On Mazur-Tate type conjectures for quadratic imaginary fields and elliptic curves

Clément Gomez

Department of Mathematics and Statistics
Faculty of Science
McGill University, Montreal

March 2014

A thesis submitted to
McGill University
in partial fulfillment
of the requirements
for the degree of
Doctor of Philosophy

To my parents

Abstract

In this thesis, we formulate and partially prove conjectures à la Mazur-Tate for two cases of L-functions. Suppose given a L-function $L(M, K, s)$ attached to an arithmetic object M over a number field K (a "motive") so that L can be twisted by characters of the Galois group G of an extension of K. To this pair (L, G), one may hope to associate a theta element $\Theta(L, G) \in A[G]$, where A is a well defined ring, that interpolates the special values $L(M, K, \chi, 1)$ of L twisted by characters χ of G. The notion of interpolation means that the evaluation of $\Theta(L, G)$ at χ gives the value $L(M, K, \chi, 1)$ or at least a simple and explicit transformation of the value $L(M, K, \chi, 1)$. Following the ideas of Mazur and Tate, the theta element should capture the arithmetic properties of L or more precisely the arithmetic properties of the geometric objects M and K from which L is constructed.

The first chapter is devoted to the case of Artin L-functions associated to a quadratic imaginary field K and twisted by characters of the Galois groups of ray class field extensions $K(\mathfrak{m})$ of K. The theta element captures information about the class number formulas of the fields $K(\mathfrak{m})$. For the second chapter, the underlying geometric object is a pair (K, E) of a quadratic imaginary field K and an elliptic curve E defined over $\mathbb{Q}$. The theta element should capture there information about the rank of the Mordell-Weil groups $E(K)$.

The key ingredient in the study of the theta elements in both cases is the existence of a set of cohomology classes in appropriate cohomology groups that satisfy local and global compatibilities. These systems, sometimes called *Euler system* or *Kolyvagin system* even if the literature is not unified on this appellation, arise from purely geometric considerations. In chapter 1, these classes, called in that case *elliptic units* are constructed by considering units in the ray class fields of K, whereas in chapter 2, they arise by considering the *Heegner points* over K in a *Shimura curves* associated to E and K.

Each chapter has the form of an article and can be read independently from the other one.

Abrégé

Dans cette thèse, nous formulons et prouvons partiellement des conjectures à la Mazur-Tate pour deux cas précis de fonctions L. Supposons donnée une fonction $L(M, K, s)$ attachée à un object arithmétique M défini sur un corps de nombre K et supposons que cette fonction L puisse être tordue par les caractères associés au groupe de Galois G d'une extension de K. Dans une telle situation, il est naturel d'espérer associer à cette paire (L, G) un élément theta $\Theta(L, G)$ dans un anneau de groupe $A[G]$ qui interpoles les valeurs spéciales $L(M, K, \chi, 1)$ de L tordue par les caractères χ de G. Par interpolation, nous entendons ici que l'évaluation de $\Theta(L, G)$ en χ donne la valeur $L(M, K, \chi, 1)$ ou au moins une transformation explicite de cette valeur. Selon les idées de Mazur et Tate, l'élément $\Theta(L, G)$ est alors censé capturé les propriétés arithmétiques et géometriques des objets M et K associés à L.

Le premier chapitre est consacré au cas des fonctions L d'Artin associées à un corps quadratique imaginaire K et tordues par les caractères des groupes de Galois des extensions des corps de classe de rayon $K(\mathfrak{m})$. Dans ce cas, l'élement theta capture des informations sur les formules du nombre de classe des corps $K(\mathfrak{m})$. Dans le second chapitre, l'object géometrique sous-jacent est une paire (E, K) constituée d'une courbe elliptique E définie sur $\mathbb{Q}$ et d'un corps quadratique imaginaire K. L'élément theta capture ici des informations sur le rang du groupes de Mordell-Weil $E(K)$.

L'ingrédient principal dans l'étude des élément theta dans les deux cas est l'existence d'un ensemble de classes cohomologiques dans des groupes de cohomologie galoisienne précis satisfaisant des compatibilités locales et globales. Ces ensembles parfois dénommés *systèmes d'Euler* ou *systèmes de Kolyvagin* (même si la littérature n'est pas encore unifiée sur le sujet) proviennent de considérations purement géometriques. Dans le premier chapitre, ces classes dénommées *unités elliptiques* sont construites à partir d'unités globales dans les extensions de corps de classe de rayon de K alors que dans le second chapitre, ces classes proviennent des points de Heegner sur des courbes de Shimura associées à E et K.

Chaque chapitre a la forme d'un article indépendant.

Acknowledgments

I would like to thank my supervisor Henri Darmon for giving me the opportunity to work under his direction at McGill University. His patience and his guidance were extremely appreciable throughout all stages of the work and God knows where I would be without his choice of a subject that perfectly corresponds to my tastes as a mathematician.

It is a great pleasure to thank Professor Meinolf Geck for introducing me to the beauty of algebraic geometry. His book along with the time I spent under his direction in Aberdeen opened my mind on the beauty of advanced mathematics.

I would also express my deepest gratitude to Professor David Harari. His course in Orsay on Galois cohomology was of an unbelievably quality and is still today one of the foundations of my mathematical knowledge.

Finally, I'm very grateful to all my student colleagues for all the fruitful conversations that we shared. Among them I would especially cite Jay Taylor, Francesc Castella, Antoine Jacono and Luca Candelori.

Contents

Chapter 1

Refined class number formulas for elliptic units

Summary

We generalize the notion of Kolyvagin and pre-Kolyvagin systems to prove "refined class number formulas" for quadratic extensions of a quadratic imaginary K fields of class number one. Our main result generalises the results and conjectures of [5], by replacing circular units in abelian extensions of $\mathbb{Q}$ by elliptic units in abelian extensions of K.

1.1 Introduction

Thanks to the work of Mazur and Tate [15], we can attach to any extension K/k of global fields a Stickelberger-type element $\theta_G \in \mathbb{Z}[G]$ where $G := \mathrm{Gal}(K/k)$. This element interpolates special values of L-functions over K twisted by complex characters of G: For any complex character χ of G, $\chi(\theta_G)$ is essentially the special value $L(K, \chi, 0)$. In settings where these values vanish identically, it is natural to consider their derivatives. For the case where F is a real quadratic field, writing $G_n := \mathrm{Gal}(F(\mu_n)/F)$, Darmon defined a Stickelberger-type element $\theta'_{G_n} \in \mathcal{O}^*_{F(\mu_n)} \otimes \mathbb{Z}[G_n]$. In a similar sense as θ_G, the element θ'_{G_n} interpolates special values of $L'(w_F\chi, 0)$ where w_F is the quadratic character associated to $F/\mathbb{Q}$ and χ is a character of G_n. The construction of θ'_{G_n} relies essentially on the properties of the cyclotomic units over $\mathbb{Q}$. In [5], Darmon studies the algebraic properties of θ_{G_n} and conjectures "refined class number formulas" for its leading term. Theses formulas were then proved (up to a power of 2) by Mazur and Rubin in [13] using their notion of *pre-Kolyvagin system*.

To construct a similar Stickelberger-type element for field other than $\mathbb{Q}$, we need something to replace the cyclotomic units. In the case where K is a quadratic imaginary field, we have the notion of elliptic units. Elliptic units and cyclotomic seem to mirror perfectly: Cyclotomic units are global units associated to ray class fields of $\mathbb{Q}$ whereas elliptic units are global units associated to ray class fields of K. Furthermore, both objects are constructed using torsion points of algebraic groups (roots of unity for cyclotomic units versus torsion points over a well-chosen elliptic curve for elliptic units) and both objects satisfy norm compatibilities. It is a common belief that all theorems based on cyclotomic units and the base field $\mathbb{Q}$ can be translated in terms of elliptic units and the base field K.

In the spirit of the correspondence between cyclotomic units and elliptic units, we formulate "refined class number formulas" over the base field K involving the same kind of Stickelberger-type element but made this time from elliptic units. This element has the same properties as θ'_{G_n}: It interpolates special values of $L'(w_H\chi, 0)$, where w_H is the quadratic character associated to a quadratic extension H/K (See [7]). We follow closely [13] in our proof of the resulting conjecture.

The formulas that we prove are indexed by ideals in K. When the ideal is trivial, the associated formula follows from Dirichlet's class number formula and Kronecker's second limit formula.

For any ideal, we use some kind of "induction". More precisely, both sides of the formulas indexed by the ideals form systems that satisfy some local and global compatibilities. Such systems are called pre-Kolyvagin systems. In good cases like ours, the values of a pre-Kolyvagin system only depend on its value for the trivial ideal. All the formulas follow then from the formula at the trivial ideal.

1.1 Introduction

The compatibilities satisfied by pre-Kolyvagin systems are quite involved. Historically, Mazur and Rubin first developed the notion of Kolyvagin system, whose set of axioms is cleaner and whose properties have been well studied in [12]. However, the difference of both notions is only formal since they are isomorphic (see Proposition 1.6.3).

Finally, we also deal with the notion of *Euler systems* (and especially the Euler system of elliptic units). Their well-known properties allow us to construct Kolyvagin systems. This paper is hopefully a good introduction to these three notions and their relations to each other.

The paper is organized as follows. In the first three sections, we define the elements involved in our "refined class number formula" and we state our main result. In Sections 5 and 6, we describe the notions of Kolyvagin systems and pre-Kolyvagin systems in a very general setting. In Section 7, we apply these concepts to the Galois representation $\mathbb{Z}_p(1) \otimes \psi$ that we'll define. In Sections 8 and 9, we study in details the elements defined in the first sections to understand how they match with the definition of pre-Kolyvagin systems associated to $\mathbb{Z}_p(1) \otimes \psi$. Finally, Section 10 is devoted to the proof of the formulas by using all the tools previously described.

We now briefly summarize our key results. Let K be a quadratic imaginary field of class number one and let H be a quadratic extension of K. Denote by σ the non trivial element in $\mathrm{Gal}(H/K)$. If M is a $\mathrm{Gal}(H/K)-$module, we let M^- be the subgroup of elements of M on which σ acts as -1.

Denote by ψ the quadratic Hecke character associated to H/K and let $\mathfrak{f}$ be its conductor, which we assume non trivial and prime to 6.

