A cohomological version of Ribet's Method

Dissertation zur Erlangung des Doktorgrades
der Naturwissenschaften (Dr. rer. nat.)
der Fakultät für Mathematik
der Universität Regensburg

vorgelegt von

Chiara Sabadin

aus Venezia, Italien

im Jahr 2026

Promotionsgesuch eingereicht am:

Die Arbeit wurde angeleitet von: Prof. Dr. Guido Kings

Contents

1. Introduction

In Number Theory one of the most famous results is Fermat's Last Theorem, stating that there exists no non-trivial positive integer solution (x, y, z) to the equation

$$x^n + y^n = z^n \text{ for any } n > 2.$$

Claimed in the 17th century on a marginal note by Fermat, for centuries mathematicians tried to prove this statement, and a lot of the current results and techniques in Number Theory and Arithmetic Geometry are due to this process. The Theorem was proved by Andrew Wiles[1] only in 1994 in the two milestone papers "Modular elliptic curves and Fermat's Last Theorem" ([Wil95]) and "Ring theoretic properties of certain Hecke algebras" ([TW95]).
This thesis focuses on one of the key techniques that led to Wiles' proof: Ribet's Method ([Rib76]), that relates special values of the Riemann ζ-function with Galois representations attached to modular forms. The goal of this thesis is to give a cohomological version of this method, using classes in the étale cohomology of a modular curve, instead of modular forms.

1.1. Irregular primes and Kummer's Criterion

For l an odd prime number, let us consider the cyclotomic field $\mathbb{Q}(\mu_l)$, where μ_l denotes the group of l-th roots of unity. Recall that the class number of $\mathbb{Q}(\mu_l)$ is the (finite) order of the class group A of $\mathbb{Q}(\mu_l)$. Until the beginning of the 19th century, it was wrongly believed that the ring of integers $\mathbb{Z}[\mu_l]$ of $\mathbb{Q}(\mu_l)$ was a unique factorization domain. It was only in 1847 that Ernst Kummer, in his attempts on solving Fermat's Last Theorem, proved this statement wrong. But, by doing so, he realised that Fermat's Last Theorem was indeed true for a particular set of exponents n, the so-called regular primes.

Definition 1.1.1. An (odd) prime l is an *irregular prime* if l divides the class number of $\mathbb{Q}(\mu_l)$.
A prime is said to be *regular* if it is not irregular.

Kummer showed in 1847 that Fermat's Last Theorem held for regular primes ([Con]), hence, to complete Fermat's Last Theorem proof, it was enough to show that the Theorem was also holding for irregular primes. Since there exists an infinite number of irregular primes ([Was97] 5.17), in order to study them better, Kummer gave a more arithmetic characterization of irregular primes, nowadays known as *Kummer's Criterion*:

[1] with contributions, among many, of Taniyama, Shimura, Weil, Frey, Ribet and Taylor.

Lemma 1.1.2. *An odd prime prime l is irregular if and only if there exists an even integer k, $2 \leqslant k \leqslant l-3$, such that $l \mid B_k$, where $B_k \in \mathbb{Q}$ is the k-th Bernoulli number defined by*

$$\frac{x}{e^x - 1} + \frac{x}{2} - 1 = \sum_{n \geqslant 2} \frac{B_n}{n!} x^n.$$

Let us now define the *Riemann ζ-function* as the analytic continuation to $\mathbb{C} \smallsetminus \{1\}$ of

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s}, \qquad\qquad s \in \mathbb{C},\ Re(s) > 1$$

and recall its relation with the Bernoulli numbers given by

$$B_n = -n\zeta(1-n) \text{ for any } n \geqslant 1.$$

In light of this relation, we notice that Kummer's Criterion is equivalent to say that a prime l is irregular if and only if there exists an even integer $2 \leqslant k \leqslant l-3$ with the property that $l \mid \zeta(1-k)$.

1.2. Ribet's Method

Kummer's Criterion showed that, in order to prove Fermat's Last Theorem, it was more convenient to focus on the arithmetic side of the picture. At the beginning of 20th century, a stronger version of Kummer's Criterion, now known as *Herbrand-Ribet Theorem*, was stated. Let us consider the cyclotomic character

$$\chi\colon \operatorname{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/l\,\mathbb{Z})^\times \text{ defined by } \sigma(\zeta_l) = \zeta_l^{\chi(\sigma)},$$

for ζ_l a primitive l-th root of unity, and define

$$C := A/A^l = A/\{a^l \mid a \in A\}$$

to be the maximal l-quotient of the class group A of $\mathbb{Q}(\mu_l)$. Then the Galois group $\operatorname{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})$ acts naturally on C and we obtain a canonical decomposition

$$C = \bigoplus_{i=1}^{l-1} C(\chi^i) = \bigoplus_{i=1}^{l-1} \{c \in C \mid \sigma(c) = \chi^i(\sigma)c \text{ , for every } \sigma \in \operatorname{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})\}$$

of C into χ^i-eigenspaces. In this setting, we can state the Herbrand-Ribet Theorem[2]:

Theorem 1.2.1. *Let k be an even integer such that $2 \leqslant k \leqslant l-3$. Then $l \mid \zeta(1-k)$ if and only if $C(\chi^{1-k}) \neq 0$.*

[2] Let us notice that this is indeed a stronger result than Kummer's Criterion, indeed it does not only show when the class group A has order divisible by l (and hence $C \neq 0$), but it even gives the specific non-trivial eigenspace of C.

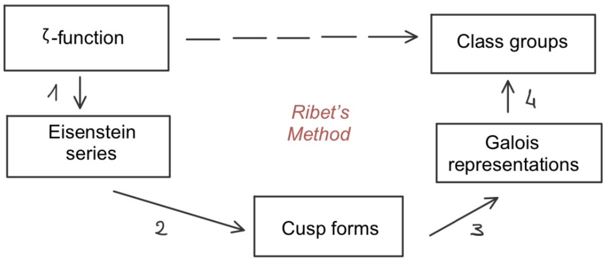


Figure 1.1.: Schematic version of Ribet's Method

The sufficient condition of this statement was proved by Herbrand in 1932 using Algebraic Number Theory ([Her32]), while the other implication was proved only in 1976 by Ribet in his paper "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$" ([Rib76]). In its proof Ribet developed what is now known as Ribet's Method, a way of relating the Riemann ζ-function and the class group of $\mathbb{Q}(\mu_l)$ using modular forms and Galois representations attached to them. We present here a schematic version of this Method, but we refer to Chapter 4 for more details: as the special value of the Riemann ζ-function arises as constant coefficient in some Eisenstein series, we can construct a cusp form related to this Eisenstein series, and then, using this cusp form and the assumption that the prime l divides the ζ-value, construct a Galois representation ρ of the absolute Galois group of $\mathbb{Q}$ over $\mathrm{GL}_2(\mathbb{Z}/l\,\mathbb{Z})$. Then, considering the unramified extension in $\overline{\mathbb{Q}}$ given by the fixed field of $\ker\rho$ and using Class Field Theory, we conclude that the appropriate eigenspace of C is not trivial.

1.3. Cohomological version of Ribet's Method

The goal of this thesis project is to give a cohomological version of Ribet's Method, replacing the Eisenstein series and the cusp form by suitable classes in the étale cohomology of a modular curve. In particular, we will consider a modular curve $Y(l)$ with level-l-structure and we will construct an Eisenstein class (see 3.4.8)

$$ {}_c e_{k-2} \in H^1_{et}(Y(l), \mathrm{TSym}^{k-2}\mathscr{H}(1)) $$

and a cusp class (see 5.2.1)

$$ \alpha \in H^1_{et}(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2}\mathscr{H}(1)), $$

playing the role of the Eisenstein series and cusp form in Ribet's Method, where $\mathscr{H}$ is the sheaf associated to the l-torsion points of the universal elliptic curve over $Y(l)$, and $Y(l)_{\overline{\mathbb{Q}}}$ is the base change of $Y(l)$ to $\mathrm{Spec}\,\overline{\mathbb{Q}}$. We will then show that to this cusp class we can associate an unramified Galois extension of $\mathbb{Q}(\mu_l)$ as the one constructed in Ribet's Method.

Let us point out that a cohomological version of Ribet's Method is a way of approaching this statement from a geometric point of view, allowing possible further applications in Arithmetic Geometry, in particular to the Iwasawa Main Conjecture.

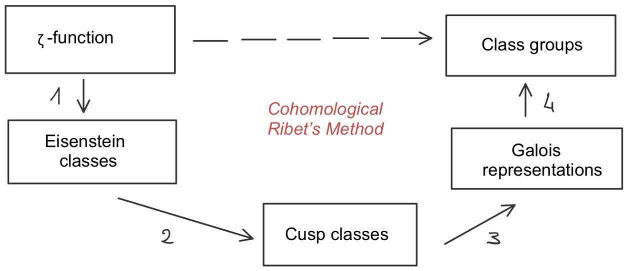


Figure 1.2.: Schematic version of Cohomological Ribet's Method

1.4. Organisation of the Thesis

In Chapter 3 we define our setting and introduce, mainly rewriting the work in [Kin15] accordingly to our notation, all the constructions and results needed for the Cohomological Ribet's Method. In Chapter 4 we give a more detailed description of Ribet's Method, based on [Rib76], while in Chapter 5 we use Chapter 3 to give a cohomological "translation" of Ribet's Method, the so-called "Cohomological Ribet's Method", showing how the cohomology classes constructed in 3 give rise to an unramified Galois extension equivalent to the one of Ribet's. At the end of this work, the reader may also find Appendix A, containing all the relevant prerequisites to understand the main part of this work.

2. Acknowledgements

"Verba volant, scripta manent". My grandma used to say it often and for this reason I have decided to dedicate a page of my thesis to express my gratitude to all the people who have accompanied me to the end of my PhD journey. They all deserve to be remembered. First, I would like to thank my advisor Guido Kings, for the opportunity of doing a PhD and for his help in these last adventurous months, and all the colleagues in my working group, especially Han-Ung Kufner, for many helpful mathematical discussions and a nice atmosphere. I would like to thank SFB 1085 and the DFG for funding and supporting my PhD. Many well-deserved thanks also go to Katrin Henkel and Birgit Tiefenbach, whose help was always very effective and whose kindness made the third floor a pleasant place to work. I would also like to thank Chenying, Christoph, Clara, Enrica, Franziska, Giacomo, Han-Ung, Kevin, Luca, Malena, Matthias, Pietro and Zhenghang: not only colleagues but good friends, the time spent together made my Regensburg years really nice! Many thanks go also to my fellow organisers of Women in Mathematics Regensburg, Alex, Eleni, Franziska and Malena: your passion and kindness helped making this group a very welcoming place, where many people in our department can feel "at home". I would also like to thank all the people I have met in the conferences I have attended, I have always had pleasant experiences and met who are now some good friends of mine, in particular I want to recall Ana, Sara, Beatrice and Guillermo. Together with many other mathematicians I have met, they showed me that in the math world there are heartful and kind people who are shaping a better environment. I would also like to thank all the people who in these last few years have helped me navigate what my future career might be with precious and endless help and advice. Thanks to Roberto, my "math big brother", whose advices have helped me toward and through my PhD. Thanks to Miriam, not only the best office-mate ever, but also a genuine, kind and inspiring friend: you are my example of enjoying our job, creating a wonderful family and being there for the people we love.

Many thanks also go to some people who know me since before my Regensburg time, you all represent more than what I am able to express with words. In particular, thanks to my friends from Venice, who show me that it matters the quality and not the quantity of a friendship. Thanks to Giacomo for showing me that strong bonds can withstand time and distance. Thanks to Giovanni. Thanks to Sara, your friendship is one of the most precious things I have. Thanks to all my family, with whom I share never-ending video-calls and whose support for what I do and who I am is always there.

3. Moments, residues and elliptic Soulé elements

In this chapter we collect definitions and statements from [Kin15] that will be needed in the following sections of the thesis.

3.1. Notation and setting

Let l be an odd prime and fix a primitive root of unity $\zeta_l \in \mathbb{Q}(\mu_l)$, where μ_l denotes the group of l-th roots of unity. Let $Y(l)$ be the modular curve parametrising elliptic curves E with level-l-structure $(\mathbb{Z}/l\,\mathbb{Z})^2 \xrightarrow{\cong} E[l]$. It is naturally a scheme over $\operatorname{Spec}\mathbb{Q}(\mu_l)$ and so, by the natural map $\operatorname{Spec}\mathbb{Q}(\mu_l) \to \operatorname{Spec}\mathbb{Q}$, also a $\mathbb{Q}$-scheme. Let $\pi : \mathcal{E} \to Y(l)$ be the universal elliptic curve and denote by $e : Y(l) \to \mathcal{E}$ its unit section. Let $X(l)$ be the compactification of $Y(l)$ and $j : Y(l) \hookrightarrow X(l)$ the open immersion. Denote by $\mathrm{Cusp} := X(l) \smallsetminus Y(l)$ the subscheme of cusps. Let us consider the Tate curve $\mathcal{E}_q$ with level-l-structure $(\mathbb{Z}/l\,\mathbb{Z})^2 \to \mathcal{E}_q[l]$ given by $(a, b) \mapsto q^a\zeta^b$ defining a section

$$\infty : \operatorname{Spec}\mathbb{Q}(\mu_l) \to \mathrm{Cusp},$$

such that, under the $\mathrm{GL}_2(\mathbb{Z}/l\,\mathbb{Z})$-equivariant isomorphism

$$\mathrm{Cusp} \cong \coprod_{\mathrm{GL}_2(\mathbb{Z}/l\,\mathbb{Z})/\pm\begin{pmatrix} * & * \\ 0 & 1\end{pmatrix}} \operatorname{Spec}\mathbb{Q}(\mu_l),$$

∞ is mapped to the component corresponding to the identity matrix. Define, for i natural number and n an integer, the *n-th Tate twist* of the (sheaf of) module $\mathbb{Z}/l^i\,\mathbb{Z}$ by

$$\mathbb{Z}/l^i\,\mathbb{Z}(n) = \begin{cases} \mu_{l^i}^{\otimes n} & n \geqslant 0 \\ \mathrm{Hom}_{\mathbb{Z}/l^i\,\mathbb{Z}}(\mathbb{Z}/l^i\,\mathbb{Z}(-n), \mathbb{Z}/l^i\,\mathbb{Z}) & n < 0 \end{cases},$$

that is naturally equipped with a $\mathrm{Gal}(\mathbb{Q}(\mu_{l^i})/\mathbb{Q})$-action given by the power χ_i^n of the cyclotomic character $\chi_i : \mathrm{Gal}(\mathbb{Q}(\mu_{l^i})) \xrightarrow{\cong} (\mathbb{Z}/l^i\,\mathbb{Z})^\times$ defined by $\sigma(\zeta_{l^i}) = \zeta_{l^i}^{\chi_i(\sigma)}$.

3.2. Preliminaries

On the modular curve $Y(l)$ let us define the étale sheaves

$$\mathscr{H}_i := (R^1\pi_*\,\mathbb{Z}/l^i\,\mathbb{Z})^\vee \tag{3.1}$$
$$\mathscr{H} := (R^1\pi_*\,\mathbb{Z}_l)^\vee \tag{3.2}$$

where $(\cdot)^\vee$ denotes (respectively) the $\mathbb{Z}/l^i\mathbb{Z}$-, $\mathbb{Z}_l$-dual.

Remark 3.2.1 (A.5.3). $\mathscr{H}_i \cong R^1\pi_*\mathbb{Z}/l^i\mathbb{Z}(1)$ and $\mathscr{H} \cong R^1\pi_*\mathbb{Z}_l(1)$.

Let us now recall the definition of divided power algebra.

Definition 3.2.2 ([BO78] Appendix A). Let R be a commutative ring, M an R-module.

1. The *divided power algebra* $\Gamma(M) = \oplus_{k\geqslant 0}\Gamma^k(M)$ is a graded augmented R-algebra, with $\Gamma_0(M) = R$, $\Gamma_1(M) = M$ and augmentation ideal $\Gamma^+(M) = \oplus_{k\geqslant 1}\Gamma^k(M)$. For any element $m \in M$, we can define $m^{[k]} \in \Gamma^k(M)$ such that $m^k = k!m^{[k]}$.
2. If M is a free R-module with basis $\{m_1, \dots, m_r\}$, then the R-module $\Gamma^k(M)$ is free with basis given by $\{m_1^{[i_1]}\cdots m_r^{[i_r]} \mid \sum_{i=1}^r i_j = k\}$.

In particular, we have an R-algebra homomorphism $\operatorname{Sym}^k M \to \Gamma^k(M)$, given by $m^k \mapsto k!m^{[k]}$, and, for M a free R-module, an R-algebra isomorphism[1] $\Gamma^k(M) \cong \operatorname{TSym}^k M$, given by $m^{[k]} \mapsto m^{\otimes k}$([Kin16] 1.2). Hence, by this isomorphism, we deduce that $\operatorname{TSym}^k M$ is compatible with arbitrary base change, and so, in particular,

$$(\operatorname{TSym}^k M)\otimes_{\mathbb{Z}_l}\mathbb{Z}/l^i\mathbb{Z} \cong \operatorname{TSym}^k(M\otimes\mathbb{Z}/l^i\mathbb{Z}),$$

and so it sheafifies well, i.e., for $\mathscr{H}$ the sheaf defined in (3.1), we can define $\operatorname{TSym}^k(\mathscr{H})$ to be the sheaf associated to the presheaf $U \mapsto \Gamma^k(\mathscr{H}(U))$. Therefore let us denote by $\operatorname{Sym}^k\mathscr{H}_i$ and $\operatorname{Sym}^k\mathscr{H}$ the k-th symmetric power as (respectively) $\mathbb{Z}/l^i\mathbb{Z}$-, $\mathbb{Z}_l$-modules and by $\operatorname{TSym}^k\mathscr{H}_i$, $\operatorname{TSym}^k\mathscr{H}$ the k-th symmetric tensor power as (respectively) $\mathbb{Z}/l^i\mathbb{Z}$-,$\mathbb{Z}_l$-modules. There is a $\mathbb{Z}_l$-algebra homomorphism

$$\operatorname{Sym}^k\mathscr{H} \to \operatorname{TSym}^k\mathscr{H}\ ,\ (v_1,\dots,v_k) \mapsto \frac{1}{k!}\sum_{\sigma\in\Sigma_k} v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(k)}$$

given by the universal property of $\operatorname{Sym}^k\mathscr{H}$ applied to the isomorphism $\mathscr{H} \to \operatorname{TSym}^1\mathscr{H}$, $h \mapsto h^{\otimes 1}$.

