Bloch-Kato Conjecture For The Adjoint Of $H^1(X_0(N))$ With Integral Hecke Algebra

Thesis by

Qiang Lin

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2004

(Defended September 19, 2003)

Acknowledgements

I would like to express to my advisor, Matthias Flach, my great appreciation for his suggestion of the topics, and for his continuous help during my graduate study and the preparation of this thesis. I would like to thank math department of Caltech and Caltech at large for providing a friendly, challenging and encouraging environment.

Abstract

Let M be a motive that is defined over a number field and admits an action of a finite dimensional semisimple $\mathbb{Q}$-algebra T. David Burns and Matthias Flach formulated in [B-F3] a conjecture, which depends on a choice of $\mathbb{Z}$-order $\mathfrak{T}$ in T, for the leading coefficient of the Taylor expansion at 0 of the T-equivariant L-function of M. For primes ℓ outside a finite set we prove the ℓ-primary part of this conjecture for the specific case where M is the trace zero part of the adjoint of $H^1(X_0(N))$ for prime N and where $\mathfrak{T}$ is the (commutative) integral Hecke algebra for cusp forms of weight 2 and the congruence group $\Gamma_0(N)$, thus providing one of the first nontrivial supporting examples for the conjecture in a geometric situation where $\mathfrak{T}$ is not the maximal order of T.

We also compare two Selmer groups, one of which appears in Bloch-Kato conjecture and the other a slight variant of what is defined by A. Wiles. A result on the Fontaine-Laffaille modules with coefficients in a local ring finite free over $\mathbb{Z}_\ell$ is obtained.

2000 Mathematics Subject Classifications: Primary 11F67, 11F80, 11G40; Secondary 14G10, 19F27 Key word and phrases: Burns-Flach conjecture, modular forms, adjoint motives.

Contents

List of Tables

Chapter 1

Introduction to Burns-Flach conjecture

In this chapter we introduce explicitly Burns-Flach conjecture given in [B-F3, §4.3] (which uses the language of perfect complexes and their determinants to virtual objects) for the interested motive here.

1.1 From history to this article

For simplicity, a motive always means the collective data of its various standard realizations and standard compatibility isomorphisms among them, which are essential in order to define its L-function and to state certain conjectures. It also goes by the name "motivic structure" in [F-P2] or "(S-integral) premotivic structure" in [D-F-G2, §1]. The special values of L-functions of motives at integers have long been an inspiring source of number theory.

A recurring phenomenon is that the values of L-functions at integers reflect arithmetic properties of the objects used to define the motives. Two prominent examples are Dirichlet's class number formula and Birch and Swinnerton-Dyer conjecture on elliptic curves.

There are vast amount of work, to compute and various conjectures to predict the value of a general L-function at zero for motive over $\mathbb{Q}$. Conjectures of Deligne [De1] and of Beilinson [Be] achieve that up to a rational factor. Then the seminal conjecture of Bloch-Kato in [B-K] describes the precise value up to sign using cohomological data. Its refinements and reformulations by Fontaine, Kato and Perrin-Riou [Fo1, Ka2, F-P2] are further refined and generalized to a (non-commutative) equivariant version, namely, the equivariant Tamagawa number conjecture of Burns-Flach [B-F3, Conjecture 4], which shall be called "Burns-Flach conjecture" for brevity. For more history of, evidence for and relations among these conjectures and the Iwasawa main conjecture, see [B-F3], [B-F4] and [Hu-Ki].

While the title of this thesis is still paying tribute to Bloch and Kato, its emphasis is on the phrase "with the integral Hecke algebra," indicating that we are actually dealing with Burns-Flach conjecture. A complete title should read as "proof of Bloch-Kato conjecture as refined by Burns-Flach except at finitely many places in the case of the trace zero part of the adjoint motive of $H^1(X_0(N))$ for prime N with the action of integral Hecke algebra for cusp forms of weight 2 and the congruence group $\Gamma_0(N)$." The upshot here is that the integral Hecke algebra is strictly contained in the maximal order of its maximal quotient, thus our proof can be viewed as one of the first examples where Burns-Flach conjecture is finer than previous conjectures. It is expected that Burns-Flach conjecture, will remain open in general for years to come to challenge mathematicians.

We assume that readers are familiar with the standard symbols in number theory and cohomology theory such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Z}_p$, G_K for a field K, $H^i(\cdot,\cdot)$. In particular, $H^i(K,V)$ for a field K and a continuous G_K-module V is the i-th continuous cohomology of G_K with coefficient in V. $\mathcal{O}_R$ is the maximal order of a commutative algebra R over a number field. We use the notation of [D-F-G2, §1] for the various realizations of these motives, as well as for their integral versions by respective Gothic letters. For example, a motive M over a number field K contains M_* for $* = B$, dR and λ (a place of K), which denotes its Betti, de Rham, λ-adic and ℓ-crystalline realization respectively, and correspondingly, its integral version $\mathcal{M}$ contains $\mathcal{M}_*$. We often use "=" to denote the canonical or understood identification between two objects.

1.2 Motives with action of Hecke algebra

Let M be a motive over a number field with an action of a finite dimensional semisimple $\mathbb{Q}$-algebra T . Let $\mathfrak{T} \subset T$ be a $\mathbb{Z}$-order such that there is a projective $\mathfrak{T}$-lattice in the realizations of M. The meaning of "projective" is given in [B-F3, Defintion 1 of §3.3]. Conjecture 4 of loc. cit. concerns the leading coefficient at $s = 0$ of the T-equivariant L-function $L(M,s)$ of M. This is the aforementioned Burns-Flach conjecture, which depends not only on M and T but also on the choice of $\mathfrak{T}$. Roughly speaking, Burns-Flach conjecture specializes to Bloch-Kato conjecture when T is commutative with maximal order $\mathfrak{T}$.

Let $f(\tau) = \sum a_n e^{2\pi i n\tau}$ be a (normalized) newform of congruence group $\Gamma_0(N)$, weight $k \geq 2$. The number field $K_f/\mathbb{Q}$ is generated by the Fourier coefficients a_i of f. We can attach a motive M_f over K_f and its integral version $\mathcal{M}_f$ to f as given in [D-F-G2, §5.4], thanks for the most part to Eichler, Shimura, Deligne, Jannsen, Scholl and Faltings. We reiterate here that a motive is treated naively as the collective data of its realizations and various compatibility isomorphisms among them. We take the trace zero endomorphisms of M_f to obtain the self-dual motive $A_f = \mathrm{ad}^0 M_f = \mathrm{Hom}_{K_f}(M_f, M_f)^0$. (The upper index 0 denotes endomorphisms of trace 0.)

In [D-F-G2, Theorem 8.10] the ℓ-primary part of Bloch-Kato conjecture for A_f, or equivalently, of Burns-Flach conjecture for $M = A_f$, $T = K_f$ and $\mathfrak{T} = \mathcal{O}_{K_f}$, was proven with ℓ outside a certain finite set S_f of primes. See §1.4 for the definition of S_f. Instead of one newform, let us consider a finite set I of newforms f and put

$$M_I = \bigoplus_{f \in I} M_f$$

$$T = \prod_{f \in I} K_f$$

$$A_I = \mathrm{Hom}_T(M_I, M_I)^0 = \bigoplus_{f \in I} A_f$$

$$B_I = A_I(1)$$

This will be our basic setting, upon which much more symbols will be introduced along the way. Note that the above definitions of A_f, M_I, A_I and B_I are kind of symbolic definitions that abstract the natural construction of various components of a motive and also its integral version.

M_I, A_I and B_I are motives with the natural action of the semisimple $\mathbb{Q}$-algebra T as K_f acts on M_f canonically for all $f \in I$. If we take direct product over I, the result of [D-F-G2, Theorem 8.10] also gives the Burns-Flach conjecture for $M = A_I, B_I$ and $\mathfrak{T} = \mathcal{O}_T = \prod_{f \in I} \mathcal{O}_{K_f}$. However, in many natural cases we have the following finer structure. There is an appropriate integral Hecke algebra $\mathfrak{T}$ that is generated by Hecke operators over $\mathbb{Z}$, or equivalently, by Hecke correspondences over $\mathbb{Z}$. The motive M_I carries a lattice, also called the integral version of M_I, which is projective over $\mathfrak{T}$. We have a canonical map $\mathfrak{T} \to T$: $t \mapsto (a_1(t(f))_{f \in I}$, where $a_1(g)$ is the first Fourier coefficient of the q-expansion of a newform g and which is consistent with their action on the motive M_I, A_I and B_I. Hence $\mathfrak{T}$ may be (considered as) contained in, but generally different from, the maximal order of T. This difference will be seen to be a key fact that the importance of this article relies on.

A typical example, which we actually work on in Chapter 3 and Chapter 4, is where I is a complete set of orbit representatives for the action of $G_{\mathbb{Q}}$ on newforms of weight 2 and congruence group $\Gamma_0(N)$ with prime N. Then $M_I = H^1(X_0(N))$, and the integral Hecke algebra $\mathfrak{T}$ generated by Hecke correspondences of $X_0(N)$ over $\mathbb{Z}$ is well known to be an order in T, which can be identified with the set of all correspondences over $\mathbb{Q}$, or with the rational Hecke algebra for cusp forms of weight 2 and the congruence group $\Gamma_0(N)$. Mazur proved in [Ma1, II, (14.2), (16.3), (15.1)] that the integral cohomology $H^1(X_0(N), \mathbb{Z})$ of $X_0(N)$ is locally free (i.e., projective) over $\mathfrak{T}$ except possibly at maximal ideals containing 2. (Just for the record, this exception at the place over 2 might be necessary as indicated by [Ki].) In this case $\mathfrak{T}$ also coincides with the full endomorphism ring of the Jacobian $J_0(N)$ of $X_0(N)$, which is proven in [Ri, Corollary 3.3], and so it is the natural ring to consider when studying the motive $H^1(X_0(N)) = H^1(J_0(N))$.

We will formulate Burns-Flach conjecture for B_I with the action of $\mathfrak{T}$ with the choice of projective $\mathfrak{T}[1/2]$-structure $\mathcal{B}$ that comes from the projective $\mathfrak{T}[1/2]$-module $H^1(X_0(N)(\mathbb{C}), \mathbb{Z}[1/2])$, or more explicitly, from the integral premotivic structure of level N and trivial character in [D-F-G2, \$4.5]. We shall focus on B_I rather than A_I because the methods there apply more directly to B_I (see in particular [D-F-G2, Lemma 8.11]). Once we proved the case on B_I, the desired result on A_I can be formulated similarly and can be seen along the same line of arguments.

1.3 Explicit Deligne's conjecture

To prepare for the statement of the Burns-Flach conjecture in \$1.4, we introduce in this section Theorem 8.5 of [D-F-G2] that is an explicit form of Deligne's conjecture.

With the index set I implicitly understood, we will write M, A, B, T instead of M_I, A_I, B_I, T_I. Throughout this article the L-functions of A and B, $L(A,s)$ and $L(B,s)$, are their T-equivariant L-functions, whose definition is given in [D-F-G2, §4] and in particular, its Remark 7.

Recall that $\mathbf{I}_{K_f}$ was defined in [D-F-G2, §1.2] as the set of embeddings $\mathrm{Hom}(K_f,\mathbb{C})$. We let $\mathbf{I}_T = \mathrm{Hom}(T,\mathbb{C})$ denote the set of ring homomorphisms $T \to \mathbb{C}$ and we then have $\mathbf{I}_T = \coprod_{f\in I} \mathbf{I}_{K_f}$. We view $L(A_f,s)$ as the tuple of functions $L(A_f,\tau,s)_{\tau\in\mathbf{I}_K}$, i.e., as a holomorphic function with values in

$$(K_f)_{\mathbb{C}} := K_f \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}^{\mathbf{I}_{K_f}}.$$

Similarly we view $L(A,s)$ as a function with values in $T_{\mathbb{C}} := T \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^{I_T}$. The special values $L(A,0)$ and $L(B,0) = L(A,1)$ then lie in $T_{\mathbb{R}} := T \otimes_{\mathbb{Q}} \mathbb{R}$.

We revert M temporarily to mean a motive with coefficients in K so as to introduce several symbols the last of which is Deligne's period $c^+(M)$. The fundamental line for M is the K-line defined by

$$\Delta(M) = \mathrm{hom}_K(\det_K M_B^+, \det_K t_M)$$

where $^+$ indicates the subspace fixed by F_∞, the action of complex conjugation, and $t_M = M_{\mathrm{dR}}/\operatorname{Fil}^0 M_{\mathrm{dR}}$. Furthermore the composition of

$$\mathbb{R}\otimes M_B^+ \to (\mathbb{C}\otimes M_B)^+ \xrightarrow{(I^\infty)^{-1}} \mathbb{R}\otimes M_{\mathrm{dR}} \to \mathbb{R}\otimes t_M$$

is an $\mathbb{R}\otimes K$-linear isomorphism. Its determinant over $\mathbb{R}\otimes K$, called Deligne's period of M and denoted by $c^+(M)$, defines a basis for $\mathbb{R}\otimes\Delta(M)$.

Now we quote verbatim Theorem 8.5 of [D-F-G2], which is an explicit form of Deligne's conjecture in the cases of A_f and B_f for a newform f of weight k, conductor N_f, character ψ, and field of definition K_f.

Theorem 1.3.1. *Let $b(A_f)\in\Delta(A_f)$ be defined by the formula*

$$\langle f, b(A_f)(f\otimes F_\infty)\rangle = \frac{i^{k-\eta}((k-2)!)^2\epsilon(M_f\otimes M_{\psi^{-1}})\prod_{p\in\Sigma_e(f)}(1+\frac{1}{p})}{2\epsilon(M_{\psi^{-1}})\epsilon(A_f)}(b_{\mathrm{dR}}\otimes\iota^{k-1}),$$

and $b(B_f)\in\Delta(B_f)$ by the formula

$$b(B_f) = (1-k)\epsilon(A_f)\mathrm{tw}(b(A_f)). \tag{1.1}$$

Then $L(A_f,0)(1\otimes b(A_f)) = c^+(A_f)$ and $L(B_f,0)(1\otimes b(B_f)) = c^+(B_f)$.

We explain very briefly the content of this theorem below. Readers are advised to check the original paper for a full explanation. The fundamental line $\Delta(A_f)$ is identified with

$$\hom_K(\mathrm{Fil}^{k-1}M_{f,\mathrm{dR}}\otimes\mathbb{Q}\cdot F_\infty, M_{f,\mathrm{dR}}/\mathrm{Fil}^{k-1}M_{f,\mathrm{dR}}).$$

There is also a perfect alternating pairing induced from the Poincaré duality for $X_1(N)$,

$$\langle\cdot,\cdot\rangle \;:\; M_f\otimes_{K_f}M_f\to M_\psi(1-k),$$

where $M_\psi(1-k)$ denotes the $(1-k)$-Tate twist of the Dirichlet motive associated to ψ. F_∞ is naturally viewed as a basis of $A^+_{f,B}$.

$\eta = 0$ or 1 so that $\eta \equiv k \bmod 2$. $\epsilon(M)$ is the well-known epsilon factor appearing in the functional equation of a motive M defined in [De2] or [Ta, Theorem 3.4.1].

$\Sigma_e(f)$ is the set of primes p such that $M^{I_p}_{f,\lambda} = 0$ for any $\lambda \nmid p$ and $L_p(A_f, s) = (1+p^{-s})^{-1}$. A basis of $M_{\psi,\mathrm{dR}}$ is

$$b_{\mathrm{dR}} = \sum_{a \in (\mathbb{Z}/N_f\mathbb{Z})^\times} \psi(a) \otimes e^{2\pi i a/N_f} \in \mathcal{O}_{K_f} \otimes \mathcal{O}_{\mathbb{Q}[e^{2\pi i/N_f}]})[1/N_f],$$

ι is the canonical basis of $\mathcal{T}_{\mathrm{dR}}$, where $\mathcal{T}$ is the "dual of integral Tate motive."

Identifying $\Delta(B_f)$ with

$$\hom_K(\mathrm{Fil}^{k-1} M_{f,\mathrm{dR}} \otimes \mathbb{Q}(2)_B, (M_{f,\mathrm{dR}}/\,\mathrm{Fil}^{k-1} M_{f,\mathrm{dR}}) \otimes \mathbb{Q}(2)_{\mathrm{dR}}),$$

we define the isomorphism of K-lines

$$\mathrm{tw} : \Delta(A_f) \to \Delta(B_f) \tag{1.2}$$

so that $\mathrm{tw}(\phi)(x \otimes y) = \phi(x \otimes F_\infty) \otimes \beta(y)$, where the basis β of $\Delta(\mathbb{Q}(2))$ sends $(2\pi i)^2$ to ι^{-2}. This ends our explanation of Theorem 1.3.1.

The fundamental line $\Delta(A)$ is a free rank one T-module with basis

$$b(A) = \prod_{f \in I} b(A_f).$$

We also have $c^+(A) = \prod_{f \in I} c^+(A_f)$. In general, by taking the direct product over I, all computations in [D-F-G2, §8.2] immediately carry over from A_f, B_f, K_f etc. to A_I, B_I, T_I etc.

Remark 1.3.2. *Deligne's conjecture predicts that $L(A_f, 0)^{-1} c^+(A_f) \in \mathbb{R} \otimes \Delta(A_f)$ is an element in its T-rational subspace $1 \otimes \Delta(A_f) = \Delta(A_f)$. The above theorem computes explicitly that this value is $b(A_f) \in \Delta(A_f)$. The same applied to B_f. Taking direct product over I, we obtain the later equality in (1.9).*

1.4 The Burns-Flach conjecture in our case

Our choice of integral version $\mathcal{M}$ of M comes from [D-F-G2]. Specifically, $\mathcal{M}_f$ is the integral premotivic structure associated to f defined in §5.4 of loc. cit. We construct $\mathcal{M}$ from all $\mathcal{M}_f$, $f \in I$ and then $\mathcal{A}$ and $\mathcal{B}$ from $\mathcal{M}$ naturally. Note that this choice is the same as in the typical example mentioned in §1.2.

We denote by S_I the set of prime numbers ℓ so that there exists an $f \in I$ and $\lambda \in S_f$ with $\lambda \mid \ell$. Here S_f is the finite set of primes λ in K_f such that either $\lambda \mid Nk!$ or the two-dimensional residual Galois representation $\mathcal{M}_{f,\lambda}/\lambda\mathcal{M}_{f,\lambda}$ is not absolutely irreducible when restricted to G_F, where

$F = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$ and $\lambda \mid \ell$. Clearly, we only expect to prove the Burns-Flach conjecture for primes $\ell \notin S_I$ as our result will be built on the result of [D-F-G2, §8].

Recall M means M_I. $\mathcal{M}_\ell$, a Galois stable lattice inside M_ℓ, is assumed to be free of rank two over the semilocal finite flat $\mathbb{Z}_\ell$-algebra $\mathfrak{T}_\ell := \mathfrak{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. We have $\mathcal{B}_\ell = \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_\ell, \mathcal{M}_\ell)^0(1)$ is a free $\mathfrak{T}_\ell$-module of rank 3.

Let

$$D_\ell := D_{\mathrm{crys}}(B_\ell) := H^0(\mathbb{Q}_\ell, B_{\mathrm{crys},\ell} \otimes_{\mathbb{Q}_\ell} B_\ell),$$

which is free of rank 3 over T_ℓ and

$$t_B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong t_{B_\ell} := D_\ell / \operatorname{Fil}^0 D_\ell, \tag{1.3}$$

which is free of rank 2 over T_ℓ. For each place v of $\mathbb{Q}$ I_v is a fixed choice of inertia group and ϕ_v is the geometric Frobenius. We define a perfect complex of T_ℓ-modules

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) := \begin{cases} H^0(I_v, B_\ell) \xrightarrow{1-\phi_v} H^0(I_v, B_\ell) & \text{for } v \neq \ell, \\ D_\ell \xrightarrow{(1-\phi_v,\pi)} D_\ell \oplus t_{B_\ell} & \text{for } v = \ell. \end{cases}$$

So we have a canonical isomorphism of (graded) invertible T_ℓ-modules

$$\operatorname{Det}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) := \begin{cases} \operatorname{Det}_{T_\ell} H^0(I_v, B_\ell) \otimes \operatorname{Det}^{-1}_{T_\ell} H^0(I_v, B_\ell) \cong T_\ell & \text{for } v \neq \ell \\ \operatorname{Det}_{T_\ell} D_\ell \otimes \operatorname{Det}^{-1}_{T_\ell} D_\ell \otimes \operatorname{Det}^{-1}_{T_\ell} t_{B_\ell} \cong \operatorname{Det}^{-1}_{T_\ell} t_{B_\ell} & \text{for } v = \ell. \end{cases} \tag{1.4}$$

For the usage of the determinant functor Det here, readers may see [K-M]. For the importance of keeping gradation data, see [B-F3, Remark 9].