For all ideals $\mathfrak{m}$ in K, let $K(\mathfrak{m})$ be the ray class field of K with respect to $\mathfrak{m}$, let $\mathcal{N}_\mathfrak{m}$ be the set of squarefree ideals prime to $\mathfrak{m}$, let $r(\mathfrak{m})$ be the number of primes ideals dividing $\mathfrak{m}$ and let $\mathfrak{m}^+$ be the product of primes dividing $\mathfrak{m}$ that split in H (i.e. $\mathfrak{m}^+ = \prod_{\mathfrak{l}|\mathfrak{m},\psi(\mathfrak{l})=1} \mathfrak{l}$) and $\mathfrak{m}^- = \mathfrak{m}/\mathfrak{m}^+$. Note that the letter $\mathfrak{l}$ always denotes a prime ideal.

Denote by $H(\mathfrak{m})$ the compositum of H and $K(\mathfrak{m})$. When $\mathfrak{m} \in \mathcal{N}_\mathfrak{f}$, then class field theory says that

$$Gal(H(\mathfrak{m})/H) \simeq Gal(K(\mathfrak{m})/K) \simeq (\mathcal{O}_K/\mathfrak{m})^*.$$

Denote $\Gamma_\mathfrak{m}$:=$\mathrm{Gal}(K(\mathfrak{m})/K)$. By the previous remark, $\Gamma_\mathfrak{m}$ can be viewed as a subgroup or as a quotient $\Gamma_{\mathfrak{mn}}$, for $\mathfrak{m}$ and $\mathfrak{n}$ coprime.Let $I_\mathfrak{m}$ denote the augmentation ideal of $\mathbb{Z}[\Gamma_\mathfrak{m}]$, which is generated over $\mathbb{Z}$ by $\{\gamma - 1, \gamma \in \Gamma_\mathfrak{m}\}$. There is a natural homomorphism

$$I_\mathfrak{m}/I_\mathfrak{m}^2 \simeq \Gamma_\mathfrak{m}$$

defined by sending $\gamma - 1 \in I_\mathfrak{m}/I_\mathfrak{m}^2$ to $\gamma \in \Gamma_\mathfrak{m}$.

Fix an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$. For each prime $\mathfrak{p}$, fix $\pi_\mathfrak{p}$ a generator of $\mathfrak{p}$ and for any ideal $\mathfrak{m} = \prod_i \mathfrak{p}_i$, consider the generator $\pi_\mathfrak{m} := \prod_i \pi_{\mathfrak{p}_i}$.

Consider also an elliptic curve E defined over $\mathbb{Q}$ with complex multiplication by K and consider the Weierstrass model given by $E \simeq \mathbb{C}/\mathfrak{f}$.

The elliptic units that we construct using an auxiliary ideal $\mathfrak{a}$ in section 1.3 are global units $\alpha(\mathfrak{m})$ in $H(\mathfrak{m})$. We define the Stickelberger-type elements

$$\theta'(\psi, \mathfrak{m}, \mathfrak{a}) := \sum_{\gamma \in Gal(H(\mathfrak{m})/H)} \gamma(\alpha(\mathfrak{m})) \otimes \gamma \in H(\mathfrak{m})^* \otimes \mathbb{Z}[\Gamma_{\mathfrak{m}}].$$

On the other hand in section 1.2, we construct $\mathfrak{m}$-regulators $R_{\mathfrak{m}}$ in $H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ using a base of a certain subgroup of $\mathfrak{m}$ units in H and Artin symbols. If we denote $h_{\mathfrak{m}}$ the $\mathfrak{m}$ class number of H, i.e., the order of the ideal class group $Pic(\mathcal{O}_H[1/\pi_{\mathfrak{m}}])$, the main results of this article are:

Theorem 1.1.1. *For every $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$:*

$$\theta'(\psi, \mathfrak{m}, \mathfrak{a}) \in H^*(\mathfrak{m}) \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}.$$

The image of $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ in $H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ denoted $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$ is called the leading term of $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ and satisfies the following properties:

Theorem 1.1.2. *For every $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$:*

$$\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a}) \in H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6].$$

Furthermore, we have:

$$2^{-r(\mathfrak{m}^-)}\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = -\frac{w_{\mathfrak{f}} w_K}{w_H}(N_{K/\mathbb{Q}}\mathfrak{a} - \psi(\mathfrak{a}))h_{\mathfrak{m}} R_{\mathfrak{m}}$$

$$\text{in } H \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6],$$

where w_H (respectively w_K) is the number of roots of unity in H (respectively in K) and $w_{\mathfrak{f}}$ is the number of roots of unity in H which are congruent to 1 mod $\mathfrak{f}$.

1.2 The $\mathfrak{m}$-regulator of H

Suppose $\mathfrak{m} \in \mathcal{N}_{\mathfrak{f}}$. Let $X_{\mathfrak{m}}$ be the group of divisors of H supported above $\mathfrak{m}\infty$, let $E_{\mathfrak{m}} := \mathcal{O}_{H,\mathfrak{m}}^*$ the group of $\mathfrak{m}$ units of H and

$$(1-\sigma)E_{\mathfrak{m}} := \{\epsilon/\epsilon^{\sigma} : \epsilon \in E_{\mathfrak{m}}\}.$$

Let $\lambda_0 \in X_{\mathfrak{m}}$ be the archimedean place of H corresponding to our chosen embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$.

Proposition 1.2.1. *Let $\mathfrak{m} \in \mathcal{N}_{\mathfrak{f}}$ and $r = r(\mathfrak{m}^+)$:*

(i)The group $X_{\mathfrak{m}}^-$ is a free abelian group of rank $r+1$. If $\mathfrak{m}^+ = \prod_{i=1}^r \lambda_i \lambda_i^\sigma$, a basis of $X_{\mathfrak{m}}^-$ is given by $\{\lambda_0 - \lambda_0^\sigma, ..., \lambda_r - \lambda_r^\sigma\}$.

(ii) $(1-\sigma)E_{\mathfrak{m}}$ is a free abelian group of rank $r+1$, and is a subgroup of finite index in $E_{\mathfrak{m}}^-$.

Proof. (i) is clear.

(ii)We show first that $(1-\sigma)E_{\mathfrak{m}}$ is free.Suppose that

$$\epsilon/\epsilon^\sigma = -1$$

for some $\epsilon \in E_{\mathfrak{m}}$. Write $H = K(\sqrt{t})$ for some t squarefree in K. We have $\epsilon/\sqrt{t} \in K$. Choose a prime $\mathfrak{l}|\mathfrak{f}$ such that the valuation of t at $\mathfrak{l}$ is odd. (Such a prime exists by our hypothesis on $\mathfrak{f}$). Then, the valuation of ϵ at $\mathfrak{l}$ is non zero, which is a contradiction.

The part about the rank follows from Dirichlet S-unit theorem.

□

Definition 1.2.2. *A standard basis for $X_{\mathfrak{m}}^-$ is a basis of the form described in the previous proposition.*

Given a standard basis for $X_{\mathfrak{m}}^-$, a basis of $(1-\sigma)E_{\mathfrak{m}}$ is called oriented if the determinant of the logarithm embedding:

$$(1-\sigma)E_{\mathfrak{m}} \to X_{\mathfrak{m}}^- \otimes \mathbb{R}, \epsilon \mapsto \sum_0^r log|\epsilon|_{\lambda_i}.\lambda_i$$

with respect to the two basis is positive.

Definition 1.2.3. *Let $\mathfrak{m} \in \mathcal{N}_{\mathfrak{f}}$ and λ is a prime of H dividing $\mathfrak{m}^+$. Define a homomorphism:*

$$[.]_\lambda^{\mathfrak{m}} : H^* \to \Gamma_{\mathfrak{m}} \simeq I_{\mathfrak{m}}/I_{\mathfrak{m}}^2,$$

*where $[x]_\lambda^{\mathfrak{m}} := [x, H_\lambda(\mathfrak{m})/H_\lambda]^{-1}$ is the **inverse**[1] of the local Artin symbol.*

Definition 1.2.4. *Let $\mathfrak{m} \in \mathcal{N}_{\mathfrak{f}}$ and $r = r(\mathfrak{m})$. Choose a standard basis $\{\lambda_0 - \lambda_0^\sigma, ..., \lambda_r - \lambda_r^\sigma\}$ of $X_{\mathfrak{m}}^-$ and an oriented basis $\{\epsilon_0, ..., \epsilon_r\}$ of $(1-\sigma)E_{\mathfrak{m}}$.*

The $\mathfrak{m}$-regulator $R_{\mathfrak{m}} \in E_{\mathfrak{m}}^- \otimes I_{\mathfrak{m}}^r/I_{\mathfrak{m}}^{r+1}$ is:

$$R_{\mathfrak{m}} := \begin{vmatrix} \epsilon_0 & \epsilon_1 & ... & \epsilon_r \\ [\epsilon_0]_{\lambda_1}^{\mathfrak{m}} & [\epsilon_1]_{\lambda_1}^{\mathfrak{m}} & ... & [\epsilon_r]_{\lambda_1}^{\mathfrak{m}} \\ \vdots & \vdots & & \vdots \\ [\epsilon_0]_{\lambda_r}^{\mathfrak{m}} & [\epsilon_1]_{\lambda_r}^{\mathfrak{m}} & ... & [\epsilon_r]_{\lambda_r}^{\mathfrak{m}} \end{vmatrix} \in (1-\sigma)E_{\mathfrak{m}} \otimes I_{\mathfrak{m}}^r/I_{\mathfrak{m}}^{r+1}.$$

[1]We use the inverse of the local Artin symbol and not the Artin symbol as in [13] Definition 3.5. The reason follows from the explicit computation of the finite singular morphism in Proposition 1.7.1. For the same reason, it should be the inverse of the local Artin symbol in Definition 3.5 of [13].

1.3 The Euler system of elliptic units

We follow [17] to construct the *Euler system* of elliptic units as in [5].

Take an auxiliary ideal $\mathfrak{a}$ of K, prime to $6\mathfrak{f}$, that we fix once for all.

Definition 1.3.1. *Define a rational function on E*

$$\Theta_{E,\mathfrak{a}}(P) := \alpha^{-12}\Delta(E)^{N\mathfrak{a}-1}\prod_{Q\in E[\mathfrak{a}]-0}(x(P)-x(Q))^{-6},$$

where α is a generator of $\mathfrak{a}$ and $\Delta(E)$ is the discriminant of the chosen model of E. (A study of this function shows that it is actually independent of the choice of α and of our chosen Weierstrass model, this study is made in [17] Lemma 7.2.)