For an inverse system $\mathscr{F} = (\mathscr{F}_i)_{i\geqslant 1}$ of étale sheaves modulo Mittag-Leffler-zero systems over an étale scheme S, we define the continuous étale cohomology $H^n(S,\mathscr{F})$ (following [Jan88]) to be the n-th right derived functor of $\mathscr{F} \mapsto \varprojlim_i H^0(S,\mathscr{F}_i)$. In this work we will often (implicitly) make use of the following lemma:

Lemma 3.2.3. *Let $\mathscr{F} = (\mathscr{F}_i)_{i\geqslant 1}$ be a projective system, where the cohomology groups $H^0(S,\mathscr{F}_i)$ are finite for every $i \geqslant 1$, then*

$$H^1(S,\mathscr{F}) \cong \varprojlim_i H^1(S,\mathscr{F}_i)$$

For ℓ-adic sheaves, we also define $\operatorname{Ext}^i_S(\mathscr{F},\mathscr{G})$ to be the right derived functor of $\operatorname{Hom}_S(\mathscr{F},\cdot)$.

[1] where $\operatorname{TSym}^k M = \{x \in M^{\otimes k} \mid S_k(x) = x\}$, for S_k the group of k-permutations, is the k-th tensor symmetric power of M.

3.3. Analytic and cyclotomic moment maps

Let $X = \varprojlim_i X_i$ be a totally disconnected compact topological space, where each X_i is finite and discrete.

DEFINITION 3.3.1. Let

$$\mathscr{C}(X, \mathbb{Z}_l) := \{f : X \to \mathbb{Z}_l \mid f \text{ continuous}\}$$

denote the space of *continuous $\mathbb{Z}_l$-valued functions on X* endowed with the sup-norm $\|\cdot\|_\infty$.

DEFINITION 3.3.2. Let

$$\Lambda(X) := \mathrm{Hom}_{\mathbb{Z}_l}(\mathscr{C}(X, \mathbb{Z}_l), \mathbb{Z}_l)$$

be the space of *$\mathbb{Z}_l$-valued measures on X*, where $\mu \in \Lambda(X)$ is described by

$$\mu : \mathscr{C}(X, \mathbb{Z}_l) \to \mathbb{Z}_l \text{ given by } f \mapsto \mu(f) := \int_X f\mu.$$

Analogously, define the space of $\mathbb{Z}/l^i\mathbb{Z}$*-valued measures on* X by $\Lambda_i(X) := \mathrm{Hom}_{\mathbb{Z}_l}(\mathscr{C}(X, \mathbb{Z}_l), \mathbb{Z}/l^i\mathbb{Z})$.

REMARK 3.3.3.
1. Since every $f \in \mathscr{C}(X, \mathbb{Z}_l)$ is the uniform limit of locally constant functions, we have

$$\Lambda(X) = \varprojlim_i \mathrm{Hom}_{\mathbb{Z}_l}(\mathscr{C}(X_i, \mathbb{Z}_l), \mathbb{Z}_l) = \varprojlim_i \Lambda(X_i) = \varprojlim_i \Lambda_i(X_i).$$

2. For $X := H = \varprojlim_i H_i$ a profinite group, we have that $\Lambda(X)$ inherits a $\mathbb{Z}_l$-algebra structure given by

$$\mu * \nu := \mathrm{mult}_!(\mu \otimes \nu).$$

   $\Lambda(H)$ is called the *Iwasawa algebra of H*.

In this section we want to define sheaves of Iwasawa modules, i.e. sheaves that are inverse systems of sheaves of modules.

DEFINITION 3.3.4.
1. Let $(p_i : X_i \to Y(l))_i$ be a projective system of finite étale schemes over $Y(l)$ with transition maps given by the finite étale maps $\lambda_i : X_{i+1} \to X_i$. Let $X := \varprojlim_i X_i$ be the inverse limit and let $\mathscr{X}_i$ be the étale sheaf associated to X_i.[2]

2. Define on $Y(l)$ the étale sheaf

$$\Lambda_i(\mathscr{X}_i) := p_{i*}\mathbb{Z}/l^i\mathbb{Z} \in \mathrm{Sh}(Y(l)).$$

   and consider the projective system $(\Lambda_i(\mathscr{X}_i))_i$ with transition maps given by

$$\alpha_i := \mathrm{red}_{l^i} \circ \mathrm{tr}_{\lambda_i} : \Lambda_{i+1}(\mathscr{X}_{i+1}) = p_{i+1*}\mathbb{Z}/l^{i+1}\mathbb{Z} \to p_{i*}\mathbb{Z}/l^i\mathbb{Z} =: \Lambda_i(\mathscr{X}_i).$$

[2] i.e., for X_i an étale scheme over $Y(l)$, we have $\mathscr{X}_i \in Sh(Y(l))$ given by $\mathscr{X}_i(\cdot) = \mathrm{Hom}_{Y(l)}(\cdot, p_{i*}X_i)$.

Then we can define an inverse system of étale sheaves on $Y(l)$, called the *sheaf of Iwasawa modules*, by

$$\Lambda(\mathscr{X}) := (\Lambda_i(\mathscr{X}_i))_{i\geqslant 1}$$

with transition maps $(\alpha_i)_i$.

REMARK 3.3.5. 1. $\Lambda(\mathscr{X})$ is functorial, compatible with base change[3] and such that[4] $\Lambda_i(\mathscr{X}_i \times_{Y(l)} \mathscr{Y}_i) \cong \Lambda_i(\mathscr{X}_i) \otimes \Lambda_i(\mathscr{Y}_i)$.

2. $\Lambda(\mathscr{X})$ is the sheafification of the space of measures $\Lambda(X)$ defined in 3.3.2 in the sense that, for a geometric point $\overline{s} : \operatorname{Spec} \overline{K} \to Y(l)$, we have[5]

$$\Lambda_i(\mathscr{X}_i)_{\overline{s}} \cong \Lambda_i(\mathscr{X}_{i,\overline{s}}) \cong \Lambda_i(X_i)$$

3. If $X := H = \varprojlim_i H_i$ is a pro-étale group scheme over $Y(l)$ with $p_i : H_i \to Y(l)$ finite étale, then the sheaves $\Lambda_i(\mathscr{X}_i)$ are sheaves of Iwasawa $\mathbb{Z}/l^i\mathbb{Z}$-algebras with a ring structure induced by the group multiplication on H_i.

3.3.1. Analytic moment maps

Define the completion of $\operatorname{TSym}^k H$ by $\widehat{\operatorname{TSym}}^k H := \varprojlim_n \operatorname{TSym} H/(\oplus_{k\geqslant 1} \operatorname{TSym}^k H)^n$ and analogously for H_i. Note that, by [Kin15] 12.2.3, we have $\widehat{\operatorname{TSym}} H \cong \varprojlim_i \widehat{\operatorname{TSym}} H_i$.

For $H = \mathbb{Z}_l = \varprojlim_i \mathbb{Z}/l^i\mathbb{Z}$, we can then define the analytic moment map as follows:

Proposition 3.3.6. *There exists a unique $\mathbb{Z}_l$-algebras homomorphism, called analytic moment map,*

$$\operatorname{mom} : \Lambda(H) \to \widehat{\operatorname{TSym}} H \text{ given by } \delta_h \mapsto \sum_{k\geqslant 0} h^{[k]},$$

where δ_h is the Dirac distribution[6]. Moreover,

$$\operatorname{mom} = \varprojlim_i \operatorname{mom}_i : \Lambda_i(H_i) \to \widehat{\operatorname{TSym}} H_i.$$

For $e \in H$ basis of H and $x : H \to \mathbb{Z}_l$ its dual basis, we have that the image via the analytic moment map of a measure $\mu \in \Lambda(H)$ is given by

$$\operatorname{mom}(\mu) = \sum_{k\geqslant 0} (\int_H x^k \mu) e^{[k]}.$$

[3] i.e. for a $Y(l)$-scheme $\alpha : S \to Y(l)$ and $\mathscr{X}_{i,S} := \mathscr{X}_i \times_{Y(l)} S$, by proper base change, we obtain $\alpha^*\Lambda_i(\mathscr{X}_i) \cong \Lambda_i(\mathscr{X}_{i,S})$.

[4] By using the Künneth formula.

[5] For details, see [Kin16] 4.4.2 and [Kin15] 12.2.10

[6] i.e. $\delta_h(f) = f(h)$ for any $f \in \mathscr{C}(H, \mathbb{Z}_l)$

The projection onto the k-th component, called the analytic k-th moment map is given by

$$\mathrm{mom}^k : \Lambda(H) \to \mathrm{TSym}^k H$$

and, on finite level, by

$$\mathrm{mom}^k_i : \Lambda_i(H_i) \to \mathrm{TSym}^k H_i.$$

Remark 3.3.7. The analytic moment map is functorial in H.

3.3.2. Torsors and analytic moment maps

Let $N > 1$ and consider the short exact sequence of finite étale group schemes over $Y(l)$

$$0 \to \mathbb{Z}/l^i\,\mathbb{Z} \to \mathbb{Z}/l^iN\,\mathbb{Z} \xrightarrow{q_i} \mathbb{Z}/N\,\mathbb{Z} \to 0,$$

where q_i is the reduction modulo N. Let $t : Y(l) \to \mathbb{Z}/N\,\mathbb{Z}$ be a N-torsion section and define a $\mathbb{Z}/l^i\,\mathbb{Z}$-torsor

$$\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle := q_i^{-1}(t) = \{x \in \mathbb{Z}/l^iN\,\mathbb{Z} \mid x \equiv t \bmod N\} \tag{3.3}$$

over $Y(l)$ via the following cartesian diagram

$$\begin{tikzcd} \mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle \arrow[r] \arrow[d, "q_{i,t}"'] & \mathbb{Z}/l^iN\,\mathbb{Z} \arrow[d, "q_i"] \\ Y(l) \arrow[r, "t"] & \mathbb{Z}/N\,\mathbb{Z} \end{tikzcd}$$

and define $\mathbb{Z}_l\langle t\rangle$ to be the inverse limit

$$\mathbb{Z}_l\langle t\rangle := \varprojlim_i \mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle.$$

Let $\Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle), \Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z})$ and $\Lambda(\mathbb{Z}_l\langle t\rangle), \Lambda(\mathbb{Z}_l)$ be the spaces of measures defined in 3.3.2. Then $\Lambda(\mathbb{Z}_l\langle t\rangle)$ is a $\Lambda(\mathbb{Z}_l)$-module of rank one.

To the torsor $\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle$ defined in (3.3) we can associate an analytic moment map, as in 3.3.6.

Definition 3.3.8. Define the *i-th analytic moment map*

$$\mathrm{mom}^k_{i,t} := \mathrm{mom}^k_i \circ [N]_! : \Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle) \xrightarrow{[N]} \Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z}) \to \mathrm{TSym}^k\,\mathbb{Z}/l^i\,\mathbb{Z}$$

given by

$$\mu \mapsto \mu(N\cdot) \mapsto \sum_{x \in \mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle} N x^{[k]} \mu(x),$$

where mom^k_i is the map defined in 3.3.6. Define the *analytic moment map* as the inverse limit

$$\mathrm{mom}^k_t := \varprojlim_i \mathrm{mom}^k_{i,t} : \Lambda(\mathbb{Z}_l\langle t\rangle) \to \mathrm{TSym}^k\,\mathbb{Z}_l\,.$$

Remark 3.3.9. Note that $\mathrm{mom}^k_{i,t}$ is not independent of the choice of N.

3.3.3. Bernoulli measures

In the setting of 3.3.2, we want to define a measure on $\mathbb{Z}_l\langle t\rangle$.

Definition 3.3.10 (Bernoulli measure on $\Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle)$ and $\Lambda(\mathbb{Z}_l\langle t\rangle)$). Let $c \in \mathbb{Z}$ be such that $(c, 6lN) = 1$ and let $B_k(x) \in \mathbb{Q}[x]$ be the k-th Bernoulli polynomial defined by

$$\frac{te^{tx}}{e^t-1} = \sum_{k\geqslant 0} B_k(x)\frac{t^k}{k!}.$$

The map

$$B_{2,c,i}^{\langle t\rangle} : \mathbb{Z}/l^i\mathbb{Z}\langle t\rangle \to \mathbb{Z}/l^i\mathbb{Z}$$

given by

$$x \mapsto \frac{l^iN}{2}(c^2B_2(\{\frac{x}{l^iN}\}) - B_2(\{\frac{cx}{l^iN}\}),$$

where $\{x\}$ denotes the representative of $x \in \mathbb{R}/\mathbb{Z}$ in $[0,1[$, defines an element

$$B_{2,c,i}^{\langle t\rangle} \in \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle)$$

From the distribution properties of Bernoulli polynomials (see [Lan90] §2.2) we deduce that the elements $B_{2,c,i}^{\langle t\rangle} \in \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle)$ are compatible under the trace maps $\Lambda_{i+1}(\mathbb{Z}/l^{i+1}\mathbb{Z}\langle t\rangle) \to \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle)$, and therefore we can define the measure

$$B_{2,c}^{\langle t\rangle} := \varprojlim_i B_{2,c,i}^{\langle t\rangle} \in \Lambda(\mathbb{Z}_l\langle t\rangle).$$

3.3.4. A sheafified moment map for $\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle$ and $\mathbb{Z}_l\langle t\rangle$

For the torsor $\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle$ over $Y(l)$ defined in (3.3) we are given a section:

Lemma 3.3.11. *There exists a map of schemes $\sigma_{i,t} : \mathbb{Z}/l^i\mathbb{Z}\langle t\rangle \to \mathbb{Z}/l^i\mathbb{Z}$ over $Y(l)$. In particular it may be interpreted as a global section*

$$\sigma_{i,t} \in H^0(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle, q_{i,t}^*\mathbb{Z}/l^i\mathbb{Z}),$$

where $\mathbb{Z}/l^i\mathbb{Z} \in \mathrm{Sh}(Y(l))$ is the constant sheaf associated to the constant group scheme $\mathbb{Z}/l^i\mathbb{Z}$ over $Y(l)$, and $q_{i,t}$ is the structure morphism $\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle \to Y(l)$.

Proof. By the exactness of the short exact sequence of finite étale group schemes defining the torsor $\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle$, the N-multiplication map $[N] : \mathbb{Z}/l^iN\mathbb{Z} \to \mathbb{Z}/l^iN\mathbb{Z}$ factors through $\mathbb{Z}/l^i\mathbb{Z}$, leading to the map of schemes

$$\sigma_{i,t} : \mathbb{Z}/l^i\mathbb{Z}\langle t\rangle \to \mathbb{Z}/l^iN\mathbb{Z} \to \mathbb{Z}/l^i\mathbb{Z}$$

over $Y(l)$. Hence we get the desired global section $\sigma_{i,t} \in H^0(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle, q_{i,t}^*\mathbb{Z}/l^i\mathbb{Z})$. □

Definition 3.3.12. Let

$$\sigma_{i,t}^{[k]} \in H^0(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle, q_{i,t}^* \operatorname{TSym}^k \mathbb{Z}/l^i\,\mathbb{Z})$$

be the k-th tensor power of the section $\sigma_{i,t}$ defined in 3.3.11.

Notice that $\sigma_{i,t}^{[k]}$ can be seen as a map of sheaves

$$\sigma_{i,t}^{[k]} : \mathbb{Z}/l^i\,\mathbb{Z} \to q_{i,t*}q_{i,t}^*\,\mathbb{Z}/l^i\,\mathbb{Z}\,.$$

We will use the section $\sigma_{i,t}^{[k]}$ to construct a sheaf version of the analytic moment map defined in 3.3.8. In order to do so, we first need to write down a technical lemma.

Lemma 3.3.13. *Let $\mathscr{F},\mathscr{G} \in \operatorname{Sh}(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle)$. Then, for the finite étale morphism $q_{i,t}$: $\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle \to Y(l)$, we have a morphism of sheaves*

$$\gamma : q_{i,t*}\mathscr{F} \otimes q_{i,t*}\mathscr{G} \to q_{i,t*}(\mathscr{F} \otimes \mathscr{G}).$$

Proof. By finiteness of $q_{i,t}$, we have that[7] $q_{i,t*} = q_{i,t!}$. By using the projection formula[8], we get the isomorphism

$$q_{i,t!}\mathscr{F} \otimes q_{i,t*}\mathscr{G} \cong q_{i,t*}(\mathscr{F} \otimes q_{i,t}^*q_{i,t*}\mathscr{G}).$$

Using the adjunction[9] between $q_{i,t!}$ and $q_{i,t}^*$, we then obtain a map

$$q_{i,t*}(\mathscr{F} \otimes q_{i,t}^*q_{i,t*}\mathscr{G}) \to q_{i,t*}(\mathscr{F} \otimes \mathscr{G}).$$

□

We have now all the ingredients to define a sheaf version of the analytic moment map.