As explained in [B-F3, §3.2] one can construct a natural morphism

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) \to R\Gamma(\mathbb{Q}_v, B_\ell), \tag{1.5}$$

the mapping cone of which we denote by $R\Gamma_{/\mathbf{f}}(\mathbb{Q}_v, B_\ell)$.

The comparison isomorphism between etale and singular cohomology induces an isomorphism

$$R\Gamma(\mathbb{R}, B_\ell) \cong \mathbb{Q}_\ell \otimes_{\mathbb{Q}} B_B^+. \tag{1.6}$$

Let S_{bad} be the set of places v of $\mathbb{Q}$ where M has bad reduction (i.e., where $M_\ell^{I_v} \neq M_\ell$) and put $S = S_{\text{bad}} \cup \{\ell, \infty\}$. Define

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}, B_\ell) = \operatorname{Cone}(R\Gamma_{\text{et}}(\mathbb{Z}_S, B_\ell) \to \bigoplus_{v \in S_{\text{bad}} \cup \{\ell\}} R\Gamma_{/\mathbf{f}}(\mathbb{Q}_v, B_\ell))[-1]. \tag{1.7}$$

Then there is an exact triangle (of perfect complexes of T_ℓ-modules)

$$R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S, B_\ell) \to R\Gamma_{\mathbf{f}}(\mathbb{Q}, B_\ell) \to \bigoplus_{v \in S_{\mathrm{bad}} \cup \{\ell\}} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) \oplus R\Gamma(\mathbb{R}, B_\ell). \quad (1.8)$$

By [B-F3, Lemma 19] and [D-F-G2, Theorem 8.2] the complex $R\Gamma_{\mathbf{f}}(\mathbb{Q}, B_\ell)$ is acyclic. So the triangle (1.8) together with (1.3), (1.4) and (1.6) induces an isomorphism of (graded) determinants

$$\begin{aligned}\vartheta_\ell : \mathrm{Det}_{T_\ell} R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S, B_\ell) &\cong \bigotimes_{v \in S_{\mathrm{bad}} \cup \{\ell\}} \mathrm{Det}^{-1}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) \otimes \mathrm{Det}^{-1}_{T_\ell} R\Gamma(\mathbb{R}, B_\ell) \\ &\cong \mathrm{Det}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} t_B) \otimes \mathrm{Det}^{-1}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} B^+_B).\end{aligned}$$

Conjecture 1.4.1. *(The ℓ-primary part of Burns-Flach conjecture for the motive $\mathcal{B}$ with the action of $\mathfrak{T}$ and $\ell \notin S_I$) there is an identity of invertible $\mathfrak{T}_\ell$-modules*

$$\vartheta_\ell(\mathrm{Det}_{\mathfrak{T}_\ell} R\Gamma_{et,c}(\mathbb{Z}_S, \mathcal{B}_\ell)) = \mathfrak{T}_\ell \cdot b(B) = \mathfrak{T}_\ell \cdot L(B,0)^{-1} c^+(B). \quad (1.9)$$

Remark 1.4.2. *The conjecture can be formulated and expected to hold for all ℓ. The restriction on ℓ is only to emphasize our inability to prove the excluded cases because our proof relies on [D-F-G2].*

By its totality Burns-Flach conjecture means the Conjecture 4 in [B-F3], which consists of four parts. For motive B, part (i), (ii) and (iii) can be established readily. What we have (re)formulated here is actually the Conjecture

6 in loc. cit., whose validity for all primes is equivalent to part (iv).

Remark 1.4.3. *[F-P1] shows that the ℓ-primary part of Bloch-Kato conjecture is equivalent to the equality* $\vartheta_\ell(\mathrm{Det}_{\mathcal{O}_{T_\ell}} R\Gamma_{et,c}(\mathbb{Z}_S, \mathcal{B}_\ell \otimes_{\mathfrak{T}_\ell} \mathcal{O}_{T_\ell})) = \mathcal{O}_{T_\ell} \cdot L(B,0)^{-1}c^+(B)$*, which determines ℓ-primary parts of* $L(B_f,0)^{-1} \cdot c^+(B_f)$ *up to multiplication by an element in* $(\mathcal{O}_{K_f} \otimes \mathbb{Z}_\ell)^\times$ *for all $f \in I$ once we decompose each sides into its components. The equality* (1.9) *further reduces the uncertainty of determining the ℓ-primary parts of the special values by an algebraic formula, which is the main point of Burns-Flach conjecture compared to Bloch-Kato conjecture in this simplest non-trivial case. The exact extent to which this ℓ-primary part of Burns-Flach conjecture for $\mathcal{B}_I$ is finer than the combination of those of Bloch-Kato conjecture for all B_f, $f \in I$, is measured by (the cardinality of) the finite group*

$$\mathcal{O}_{T_\ell}^\times / \mathfrak{T}_\ell^\times .$$

Chapter 2

An isomorphism between tangent space and Selmer group

In the deformation theory of Galois representations there is a standard isomorphism between the relative Zariski tangent space of the universal deformation ring with a Selmer group, (i.e., a subspace of a global Galois cohomology group cut out by local conditions). This chapter is to prove in detail a variant of that isomorphism as shown in equality (2.1), which appears in [Ma2] with incomplete proof. This will be used in the next chapter. This variant, while of interest by itself, will be one of the critical steps in proving our case of Burns-Flach conjecture.

2.1 Notation

Maps between objects that are naturally topological spaces are continuous. Galois groups are topological spaces with the canonical profinite topology. Any module that is a $\mathbb{Z}_\ell$-module by restriction of scalars is equipped with the ℓ-adic topology. When we refer to an RG- module M, where M is a topological space, R a ring and G a topological group, we mean an R-module M with an R-linear continuous G-action. $H^i(G,V)$ is the continuous cochain cohomology group of G with coefficients in a continuous G-module V.

First, we introduce the common setting of both sides of the isomorphism. Let $G_{\mathbb{Q}}$ be the absolute Galois group after we fix an algebraic closure of $\mathbb{Q}$. Fix a decomposition group $G_p \subset G_{\mathbb{Q}}$ for all primes p in $\mathbb{Z}$ and $I_p \subset G_p$ its inertia group. Let ℓ be a fixed odd prime so that our representation spaces will be ℓ-adic and Σ a finite set of rational primes different from ℓ. A is a commutative complete local ring that is finite free over $\mathbb{Z}_\ell$ and whose residue field is k. Let L be a (continuous) $AG_{\mathbb{Q}}$-module that is free of rank two over A.

Let $\mathfrak{FR}$ be the full subcategory of finite $\mathbb{Z}_\ell G_\ell$-modules whose objects are quotients of G_ℓ-stable lattices in short crystalline $\mathbb{Q}_\ell$ representations of G_ℓ, where short representation V means that $\mathrm{Fil}^\ell D(V) = 0$ and $\mathrm{Fil}^0 D(V) = D(V)$, where $D(V) = (B_{\mathrm{crys},\ell} \otimes_{\mathbb{Q}_\ell} V)^{G_\ell}$ and that V has no nonzero subrepresentation V' so that $V'(\ell-1)$ is unramified. $\mathfrak{FR}$ is stable under taking finite direct sums, subobject and quotients in the category of finite $\mathbb{Z}_\ell G_\ell$-modules, and that it is equivalent to the category $\mathcal{MF}^0_{\mathrm{tor}}$ that is defined in §5.1. We assume that $L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a short crystalline representation.

Now we introduce the objects related to the right hand side of the isomorphism (i.e., the Selmer group side).

$W = \mathrm{End}^0_A(L) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell$, where $\mathrm{End}^0_A(L)$ denotes the kernel of the trace map $\mathrm{End}_A(L) \to A$. Note that W is an $AG_{\mathbb{Q}}$-module as the trace map is an $AG_{\mathbb{Q}}$-module homomorphism. $W_n = W[\ell^n] = \mathrm{End}^0_A(L) \otimes_{\mathbb{Z}_\ell} (\ell^{-n}\mathbb{Z}_\ell)/\mathbb{Z}_\ell = \mathrm{End}^0_A(L/\ell^n L) \subset \mathrm{End}_A(L/\ell^n L)$ where the last equality is given by $f \otimes_{\mathbb{Z}_\ell} (\ell^{-n} \bmod \mathbb{Z}_\ell) \mapsto f \otimes_{\mathbb{Z}_\ell} \mathrm{id}_{\mathbb{Z}_\ell/\ell^n} \in \mathrm{End}_{A\otimes_{\mathbb{Z}_\ell}\mathbb{Z}_\ell}(L \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell/\ell^n) = \mathrm{End}_A(L/\ell^n L)$. Here we use that A is finite free over $\mathbb{Z}_\ell$. Note that $W = \cup_n W_n = \varinjlim W_n$. W and W_n for all n have the (natural) discrete topologies.

For $p \neq \ell$, $H^1_f(G_p, W_n) = \ker(H^1(G_p, W_n) \to H^1(I_p, W_n))$. For $p = \ell$, recall there is a canonical A/ℓ^n-linear isomorphism between $H^1(G_\ell, \mathrm{End}_A(L/\ell^n L))$ and the A/ℓ^n-module of Yoneda extensions of $A/\ell^n G_\ell$-modules $0 \to L/\ell^n L \to E \to L/\ell^n L \to 0$ as $L/\ell^n L$ is a free A/ℓ^n-module. $H^1_f(G_\ell, W_n) \subset H^1(G_\ell, W_n)$ is the set of elements that corresponds to extensions E in $\mathfrak{FR}$ when mapped into $H^1(G_\ell, \mathrm{End}_A(L/\ell^n L))$. One checks that $H^1_f(G_\ell, W_n)$ is an A-submodule of $H^1(G_\ell, W_n)$. $H^1_f(G_p, W) = \varinjlim H^1_f(G_p, W_n)$ for every prime p. In particular, for $p \neq \ell$, $H^1_f(G_p, W) = \ker(H^1(G_p, W) \to H^1(I_p, W)) = H^1(G_{\mathbb{F}_p}, W^{I_p})$.

We note that $\varinjlim H^1(G_p, W_n) = H^1(G_p, W)$ because of the compactness of G_p and the discreteness of the topology of W. So $H^1_f(G_p, W)$ is a subset of $H^1(G_p, W)$. $H^1_\Sigma(G_{\mathbb{Q}}, W) \subset H^1(G_{\mathbb{Q}}, W)$ is the set of elements that are in $H^1_f(G_p, W)$ when restricted to $H^1(G_p, W)$ for every $p \notin \Sigma$. $H^1_\Sigma(G_{\mathbb{Q}}, W_n) \subset H^1(G_{\mathbb{Q}}, W_n)$ is the set of elements that are in $H^1_f(G_p, W_n)$ when restricted to $H^1(G_p, W_n)$ for every $p \notin \Sigma$.

All of above cohomology groups are naturally A-modules. The Selmer groups $H^1_\Sigma(G_{\mathbb{Q}}, W)$ and $H^1_\Sigma(G_{\mathbb{Q}}, W_n)$ depend on L as a $G_{\mathbb{Q}}$-module, not on the choice of G_p of any p.

Finally, we come to the setting of the left hand side of the isomorphism (i.e., the deformation theory side). Let k be the finite residue field of A whose characteristic is ℓ. Fix a basis of L over A so that the action of $G_{\mathbb{Q}}$ on L has a matrix representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$$

and its residual matrix representation

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k).$$

Let $\mathcal{O}$ be a complete local noetherian ring with residue field k. Let $\mathcal{C}_{\mathcal{O}} = \mathcal{C}$ denote the category whose objects are complete local noetherian $\mathcal{O}$-algebras and whose morphisms are local $\mathcal{O}$-algebra homomorphisms. Hence k and $\mathcal{O}$ are objects of $\mathcal{C}$. There is a canonical map from $\mathbb{Z}_\ell$ to any object of $\mathcal{C}$. We require that A is an object in $\mathcal{C}$ and hence that $\mathcal{O}$ has the same characteristic 0 as A. For example, we can take $\mathcal{O}$ to be A, or the canonical subring $W(k)$ of A, which is the ring of Witt vectors with coefficients in k.

Recall that if R is an object of $\mathcal{C}$, then an R-deformation of $\bar{\rho}$ is a strict equivalence class of liftings of $\bar{\rho}$ to $\mathrm{GL}_2(R)$ [Ma3, §8].

We say that an R-deformation is of type Σ if a lifting representing that deformation, whose representation space is M, satisfies the following conditions, which will be referred to individually by the phrases in the parenthesis:

- the $RG_{\mathbb{Q}}$-module M is minimally ramified outside $\Sigma \cup \{\ell\}$, where minimal ramification is defined in [Di], (minimal ramification);

- for every $n > 0$, the $\mathbb{Z}_\ell G_\ell$-module $M/\mathfrak{M}^n M$ is an object of the category $\mathcal{FR}$, where $\mathfrak{M}$ is the maximal ideal of R, (crystalline ramification);

- $\wedge_R^2 M$ is the one dimensional representation over R whose character is the ℓ-cyclotomic character composed with the canonical map from $\mathbb{Z}_\ell$ to R, (fixed determinant).

Assume $\bar{\rho}$ itself is a deformation of type Σ so that we can consider the functor $\mathcal{D}_\Sigma$ on $\mathcal{C}$ that associates to R the set of R-deformations of $\bar{\rho}$ of type Σ. Assume further that $\bar{\rho}$ is absolutely irreducible. By the results of Mazur [Ma3] and Ramakrishna [Ra], this functor is representable by an object of $\mathcal{C}$ that is called the universal deformation ring attached to $\bar{\rho}$ with base ring $\mathcal{O}$ of type Σ. We denote this object $R^{\rho,\mathcal{O},\Sigma}$ or simply R^Σ.

If ρ is a deformation of type Σ, the universality of R^Σ induces a ring homomorphism $\theta_\rho^\Sigma : R^\Sigma \to A$, by which A becomes an R^Σ-algebra.

2.2 The isomorphism

The standard isomorphism mentioned in the beginning of this chapter is, in our context, of the form $\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, A) = H^1_\Sigma(G_\mathbb{Q}, \mathrm{End}^0_A(L))$, where the right hand side is a suitable subset of $H^1(G_\mathbb{Q}, \mathrm{End}^0_A(L))$. However, what we will need is the following variant:

Proposition 2.2.1. *With the notation and assumptions of previous para-*

graphs, we have a canonical A-module isomorphism:

$$\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell) \cong H^1_\Sigma(G_\mathbb{Q}, W), \tag{2.1}$$

where $\Omega_{R^\Sigma/\mathcal{O}}$ is the topological R^Σ-module of relative continuous Kähler differentials of $\mathcal{O}$-algebra R^Σ that represents the functor $M \mapsto \mathrm{Der}_\mathcal{O}(R^\Sigma, M)$ for a topological R^Σ-module M.

Proof. It suffices to show the following three claims.

- $H^1_\Sigma(G_\mathbb{Q}, W) \cong \varinjlim H^1_\Sigma(G_\mathbb{Q}, W_n)$.
- $\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell) \cong \varinjlim \hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \ell^{-n}A/A)$, where $\ell^{-n}A/A$ is a shorthand for $A \otimes_{\mathbb{Z}_\ell} \ell^{-n}\mathbb{Z}_\ell/\mathbb{Z}_\ell$.
- There exists a canonical A-module isomorphism

$$\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \ell^{-n}A/A) \to H^1_\Sigma(G_\mathbb{Q}, W_n)$$

  that makes the following diagram commute,

$$\begin{array}{ccc} \hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \ell^{-n}A/A) & \to & H^1_\Sigma(G_\mathbb{Q}, W_n) \\ \downarrow & & \downarrow \\ \hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \ell^{-n-1}A/A) & \to & H^1_\Sigma(G_\mathbb{Q}, W_{n+1}). \end{array}$$

Proof of the first claim.

There is a natural map from the right hand side to the left hand side induced by the inclusion $W_n \to W$. That map is injective because of the compactness of $G_{\mathbb{Q}}$ and the discreteness of the topology of W since a (continuous) map from a compact space to a discrete space has only finitely many values. Now we prove surjectivity. Take any $\bar{c} \in H^1_\Sigma(G_{\mathbb{Q}}, W)$, which is represented by a cocycle $c : G_{\mathbb{Q}} \to W$, whose restriction to G_p, name it c_p, represents an element in $H^1_f(G_p, W) = \varinjlim H^1_f(G_p, W_n)$ for all $p \notin \Sigma$. As no confusion can arise, we will also use the same symbol for a cocycle if we restrict its domain and/or its codomain to a smaller one. As we have just said, c has only finitely many values. Suppose these values are in W_m for some m. By the deformation condition of minimal ramification, ρ is unramified at a prime when so is $\bar{\rho}$. Since the image of $\bar{\rho}$ is finite, $\bar{\rho}$ is unramified outside a set S of finitely many primes and hence so is ρ. For all primes $p \notin S \cup \Sigma$,

$$\begin{aligned} H^1_f(G_p, W) &= \varinjlim \ker(H^1(G_p, W_n) \to H^1(I_p, W_n)) \\ &= \ker(H^1(G_p, W) \to H^1(I_p, W)), \end{aligned}$$

where $H^1(I_p, W) = \hom(I_p, W)$ as I_p acts trivially on W. So, c is trivial on I_p. Hence c_p represents an element in $H^1_f(G_p, W_n)$ for all n. For all primes p in the finite set $S - \Sigma$, c_p represents an element in $H^1_f(G_p, W_{n_0})$ simultaneously for a $n_0 \geq m$ that is large enough. Hence, c also represents an element in $H^1_\Sigma(G_{\mathbb{Q}}, W_{n_0})$. This means the surjectivity we want.

Proof of the second claim.

Since $A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell = \cup_n \ell^{-n} A/A$, it suffices to prove $\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A$ is a finitely generated A-module, or, equivalently, $\Omega_{R^\Sigma/\mathcal{O}}$ is a finitely generated R^Σ-module. By Cohen structure theorem on complete local Noetherian rings of unequal characteristics as discussed after [Ei, Theorem 7.8] we have

$$R^\Sigma \cong T/I,$$

where $T = W(k)[[x_1, \cdots, x_r]]$ for an integer r, I an ideal of T. Recall there is a canonical homomorphism from $W(k)$ to any complete local ring with residue field k, which manifests in the isomorphism above. Thus $\mathcal{O}$ can be viewed as a sub-$W(k)$-algebra of R^Σ via the structure map $\mathcal{O} \to R^\Sigma$. We have two canonical R^Σ-module surjections:

$$R^\Sigma \hat{\otimes}_T \Omega_{T/W(k)} \to \Omega_{R^\Sigma/W(k)} \to \Omega_{R^\Sigma/\mathcal{O}},$$

where $\hat{\otimes}$ denotes completed tensor product. See §5.2.3 of [Hi2]. Since $\Omega_{T/W(k)}$ is a free T-module of rank r, $\Omega_{R^\Sigma/\mathcal{O}}$ is a finitely generated R^Σ-module.

Proof of the third claim.