Proposition 1.3.2. *(i) $\Theta_{E,\mathfrak{a}}$ is a rational function on E with divisor*

$$12N_{K/\mathbb{Q}}\mathfrak{a}[0] - 12\sum_{Q\in E[\mathfrak{a}]}[Q].$$

(ii) Suppose $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$ prime to $\mathfrak{a}$, and β is a generator of $\mathfrak{b}$. Then for all $P \in E(\overline{K})$

$$\prod_{R\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\beta P).$$

Proof. This is [17] Lemma 7.5 and Theorem 7.6. □

Remark: the construction of $\Theta_{E,\mathfrak{a}}$ may be done using this proposition. It is the only function on E satisfying (i) and (ii) (see the construction of these units by Kato in [Ka] 15.4 p.188).

Definition 1.3.3. *Consider the points $P_{\mathfrak{fm}} := \frac{1}{\pi_{\mathfrak{m}}} \in E[\mathfrak{fm}]$ given by our chosen isomorphism $E \simeq \mathbb{C}/\mathfrak{f}$.*

Define the elliptic units

$$\alpha(\mathfrak{m}) := \prod_{\sigma\in\Gamma_{\mathfrak{f}}}\Theta_{E,\mathfrak{a}}(\sigma(P_{\mathfrak{fm}}))^{\psi(\sigma)} \in H(\mathfrak{m})^*.$$

Proposition 1.3.4. *$\alpha(\mathfrak{m})$ is a global unit in $H^*(\mathfrak{m})$.*

Proof. For any $\sigma \in \Gamma_{\mathfrak{f}}$, and for any prime $\mathfrak{l}$ we know that $\Theta_{E,\mathfrak{a}}(\sigma(P_{\mathfrak{fm}}))$ has $\mathfrak{l}-$valuation independent of σ ([17] Theorem 7.4). The result follows from the definition of α and from the fact that $\mathfrak{f}$ is prime to 2. (For $\mathfrak{m} \neq 1$, all the $\Theta_{E,\mathfrak{a}}(\sigma(P_{\mathfrak{fm}}))$ are global units and the result follow, but it is not true that $\Theta_{E,\mathfrak{a}}(P_{\mathfrak{f}}))$ is a global unit for $\mathfrak{f}$ a power of a prime.) □

Proposition 1.3.5. *If* $\mathfrak{mp} \in \mathcal{N}_{\mathfrak{af}}$, *then*

$$N_{H(\mathfrak{mp})/H(\mathfrak{m})}\alpha(\mathfrak{mp}) = (1 - Frob_{\mathfrak{p}}^{-1})\alpha(\mathfrak{m}),$$

$$N_{H(\mathfrak{mp}^2)/H(\mathfrak{mp})}\alpha(\mathfrak{mp}^2) = \alpha(\mathfrak{mp}).$$

Proof. It follows from [17] Corollary 7.7. The assumption $\mathfrak{f}$ is prime to 6 is used in order to have an injective map $\mathcal{O}_K^* \to (\mathcal{O}_K/\mathfrak{f})^*$.

□

These "norm compatibilities" are exactly the properties that we need to have an Euler system in the sense of [16]. More precisely:

Proposition 1.3.6. *For all prime* $\mathfrak{p}$ *above* p, *the collection*

$$\{\alpha(\mathfrak{mp}^n) \in H^1(K(\mathfrak{mp}^n), \mathbb{Z}_p(1) \otimes \psi)), \mathfrak{m} \in \mathcal{N}_{\mathfrak{paf}}\}$$

is an Euler system in the sense of [16] Definition 1.1 p.21.

Definition 1.3.7. *The Theta element attached to* $(\psi, \mathfrak{m}, \mathfrak{a})$ *is defined to be*

$$\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = \sum_{\gamma \in Gal(H(\mathfrak{m})/H)} \gamma(\alpha(\mathfrak{m})) \otimes \gamma \in H(\mathfrak{m})^* \otimes \mathbb{Z}[\Gamma_{\mathfrak{m}}].$$

Remark: as mentioned in the introduction, the element $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ interpolates $L'_{\mathfrak{m}}(0, \psi)$ twisted by characters $\chi : \Gamma_{\mathfrak{m}} \to \mathbb{C}^*$ in the sense that we have the equality:

$$\sum_{\gamma \in \Gamma_{\mathfrak{m}}} \chi(\gamma) log|\gamma(\alpha(\mathfrak{m})|^2 = -w_{\mathfrak{m}}(N_{K/\mathbb{Q}}(\mathfrak{a}) - \chi(\mathfrak{a}))L'_{\mathfrak{m}}(0, \psi\chi),$$

where $w_{\mathfrak{m}}$ denotes the number of roots of unity in K congruent to 1 modulo $\mathfrak{m}$ ([7], Lemma 2.2).

1.4 Statement of the formulas

We can now state the main result of this article:

Theorem 1.4.1. *For every* $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$,

$$2^{-r(\mathfrak{m}^-)}\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = -\frac{w_{\mathfrak{f}} w_K}{w_H}(N_{K/\mathbb{Q}}\mathfrak{a} - \psi(\mathfrak{a}))h_{\mathfrak{m}} R_{\mathfrak{m}}$$

$$in\ H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6],$$

where $w_{\mathfrak{f}}$ *is the number of roots of unity in* H *which are congruent to 1 mod* $\mathfrak{f}$, w_H *is the number of roots of unity in* H , w_K *is the number of roots of unity in* K, $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ *is defined in definition* 1.3.7, $h_{\mathfrak{m}}$ *is the* $\mathfrak{m}$ *class number of* H *and* $R_{\mathfrak{m}}$ *is defined in definition* 1.2.4.

The rest of this section is devoted to the proof of the formula when $\mathfrak{m} = 1$.

We'll use two different evaluations of the derivative at $s = 0$ of

$$L_K(\psi, s) := \sum_{\mathfrak{f}\nmid\mathfrak{m}} \frac{\psi(\mathfrak{m})}{N_{K/\mathbb{Q}}\mathfrak{m}^s}.$$

Lemma 1.4.2. *$L'_K(\psi, 0)$ satisfies the equalities*

$$(i) L'_K(\psi, 0) = \frac{-1}{N_{K/\mathbb{Q}}\mathfrak{a} - \psi(\mathfrak{a})} \frac{1}{w_\mathfrak{f}} log|\alpha(1)|^2,$$
$$(ii) L'_K(\psi, 0) = \frac{h_H w_K R_H}{w_H},$$

where R_H is the regulator of the field H.

Proof. (i) is a well-known property of elliptic units which follows from the Kronecker second limit formula. It is for instance proven in [7] Lemma 2.2, where our element $\Theta_{E,\mathfrak{a}}(P_\mathfrak{f})$ is denoted ${}_\mathfrak{a}z_\mathfrak{f}$.

(ii) From class field theory (the general case is made in [21] chap.2, section 4 p.101), we know that

$$\frac{\zeta_H(s)}{\zeta_K(s)} = L_K(\psi, s).$$

Hence using Dirichlet's class number formula at $s = 0$:

$$\lim_{s\to 0} s^{-1}\zeta_H(s)' = \frac{h_H R_H}{w_H} \quad \text{and} \quad \lim_{s\to 0} \zeta_K(s) = \frac{h_K R_K}{w_K}$$

since the rank of the unit group of $\mathcal{O}_H$ is 1 and the rank of the unit group of $\mathcal{O}_K$ is 0.

Finally, since $h_K = 1$ and $R_K = 1$, we obtain the desired formula:

$$L'_K(\psi, 0) = \frac{h_H w_K R_H}{w_H}.$$

□

Proof of Theorem 1.4.1 when $\mathfrak{m} = 1$.

Take ϵ a generator of $\mathcal{O}_H^*$ modulo its roots of unity whose existence is assured by Dirichlet's unit theorem and choose ϵ such that $|\epsilon| > 1$, then by definition of the regulator of H

$$R_H := 2log|\epsilon|.$$

But then since $N_{H/K}(\epsilon) = \epsilon\epsilon^\sigma$ is a unit in K, we have $|\epsilon\epsilon^\sigma| = 1$ and

$$R_H := 2log|\epsilon| = log|\epsilon|^2 = log|\frac{\epsilon}{\epsilon^\sigma}|.$$

On the other hand, by definition:

$$R_1 = \frac{\epsilon}{\epsilon^\sigma}.$$

(thanks to our choice of the unit ϵ, the basis is oriented with respect to the standard basis $\lambda_0 - \lambda_0^\sigma$).

So finally, we have

$$L'_K(\psi, 0) = \frac{R_H h_H w_K}{w_H} = 2\frac{log|R_1| h_H w_K}{w_H} = \frac{-1}{N\mathfrak{a} - \psi(\mathfrak{a})} \frac{1}{w_\mathfrak{f}} log|\alpha(1)|^2$$

and

$$-\frac{w_K w_\mathfrak{f}}{w_H}(N\mathfrak{a} - \psi(\mathfrak{a}))h_H.R_1 = \omega\alpha(1) \in H^* \otimes \mathbb{Z},$$

where ω is a root of unity in H.

Since ω has order dividing 6, it disappears when we tensor by $\mathbb{Z}[1/6]$.

□

Remark: if we want to avoid tensoring by $\mathbb{Z}[1/3]$, we have to assume that H doesn't contain the third roots of unity.

1.5 Kolyvagin system over number fields

As we've seen, Theorem 1.4.1 holds when $\mathfrak{m} = 1$. For the general cases, we introduce now the notions of Kolyvagin system and pre-Kolyvagin system to prove Theorem 1.4.1 by "induction".

In [12] and [13], Kolyvagin systems and pre-Kolyvagin systems are defined over $\mathbb{Q}$. We generalize now these notions in a natural way, to allow us to consider Kolyvagin system over any number field. This section is devoted to the definition of Kolyvagin systems and their first properties. The next section is devoted to the definition of pre-Kolyvagin systems and the isomorphism between them.

We work in a very general setting for the two next sections before coming back to the ones in the introduction.

Let R denote a valuation ring with maximal ideal β generated by π_β an uniformizer and with finite residue field $k := R/\beta R$ of characteristic p.

Let K be a number field.