Definition 3.3.14. Define the *i-th cyclotomic sheafified moment map*

$$\operatorname{mom}_{i,t}^k : \Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle) \to \operatorname{TSym}^k \mathbb{Z}/l^i\,\mathbb{Z} \cong \mathbb{Z}/l^i\,\mathbb{Z}$$

as the composition $\operatorname{tr}_{q_{i,t}} \circ \gamma \circ (\operatorname{id} \otimes \sigma_{i,t}^{[k]})$, i.e.

$$\operatorname{mom}_{i,t}^k : \Lambda_i(\mathbb{Z}/l^i\,\mathbb{Z}\langle t\rangle) := q_{i,t*}\,\mathbb{Z}/l^i\,\mathbb{Z} \overset{\operatorname{id}\otimes\sigma_{i,t}^{[k]}}{\to} q_{i,t*}\,\mathbb{Z}/l^i\,\mathbb{Z} \otimes_{\mathbb{Z}/l^i\,\mathbb{Z}} q_{i,t*}q_{i,t}^*\,\mathbb{Z}/l^i\,\mathbb{Z} \overset{\gamma}{\to}$$
$$q_{i,t*}(\mathbb{Z}/l^i\,\mathbb{Z} \otimes q_{i,t}^*\,\mathbb{Z}/l^i\,\mathbb{Z}) \cong q_{i,t*}q_{i,t}^*\,\mathbb{Z}/l^i\,\mathbb{Z} \overset{\operatorname{tr}_{q_{i,t}}}{\to} \mathbb{Z}/l^i\,\mathbb{Z},$$

where $\operatorname{tr}_{q_{i,t}}$ is the trace map $q_{i,t*}q_{i,t}^* \to \operatorname{id}$ given by the adjunction $q_{i,t!} = q_{i,t*} \rightleftharpoons q_{i,t}^*$ (see [Aut] 59.66.1).

[7] see [Aut] 59.70.7.
[8] see for example [Mil04] 22.7.
[9] see for example [Aut] 59.66.

Moreover, by compatibility of $\mathrm{mom}^k_{i,t}$ with respect to the trace map $\Lambda_{i+1}(\mathbb{Z}/l^{i+1}\mathbb{Z}\langle t\rangle) \to \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle)$, we define the *cyclotomic sheafified moment map* as the inverse limit

$$\mathrm{mom}^k_t := \varprojlim_i \mathrm{mom}^k_{i,t} : \Lambda(\mathbb{Z}_l\langle t\rangle) \to \mathrm{TSym}^k \mathbb{Z}_l\,.$$

They induce on cohomology the morphisms

$$\mathrm{mom}^k_{i,t} : H^1(Y(l), \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle) \to H^1(Y(l), \mathbb{Z}/l^i\mathbb{Z})$$

and

$$\mathrm{mom}^k_t : H^1(Y(l), \Lambda(\mathbb{Z}_l\langle t\rangle)) \to H^1(Y(l), \mathbb{Z}_l).$$

Let us notice that, on stalks, the cyclotomic sheafified moment map coincides with the analytic one constructed in 3.3.8, for details we refer to [Kin15] Lemma 12.2.14.

3.4. Elliptic Soulé elements and the elliptic moment maps

Consider the short exact sequence of finite étale group schemes over $Y(l)$

$$0 \to \mathcal{E}[l^i] \to \mathcal{E}[l^iN] \to \mathcal{E}[N] \to 0, \tag{3.4}$$

where $\pi : \mathcal{E} \to Y(l)$ is the universal elliptic curve defined in 3.1.

For every N-torsion section $t \in \mathcal{E}[N](Y(l))$, define the $\mathcal{E}[l^i]$-torsor $\mathcal{E}[l^i]\langle t\rangle$ by the cartesian diagram

$$\begin{tikzcd} \mathcal{E}[l^i]\langle t\rangle \arrow[r] \arrow[d, "p_{i,t}"'] & \mathcal{E}[l^iN] \arrow[d] \\ Y(l) \arrow[r, "t"] & \mathcal{E}[N]. \end{tikzcd}$$

and define $\mathcal{E}\langle t\rangle$ to be the inverse limit

$$\mathcal{E}\langle t\rangle := \varprojlim_i \mathcal{E}[l^i]\langle t\rangle.$$

Let $\mathscr{H}_i, \mathscr{H}_i\langle t\rangle$ and $\mathscr{H}\langle t\rangle \in \mathrm{Sh}(Y(l))$ be the sheaves associated to $\mathcal{E}[l^i]$,$\mathcal{E}[l^i]\langle t\rangle$ and $\mathcal{E}\langle t\rangle$, and $\Lambda_i(\mathscr{H}_i), \Lambda_i(\mathscr{H}_i\langle t\rangle)$ and $\Lambda(\mathscr{H}\langle t\rangle) \in \mathrm{Sh}(Y(l))$ the sheaves defined in 3.3.4.

Using the fact that the map $p_{i,t}$ is finite, we have the following identification:

Lemma 3.4.1. *For the $\mathcal{E}[l^i]$- torsor $p_{i,t} : \mathcal{E}[l^i]\langle t\rangle \to Y(l)$ above, we have a canonical isomorphism*

$$H^1(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i}) \cong H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)).$$

Proof. Let us consider the Leray spectral sequence associated to $p_{i,t} : \mathcal{E}[l^i]\langle t\rangle \to Y(l)$ and $\mu_{l^i} \in \mathrm{Sh}(\mathcal{E}[l^i]\langle t\rangle)$, i.e.

$$E_2^{p,q} = H^p(Y(l), R^q p_{i,t*}\mu_{l^i}) \Rightarrow H^n(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i}).$$

Since the morphism $p_{i,t}$ is finite, then, by A.3.7, we have that

$$E_2^{p,q} = H^p(Y(l), R^q p_{i,t*}\mu_{l^i}) = 0 \text{ for every } q > 0.$$

Hence, by A.3.8,

$$E_2^{1,0} = H^1(Y(l), p_{i,t*}\mu_{l^i}) \cong H^1(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i}) = E^1,$$

where, by definition, $p_{i,t*}\mu_{l^i} \cong \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)$. □

We can construct a section for the torsor $\mathcal{E}[l^i]\langle t\rangle$ defined above.

Lemma 3.4.2. *There exists a map of schemes $\tau_{i,t} : \mathcal{E}[l^i]\langle t\rangle \to \mathcal{E}[l^i]$. In particular, it may be interpreted as a global section*

$$\tau_{i,t} \in H^0(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^*\mathscr{H}_i).$$

Proof. By the exactness of the short exact sequence (3.4), we get that the N-multiplication map $[N] : \mathcal{E}[l^iN] \to \mathcal{E}[l^iN]$ factors through $\mathcal{E}[l^i]$. Hence we obtain a map of schemes over $Y(l)$

$$\tau_{i,t} : \mathcal{E}[l^i]\langle t\rangle \to \mathcal{E}[l^iN] \to \mathcal{E}[l^i]$$

and so we obtain a global section

$$\tau_{i,t} \in H^0(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^*\mathscr{H}_i).$$

□

Definition 3.4.3. Let

$$\tau_{i,t}^{[k]} \in H^0(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i)$$

be the k-th tensor power of the section $\tau_{i,t}$ defined in 3.4.2.

Remark 3.4.4. The section $\tau_{i,t}^{[k]}$ can be seen as a map of sheaves

$$\tau_{i,t}^{[k]} : \mathbb{Z}/l^i\,\mathbb{Z} \to p_{i,t*}p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i$$

over $Y(l)$.

The section $\tau_{i,t}^{[k]}$ can be used to construct a sheafified moment map in the elliptic curve case, analogously to the cyclotomic case. Lemma 3.3.13 holds indeed also for sheaves $\mathscr{F}, \mathscr{G} \in \operatorname{Sh}(\mathcal{E}[l^i]\langle t\rangle)$ and the finite morphism $p_{i,t} : \mathcal{E}[l^i]\langle t\rangle \to Y(l)$.

Therefore we can define a sheafified moment map for elliptic curves.

Definition 3.4.5. Let us define the *i-th elliptic sheafified moment map*

$$\underline{\operatorname{mom}}_{i,t}^k : \Lambda_i(\mathscr{H}_i\langle t\rangle) \to \operatorname{TSym}^k \mathscr{H}_i$$

as the composition $\mathrm{tr}_{p_{i,t}} \circ \gamma \circ (\mathrm{id} \otimes \tau_{i,t}^{[k]})$, i.e.

$$\underline{\mathrm{mom}}_{i,t}^k : \Lambda_i(\mathscr{H}_i\langle t\rangle) := p_{i,t*}\,\mathbb{Z}/l^i\,\mathbb{Z} \overset{id\otimes\tau_{i,t}^{[k]}}{\to} p_{i,t*}\,\mathbb{Z}/l^i\,\mathbb{Z} \otimes_{\mathbb{Z}/l^i\,\mathbb{Z}} p_{i,t*}p_{i,t}^* \,\mathrm{TSym}^k\,\mathscr{H}_i \overset{\gamma}{\to}$$
$$p_{i,t*}(\mathbb{Z}/l^i\,\mathbb{Z} \otimes p_{i,t}^*\,\mathrm{TSym}^k\,\mathscr{H}_i) \cong p_{i,t*}p_{i,t}^*\,\mathrm{TSym}^k\,\mathscr{H}_i \overset{\mathrm{tr}_{p_{i,t}}}{\to} \mathrm{TSym}^k\,\mathscr{H}_i$$

where $\mathrm{tr}_{p_{i,t}}$ is the trace map $p_{i,t*}p_{i,t}^* \to \mathrm{id}$ given by the adjunction $p_{i,t!} = p_{i,t*} \rightleftharpoons p_{i,t}^*$. Moreover, by compatibility of $\underline{\mathrm{mom}}_{i,t}^k$ with respect to the trace maps $\Lambda_{i+1}(\mathscr{H}_{i+1}\langle t\rangle) \to \Lambda_i(\mathscr{H}_i\langle t\rangle)$, we define the *elliptic sheafified moment map* as the inverse limit

$$\underline{\mathrm{mom}}_t^k := \varprojlim_i \underline{\mathrm{mom}}_{i,t}^k : \Lambda(\mathscr{H}\langle t\rangle) \to \mathrm{TSym}^k\,\mathscr{H}.$$

They induce on cohomology the morphisms

$$\underline{\mathrm{mom}}_{i,t}^k : H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)) \to H^1(Y(l), \mathrm{TSym}^k\,\mathscr{H}_i(1))$$

and

$$\underline{\mathrm{mom}}_t^k : H^1(Y(l), \Lambda(\mathscr{H}\langle t\rangle)(1)) \to H^1(Y(l), \mathrm{TSym}^k\,\mathscr{H}(1)).$$

3.4.1. Elliptic Soulé elements and their twists

The following theorem by Kato provides us with norm-compatible elliptic units on elliptic curves.

Theorem 3.4.6 ([Kat04] 1.10)**.** *Let $c > 1$ be an integer such that $(c, 6lN) = 1$ and let $E \to Y(l)$ be an elliptic curve. Then there exists a unique unit*

$${}_c\vartheta_E \in \mathcal{O}(E \smallsetminus E[c])^\times$$

such that:

1. $\mathrm{div}\,{}_c\vartheta_E = c^2(0) - E[c]$, *where* (0) *and* $\mathcal{E}[c]$ *are considered as Cartier divisors on* E*;*
2. $[d]_*{}_c\vartheta_E = {}_c\vartheta_E$ *for every* $(d, 6c) = 1$*;*
3. *for every isogeny of elliptic curves* $\varphi : E \to E'$ *such that* $(\deg\varphi, c) = 1$*, we have* $\varphi_*({}_c\vartheta_E) = {}_c\vartheta_{E'}$*;*
4. *for* $\tau \in \mathcal{H} = \{x \in \mathbb{C} \mid \mathrm{Im}\,x > 0\}$ *and* $z \in \mathbb{C} \smallsetminus c^{-1}(\mathbb{Z}\tau + \mathbb{Z})$*, denote by* ${}_c\vartheta(\tau, z)$ *the value at* z *of* ${}_c\vartheta$ *for the elliptic curve* $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ *over* $\mathbb{C}$*. Then*

$${}_c\vartheta(\tau, z) = q_\tau^{(c^2-1)/12}(-q_z)^{(c-c^2)/2}\frac{(1-q_z)^{c^2}}{1-q_z^c}\tilde{\gamma}_{q_\tau}(q_z)^{c^2}\tilde{\gamma}_{q_\tau}(q_z^c)^{-1},$$

where $q_\tau := e^{2\pi i\tau}$*,* $q_z := e^{2\pi i z}$ *and*

$$\tilde{\gamma}_{q_\tau}(q_z) = \prod_{n\geqslant 1}(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1}).$$

Hence, for the universal elliptic curve $\pi : \mathcal{E} \to Y(l)$ defined in 3.1, Theorem 3.4.6 gives us the function, called *Kato's elliptic unit*,

$$_c\vartheta_{\mathcal{E}} : \mathcal{E} \smallsetminus \mathcal{E}[c] \to \mathbb{G}_m$$

that is norm compatible, i.e. $[l^i]_*({}_c\vartheta_{\mathcal{E}}) = {}_c\vartheta_{\mathcal{E}}$, and such that, for a section $t \neq e$ as in (3.4), ${}_c\vartheta_{\mathcal{E}}$ is an invertible function on $\mathcal{E}[l^i]\langle t\rangle$[10].

We use now Kato's elliptic unit to define the following elements.

Definition 3.4.7. Let us define the *i-th elliptic Soulé element* by

$$\mathcal{ES}_{c,i}^{\langle t\rangle} := \partial_i({}_c\vartheta_{\mathcal{E}}) \in H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)),$$

where $\partial_i : \mathbb{G}_m(\mathcal{E}[l^i]\langle t\rangle) \to H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1))$ is the Kummer map[11] and where we used the identification in 3.4.1.

Define the *elliptic Soulé element* as the inverse limit

$$\mathcal{ES}_{c}^{\langle t\rangle} := \varprojlim_i \mathcal{ES}_{c,i}^{\langle t\rangle} \in H^1(Y(l), \Lambda(\mathscr{H}\langle t\rangle)(1)).$$

By using the section $\tau_{i,t}^{[k]}$, constructed in 3.4.3, we can twist the i-th elliptic Soulé element $\mathcal{ES}_{c,i}^{\langle t\rangle}$ defined above, in order to construct elements that belong to a twisted Galois representation.

Definition 3.4.8. Let us define the *i-th twisted elliptic Soulé element* by

$${}_ce_{k,i}(t) := (\mathrm{tr}_{p_{i,t}} \circ p_{i,t*})(\mathcal{ES}_{c,i}^{\langle t\rangle} \cup \tau_{i,t}^{[k]}) \in H^1(Y(l), \mathrm{TSym}^k \mathscr{H}_i(1))$$

and the *twisted elliptic Soulé element*[12] as the inverse limit

$${}_ce_k(t) := \varprojlim_i {}_ce_{k,i}(t) \in H^1(Y(l), \mathrm{TSym}^k \mathscr{H}(1)).$$

The twisted elliptic Soulé element is related to the elliptic Soulé element via the elliptic sheafified moment map.

Lemma 3.4.9. *We have*

$$\underline{\mathrm{mom}}_{i,t}^k(\mathcal{ES}_{c,i}^{\langle t\rangle}) = {}_ce_{k,i}(t)$$

and

$$\underline{\mathrm{mom}}_{t}^k(\mathcal{ES}_{c}^{\langle t\rangle}) = {}_ce_{k}(t).$$

[10] Indeed, since $(c, 6lN) = 1$, we have $\mathcal{E}[l^i]\langle t\rangle \subseteq \mathcal{E} \smallsetminus \mathcal{E}[c]$.

[11] i.e. $\partial_i : H^0(\mathcal{E}[l^i]\langle t\rangle, \mathbb{G}_m) \to H^1(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i})$ is the connecting morphism of the long exact sequence given by $\Gamma(\mathcal{E}[l^i]\langle t\rangle, \cdot)$ applied to the short exact sequence

$$0 \to \mu_{l^i} \to \mathbb{G}_m \to \mathbb{G}_m \to 0$$

of sheaves on $\mathcal{E}[l^i]\langle t\rangle$.

[12] Note that both the elliptic Soulé element $\mathcal{ES}_c^{\langle t\rangle}$ and the twisted elliptic Soulé element ${}_ce_k(t)$ can be defined over any scheme S such that E is an elliptic curve over it.

Proof. By the isomorphism $H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)) \cong H^1(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i})$ described in 3.4.1 and by using a similar argument to get the isomorphism $H^0(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i) \cong H^0(Y(l), p_{i,t*}p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i)$, we conclude by using the following commutative diagram

$$\begin{tikzcd} H^1(\mathcal{E}[l^i]\langle t\rangle, \mu_{l^i}) \otimes H^0(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i)) \arrow[r, "\cup"] \arrow[d, "\cong"] & H^1(\mathcal{E}[l^i]\langle t\rangle, p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i(1)) \arrow[d, "p_{i,t*}"] \\ H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle(1)) \otimes H^0(Y(l), p_{i,t*}p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i) \arrow[r, "\cup"] & H^1(Y(l), p_{i,t*}p_{i,t}^* \operatorname{TSym}^k \mathscr{H}_i(1)). \end{tikzcd}$$

□

REMARK 3.4.10 ([Kin15] 12.3.13). We have ${}_c e_{k,i}(-t) = (-1)^k {}_c e_{k,i}(t)$.

3.5. Residue at the cusp ∞

Let us recall, from 3.1, the open immersion $j : Y(l) \to X(l)$ and the closed immersion $\infty : \operatorname{Spec} \mathbb{Q}(\mu_l) \to X(l)$.

The goal of this section is to define a residue map at the cusp ∞. First, we need a technical remark.