The method is explained partially by B. Mazur in [Ma2]. We have

$$
\begin{aligned}
&\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \ell^{-n}A/A) \\
&= \hom_{R^\Sigma}(\Omega_{R^\Sigma/\mathcal{O}}, \hom_A(A, \ell^{-n}A/A)) \\
&= \hom_{R^\Sigma}(\Omega_{R^\Sigma/\mathcal{O}}, A/\ell^n) \\
&= \mathrm{Der}_{\mathcal{O}}(R^\Sigma, A/\ell^n) \\
&= \{\phi \in \hom_{\mathcal{O}-\text{algebra}}(R^\Sigma, A/\ell^n[\epsilon]) : \phi(r) \equiv (\theta_\rho^\Sigma(r) \mod \ell^n) \mod \epsilon\} \\
&= \{\rho\text{-relative deformation of } \bar{\rho} \text{ to } A/\ell^n[\epsilon] \text{ of type } \Sigma\},
\end{aligned}
$$

where $A/\ell^n[\epsilon] = A/\ell^n[X]/(X^2)$ with $\epsilon = X \mod (X^2)$ so $A/\ell^n[\epsilon]$ is an object in $\mathcal{C}$ with the square zero idea (ϵ). Also the second equality from the bottom is given by $d \mapsto (r \mapsto (\theta_\rho^s(r) \mod \ell^n + d(r)\epsilon))$. From now on, we view A/ℓ^n as a subset of $A/\ell^n[\epsilon]$ and $\mathrm{GL}_2(A/\ell^n)$ as a subset of $\mathrm{GL}_2(A/\ell^n[\epsilon])$ in the natural way whenever necessary.

We say a lifting of $\bar{\rho}$ to $A/\ell^n[\epsilon]$ is ρ-relative if its reduction module (ϵ) is $\rho_L \mod \ell^n$. A deformation of $\bar{\rho}$ to $A/\ell^n[\epsilon]$ is said to be ρ-relative if it is represented by a ρ-relative lifting of $\bar{\rho}$. We will produce a bijection from the set in the last row of above array, name it $t_{\rho,n}$, to $H^1_\Sigma(G_{\mathbb{Q}}, W_n)$.

Let $\theta : G_{\mathbb{Q}} \to \mathrm{GL}_2(A/\ell^n[\epsilon])$ be a ρ-relative lifting of $\bar{\rho}$. There is a canonical such lifting, call it θ_0: namely, the composition of $\rho_L \mod \ell^n$ and the natural embedding $\mathrm{GL}_2(A/\ell^n) \hookrightarrow \mathrm{GL}_2(A/\ell^n[\epsilon])$. We associate to θ the difference cocycle

$$c_\theta : G_{\mathbb{Q}} \to M_2(A/\ell^n) \cong \mathrm{End}_A(L/\ell^n L)$$

by $1 + \epsilon \cdot c_\theta(g) = \theta(g) \cdot \theta_0(g)^{-1}$ for $g \in G_{\mathbb{Q}}$, where $M_2(A/\ell^n)$ denotes the underlying additive group of the A/ℓ^n-algebra of 2×2 matrices with entries in A/ℓ^n and where the latter isomorphism is induced by the fixed basis of L. c_θ is well defined, i.e., $\theta(g) \cdot \theta_0(g)^{-1} \in 1 + \epsilon \cdot M_2(A/\ell^n)$, because θ is ρ-relative. This construction is independent of the choice of the basis of L. In fact, we can make each step of the construction coordinate free. Check that this construction provides a bijection between the set of ρ-relative liftings of $\bar{\rho}$ to $A/\ell^n[\epsilon]$, and the set $Z^1(G_{\mathbb{Q}}, \mathrm{End}_A(L/\ell^n L))$ of 1-cocycles. Then check that under this bijection, two liftings are strictly equivalent if and only if their associated cocycles are cohomologous.

A straightforward reduction of definitions shows that θ satisfies the deformation condition of fixed determinant if and only if the values of c_θ reside in $W_n = \mathrm{End}^0_A(L/\ell^n L)$, a direct summand of $AG_{\mathbb{Q}}$-module $\mathrm{End}_A(L/\ell^n L)$. Combining with the previous paragraph, we see that the map

$$\text{the } A/\ell^n[\epsilon]\text{-deformation class of } \theta \;\mapsto\; \text{the cohomology class of } c_\theta \qquad (2.2)$$

is a bijection between the set of ρ-relative $A/\ell^n[\epsilon]$-deformations of $\bar{\rho}$ with fixed determinant and $H^1(G_{\mathbb{Q}}, W_n)$.

Now we will check that θ is minimally ramified at any prime p outside Σ and different from ℓ if and only if the restrictions of θ and θ_0 to I_p can be brought one into another by conjugation by elements in the kernel of reduction $\mathrm{GL}_2(A/\ell^n[\epsilon]) \to \mathrm{GL}_2(A/\ell^n)$, which in turn if and only if the cocycle c_θ is cohomologous to zero when restricted to $I_p \subset G_p$. A straightforward calculation shows the second "if and only if." Now we will prove the first "if and only if." There are three cases according to the ramification of $\bar{\rho}$. In each case, the "if" part is trivial. So we will write only the proof of "only if" part, assuming that θ is minimally ramified at a prime p outside Σ and different from ℓ. We use $\tilde{}$ to denote composition with the Teichmüller lift

$$k^\times \to W(k)^\times \to A/\ell^n,$$

(or its further composition with $A/\ell^n \hookrightarrow A/\ell^n[\epsilon]$) as in [Di], where all three cases of minimal ramification are given.

Case 1. $\bar{\rho}|_{I_p} \sim \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}$. Then after a suitable choice of basis of V_{θ_0} and a corresponding choice of basis of V_θ, we may assume $\theta_0|_{I_p} = \begin{pmatrix} \tilde{\xi}_1 & 0 \\ 0 & \tilde{\xi}_2 \end{pmatrix}$ and $\theta|_{I_p} = \theta_0 + \epsilon \cdot m \sim \begin{pmatrix} \tilde{\xi}_1 & 0 \\ 0 & \tilde{\xi}_2 \end{pmatrix}$ for a map $m = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} : I_p \to M_2(A/\ell^n)$. Assume $\tilde{\xi}_1 \neq \tilde{\xi}_2$, otherwise $\theta_0|_{I_p} = \theta|_{I_p}$ already. We know

$$(a+\epsilon b)\theta|_{I_p}(a+\epsilon b)^{-1} = \begin{pmatrix} \tilde{\xi}_1 & 0 \\ 0 & \tilde{\xi}_2 \end{pmatrix},$$

for some $a = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $b = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in M_2(A/\ell^n)$. Expanding the equality, we find it is equivalent to

$$a = \begin{pmatrix} a_1 & 0 \\ 0 & a_4 \end{pmatrix}, \text{ and } \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} = \begin{pmatrix} 0 & b_2 a_4^{-1}(\tilde{\xi}_1 - \tilde{\xi}_2) \\ b_3 a_1^{-1}(\tilde{\xi}_2 - \tilde{\xi}_1) & 0 \end{pmatrix}.$$

Hence $\theta|_{I_p}$ is brought to $\theta_0|_{I_p}$ by conjugation by $\begin{pmatrix} 1 & \epsilon \cdot b_2 a_4^{-1} \\ \epsilon b_3 a_1^{-1} & 1 \end{pmatrix}$

Case 2. $\bar{\rho}|_{I_p} \sim \xi \otimes \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Then after suitable choices of bases, we may assume $\theta_0|_{I_p} = \tilde{\xi} \otimes \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ and $\theta|_{I_p} = \theta_0 + \epsilon \cdot m \sim \tilde{\xi} \otimes \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. After twisting θ and θ_0 with $\tilde{\xi}^{-1}$, this case is explained in [Ma3, §29].

Case 3. $\bar{\rho}|_{I_p} \sim \mathrm{Ind}_{I_M}^{I_P} \xi$, where M is a ramified quadratic extension of $\mathbb{Q}_p$ and ξ is a character of I_M that is not equal to its conjugate ξ' under the action of a lift σ of the nontrivial element in $\mathrm{Gal}(M/\mathbb{Q}_p)$ to I_p. Note that $I_p = I_M \cup \sigma I_M$. Then after suitable choices of bases, we may assume $\theta_0|_{I_M} = \begin{pmatrix} \tilde{\xi} & 0 \\ 0 & \tilde{\xi}' \end{pmatrix}$ and $\theta_0(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as $\theta_o|_{I_p} \sim \mathrm{Ind}_{I_M}^{I_P} \tilde{\xi}$ and that $\theta|_{I_p} = \theta_0 + \epsilon \cdot m \sim \mathrm{Ind}_{I_M}^{I_P} \tilde{\xi}$. So, for some $a \in \mathrm{GL}(A/\ell^n[\epsilon])$, $a\theta|_{I_M} a^{-1} = \begin{pmatrix} \tilde{\xi} & 0 \\ 0 & \tilde{\xi}' \end{pmatrix}$ and $a\theta(\sigma)a^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Write $\bar{a}$ for the reduction of a to $\mathrm{GL}_2(A/\ell^n)$. Then $\bar{a}\theta_0(\tau)\bar{a}^{-1} = \theta_0(\tau)$ for $\tau \in I_p$.

Check that this implies $\bar{a}$ is a scalar matrix. Hence, $\theta|_{I_p}$ is brought to $\theta_0|_{I_p}$ by conjugation by $\bar{a}^{-1}a$, which reduces to the identity matrix of $\mathrm{GL}(A/\ell^n)$.

Now we deal with the deformation condition of crystalline ramification at ℓ. We naturally identify the representation space of θ, V_θ with A/ℓ^n-module $L/\ell^n L \oplus \epsilon \cdot L/\ell^n L$ as θ is a ρ-relative lifting. Then we have an extension of $(A/\ell^n)G_{\mathbb{Q}}$-modules

$$0 \to \epsilon \cdot L/\ell^n L \to V_\theta \to L/\ell^n L \to 0,$$

which, by the canonical isomorphism mentioned when defining $H^1_f(G_\ell, W_n)$, corresponds to the elements in $H^1(G_\ell, W_n)$ represented by cocycle c'_θ given by

$$\epsilon \cdot (c'_\theta(g)(e)) = \theta(g)(\alpha(\theta(g)^{-1}e)) - e$$

for $g \in G_{\mathbb{Q}}$ and $e \in L/\ell^n L$, where $\alpha : L/\ell^n L \to V_\theta$ is any fixed A/ℓ^n-module splitting of the above extension. Choosing α to be the natural splitting, we find that c'_θ is none other than c_θ restricted to G_ℓ. [La, Chapter 10, Corollary 5.7], or the Krull intersection theorem as stated in [Ei, Corollary 5.4], tells that the maximal ideal of the finite local ring $A/\ell^n[\epsilon]$ is nilpotent. So θ satisfies the deformation condition of crystalline ramification if and only if V_θ is an object in $\mathfrak{FR}$, i.e., if and only if the cocycle c_θ restricted to G_ℓ represents an element in $H^1_f(G_\ell, W_n)$. Just tautology.

Pulling together the conclusions of above paragraphs on local ramification restrictions and the definition of $H^1_\Sigma(G_\mathbb{Q}, W_n)$, we see that the map (2.2) is a bijection between $t_{\rho,n}$ and $H^1_\Sigma(G_\mathbb{Q}, W_n)$. So we have constructed a bijection between $\hom_A(\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ and $H^1_\Sigma(G_\mathbb{Q}, W_n)$. It is straightforward to verify that the bijection is actually an A-module isomorphism. It is much more tedious to check the diagram in the third claim is commutative. □

Remark: The isomorphism is functorial in an obvious way if we shrink the set Σ.

Remark: Suppose we choose $\mathcal{O}$ to be A. Let η be the kernel of θ^Σ_ρ : $R_{\Sigma,A} \to A$. Then $R^\Sigma = A \oplus \eta$ as A-module. We have a topological A-module isomorphism

$$\Omega_{R^\Sigma/\mathcal{O}} \otimes_{R^\Sigma} A = \eta/\eta^2.$$

This is proved by showing directly that the obvious homomorphism from the left hand side to the right hand side is an isomorphism.

Chapter 3

Reduction and proof of $\mathrm{ad}^0(H^1(N))(1)$

We shall focus on B_I rather than A_I because the methods of [D-F-G2] apply more directly to B_I (see in particular its Lemma 8.11). Once we proved the case on B_I, the desired result on A_I can be formulated similarly and can be seen along the same line of arguments.

3.1 A reformulation in classical terms

In this section we transform the left equality of (1.9) into a concrete identity of elements in $T_\ell^\times/\mathfrak{T}_\ell^\times$.

In order to do that, or what amount to the same thing, reformulate the Burns-Flach conjecture 1.4.1 in classical terms such as the Fitting ideal of H^1_Σ, one needs to construct the triangle (1.8) with B_ℓ replaced by $\mathcal{B}_\ell$.

Assumption: The submodule $\mathrm{Fil}^0(\mathcal{B}_{\ell\text{-crys}})$ is a $\mathfrak{T}_\ell$-direct summand of $\mathcal{B}_{\ell\text{-crys}}$.

Readers are cautioned that a general motive does not determine its integral version(s) in any canonical way. We can use the notation $\mathcal{B}$, $\mathcal{B}_{\ell\text{-crys}}$ and $\mathcal{B}_\ell$

as we have specified $\mathcal{B}$ explicitly in §1.4. In our case of $M = H^1(X_0(N))$ we know by Mazur's results [Ma1] that $\mathrm{Fil}^0\,\mathcal{M}_{\ell\text{-crys}} \cong H^0(X_0(N)/\mathbb{Z}_\ell, \Omega^1)$ is a free $\mathfrak{T}_\ell$-module of rank 1. Since $\mathfrak{T}_\ell$ is Gorenstein the $\mathbb{Z}_\ell$- dual $\mathcal{M}_{\ell\text{-crys}}/\,\mathrm{Fil}^0 \cong H^1(X_0(N)/\mathbb{Z}_\ell, \mathcal{O})$ is also free of rank 1 over $\mathfrak{T}_\ell$ and hence $\mathcal{M}_{\ell\text{-crys}}$ is free over $\mathfrak{T}_\ell$. By linear algebra the $\mathrm{Fil}^i(\mathcal{B}_{\ell\text{-crys}}) = \mathrm{Fil}^i\,\mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{M}_{\ell\text{-crys}}(1))^0$ is then also free over $\mathfrak{T}_\ell$.

The assumption still needs to be verified, however, in more general situations. Ideally the only thing we'd like to assume is that $\mathcal{M}_\ell$ is free over $\mathfrak{T}_\ell$. Proposition 5.1.2 implies $\mathcal{M}_{\ell\text{-crys}}$ is free over $\mathfrak{T}_\ell$ if $\mathbb{V}(\mathcal{M}_{\ell\text{-crys}}) \cong \mathcal{M}_\ell$ and Proposition 5.1.1 and remark 5.1.3 imply that $\mathrm{Fil}^i\,\mathcal{M}_{\ell\text{-crys}}$ is also free over $\mathfrak{T}_\ell$.

Under the assumption we can define a perfect complex $R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, \mathcal{B}_\ell)$ of $\mathfrak{T}_\ell$-modules by

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, \mathcal{B}_\ell) = \mathrm{Fil}^0\,\mathcal{B}_{\ell\text{-crys}} \xrightarrow{1-\phi^0} \mathcal{B}_{\ell\text{-crys}}$$

and a map (in the derived category) $R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, \mathcal{B}_\ell) \to R\Gamma(\mathbb{Q}_\ell, \mathcal{B}_\ell)$ as follows. There is a commutative diagram of $G_{\mathbb{Q}_\ell}$-modules (with $\mathcal{B}_{\ell\text{-crys}}$ having trivial action)

$$\begin{array}{ccc}
\mathrm{Fil}^0\,\mathcal{B}_{\ell\text{-crys}} & \xrightarrow{1-\phi^0} & \mathcal{B}_{\ell\text{-crys}} \\
\downarrow & & \downarrow \\
\mathcal{B}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{Fil}^0 A_{\mathrm{crys},\ell}[-k](-k) & \xrightarrow{1\otimes(1-\phi^0)} & \mathcal{B}_\ell \otimes_{\mathbb{Z}_\ell} A_{\mathrm{crys},\ell}[-k](-k) \\
\| & & \| \\
\mathcal{B}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{Fil}^k A_{\mathrm{crys},\ell}(-k) & \xrightarrow{1\otimes(1-p^{-k}\phi)} & \mathcal{B}_\ell \otimes_{\mathbb{Z}_\ell} A_{\mathrm{crys},\ell}(-k)
\end{array} \tag{3.1}$$

where $[k]$ (resp. (k)) denotes filtration shift (resp. Tate twist) and $A_{\mathrm{crys},\ell}$ is the ring defined by Fontaine. The lower row is a resolution of the $G_{\mathbb{Q}_\ell}$-module $\mathcal{B}_\ell$ obtained by tensoring the exact sequence [B-K, (2.5.1)]

$$0 \to \mathbb{Z}_p(k) \to \mathrm{Fil}^k A_{\mathrm{crys},\ell} \xrightarrow{1-p^{-k}\phi} A_{\mathrm{crys},\ell} \to 0,$$

with $\mathcal{B}_\ell(-k)$.

Denoting the lower row in (3.1) by $E^\bullet(\mathcal{B}_\ell)$ and the standard continuous cochain resolution by $C^\bullet(G_{\mathbb{Q}_\ell}, -)$ we have maps

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, \mathcal{B}_\ell) \xrightarrow{(3.1)} E^\bullet(\mathcal{B}_\lambda) \to C^\bullet(G_{\mathbb{Q}_\ell}, E^\bullet(\mathcal{B}_\ell)) \leftarrow C^\bullet(G_{\mathbb{Q}_\ell}, \mathcal{B}_\ell) = R\Gamma(\mathbb{Q}_\ell, \mathcal{B}_\ell)$$

as desired. Tensoring with $\mathbb{Q}_\ell$, we obtain the map $R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, B_\ell) \to R\Gamma(\mathbb{Q}_\ell, B_\ell)$ defined in [B-F3, §3.2].

We are lucky that the complex $R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell, \mathcal{B}_\ell)$ already turns out to be perfect over $\mathfrak{T}_\ell$. This is not necessarily the case for the complex

$$R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, \mathcal{B}_\ell) = H^0(I_v, \mathcal{B}_\ell) \xrightarrow{1-\phi_v} H^0(I_v, \mathcal{B}_\ell)$$

for $v \in S_{\mathrm{bad}}$ since the submodule $H^0(I_v, \mathcal{B}_\ell)$ of $\mathcal{B}_\ell$ is not always $\mathfrak{T}_\ell$-free. Therefore when defining the global complex $R\Gamma_{\mathbf{f}}(\mathbb{Q}, \mathcal{B}_\ell)$ we do not follow (1.7) but we choose a set $\Sigma \subseteq S_{\mathrm{bad}}$ so that $R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, \mathcal{B}_\ell)$ is $\mathfrak{T}_\ell$-perfect for $v \notin \Sigma$ and define

$$R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell)=\mathrm{Cone}(R\Gamma_{et}(\mathbb{Z}_S,\mathcal{B}_\ell)\to\bigoplus_{v\in\Sigma'}R\Gamma_{/\mathbf{f}}(\mathbb{Q}_\ell,\mathcal{B}_\ell)\oplus\bigoplus_{v\in\Sigma}R\Gamma(\mathbb{Q}_v,\mathcal{B}_\ell)[-1] \tag{3.2}$$

where $\Sigma'=S_{\mathrm{bad}}\cup\{\ell\}\setminus\Sigma$. With this definition there is an exact triangle of perfect complexes of $\mathfrak{T}_\ell$-modules

$$R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S,\mathcal{B}_\ell)\to R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell)\to\bigoplus_{v\in\Sigma'}R\Gamma_{\mathbf{f}}(\mathbb{Q}_v,\mathcal{B}_\ell)\oplus R\Gamma(\mathbb{R},B_\ell). \tag{3.3}$$

and a map of triangles of perfect complexes of B_ℓ-modules

$$\begin{array}{ccccc} R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S,B_\ell) & \longrightarrow & R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},B_\ell) & \longrightarrow & \bigoplus_{v\in\Sigma'}R\Gamma_{\mathbf{f}}(\mathbb{Q}_v,B_\ell)\oplus R\Gamma(\mathbb{R},B_\ell) \\ \downarrow & & \downarrow & & \downarrow \\ R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S,B_\ell) & \longrightarrow & R\Gamma_{\mathbf{f}}(\mathbb{Q},B_\ell) & \longrightarrow & \bigoplus_{v\in S_{\mathrm{bad}}\cup\{\ell\}}R\Gamma_{\mathbf{f}}(\mathbb{Q}_v,B_\ell)\oplus R\Gamma(\mathbb{R},B_\ell), \end{array} \tag{3.4}$$

where the upper row is (3.3) tensored with $\mathbb{Q}_\ell$.