Let T be a free R-module of finite rank equipped with a continuous action of G_K unrammified for almost all primes in K, let $\mathcal{F}$ be a *Selmer structure* on T, and let $\mathcal{P}$ be a sets of primes in K disjoint from $\Sigma(\mathcal{F})$. Denote also $\mathcal{N}(\mathcal{P})$ to be the set of squarefree products of primes in $\mathcal{P}$.

For all prime ideal $\mathfrak{l}$ where T is unramified, denote $J_\mathfrak{l} \subseteq R$ to be the ideal generated by $\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{l}) - 1$ and $\det(1 - \ \mathrm{Frob}_\mathfrak{l}|T)$.

For any ideal $\mathfrak{m}$, denote $J_\mathfrak{m} := \sum_{\mathfrak{l}|\mathfrak{m}} J_\mathfrak{l}$.

For any ideal $\mathfrak{m}$, denote $\mathfrak{m}^+ := \prod_{\mathfrak{l}|\mathfrak{m},\mathfrak{l}\in\mathcal{P}} \mathfrak{l}$, $\mathfrak{m}^- := \mathfrak{m}/\mathfrak{m}^+$ and $r(\mathfrak{m})$ the number of primes $\mathfrak{l}$ dividing $\mathfrak{m}$. (For our choice of $\mathcal{P}$ in section 1.7, the notation $\mathfrak{m}^+$ will be consistent with the one that we've made in the setting.)

For any $\mathfrak{l}$ denote $G_\mathfrak{l}$ the residue field of K^2 at $\mathfrak{l}$ and let

$$G_\mathfrak{m} := \bigotimes_{\mathfrak{l}|\mathfrak{m}} G_\mathfrak{l}.$$

Finally, when T is unramified at $\mathfrak{l}$ denote $\phi_\mathfrak{l}^{fs}$ the *finite singular morphism* $H^1_f(K_\mathfrak{l}, T/I_\mathfrak{l}T) \to H^1_s(K_\mathfrak{l}, T/I_\mathfrak{l}T) \otimes G_\mathfrak{l}$.

(The reader is refered to [12] Definitions 1.2.2 and 2.1.1 for the definitions of finite singular morphism and Selmer structure.)

Following [12], we generalize the definition of Kolyvagin systems:

Definition 1.5.1. *A Kolyvagin system for $(K, T, \mathcal{F}, \mathcal{P})$ is a collection of cohomology classes:*

$$\{\kappa_\mathfrak{m} \in H^1_{\mathcal{F}(\mathfrak{m}^+)}(K, T/I_{\mathfrak{m}^+}T) \otimes G_{\mathfrak{m}^+}, \mathfrak{m} \subseteq \mathcal{O}_K\}^3$$

such that:

(i)$\kappa_\mathfrak{m} = \kappa^+_\mathfrak{m}$,

(ii)if $\mathfrak{l}|\mathfrak{m}^+$ *then* $(\kappa(\mathfrak{m})_\mathfrak{l} = (\phi_\mathfrak{l}^{fs} \otimes 1)(\kappa(\mathfrak{m}/\mathfrak{l}))$.

Let $\boldsymbol{KS}(K, T, \mathcal{F}, \mathcal{P})$ *denote the R-module of Kolyvagin system for the quadruple* $(K, T, \mathcal{F}, \mathcal{P})^4$.

Following [12], we write now hypotheses that play an important role in order to work with Kolyvagin system.

Let fix a quadruple $(T, \mathcal{F}, \mathcal{P}, K)$.

Definition 1.5.2. *If $k \in \mathbb{Z}^+$, let $\mathcal{P}_k$ be the set of prime ideals $\mathfrak{l} \notin \Sigma(\mathcal{F})$ satisfying:*

$\bullet T/(\beta^k T + (Frob_\mathfrak{l} - 1)T)$ is a free of rank one over R/β^k, and

$\bullet J_\mathfrak{l} \subseteq \beta^k$.

Let $\mathcal{P}_0 := \mathcal{P}_1 \cup \{\mathfrak{l} \notin \Sigma(\mathcal{F})$ such that $J_\mathfrak{l} = R\}$.

[2]This notation may seem unusual but in our spirit we consider elements of the residue fields as elements of the Galois group of ray class field extensions.

[3]The module $H^1_{\mathcal{F}(\mathfrak{m}^+)}(K, T/I_{\mathfrak{m}^+}T)$ is a submodule of $H^1(K, T/I_{\mathfrak{m}^+}T)$ defined by local conditions. See [12] Definition 2.1.1.

[4]In [12], a Kolyvagin system takes values at ideals in $\mathcal{N}(\mathcal{P})$. Here, we extend it "trivially" to all ideals of K by property (ii).

Consider the following properties:

(H.0) T is a free $R-$ module of finite rank.

(H.1) $T \otimes_R k$ is an absolutely irreducible $k[G_K]$ representation.

(H.2)There is a $\rho \in G_K$ such that $\rho = 1$ on μ_{p^∞} and $T/(\rho - 1)T$ is free of rank one over R.

(H.3) $H^1(K(T, \mu_{p^\infty}, T/\beta T) = H^1(K(T^*, \mu_{p^\infty}, T^*[\beta]) = 0$.[5]

(H.4)Either,

(H.4.a) $Hom_{k[[G_K]]}(T/\beta T, T^*[\beta]) = 0$, or

(H.4.b) $p > 4$.

(H.5) $\mathcal{P}_t \subset \mathcal{P} \subset \mathcal{P}_0$ for some $t \in \mathbb{Z}^+$, $\mathcal{P}_k$ is given by Definition 1.5.2.[6]

(H.6) For every $\mathfrak{l} \in \Sigma(\mathcal{F})$, the local condition $\mathcal{F}$ at $\mathfrak{l}$ is cartesian ([12], Definition 1.1.4) on the category $Quot_R(T)$ of quotients of T.

Proposition 1.5.3. *Suppose that $(K, T, \mathcal{F}, \mathcal{P})$ satisfies (H.0) to (H.6), then:*

(i) There exist integers $\chi(T)$ and $\chi(T^*)$ depending on the choice of the Selmer structure such that $\chi(T)\chi(T^*) = 0$ and such that for all ideals $\mathfrak{m} \in \mathcal{N}(\mathcal{P})$ and all $k \in \mathbb{Z}^+$:

$$H^1_{\mathcal{F}(\mathfrak{m})}(K, T/\beta^k T) \oplus (R/\beta^k)^{\chi(T^*)} \simeq H^1_{\mathcal{F}(\mathfrak{m})^*}(K, T^*[\beta^k]) \oplus (R/\beta^k)^{\chi(T)}.$$

The integer $\chi(T)$ is called the core ranks of $\boldsymbol{KS}(K, T, \mathcal{F}, \mathcal{P})$.

(ii) If $\chi(T) < 2$ then $\boldsymbol{KS}(K, T, \mathcal{F}, \mathcal{P})$ is a free $R-$module of rank $\chi(T)$.

(iii) Suppose $\chi(T) = 1$ and $\kappa \in \boldsymbol{KS}(K, T, \mathcal{F}, \mathcal{P})$, $\kappa \neq 0$ then:
$corank_R(H^1_{\mathcal{F}^*}(K, T^*) = min(r(\mathfrak{m})|k_\mathfrak{m} \neq 0)$.

Proof. Everything follows from [12] adapted to base field K: (i) is Theorem 5.2.5,(ii) is Theorem 5.2.10,(iii) is Theorem 5.2.12.(v).

□

1.6 Pre-Kolyvagin system over number fields

Following [13], we generalize the definition of pre-Kolyvagin systems:

Consider $\Gamma_\mathfrak{l} := G_\mathfrak{l}$ and

$$\Gamma_\mathfrak{m} := \prod_{\mathfrak{l}|\mathfrak{m}} \Gamma_\mathfrak{l}.$$

$\Gamma_\mathfrak{m}$ can be viewed either as the direct product of the residue fields or as the Galois group of the ray class field extension of conductor $\mathfrak{m}$ over K. Denote $P_\mathfrak{n}$, the composition

$$\mathbb{Z}[\Gamma_\mathfrak{m}] \to \mathbb{Z}[\Gamma_\mathfrak{n}] \to \mathbb{Z}[\Gamma_\mathfrak{m}].$$

[5]There is a small erratum concerning the use of theses hypotheses in [12] which is corrected in appendix B.

[6]The change (H.5) comparing to [12] 3.5 p.27 is armless, since for $\mathfrak{m}$ divided by elements in $\{\mathfrak{l}|J_\mathfrak{l} = R\}$, $T/I_{\mathfrak{m}^+}T = 0$ and all the additional modules that we consider are trivial.

As in [13], let $\mathcal{I}_{\mathfrak{m}}^{new} \subseteq I_{\mathfrak{m}}^{r(\mathfrak{m})^+}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ be the (cyclic) subgroup generated by monomials $\prod_{\mathfrak{l}|\mathfrak{m}^+}(\gamma_{\mathfrak{l}}-1)$ where each $\gamma_{\mathfrak{l}} \in \Gamma_{\mathfrak{l}}$. We have an isomorphism $\mathcal{I}_{\mathfrak{m}}^{new} \simeq \Gamma_{\mathfrak{m}^+}$ ([13], Proposition 4.2.(iv)), so we'll consider the classes for a Kolyvagin system to lie in $H^1_{\mathcal{F}(\mathfrak{m}^+)}(K, T/I_{\mathfrak{m}^+}T) \otimes \mathcal{I}_{\mathfrak{m}}^{new}$.

Let $\mathcal{I}_{\mathfrak{m}}^{old} \subseteq I_{\mathfrak{m}}^{r(\mathfrak{m})^+}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ be the subgroup generated by monomials $\prod_{i=1}^{r(\mathfrak{m})^+}(\gamma_{\mathfrak{l}_i}-1)$ where each $\gamma_{\mathfrak{l}_i} \in \Gamma_{\mathfrak{l}_i}$ for some $\mathfrak{l}_i$ dividing $\mathfrak{m}$ and

$$\{\mathfrak{l}_1, ..., \mathfrak{l}_{r(\mathfrak{m})^+}\} \neq \{\mathfrak{l} : \mathfrak{l}|\mathfrak{m}^+\}.$$

We also have the decomposition $I_{\mathfrak{m}}^{r(\mathfrak{m})^+}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} = \mathcal{I}_{\mathfrak{m}}^{new} \oplus \mathcal{I}_{\mathfrak{m}}^{old}$ ([13] Proposition 4.2 (i)) and we denote $\langle x \rangle^{new}$ the projection of $I_{\mathfrak{m}}^{r(\mathfrak{m})^+}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ onto $\mathcal{I}_{\mathfrak{m}}^{new}$.