REMARK 3.5.1. For $\mathbb{Z}/l^i\mathbb{Z}(1) \in \operatorname{Sh}(Y(l))$, by [Mil13] 16.11, we have that

$$R^q j_* \mathbb{Z}/l^i\mathbb{Z}(1) = \begin{cases} \mathbb{Z}/l^i\mathbb{Z}(1) & q = 0 \\ \infty_* \mathbb{Z}/l^i\mathbb{Z} & q = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Hence we obtain that

$$\infty^* R^1 j_* \mathbb{Z}/l^i\mathbb{Z}(1) \cong \mathbb{Z}/l^i\mathbb{Z} \quad \text{and} \quad R^2 j_* \mathbb{Z}/l^i\mathbb{Z}(1) = 0.$$

Let us now consider the Leray spectral sequence for the open immersion $j : Y(l) \to X(l)$ and the sheaf $\operatorname{TSym}^{k-2} \mathscr{H}_i(1) \in \operatorname{Sh}(Y(l))$, i.e.

$$E_2^{p,q} = H^p(X(l), R^q j_* \operatorname{TSym}^{k-2} \mathscr{H}_i(1)) \Rightarrow H^n(Y(l), \operatorname{TSym}^{k-2} \mathscr{H}_i(1))$$

and its 1-edge morphism

$$\underline{\operatorname{res}}_i : H^1(Y(l), \operatorname{TSym}^{k-2} \mathscr{H}_i(1)) \to H^0(X(l), R^1 j_* \operatorname{TSym}^{k-2} \mathscr{H}_i(1)).$$

DEFINITION 3.5.2. The *i-th residue morphism at* ∞ is given by the composition

$$\underline{\operatorname{res}}_{i,\infty} := \infty^* \circ \underline{\operatorname{res}}_i : H^1(Y(l), \operatorname{TSym}^{k-2} \mathscr{H}_i(1)) \to H^0(\operatorname{Spec} \mathbb{Q}(\mu_l), \mathbb{Z}/l^i\mathbb{Z}) \cong \mathbb{Z}/l^i\mathbb{Z},$$

as $\infty^* R^1 j_* \operatorname{TSym}^{k-2} \mathscr{H}_i(1) \cong \mathbb{Z}/l^i\mathbb{Z}$ by [Kin15] 12.5.4.
The *residue morphism at* ∞ is given by the inverse limit

$$\underline{\operatorname{res}}_\infty := \varprojlim_i \underline{\operatorname{res}}_{i,\infty} : H^1(Y(l), \operatorname{TSym}^{k-2} \mathscr{H}(1)) \to H^0(\operatorname{Spec} \mathbb{Q}(\mu_l), \mathbb{Z}_l) \cong \mathbb{Z}_l\,.$$

3.5.1. Compatibility of residue and moment morphisms

Let us now consider the following commutative diagram, made by combining the diagrams in 3.4 and 3.3.2 defining respectively the torsors $\mathcal{E}[l^i]\langle t\rangle$ and $\mathbb{Z}/l^i\mathbb{Z}\langle t\rangle$.

$$\begin{tikzcd}
& & & & \mathcal{E}[l^i]\langle t\rangle \arrow[r,"\alpha_i"] \arrow[dll] \arrow[dd,"p_{i,t}"] & \mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle \arrow[dll] \arrow[dd,"q_{i,t}"] \\
0 \arrow[r] & \mu_{l^iN} \arrow[r] & \mathcal{E}[l^iN] \arrow[r,"a_i"] \arrow[dd] & \mathbb{Z}/l^iN\mathbb{Z} \arrow[r] \arrow[dd] & 0 & \\
& & & & Y(l) \arrow[r, equal] \arrow[dll,"t"] & Y(l) \arrow[dll,"\alpha(t)"] \\
& & \mathcal{E}[N] \arrow[r,"\alpha"] & \mathbb{Z}/N\mathbb{Z} & &
\end{tikzcd}$$

where $a_i : \mathcal{E}[l^iN] \to \mathbb{Z}/l^iN\mathbb{Z}$ induces a finite morphism of schemes

$$\alpha_i : \mathcal{E}[l^i]\langle t\rangle \to \mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle$$

over $Y(l)$. We then get a finite morphism

$$\alpha_{i!} : \Lambda_i(\mathscr{H}_i\langle t\rangle) \to \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle)$$

of sheaves over $Y(l)$.

In this setting, we can now define another residue map at the cusp ∞.

Definition 3.5.3. Let us consider the Leray spectral sequence for the open immersion $j : Y(l) \to X(l)$ and the sheaf $\Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle)(1) \in \mathrm{Sh}(Y(l))$, i.e.

$$H^p(X(l), R^qj_*\Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle)(1)) \Rightarrow H^n(Y(l), \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle)(1)). \tag{3.5}$$

Define the *i-th cyclotomic residue morphism at ∞* by

$$\begin{aligned}\mathrm{res}_{i,\infty} : H^1(Y(l), \Lambda_i(\mathscr{H}_i\langle t\rangle)(1)) &\xrightarrow{\alpha_i} H^1(Y(l), \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle)(1)) \to \\ &\to H^0(\operatorname{Spec}\mathbb{Q}(\mu_l), \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle) \cong \Lambda_i(\mathbb{Z}/l^i\mathbb{Z}\langle\alpha(t)\rangle),\end{aligned}$$

where the last map is given by the composition of the pullback via the closed immersion ∞ and the 1-edge morphism in the spectral sequence (3.5). Define the *cyclotomic residue morphism at ∞* to be the inverse limit

$$\mathrm{res}_\infty := \varprojlim \mathrm{res}_{i,\infty} : H^1(Y(l), \Lambda(\mathscr{H}\langle t\rangle)(1)) \to H^0(\operatorname{Spec}\mathbb{Q}(\mu_l), \Lambda(\mathbb{Z}_l\langle\alpha(t)\rangle) \cong \Lambda(\mathbb{Z}_l\langle\alpha(t)\rangle).$$

The cyclotomic residue morphism and the residue morphism defined in 3.5.2 are compatible with the cyclotomic and elliptic sheafified moment maps defined in 3.3.14 and 3.4.5.

Proposition 3.5.4. *There exists a commutative diagram*

$$\begin{tikzcd} H^1(Y(l),\Lambda(\mathscr{H}\langle t\rangle)(1)) \arrow[r, "\mathrm{res}_\infty"] \arrow[d, "\underline{\mathrm{mom}}_t^{k-2}"] & H^0(\operatorname{Spec}\mathbb{Q}(\mu_l),\Lambda(\mathbb{Z}_l\langle\alpha(t)\rangle)) \cong \Lambda(\mathbb{Z}_l\langle\alpha(t)\rangle) \arrow[d, "\mathrm{mom}_{\alpha(t)}^{k-2}"] \\ H^1(Y(l),\mathrm{TSym}^{k-2}\mathscr{H}(1)) \arrow[r, "\underline{\mathrm{res}}_\infty"] & H^0(\operatorname{Spec}\mathbb{Q}(\mu_l),\mathbb{Z}_l) \cong \mathbb{Z}_l\,. \end{tikzcd}$$

For further applications, we compute now the cyclotomic residue at the cusp ∞ of the elliptic Soulé element $\mathcal{ES}_c^{\langle t\rangle} \in H^1(Y(l),\Lambda(\mathscr{H}\langle t\rangle)(1))$ defined in 3.4.7.

Lemma 3.5.5 ([Kin15] 12.5.8)**.** *We have*[13]

$$\mathrm{res}_\infty(\mathcal{ES}_c^{\langle t\rangle}) = B_{2,c}^{\alpha(t)},$$

where $B_{2,c}^{\alpha(t)}$ *is the Bernoulli measure defined in 3.3.10.*

The proof of this lemma is rather technical and strongly relies on the explicit description of the elliptic units via the local parameter q. For details, we refer to [Kin15].

We conclude by giving the residue at the cusp ∞ of the twisted elliptic Soulé element ${}_ce_{k-2}(t) \in H^1(Y(l),\mathrm{TSym}^{k-2}\mathscr{H}(1))$ defined in 3.4.8.

Lemma 3.5.6 ([Kin15] 12.5.9)**.** *For* $t=(a,b)\in\mathcal{E}[l](Y(l))\smallsetminus\{e\}$ *and* $c\equiv 1$ *mod* l*, we have*

$$\underline{\mathrm{res}}_\infty({}_ce_{k-2}(t)) = \frac{l^{k-1}}{(k-2)!k}\frac{c^k-1}{c^{k-2}}B_k(\frac{a}{l}).$$

[13]Note that in [Kin15] 12.5.8, the result is proved for elements over the formal completion $\widehat{Y(l)}_\infty$ of the modular curve $Y(l)$. But, since the residue map $\mathrm{res}_\infty : H^1(Y(l),\mathrm{TSym}^{k-2}\mathscr{H}(1)) \to H^0(\operatorname{Spec}\mathbb{Q}(\mu_l),\mathbb{Z}_l)$ factors through $H^1(\widehat{Y(l)}_\infty,\mathrm{TSym}^{k-2}\mathscr{H}(1)) \to H^0(\operatorname{Spec}\mathbb{Q}(\mu_l),\mathbb{Z}_l)$, for convenience we state this result for $Y(l)$.

4. Ribet's Method

In this section we give an overview of Ribet's Method (see [Rib76]), explaining its origins and of what it consists.

4.1. Herbrand-Ribet Theorem

Let l be the odd prime defined in Section 3 and denote by A the ideal class group of the cyclotomic field $\mathbb{Q}(\mu_l)$. Define $C := A/A^l$ to be the maximal l-quotient of A, where $A^l = \{a^l \mid a \in A\}$[1]. Let

$$\chi : \mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q}) \to \mathbb{F}_l^* \text{ given by } \sigma \mapsto \chi(\sigma), \text{ for } \sigma(\zeta_l) = \zeta_l^{\chi(\sigma)},$$

be the cyclotomic character and note that it generates the character group of $\mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})$. Then, since the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on C factors through $\mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})$, by Maschke's Theorem ([FH04] 1.6), C can be canonically decomposed into χ-eigenspaces as

$$C = \bigoplus_{i \bmod l-1} C(\chi^i),$$

where each eigenspace $C(\chi^i)$ is given by

$$C(\chi^i) := \{c \in C \mid \sigma(c) = \chi^i(\sigma)(c) \text{ for every } \sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})\}.$$

Herbrand-Ribet Theorem relates special values of the Riemann ζ-function and the class group A of $\mathbb{Q}(\mu_l)$.

Theorem 4.1.1 (Herbrand-Ribet Theorem, [Rib76] 1.1)**.** *Define the Riemann ζ-function to be the analytic continuation to $\mathbb{C} \smallsetminus \{1\}$ of*

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s}, \qquad s \in \mathbb{C},\ Re(s) > 1$$

and let $4 \leqslant k \leqslant l-3$ be an even integer[2]*. Then*

$$l \mid \zeta(1-k) \text{ if and only if } C(\chi^{1-k}) \neq 0.$$

[1] Hence l divides the order of A if and only if its quotient C is not trivial.

[2] Notice that in the original statement in [Rib76] k is assumed to be bigger than 2, but, since in our work we will assume that $l \mid \zeta(1-k)$, where $\zeta(1-k) = -\frac{B_k}{k}$ and $B_2 = \frac{1}{6}$, it is enough to assume $k \geqslant 4$.

The necessary condition for the non-triviality of $C(\chi^{1-k})$ was proven by Herbrand in 1932 in [Her32] and involves classical Algebraic Number Theory. Nevertheless, the opposite implication turned out to be more involved and was proved only in 1976 by Ribet in [Rib76], for which he developed what it is now called "Ribet's Method". We will explain this method in the following with more details.
Herbrand-Ribet Theorem was further generalized by Mazur and Wiles in [MW84] as a consequence of the Iwasawa Main Conjecture for $\mathbb{Q}$, which they proved using a generalization of Ribet's Method.

Theorem 4.1.2 (Mazur-Wiles, [MW84])**.** *Let $4 \leqslant k \leqslant l-3$ be an even integer. Then the power of l dividing $\zeta(1-k)$ is exactly the power of l dividing the order of $C(\chi^{1-k})$.*

4.2. Ribet's Method

By "Ribet's Method" we mean the strategy that Ribet used to prove the sufficient condition of Theorem 4.1.1. Indeed, instead of proving directly the implication, he understood that introducing in the picture modular forms and their associated Galois representations would have proved the claim. An important step in the proof was realizing that the desired implication of Theorem 4.1.1 was equivalent to construct a certain unramified extension of $\mathbb{Q}(\mu_l)$. This latter statement was then generalized even further to a result involving unramified Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In this section we will firstly introduce these two other results and then briefly see how Ribet proved them.

4.2.1. Unramified extensions and unramified Galois representations in the case $l \mid \zeta(1-k)$

Under the assumption that the odd prime l divides $\zeta(1-k)$, showing that the χ^{1-k}-eigenspace $C(\chi^{1-k})$ of C is not trivial is equivalent to prove the existence of a non-trivial unramified Galois extension of $\mathbb{Q}(\mu_l)$, indeed:

Theorem 4.2.1 ([Rib76] 1.2)**.** *Let $l \mid \zeta(1-k)$. Then there exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_l)$ such that:*

1. *$E/\mathbb{Q}(\mu_l)$ is unramified;*
2. *$\mathrm{Gal}(E/\mathbb{Q}(\mu_l))$ is a non-zero abelian group of exponent l;*
3. *For any $\sigma \in Gal(E/\mathbb{Q})$ and any $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\mu_l))$, we have $\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau$.*

The equivalence between Theorem 4.1.1 and Theorem 4.2.1 strongly relies on the functoriality of the Artin symbol $\left[\frac{E/\mathbb{Q}(\mu_l)}{\cdot}\right] : A \to \mathrm{Gal}(E/\mathbb{Q}(\mu_l))$. More details can be found in [Rib76] and in [Sab22].

The powerful insight of Ribet's Method was the realization that, instead of proving the existence of such an unramified extension, it was sufficient to prove the existence of a specific unramified Galois representation.

Theorem 4.2.2 ([Rib76] 1.3)**.** *Let $l \mid \zeta(1-k)$. Then there exists a finite field $F \supseteq \mathbb{F}_l$ and a continuous Galois representation*

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

such that:

1. *ρ is unramified at every prime $p \neq l$ (i.e. $\rho\mid_{I_p}$ is the trivial representation, where I_p is the inertia group at p);*

2. *ρ is an extension of the 1-dimensional representation with character χ^{k-1} by the trivial 1-dimensional representation, i.e.*

$$\rho(\sigma) = \begin{pmatrix} 1 & b(\sigma) \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} \text{ for every } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q});$$

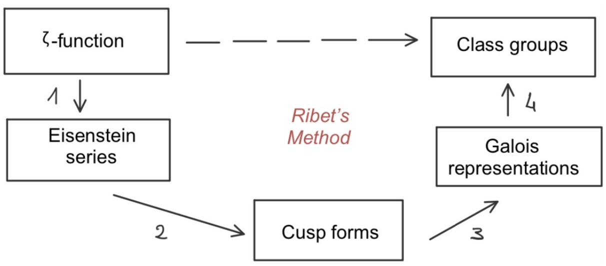
3. *ρ is not diagonalizable, i.e. b is not identically zero;*

4. *$\rho|_{D_l}$ is diagonalizable, i.e. $b(D_l) = 0$, where D_l is the decomposition group for l in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Such representation ρ can be constructed, thanks to [Shi94] and [Shi72], starting from cusp forms. Ribet's Method consists in the proof of Theorem 4.2.2. If we then consider $E := \overline{\mathbb{Q}}^{\ker \rho}$, the extension $E/\mathbb{Q}$ satisfies Theorem 4.2.1.

4.2.2. Ribet's Method

Ribet's Method was developed to show how a divisibility of some special value of the Riemann ζ-function implies the non vanishing of class groups of cyclotomic fields. In order to do so, Ribet considered an Eisenstein series related to the ζ-value, from it he constructed a cusp form and then he associated it a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation satisfying Theorem 4.2.2. We will now give more details about each step of Ribet's Method, that is represented graphically below. All details can be found in [Rib76] and in [Sab22].



Step 1: ζ-function $\Rightarrow$ Eisenstein series. Consider the weight k modular form given by the Eisenstein series

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n \geqslant 1} \sum_{d \mid n} d^{k-1} q^n$$

on $\mathrm{SL}_2(\mathbb{Z})$. Notice that for $k = 4, 6$ we have respectively

$$E_4 = \frac{1}{240} + \cdots \text{ and } E_6 = -\frac{1}{504} + \cdots .$$

Step 2: Eisenstein series $\Rightarrow$ Cusp forms. For every even integer $k \geqslant 4$, there exists a modular form $g := (240E_4)^a(-540E_6)^b \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ of weight k, where $k = 4a + 6b$ for $a, b \geqslant 0$, with constant term equal to 1 and integers coefficients. With such a g, we can construct the cusp form

$$g' := E_k - \frac{\zeta(1-k)}{2} g \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})).$$

Notice that, by construction, it has zero constant term and that, by the assumption $l \mid \zeta(1-k)$,

$$g' \equiv E_k \bmod l.$$

By Deligne-Serre lifting theorem (see [Rib76] 3.5), there exists a cuspidal eigenform $f \in \mathcal{S}_k(\mathcal{O}_K)$ such that

$$f \equiv g' \equiv E_k \bmod \mathfrak{l},$$

where K is a number field generated by the coefficients of g' and $\mathfrak{l}$ a prime above l. By the congruence above, we deduce also that f is $\mathfrak{l}$-ordinary, i.e. $a_l(f)$ is a $\mathfrak{l}$-unit.

Step 3: Cusp forms $\Rightarrow$ Galois representations. To such a cuspidal $\mathfrak{l}$-ordinary eigenform f, see [Rib76] 3.7, we can associate a continuous Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_{\mathfrak{l}}) \text{ given by } \begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

that is irreducible (because f is cuspidal), unramified at every prime $p \neq l$ and such that $\rho|_{D_l}$ is diagonalizable (because f is $\mathfrak{l}$-ordinary). The representation ρ satisfies Theorem 4.2.2.