If ω is a T-basis of $\det_T(t_B)$ and h a T-basis of $\det_T B_B^+$, then $h^{-1}\otimes\omega$ is a T-basis of $\Delta(B)$. If b is any other T-basis of $\Delta(B)$ we denote by $b\cdot h\otimes\omega^{-1}$ the unique scalar $\lambda\in T^\times$ so that $b=\lambda\cdot h^{-1}\otimes\omega$. Denote by $W^\vee=\mathrm{Hom}_{\mathrm{cont}}(W,\mathbb{Q}_\ell/\mathbb{Z}_\ell)$ the Pontryagin dual of a profinite or discrete $\mathbb{Z}_\ell$-module W.

Lemma 3.1.1. *Let ω be T-basis of $\det_T(t_B)$ that is also a $\mathfrak{T}_\ell$-basis of the $\mathfrak{T}_\ell$-lattice $\det_{\mathfrak{T}_\ell}(\mathcal{B}_{\ell\text{-}crys}/\operatorname{Fil}^0\mathcal{B}_{\ell\text{-}crys})$, and let h be a T-basis of $\det_T B_B^+$ that is also* *a* $\mathfrak{T}_\ell$*-basis of* $\det_{\mathfrak{T}_\ell}(\mathcal{B}_\ell^+)$. *Put*

$$L^\Sigma(B,0) = L(B,0)\prod_{v\in\Sigma} L_v(B,0)^{-1}$$

and

$$b^\Sigma(B) = L^\Sigma(B,0)^{-1}c^+(B).$$

For any prime $\ell \notin S_I$ *the Burns-Flach conjecture 1.4.1 is equivalent to the identity*

$$\mathfrak{T}_\ell \cdot b^\Sigma(B) \cdot h \otimes \omega^{-1} = \# H^1_\Sigma(\mathbb{Q}, A_\ell/\mathcal{A}_\ell)^\vee, \tag{3.5}$$

where $\#W$ *denotes the Fitting ideal of a finite* $\mathfrak{T}_\ell$*-module* W *of finite projective dimension (i.e., the class of* W *in the relative algebraic K-group* $K_0(\mathfrak{T}_\ell, \mathbb{Q}_\ell) \cong T_\ell^\times/\mathfrak{T}_\ell^\times$*).*

Proof. Noting that the vertical maps in (3.4) are quasi-isomorphisms we obtain a commutative diagram of isomorphisms of (graded) invertible T_ℓ-modules

$$\begin{array}{ccc}
\mathrm{Det}_{T_\ell} R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S, B_\ell) & = & \mathrm{Det}_{T_\ell} R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S, B_\ell) \\
\downarrow & & \downarrow \\
\mathrm{Det}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}, B_\ell)\otimes & & \mathrm{Det}_{T_\ell} R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q}, B_\ell)\otimes \\
\bigotimes_{v\in S_{\mathrm{bad}}\cup\{\ell\}} \mathrm{Det}^{-1}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell)\otimes & \xrightarrow{\alpha} & \bigotimes_{v\in\Sigma'} \mathrm{Det}^{-1}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell)\otimes \\
\mathrm{Det}^{-1}_{T_\ell} R\Gamma(\mathbb{R}, B_\ell) & & \mathrm{Det}^{-1}_{T_\ell} R\Gamma(\mathbb{R}, B_\ell) \\
\beta\downarrow & & \downarrow \\
\mathrm{Det}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} t_B) & \xrightarrow{\prod_{v\in\Sigma} L_v(B,0)} & \mathrm{Det}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} t_B) \\
\otimes\, \mathrm{Det}^{-1}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} B_B^+) & & \otimes\, \mathrm{Det}^{-1}_{T_\ell}(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} B_B^+)
\end{array} \tag{3.6}$$

where the left hand vertical map is ϑ_ℓ and all unspecified tensor product are over T_ℓ. The factor $L_v(B,0)$ appears because for $v \in \Sigma$ the isomorphism

$$\mathrm{Det}_{T_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) \cong T_\ell \tag{3.7}$$

given in (1.4) (which is used for β) differs from the isomorphism (3.7) induced by the quasi-isomorphism $R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, B_\ell) \to 0$ (which is used for α) by precisely this factor (see [B-F2, Lemma 1]). So conjecture 1.4.1 is equivalent to

$$\prod_{v\in\Sigma} L_v(B,0)\vartheta_\ell(\mathrm{Det}_{\mathfrak{T}_\ell} R\Gamma_{\mathrm{et},c}(\mathbb{Z}_S, \mathcal{B}_\ell)) = \mathfrak{T}_\ell \cdot b^\Sigma(B) = \mathfrak{T}_\ell \cdot L^\Sigma(B,0)^{-1}c^+(B).$$

Using the commutativity of (3.6) together with (3.3) this is equivalent to

$$\mathrm{Det}_{\mathfrak{T}_\ell} R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell) \otimes \mathrm{Det}^{-1}_{\mathfrak{T}_\ell} R\Gamma_{\mathbf{f}}(\mathbb{Q}_\ell,\mathcal{B}_\ell) \otimes \mathrm{Det}^{-1}_{\mathfrak{T}_\ell} R\Gamma(\mathbb{R},\mathcal{B}_\ell) = \mathfrak{T}_\ell \cdot b^{\Sigma}(B)$$

or

$$\mathrm{Det}_{\mathfrak{T}_\ell} R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell) = \mathfrak{T}_\ell \cdot b^{\Sigma}(B) \cdot h \otimes \omega^{-1}.$$

It remains to compute the cohomology of $R\Gamma_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell)$ and this can be done along the lines of [B-F1, (1.35)-(1.37)]. We have

$$H^0_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell) = H^0(\mathbb{Q},\mathcal{B}_\ell) = 0,$$

where the last equality holds as $M_{f,\lambda}$ is absolutely irreducible and not isomorphic to $M_{f,\lambda}(1)$ for $\lambda \mid \ell$ a place of K_f. We also have

$$H^3_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell) \cong H^0(\mathbb{Q}, A_\ell/\mathcal{A}_\ell)^{\vee} = 0,$$

where the last equality is equivalent to the assumption on ℓ that $\mathcal{M}_{f,\lambda}/\lambda\mathcal{M}_{f,\lambda}$ is absolutely irreducible when restricted to $G_{\mathbb{Q}\left(\sqrt{(-1)^{(\ell-1)/2}\ell}\right)}$. Moreover we know $H^1_{\mathbf{f},\Sigma}(\mathbb{Q},B_\ell) = H^1_{\mathbf{f}}(\mathbb{Q},B_\ell) = 0$ and hence $H^1_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell) = H^0(\mathbb{Q},B_\ell/\mathcal{B}_\ell) = 0$ since $\ell \notin S_I$. Finally using Tate-Poitou duality, we have an exact sequence

$$0 \to H^2_{\mathbf{f},\Sigma}(\mathbb{Q},\mathcal{B}_\ell)^{\vee} \to H^1(\mathbb{Z}_S, A_\ell/\mathcal{A}_\ell) \to \bigoplus_{v\in\Sigma'} \frac{H^1(\mathbb{Q}_v, A_\ell/\mathcal{A}_\ell)}{H^1_{\mathbf{f}}(\mathbb{Q}_v, A_\ell/\mathcal{A}_\ell)},$$

which identifies $H^2_{\mathbf{f},\Sigma}(\mathbb{Q}, \mathcal{B}_\ell)$ with $H^1_\Sigma(\mathbb{Q}, A_\ell/\mathcal{A}_\ell)^\vee$. □

3.2 Reduction to a concrete problem

From now on we shall focus on our case of $M = H^1(X_0(N))$ with N prime, since we can not prove the conjecture in its full generality. We recall the restriction on ℓ: $\ell \notin S_I$, which enable us to use many facts in [D-F-G2]. We note that the reformulation in the previous section is valid.

Let $\mathfrak{T}_\ell = \prod_{\mathfrak{m}} \mathfrak{T}_{\mathfrak{m}}$ be the decomposition of $\mathfrak{T}_\ell$ into complete local $\mathcal{O}_\ell$-algebras, where $\mathfrak{m}$ runs through all maximal ideals of $\mathfrak{T}$ containing ℓ. For each $\mathfrak{m}$ we denote by $R^\Sigma_{\mathfrak{m}}$ the universal deformation ring attached to the Galois representation $\mathcal{M}_{f,\lambda}/\lambda\mathcal{M}_{f,\lambda}$ over the finite field $\mathfrak{T}_{\mathfrak{m}}/\mathfrak{m}$ of type Σ, where f is a newform associated to the maximal ideal $\mathfrak{m}$ of $\mathfrak{T}$ (that is, $\mathfrak{m}$ is the kernel of the algebra homomorphism $\mathfrak{T} \to \mathbb{C}$, $t \mapsto a_1(t(f))$) and λ is the place of K_f whose valuation ring contains $\mathfrak{m} \cap K_f$. Note $\mathcal{M}_{f,\lambda}$ is short crystalline as $\ell \nmid 2N$. Put $R^\Sigma_\ell = \prod_{\mathfrak{m}} R^\Sigma_{\mathfrak{m}}$, so that there is a natural surjection $R^\Sigma_\ell \to \mathfrak{T}_\ell$ that comes from the surjection $R^\Sigma_{\mathfrak{m}} \to \mathfrak{T}_{\mathfrak{m}}$ for all $\mathfrak{m}$.

We know by equality (2.1) that there is a canonical isomorphism of $\mathfrak{T}_\ell$-modules

$$\mathrm{Hom}_{\mathfrak{T}_\ell}(\Omega_{R^\Sigma_\ell/\mathbb{Z}_\ell} \otimes_{R^\Sigma_\ell} \mathfrak{T}_\ell, T_\ell/\mathfrak{T}_\ell) \cong H^1_\Sigma(\mathbb{Q}, A_\ell/\mathcal{A}_\ell).$$

The powerful method of Diamond-Taylor-Wiles that is implemented in [D-F-G2, §7.2 and §7.3] leads to the fact $R^\Sigma_{\mathfrak{m}}$ is a local complete intersection over $\mathfrak{T}_{\mathfrak{m}}$. So for each $\mathfrak{m}$ there is an integer $r_\mathfrak{m}$ and power series $g_1, ..., g_{r_\mathfrak{m}} \in \mathbb{Z}_\ell[[X_1, ...X_{r_\mathfrak{m}}]]$ such that

$$R^\Sigma_\mathfrak{m} \cong \mathbb{Z}_\ell[[X_1, ...X_{r_\mathfrak{m}}]]/(g_1, ..., g_{r_\mathfrak{m}}).$$

In particular,

$$\Omega_{R^\Sigma_\ell/\mathbb{Z}_\ell} \otimes_{R^\Sigma_\ell} \mathfrak{T}_\ell$$

is a finite $\mathfrak{T}_\ell$-module of finite projective dimension whose Fitting ideal is generated by the element

$$\Delta^\Sigma = \pi\left(\det\left(\frac{\partial g_i}{\partial X_j}\right)_{1\leq i,j\leq r_\mathfrak{m}}\right)_\mathfrak{m},$$

where $\pi : \prod_\mathfrak{m} \mathbb{Z}_\ell[[X_1, ...X_{r_\mathfrak{m}}]] \to \prod_\mathfrak{m} R^\Sigma_\mathfrak{m} = R^\Sigma_\ell \to \prod_\mathfrak{m} \mathfrak{T}_\mathfrak{m} = \mathfrak{T}_\ell$ is the composite ring homomorphism.

Assuming that $\mathfrak{T}_\ell$ is Gorenstein we have

$$H^1_\Sigma(\mathbb{Q}, A_\ell/\mathcal{A}_\ell)^\vee \cong \Omega_{R^\Sigma_\ell/\mathbb{Z}_\ell} \otimes_{R^\Sigma_\ell} \mathfrak{T}_\ell$$

so that we need to show

$$\mathfrak{T}_\ell \cdot b^\Sigma(B) \cdot h \otimes \omega^{-1} = \mathfrak{T}_\ell \cdot \Delta^\Sigma.$$

The restriction on ℓ at the beginning of this chapter ensure us to use the explanation in [D-F-G2, §8.2] so that we know the element $b^\Sigma(B)$ is uniquely determined by the scalar $\lambda(b^{\Sigma}(B)) \in T^{\times}$ such that

$$< f, b^{\Sigma}(B)(f \otimes (2\pi i)^2) \otimes \iota^2 >= \lambda(b^{\Sigma}(B)) \cdot b_{dr} \otimes \iota^1$$

and similarly for $h \otimes \omega^{-1}$. Hence we have

$$b^{\Sigma}(B) \cdot h \otimes \omega^{-1} = \frac{\lambda(b^{\Sigma}(B))}{\lambda(h \otimes \omega^{-1})}.$$

Note that we are only interested in $\lambda(b^{\Sigma}(B))$ up to factors in $\mathfrak{T}_{\ell}^{\times}$, hence we can forget the factor $i^{k-\eta}((k-2)!)^2/2$ occurring in Theorem 8.5. This factor is the same for all $f \in I$ hence lies in the diagonally embedded $\mathbb{Z}_{\ell}^{\times} \subset \mathfrak{T}_{\ell}^{\times}$.

In our case of $M = H^1(X_0(N))$ with N prime, we can take $\Sigma = \emptyset$ because we have

Lemma 3.2.1. *$R\Gamma_{\mathbf{f}}(\mathbb{Q}_v, \mathcal{B}_{\ell})$ is $\mathfrak{T}_{\ell}$-perfect for all $v \nmid \ell$.*

Proof. This is clear if $v \nmid N$ as then $\mathcal{M}_{\ell}$ is unramified due to the good reduction of $X_0(N)$ at primes other than N.

Now suppose $v = N$. Then then action of I_v on the $\mathcal{M}_{\ell}$ is unipotent and

$\mathfrak{T}_\ell$-equivariant but nontrivial on any constituent of $\mathcal{M}_\ell$. Then

$$\begin{aligned}
&\mathcal{B}_\ell^{I_N} = \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_\ell, \mathcal{M}_\ell(1))^{I_N} \\
&= \{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in M_2(\mathfrak{T}_\ell) \mid \begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} 1 & \phi(\sigma) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \phi(\sigma) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\} \\
&= \{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in M_2(\mathfrak{T}_\ell) \mid \phi(\sigma)a = 0, \phi(\sigma)c = 0\} \\
&= \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathfrak{T}_\ell)\},
\end{aligned}$$

where σ runs through I_N, acting on $\mathcal{M}_\ell$ by $\begin{pmatrix} 1 & \phi(\sigma) \\ 0 & 1 \end{pmatrix}$. Hence $\mathcal{B}_\ell^{I_N}$ is a free $\mathfrak{T}_\ell$ module. □

We also know that $\mathcal{M}_{f,\lambda}$ for $f \in I$ is minimally ramified at all maximal ideals of $\mathcal{O}_{K_f}$ not containing ℓ. From now on, we replace Σ by $\emptyset$ or do not write it at all. By the results of Chapter 7 of [D-F-G2] the map $R_\ell^\emptyset \to \mathfrak{T}_\ell$ is an isomorphism.

Now let us look at Theorem 1.3.1 for each $f \in I$. We have $k = 2$, $\eta = 0$. Moreover, the character ψ for f is trivial so we can forget the degenerated Dirichlet motive $M_{\psi^{-1}} = K_f$. There is no exceptional primes as we know an exceptional prime p must be N since p must divide the level prime number N. However, [Hi3, Theorem 4.2.4] says that decomposition group at p acting on $M_{f,\lambda}$ for a prime $\lambda \mid \ell$ in K_f is equivalent to a diagonal representation:

$$\sigma \mapsto \begin{pmatrix} \eta(\sigma)\chi_\ell(\sigma) & * \\ 0 & \eta(\sigma), \end{pmatrix}$$

where $\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character and η is an unramified character. Hence the dimension of $M_{f,\lambda}^{I_p}$ is not zero so p is not exceptional.

$\epsilon(M_f)$ equals $\pm N$ whereas $\epsilon(A_f) = N^2$. The sign of $\epsilon(M_f)$ depends on f. It coincides, however, with the eigenvalue of the endomorphism of $J_0(N)$ on f induced by the conjugation on $\Gamma_0(N)$ by $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Hence the tuple of $\epsilon(M_f)$ for $f \in I$ is an element of $\mathfrak{T}^\times$ by [Ri, Corollary 3.3]. So we can forget all factors in Theorem 1.3.1, where we have trivial character ψ and no exceptional primes, in the sense that $\lambda(b(B)) \in \mathfrak{T}_\ell^\times$.

In order to make further progress, we also fix a number field K large enough to contain all complex embeddings of all fields K_f for $f \in I$ and replace M by $M \otimes K$, T by $T \otimes_{\mathbb{Q}} K \cong \prod_{\mathbf{I}_T} K$, $\mathfrak{T}$ by $\mathfrak{T} \otimes_{\mathbb{Z}} \mathcal{O}$ and A by $A \otimes K$. Here $\mathcal{O}$ denotes the ring of integers of K. Then we have $\mathfrak{T}_\ell = T_\ell \cap (\mathfrak{T}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{O}_\ell)$. By Theorem 4.1 and Lemma 11 of [B-F3] Burns-Flach conjecture for this scalar extended motive implies the one for the original motive.

Now we analyze $\lambda(h \otimes \omega^{-1})$. The invertible $\mathfrak{T}_\ell$-module $\det_{\mathfrak{T}_\ell}(\mathcal{B}_\ell^+)$ can be analyzed as in [D-F-G2, §8.2] and we find that the isomorphism $\det_T B_B^+ \cong T(2)_B$ can be chosen to induce an isomorphism $\det_{\mathfrak{T}_\ell}(\mathcal{B}_\ell^+) \cong \mathfrak{T}_\ell(2)$ under which h maps to $(2\pi i)^2$. The isomorphism of [D-F-G2, equation (43)]

$$\det_T t_B \cong \mathrm{Hom}_T(\mathrm{Fil}^1 M_{\mathrm{dR}}, M_{\mathrm{dR}}/\,\mathrm{Fil}^1) \otimes_{\mathbb{Q}} \mathbb{Q}(2)_{\mathrm{dR}}$$

likewise induces an isomorphism

$$\det_{\mathfrak{T}_\ell}(\mathcal{B}_{\ell\text{-crys}}/\operatorname{Fil}^0\mathcal{B}_{\ell\text{-crys}}) \cong \operatorname{Hom}_{T_\ell}(\operatorname{Fil}^1\mathcal{M}_{\ell\text{-crys}}, \mathcal{M}_{\ell\text{-crys}}/\operatorname{Fil}^1)\otimes_{\mathbb{Z}_\ell}\mathbb{Z}(2)_{\ell\text{-crys}}.$$

Hence we can view $\omega\otimes\iota^2$ as a basis of $\operatorname{Hom}_{T_\ell}(\operatorname{Fil}^1\mathcal{M}_{\ell\text{-crys}}, \mathcal{M}_{\ell\text{-crys}}/\operatorname{Fil}^1)$.