Definition 1.6.1. *If $\mathfrak{m} \in \mathcal{N}$ and $\mathfrak{d} = \prod_{i=1}^{t} \mathfrak{l}_i$ divides $\mathfrak{m}^+$, let $M_{\mathfrak{m},\mathfrak{d}} = (m_{i,j})$ be the $t \times t$ matrix with entries in $J_{\mathfrak{m}}/J_{\mathfrak{m}}^2$ given by*

$$m_{i,j} = \begin{cases} P_{\mathfrak{m}/\mathfrak{d}}(Frob_{\mathfrak{l}_i} - 1) & \text{if } i = j \\ P_{\mathfrak{l}_j}(Frob_{\mathfrak{l}_i} - 1) & \text{if } i \neq j. \end{cases}$$

Definition 1.6.2. *Keep the setting of previous section.*

A pre-Kolyvagin system for $(K, T, \mathcal{F}, \mathcal{P})$ is a collection of cohomology classes:

$$\{\kappa_{\mathfrak{m}} \in H^1(K, T/J_{\mathfrak{m}^+}T) \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}, \mathfrak{m} \subseteq \mathcal{O}_K\}$$

such that:

(*i*) *If $\mathfrak{l} \nmid \mathfrak{m}$, then $\kappa(\mathfrak{m})_{\mathfrak{l}} \in H^1_{\mathcal{F}}(K_{\mathfrak{l}}, T/J_{\mathfrak{m}^+}T) \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$.*

(*ii*) *If $\mathfrak{l} \mid \mathfrak{m}^+$, then $(1 \otimes P_{\mathfrak{m}/\mathfrak{l}})\kappa(\mathfrak{m}) = \kappa(\mathfrak{m}/\mathfrak{l})P_{\mathfrak{m}/\mathfrak{l}}(1 - Frob_{\mathfrak{l}})$.*

(*iii*) *If $\mathfrak{l} \mid \mathfrak{m}^+$, then $\langle \kappa(\mathfrak{m})_{\mathfrak{l},tr} \rangle_{\mathfrak{m}}^{new} = (\phi_{\mathfrak{l}}^{fs} \otimes 1)(\langle \kappa(\mathfrak{m}/\mathfrak{l})_{\mathfrak{l}} \rangle_{\mathfrak{m}/\mathfrak{l}}^{new})$.*

(*iv*) *If $\mathfrak{l} \mid \mathfrak{m}^+$, then $\sum_{\mathfrak{n}|\mathfrak{m}^+} \langle \kappa(\mathfrak{m}/\mathfrak{n})_{\mathfrak{l},f} \rangle_{\mathfrak{m}/\mathfrak{n}}^{new}) \mathcal{D}_{\mathfrak{n}} = 0$.*

(*v*) *If $\mathfrak{l} \mid \mathfrak{m}/\mathfrak{m}^+$, then $\langle \kappa(\mathfrak{m}) \rangle_{\mathfrak{m}}^{new} = \langle \kappa(\mathfrak{m}/\mathfrak{l}) \rangle_{\mathfrak{m}/\mathfrak{l}}^{new}$.*

The equalities in (ii) and (iv) lie in $H^1(K, T/J_{\mathfrak{m}^+}T) \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ since we have a natural map $H^1(K, T/J_{\mathfrak{m}^+}T) \to H^1(K, T/J_{\mathfrak{m}\mathfrak{n}^+}T)$ for any

ideal $\mathfrak{n}$ *prime to* $\mathfrak{m}$.

We denote by $\boldsymbol{PKS}(K,T,\mathcal{F},\mathcal{P})$*, the module of pre-Kolyvagin system for* $(K,T,\mathcal{F},\mathcal{P})$.

Proposition 1.6.3. *We have an isomorphism of R-module:*

$$\boldsymbol{PKS}(K,T,\mathcal{F},\mathcal{P}) \simeq \boldsymbol{KS}(K,T,\mathcal{F},\mathcal{P})$$
$$\kappa_{\mathfrak{n}} \to \tilde{\kappa_{\mathfrak{n}}} := \sum_{\mathfrak{d}|\mathfrak{n}^+} \kappa_{\mathfrak{n}/\mathfrak{d}} \mathcal{D}_{\mathfrak{n},\mathfrak{d}}$$

with $\kappa_1 = \tilde{\kappa_1}$.

Proof. The proof is of injectivity is the same as in [13] Proposition 6.5 with the following remarks:

• If A is a R-module, and $x \in A \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ is such that $P_{\mathfrak{m}/\mathfrak{l}}(x) = 0$ for all $\mathfrak{l}|\mathfrak{m}^+$ then $x \in A \otimes \mathcal{I}_{\mathfrak{m}}^{new}$. (We don't need any more hypothesis on $H^1(K,T)$ unlike in [13], where they use that $H^1(\mathbb{Q},T)$ is a free $\mathbb{Z}_p$-module). The proof of this fact is made in the appendix.

• The map $H^1(K,T/J_{\mathfrak{m}^+}T) \to H^1(K,T/J_{\mathfrak{m}\mathfrak{n}^+}T)$ sends $H^1_{\mathcal{F}}(K,T/J_{\mathfrak{m}^+}T)$ to $H^1_{\mathcal{F}}(K,T/J_{\mathfrak{m}\mathfrak{n}^+}T)$ by definition of a propagated local condition ([12] example 1.1.2).

• The following diagram, with $\mathfrak{l}|\mathfrak{m}^+$ and $\mathfrak{m}$ prime to p is commutative (it's easily seen by coming back to the definition of $\phi_{\mathfrak{l}}^{fs}$):

$$\begin{array}{ccc} H^1_f(K_{\mathfrak{l}},T/J_{\mathfrak{m}^+}T) & \xrightarrow{\phi_{\mathfrak{l}}^{fs}} & H^1_{tr}(K_{\mathfrak{l}},T/J_{\mathfrak{m}^+}T)\otimes\Gamma_{\mathfrak{l}} \\ \downarrow & & \downarrow \\ H^1_f(K_{\mathfrak{l}},T/J_{\mathfrak{m}\mathfrak{n}^+}T) & \xrightarrow{\phi_{\mathfrak{l}}^{fs}} & H^1_{tr}(K_{\mathfrak{l}},T/J_{\mathfrak{m}\mathfrak{n}^+}T)\otimes\Gamma_{\mathfrak{l}}. \end{array}$$

The proof of surjectivity is done by induction:

Let $\tilde{\kappa_{\mathfrak{n}}} \in \mathbf{KS}(K,T,\mathcal{F},\mathcal{P})$ since $\mathcal{D}_{\mathfrak{n},1} = 1$, we define by induction an element $\kappa_{\mathfrak{n}}$ such that:

$$\kappa_1 = \tilde{\kappa_1},$$

$$\kappa_{\mathfrak{n}} = \tilde{\kappa_{\mathfrak{n}}} - \sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{d}\neq 1} \kappa_{\mathfrak{n}/\mathfrak{d}} \mathcal{D}_{\mathfrak{n},\mathfrak{d}},$$

and we want to prove that $\kappa_{\mathfrak{n}} \in \mathbf{PKS}(K,T,\mathcal{F},\mathcal{P})$.

We check by induction on $r(\mathfrak{n})$ the five properties of a pre-Kolyvagin system:

Property (i) is immediate.

Property (ii): if $\mathfrak{l}|\mathfrak{n}^+$:

$$\begin{aligned}
(1\otimes P_{\mathfrak{n}/\mathfrak{l}})\kappa_{\mathfrak{n}} &= (1\otimes P_{\mathfrak{n}/\mathfrak{l}})(\tilde{\kappa_{\mathfrak{n}}}) - (1\otimes P_{\mathfrak{n}/\mathfrak{l}})(\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{d}\neq 1}\kappa_{\mathfrak{n}/\mathfrak{d}}\mathcal{D}_{\mathfrak{n},\mathfrak{d}})\\
&= -(1\otimes P_{\mathfrak{n}/\mathfrak{l}})(\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{d}\neq 1}\kappa_{\mathfrak{n}/\mathfrak{d}}\mathcal{D}_{\mathfrak{n},\mathfrak{d}})\\
&= -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}|\mathfrak{d}}\kappa_{\mathfrak{n}/\mathfrak{d}}P_{\mathfrak{n}/\mathfrak{l}}(\mathcal{D}_{\mathfrak{n},\mathfrak{d}})\\
&\qquad -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}\nmid\mathfrak{d},\mathfrak{d}\neq 1}(1\otimes P_{\mathfrak{n}/\mathfrak{l}})(\kappa_{\mathfrak{n}/\mathfrak{d}})P_{\mathfrak{n}/\mathfrak{l}}(\mathcal{D}_{\mathfrak{n},\mathfrak{d}})\\
(a)\qquad &= -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}|\mathfrak{d}}\kappa_{\mathfrak{n}/\mathfrak{d}}P_{\mathfrak{n}/\mathfrak{d}}(Fr_{\mathfrak{l}}-1)(\mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}/\mathfrak{l}})\\
&\qquad -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}\nmid\mathfrak{d},\mathfrak{d}\neq 1}(1\otimes P_{\mathfrak{n}/\mathfrak{l}})(\kappa_{\mathfrak{n}/\mathfrak{d}})(\mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}})\\
(b)\qquad &= -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}|\mathfrak{d}}\kappa_{\mathfrak{n}/\mathfrak{d}}P_{\mathfrak{n}/\mathfrak{d}}(Fr_{\mathfrak{l}}-1)(\mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}/\mathfrak{l}})\\
&\qquad -\sum_{\mathfrak{d}|\mathfrak{n}^+,\mathfrak{l}\nmid\mathfrak{d},\mathfrak{d}\neq 1}\kappa_{\mathfrak{n}/\mathfrak{d}\mathfrak{l}}P_{\mathfrak{n}/\mathfrak{d}}(1-Fr_{\mathfrak{l}})(\mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}})\\
&= \kappa_{\mathfrak{n}/\mathfrak{l}}P_{\mathfrak{n}/\mathfrak{l}}(Fr_{\mathfrak{l}}-1),
\end{aligned}$$

where (a) holds since:

$$P_{\mathfrak{n}/\mathfrak{l}}(\mathcal{D}_{\mathfrak{n},\mathfrak{d}}) = \begin{cases} P_{\mathfrak{n}/\mathfrak{d}}(Fr_{\mathfrak{l}}-1)\mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}/\mathfrak{l}} & \text{if } \mathfrak{l}|\mathfrak{d}\\ \mathcal{D}_{\mathfrak{n}/\mathfrak{l},\mathfrak{d}} & \text{if } \mathfrak{l}\nmid\mathfrak{d}, \end{cases}$$

and (b) holds by induction.

