdots \wedge B_{k_i} \otimes r \mapsto B_{k_1} \otimes \cdots \otimes B_{k_i} \otimes r.$$

The maps g_i are given by:

$$X_1 \otimes X_2 \otimes \cdots \otimes X_i \otimes r \mapsto \sum_{j=1}^{i} (-1)^j X_1 \otimes X_2 \otimes \cdots \hat{X}_j \cdots \otimes X_i \otimes X_j r.$$

The image of the map g_1 is precisely our ideal J. The fact that the bottom row of (32) is a complex, as well as the commutativity of the diagram, is clear. The $\mathbf{B}$-acyclicity of the $W_i \otimes R$ follows from Theorem 6.8. □

6.6 A cascade of cohomology classes

Theorem 6.14. *Let $\iota\colon J' \to J$ be the inclusion and let*

$$\iota_*\colon H^1(\mathbf{B}, J') \longrightarrow H^1(\mathbf{B}, J)$$

be the induced map on first rational cohomology groups. Then $\iota_* = 0$.

Proof. Let the notation be as in Theorem 6.13. Recall $\operatorname{im}(f_1) = J'$. Let

$$\alpha_1 \in H^1(\mathbf{B}, J') = H^1(\mathbf{B}, \operatorname{im}(f_1)).$$

We need to show that $\iota_{0,*}\alpha_1 = 0$. The long exact sequence in cohomology associated to

$$0 \to \ker(f_1) \to V \otimes R \to \operatorname{im}(f_1) \to 0$$

yields a class $\alpha_2 \in H^2(\mathbf{B}, \ker(f_1))$ that represents the obstruction to lifting α_1 to a class in $H^1(\mathbf{B}, V \otimes R)$. Writing $\ker(f_1) = \operatorname{im}(f_2)$, we can view $\alpha_2 \in H^2(\mathbf{B}, \operatorname{im}(f_2))$ and repeat the process above, using the coboundary in the long exact sequence associated to

$$0 \to \ker(f_2) \to \bigwedge^2 V \otimes R \to \operatorname{im}(f_2) \to 0$$

to obtain $\alpha_3 \in H^3(\mathbf{B}, \ker(f_2))$. Continuing in this way we obtain

$$\alpha_i \in H^i(\mathbf{B}, \ker(f_{i-1})) = H^i(\mathbf{B}, \operatorname{im}(f_i))$$

for $i = 1, \ldots, r+1$. Note that $\alpha_{r+1} = 0$ since $\ker(f_r) = 0$.

For each $i = 1, \ldots, r+1$, define

$$\beta_i = \iota_{i-1,*}\alpha_i \in H^i(\mathbf{B}, \operatorname{im}(g_i)).$$

In particular, we have $\beta_1 = \iota_{0,*}\alpha_1$, which is the class we are trying to show vanishes. The bottom row of (32) is a complex but we do not claim it is exact. Nevertheless the obstruction to $\beta_i \in H^i(\mathbf{B}, \operatorname{im}(g_i))$ lifting to a class in $H^i(\mathbf{B}, W_i \otimes R)$ is precisely the image of $\beta_{i+1} \in H^{i+1}(\mathbf{B}, \operatorname{im}(g_{i+1}))$ in $H^{i+1}(\mathbf{B}, \ker(g_i))$. Now $\beta_{r+1} = 0$ since $\alpha_{r+1} = 0$, and hence we conclude that β_r lifts to a class in $H^r(\mathbf{B}, W_r \otimes R)$. However, by acyclicity we have $H^r(\mathbf{B}, W_r \otimes R) = 0$ and hence $\beta_r = 0$. Therefore, β_{r-1} lifts to a class in $H^{r-1}(\mathbf{B}, W_{r-1} \otimes R)$; again this cohomology group vanishes so $\beta_{r-1} = 0$. This downward cascading continues and we obtain $\beta_i = 0$ for all i. In particular $\beta_1 = 0$ as desired. □

As explained in §6.2, Theorem 6.14 implies that $\overline{\boldsymbol{e}} \in H^0(\mathbf{B}, R/J)$ lies in $\overline{A} \subset R/J$. From the discussion of §5.3, it follows that $\det(D') - \det(D) = -\det(D) \in I$. This completes the proof of Theorem 1.3.

References

[1] Joël Bellaïche. Ribet's lemma, generalizations, and pseudocharacters. 2009. `https://people.brandeis.edu/~jbellaic/RibetHawaii3.pdf`.

[2] Joël Bellaïche and Gaëtan Chenevier. Families of Galois representations and Selmer groups. *Astérisque* 324:xii+314, 2009.

[3] R. Brauer and C. Nesbitt. On the modular characters of groups. *Ann. of Math. (2)* 42:556–590, 1941.

[4] Samit Dasgupta and Mahesh Kakde. On the Brumer-Stark conjecture. *Ann. of Math. (2)* 197 (1):289–388, 2023.

[5] Samit Dasgupta, Mahesh Kakde, Jesse Silliman, and Jiuya Wang. The Brumer–Stark Conjecture over $\mathbf{Z}$, 2023.

[6] ———. The Residually Indistinguishable Case of Ribet's Method for GL_2, 2023.

[7] Corrado De Concini and Claudio Procesi. *The invariant theory of matrices*. University Lecture Series, vol. 69. American Mathematical Society, Providence, RI, 2017.

[8] Eric M. Friedlander and Brian J. Parshall. Cohomology of Lie algebras and algebraic groups. *Amer. J. Math.* 108 (1):235–253 (1986), 1986.

[9] Jens Carsten Jantzen. *Representations of algebraic groups*. Mathematical Surveys and Monographs, vol. 107. American Mathematical Society, Providence, RI, 2nd ed., 2003.

[10] Barry Mazur. How can we construct abelian Galois extensions of basic number fields?. *Bull. Amer. Math. Soc. (N.S.)* 48 (2):155–209, 2011.

[11] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.* 76 (2):179–330, 1984.

[12] Andreas Nickel. Notes on noncommutative Fitting invariants. Development of Iwasawa theory—the centennial of K. Iwasawa's birth. Adv. Stud. Pure Math., vol. 86. Math. Soc. Japan, Tokyo., pages 27–60. [2020] ©2020. With an appendix by Henri Johnston and Nickel.

[13] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.* 34 (3):151–162, 1976.

[14] Amit Ophir and Ariel Weiss. On Ribet's Lemma for GL_2 modulo prime powers. 2021. `https://arxiv.org/abs/2111.01559`.

[15] A. Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)* 131 (3):493–540, 1990.