Now note that the pairing $<,>$ is induced by a perfect (Poincare duality) pairing on $\mathcal{M}$. In particular it induces isomorphisms of free rank 1 $\mathfrak{T}_\ell$-modules

$$\mathcal{M}_\ell \cong \operatorname{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_\ell, \mathcal{O}_\ell)$$

(see the axioms in [D-F-G2, §7.2]) and

$$\mathcal{M}_{\ell\text{-crys}} \cong \operatorname{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell).$$

Note that $\mathfrak{T}_\ell$ is a finite flat Gorenstein $\mathcal{O}_\ell$-algebra contained in the maximal $\mathcal{O}_\ell$-order

$$\prod_{\mathbf{I}_T}\mathcal{O}_\ell$$

of T_ℓ. By definition $\lambda(h\otimes\omega^{-1})$ is the element $(\lambda_\tau)_{\tau\in\mathbf{I}_T}$ of this product given by

$$< f^\tau, (h\otimes\omega^{-1})(f^\tau\otimes(2\pi i)^2)\otimes\iota^2 >=< f^\tau, (\omega\otimes\iota^2)(f^\tau) >= \lambda_\tau\cdot b_{\mathrm{dR}}\otimes\iota,$$

where we view τ as an embedding $K_f\to K$.

3.3 Differ by a unit in $\mathfrak{T}_\ell$

At this point we have nearly reduced the problem to an algebraic one. We are given

- A local complete intersection $R_\ell^\emptyset \cong \mathfrak{T}_\ell$ finite flat over $\mathcal{O}_\ell$ so that $\mathfrak{T}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \prod_{\mathbf{I}_T} K_\ell$.

- A free $\mathfrak{T}_\ell$-module $\mathcal{M}_{\ell\text{-crys}}$ of rank two with a perfect $\mathcal{O}_\ell$-linear $\mathfrak{T}_\ell$-balanced alternating pairing $<,>$. $\mathcal{M}_{\ell\text{-crys}}$ contains a totally isotropic free rank 1 $\mathfrak{T}_\ell$-submodule $\operatorname{Fil}^1 \mathcal{M}_{\ell\text{-crys}}$ so that $M_{\ell\text{-crys}}/\operatorname{Fil}^1$ is also $\mathfrak{T}_\ell$-free. Hence we can pick a $\mathfrak{T}_\ell$-isomorphism $\omega : \operatorname{Fil}^1 \mathcal{M}_{\ell\text{-crys}} \to M_{\ell\text{-crys}}/\operatorname{Fil}^1$.

- For each $\tau \in \mathbf{I}_T$ we are given a $\mathcal{O}_\ell$-generator f^τ of

$$\{x \in \operatorname{Fil}^1 \mathcal{M}_{\ell\text{-crys}} | tx = \pi_\tau(t)x\}$$

  (the π_τ-eigenspace) where $\pi_\tau : \mathfrak{T}_\ell \to \mathcal{O}_\ell$ is the $\mathcal{O}_\ell$-algebra homomorphism given by projection onto the component indexed by $\tau \in \mathbf{I}_T$.

- Some knowledge of the modular forms, especially that all f^τ are newforms, i.e., having first Fourier coefficient equal to 1.

The final problem: Show that the elements

$$\left(< f^\tau, \omega(f^\tau) >\right)_\tau \in \prod_{\mathbf{I}_T} \mathcal{O}_\ell$$

and

$$\Delta^{\emptyset} \in \mathfrak{T}_\ell \subset \prod_{\mathbf{I}_T} \mathcal{O}_\ell$$

differ by an element in $\mathfrak{T}_\ell^\times$ (in particular this implies that $\big(< f^\tau, \omega(f^\tau) >\big)_\tau$ lies in $\mathfrak{T}_\ell$). Note that this problem does not depend on the choice of ω. Any other choice is of the form $\lambda\omega$ with $\lambda \in \mathfrak{T}_\ell^\times$ and we have

$$< f^\tau, \lambda\omega(f^\tau) >=< f^\tau, \omega(\lambda{\cdot}f^\tau) >=< f^\tau, \omega(\pi_\tau(\lambda)f^\tau) >= \pi_\tau(\lambda) < f^\tau, \omega(f^\tau) > .$$

Hence we only change the element $\big(< f^\tau, \omega(f^\tau) >\big)_\tau$ by $\lambda \in \mathfrak{T}_\ell^\times$.

In any case, the problem is now sufficiently concrete. We exploit the fact that $\mathfrak{T}_\ell$, being a complete intersection over $\mathcal{O}_\ell$, is Gorenstein. In particular one can choose a Gorenstein trace $\phi : \mathfrak{T}_\ell \to \mathcal{O}_\ell$, i.e., a $\mathfrak{T}_\ell$-basis of $\mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell)$. This choice induces an isomorphism

$$\mathrm{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell) \cong \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathfrak{T}_\ell),$$

in other words there is a unique $\mathfrak{T}_\ell$-bilinear pairing $<< -, - >>$ on $\mathcal{M}_{\ell\text{-crys}}$ so that $\phi(<< x, y >>) =< x, y >$. Since π_τ are $\mathcal{O}_\ell$-linear there are also unique elements $e_\tau \in \mathfrak{T}_\ell$ so that $\pi_\tau(x) = \phi(e_\tau \cdot x)$ for all $x \in \mathfrak{T}_\ell$.

Proof of the final problem:

Since ϕ is a $\mathfrak{T}_\ell$-basis of $\mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell)$, we can define a $\mathfrak{T}_\ell$-isomorphism $\gamma : \mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell) \to \mathfrak{T}_\ell$ so that $t\phi \mapsto t$ for $t \in \mathfrak{T}_\ell$.

From [M-R, Appendix A.13], we know that there exists some element μ in $\mathfrak{T}_\ell^\times$ so that the first of the following equalities holds.

$$(\mu\Delta^\emptyset)\phi = \mathrm{tr}_{\mathfrak{T}_\ell/\mathcal{O}_\ell} = \sum_{\tau\in I_T}\pi_\tau = \sum_{\tau\in I_T} e_\tau\phi = (\sum_{\tau\in I_T} e_\tau)\phi,$$

where $e_\tau = \gamma(\pi_\tau)$. (The second equality can be explained if we realize that $\mathrm{tr}_{\mathfrak{T}_\ell/\mathcal{O}_\ell} = \mathrm{tr}_{\mathfrak{T}_\ell\otimes K/K}|_{\mathfrak{T}_\ell}$ and $\mathfrak{T}_\ell\otimes K = \prod_{I_T} K$). Since γ is an isomorphism, we have

$$\mu\Delta^\emptyset = \sum_{\tau\in I_T} e_\tau.$$

We have a $\mathfrak{T}_\ell$-module isomorphism

$$\kappa : \mathrm{Fil}^1 M_{\ell\text{-crys}} = S_2(\Gamma_0(N), \mathcal{O}_\ell) \to \mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell)$$

defined by $\kappa(f) = (t \mapsto (a_1(Tf)))$. See [D-I, §12.3], [D-D-T, lemma 1.34] or [Hi2, Theorem 3.17].

Proposition 3.3.1. $\kappa^{-1}(\pi_\tau) = f^\tau$.

Proof. : for all $t \in \mathfrak{T}_\ell$,

$$t(\kappa^{-1}(\pi_\tau)) = \kappa^{-1}(t(\pi_\tau)) = \kappa^{-1}(\pi_\tau(t)\pi_\tau) = \pi_\tau(t)\kappa^{-1}(\pi_\tau),$$

where the middle equality is justified by

$$t(\pi_\tau)(x) = \pi_\tau(tx) = \pi_\tau(x)\pi_\tau(x) = (\pi_\tau(x)\pi_\tau)(x).$$

So $k^{-1}(\pi_\tau)$ is in the π_τ-eigenspace of $\mathrm{Fil}^1 \mathcal{M}_{\ell\text{-crys}}$, which is generated by f^τ. So $k^{-1}(\pi_\tau) = cf^\tau$ for some $c \in \mathcal{O}_\ell$. Then

$$c = a_1(cf^\tau) = a_1(1 \cdot (cf^\tau)) = \kappa(cf^\tau)(1) = \pi_\tau(1) = 1,$$

where in the first equality we use the fact that f^τ is a newform, i.e., its first Fourier coefficient is equal to 1. Other equalities are formal. □

Now note the perfect pairing (Poincare duality) on $\mathcal{M}$ induces an isomorphism of free rank 1 $\mathfrak{T}_\ell$-modules

$$\beta : \mathcal{M}_{\ell\text{-crys}} \cong \mathrm{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell),$$

$$\beta(x)(y) = < x, y >,$$

where the $\mathfrak{T}_\ell$-module structure of $\mathrm{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell)$ is induced by that of $\mathcal{M}_{\ell\text{-crys}}$. β is $\mathfrak{T}_\ell$-linear as

$$\beta(tx)(y) =< tx, y >=< x, ty >= (t\beta(x))y,$$

where the central equality results from the fact that Hecke operators are self-adjoint with respect to the pairing.

Define

$$\alpha : \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathfrak{T}_\ell) \to \mathrm{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell),$$

by $\alpha(f) = \phi \circ f$. To see that α is an isomorphism, we assume that $\mathcal{M}_{\ell\text{-crys}} = \mathfrak{T}_\ell \oplus \mathfrak{T}_\ell$ without loss of generality. Then we have commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathfrak{T}_\ell) & \cong & \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathfrak{T}_\ell, \mathfrak{T}_\ell) \oplus \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathfrak{T}_\ell, \mathfrak{T}_\ell) \\ \downarrow \alpha & & \downarrow\ \alpha_1 \oplus \alpha_1 \\ \mathrm{Hom}_{\mathcal{O}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathcal{O}_\ell) & \cong & \mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell) \oplus \mathrm{Hom}_{\mathcal{O}_\ell}(\mathfrak{T}_\ell, \mathcal{O}_\ell), \end{array}$$

where $\alpha_1(f) = \phi \circ f$. Note that $\alpha_1 = \gamma \circ (f \mapsto f(1))$ is an isomorphism. Hence so is α. More over, α is $\mathfrak{T}_\ell$-linear.

Consider $\mathfrak{T}_\ell$-isomorphism $\alpha^{-1} \circ \beta$. It corresponds to the $\mathfrak{T}_\ell$-bilinear pairing $<< -, - >>$ on $\mathcal{M}_{\ell\text{-crys}}$ defined by $<< x, y >>= ((\alpha^{-1} \circ \beta)(x))(y)$. Then

$$\phi(<< x, y >>) = (\phi \circ (\alpha^{-1} \circ \beta(x)))(y) = \beta(x)(y) =< x, y > .$$

Let Fil^1 be a shorthand for $\mathrm{Fil}^1 \mathcal{M}_{\ell\text{-crys}}$. Since $\mathcal{M}_{\ell\text{-crys}}/\mathrm{Fil}^1$ is $\mathfrak{T}_\ell$ free, we can pick a $\mathfrak{T}_\ell$-submodule Comp of $\mathcal{M}_{\ell\text{-crys}}$ so that $\mathcal{M}_{\ell\text{-crys}} = \mathrm{Fil}^1 \oplus \mathrm{Comp}$. We identify $M_{\ell\text{-crys}}/\mathrm{Fil}^1$ with Comp. Note that Fil^1 and Comp are free rank 1 $\mathfrak{T}_\ell$-modules.

Proposition 3.3.2. $<< \mathrm{Fil}^1, \mathrm{Fil}^1 >>= 0$

Proof. For all $x, y \in \mathrm{Fil}^1$,

$$\pi_\tau << x, y >>= \phi(\mathrm{e}_\tau << x, y >>) = \phi << e_\tau x, y >>=< e_\tau x, y >= 0.$$

The last equality holds as Fil^1 is a totally isotropic $\mathfrak{T}_\ell$-submodule of $\mathcal{M}_{\ell\text{-crys}}$. Since τ is arbitrary, $<< x, y >>= 0$. □

We have $\mathfrak{T}_\ell$-isomorphism $\alpha^{-1}\beta : \mathcal{M}_{\ell\text{-crys}} \cong \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathfrak{T}_\ell)$, or more explicitly, $\alpha^{-1}\beta : \mathrm{Fil}^1 \oplus \mathrm{Comp} \cong \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathcal{M}_{\ell\text{-crys}}, \mathfrak{T}_\ell) \oplus \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathrm{Comp}, \mathfrak{T}_\ell.)$ Once we choose a $\mathfrak{T}_\ell$-base for each of the four free rank 1 $\mathfrak{T}_\ell$-modules in the last congruence, the matrix of $\alpha^{-1}\beta$ is of the form

$$\begin{pmatrix} 0 & * \\ * & * \end{pmatrix},$$

where the upper left 0 is implied by the claim above. Since $\alpha^{-1}\beta$ is an isomorphism, the above matrix is invertible. In particular, the lower left element of the matrix must be a unit in $\mathfrak{T}_\ell$. That is, if we let

$$\theta = \alpha^{-1}\beta|_{\mathrm{Fil}^1 \to \mathrm{Hom}_{\mathfrak{T}_\ell}(\mathrm{Comp},\ \mathfrak{T}_\ell)},$$

θ is a $\mathfrak{T}_\ell$-isomorphism.

By slight abuse of notation, let the same symbol α denote the map

$$\mathrm{Hom}_{\mathfrak{T}_\ell}(\mathrm{Comp}, \mathfrak{T}_\ell) \to \mathrm{Hom}_{\mathcal{O}_\ell}(\mathrm{Comp}, \mathcal{O}_\ell)$$

such that $\alpha(f) = \phi \circ f$. As before, α is a $\mathfrak{T}_\ell$-isomorphism. Let $v = \alpha \circ \theta : \mathrm{Fil}^1 \to \mathrm{Hom}_{\mathcal{O}_\ell}(\mathrm{Comp}, \mathcal{O}_\ell)$, still a $\mathfrak{T}_\ell$-isomorphism. Check that $v(x)(y) = \phi << x, y >>$. On the other hand, fixing a $\mathfrak{T}_\ell$-basis $\{b\}$ for Comp thereafter, we can define

$$v_0 : \mathrm{Fil}^1 \to \mathrm{Hom}_{\mathcal{O}_\ell}(\mathrm{Comp}, \mathcal{O}_\ell)$$

by $v_0(f)(tb) = \kappa(f)(t)$. Since v_0 and v are isomorphisms between free rank 1 $\mathfrak{T}_\ell$-modules, we have $v = \epsilon v_0$ for some $\epsilon \in \mathfrak{T}_\ell^\times$.

Since the desired result does not depend on the choice of ω, we will prove the result by choosing a particular ω and showing that $\left(< f^\tau, \omega(f^\tau) >\right)_\tau$ and $\mu\Delta^\emptyset$ are actually equal for this choice. In fact, we choose $\omega : \mathrm{Fil}^1 \to \mathrm{Comp}$ such that $\omega(x) = ((\gamma\kappa(x))\epsilon^{-1})b$. It is seen that ω is a $\mathfrak{T}_\ell$-isomorphism.

So

$$\begin{aligned} & < f^\tau, \omega(f^\tau) > \\ &= \phi << f^\tau, \omega(f^\tau) >> \\ &= v(f^\tau)(\omega(f^\tau)) \\ &= ((\epsilon v_0) f^\tau)(((\gamma\kappa(f^\tau))\epsilon^{-1})b) \\ &= \kappa(f^\tau)(\epsilon(\gamma\kappa(f^\tau))\epsilon^{-1}) \\ &= \pi_\tau(e_\tau). \end{aligned}$$

Hence to prove that $\left(< f^{\tau}, \omega(f^{\tau}) >\right)_{\tau}$ and $\mu\Delta^{\emptyset}$ are equal, is equivalent to showing that for all $\tau \in I_T$,

$$\pi_{\tau}(e_{\tau}) = \pi_{\tau}(\sum_{\sigma \in I_T} e_{\sigma}).$$

Now we prove the following proposition, thus ending the whole proof.

Proposition 3.3.3. $\pi_{\tau}(e_{\sigma}) = 0$ *for* $\sigma \neq \tau$.

Proof. Since $e_{\sigma} = \gamma(\kappa(f^{\sigma}))$, where γ and κ are $\mathfrak{T}_{\ell}$ linear, the fact that f^{σ} is in the π_{σ}-eigenspace of Fil^1 is translated to be that e_{σ} is in the π_{σ}-eigenspace of $\mathfrak{T}_{\ell}$. Choose some element $t \in \mathfrak{T}_{\ell}$ such that $\pi_{\sigma}(t) \neq \pi_{\tau}(t)$. Then $te_{\sigma} = \pi_{\sigma}(t)e_{\tau}$. Apply π_{τ} to both sides. As π_{τ} is an algebra homomorphism, left side becomes $\pi_{\tau}(t)\pi_{\tau}(e_{\sigma})$. As π_{τ} is $\mathcal{O}_{\ell}$-linear, the right side becomes $\pi_{\sigma}(t)\pi_{\tau}(e_{\sigma})$. Now comparing both sides leads to the desired claim. □

Chapter 4

A non-trivial example

Remark 1.4.3 says that the exact extent to which the conjecture of Burns-Flach is finer than that of Bloch-Kato in our case is measured by the group $\mathcal{O}_{T_\ell}^\times/\mathfrak{T}_\ell^\times$. To show that what we have proved is not vacuous, it is imperative that we have a concrete example for which our proof of the conjecture of Burns-Flach works and that this group is nontrivial.

We recall or introduce a few symbols first. $\mathfrak{T}$ is the integral Hecke algebra generated over $\mathbb{Z}$ by the Hecke operators on $S_2(\Gamma_0(N))$, the vector space of cusp forms of weight 2, level prime number N and trivial character. Since N is prime, $S_2(\Gamma_0(N))$ is generated by newforms as there is no forms in $S_2(\Gamma_0(1)) = S_2(\mathrm{SL}_2(N))$. $T = \mathfrak{T} \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_f K_f$, where f runs through non-conjugate newforms in $S_2(\Gamma_0(\mathbb{Z}))$ and where K_f is the field of definition of f. S_I is the set of prime number ℓ such that either:

- $\lambda \mid 2N$, or
- there exist a newform f and a prime $\lambda \mid \ell$ in K_f such that the two-dimensional residual Galois representation $\mathcal{M}_{f,\lambda}/\lambda\mathcal{M}_{f,\lambda}$ is not absolutely

irreducible when restricted to G_F, where $\mathcal{M}_f$ is the premotivic structure associated to f defined in [D-F-G2, §5.4] and $F = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$ and $\lambda \mid \ell$.

We want to choose N and ℓ to satisfy

- condition 1: $\ell \notin S_I$, and
- condition 2: $(\mathfrak{T}_\ell)^\times$ is a proper subgroup of $\mathcal{O}_{T_\ell}^\times$.

We set the first condition as we use the result of [D-F-G2, §8.2] to prove Burns-Flach conjecture in our case while the second condition is the requirement of non-trivial refinement.

Example: The above two conditions are satisfied for $N = 89$ and $\ell = 5$.

$S_2(\Gamma_0(89))$ contains 7 (normalized) newforms, 5 of which are Galois conjugate to each other. Let f_1, f_2, f_3 be three non-Galois-conjugate (normalized) newforms in $S_2(\Gamma_0(89))$. We list in table 4.1 the eigenvalues of the first 15 Hecke operators acting on them, or equivalently, the first 15 coefficients of their q-expansions, which can be found by [St3] or in [St1].

Now let us check condition 1. Suppose it is not satisfied. Since $5 \nmid 2 \cdot 89$, there is a prime $\lambda \mid 5$ in S_f where $f = f_i$ for some $i \in 1, 2, 3$ such that the two-dimensional residual Galois representation $\mathcal{M}_{f,\lambda}/\lambda\mathcal{M}_{f,\lambda}$ is not absolutely irreducible when restricted to G_F. By [D-F-G2, Lemma 7.14], the original representation is not absolutely irreducible either. By the proof of [D-F-G2, Lemma 7.13] , we must have

$$a_p(f) \equiv p+1 \mod \lambda \tag{4.1}$$

for all primes $p \equiv 1 \mod N$. Choose $p = 2*89+1 = 179$. Then $p+1 \equiv 0 \mod \lambda$. The following values of a_{179}'s can be found the same way as above.

$$a_{179}(f_1) = 14 \not\equiv 0 \mod \lambda$$

$$a_{179}(f_2) = 4 \not\equiv 0 \mod \lambda$$

$$a_{179}(f_3) = (-4a^4 + 4a^3 + 32a^2 - 16a - 42) \not\equiv 0 \mod \lambda.$$

The last inequality comes from the fact that the norm of $a_{179}(f_3)$ is 413408, which is not divisible by 5 and which is obtained by software package Pari as follows:

```
?norm(Mod(-4*a^4+4*a^3+32*a^2-16*a-42,a^5+a^4-10*a^3-10*a^2+21*a+17))
\%1=413408
```

Hence, (4.1) is not true for any f. So condition 1 is satisfied.