Property (iii) is induction using property (i) of a pre-Kolyvagin system and property (ii) of a Kolyvagin system.

Property (iv) follows by projecting the equality $\tilde{\kappa_{\mathfrak{n}}} := \sum_{\mathfrak{d}|\mathfrak{n}^+}\kappa_{\mathfrak{n}/\mathfrak{d}}\mathcal{D}_{\mathfrak{n},\mathfrak{d}}$ on $H^1_f(K_{\mathfrak{l}},T/I_{\mathfrak{m}}T)\otimes\mathcal{I}^{new}_{\mathfrak{m}}$ since $\langle\kappa_{\mathfrak{n}/\mathfrak{d}}\mathcal{D}_{\mathfrak{n},\mathfrak{d}}\rangle^{new}_{\mathfrak{n}} = \langle\kappa_{\mathfrak{n}/\mathfrak{d}}\rangle^{new}_{\mathfrak{n}/\mathfrak{d}}\mathcal{D}_{\mathfrak{d}}$ and since

$$(\tilde{\kappa_{\mathfrak{n}}})_{\mathfrak{l},f} = 0.$$

Property (v) is immediate by induction and using property (i) of a Kolyvagin system.

□

Remark: it's easy to see that a Kolyvagin system only depends on its values on ideals in $\mathcal{N}(\mathcal{P})$. By the previous isomorphism, it is also true for a

pre-Kolyvagin system even if it isn't clear at first sight since we haven't the equality $\kappa_{\mathfrak{m}} = \kappa_{\mathfrak{m}}^{+}$.

Finally, we end this section with a proposition that will be useful later for our application of this machinery.

Definition 1.6.4. *If $\mathfrak{m} \in \mathcal{N}$, let $\mathfrak{S}(\mathfrak{m})$ denote the set of permutations of the primes dividing $\mathfrak{m}^+$, and let $\mathfrak{S}_1(\mathfrak{m}) \subset \mathfrak{S}(\mathfrak{m})$ be the subset:*

$$\mathfrak{S}_1(\mathfrak{m}) := \{\sigma \in \mathfrak{S}(\mathfrak{m}) : \text{ the primes not fixed by } \sigma \text{ form a single } \sigma\text{-orbit } \}.$$

If $\sigma \in \mathfrak{S}(\mathfrak{m})$, let $\mathfrak{d}_\sigma := \prod_{\substack{\mathfrak{l} | \mathfrak{m}^+ \\ \sigma(\mathfrak{l}) \neq \mathfrak{l}}} \mathfrak{l}$ the product of all the primes not fixed by σ, and define:

$$\Pi(\sigma) := \prod_{\mathfrak{q} | \mathfrak{d}_\sigma} P_{\mathfrak{q}}(Frob_{\sigma(\mathfrak{q})} - 1).$$

Proposition 1.6.5. *Property (iv) of a pre-Kolyvagin system can be replaced by*

(iv)' If $\mathfrak{l} \mid \mathfrak{m}^+$, then $\langle \kappa(\mathfrak{m})_{\mathfrak{l},f} \rangle_{\mathfrak{m}}^{new} = \sum_{\substack{\sigma \in \mathfrak{S}_1(\mathfrak{m}) \\ \sigma(\mathfrak{l}) \neq \mathfrak{l}}} \langle \kappa(\mathfrak{m}/\mathfrak{d}_\sigma)_{\mathfrak{l},f} \rangle_{\mathfrak{m}/\mathfrak{d}_\sigma}^{new} \Pi(\sigma)$.

Proof. This is the same proof as Lemma 6.8 in [13], replacing the primes (n, l, d) in $\mathbb{Q}$ by primes $(\mathfrak{m}, \mathfrak{l}, \mathfrak{d})$ in K. □

1.7 The Kolyvagin system $\mathbf{KS}(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$

We come back to our main settings where K is defined in the beginning and we work with the $\mathbb{Z}_p[G_K]$-module $\mathbb{Z}_p(1) \otimes \psi$. The module $\mathbb{Z}_p(1) \otimes \psi$ is a one dimensional representation over $\mathbb{Z}_p$ with G_K acting via the product of ψ and the cyclotomic character. The aim of this section is to study in details $\mathbf{KS}(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$ for a well chosen Selmer structure $\mathcal{F}_f$ defined in 1.7.2. We explicit first the different modules and morphisms (Proposition 1.7.1) and we show then that the core rank of $\mathbf{KS}(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$ is one (Proposition 1.7.5). The choice of the particular Selmer structure $\mathcal{F}_f$ will be clear in section 1.10 when we show that both hand sides of the formulas of Theorem 1.4.1 form a pre-Kolyvagin system with respect to $\mathcal{F}_f$ (Propositions 1.10.1 and 1.10.2).

We suppose $p \neq 2$ and for the notations, if M is a module, denote $\hat{M}$ its completion by power of p (ie. $\hat{M} := \varprojlim_n M/p^n M$).

Proposition 1.7.1. *Suppose $\mathfrak{l} \nmid p$, we have the following isomorphisms:*

(i) $H^1(K, \mathbb{Z}_p(1) \otimes \psi) \simeq \hat{H}^{\times -}$.

(ii) $H^1(K_\mathfrak{l}, \mathbb{Z}_p(1) \otimes \psi) \simeq \hat{H}_\mathfrak{l}^{\times -}$, where $H_\mathfrak{l} := H \otimes_K K_\mathfrak{l} \simeq \bigoplus_{\lambda | \mathfrak{l}} H_\lambda$.

(iii) $H_f^1(K_\mathfrak{l}, \mathbb{Z}_p(1) \otimes \psi) \simeq \hat{\mathcal{O}_{H_\mathfrak{l}}^{\times}}^{-}$, where $\mathcal{O}_{H_\mathfrak{l}} := \mathcal{O}_H \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{l}} \simeq \bigoplus_{\lambda | \mathfrak{l}} \mathcal{O}_{H_\lambda}$.

(iv) If $\mathfrak{l}$ *is split in* H, $\mathfrak{l} = \lambda\lambda^\sigma$, *choose* $\pi_\mathfrak{l}$ *a generator of* $\mathfrak{l}$, *then*

$$H^1_{tr}(K_\mathfrak{l}, \mathbb{Z}_p(1) \otimes \psi) \text{ is the subgroup generated by } (\pi_\mathfrak{l}, \pi_\mathfrak{l}^{-1}).$$

The finite singular morphism is defined by:

$$H^1_f(K_\mathfrak{l}, \mathbb{Z}_p(1) \otimes \psi) \xrightarrow{\sim} H^1_{tr}(K_\mathfrak{l}, \mathbb{Z}_p(1) \otimes \psi) \otimes \Gamma_\mathfrak{l}$$

$$\phi^{fs}_\mathfrak{l} : (x_\lambda, x_{\lambda^\sigma}) \to (\pi_\mathfrak{l}, \pi_\mathfrak{l}^{-1}) \otimes [x_\lambda^{-1}, K_\mathfrak{l}(\mathfrak{l})].^7$$

Proof. Proof of (i): We use the inflation-restriction map:

$H^1(H/K, (\mu_p^k \otimes \psi)^{G_H}) \hookrightarrow H^1(K, \mu_p^k \otimes \psi) \to H^1(H, \mu_p^k \otimes \psi)^{Gal(H/K)} \to H^2(H/K, (\mu_p^k \otimes \psi)^{G_H})$.

Since $\mathrm{Gal}(H/K)$ has order 2 and $p \neq 2$, we have $H^i(H/K, \mu_p^k \otimes \psi) = 0$ and $H^1(K, \mu_p^k \otimes \psi) \simeq H^1(H, \mu_p^k \otimes \psi)^{Gal(H/K)} \simeq (H^1(H, \mu_p^k) \otimes \psi)^{Gal(H/K)}$

Now, if L is a field with algebraic closure $\overline{L}$. We have the following short exact sequence:

$$1 \to \mu_{p^k} \to \overline{L}^* \to \overline{L}^* \to 1.$$

By Hilbert 90, taking the long exact sequence in group cohomology, we have $H^1(L, \mu_p^k) \simeq (L^*/(L^*)^{p^k}$.

As a remark, the map $L^*/(L^*)^{p^k} \to H^1(L, \mu_p^k)$ is given by:

$$x \longrightarrow (g \to g(\beta_x)/\beta_x),$$

where β_x is any p^k-root of x in $\overline{L}$.

(ii) is similar.

(iii) is similar, using the following property:

If L is a local field with residue field of characteristic prime to p, then $H^1_f(L, \mu_p^k) \simeq (\mathcal{O}_L^*/(\mathcal{O}_L^*)^{p^k})$.

It is a well-known result proven by using the short exact sequence:

$$1 \to \mu_{p^k} \to \mathcal{O}^*_{L,unr} \to \mathcal{O}^*_{L,unr} \to 1.$$

(iv) The map $(x_\lambda, x_{\lambda^\sigma}) \to (\pi_\mathfrak{l}, \pi_\mathfrak{l}^{-1}) \otimes [x_\lambda, K_\mathfrak{l}(\mathfrak{l})]$ $\varphi^{fs}_\mathfrak{l}$ doesn't depend on the choice of λ versus λ^σ and is an isomorphisms of free rank one module over $\mathbb{Z}_p/(\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{l}) - 1)\mathbb{Z}_p$. (by Lemma 1.2.3 of [12] for $\phi^{fs}_\mathfrak{l}$ and by Hensel Lemma for $\varphi^{fs}_\mathfrak{l}$.)