Step 4: Galois Representations $\Rightarrow$ Class groups. By construction of ρ, $E := \overline{\mathbb{Q}}^{\ker \rho}$ satisfies Theorem 4.2.1.

5. A cohomological version of Ribet's Method

The goal of this thesis is to give a cohomological version of Ribet's Method, in particular we want to "translate" this method cohomologically using étale cohomology of modular curves to construct an unramified extension satisfying Theorem 4.2.1. Let k be an even integer, $4 \leqslant k \leqslant l-3$, and assume for the rest of the thesis that $l \mid B_k$. The key idea to go from the world of Galois representations to the world of étale cohomology is using extension classes. Indeed, a Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l\,\mathbb{Z}) \text{ given by } \sigma \mapsto \begin{pmatrix} 1 & b(\sigma) \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix},$$

i.e. an extension of the 1-dimensional representation with character χ^{k-1} by the trivial 1-dimensional representation, gives rise to an element of the extension group

$$\mathrm{Ext}^1_{\mathbb{Q}}(\mathbb{Z}/l\,\mathbb{Z}(k-1), \mathbb{Z}/l\,\mathbb{Z}).$$

By duality this corresponds to an element in

$$\mathrm{Ext}^1_{\mathbb{Q}}(\mathbb{Z}/l\,\mathbb{Z}, \mathbb{Z}/l\,\mathbb{Z}(1-k)).$$

By definition of group cohomology, the extension group above is the first right derived functor

$$\mathrm{Ext}^1_{\mathbb{Q}}(\mathbb{Z}/l\,\mathbb{Z}, \mathbb{Z}/l\,\mathbb{Z}(1-k)) = R^1(\mathbb{Z}/l\,\mathbb{Z}(1-k) \mapsto (\mathbb{Z}/l\,\mathbb{Z}(1-k))^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}) = H^1_{\mathrm{Gal}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/l\,\mathbb{Z}(1-k)).$$

The following result gives us a comparison between Galois and étale cohomology:

Proposition 5.0.1 (A.4.1)**.** *For K a field, there exists an equivalence of categories*

$$\{\textit{étale sheaves on } \mathrm{Spec}\, K\} \leftrightarrow \left\{\mathrm{Gal}(\overline{K}/K) - \textit{modules}\right\}.$$

Hence we obtain that

$$H^1_{\mathrm{Gal}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/l\,\mathbb{Z}(1-k)) \cong H^1(\mathrm{Spec}\,\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(1-k)),$$

showing us that constructing a Galois representation ρ as in Theorem 4.2.2 is equivalent to construct a class in $H^1(\mathrm{Spec}\,\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(1-k))$ satisfying particular properties. In particular, due to the work of [HP92] and [MW84], it will be enough to construct a class in $H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2}\mathscr{H}(1))$ satisfying [HP92] Propositions 2 and 3 that will give rise to an extension satisfying Theorem 4.2.1.

5.1. Action of the Hecke algebra on cohomology of modular curves

Let us consider the level-l modular curve $Y(l)$ over $\operatorname{Spec}\mathbb{Q}(\mu_l)$ defined in 3.1 together with the open immersion $j : Y(l) \to X(l)$ and the closed immersion $\infty : \operatorname{Spec}\mathbb{Q}(\mu_l) \to X(l)$. For the cusp ∞, we define $Y_\infty := Y(l) \cup \{\infty\}$ and we still denote by j and ∞ the induced immersions.

For the Hecke algebra

$$H := \mathbb{Z}_l[T_2, T_3, \ldots, T_l, \ldots],$$

i.e. the $\mathbb{Z}_l$-algebra generated by the Hecke operators T_i (see Appendix A for a precise definition of these operators), define the *Eisenstein ideal* $I \subseteq H$ to be the kernel of the homomorphism

$$\varphi : H \to \mathbb{Z}_l \text{ given by } T_p \mapsto p^{k-1} + 1.$$

Let $m_{Eis} := (I, l) \in H$ be the maximal ideal generated by l and the Eisenstein ideal I and let H_{Eis} be the localisation of H at m_{Eis}. For any H-module M, we define the H_{Eis}-module $M_{Eis} := M \otimes_{\mathbb{Z}_l} H_{Eis}$. Finally, let $\overline{H}_{Eis}$ be the image of H into $\operatorname{End}_{\mathbb{Z}_l}(H^1(Y_\infty, \operatorname{TSym}^{k-2}\mathscr{H}(1))_{Eis})$ and I_{Eis} the image of the Eisenstein ideal I in $\overline{H}_{Eis}$.

5.1.1. A short exact sequence induced by the residue map at the cusp ∞

Let us define $Y(l)_{\overline{\mathbb{Q}}} := Y(l) \times_{\operatorname{Spec}\mathbb{Q}(\mu_l)} \operatorname{Spec}\overline{\mathbb{Q}}$ and $(Y_\infty)_{\overline{\mathbb{Q}}} := Y_\infty \times_{\operatorname{Spec}\mathbb{Q}(\mu_l)} \operatorname{Spec}\overline{\mathbb{Q}}$ to be the base change respectively of $Y(l)$ and Y_∞ to $\operatorname{Spec}\overline{\mathbb{Q}}$ and analogously define the base change $\infty_{\overline{\mathbb{Q}}}$. Denote by $j_{\overline{\mathbb{Q}}}$ and $\infty_{\overline{\mathbb{Q}}}$ the induced maps.

Consider the Leray spectral sequence for $Rj_{\overline{\mathbb{Q}}*}$ over $\operatorname{TSym}^{k-2}\mathscr{H}(1) \in \operatorname{Sh}(Y(l)_{\overline{\mathbb{Q}}})$, i.e.

$$E_2^{p,q} := H^p((Y_\infty)_{\overline{\mathbb{Q}}}, R^q j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \Rightarrow E^n := H^n(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1)). \quad (5.1)$$

Lemma 5.1.1. *The residue morphism at ∞, constructed in 3.5.2, induces a short exact sequence of $H \times \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules*

$$0 \to H^1((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \to H^1(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1)) \to \mathbb{Z}_l \to 0$$

Proof. Consider the exact sequence of low degree (see A.3.6) associated to the Leray spectral sequence in (5.1), i.e.

$$\begin{aligned} 0 \to H^1((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \to H^1(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1)) \to \\ H^0((Y_\infty)_{\overline{\mathbb{Q}}}, R^1 j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \to H^2((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)). \end{aligned}$$

For[1] $\operatorname{Cusp} = \operatorname{Cusp}_0 \cup \{\infty\}$, let us define $M^\sharp$ on $(Y_\infty)_{\overline{\mathbb{Q}}}$ to be the continuation of $\operatorname{TSym}^{k-2}\mathscr{H}(1)$ via $j_{\overline{\mathbb{Q}}!}$ at $\{\infty\}$ and via $j_{\overline{\mathbb{Q}}*}$ at Cusp_0. Then, by [Har93] p.114[2], we have the short exact sequence

$$0 \to j_{\overline{\mathbb{Q}}!}\operatorname{TSym}^{k-2}\mathscr{H}(1) \to M^\sharp \to Rj_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)|_{\operatorname{Cusp}_0} \to 0$$

[1] where Cusp_0 denotes all the cusps above the cusp zero.

[2] Note that we consider $\operatorname{TSym}^{k-2}\mathscr{H}(1)$ that is isomorphic to $M_{k-2}(k-1)$ of [Har93] and [HP92]. Moreover, the role of Cusp_0 and ∞ are inverted with respect to Σ_0 and Σ_∞ in [Har93].

that gives rise to the long exact sequence

$$\cdots \to H^2((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}!}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \to H^2((Y_\infty)_{\overline{\mathbb{Q}}}, M^\sharp) \to \\ H^2(\mathrm{Cusp}_0, Rj_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \to \cdots \tag{5.2}$$

For the left hand side, by Poincarè duality[3], we have

$$H^2((Y_\infty)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1)) \cong H^0_c((Y_\infty)_{\overline{\mathbb{Q}}}, (\operatorname{TSym}^{k-2}\mathscr{H}(1))^\vee(1))^\vee.$$

By considering the injective map

$$H^0_c((Y_\infty)_{\overline{\mathbb{Q}}}, (\operatorname{TSym}^{k-2}\mathscr{H}(1))^\vee(1)) \hookrightarrow H^0((Y_\infty)_{\overline{\mathbb{Q}}}, (\operatorname{TSym}^{k-2}\mathscr{H}(1))^\vee(1)),$$

where the right hand side vanishes because the local system has no global sections for $k > 2$, we deduce that $H^0_c((Y_\infty)_{\overline{\mathbb{Q}}}, (\operatorname{TSym}^{k-2}\mathscr{H}(1))^\vee(1))^\vee = 0$ and so also $H^2((Y_\infty)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1)) = 0$. For the right hand term in (5.2), by the fact that the sheaf $Rj_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)$ is not trivial only on[4] $\infty_{\overline{\mathbb{Q}}}$, we deduce that

$$H^2(\mathrm{Cusp}_0, Rj_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) = 0.$$

Therefore also $H^2((Y_\infty)_{\overline{\mathbb{Q}}}, M^\sharp) = 0$. By definition of $M^\sharp$ and the fact that $Rj_{\overline{\mathbb{Q}}!}$ is exact[5], we then deduce that

$$H^2((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) = 0.$$

Moreover, again by the fact that the sheaf $Rj_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)$ is not trivial only on $\infty_{\overline{\mathbb{Q}}}$, we deduce also that

$$H^0((Y_\infty)_{\overline{\mathbb{Q}}}, R^1j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \cong H^0(\infty_{\overline{\mathbb{Q}}}, \infty^*R^1j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1)) \cong \mathbb{Z}_l,$$

where the last isomorphism comes from $\infty^*_{\overline{\mathbb{Q}}}R^1j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1) \cong \mathbb{Z}_l$ by [Kin15] 12.5.4. □

After tensoring the short exact sequence in 5.1.1 with the localisation H_{Eis}, we obtain the exact sequence of $H_{Eis} \times \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules

$$H^1((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\operatorname{TSym}^{k-2}\mathscr{H}(1))_{Eis} \to H^1(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1))_{Eis} \to \mathbb{Z}_l \to 0. \tag{5.3}$$

5.2. Construction of a cusp class

To have an element analogous to the cusp form of Ribet's Method, we would like to construct a class in $H^1(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1))$ with a relation with the value of the Riemann ζ-function at $1-k$. This is done by using the residue at the cusp ∞ constructed in 3.5.2, that will play the role of the constant coefficient in the series expansion of the cusp form. In particular, we want to find a class $\alpha \in H^1(Y(l)_{\overline{\mathbb{Q}}}, \operatorname{TSym}^{k-2}\mathscr{H}(1))$ such that

$$\underline{\mathrm{res}}_\infty(\alpha) \equiv 0 \text{ modulo } l.$$

[3] [Mil80] VI 11.1.
[4] [Mil04] Proposition 16.11.
[5] see [Fu15] 5.5.1.

Definition 5.2.1. Define, for $t = (a, b) \in \mathcal{E}[l](Y(l)) \smallsetminus \{e\}$ and $c \equiv 1 \bmod l$, the *cusp class* to be

$$\alpha := f^* \left({}_c e_{k-2}(t) + \xi \frac{c^k - 1}{c^{k-2}} \frac{1}{(k-2)!(l-1)} \sum_{\mathbf{1} \neq \psi \bmod l} \overline{\chi}(a) L(1-k, \chi) \right) \in H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2} \mathscr{H}(1)),$$

for $\xi \in H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2} \mathscr{H}(1))$ such that $\underline{\mathrm{res}}_\infty(\xi) = 1$ and $f : Y(l)_{\overline{\mathbb{Q}}} \to Y(l)$ the map induced by the base change.

Then we have the following:

Lemma 5.2.2. *The image of the cusp class α via the residue morphism*

$$\underline{\mathrm{res}}_\infty : H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2} \mathscr{H}(1)) \to \mathbb{Z}_l$$

is given by

$$\underline{\mathrm{res}}_\infty(\alpha) = -\frac{c^k - 1}{c^{k-2}} \frac{1}{(k-2)!(l-1)} \zeta(1-k).$$

In particular, since $l \mid B_k$,

$$\underline{\mathrm{res}}_\infty(\alpha) \equiv 0 \ \mathit{mod}\ l.$$

Proof. By Lemma 3.5.6 and Definition 5.2.1, we have

$$\begin{aligned}
&\underline{\mathrm{res}}_\infty \left({}_c e_{k-2}(t) + \xi \frac{c^k - 1}{c^{k-2}} \frac{1}{(k-2)!(l-1)} \sum_{\mathbf{1} \neq \psi \bmod l} \overline{\chi}(a) L(1-k, \chi) \right) \\
&= \underline{\mathrm{res}}_\infty({}_c e_{k-2}(t)) + \underline{\mathrm{res}}_\infty(\xi) \frac{c^k - 1}{c^{k-2}} \frac{1}{(k-2)!(l-1)} \sum_{\mathbf{1} \neq \psi \bmod l} \overline{\chi}(a) L(1-k, \chi) \\
&= \frac{l^{k-1}}{k(k-2)!} \frac{c^k - 1}{c^{k-2}} B_k(\frac{a}{l}) + \frac{c^k - 1}{c^{k-2}} \frac{1}{(k-2)!(l-1)} \sum_{\mathbf{1} \neq \psi \bmod l} \overline{\chi}(a) L(1-k, \chi).
\end{aligned}$$

Let us consider the Hurwitz zeta function defined by the analytic continuation to $\mathbb{C} \smallsetminus \{1\}$ of

$$\zeta(s, a) = \sum_{n \geqslant 0} \frac{1}{(n+a)^s}, \text{ for } Re(s) > 1,\ a \neq 0, -1, -2, \ldots.$$

By the relation between the Hurwitz zeta function and the Bernoulli polynomials, we have that

$$B_k(\frac{a}{l}) = -k\zeta(1-k, \frac{a}{l}),$$

and, by the relation between the Hurwitz zeta function and the Dirichlet L-function, we have

$$\zeta(1-k, \frac{a}{l}) = \frac{l^{1-k}}{l-1} \sum_{\psi \bmod l} \overline{\chi}(a) L(1-k, \chi),$$

where ψ runs all over the Dirichlet characters modulo l. Therefore we obtain that

$$\frac{l^{k-1}}{k(k-2)!}\frac{c^k-1}{c^{k-2}}B_k(\frac{a}{l}) = -\frac{c^k-1}{c^{k-2}}\frac{1}{(k-2)!(l-1)}\sum_{\psi \bmod l}\overline{\chi}(a)L(1-k,\chi),$$

leading to

$$\underline{\mathrm{res}}_\infty\left({}_c e_{k-2}(t) + \xi\frac{c^k-1}{c^{k-2}}\frac{1}{(k-2)!(l-1)}\sum_{\mathbf{1}\neq\psi \bmod l}\overline{\chi}(a)L(1-k,\chi)\right) = -\frac{c^k-1}{c^{k-2}}\frac{1}{(k-2)!(l-1)}\zeta(1-k).$$

By base change, we then obtain

$$\underline{\mathrm{res}}_\infty(\alpha) = -\frac{c^k-1}{c^{k-2}}\frac{1}{(k-2)!(l-1)}\zeta(1-k).$$

In particular, since $l \mid B_k$ and so also $l \mid \zeta(1-k)$, we have $\underline{\mathrm{res}}_\infty(\alpha) \equiv 0$ modulo l. $\square$

5.3. A splitting short exact sequence induced by the residue

Let us define the $H_{Eis}\times\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules $X := \mathrm{Im}(H^1((Y_\infty)_{\overline{\mathbb{Q}}}, j_{\overline{\mathbb{Q}}*}\,\mathrm{TSym}^{k-2}\mathscr{H}(1))_{Eis} \to H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2}\mathscr{H}(1))_{Eis})$ and $Y := H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2}\mathscr{H}(1))_{Eis}$ so that the exact sequence constructed in (5.3) becomes

$$0 \to X \to Y \to \mathbb{Z}_l \to 0.$$

Then the $H_{Eis}\times\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module X satisfies the following Proposition:

Proposition 5.3.1 ([HP92] Satz 3). *Let τ denote the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation on X. Then:*

1. *τ is unramified outside l, i.e. $\tau|_{I_p} = \mathrm{id}$ for every prime $p \neq l$, where I_p is the inertia group at p;*
2. *There is an isomorphism of Galois modules[6] $Y/X \cong \mathbb{Z}_l$;*
3. *For $p \neq l$, let φ_p be the geometric Frobenius at p acting on $\mathbb{Z}_l(1)$ via multiplication by p^{-1}. Then $\mathrm{tr}(\tau(\varphi_p)) = T_p$ and $\det(\tau(\varphi_p)) = p^{k-1}$ and, for λ_l the eigenvalue of $\tau(\varphi_l)$ on this module, we have $\lambda_l + l^{k-1}/\lambda_l = T_l$;*
4. *The module $(X\otimes\mathbb{Q}_l)^{I_l}$ is free of rank 1 over $\overline{H}_{Eis}\otimes\mathbb{Q}_l$, where I_l is the inertia group at l;*

[6] Note that in this work we work with the sheaf $\mathrm{TSym}^{k-2}\mathscr{H}(1) \in \mathrm{Sh}(Y(l))$, where $\mathscr{H} := (R^1\pi_*\mathbb{Z}_l)^\vee$, while [HP92] use $M_{k-2} := \mathrm{TSym}^{k-2}R^1\pi_*\mathbb{Z}_l$. Hence the different twist in our statement of Satz 3 comes from the isomorphism $M_{k-2}(k-1) \cong \mathrm{TSym}^{k-2}\mathscr{H}(1)$. This isomorphism equips Y and X of an additional $(k-1)$-Hecke action compared to the one in [HP92], leading to the isomorphism above.