Now let us check condition 2. By [A-S], the integral Hecke algebra $\mathfrak{T}$ is generated (as an abelian group) inside $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(a)$ by the operators T_n with $n \leq 2 \cdot 89/12 \cdot (1 + 1/89) = 15$, i.e., generated by the rows of table 4.1 (of course not considering the first row and first column). By row operations, we

n	$a_n(f_1)$	$a_n(f_2)$	$a_n(f_3)$
1	1	1	1
2	-1	1	a
3	-1	2	$-a^4/2 + a^3/2 + 7a^2/2 - 5a/2 - 4$
4	-1	-1	$a^2 - 2$
5	-1	-2	$-a^2 + 4$
6	1	2	$a^4 - 3a^3/2 - 15a^2/2 + 13a/2 + 17/2$
7	-4	2	$a^4/2 - 4a^2 - a + 13/2$
8	3	-3	$a^3 - 4a$
9	-2	1	$a^2 - a - 4$
10	1	-2	$-a^3 + 4a$
11	-2	-4	$-a^3 + 5a + 2$
12	1	-2	$-3a^4/2 + 3a^3/2 + 19a^2/2 - 15/2a - 9$
13	2	2	$-a^4 + a^3 + 8a^2 - 5a - 11$
14	4	2	$-a^4/2 + a^3 + 4a^2 - 4a - 17/2$
15	1	-4	$a^4/2 - a^3/2 - 5a^2/2 + 5a/2 + 1$

Table 4.1: Hecke operator T_n on newforms in $S_2(\Gamma_0(89))$

Here a is a root of $a^5 + a^4 - 10a^3 - 10a^2 + 21a + 17 = 0$.

find that $\mathfrak{T}$ is also generated by 7 linearly-independent elements

$$(1, \quad 0, \quad 5)$$

$$(0, \quad 1, \quad -4)$$

$$(0, \quad 0, \quad (a^4 + 1)/2 - 1)$$

$$(0, \quad 0, \quad (a^3 + a^2 + a + 1)/2 + 3)$$

$$(0, \quad 0, \quad a^2 - 1)$$

$$(0, \quad 0, \quad a - 1)$$

$$(0, \quad 0, \quad 10)$$

in $\mathcal{O}_T \cong \mathbb{Z} \times \mathbb{Z} \times \mathcal{O}_{K_{f_3}}$. Note that $\{(a^4 + 1)/2, (a^3 + a^2 + a + 1)/2, a^2, a, 1\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{K_{f_3}}$ as shown by the following Pari session:

```
? nfinit(a^5+a^4-10*a^3-10*a^2+21*a+17).zk

%1 = [1, a, a^2, 1/2*a^3 + 1/2*a^2 + 1/2*a + 1/2, 1/2*a^4 + 1/2]
```

The set of 7 elements above also generates $\mathfrak{T}_5 = \mathfrak{T} \otimes_{\mathbb{Z}} \mathbb{Z}_5$ as a $\mathbb{Z}_5$-module. Since the unit $(1, 1, -1) \in \mathcal{O}_{T_5}$ is not in $\mathfrak{T}_5$, we have verified condition 2.

For completeness, let us determine the quotient $\mathcal{O}_{T_\ell}^\times/\mathfrak{T}_\ell^\times$ in this case.

As 2 is invertible in $\mathbb{Z}_5$, $\mathcal{O}_{K_{f_3},5}$ as a $\mathbb{Z}_5$-module is generated by $\{a^4 - 1, a^3 - 1, a^2 - 1, a - 1, 1\}$, or equivalently, by $\{b^4, b^3, b^2, b, 1\}$ with $b = a - 1$. The ideal $(5, b)$ in $\mathcal{O}_{K_{f_3},5}$ is generated by $\{b^4, b^3, b^2, b, 5\}$ as a $\mathbb{Z}_5$-module as $b^5 = -6b^4 - 4b^3 + 24b^2 + 20b - 20$. Hence the map $\alpha : \mathbb{Z}_5/(5) \to \mathcal{O}_{K_{f_3},5}/(5, b)$ induced by the inclusion $\mathbb{Z}_5 \to \mathcal{O}_{K_{f_3},5}$ is a ring isomorphism.

$\mathfrak{T}_5$ is generated by $(1, 0, 0)$, $(0, 1, 1)$, $(0, 0, 5)$, $(0, 0, b)$, $(0, 0, b^2)$, $(0, 0, b^3)$, and $(0, 0, b^4)$, while $\mathcal{O}_{T_5}$ is generated by the same set except that $(0, 0, 5)$ is replaced by $(0, 0, 1)$. So, $\mathfrak{T}_5$ is exactly the elements (x_1, x_2, x_3) in $\mathcal{O}_{T_5}$ such that $\alpha(\overline{x_2}) = \overline{x_3}$. As $\mathcal{O}_{T_5}$ is an integral extension of $\mathfrak{T}_5$, $\mathfrak{T}_5^\times = \mathcal{O}_{T_5}^\times \cap \mathfrak{T}_5$. Hence, $\mathfrak{T}_5^\times$ is exactly the elements (x_1, x_2, x_3) in $\mathcal{O}_{T_5}^\times$ such that $\alpha(\overline{x_2}) = \overline{x_3}$, or, equivalently, the kernel of the homomorphism

$$\mathcal{O}_{T_5}^\times = \mathbb{Z}_5^\times \times \mathbb{Z}_5^\times \times \mathcal{O}_{K_{f_3},5}^\times \to (\mathbb{Z}_5/5\mathbb{Z}_5)^\times$$

$$(x_1, x_2, x_3) \mapsto \overline{x_2}\ \alpha^{-1}(\overline{x_3}).$$

Since this homomorphism is surjective, $\mathcal{O}_{T_5}^\times/\mathfrak{T}_5^\times \cong (\mathbb{Z}_5/5\mathbb{Z}_5)^\times$. Its order, 4, indicates that all we have done is a small refinement indeed. We wonder if there is an easier way to achieve it.

Chapter 5

An isomorphism of two Selmer groups

One type of Selmer groups is defined by Bloch and Kato and employed in their conjecture while another type is given in [D-F-G2, §7.1] and reintroduced in 2.1. This chapter presents in proposition 5.3.4 an isomorphism between these two types under some conditions, which can be viewed as a kind of global version of the isomorphism in [D-F-G2, §7.1], whose statements and proofs are followed quite closely here. The comparison of Selmer groups is considered one of the first steps to understand these groups. In the course of proving the isomorphism, we also obtain proposition 5.1.1 on the A-linear Fontaine-Laffaille theory, where A is a commutative complete local noetherian ring finite over $\mathbb{Z}_\ell$.

This chapter is independent of the other chapters except that proposition 5.1.1 is mentioned in §3.1.

5.1 The theory of Fontaine and Laffaille

We introduce some of the theory of Fontaine and Laffaille in [F-L] in a way that fits for later use. The main point here is to extend the coefficients of various modules to A or A/ℓ, where A is a commutative complete local noetherian ring finite over $\mathbb{Z}_\ell$.

By common abuse of notation, we use the same symbol to denote an object of a category or its image under a forgetful functor when it is clear which one we refer to.

Let $\mathbb{Z}_\ell$-$\mathcal{MF}$, or simply $\mathcal{MF}$, denote the category whose object X is a finitely generated $\mathbb{Z}_\ell$-module equipped with

- a decreasing filtration such that $\mathrm{Fil}^a X = X$ and $\mathrm{Fil}^b X = 0$ for some $a, b \in \mathbb{Z}$, and for each $i \in \mathbb{Z}$, $\mathrm{Fil}^i X$ is a $\mathbb{Z}_\ell$-module direct summand of X;
- $\mathbb{Z}_\ell$-linear maps $\phi^i : \mathrm{Fil}^i X \to X$ for $i \in \mathbb{Z}$ satisfying $\phi^i|_{\mathrm{Fil}^{i+1} X} = \ell\phi^{i+1}$ and $X = \sum \mathrm{Im}\phi^i$,

and whose morphisms are $\mathbb{Z}_\ell$-module homomorphisms respecting filtration and commuting with ϕ^i for all i. $\mathcal{MF}$ is naturally a $\mathbb{Z}_\ell$-linear category. It follows from [F-L, 1.8] that $\mathcal{MF}$ is an abelian category such that the forgetful functor from it to the category of $\mathbb{Z}_\ell$-modules is exact.

For any subcategory $\mathcal{C}$ of $\mathcal{MF}$, let $\mathcal{C}^0$ denote its full subcategory of objects X satisfying $\mathrm{Fil}^0 X = X$ and $\mathrm{Fil}^\ell X = 0$ and having no non-trivial quotients X' such that $\mathrm{Fil}^{\ell-1} X' = X'$. Also, let $\mathcal{MF}_{\mathrm{tor}}$ denote its full subcategory of objects of finite length, i.e., objects that are torsion $\mathbb{Z}_\ell$-modules. It follows from [F-L, 6.1] that $\mathcal{MF}^0_{\mathrm{tor}}$ is an abelian category, stable under taking subobjects, quotients, finite direct products and extensions in $\mathcal{MF}$.

Now we extends the coefficients to A or A_ℓ. Let A-$\mathcal{MF}$ denote the category any of whose object is an object X in $\mathcal{MF}$ equipped with a ring homomorphism $A \to \mathrm{End}_{\mathcal{MF}}(X)$, $a \mapsto a_X$ for all $a \in A$, which becomes the structure map $\mathbb{Z}_\ell \to \mathrm{End}_{\mathcal{MF}}(X)$ if composed with the natural map $\mathbb{Z}_\ell \to A$, and whose morphisms should be compatible with the extra structure, namely, for X and X' in A-$\mathcal{MF}$, a morphism $f : X \to X'$ in $\mathbb{Z}_\ell$-$\mathcal{MF}$ is also a morphism in A-$\mathcal{MF}$ if and only if $f \cdot a_X = a_{X'} \cdot f$ for all $a \in A$. Explicitly, an object of A-$\mathcal{MF}$ is a finitely generated A-module X equipped with

- a decreasing A-module filtration such that $\mathrm{Fil}^a X = X$ and $\mathrm{Fil}^b X = 0$ for some $a, b \in \mathbb{Z}$, and for each $i \in \mathbb{Z}$, $\mathrm{Fil}^i X$ is a $\mathbb{Z}_\ell$-module direct summand of X;

- A-linear maps $\phi^i = \phi^i_X : \mathrm{Fil}^i X \to X$ for $i \in \mathbb{Z}$ satisfying $\phi^i|_{\mathrm{Fil}^{i+1}X} = \ell\phi^{i+1}$ and $X = \sum \mathrm{Im}\phi^i$,

and a morphism is an A-module homomorphism respecting filtration and commuting with ϕ^i for all i.

Substituting A/ℓ for A in the previous paragraph, we obtain the category A/ℓ-$\mathcal{MF}$. A-$\mathcal{MF}^0$ and A/ℓ-$\mathcal{MF}^0$ are the full subcategories of A-$\mathcal{MF}$ and A/ℓ-$\mathcal{MF}$ respectively whose objects are actually in $\mathcal{MF}^0$.

We note that the description of an object in A-$\mathcal{MF}$ is the same as the description of an object in $\mathbb{Z}_\ell$-$\mathcal{MF}$ with $\mathbb{Z}_\ell$ replaced by A everywhere with one exception. The following proposition reveals that under a mild condition, there is no exception. The proposition still holds with almost the same proof even if A is not commutative. However, this is irrelevant to this article.

Proposition 5.1.1. *Let X be an object of A-$\mathcal{MF}$ whose underlying module is a free A-module. Then $\mathrm{Fil}^i X$ is in fact an A-module direct summand of (the underlying module of) X and a free A-module for all i.*

Proof. We do induction on the nontrivial filtration length n of X. If $n = 0$, i.e., $X = 0$, it is trivial. Suppose it is true if the nontrivial filtration length is less than n. Let $X \in A$-$\mathcal{MF}$ whose non-trivial filtration length is n. Shifting the filtration indices if necessary, we can assume $X = \mathrm{Fil}^0 X \supset \mathrm{Fil}^1 X \cdots \supset \mathrm{Fil}^n = 0$.

We first deal with $\mathrm{Fil}^1 X$. Let M be the matrix representation of ϕ^0 with respect to a basis of X over A. Since A is a local ring, using elementary row and column operations, we know that there exist two invertible matrices M_α and M_β such that

$$M_\alpha M M_\beta = \begin{pmatrix} I & 0 \\ 0 & M_1 \end{pmatrix},$$

where I is the identity matrix and M_1 is a square matrix whose entries are in $\mathfrak{M}$, the maximal ideal of A. Let M_α and M_β correspond to A-linear isomorphisms α and β respectively. We identify the domain of β with the codomain of α in such a way that the bases for them coincide. Replacing $\mathrm{Fil}^i X$ by

$\beta^{-1}(\mathrm{Fil}^i X)$ and ϕ^i by $\alpha \circ \phi^i \circ \beta$ for all i, we can assume from now on that M has the block diagonal form of the right hand side of above equality.

Let $X = X_0 \oplus X_1$ such that it corresponds to the block form of M. Consider $x \in N = X_0 \cap \mathrm{Fil}^1 X$. Then $x = \phi^0(x) = \ell\phi^1(x)$. Since X_0 and $\mathrm{Fil}^1 X$ are $\mathbb{Z}_\ell$-module direct summands of X, $\phi^1(x) \in N$. So $x \in \ell N$, i.e., $N \subset \ell N$. Note that $\ell \in \mathfrak{M}$. By Nakayama's lemma, $N = 0$. Hence,

$$\mathrm{rank}_{\mathbb{Z}_\ell} X_0 + \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Fil}^1 X = \mathrm{rank}_{\mathbb{Z}_\ell}(X_0 + \mathrm{Fil}^1 X) \leq \mathrm{rank}_{\mathbb{Z}_\ell} X. \tag{5.1}$$

We have $X = \sum_{i \geq 0} \mathrm{Im}\phi^i$. Then

$$X_1 = \frac{\mathrm{Im}\phi^0}{X_0} + \frac{X_0 + \sum_{i \geq 1} \mathrm{Im}\phi^i}{X_0}.$$

Note that $\mathrm{Im}\phi^0 / X_0 = \phi^0(X_1) \subset \mathfrak{M} X_1$. By Nakayama's lemma,

$$X = X_0 + \sum_{i \geq 1} \mathrm{Im}\phi^i. \tag{5.2}$$

So we have the first inequality of the following:

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_\ell} X &\leq \mathrm{rank}_{\mathbb{Z}_\ell} X_0 + \mathrm{rank}_{\mathbb{Z}_\ell} \textstyle\sum_{i \geq 1} \mathrm{Im}\phi^i \\ &= \mathrm{rank}_{\mathbb{Z}_\ell} X_0 + \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Im}\phi^1 \\ &\leq \mathrm{rank}_{\mathbb{Z}_\ell} X_0 + \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Fil}^1 X, \end{aligned} \tag{5.3}$$

where the second equality is ensured by the fact that $\phi^i|_{\mathrm{Fil}^{i+1} X} = \ell\phi^{i+1}$ for all

i.

Combining (5.1) with (5.3), we see that all inequalities must be equalities and hence,

$$\mathrm{rank}_{\mathbb{Z}_\ell} X = \mathrm{rank}_{\mathbb{Z}_\ell} X_0 + \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Fil}^1 X, \tag{5.4}$$

which leads to equality:

$$\dim_{\mathbb{F}_\ell} \frac{X}{\ell X} = \dim_{\mathbb{F}_\ell} \frac{X_0}{\ell X_0} + \dim_{\mathbb{F}_\ell} \frac{\mathrm{Fil}^1 X}{\ell\, \mathrm{Fil}^1 X}, \tag{5.5}$$

where we can naturally identify each quotient on the right hand side with an $\mathbb{F}_\ell$-vector subspace of the quotient on the left hand side as X_0 and $\mathrm{Fil}^1 X$ are $\mathbb{Z}_\ell$-module direct summands of X.

The intersection of those two quotients on the right is zero. To prove this claim, let us take an arbitrary element in the intersection, which is $x_0 + \ell X$ for some $x_0 \in X_0$ and $x_1 + \ell X$ for some $x_1 \in \mathrm{Fil}^1 X$. So $x_0 = x_1 \mod \ell X$. Applying the natural projection $\pi : X \to X_0$ to this congruence equality, we have

$$x_0 = \pi(x_1) \mod \ell X_0,$$

because $\pi(\ell X) \cap X_0 = \ell X_0$. On the other hand,

$$\pi(x_1) = \phi^0(\pi(x_1)) = \pi\phi^0(x_1) = \pi\ell\phi^1(x_1) \in \pi(X) \cap \ell X = \ell X_0.$$

So $x_0 = 0 \mod \ell X_0$ and the claim is established. Then from (5.5), we see that

$$\frac{X}{\ell X} = \frac{X_0}{\ell X_0} + \frac{\mathrm{Fil}^1 X}{\ell \,\mathrm{Fil}^1 X}.$$

Nakayama's lemma tells us that $X = X_0 + \mathrm{Fil}^1 X$. Then by (5.4), we must have $X = X_0 \oplus \mathrm{Fil}^1 X$. So $\mathrm{Fil}^1 X$ is an A-module direct summand of X. Since a projective module over a local ring is free, $\mathrm{Fil}^1 X$ is a free A-module. So the desired conclusion is true for $\mathrm{Fil}^1 X$.

(5.2) and the first inequality in (5.3), where all inequalities are actually equalities as shown before, imply that $X = X_0 \oplus \sum_{i \geq 1} \mathrm{Im}\phi^i$. Thus being a projective module over a local ring, $\sum_{i \geq 1} \mathrm{Im}\phi^i$ is a free A-module. It has the same rank over A as $\mathrm{Fil}^1 X$ as shown by the last (in)equality in (5.3). Let γ be an A-linear isomorphism from $\sum_{i \geq 1} \mathrm{Im}\phi^i$ to $\mathrm{Fil}^1 X$.

Construct an object Y of A-$\mathcal{MF}$ from X as follows. Y is $\mathrm{Fil}^1 X$ equipped with extra structure:

- $\mathrm{Fil}^i Y = \mathrm{Fil}^1 X$ for all $i \leq 1$, $\mathrm{Fil}^i Y = \mathrm{Fil}^i X$ for all $i \geq 1$,
- $\phi_Y^{i-1} = \ell \phi_Y^i$ for all $i \leq 1$, $\phi_Y^i = \gamma \circ \phi_X^i$ for all $i \geq 1$.

Then Y is an object of A-$\mathcal{MF}$ whose nontrivial filtration length is less than n. By induction assumption, $\mathrm{Fil}^i Y$ is an A-module direct summand of $\mathrm{Fil}^1 Y$ and a free A-module for all i. In other words, $\mathrm{Fil}^i X$ is an A-module direct summand of $\mathrm{Fil}^1 X$ and a free A-module for all $i \geq 1$. Since $\mathrm{Fil}^1 X$ is an A-module direct summand of X, $\mathrm{Fil}^i X$ is an A-module direct summand of X. So the desired conclusion for $\mathrm{Fil}^i X$ is true if $i \geq 1$, while it is trivially true if $i \leq 0$. Thus we conclude our induction. $\square$

Let $\mathbb{Z}_\ell$-$\mathcal{GR}$, or simply $\mathcal{GR}$, be the full subcategory of $\mathbb{Z}_\ell G_\ell$-modules whose objects are isomorphic to quotients of the form L_1/L_2, where $L_2 \subset L_1$ are finitely generated G_ℓ-stable $\mathbb{Z}_\ell$-submodules in short crystalline representations. In the same way as we define A-$\mathcal{MF}$ and A/ℓ-$\mathcal{MF}$ from $\mathcal{MF}$, we define category A-$\mathcal{GR}$ and category A/ℓ-$\mathcal{GR}$ from $\mathcal{GR}$.