We recall now the definition of $\phi^{fs}_\mathfrak{l}$ in [12] section 1.2:

$\phi^{fs}_\mathfrak{l}$ is the composition:

[7] As mentioned in Section 2, this formula isn't the same as in [13]. The Definition 5.1 in [13] should be corrected to agree with Definition 1.2.2 in [12].

$$H^1_f(K_\mathfrak{l}, \mu_p^k \otimes \psi) \xrightarrow{\sim} \mu_p \xrightarrow{Id} \mu_p \xleftarrow{\sim} H^1_s(K_\mathfrak{l}, \mu_p^k \otimes \psi) \otimes \Gamma_\mathfrak{l},$$

where the first isomorphism is done by evaluating the cocycle class at $\mathrm{Frob}_\mathfrak{l}$ and the later by sending the class $f \otimes \gamma$ to $f(\gamma)$. Choose λ a prime in H above $\mathfrak{l}$ and write $g_x := [x_\lambda, K_\mathfrak{l}(\mathfrak{l})]^{-1}$. Write $\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{l}) - 1 = p^k.v$ where v is prime with p, by (iii) we have to prove:

$$\mathrm{Frob}_\mathfrak{l}(\beta_x)/\beta_x = g_x(\beta_\pi)/\beta_\pi,$$

where β_x (resp. β_π) is a p^k-roots of x_λ (resp.$\pi_\mathfrak{l}$).

Choose α_x a $p^k v$-roots of x_λ and α_π a $p^k v$- roots of $\pi_\mathfrak{l}$. As a remark, α_π is an uniformizer in $K_\mathfrak{l}(\mathfrak{l})$, and $\mathbf{N}_{K_\mathfrak{l}(\mathfrak{l})^{unr}/K_\mathfrak{l}^{unr}}(\alpha_x) = x_\lambda$ since the $p^k v$-roots of unity belong to $K_\mathfrak{l}$ by Hensel lemma.

We are in the settings of the corollary of Theorem 2 of [18] p.208 that shows:

$$\mathrm{Frob}_\mathfrak{l}(\alpha_x)/\alpha_x = g_x(\alpha_\pi)/\alpha_\pi$$

.

The result follows by taking the v-power on both sides. □

Definition 1.7.2. *For any prime $p \neq 2$ consider the Selmer structure $\mathcal{F}_f$ for the G_K-module $T := \mathbb{Z}_p(1) \otimes \psi$ to be:*

- $\Sigma(\mathcal{F}_f) = \{\infty, \mathfrak{p}|p\}$,
- $H^1_{\mathcal{F}_f}(K_\mathfrak{p}, T) = (\bigoplus_{\lambda|\mathfrak{p}} \mathcal{O}_{H_\lambda})^\psi$
- $H^1_{\mathcal{F}_f}(\mathbb{C}, T) = H^1(\mathbb{C}, T) = 0$.

Let $\mathcal{P} := \{$ primes in K coprime with $\mathfrak{a}\mathfrak{f}p$ that split in $H\}$.

As promised, the notations are coherent between the settings and notations in section 1.5.

Proposition 1.7.3. ***KS***$(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$ *satisfies (H.0) to (H.6).*

Proof. With the notations of section 1.5, we have:

$$T/\beta T \simeq \mu_p \otimes \psi \text{ and } T^*[\beta] \simeq \mathbb{Z}/p\mathbb{Z} \otimes \psi.$$

(H.0),(H.1),(H.5) and (H.6) are immediate. For (H.2), we take $\rho = id$. (H.3) follows from the fact that $p \neq 2$ so $\mu_p \otimes \psi$ and $\mathbb{Z}/p\mathbb{Z} \otimes \psi$ have a non trivial Galois action. (H.4) follows by the incompatibility of the action of G_K on μ_p and $\mathbb{Z}/p\mathbb{Z}$.

□

Proposition 1.7.4. *The core rank $\chi(T)$ of* ***KS***$(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$ *is one.*

Proof. By [12] Proposition 2.3.5, applied to $T^*[p] \simeq \mathbb{Z}/p\mathbb{Z} \otimes \psi$, we have:

$$\begin{aligned} &length(H^1_{\mathcal{F}_f}(K, T/pT)) - length(H^1_{\mathcal{F}^*_f}(K, T^*[p])) \\ &\quad = length(H^0(K, T/pT) - length(H^0(K, T^*[p]) \\ &\quad + \sum_{\mathfrak{m} \in \Sigma(\mathcal{F}_f)} length(H^0(K_\mathfrak{m}, T^*[p])) - length(H^1_{\mathcal{F}^*_f}(K_\mathfrak{m}, T^*[p])). \end{aligned}$$

We compute now the two parts of the inequality. In our case, $\Sigma(\mathcal{F}_f)$ is the place at infinity and all places over p.

By the properties of the core rank in Proposition 1.5.3:
$length(H^1_{\mathcal{F}_f}(K, T/pT)) - length(H^1_{\mathcal{F}^*_f}(K, T^*[p])) = \chi(T) - \chi(T^*)$.

On the other hand:
$\bullet H^0(K, T/pT) = H^0(K, T^*[p]) = 0$.
$\bullet H^0(\mathbb{C}, T^*[p]) \simeq \mathbb{Z}/p\mathbb{Z}$ and $H^1_{\mathcal{F}^*_f}(\mathbb{C}, T^*[p]) = 0$.
• For the primes $\mathfrak{p}$ above p, denote $G_\mathfrak{p} := \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$.
By definition of the dual Selmer structure:
$H^1_{\mathcal{F}^*_f}(K_\mathfrak{p}, T^*[p]) = (\bigoplus_{\lambda|\mathfrak{p}} Hom(G_\lambda/I_\lambda, \mathbb{Z}/p\mathbb{Z}))^\psi$.

$$H^0(K_\mathfrak{p}, T^*[p]) = (T^*[p])^{G_\mathfrak{p}}.$$

In order to understand the action of $G_\mathfrak{p}$ on T^* and $T^*[p]$, we have to consider the different cases where $\mathfrak{p}$ is inert, splits or ramifies in H:

1/ $\mathfrak{p}$ is inert or ramifies in H. Then the action of $G_\mathfrak{p}$ is non trivial on T^* and:

$$(T^*)^{G_\mathfrak{p}} = (T^*[p])^{G_\mathfrak{p}} = 0,$$

In this case, there is only one prime λ over $\mathfrak{p}$ in H and

$$H^1_{\mathcal{F}^*_f}(K_\mathfrak{p}, T^*[p]) = (Hom(G_\lambda/I_\lambda, \mathbb{Z}/p\mathbb{Z})^\psi,$$

where the action of σ is given by conjugation.

Since $\sigma^{-1} g \sigma = g$ for any $g \in G_\lambda/I_\lambda$,(recall that the action of g is given on roots of unity) it follows that for $f \in Hom(G_\lambda/I_\lambda, \mathbb{Z}/p\mathbb{Z})^\psi$ we have

$$\sigma.f(g) = -f(g) = f(\sigma^{-1} g \sigma) = f(g).$$

It follows that $f = 0$ by assumption $p \neq 2$ and we have finally

$$Hom(G_\lambda/I_\lambda, \mathbb{Z}/p\mathbb{Z})^\psi = 0.$$

2/ $\mathfrak{p}$ splits in H, write $\mathfrak{p} = \lambda_1 \lambda_2$. In this case $G_\mathfrak{p}$ acts trivially on T^* and $T^*[p]$ and:

$$H^0(K_\mathfrak{p}, T^*[p]) \simeq \mathbb{Z}/p\mathbb{Z},$$

$$H^1_{\mathcal{F}^*_f}(K_\mathfrak{p}, T^*[p]) \simeq (\bigoplus_{\lambda_i|\mathfrak{p}} Hom(G_{\lambda_i}/I_{\lambda_i}, \mathbb{Z}/p\mathbb{Z}))^\psi \simeq Hom(G_{\lambda_1}/I_{\lambda_1}, \mathbb{Z}/p\mathbb{Z}),$$

where the last isomorphism holds since the action of σ is just sending elements in $G_{\lambda_1}/I_{\lambda_1}$ to $G_{\lambda_2}/I_{\lambda_2}$ and reciprocally.

It follows that $H^1_{\mathcal{F}^*_f}(K_\mathfrak{p}, T^*[p])$ has length one since $G_{\lambda_1}/I_{\lambda_1} \simeq \hat{\mathbb{Z}}$.

Finally, in both cases:

$$length(H^0(K_\mathfrak{p}, T^*[p])) - length(H^1_{\mathcal{F}^*}(K_\mathfrak{p}, T^*[p])) = 0,$$

and

$$\chi(T) - \chi(T^*) = 1.$$

Since either $\chi(T)$ or $\chi(T^*)$ is equal is 0 by Proposition 1.5.3, we have $\chi(T) = 1$.

□

Proposition 1.7.5. *$corank(H^1_{\mathcal{F}^*}(K, T^*)) = 0$.*

Proof. Using the same arguments as in the proof of 1.7.1, we have the following isomorphisms:

$H^1(K, T^*) \simeq Hom(G_H, \mathbb{Q}_p/\mathbb{Z}_p)^\psi$,

$H^1(K_\mathfrak{l}, T^*) \simeq \bigoplus_{\lambda|\mathfrak{l}} Hom(G_{H_\lambda}, \mathbb{Q}_p/\mathbb{Z}_p)^\psi$,

$H^1_s(K, T^*) \simeq \bigoplus_{\lambda|\mathfrak{l}} Hom(I_\lambda, \mathbb{Q}_p/\mathbb{Z}_p)^\psi$, where I_λ is the inertial subgroup at λ.

Since the condition at $\mathfrak{p}|p$ for $\mathcal{F}$ is the relaxed condition, we have:

$$H^1_{\mathcal{F}^*}(K, T^*) \subseteq Hom(Gal(L/H), \mathbb{Q}_p/\mathbb{Z}_p)^\psi,$$

where L is the Hilbert class field of H.

By global class field theory, $\mathrm{Gal}(L/H) \simeq Cl(H)$ and

$$H^1_{\mathcal{F}^*}(K, T^*) \subseteq Hom(Cl(H)^\psi, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since $Cl(H)$ is finite:

$$corank(H^1_{\mathcal{F}^*}(K, T^*)) := dim_{\mathbb{Q}_p}(Hom(H^1_{\mathcal{F}^*}(K, T^*)), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p = 0.$$

□

1.8 Formal properties of $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$

We have now the formal tools to complete the proof of Theorem 1.4.1. Using the explicit formula of the finite singular morphism in Proposition 1.7.1, it is straightforward (even though quite laborious) to show that the right-hand side of Theorem 1.4.1 is a pre-Kolyvagin system for $\mathcal{F}_f$. Nevertheless, the left-hand side asks for some more work. It's not even obvious that it belongs to the right module for a pre-Kolyvagin system. This sections is devoted to prove that the element $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ belongs to $H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}$.