5. *For every direct summand K_l of $\overline{H}_{Eis} \otimes \mathbb{Q}_l$, the Galois representation on $X \otimes \mathbb{Q}_l$ is irreducible.*

Let us now consider the cusp class α defined in 5.2.1.

Proposition 5.3.2. *The cusp class $\alpha \in H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2} \mathscr{H}(1))$ gives rise to a splitting*

$$0 \to X \to X \oplus \alpha_{Eis} \mathbb{Z}_l \to \mathbb{Z}_l \to 0,$$

Proof. The proof follows immediately from Lemma 5.2.2, as we define α_{Eis} to be the image of α in $H^1(Y(l)_{\overline{\mathbb{Q}}}, \mathrm{TSym}^{k-2} \mathscr{H}(1))_{Eis}$. □

Let us notice that $X \oplus \alpha_{Eis} \mathbb{Z}_l$ is a submodule of Y, such that, by [HP92] §2,

$$Y/(X \oplus \alpha_{Eis} \mathbb{Z}_l) \cong \mathbb{Z}_l / l^\delta \mathbb{Z}_l \cong \mathbb{Z} / l^\delta \mathbb{Z},$$

where $l^\delta || \zeta(1-k)$. Therefore:

Proposition 5.3.3 ([HP92] Satz 4)**.** *There exists a $\overline{H}_{Eis} \times \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant embedding*

$$\mathbb{Z} / l^\delta \mathbb{Z} \hookrightarrow X / l^\delta X,$$

giving rise to the morphism

$$\varphi_\delta : \overline{H}_{Eis} \to \mathbb{Z} / l^\delta \mathbb{Z} \text{ given by } T_p \mapsto p^{k-1} + 1.$$

Such a structure on $\overline{H}_{Eis}$ gives rise to an unramified extension as in 4.2.1. We will outline the proof of this fact, due to [HP92] §3, in the next section.

5.3.1. Summary of the construction of an unramified extension

In this section we summarise the strategy used by Harder-Pink in [HP92] §3 to construct an unramified extension satisfying Theorem 4.2.1, starting from the results in the previous section.

The representation $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\overline{H}_{Eis}}(X)$ constructed in 5.3.1 gives rise to an infinite extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{GL}_{\overline{H}_{Eis}}(X)$, where we identify $\mathrm{Gal}(L/\mathbb{Q})$ with its image via this inclusion. We will use it to construct an extension satisfying Theorem 4.2.1.

Proposition 5.3.4 ([HP92] §3)**.** *There exists an extension $K_1/\mathbb{Q}$ that is non trivial and unramified over $\mathbb{Q}(\mu_l)$.*

Sketch of proof. From 5.3.1.3, we have that the homomorphism $\det : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (H_{Eis} \otimes \mathbb{Q}_l)^*$ induces a non-trivial homomorphism

$$\overline{\det} : \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z} / l \mathbb{Z})^*,$$

sending the complex conjugation σ_c to -1. Then we can write $\mathrm{Gal}(L/\mathbb{Q}) = G_1 \rtimes W$, for $G_1 := \ker \overline{\det}$ and $W \subseteq I_l$ the image of a section of $\overline{\det}$. W induces a decomposition

$X = X_- \oplus X_+$ into σ_c-eigenspaces, where, by 5.3.1.4, we have that $X_+ = X^{I_l} = X^W$ is such that $X_+ \otimes \mathbb{Q}_l$ is a rank one $\overline{H}_{Eis} \otimes \mathbb{Q}_l$-module and $X_- \otimes \mathbb{Q}_l$ is a free rank one $\overline{H}_{Eis} \otimes \mathbb{Q}_l$-module. Hence, for every $x \in X$, we can write $x = x_- + x_+$ and then we obtain an action of $\mathrm{Gal}(L/\mathbb{Q})$ on X described by

$$\sigma(x) = \tau(\sigma)\begin{pmatrix} x_- \\ x_+ \end{pmatrix} = \begin{pmatrix} a(\sigma)x_- + b(\sigma)x_+ \\ c(\sigma)x_- + d(\sigma)x_+ \end{pmatrix}, \text{ for } \sigma \in \mathrm{Gal}(L/\mathbb{Q}), x \in X,$$

where $a(\sigma) \in \mathrm{End}_{\overline{H}_{Eis}}(X_-)$ and $b(\sigma) \in \mathrm{Hom}_{\overline{H}_{Eis}}(X_+, X_-)$, and by

$$\begin{pmatrix} \chi_\infty^{k-1}(\sigma) & * \\ 0 & 1 \end{pmatrix} \text{ for } \sigma \in I_l,$$

where χ_∞ is the cyclotomic character $\mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q}) \to \mathbb{Z}_l^*$. By [HP92] 3.1.4 and 3.1.5, we have that the Eisenstein ideal I_{Eis} is generated by the elements $a(\sigma) - \det(\sigma)$ and $d(\sigma) - 1$ for σ varying in $\mathrm{Gal}(L/\mathbb{Q})$, hence, since $\overline{H}_{Eis} = \mathbb{Z}_l + I_{Eis}$, $\overline{H}_{Eis}$ is a $\mathbb{Z}_l$-algebra generated by the $a(\sigma), d(\sigma)$'s. Let now $B \subseteq \mathrm{Hom}_{\overline{H}_{Eis}}(X_+, X_-)$ and $C \subseteq \mathrm{Hom}_{\overline{H}_{Eis}}(X_-, X_+)$ be the $\overline{H}_{Eis}$-modules[7] generated by respectively the $b(\sigma)$'s and the $c(\sigma)$'s. Since, by [HP92] 3.1.4, for every $\sigma, \sigma' \in \mathrm{Gal}(L/\mathbb{Q})$ we have $b(\sigma)c(\sigma') \in I_{Eis}$, we may define $I' := BC \subseteq I_{Eis}$. Let us consider the homomorphism

$$\psi_1 : \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \mapsto \begin{pmatrix} \overline{a}(\sigma) & 0 \\ 0 & \overline{d}(\sigma) \end{pmatrix},$$

where $\overline{a}(\sigma), \overline{d}(\sigma) \in (\overline{H}_{Eis}/I')^*$. Let $\mathbb{Q}(\psi_1)$ be the extension of $\mathbb{Q}$ such that the morphism ψ_1 factors faithfully over $\mathrm{Gal}(\mathbb{Q}(\psi_1)/\mathbb{Q})$. As this extension is totally ramified only at l, we have a surjection $I_l \to \mathrm{Gal}(\mathbb{Q}(\psi_1)/\mathbb{Q})$ so that $a(\sigma) \equiv 1$ and $d(\sigma) \equiv \chi_\infty^{k-1}(\sigma)$ modulo I'. Therefore $I' := BC = I_{Eis}$ and we obtain a cyclotomic extension L_0 over $\mathbb{Q}$, generated by the homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/l^\delta\mathbb{Z})^* = (\overline{H}_{Eis}/I_{Eis})^*$. Let us now consider the homomorphism[8]

$$\psi_2 : \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \mapsto \begin{pmatrix} \overline{a}(\sigma) & \overline{b}(\sigma) \\ 0 & \overline{d}(\sigma) \end{pmatrix},$$

where $\overline{a}(\sigma), \overline{d}(\sigma) \in (\overline{H}_{Eis}/I')^*$ and $\overline{b}(\sigma) \in B/I_{Eis}B$. It defines an extension $K_1/\mathbb{Q}$ unramified over L_0 and such that

$$\mathrm{Gal}(K_1/L_0) \cong B/I_{Eis}B,$$

with $\mathrm{Gal}(L_0/\mathbb{Q})$ operating via χ_∞^{1-k} and where, via the theory of Fitting ideals and the fact that $\overline{H}_{Eis}/I_{Eis} = \mathbb{Z}/l^\delta\mathbb{Z}$, we have $l^\delta \mid \mathrm{ord}(B/I_{Eis}B)$. □

[7] By definition they are $\mathbb{Z}_l$-modules, but by [HP92] 3.1.6, they are indeed $\overline{H}_{Eis}$-modules.
[8] The map ψ_2 is an homomorphism by definition of I'.

5.4. A different cohomological approach

In this section we present a different cohomological approach to Ribet's Method. This approach did not lead us to the conclusion we were looking for, but, since it uses techniques that can be useful for further approaches, we include it in the present work.

As we have seen at the beginning of this chapter, to construct a Galois representation ρ as the one constructed in Theorem 4.2.2, it is enough to construct a cohomology class in[9] $H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$ satisfying the following equivalent properties:

	Galois representation (Ribet's method)	Galois cohomology
a)	$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l\,\mathbb{Z}),\ \sigma \mapsto \begin{pmatrix} 1 & b(\sigma) \\ 0 & \chi^{k-l}(\sigma) \end{pmatrix}$	$\tilde{D}_{l-k} \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$
b)	$b(\sigma) \not\equiv 0$	$\tilde{D}_{l-k} \neq 0$
c)	$\rho(I_p) = \mathbb{I}_2\ \forall p \neq l$ prime	$\tilde{D}_{l-k}\vert_{I_p} = 0\ \forall p \neq l$ prime
d)	$b(D_l) = 0$	$\tilde{D}_{l-k}\vert_{D_l} = 0$

Hence to prove that this cohomological approach holds, we would need to show that properties a) to d) hold in the Galois cohomology version. To do that, we first construct a class in étale cohomology and then, using Theorem 5.0.1, obtain a suitable class in $H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$.

5.4.1. Constructing an Eisenstein class

Let $n \geqslant 0$. To be analogous to the Eisenstein series of Ribet's Method, we would like to find a relation between some class in $H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1))$ and the value $\zeta(1-k)$. This is done by using the residue at the cusp ∞, that will play the role of the constant coefficient in the series expansion of the modular form.

Definition 5.4.1. For $c \equiv 1 \bmod l$ and $t = (a, b) \in \mathcal{E}[l](Y(l)) \smallsetminus \{e\}$, define the *Eisenstein class* to be

$$e'_n := {}_c e_{n,1}(t) - (\underline{\mathrm{res}}_\infty({}_c e_{n,1}(t)) - \zeta(1-k))\xi \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1)),$$

for $\xi \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1))$ such that $\underline{\mathrm{res}}_{1,\infty}(\xi) = 1$ and ${}_c e_{1,n}(t)$ the n-th twisted elliptic Soulé element defined in 3.4.8.

By its construction and by the running assumption $l \mid \zeta(1-k)$, we immediately deduce the following lemma.

Lemma 5.4.2. $\underline{\mathrm{res}}_{1,\infty}(e'_n) \equiv 0$ *modulo* l.

5.4.2. Constructing a cusp class

To construct the cusp class, we will use the class constructed in 5.4.1, whose residue at the cusp ∞ is zero, but we also need an auxiliary Eisenstein class.

[9] Note that $C(\chi^{1-k}) = C(\chi^{l-k})$ since $l - k \equiv 1 - k \bmod l - 1$.

An auxiliary class

The auxiliary class that we construct is defined analogously to the class ${}_ce_{n,1}(t)$ in 3.4.8.

Definition 5.4.3 ([Kin15] 12.6.3). Let us define an invertible function

$$\eta : \mathcal{E}[l]\langle t\rangle \to \mathbb{G}_m$$

given by

$$x \mapsto (q^{\frac{1}{l}})^{B^{\langle t\rangle}_{\alpha,2,c,1}(x)} = (q^{\frac{1}{l^2}})^{B^{\langle\alpha(t)\rangle}_{2,c,1}(\alpha(x))},$$

where the map

$$B^{\langle t\rangle}_{\alpha,2,c,1} : \mathcal{E}[l]\langle t\rangle \to \mathbb{Z}/l\,\mathbb{Z},$$

is defined by

$$x \mapsto \frac{l}{2}(c^2 B_2(\{\frac{\alpha_1(x)}{l^2}\}) - B_2(\{\frac{c\alpha_1(x)}{l^2}\}) = \frac{1}{l}B^{\langle\alpha(t)\rangle}_{2,c,1}(\alpha(x))$$

for $\{\cdot\}$ the representative of $\cdot \in \mathbb{R}/\mathbb{Z}$ in $[0,1[$ and where the last equality holds by definition of $B^{\langle\cdot\rangle}_{2,c,1}$ of 3.3.10. It gives rise to an element

$$B^{\langle t\rangle}_{\alpha,2,c,1} \in \Lambda_1(\mathscr{H}_1\langle t\rangle)$$

and so a global section

$$B^{\langle t\rangle}_{\alpha,2,c,1} \in H^0(Y(l), \Lambda_1(\mathscr{H}_1\langle t\rangle)).$$

Then we can define an auxiliary element (analogous to the elliptic Soulé element) as follows:

Lemma 5.4.4 ([Kin15] 12.6.3)**.** *For t a non-zero l-torsion section of $\mathcal{E}$ such that $\alpha(t) = 0$ and $c \equiv 1$ modulo l, define the auxiliary element*

$$\mathcal{GS}^{\langle t\rangle}_{c,1} := \partial(\eta) \in H^1(\mathcal{E}[l]\langle t\rangle, \mu_l),$$

where $\partial : \mathbb{G}_m(\mathcal{E}[l]\langle t\rangle) \to H^1(Y(l), \Lambda_1(\mathscr{H}_1\langle t\rangle)(1))$ is the Kummer map. Then $\mathcal{GS}^{\langle t\rangle}_{c,1}$ is given by the cup product

$$\mathcal{GS}^{\langle t\rangle}_{c,1} = \partial(q^{\frac{1}{l}}) \cup B^{\langle t\rangle}_{\alpha,2,c,1} \in H^1(Y(l), \Lambda_1(\mathscr{H}_1\langle t\rangle)(1)).$$

As with the elliptic Soulé element, we compute now the cyclotomic residue at the cusp ∞ of the auxiliary element.

Lemma 5.4.5 ([Kin15] 12.6.4)**.** *We have*

$$\mathrm{res}_{1,\infty}(\mathcal{GS}^{\langle t\rangle}_{c,1}) = B^{\langle\alpha(t)\rangle}_{2,c,1}.$$

Proof. The cyclotomic residue $\mathrm{res}_{1,\infty} : H^1(Y(l), \Lambda_1(\mathscr{H}_1\langle t\rangle)(1)) \to \Lambda_1(\mathbb{Z}/l\,\mathbb{Z}\langle\alpha(t)\rangle)$, defined in 3.5.3, factors, by definition, through $\alpha_{1!} : \Lambda_1(\mathscr{H}_1\langle t\rangle) \to \Lambda_1(\mathbb{Z}/l\,\mathbb{Z}\langle\alpha(t)\rangle)$. By definition of $B^{\langle t\rangle}_{\alpha,2,c,1}$, we have that

$$\alpha_{1!}B^{\langle t\rangle}_{\alpha,2,c,1} = lB^{\langle t\rangle}_{\alpha,2,c,1} = l\frac{1}{l}B^{\langle\alpha(t)\rangle}_{2,c,1},$$

hence

$$\mathrm{res}_{1,\infty}(\mathcal{GS}^{\langle t\rangle}_{c,1}) = \mathrm{res}_{1,\infty}(\partial(q^{\frac{1}{l}}) \cup B^{\langle t\rangle}_{\alpha,2,c,1}) = B^{\langle\alpha(t)\rangle}_{2,c,1}.$$

□

Analogously to the construction of the twisted elliptic Soulé element, the auxiliary class we are looking for is the image of the auxiliary element via the elliptic moment map:

Definition 5.4.6 ([Kin15] 12.6.5). Let

$$\underline{\mathrm{mom}}^n_{1,t} : H^1(Y(l), \Lambda_1(\mathscr{H}_1\langle t\rangle)(1)) \to H^1(Y(l), \mathrm{TSym}^n\,\mathscr{H}_1(1))$$

be the 1-th elliptic sheafified moment map defined in 3.4.5. Define the *auxiliary class* to be

$${}_cg_{n,1}(t) := \underline{\mathrm{mom}}^n_{1,t}(\mathcal{GS}^{\langle t\rangle}_{c,1}) \in H^1(Y(l), \mathrm{TSym}^n\,\mathscr{H}_1(1)).$$

We deduce therefore, by 5.4.5 and the compatibility in 3.5.4, that the residue at the cusp ∞ of the auxiliary class coincides with the residue at the cusp ∞ of the twisted elliptic Soulé element, i.e.

Proposition 5.4.7. *We have*

$$\underline{\mathrm{res}}_{1,\infty}({}_cg_{n,1}(t)) = \underline{\mathrm{res}}_{1,\infty}({}_ce_{n,1}(t)).$$

Due to its definition, the auxiliary class satisfies also a property relating the vanishing of its residue at the cusp ∞ with its own vanishing.

Proposition 5.4.8 ([Kin15] 12.6.6)**.** *Assume that* $\underline{\mathrm{res}}_{1,\infty}({}_cg_{n,1}(t)) = 0$. *Then*

$${}_cg_{n,1}(t) = 0.$$

Proof. By 5.4.4, we have that

$$\underline{\mathrm{mom}}^n_{1,t}(\mathcal{GS}^{\langle t\rangle}_{c,1}) = \partial(q^{\frac{1}{l}}) \cup \underline{\mathrm{mom}}^n_{1,t}(B^{\langle t\rangle}_{\alpha,2,c,1}),$$

where $\underline{\mathrm{mom}}^n_{1,t}(B^{\langle t\rangle}_{\alpha,2,c,1}) \in H^0(Y(l), \mathrm{TSym}^n\,\mathscr{H}_1)$. Considering the Tate filtration over $Y(l)$, i.e.

$$0 \to \mathbb{Z}/l\,\mathbb{Z}(1) \to \mathscr{H}_1 \xrightarrow{\alpha} \mathbb{Z}/l\,\mathbb{Z} \to 0,$$

we have that the morphism α induces, for weight reasons, an isomorphism

$$H^0(Y(l), \mathrm{TSym}^n\,\mathscr{H}_1) \xrightarrow{\cong} H^0(Y(l), \mathrm{TSym}^n\,\mathbb{Z}/l\,\mathbb{Z}) \cong \mathbb{Z}/l\,\mathbb{Z}$$

sending

$$\underline{\mathrm{mom}}^n_{1,t}(B^{\langle t\rangle}_{\alpha,2,c,1}) \mapsto \underline{\mathrm{res}}_{1,\infty}({}_cg_{n,1}(t)).$$

Since by assumption the right hand term in the isomorphism is zero, we deduce that the cup product defining ${}_cg_{n,1}(t)$ is also zero. □

The auxiliary Eisenstein class

Definition 5.4.9. For t and c as above, let us define the *auxiliary Eisenstein class* to be

$$g'_n := {}_c g_{n,1}(t) - \underline{\mathrm{res}}_{1,\infty}({}_c g_{n,1}(t))\xi \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1)),$$

where $\xi \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1))$ is the element defined in 5.4.1.