The category $\mathcal{MF}^0_{\text{tor}}$ is $\mathbb{Z}_\ell$-linearly equivalent, via the functor, also mentioned at §1.2,

$$X \mapsto \mathbb{V}(X) := \hom(\underline{U}_S(X), \mathbb{Q}_\ell/\mathbb{Z}_\ell),$$

to $\mathcal{FR}$, where $\underline{U}_S(X) = \hom_{(\text{some appropriate category})}(X, A_{\text{crys},\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, and $\mathcal{FR}$, already introduced in §2.1, is the full subcategory of $\mathcal{GR}$ of objects of finite length [F-L, 6.1]. Extend $\mathbb{V}$ to a fully faithful functor on $\mathcal{MF}^0$ by setting $\mathbb{V}(X) = \operatorname{proj\,lim} \mathbb{V}(X/\ell^n X)$. Then $\mathbb{V}$ defines an equivalence between $\mathcal{MF}^0$ and $\mathcal{GR}$. By functoriality, the functor $\mathbb{V}$ also defines an A-linear equivalence between A/ℓ-$\mathcal{MF}^0$ and A/ℓ-$\mathcal{GR}$ and between A-$\mathcal{MF}^0$ and A-$\mathcal{GR}$.

We know $\mathcal{GR}$ and $\mathcal{FR}$ are abelian categories. Note that we can describe A-$\mathcal{GR}$ (resp. A/ℓ-$\mathcal{GR}$) as the full subcategory of the abelian category of finitely–generated–over–$\mathbb{Z}_\ell$ AG_ℓ-modules, consisting of objects that fall into $\mathcal{GR}$ (resp. $\mathcal{FR}$) under the exact forgetful functor to the abelian category of finitely–generated–over–$\mathbb{Z}_\ell$ $\mathbb{Z}_\ell G_\ell$-modules. (The condition of being finite $\mathbb{Z}_\ell$-modules is to guarantee that the categories are abelian so that the argument right below would work. Note that the modules here are, by the convention throughout this article, modules with continuous G_ℓ action on its $\mathbb{Z}_\ell$-adic topology.) Therefore A-$\mathcal{GR}$ and A/ℓ-$\mathcal{GR}$ are abelian categories. By equivalence of categories, so are A/ℓ-$\mathcal{MF}^0$ and A-$\mathcal{MF}^0$.

Note that the forgetful functor from A/ℓ-$\mathcal{GR}$ to $\mathcal{GR}$ is exact. By equivalence of categories, the forgetful functor from A/ℓ-$\mathcal{MF}^0$ to $\mathcal{MF}^0$ is exact. Hence, the forgetful functor from A/ℓ-$\mathcal{MF}^0$ to the category of A-modules is exact. The same arguments exist for A-$\mathcal{MF}^0$.

In a word, A-$\mathcal{MF}^0$, A/ℓ-$\mathcal{MF}^0$, A-$\mathcal{GR}$ and A/ℓ-$\mathcal{GR}$ are A-linear abelian categories such that the forgetful functors from them to the category of A-modules are exact.

Now we state a proposition that applies to $\mathbb{V}$. We know that $\mathbb{V}$, as a functor on $\mathcal{MF}^0$, preserves the lengths of underlying $\mathbb{Z}_\ell$-modules. For any A-module, its length as a $\mathbb{Z}_\ell$-module is $[k : \mathbb{F}_\ell]$ times its length as an A-module, where k is the residue field of A. So $\mathbb{V}$, as a functor on A-$\mathcal{MF}^0$, also preserves the lengths of underlying A-modules.

Proposition 5.1.2. *Let A be a commutative complete local noetherian ring. Suppose we are given two A-linear abelian categories such that there exist exact forgetful functors from them to the category of A-modules, where the A-module structure of an object is provided by its original A-linear structure. Then an equivalence between them that preserves lengths of the underlying A-modules also preserves the freeness and ranks of the underlying A-modules (of objects* *whose underlying A-modules are free).*

Proof. Let $\Theta : \mathcal{E} \to \mathcal{F}$ be the equivalence in the proposition and $\mathfrak{M}$ be the maximal ideal of A. Suppose $\Theta(E) = F$, where F is a free A-module of rank r.

For any ideal I of A generated by $a_1, \cdots, a_n$, we have an exact sequence in the category of A-modules:

$$E^n \xrightarrow{\beta} E \to E/IE \to 0,$$

where $\beta((x_1, \cdots, x_n)) = \sum a_i x_i,\ x_i \in E$. β is, in fact, in $\mathcal{E}$ because $\mathcal{E}$ is an A-linear abelian category. The exact forgetful functors of $\mathcal{E}$ to the category of A-modules ensures that E/IE, the cokernel of β in the category of A-modules, must be (the underlying A-module of) the cokernel of β in $\mathcal{E}$. So we can view the above sequence as exact in $\mathcal{E}$. Applying Θ, we get an exact sequence in $\mathcal{F}$:

$$F^n \xrightarrow{\Theta(\beta)} F \to \Theta(E/IE) \to 0,$$

where $\Theta(\beta)$ has the same definition as β. Since the cokernel of $F^n \xrightarrow{\Theta(\beta)} F$ in $\mathcal{F}$ is F/IF for the same reason as above, we obtain that $\Theta(E/IE) \cong F/IF$. Hence as A-modules,

$$\text{length}(E/IE) = \text{length}(\Theta(E/IE)) = \text{length}(F/IF) = r \cdot \text{length}(A/I), \quad (5.6)$$

where lengths might be infinity.

Let $\mathfrak{M}$ take the place of I. Then (5.6) becomes

$$\dim_{A/\mathfrak{M}}(E/\mathfrak{M}E) = \dim_{A/\mathfrak{M}}(F/\mathfrak{M}F) = r.$$

By Nakayama's lemma, we have a surjection of A-modules: $A^r \to E$, which is completed to an exact sequence:

$$0 \to K \to A^r \to E \to 0.$$

Tensoring it with $A/\mathfrak{M}^k$ over A for an integer k, we get an exact sequence

$$K \otimes_A A/\mathfrak{M}^k \to (A/\mathfrak{M}^k)^r \to E/\mathfrak{M}^k E \to 0.$$

So we have

$$\text{length(image of } K \otimes_A A/\mathfrak{M}^k) = r \cdot \text{length}(A/\mathfrak{M}^k) - \text{length}(E/\mathfrak{M}^k E).$$

One can show that $\text{length}(A/\mathfrak{M}^k)$ is finite by induction as A is noetherian. Hence, (5.6) says that the right hand side of the above equality is 0. Then $K \in \mathfrak{M}^k \cdot A^r$. Let k goes to infinity, we see that $K = 0$ as A is complete with respect to $\mathfrak{M}$. So $A^r \cong E$. $\square$

Remark 5.1.3. *All propositions still holds if we change A to be a finite product of commutative complete noetherian local rings finite free over $\mathbb{Z}_\ell$, or, what is* *exactly the same, a commutative semi-local ring finite free over $\mathbb{Z}_\ell$. This can be seen by decomposing into or taking product over components indexed by the Wedderburn factors of A for various concepts.*

5.2 Notation

We continue to use the notation of §2.1. Fix an odd prime ℓ, a commutative complete local ring A finite free over $\mathbb{Z}_\ell$, a continuous $AG_{\mathbb{Q}}$-module L free of rank two over A and $W = \mathrm{End}^0_A(L) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell$, where the superscript 0 means endomorphisms of trace 0. Let T=$\mathrm{End}^0_A(L)$, $B = A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, $V_1 = L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and $V = T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathrm{End}^0_B(V_1)$. So we have an exact sequence

$$0 \to T \to V \to W \to 0. \tag{5.7}$$

We assume that V_1 is a short crystalline representation of G_ℓ, where the meaning of short is defined in §2.1.

Bloch and Kato define a divisible B-submodule $H^1_{\mathrm{f}}(G_p, W) \subset H^1(G_p, W)$ for each p. Explicitly,

$$H^1_{\mathrm{f}}(G_p, V) := \begin{cases} \ker(H^1(G_p, V) \to H^1(I_p, V)) = H^1(G_{\mathbb{F}_p}, V^{I_p}) & \text{for } p \neq \ell, \\ \ker(H^1(G_\ell, V) \to H^1(G_\ell, B_{\mathrm{crys}} \otimes_{\mathbb{Q}_\ell} V)) & \text{for } p = \ell, \end{cases}$$

where B_{crys} is the ring $B_{\mathrm{crys},\ell}$ defined by Fontaine [F-P2, I.2.1]. Then $H^1_{\mathrm{f}}(G_p, W)$

is the image of $H^1_{\mathfrak{f}}(G_p, V)$ under the natural map. Their Selmer group

$$H^1_{\mathfrak{f}}(G_{\mathbb{Q}}, W) \subset H^1(G_{\mathbb{Q}}, W)$$

is the A-submodule of elements with restrictions in $H^1_{\mathfrak{f}}(G_p, W)$ for all primes p.

5.3 The isomorphism of two Selmer groups

We first prepare two isomorphisms in the next two propositions.

Proposition 5.3.1. *Let $p \neq \ell$ and suppose W^{I_p} is divisible. Then*

$$H^1_{\mathfrak{f}}(G_p, W) = H^1_f(G_p, W),$$

where $H^1_f(G_p, W)$ is defined in §2.1.

Proof. We have a long exact sequence:

$$0 \to T^{I_p} \to V^{I_p} \to W^{I_p} \xrightarrow{\delta} H^1(I_p, T) \to \cdots .$$

$\mathrm{Im}(\delta)$ is divisible as so is W^{I_p}. But $H^1(I_p, T)$ has no nontrivial ℓ-divisible subgroups by [N-S-W, Proposition 2.3.7]. So $\mathrm{Im}(\delta) = 0$. Replacing $H^1(I_p, T)$ by 0 in the above sequence, we have a short exact sequence of $G_p/I_p = G_{\mathbb{F}_p}$-

modules, which induces a long exact sequence:

$$\cdots \to H^1(G_{\mathbb{F}_p}, V^{I_p}) \xrightarrow{\alpha} H^1(G_{\mathbb{F}_p}, W^{I_p}) \xrightarrow{\beta} H^2(G_{\mathbb{F}_p}, T) \to \cdots$$

What we want to prove is none other than that α is surjective. So it suffices to show $H^2(G_{\mathbb{F}_p}, T) = 0$. We have

$$H^2(G_{\mathbb{F}_p}, T) = \varprojlim H^2(G_{\mathbb{F}_p}, T/\ell^n T) = 0.$$

The first equality holds by [N-S-W, Corollary 2.3.5] and the second by Proposition 1.6.13(ii) of loc. cit. $\square$

Proposition 5.3.2. $H^1_{\mathfrak{f}}(G_\ell, W) = H^1_f(G_\ell, W)$ *is divisible of* $\mathbb{Z}_\ell$*-corank*

$$d = \dim_{\mathbb{Q}_\ell} H^0(G_\ell, V) + \dim_{\mathbb{Q}_\ell} V - \dim_{\mathbb{Q}_\ell} \mathrm{Fil}^0 D_{\mathtt{crys}}(V).$$

Here $D_{\mathrm{crys}}(V)= (B_{\mathrm{crys}} \otimes_{\mathbb{Q}_\ell} V)^{G_\ell}$. The $\mathbb{Z}_\ell$-corank of a $\mathbb{Z}_\ell$-module M is the rank of $M^\vee/(M^\vee)_{\mathrm{tor}}$ over $\mathbb{Z}_\ell$, where $M^\vee = \hom_{\mathbb{Z}_\ell}(M, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$.

Proof. First we show $H^1_{\mathfrak{f}}(G_\ell, W) \subset H^1_f(G_\ell, W)$. Let $\alpha \in H^1_{\mathfrak{f}}(G_\ell, W)$ be the image of some class $\bar{c} \in H^1_{\mathfrak{f}}(G_\ell, V)$ represented by cocycle $c \in Z^1(G_\ell, V)$, which corresponds to a BG_ℓ-module extension

$$0 \to V \to E \to B \to 0, \tag{5.8}$$

where B has trivial G_ℓ action and $E = V \oplus B$ with G_ℓ action $g(v,b) = (g(v) + bc(g), b)$. We construct a commutative diagram of exact rows

$$\begin{array}{ccccccccc}
0 & \to & V \otimes_B V_1 & \to & E \otimes_B V_1 & \to & B \otimes_B V_1 & \to & 0 \\
 & & \downarrow & \text{push-out} & \downarrow & & \downarrow & & \\
0 & \to & V_1 & \to & E' & \to & V_1 & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & L & \to & L' & \to & L & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & L/\ell^n L & \to & L'/\ell^n L' & \to & L/\ell^n L & \to & 0
\end{array}$$

as follows. The first row, (5.8)$\otimes_B V_1$, is exact as V_1 is free over B. The upper left vertical arrow is the evaluation map. Then we make the upper left square a BG_ℓ-module push-out diagram and complete first two rows so that it commutes and that the second row is exact. See [Ei, A3.26c]. We require that the third row be exact and the arrows from it to the second row are natural injections. Then L' is a uniquely determined free A-module. The arrows to the fourth row are natural projections. Then the fourth row is also exact. We pick n large enough so that $\mathrm{Im}(c) \subset T \otimes_{\mathbb{Z}_\ell} \ell^{-n}\mathbb{Z}_\ell/\mathbb{Z}_\ell$. Then the map from $\bar{c}$ to α factors through the image of c in $H^1(G_\ell, W_n)$. Call this image β.

(By the way, if we know E', we can get E by constructing the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & V \oplus B & \to & F & \to & B \cdot \mathrm{id}_{V_1} & \to & 0 \\ & & \downarrow & & \downarrow & \text{(pull-back)} & \downarrow & & \\ 0 & \to & V \oplus B & \to & \hom_B(V_1, E') & \to & V \oplus B & \to & 0, \end{array}$$

where $V \oplus B = \mathrm{End}_B(V_1)$. Then $E = F/B$.)

We have defined $H^1_f(G_\ell, W_n)$ using the one-one correspondence between elements of $H^1(G_\ell, W_n)$ and Yoneda extensions of $L/\ell^n L$ by itself in the category of $\mathbb{Z}_\ell/\ell^n G_\ell$-modules. A long but routine check demonstrates that the fourth row and β corresponds to each other under that correspondence. Hence, to show $\alpha \in H^1_f(G_\ell, W)$, it is enough to show $\beta \in H^1_f(G_\ell, W_n)$, or equivalently by definition, that E' is a short crystalline representation since L' is a G_ℓ-stable $\mathbb{Q}_\ell$-lattice in E'. By the following lemma, we see that E' is crystalline if E is crystalline, a fact which we will prove right after the proof of the lemma. Since V_1 is short, so is E'.

Lemma 5.3.3. *Crystalline representations (over $\mathbb{Q}$) are stable under taking finite direct sum, subobject, quotient object, internal homomorphism and tensor product over B in the category of (finitely generated) BG_ℓ-modules.*

Proof. We know that crystalline representations are stable under taking finite direct sum, subobject, quotient object, internal homomorphism and tensor product in the category of $\mathbb{Q}_\ell G_\ell$-modules. So they are also stable under taking finite direct sum, subobject, quotient object in the category of BG_ℓ-modules as the forgetful functor from this category to the category of $\mathbb{Q}_\ell G_\ell$-modules is exact. The internal homomorphisms of two objects in the category of BG_ℓ-modules is a subobject of the internal homomorphisms of these two object in the category of $\mathbb{Q}_\ell G_\ell$-modules. The tensor product of two objects in the category of BG_ℓ-modules is a quotient object of the tensor product of these two objects in the category of $\mathbb{Q}_\ell G_\ell$-modules. Hence, crystalline representations are also stable under taking internal homomorphism and tensor product in the category of BG_ℓ-modules. Now the lemma is proved.

So V is also crystalline. We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & V & \to & E & \to & B & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & B_{\text{crys}} \otimes_{\mathbb{Q}_p} V & \to & B_{\text{crys}} \otimes_{\mathbb{Q}_p} E & \to & B_{\text{crys}} \otimes_{\mathbb{Q}_p} B & \to & 0, \end{array}$$

which induces a commutative diagram of cohomology groups with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & V^{G_\ell} & \to & E^{G_\ell} & \to & B^{G_\ell} & \xrightarrow{r} & H^1(G_\ell, V) & \to \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow s & \\ 0 & \to & D_{\text{crys}}(V) & \to & D_{\text{crys}}(E) & \to & D_{\text{crys}}(B) & \xrightarrow{t} & H^1(G_\ell, B_{\text{crys}} \otimes_{\mathbb{Q}_\ell} V) & \to, \end{array}$$

where the third vertical arrow is just the identity map of B. So

$$\begin{aligned}\dim_{\mathbb{Q}_\ell}(D_{\text{crys}}(E)) &= \dim_{\mathbb{Q}_\ell}(D_{\text{crys}}(V)) + \dim_{\mathbb{Q}_\ell}(D_{\text{crys}}(B)) - \dim_{\mathbb{Q}_\ell}(\text{Im}(t)) \\ &= \dim_{\mathbb{Q}_\ell} V + \dim_{\mathbb{Q}_\ell} B - \dim_{\mathbb{Q}_\ell}(< t(1 \otimes_{\mathbb{Q}_\ell} 1) >_{B-module}) \\ &= \dim_{\mathbb{Q}_\ell} E - \dim_{\mathbb{Q}_\ell}(< s(r(1)) >_{B-module})\end{aligned}$$

Note that $r(1) = \bar{c}$. By definition of $H^1_{\mathfrak{f}}(G_\ell, V)$, $s(\bar{c}) = 0$. So E is crystalline.

The divisibility of $H^1_{\mathfrak{f}}(G_\ell, W)$ follows from its definition, and its $\mathbb{Z}_\ell$-corank is equal to the $\dim_{\mathbb{Q}_\ell} H^1_{\mathfrak{f}}(G_\ell, V)$, which is computed to be d in [B-K, §3.8.4] or [F-P2, §3.3 of Chapter 3]. We explain why the corank is equal to the $\dim_{\mathbb{Q}_\ell} H^1_{\mathfrak{f}}(G_\ell, V)$. We have a commutative diagram

$$\begin{array}{ccccccccc} & & H^1(G_\ell, T) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell & \cong & H^1(G_\ell, V) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \to & H^1(G_\ell, T) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell & \to & H^1(G_\ell, W) & \to & H^2(G_\ell, T)_{\text{tor}} & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & H^1(G_\ell, T)/\ell^m & \to & H^1(G_\ell, T/\ell^m) & \to & H^2(G_\ell, T)[\ell^m] & \to & 0, \end{array}$$

where the third row is exact and the second row, as the direct limit of the third row, is also exact. The group $H^2(G_\ell, T)_{\text{tor}}$ is finite. See [N-S-W, §2.3.7-to §2.3.10] for all non-trivial facts in the diagram. The first two rows show $H^1(G_\ell, W)$ is nearly a co-lattice in $H^1(G_\ell, V)$ in a sense that can be made clear and hence so is $H^1_{\mathfrak{f}}(G_\ell, W)$ in $H^1_{\mathfrak{f}}(G_\ell, V)$.