By its construction, we have

Lemma 5.4.10.

$$\underline{\mathrm{res}}_{1,\infty}(g'_n) = 0.$$

The cusp class

Definition 5.4.11. Let us define the *cusp class*

$$f_n := e'_n - g'_n \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1)).$$

From the previous results, we can immediately deduce the following Proposition.

Proposition 5.4.12. *Let f_n be the cusp class defined above. Then:*

1. $\underline{\mathrm{res}}_{1,\infty}(f_n) \equiv 0$ *modulo l;*
2. $f_n \equiv {}_c e_{n,1}(t) - {}_c g_{n,1}(t)$ *modulo l.*

Proof. The statements follow from 5.4.7, 5.4.2, 5.4.10 and the assumption $l \mid \zeta(1-k)$. $\square$

5.4.3. Constructing a Galois representation associated to the cusp class

In the previous step, we have constructed the cusp class $f_n \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1))$. To proceed analogously to Ribet's Method, we need now to associate to such a class a two-dimensional Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathbb{Z}/l\,\mathbb{Z}$ satisfying the table in 5.4. Hence it is enough to construct a cohomology class in $H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$ satisfying the properties described in 5.4.

Constructing an element in $H^1(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$

Let us start by associating to the cusp class $f_n \in H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1))$ a suitable Galois cohomology class. Since, by 5.4.12, we have that $\underline{\mathrm{res}}_{1,\infty}(f_n) \equiv 0$ modulo l, we can see the cusp class f_n as an element of $H^1(X(l), j_* \mathrm{TSym}^n \mathscr{H}_1(1))$, for $j : Y(l) \to X(l)$ the open immersion defined in 3.1.
Let us now consider the derived functor $\infty^* Rj_*$ and its induced diagram[10]

$$\begin{tikzcd}[column sep=small] & H^1(Y(l), \mathrm{TSym}^n \mathscr{H}_1(1)) \arrow[d] \arrow[dr, "\underline{\mathrm{res}}_{1,\infty}"] & \\ H^1(\mathrm{Spec}\,\mathbb{Q}(\mu_l), \infty^* j_* \mathrm{TSym}^n \mathscr{H}_1(1)) \arrow[r, "\beta"] & H^1(\mathrm{Spec}\,\mathbb{Q}(\mu_l), \infty^* Rj_* \mathrm{TSym}^n \mathscr{H}_1(1)) \arrow[r, "\gamma"] & H^0(\mathrm{Spec}\,\mathbb{Q}(\mu_l), \infty^* R^1 j_* \mathrm{TSym}^n \mathscr{H}_1(1)) \end{tikzcd} \tag{5.4}$$

[10] see [HK99a].

where the vertical arrow comes from the isomorphism $R\Gamma(X(l), Rj_* \operatorname{TSym}^n \mathscr{H}_1(1)) \cong R\Gamma(Y(l), \operatorname{TSym}^n \mathscr{H}_1(1))$ and the bottom row is exact for weight reasons of $\infty^* Rj_* \operatorname{TSym}^n \mathscr{H}_1(1)$. This diagram is the key tool to associate a Galois cohomology class in $H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ to the cusp class f_n.

Proposition 5.4.13. *There exists an element*

$$D_{n+1} \in H^1(\operatorname{Spec} \mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$$

given by the evaluation of the cusp class f_n at ∞, i.e.

$$D_{n+1} := \infty^*(f_n)$$

Proof. From the diagram (5.4) above, since, by 5.4.12, $\underline{\mathrm{res}}_{1,\infty}(f_n) = 0$ for $f_n \in H^1(Y(l), \operatorname{TSym}^n \mathscr{H}_1(1))$ we get, by exactness, a class

$$D_{n+1} \in H^1(\operatorname{Spec} \mathbb{Q}(\mu_l), \infty^* j_* \operatorname{TSym}^n \mathscr{H}_1(1))$$

given by $\beta(D_{n+1}) = a$, for $a \in H^1(\operatorname{Spec} \mathbb{Q}(\mu_l), \infty^* Rj_* \operatorname{TSym}^n \mathscr{H}_1(1))$ such that $\underline{\mathrm{res}}_{1,\infty}(f_n)$ factors through $a \in \ker \gamma$. Hence, by construction, we have

$$D_{n+1} := \infty^* f_n \in H^1(\operatorname{Spec} \mathbb{Q}(\mu_l), \infty^* j_* \operatorname{TSym}^n \mathscr{H}_1(1)).$$

By [Kin15] 12.5.4, we have the isomorphism

$$\infty^* j_* \operatorname{TSym}^n \mathscr{H}_1(n) \cong \mathbb{Z}/l\,\mathbb{Z}(n+1),$$

and so we conclude that

$$D_{n+1} \in H^1(\operatorname{Spec} \mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1)).$$

□

By using Theorem 5.0.1, we still denote by D_{n+1} the element in $H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ isomorphic to the element constructed in 5.4.13. To study further the element D_{n+1}, we give now a definition that allows us to give an equivalent description of it.

Definition 5.4.14 ([HK03] 3.1). For any $r \in \mathbb{Z}$, $s \geqslant 1$ and an integer $m \geqslant 1$, define the *s-th cyclotomic Soulé element* by

$$c_r(\zeta_m)_s := \operatorname{cor}_{\mathbb{Q}(\mu_{l^s m})/\mathbb{Q}(\mu_m)}(1 - \zeta_{l^s m}) \otimes (\zeta_{l^s m}^m)^{\otimes r-1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_m), \mathbb{Z}/l^s\,\mathbb{Z}(r)),$$

where $\operatorname{cor}_{\mathbb{Q}(\mu_{l^s m})/\mathbb{Q}(\mu_m)} : \mathbb{Q}(\mu_{l^s m}) \to \mathbb{Q}(\mu_m)$ is the corestriction map (see [Bro82]). The elements $(c_r(\zeta_m)_s)_s$ are compatible with respect to the reduction maps $\mathbb{Z}/l^s\,\mathbb{Z} \to \mathbb{Z}/l^{s-1}\,\mathbb{Z}$, and so we can define the *cyclotomic Soulé element* as the inverse limit

$$c_r(\zeta_m) := \varprojlim_s c_r(\zeta_m)_s \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_m), \mathbb{Z}_l(r)).$$

We can use the cyclotomic Soulé element $c_r(\zeta_m)_s$ defined in 5.4.14 for $m = l$, $s = 1$ and $r = n+1$ to describe the element $D_{n+1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ as follows[11].

Proposition 5.4.15 ([Kin15] 12.6.9)**.** *We have*

$$D_{n+1} = \frac{1}{2n!l^n}\left(c^2(c_{n+1}(\zeta_l)_1 + (-1)^n c_{n+1}(\zeta_l^{-1})_1) + c^{-n}(c_{n+1}(c\zeta_l)_1 + (-1)^n c_{n+1}(c\zeta_l^{-1})_1)\right)$$

in $H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$.

Hence, to study properties of the element $D_{n+1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$, it will be enough to study the element $c_{n+1}(\zeta_l)_1$ defined above.

Constructing a class in $H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$

The element $D_{n+1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ constructed in 5.4.13 clearly does not satisfy Property a) of 5.4, but we can use it to construct a class in $H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$ satisfying Property a).

Proposition 5.4.16. *There exists a non-zero element*

$$\tilde{D}_{l-k} \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$$

satisfying Property a) and b) of 5.4.

Proof. As we have seen in 5.4.15, the non vanishing of $D_{n+1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ depends on the non vanishing of the cyclotomic Soulé element $c_{n+1}(\zeta_l)_1 \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$. But the element $c_{n+1}(\zeta_l)_1$, defined in 5.4.14 by

$$c_{n+1}(\zeta_l)_1 = \mathrm{cor}_{\mathbb{Q}(\mu_{l^2})/\mathbb{Q}(\mu_l)}((1-\zeta_{l^2}) \otimes (\zeta_{l^2}^l)^{\otimes n}),$$

is, by using the projection formula

$$\mathrm{cor}_{\mathbb{Q}(\mu_{l^2})/\mathbb{Q}(\mu_l)}(a \otimes \mathrm{res}^{\mathbb{Q}(\mu_l)}_{\mathbb{Q}(\mu_{l^2})}(b)) = \mathrm{cor}_{\mathbb{Q}(\mu_{l^2})/\mathbb{Q}(\mu_l)}(a) \otimes b, \text{ for } {\scriptstyle a \in H^1(\mathbb{Q}(\mu_{l^2}), \mathbb{Z}/l\,\mathbb{Z}(n+1)) \atop \scriptstyle b \in H^1(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))},$$

equal to

$$(\mathrm{cor}_{\mathbb{Q}(\mu_{l^2})/\mathbb{Q}(\mu_l)}(1-\zeta_{l^2})) \otimes \zeta_l^{\otimes n} = (1-\zeta_l) \otimes \zeta_l^{\otimes n}.$$

Hence $0 \neq c_{n+1}(\zeta_l)_1 \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$ and so also $0 \neq D_{n+1} \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$. Consider now Shapiro's isomorphism (see [Bro82] 6.2)

$$H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1)) \cong H^1_{\mathrm{Gal}}(\mathbb{Q}, \bigoplus_{\varphi \in \widehat{\mathrm{Gal}(\mathbb{Q}(\mu_l)}/\mathbb{Q})} \mathbb{Z}/l\,\mathbb{Z}(\varphi)(n+1)).$$

Then, since $D_{n+1} \neq 0 \in H^1_{\mathrm{Gal}}(\mathbb{Q}(\mu_l), \mathbb{Z}/l\,\mathbb{Z}(n+1))$, there exists a character $\varphi \in \mathrm{Gal}(\widehat{\mathbb{Q}(\mu_l)}/\mathbb{Q})$ such that $p_\varphi(D_{n+1}) \neq 0 \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(\varphi)(n+1))$, for p_φ the projection to the φ-component. Taking n such that[12] $\mathbb{Z}/l\,\mathbb{Z}(\varphi)(n+1) \cong \mathbb{Z}/l\,\mathbb{Z}(l-k)$, we obtain $0 \neq \tilde{D}_{l-k} \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k))$, satisfying the claim. □

[11] Note that, since by Lemma 5.4.12 $f_n \equiv {}_c e_{n,1}(t) - {}_c g_{n,1}(t)$ modulo l, then we can apply [Kin15] 12.6.9 to f_n.

[12] This is possible since $\mathrm{Gal}(\mathbb{Q}(\widehat{\mu_l)/\mathbb{Q}}) = \langle \chi \rangle$, for χ the cyclotomic character.

$\tilde{D}_{l-k}$ is unramified at every prime $p \neq l$

DEFINITION 5.4.17. Consider the representation $\mathbb{Q}_l(l-k)$ and the associated inclusion map $i : \mathbb{Z}_l(l-k) \hookrightarrow \mathbb{Z}_l(l-k) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathbb{Q}_l(l-k)$ and define, for every prime $p \neq l$, the *$\mathbb{Q}_l$-finite cohomology at p* by

$$H^1_f(\mathbb{Q}_p, \mathbb{Q}_l(l-k)) := \ker(H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Q}_l(l-k)) \to H^1_{\mathrm{Gal}}(I_p, \mathbb{Q}_l(l-k)),$$

where I_p denotes the inertia group at p, and the *$\mathbb{Z}/l\,\mathbb{Z}$-finite cohomology at p* by

$$H^1_f(\mathbb{Q}_p, \mathbb{Z}/l\,\mathbb{Z}(l-k)) := \mathrm{red}_l \circ i^{-1}(H^1_f(\mathbb{Q}_p, \mathbb{Q}_l(l-k))),$$

where red_l is the reduction modulo l. For the definition at l, we refer to [Rub00] Remark 3.6. Moreover, define the *finite cohomology* over $\mathbb{Q}_l$ (resp. over $\mathbb{Z}/l\,\mathbb{Z}$) by[13]

$$H^1_f(\mathbb{Q}, \mathbb{Q}_l(l-k)) := \{x \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Q}_l(l-k)) \mid loc_p x \in H^1_f(\mathbb{Q}_p, \mathbb{Q}_l(l-k)) \text{ for every prime } p\}$$

(resp.

$$H^1_f(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k)) := \mathrm{red}_l \circ i^{-1}(H^1_f(\mathbb{Q}, \mathbb{Q}_l(l-k))).$$

Lemma 5.4.18. *We have*

$$\mathrm{loc}_p(\tilde{D}_{l-k}) \in H^1_f(\mathbb{Q}_p, \mathbb{Z}/l\,\mathbb{Z}(l-k))$$

for every prime p.

Proof. By [HK03] Lemma 1.2.6 and [Fon92] 4.4, we have that, since $l-k \geqslant 2$,

$$H^1_f(\mathbb{Q}, \mathbb{Q}_l(l-k)) \cong H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Q}_l(l-k))$$

for every prime $p \neq l$. Therefore, by definition 5.4.17, we have that, for every prime p,

$$\mathrm{loc}_p(\tilde{D}_{l-k}) \in H^1_f(\mathbb{Q}_p, \mathbb{Z}/l\,\mathbb{Z}(l-k)).$$

□

The above Lemma shows, by definition 5.4.17, that, for every prime $p \neq l$, we have

$$\tilde{D}_{l-k}|_{I_p} = 0 \in H^1_{\mathrm{Gal}}(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k)),$$

so that $\tilde{D}_{l-k}$ satisfies also Property c) of 5.4.

[13] where $\mathrm{loc}_p : H^1(\mathbb{Q}, \mathbb{Z}/l\,\mathbb{Z}(l-k)) \to H^1(\mathbb{Q}_p, \mathbb{Z}/l\,\mathbb{Z}(l-k))$ is the localization map at p.

A. Appendix

In this appendix the reader can find all the relevant definitions, statements and settings necessary to understand the work above. For details, see for example [Sil09], [KM85], [Aut], [Tam94] and [Mil04].

A.1. Hecke operators and Hecke algebra

Let $\mathcal{H} := \{\tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0\}$ be the upper half plane.

Definition A.1.1. Let N be a positive integer. The *principal congruence subgroup of level* N is the group

$$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}.$$

It is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Definition A.1.2. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Γ is called a *congruence subgroup (of level N)* if there exists an $N \in \mathbb{Z}_{>0}$ such that $\Gamma(N) \subseteq \Gamma$.

Definition A.1.3. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and k be a positive integer. The *weight-k operator* $[\gamma]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ is defined by

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)), \tau \in \mathcal{H}.$$

Definition A.1.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, k a positive integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if:

1. f is holomorphic;
2. f is weight-k invariant under Γ, i.e. $f[\gamma]_k(\tau) = f(\tau)$ for every $\gamma \in \Gamma$ and $\tau \in \mathcal{H}$;
3. $f[\gamma]_k$ is holomorphic at ∞ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

If, in addition, $a_0 = 0$ in the Fourier expansion of $f[\gamma]_k$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then f is a *cusp form of weight k with respect to* Γ.
The modular forms (resp. cusp forms) of weight k with respect to Γ are denoted by $\mathcal{M}_k(\Gamma)$ (resp. $\mathcal{S}_k(\Gamma)$).

Definition A.1.5. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The *cusps* of Γ are the Γ-equivalence classes of $\mathbb{Q} \cup \{\infty\}$.

Definition A.1.6. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\Gamma_1, \Gamma_2 \subseteq \mathrm{SL}_2(\mathbb{Z})$ be congruence subgroups. Then the *weight-k* $\Gamma_1\alpha\Gamma_2$ *double-coset operator* takes $f \in \mathcal{M}_k(\Gamma_1)$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k \in \mathcal{M}_k(\Gamma_2)$$

where the $\{\beta_j\}$ are orbit representatives, i.e. $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ disjoint union.

Definition A.1.7. For n a positive natural number and

$$\alpha_n \in \left\{ \gamma \in M_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \pmod N, \det\gamma = n \right\},$$

define the *Hecke operator* T_n to be the weight-k double coset operator $[\alpha_n]_k$, i.e.

$$T_n : \mathcal{M}_k(\Gamma(N)) \to \mathcal{M}_k(\Gamma(N)) \text{ given by } f \mapsto T_n f := f[\alpha_n]_k.$$

Define the *Hecke algebra* H to be the $\mathbb{Z}$-algebra

$$H := \mathbb{Z}[T_1, T_2, \dots]$$

generated by the Hecke operators.

Remark A.1.8. Analogous definitions hold also for Hecke operators on modular forms with coefficients in $\mathbb{Z}_l$ and the attached $\mathbb{Z}_l$-Hecke algebra. These are the objects that we will use in our main work.

A.2. Étale cohomology

Definition A.2.1. Let $f : X \to Y$ be a morphism of schemes locally of finite presentation, $x \in X$ and $y := f(x)$. Then f is *étale* if it is unramified and flat at x, for every $x \in X$.

Definition A.2.2. Let X be a scheme and denote by Et/X the category of étale schemes over X.

Definition A.2.3. Define the *étale site* X_{et} *of* X to be the category Et/X, together with coverings given by the families of morphisms $(\varphi_i : X_i' \to X')_i$ in Et/X, for $X' = \bigcup_i \varphi(X_i')$.
The category of abelian sheaves on X_{et} is denoted by $\mathrm{Sh}(X_{et})$. Its objects are called *étale sheaves* on X.

Definition A.2.4. Let F be an abelian sheaf on X_{et}, X' an étale scheme over X. Then the sheaf cohomology groups $H^q(X', F)$ are denoted by $H^q_{et}(X', F)$.[1]

[1] But in the main work, we will drop the pedix $\cdot_{et}$.

A.3. Leray spectral sequences

Definition A.3.1. Let $A \in \mathcal{C}$, $\mathcal{C}$ abelian. A decreasing *filtration* of A is a family $(F^p(A))_{p\in\mathbb{Z}}$ of subobjects $F^p(A)$ of A such that $F^{p+1}(A) \subseteq F^p(A)$ for every p. Let $gr_p(A) = F^p(A)/F^{p+1}(A)$. If A, B are two filtered objects in $\mathcal{C}$, a morphism $u : A \to B$ is compatible with the filtration if $u(F^p(A)) \subseteq F^p(B)$ for every $p \in \mathbb{Z}$.

Definition A.3.2. A *spectral sequence* in the abelian category $\mathcal{C}$ is a system $E = (E_r^{pq}, E^n)$ consisting of:

1. objects $E_r^{pq} \in \mathcal{C}$ for every $(p, q) \in \mathbb{Z}^2$ and $r \geqslant 2$
2. morphisms $d_r^{pq} : E_r^{pq} \to E_r^{p+r,q-r+1}$ in $\mathcal{C}$ such that $d_r^{p+r,q-r+1} \circ d_r^{pq} = 0$
3. isomorphisms $\alpha_r^{pq} : \ker(d_r^{pq})/\operatorname{Im}(d_r^{p-r,q-r+1}) \xrightarrow{\cong} E_{r+1}^{pq}$
4. decreasingly filtered objects $E^n \in \mathcal{C}$ for every $n \in \mathbb{Z}$
5. isomorphisms $\beta^{pq} : E_\infty^{pq} \to gr_p(E^{p+q})$.

The E_2^{pq} are called the *initial terms* and the E^n the *limit terms* of the spectral sequence. We write $E_2^{pq} \Rightarrow E^n$ for $E = (E_r^{pq}, E^n)$.

Definition A.3.3. A *morphism of spectral sequences*

$$u : E = (E_r^{pq}, E^n) \to E' = (E_r^{'pq}, E^{'n})$$

in $\mathcal{C}$ is a system of morphisms $(u_r^{pq} : E_r^{pq} \to E_r^{'pq}, u^n : E^n \to E^{'n})$ where the u^n are compatible with the filtrations of E^n and $E^{'n}$ and the u_r^{pq}, resp. u^n, commute with d_r^{pq}, α_r^{pq}, resp β^{pq}.

Definition A.3.4. A spectral sequence $E = (E_r^{pq}, E^n)$ in $\mathcal{C}$ is a *cohomological spectral sequence* if $E_2^{pq} = 0$ for $p, q < 0$.

Proposition A.3.5. *For every cohomological spectral sequence $E = (E_r^{pq}, E^n)$ in $\mathcal{C}$ there are morphisms $E_2^{n,0} \to E^n$ and $E^n \to E_2^{0,n}$ that are functorial in E and that are called edge morphisms.*

Proposition A.3.6. *For a cohomological spectral sequence $E_2^{pq} \Rightarrow E^n$ the sequence*

$$0 \to E_2^{1,0} \to E^1 \to E_2^{0,1} \to E_2^{2,0} \to E^2$$

is exact and called the exact sequence of terms of low degree (or five terms sequence) belonging to $E_2^{pq} \Rightarrow E^n$.

Proposition A.3.7. *Let $f : X \to Y$ be a finite morphism of schemes, $F \in \operatorname{Sh}(X_{et})$ an abelian sheaf. Then*

$$R^q f_* F = 0 \text{ for every } q > 0.$$

Proposition A.3.8. *If $E_2^{pq} = 0$ for every $q > 0$, then the edge morphism $E_2^{n,0} \xrightarrow{\cong} E^n$ is an isomorphism for every n.*

Definition A.3.9. Let $f : Y \to X$ be a morphism of schemes and F an abelian sheaf on Y. Define the *Leray spectral sequence* to be the spectral sequence

$$E_2^{pq} = H_{et}^p(X, R^q f_*(F)) \Rightarrow E^n = H_{et}^n(Y, F)$$

A.4. Galois action on étale cohomology

By [Del22] II 4.4, we have, for a field K and a sheaf $F \in Sh(X_{et})$ on the scheme $X := \operatorname{Spec} K$, an isomorphism

$$H^1_{et}(K, F) \cong H^1_{\mathrm{Gal}}(\mathrm{Gal}(K^{sep}/K), \varinjlim_{L/K} F(\operatorname{Spec} L))$$

for L such that $K \subseteq L \subseteq K^{sep}$.

The above isomorphism comes from the following equivalence of categories.

Proposition A.4.1 ([Del22] II 4.4)**.** *For K a field, there exists an equivalence of categories*

$$\{\textit{étale sheaves on } \operatorname{Spec} K\} \leftrightarrow \left\{\mathrm{Gal}(\overline{K}/K) - \textit{modules}\right\}.$$

Proof. ($\to$) Let $F \in Sh(\operatorname{Spec} K)$ and define $M_F := \lim_L F(L)$, for $L \subseteq \overline{K}$ finite and Galois over K. Then M_F is a discrete $\mathrm{Gal}(\overline{K}/K)$-module.

($\leftarrow$) Let M be a discrete $\mathrm{Gal}(\overline{K}/K)$-module and define $F_M \in \mathrm{Sh}(\operatorname{Spec} K)$ by $F_M(L) := M^{Gal(\overline{K}/L)}$.

□

A.4.1. Transport of structures for étale cohomology

The notion "*transport of structures*" heuristically means that if we have an object A with some structure and an isomorphism between this object A and an object B, then, through this isomorphism, also B gains this structure. Transport of structures gives rise to a Galois action on étale cohomology.

Let X be a scheme over the field K and K_1, K_2 be two algebraic closures of K with $\sigma_i : K \hookrightarrow K_i$ the corresponding inclusions. Let $\alpha : K_1 \to K_2$ be an isomorphism, then, by functoriality, we have an isomorphism

$$H^i_{et}(X \otimes_K K_1, \mathbb{Q}_l) \cong H^i_{et}(X \otimes_K K_2, \mathbb{Q}_l)$$

of $\mathbb{Q}_l$-vector spaces. Therefore every automorphism in $\mathrm{Aut}(\overline{K}/K)$ gives rise to a corresponding automorphism of $H^i_{et}(X_{\overline{K}}, \mathbb{Q}_l)$, defining an action of the Galois group $\mathrm{Gal}(\overline{K}/K)$ on $H^i_{et}(X_{\overline{K}}, \mathbb{Q}_l)$.

A.5. Tate module

Let E/S be an elliptic curve. For $n \in \mathcal{O}_S^\times$, define the *scheme of n-torsion points*

$$E[n] := \{P \in E(S) \mid nP = 0\}.$$

Remark A.5.1. $E[n]$ is a finite étale group scheme over S.

Definition A.5.2. For an elliptic curve $\pi : E \to S := \operatorname{Spec} K$ and a prime $l \in \mathcal{O}_S^\times$, define the *Tate module* to be the $\mathbb{Z}_l$-module

$$T_l(E) := \varprojlim_m E[l^m],$$

where the transition maps $E[l^m] \to E[l^{m-1}]$ are given by multiplication by l maps. It is equipped with a $\mathrm{Gal}(\overline{K}/K)$-action.

Proposition A.5.3. *The $\mathbb{Z}_l$-module $\mathscr{H} := (R^1\pi_* \mathbb{Z}_l)^\vee$ is isomorphic, in every fibre, to the Tate module $T_l(E)$.*

Proof. Let us consider the Weil pairing

$$E[l^i] \times E[l^i] \to \mu_{l^i}$$

associated to the elliptic curve $\pi : E \to S$ and, by taking the inverse limit, we obtain the perfect pairing

$$T_lE \times T_lE \to \mathbb{Z}_l(1) \colon = \varprojlim_i \mu_{l^i},$$

so that $(T_lE)^\vee \cong T_lE(-1)$.
Claim: $(T_lE)^\vee \cong H^1(E_\tau, \mathbb{Z}_l)$, for τ a geometric point of S and E_τ the localization of E at it. By [Mil13] 11.3, we have that

$$H^1_{et}(E_\tau, \mathbb{Z}_l) \cong \mathrm{Hom}(\pi_1(E), \mathbb{Z}_l)$$

where $\pi_1(E)$ is the étale fundamental group with base point the origin of E. But the étale fundamental group of E is isomorphic to T_lE, since

$$\pi_1(E) = \varprojlim_i \mathrm{Aut}(E_i) = \varprojlim_i ([l^i] : E_i \to E) = \varprojlim_i E[l^i] = T_lE.$$

As $\mathrm{Hom}(T_lE, \mathbb{Z}_l) =: (T_lE)^\vee$, we proved the claim. By base change we have

$$(R^1\pi_* \mathbb{Z}_l)_\tau \cong H^1_{et}(E_\tau, \mathbb{Z}_l).$$

Therefore,

$$\mathscr{H}_\tau \cong H^1_{et}(E_\tau, \mathbb{Z}_l)^\vee \cong T_lE.$$

□

Remark A.5.4. In particular, since $(T_lE)^\vee \cong T_lE(-1)$, we have

$$\mathscr{H} \cong R^1\pi_* \mathbb{Z}_l(1).$$

A.6. Modular curve parametrising elliptic curves

Definition A.6.1. Let $\mathscr{E}ll$ be the category whose objects are elliptic curves $\pi : E \to S$ over a variable base scheme and whose morphisms are given by the commutative diagrams

$$\begin{array}{ccc} E' & \xrightarrow{\varphi} & E \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ S' & \xrightarrow{f} & S \end{array}$$

such that the induced map $(\varphi, \pi') : E'/S' \to f^*E := E \times_S S'$ is an isomorphism of elliptic curves over S'. We write $(\varphi, f) : E'/S' \to E/S$.

Definition A.6.2. Define a *moduli problem for elliptic curves* to be a contravariant functor

$$\mathscr{P} : \mathscr{E}ll \to \text{Sets},$$

and, for an elliptic curve E/S, define a *level-$\mathscr{P}$-structure* on E/S to be an element of the set $\mathscr{P}(E/S)$. A moduli problem $\mathscr{P}$ is *representable* if the functor $\mathscr{P}$ is representable, i.e. if there exists an elliptic curve $\mathcal{E}/M(\mathscr{P}) \in \mathscr{E}ll$ and an element $\alpha_{univ} \in \mathscr{P}(\mathcal{E}/M(\mathscr{P}))$ such that, for any $E/S \in \mathscr{E}ll$,

$$\mathrm{Hom}_{\mathscr{E}ll}(E/S, \mathcal{E}/M(\mathscr{P})) \to \mathscr{P}(E/S) \text{ given by } \varphi \mapsto \mathscr{P}(\varphi)(\alpha_{univ})$$

is an isomorphism. If $\mathscr{P}$ is representable, then the scheme $M(\mathscr{P})$ represents the functor

$$\begin{aligned} S \mapsto \{&\text{isomorphism classes of pairs } (E/S, \varphi), \text{ for } E/S \text{ elliptic curve} \\ &\text{and } \alpha \in \mathscr{P}(E/S) \text{ a level-}\mathscr{P}\text{-structure on } E/S\} \end{aligned}$$

and $\mathcal{E}$ is called *universal elliptic curve* with level-$\mathscr{P}$-structure over $M(\mathscr{P})$.

We want now to give an example of moduli problem that will be used in the main work.

Definition A.6.3. Let $N \geqslant 3$ and define the *level-N-moduli problem* to be the contravariant functor

$$E/S \mapsto \{S\text{-group scheme isomorphisms } (\mathbb{Z}/N\,\mathbb{Z})^2 \xrightarrow{\cong} E[N]\}.$$

It is representable by the smooth affine curve $Y(N)$ of relative dimension 1, called the *modular curve*, over $\mathbb{Z}[1/N, \mu_N]$.
Let $X(N)$ be its smooth compactification and denote by $j : Y(N) \hookrightarrow X(N)$ the associated open immersion. Denote by Cusp the subscheme of cusps $\mathrm{Cusp} := X(N) \smallsetminus Y(N)$.

Bibliography

[Aut] The Stacks Project Authors. *Stacks Project*. URL: `https://stacks.math.columbia.edu/`.

[BO78] P. Berthelot and A. Ogus. *Notes on Crystalline Cohomology. (MN-21)*. Princeton University Press, 1978.

[Bro82] K. S. Brown. *Cohomology of Groups*. Springer New York, 1982.

[Con] K. Conrad. *Fermat's Last theorem for regular primes*. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf`.

[Del22] P. Deligne. *Étale cohomology: Starting points (notes by J. F. Boutot, translated by J.S. Milne)*. 2022. URL: `https://www.jmilne.org/math/Documents/DeligneArcata.pdf`.

[Fon92] J.M. Fontaine. "Valeurs spéciales des fonctions L des motifs". In: Astérisque 206 (1992). talk:751, pp. 205–249.

[Fu15] L. Fu. *Etale Cohomology Theory: Revised Edition*. World Scientific, 2015.

[FH04] W. Fulton and J. Harris. *Representation Theory*. Springer New York, 2004.

[Har93] G. Harder. *Eisensteinkohomologie und die Konstruktion gemischter Motive*. Springer Berlin Heidelberg, 1993.

[HP92] G. Harder and R. Pink. "Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbb{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen". In: *Mathematische Nachrichten* 159.1 (1992), pp. 83–99.

[Her32] J. Herbrand. "Sur les classes des corps circulaires". In: *Journal de Mathématiques Pures et Appliquées* 11 (1932), pp. 417–441.

[Hub15] A. Huber. "The Comparison Theorem for the Soulé–Deligne Classes". In: London Mathematical Society Lecture Note Series (2015). Ed. by John Coates et al., pp. 210–238.

[HK99a] A. Huber and G. Kings. "Degeneration of l -adic Eisenstein classes and of the elliptic polylog". In: *Inventiones Mathematicae* 135.3 (1999), pp. 545–594.

[HK99b] A. Huber and G. Kings. "Dirichlet motives via modular curves". In: *Annales scientifiques de l'École Normale Supérieure* 32.3 (1999), pp. 313–345.

[HK03] A. Huber and G. Kings. "Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters". In: *Duke Mathematical Journal* 119.3 (2003).

[Jan88] U. Jannsen. "Continuous Étale Cohomology." In: *Mathematische Annalen* 280.2 (1988), pp. 207–246.

[Kat04] K. Kato. "p-adic Hodge theory and values of zeta functions of modular forms". In: *Cohomologie p-adiques et applications arithmétiques (III)*. Ed. by Berthelot Pierre et al. Astérisque 295. Société mathématique de France, 2004, pp. 117–290.

[KM85] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Vol. 108. Annals of Mathematics Studies. Princeton University Press, 1985.

[Kin15] G. Kings. "Eisenstein Classes, Elliptic Soulé Elements and the l-Adic Elliptic Polylogarithm". In: *The Bloch–Kato Conjecture for the Riemann Zeta Function*. Ed. by John Coates et al. London Mathematical Society Lecture Note Series. Cambridge University Press, 2015, pp. 239–296.

[Kin16] G. Kings. "On p-adic Interpolation of Motivic Eisenstein Classes". In: *Elliptic Curves, Modular Forms and Iwasawa Theory*. Springer International Publishing, 2016, pp. 335–371.

[Kin22] G. Kings. *Lecture Notes on Étale Cohomology*. 2022.

[Lan90] S. Lang. *Cyclotomic Fields I and II*. Springer New York, 1990.

[MW84] B Mazur and A. Wiles. "Class fields of abelian extensions of Q." In: *Inventiones mathematicae* 76 (1984), pp. 179–330.

[Maz11] B. Mazur. "How can we construct abelian Galois extensions of basic number fields?" In: *Bulletin of the American Mathematical Society* 48.2 (2011), pp. 155–155.

[Mil80] J.S. Milne. *Etale Cohomology (PMS-33)*. Princeton University Press, 1980.

[Mil04] J.S. Milne. *Arithmetic duality theorems, Second edition*. 2004. URL: `https://www.jmilne.org/math/Books/ADTnot.pdf`.

[Mil13] J.S. Milne. *Lectures on ´etale cohomology*. 2013. URL: `https://www.jmilne.org/math/CourseNotes/LEC.pdf`.

[Rib76] K. A. Ribet. "A Modular Construction of Unramified p-Extension of $\mathbb{Q}(\mu_p)$." In: *Inventiones mathematicae* 34 (1976), pp. 151–162.

[Rub00] K Rubin. *Euler Systems*. Princeton University Press, 2000.

[Sab22] C. Sabadin. *Master Thesis*. 2022.

[Shi72] G. Shimura. "Class fields over real quadratic fields and Hecke operators". In: *Annals of Mathematics. Second Series* 95 (1972), pp. 130–190.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Princeton University Press, Princeton, NJ, 1994.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[Tam94] G. Tamme. *Introduction to Étale Cohomology*. Springer Berlin Heidelberg, 1994.

[TW95] R. Taylor and A. Wiles. "Ring-Theoretic Properties of Certain Hecke Algebras". In: *Annals of Mathematics* 141.3 (1995), pp. 553–572.

[Was97] L.C. Washington. *Introduction to Cyclotomic Fields*. Springer New York, 1997.

[Wil95] A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem". In: *The Annals of Mathematics* 141.3 (1995), pp. 443–551.