To finish the whole proof, it suffices to prove that

$$\dim_{\mathbb{F}_\ell} H^1_f(G_\ell, W)[\ell] \leq d.$$

Recall that finite AG_ℓ-module W_1 is defined by the exact sequence

$$0 \to W_1 \to W \xrightarrow{\ell} W \to 0,$$

which induces the exact sequence

$$0 \to \mathbb{F}_\ell \otimes_{\mathbb{Z}} W^{G_\ell} \to H^1(G_\ell, W_1) \to H^1(G_\ell, W)[\ell] \to 0.$$

Since $H^1_f(G_\ell, W_1)$ is the preimage of $H^1_f(G_\ell, W)$ of map $H^1(G_\ell, W_1) \to H^1(G_\ell, W)$, we derive another exact sequence

$$0 \to \mathbb{F}_\ell \otimes_{\mathbb{Z}} W^{G_\ell} \to H^1_f(G_\ell, W_1) \to H^1_f(G_\ell, W)[\ell] \to 0.$$

So we have the first equality of the following:

$$\begin{aligned} \dim_{\mathbb{F}_\ell} H^1_f(G_\ell, W)[\ell] &= \dim_{\mathbb{F}_\ell} H^1_f(G_\ell, W_1) - \dim_{\mathbb{F}_\ell}(\mathbb{F}_\ell \otimes_{\mathbb{Z}_\ell} W^{G_\ell}) \\ &= \dim_{\mathbb{F}_\ell} H^1_f(G_\ell, W_1) - \dim_{\mathbb{F}_\ell} W_1^{G_\ell} + \dim_{\mathbb{Q}_\ell} H^0(G_\ell, V). \end{aligned}$$

The second equality holds as once we write $W^{G_\ell} \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m \oplus U$ with U a finite torsion $\mathbb{Z}_\ell$-module, then $\dim_{\mathbb{F}_\ell}(\mathbb{F}_\ell \otimes_{\mathbb{Z}_\ell} W^{G_\ell}) = \dim_{\mathbb{F}_\ell} U/\ell U = \dim_{\mathbb{F}_\ell} U[\ell]$, $\dim_{\mathbb{F}_\ell} W_1^{G_\ell} = \dim_{\mathbb{F}_\ell}(\ell^{-1}\mathbb{Z}_\ell/\mathbb{Z}_\ell)^m \oplus U[\ell] = m + \dim_{\mathbb{F}_\ell} U[\ell]$ and $\dim_{\mathbb{Q}_\ell} H^0(G_\ell, V) =$

m. The last equality can be proved as in the following paragraph.

As $H^0(G_\ell, V) = H^0(G_\ell, T) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, $\dim_{\mathbb{Q}_\ell} H^0(G_\ell, V) = \dim_{\mathbb{Z}_\ell} H^0(G_\ell, T)$. It is clear that $\dim_{\mathbb{Z}_\ell} H^0(G_\ell, T) \leq m$. Suppose we are given $w_i \in W^{G_\ell}[\ell^i]$ corresponding to $(\overline{1/\ell^i}, 0, \cdots, 0; 0)$. Then $w_i = w_i' \otimes \overline{1/\ell^i}$ for $w_i \in T$. If $j > i$, $p^{j-i} w_j = w_i$. Hence, $(w_j' - w_i') \otimes \overline{1/\ell^i} = 0$, i.e., $w_j' - w_i' \in \ell^i T$. Hence $\lim_i w_i'$ converges to some element w in T. w is in T^{G_ℓ} as action by G_ℓ is continuous on T. Continuing in this way, we can construct m elements in T^{G_ℓ} that are $\mathbb{Z}_\ell$-linear independent. So $\dim_{\mathbb{Z}_\ell} H^0(G_\ell, T) \geq m$. Hence the desired equality.

Therefore it suffices to prove that

$$\dim_{\mathbb{F}_\ell} H^1_f(G_\ell, W_1) - \dim_{\mathbb{F}_\ell} H^0(G_\ell, W_1) = \dim_{\mathbb{Q}_\ell} V - \dim_{\mathbb{Q}_\ell} \mathrm{Fil}^0 D_{\mathrm{crys}}(V). \quad (5.9)$$

Choosing an object $\mathcal{D}$ in A-$\mathcal{MF}^0$ such that $\mathbb{V}(\mathcal{D}) \cong L \in A$-$\mathcal{GR}$. Proposition 5.1.2 shows that $\mathcal{D}$ is a free A-module. Proposition 5.1.1 tells further that $\mathrm{Fil}^i\mathcal{D}$ is an A-module direct summand of $\mathcal{D}$ and a free A-module for all i.

Let $\mathcal{D}_{/\ell}$ be the cokernel of multiplication by ℓ on $\mathcal{D}$. By the equivalence of the categories, $\mathbb{V}(\mathcal{D}_{/\ell}) \cong L/\ell L$. We have $\mathrm{Fil}^i\mathcal{D}_{/\ell} = \mathrm{Fil}^i\mathcal{D}/(\mathrm{Fil}^i\mathcal{D} \cap \ell\mathcal{D}) = \mathrm{Fil}^i\mathcal{D}/\ell\,\mathrm{Fil}^i\mathcal{D}$, the latter equality ensured by the fact that $\mathrm{Fil}^i\mathcal{D}$ is a $\mathbb{Z}_\ell$-module direct summand of $\mathcal{D}$.

We now construct the following exact sequence

$$\begin{array}{cccccc} 0 & \rightarrow & \hom_{A/\ell\text{-}\mathcal{MF}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) & \rightarrow & \hom_{A/\ell,\mathrm{Fil}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) & \\ & \stackrel{1-\phi}{\rightarrow} & \hom_{A/\ell}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) & \stackrel{\pi}{\rightarrow} & \mathrm{Ext}^1_{A/\ell\text{-}\mathcal{MF}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) & \rightarrow \ 0, \end{array} \quad (5.10)$$

where Ext^1 is the abelian group of Yoneda extensions in an abelian category with enough objects, like push out, pull back, etc.

The first nonzero map is a part of the forgetful functor. Since each filtration of $\mathcal{D}$ is an A-module direct summand of $\mathcal{D}$, each filtration of $\mathcal{D}/\ell$ is also an A/ℓ-module direct summand of $\mathcal{D}/\ell$. Hence we have $\mathrm{Fil}^i\mathcal{D}_{/\ell} = \mathcal{D}_{i/i+1} \oplus \mathrm{Fil}^{i+1}\mathcal{D}_{/\ell}$ for some choice of an A/ℓ-module $\mathcal{D}_{i/i+1}$. Note that $\mathcal{D}_{/\ell} = \oplus \mathcal{D}_{i/i+1}$ and that $\phi^i(\mathrm{Fil}^{i+1}\mathcal{D}_{/\ell}) = 0$. Define $\phi \in \mathrm{End}_{A/\ell}(\mathcal{D}_{/\ell})$ such that $\phi|_{\mathcal{D}_{i/i+1}} = \phi^i$. Then $\phi(\mathcal{D}_{/\ell}) = \Sigma\mathrm{Im}(\phi^i) = \mathcal{D}_{/\ell}$. So ϕ is an isomorphism as $\mathcal{D}_{/\ell}$ has finite length as $\mathbb{Z}_\ell$-modules. By abuse of notation, let ϕ also denote its adjoint action on $\mathrm{End}_{A/\ell}(\mathcal{D}_{/\ell})$ so that the second nonzero map is defined. Now we explain the construction of π. For $\eta \in \mathrm{hom}_{A/\ell}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell})$ we define an extension E_η of $\mathcal{D}_{/\ell}$ by itself in A/ℓ-$\mathcal{MF}$ with underlying A/ℓ-module $\mathcal{D}_{/\ell} \oplus \mathcal{D}_{/\ell}$, filtration

$$\mathrm{Fil}^i E_\eta := \mathrm{Fil}^i\mathcal{D}_{/\ell} \oplus \mathrm{Fil}^i\mathcal{D}_{/\ell}$$

and Frobenius map $\phi^i : \mathrm{Fil}^i E_\eta \to E_\eta$

$$\phi^i(x, y) = (\phi^i(x) + \eta\phi^i(y), \phi^i(y)).$$

Then $\pi(\eta)$ is the class of the Yoneda extension E_η in Ext^1 . The verification of the exactness of the sequence (5.10) is straightforward. (To show π is a surjection, we use the fact that $\mathcal{D}_{/\ell}$ is free over A/ℓ, which is true as $\mathcal{D}$ is free over A.)

Here comes a small twist of proof. We can redo the proof from the very beginning up to now with trivial modifications if we consider $\mathrm{End}_A(L)$ instead of $\mathrm{End}^0_A(L)$, i.e., consider $\widetilde{T} = \mathrm{End}_A(L)$, $\widetilde{W} = \widetilde{T} \otimes /\mathbb{Z}_\ell$, and $\widetilde{V} = \widetilde{T} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, etc while $\ell, A, L, \mathcal{D}$ are the same as before. Now we verify (5.10) implies (5.9).

$$\begin{aligned} H^1_f(G_\ell, \widetilde{W}_1) &= \{\text{Yoneda extensions of } L/\ell \text{ by itself in } A/\ell\text{-}\mathcal{GR}\} \\ &= \{\text{Yoneda extensions of } \mathcal{D}_{/\ell} \text{ by itself in } A/\ell\text{-}\mathcal{MF}^0\} \\ &= \mathrm{Ext}^1_{A/\ell\text{-}\mathcal{MF}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) \end{aligned}$$

$$\begin{aligned} H^0(G_\ell, \widetilde{W}_1) &= (\hom_{A/\ell}(L/\ell L, L/\ell L))^{G_\ell} \\ &= \hom_{A/\ell G_\ell}(L/\ell L, L/\ell L) \\ &= \hom_{\mathcal{FR}(A/\ell)}(L/\ell L, L/\ell L) \\ &= \hom_{A/\ell\text{-}\mathcal{MF}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) \end{aligned}$$

$$\begin{aligned} \dim_{\mathbb{Q}_\ell} \widetilde{V} &= \dim_{\mathbb{Q}_\ell} \hom_B(V_1, V_1) \\ &= \dim_{\mathbb{Z}_\ell} \hom_A(L, L) \\ &= \dim_{\mathbb{Z}_\ell} \hom_A(\mathcal{D}, \mathcal{D}) \\ &= \dim_{\mathbb{F}_\ell} \hom_{A/\ell}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell}) \end{aligned}$$

The second last equality holds because L and $\mathcal{D}$ are free over A of the same rank by Proposition 5.1.2.

$$\begin{aligned}\dim_{\mathbb{Q}_\ell} \mathrm{Fil}^0 D_{\mathrm{crys}}(\widetilde{V}) &= \dim_{\mathbb{Q}_\ell} \mathrm{Fil}^0 (B_{\mathrm{crys}} \otimes_{\mathbb{Q}_\ell} (\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{End}_A(L))^{G_\ell} \\ &= \dim_{\mathbb{Q}_\ell} \mathrm{Fil}^0 (\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{End}_A(\mathcal{D})) \\ &= \dim_{\mathbb{Z}_\ell} \mathrm{Fil}^0 (\mathrm{End}_A(\mathcal{D})) \\ &= \dim_{\mathbb{Z}_\ell} \hom_{A,\mathrm{Fil}}(\mathcal{D}, \mathcal{D}) \\ &= \dim_{\mathbb{F}_\ell} \hom_{A/\ell,\mathrm{Fil}}(\mathcal{D}_{/\ell}, \mathcal{D}_{/\ell})\end{aligned}$$

The last equality holds as $\mathrm{Fil}^i \mathcal{D}_{/\ell}$ are free over A/ℓ of the same rank as $\mathrm{Fil}^i \mathcal{D}$ over A.

The fourth equality from the bottom requires more explanation. One sees from [F-L, 8.4] that for $X \in \mathcal{MF}$, the natural map of filtered Galois ϕ-modules

$$B_{\mathrm{crys}} \otimes_{\mathbb{Z}_\ell} X \to B_{\mathrm{crys}} \otimes_{\mathbb{Z}_\ell} \mathbb{V}(X)$$

is an isomorphism, which leads to isomorphism of filtered ϕ-modules:

$$\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} X \to (B_{\mathrm{crys}} \otimes_{\mathbb{Z}_\ell} \mathbb{V}(X))^{G_\ell}. \tag{5.11}$$

So we need to show that $\mathbb{V}(\mathrm{End}_A L) = \mathrm{End}_A \mathcal{D}$, which can be proved by tracing the definition of $\mathbb{V}$. Note that $\mathrm{End}_A L$ is indeed an object of A-$\mathcal{MF}^0$.

So we have proved the equality $H^1_{\mathfrak{f}}(G_\ell, \widetilde{W}) = H^1_f(G_\ell, \widetilde{W})$ holds. If we change $\widetilde{W}$ back to W, the equality still holds as $\widetilde{W} = W \oplus (A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, $H^1_{\mathfrak{f}}(G_\ell, W) \subset H^1_f(G_\ell, W)$, $H^1_{\mathfrak{f}}(G_\ell, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell) \subset H^1_f(G_\ell, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, $H^1_{\mathfrak{f}}(G_\ell,$

$\widetilde{W}) = H^1_{\mathfrak{f}}(G_\ell, W) \oplus H^1_{\mathfrak{f}}(G_\ell, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, and $H^1_f(G_\ell, \widetilde{W}) = H^1_f(G_\ell, W) \oplus H^1_f(G_\ell, A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, where A is identified with the maps from L to itself that are multiplication by elements of A. □

Combining Propositions 5.3.1 and 5.3.2, we arrive at the following desired equality .

Proposition 5.3.4. *If* W^{I_p} *is divisible for all* $p \neq \ell$, *then*

$$H^1_\emptyset(G_{\mathbb{Q}}, W) = H^1_{\mathfrak{f}}(G_{\mathbb{Q}}, W).$$

Bibliography

[A-S] A. Agashe and W. Stein, *Generating the Hecke algebra as a $\mathbb{Z}$-module,* http://modular.fas.harvard.edu/papers/generating_hecke/appdx.dvi, Accessed by September 19, 2003

[Be] A. Beilinson, *Higher regulators and values of L-functions,* J. Soviet. Math. **30** (1985), pp. 2036–2070.

[B-F1] D. Burns and M. Flach, *Motivic L-functions and Galois module structures,* Math. Ann. **305** (1996) pp. 65–102.

[B-F2] D. Burns and M. Flach, *On Galois structure invariants associated to Tate motives,* Amer. J. Math. **120** (1998) pp. 1343–1397.

[B-F3] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients,* Doc. Math. **6** (2001), pp. 501–570 (electronic).

[B-F4] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients, II*, Am. J. Math. **125** (2003), pp. 475–512.

[B-K] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives,* in: The Grothendieck Festschrift, Vol. 1. Birkhäuser (1990), pp. 333–400.

[De1] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales,* in: Automorphic forms, representations and L-functions, Proc. Symp. Pure Math., American Math. Soc., **33** (1979), pp. 313–346.

[De2] P. Deligne, *Les constantes de l'équation fonctionnelle des fonctions L,* in: Modular functions of one variable. II, Lecture Notes in Math. **349**, Springer-Verlag, Berlin, 1997, 501–595.

[D-D-T] H. Darmon, F. Diamond and R. Taylor, *Fermat's last theorem,* in: Current developments in mathematics, 1995 (Cambridge, MA), pp. 1–154, Internat. Press, Cambridge, MA, 1994

[D-F-G1] F. Diamond, M. Flach and L. Guo, *The Bloch-Kato conjecture for adjoint motives of modular forms,* Mathematical Research Letters **8** (2001), pp. 437–442.

[D-F-G2] F. Diamond, M. Flach and L. Guo, *On the Bloch-Kato conjecture for adjoint motives of modular forms,* preprint, version August 9, 2001, (to appear in a shorter version?).

[Di] F. Diamond, *An extension of Wiles's results,* in: Modular Forms and Fermat's Last Theorem, Springer-Verlag, 1997, pp. 475–489.

[D-I] F. Diamond, J. Im, *Modular forms and modular curves,* in: Seminar on Fermat's Last Theorem Toronto, ON,(1993–1994), pp. 39–133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[Ei] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry,* Springer-Verlag, 1995

[Fo1] J.-M. Fontaine, *Valeurs spéciales des fonctions L des motifs,* in: Séminaire Bourbaki, exposé 751, février 1992, Astérisque No. 206 (1992), pp. 205–249.

[Fo2] J.-M. Fontaine, *Le corps des périodes p-adiques,* Astérisque No. 223(1994), pp. 59–111.

[F-L] J.-M. Fontaine and G. Laffaille, *Construction de représentations p-adiques,* Ann. Sci. Ec. Norm. Super. **15** (1982), pp. 547–608.

[F-P1] J.-M. Fontaine and B. Perrin-Riou, *Autour des conjectures de Bloch et Kato. III. Le cas général.* C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. **7**, 421–428.

[F-P2] J.-M. Fontaine and B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonction L,* in: Motives, Proc. Symp. in Pure Math. **55**, Part 1 (1994), pp. 599–706.

[Hi1] H. Hida, *Congruences of cusp forms and Hecke algebras*, in: Séminaire de théorie des nombres, Paris 1983–84, 133–146, Progr. Math., 59, Birkhuser Boston, Boston, MA, 1985.

[Hi2] H. Hida, *Modular Forms and Galois Cohomology,* Cambridge university press, 2000. (A list of misprints at http://www.math.ucla.edu/ hida/)

[Hi3] H. Hida, *Geometric Modular Forms and Elliptic Curves,* World Scientific Publishing Co., Singapore, 2000, (A list of misprints at http://www.math.ucla.edu/ hida/)

[Hu-Ki] A. Huber and G. Kings, *Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture*, in: Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), pp. 149–162, Higher Ed. Press, Beijing, 2002.

[Ka1] K. Kato, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* B_{dR}*, Part I,* in: Arithmetic algebraic geometry (ed. E. Ballico), pp. 50–163, Lecture Notes in Math. 1553, Springer, New York, 1993.

[Ka2] K. Kato, *Iwasawa theory and p-adic Hodge theory,* Kodai Math. J. **16** (1993), pp. 1–31.

[Ki] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms,* J. Number Theory **97** (2002), no. 1, pp. 157–164.

[K-M] F. Knudsen and D. Mumford, *The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div',* Math. Scand. **39** (1976) pp.19–55.

[La] S. Lang, *Algebra,* third edition, Addison-Wesley, 1999.

[L-S] J.-C. Lario and R. Schoof, *Some computation with Hecke rings and deformation rings,* http://modular.fas.harvard.edu/papers/generating_hecke/schoof.dvi

[Ma1] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), pp. 33–186 (1978).

[Ma2] B. Mazur, *Galois Deformation and Hecke Curves,* very rough preprint for course Math257 at Harvard, 1994.

[Ma3] B. Mazur, *An introduction to the representations of Galois representations,* in: Modular Forms and Fermat's Last Theorem, Springer-Verlag, 1997, pp. 243–311.

[Mi] J. S. Milne, *Arithmetic duality theorems*, Perspect. Math., Vol 1, Academic Press, 1986.

[M-R] B. Mazur, L. Roberts, *Local Euler characterictics,* Invent. math. **9** (1970), pp. 201–234.

[N-S-W] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields,* Springer-Verlag, 2000

[PR] B. Perrin-Riou, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, 3, Paris, 2000.

[Ra] R. Ramakhrishna, *On a variation of Mazur's deformation functor,* Compositio Math. **87** (1993), pp. 269–286

[Ri] K.A. Ribet, *Endomorphism of semi-stable abelian varieties over number fields,* Annals of Mathematics, 2nd series. Vol. **101**, no. 3 (May, 1975), pp. 555–562.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Princeton University Press, 1994.

[St1] W. Stein, http://modular.fas.harvard.edu/Tables/MotiveDecomp_N1-125_k2, Accessed by September 19, 2003

[St2] W. Stein, http://modular.fas.harvard.edu/Tables/discsk.gp, Accessed by September 19, 2003

[St3] W. Stein, *Modular form explorer,* http://modular.fas.harvard.edu /mfd/mfe/, Accessed by September 19, 2003

[Sw] R. G. Swan, *Algebraic K-theory,* Lecture Note in Math. **76**, Springer, 1968.

[Ta] J. Tate, *Number Theoretic Background*, Proc. Symp. Pure Math. **33** Vol. 23–26, Amer. Math. Soc. 1979.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Annals of Math. **141** (1995), pp. 443–551.