Recall the definition:

$$\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = \sum_{\sigma \in Gal(H(\mathfrak{m})/H)} \sigma(\alpha(\mathfrak{m})) \otimes \sigma \in H(\mathfrak{m})^* \otimes \mathbb{Z}[\Gamma_{\mathfrak{m}}].$$

Any element $\gamma \in \mathrm{Gal}(H(\mathfrak{m})/K)$ acts on left of $H(\mathfrak{m})^* \otimes \mathbb{Z}[\Gamma_{\mathfrak{m}}]$.

Lemma 1.8.1.

$$\gamma.\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = \psi(\gamma).\theta'(\psi, \mathfrak{m}, \mathfrak{a}).\gamma(\mathfrak{m})^{-1}.$$

Proof. Change of variable. □

Lemma 1.8.2. *If* $\mathfrak{n}|\mathfrak{m}$ *then:*

$$(1 \otimes P_{\mathfrak{n}})\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = \theta'(\psi, \mathfrak{n}, \mathfrak{a}). \prod_{\mathfrak{p}|\mathfrak{m}/\mathfrak{n}} (1 - \psi(\mathfrak{p}) Frob_{\mathfrak{p}}).$$

Proof. Writte $\mathfrak{m} = \mathfrak{l}\mathfrak{n}$,

$$\begin{aligned}
(1 \otimes P_{\mathfrak{n}})\theta'(\psi, \mathfrak{m}, \mathfrak{a}) &= \sum_{\sigma \in \Gamma_{\mathfrak{n}}} (N_{\mathfrak{m},\mathfrak{n}} \sigma(\alpha(\mathfrak{m})) \otimes \sigma) \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{n}}} (\prod_{\mathfrak{p}|\mathfrak{l}} (1 - \mathrm{Frob}_p^{-1}) \sigma(\alpha(\mathfrak{n})) \otimes \sigma) \\
&= \prod_{\mathfrak{p}|\mathfrak{l}} (1 - \mathrm{Frob}_p^{-1}).\theta'(\psi, \mathfrak{n}, \mathfrak{a}) \\
&= \theta'(\psi, \mathfrak{n}, \mathfrak{a}). \prod_{\mathfrak{p}|\mathfrak{l}} (1 - \psi(\mathfrak{p}) \mathrm{Frob}_p) \text{ (Lemma 1.8.1).}
\end{aligned}$$

□

Lemma 1.8.3. *The following equality holds:*

$$\theta'(\psi, \mathfrak{m}, \mathfrak{a}) = \sum_{\sigma \in \Gamma_{\mathfrak{m}}} \sigma(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{l} | \mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1).P_{\mathfrak{m}^-}(\sigma)$$

$$- \sum_{\mathfrak{n} | \mathfrak{m}^+, \mathfrak{n} \neq \mathfrak{m}^+} \left(\theta'(\psi, \mathfrak{n}\mathfrak{m}^-, \mathfrak{a}). \prod_{\mathfrak{l} | \mathfrak{m}^+/\mathfrak{n}} P_{\mathfrak{m}/\mathfrak{n}}(Frob_{\mathfrak{l}} - 1) \right).$$

Proof. It follows directly by developing

$$\sum_{\sigma \in \Gamma_{\mathfrak{m}}} \sigma(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{p} | \mathfrak{m}^+} (P_{\mathfrak{p}}(\sigma) - 1).P_{\mathfrak{m}^-}(\sigma)$$

and using Lemma 1.8.2.

□

Proposition 1.8.4. *The element $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ belongs to $H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}$.*

Proof. Its is clear by induction using the previous lemma.

□

1.9 The leading term of $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$

We study now the image of $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ in $H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$ denoted $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$. The key is to understand their local behaviors, to see that the collection $\{2^{r(\mathfrak{m}^-}\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})\}$ forms a pre-Kolyvagin system. To do so, we use the norm map compatibilities between the $\alpha(\mathfrak{m})$ as an Euler system. Using these compatibilities and a method due to Kolyvagin, we construct a collection of *derivative classes* in $H^1(K, \mathbb{Z}_p(1) \otimes \psi)$ for which all the local behaviors are known. Finally, we show the relation between these classes and $\theta'(\psi, \mathfrak{m}, \mathfrak{a})$ (Proposition 1.9.7).

Let start with the method of Kolyvagin to construct derivative classes in $H^1(K, \mathbb{Z}_p(1) \otimes \psi)$ from the Euler system described in section 3. We follow the usual construction as made in details in [16] chap IV.

For any prime $\mathfrak{l} \in \mathcal{N}_{\mathfrak{f}}$, choose a generator $\gamma_{\mathfrak{l}}$ of $\Gamma_{\mathfrak{l}}$ and define:

$$D_{\mathfrak{l}} := \sum_{i=1}^{N_{K/\mathbb{Q}}\mathfrak{l}-2} i\gamma_{\mathfrak{l}}^i \in \mathbb{Z}[\Gamma_{\mathfrak{l}}], D_{\mathfrak{m}} = \prod_{\mathfrak{l} | \mathfrak{m}} D_{\mathfrak{l}} \in \mathbb{Z}[\Gamma_{\mathfrak{m}}],$$

$$N_{\mathfrak{l}} := \sum_{i=1}^{N_{\mathfrak{l}}-1} \gamma_{\mathfrak{l}}^i \in \mathbb{Z}[\Gamma_{\mathfrak{l}}].$$

Lemma 1.9.1.

$$(\gamma_\mathfrak{l} - 1)D_\mathfrak{l} = N_{K/\mathbb{Q}}\mathfrak{l} - 1 - N_\mathfrak{l}.$$

Proof. This is a simple computation. □

Remark: the previous property is the only property that we use in the construction of the derivative classes. Any other element in the group ring with this property leads to the same construction.

Consider the element:

$$\beta(\mathfrak{m}) := D_\mathfrak{m}\alpha(\mathfrak{m}).$$

Let $n(\mathfrak{m})$ be the maximal divisor of $\gcd_{\mathfrak{l}|\mathfrak{m}}(\mathbf{N}_{K/\mathbb{Q}}\mathfrak{l} - 1)$ prime to 6.

Lemma 1.9.2. $\beta(\mathfrak{m}) \in (H(\mathfrak{m})^*/(H(\mathfrak{m})^{*n(\mathfrak{m})})^{\Gamma_\mathfrak{m}}$.

Proof. By induction, since it is clear for $\beta(\mathfrak{1})$:

For all $\mathfrak{l}$, consider $\gamma_\mathfrak{l}$ as an element of $\Gamma_\mathfrak{m}$, and write $\mathfrak{m} = \mathfrak{l}\mathfrak{n}$ we have:

$$\begin{aligned}
(\gamma_\mathfrak{l} - 1)D_\mathfrak{m}\alpha(\mathfrak{m}) &= (\gamma_\mathfrak{l} - 1)D_\mathfrak{l}D_\mathfrak{n}\alpha(\mathfrak{m}) \\
&= D_\mathfrak{n}(N_{K/\mathbb{Q}}\mathfrak{l} - 1 - N_\mathfrak{l})\alpha(\mathfrak{m}) \text{ (Lemma 1.9.1)} \\
&= D_\mathfrak{n}(-N_\mathfrak{l})\alpha(\mathfrak{m}) \text{ (by definition of } n(\mathfrak{m})) \\
&= (\mathrm{Frob}_\mathfrak{l}^{-1} - 1)D_\mathfrak{n}\alpha(\mathfrak{n}) \text{ (by prop. 1.3.5)} \\
&= 0 \text{ (by the induction hypothesis).}
\end{aligned}$$

□

Proposition 1.9.3. *The element $\beta(\mathfrak{m})$ has a canonical inverse image under the map $H^*/(H)^{*n(\mathfrak{m})} \to (H(\mathfrak{m})^*/(H(\mathfrak{m})^{*n(\mathfrak{m})})^{\Gamma_\mathfrak{m}}$.*

Proof. Since $H(\mathfrak{m})$ doesn't contain $n(\mathfrak{m})$ roots of unity, the inflation restriction exact sequence shows that the natural map

$$H^*/(H)^{*n(\mathfrak{m})} \to (H(\mathfrak{m})^*/(H(\mathfrak{m})^{*n(\mathfrak{m})})^{\Gamma_\mathfrak{m}}$$

is an isomorphism.

Remark: the same property stays true if we define

$$n(\mathfrak{m}) := gcd_{\mathfrak{l}|\mathfrak{m}}(\mathbf{N}_{K/\mathbb{Q}}\mathfrak{l} - 1).$$

In this case, the map $H^*/(H)^{*n(\mathfrak{m})} \to (H(\mathfrak{m})^*/(H(\mathfrak{m})^{*n(\mathfrak{m})})^{\Gamma_\mathfrak{m}}$ is NOT an isomorphism but Lemma V.4.13 of [16] shows, using the norm compatibilities of α as an Euler system, that such a canonical inverse exits. Nevertheless, since we inverse 6 in our formula, the weaker property is sufficient for our purpose.

□

Definition 1.9.4. *We define $\kappa(\mathfrak{m})$ to be the canonical inverse image of $\beta(\mathfrak{m})$.*

The elements $\kappa(\mathfrak{m})$ are the derivative classes associated to the Euler system $\alpha(\mathfrak{m})$. They depend on the choice of the generators $\gamma_{\mathfrak{l}}$ that we chose. Nevertheless, in what follow, we consider the elements $\kappa(\mathfrak{m}) \otimes \prod_{\mathfrak{l}|\mathfrak{m}}(\gamma_{\mathfrak{l}} - 1)$ in $H^*/(H)^{*n(\mathfrak{m})} \otimes I_{\mathfrak{m}}^{r(\mathfrak{m})}/I_{\mathfrak{m}}^{r(\mathfrak{m})+1}$. These elements don't depend on any choice.

As a remark we haven't made any choice of prime p to consider our derivative classes. To be more precise, the derivative classes associated to the module $\mathbb{Z}_p \otimes \psi$ are the classes $\kappa(\mathfrak{m})$ considered as elements in

$$H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m})}/I_{\mathfrak{m}}^{r(\mathfrak{m})+1} \otimes \mathbb{Z}_p.$$

Proposition 1.9.5. *If λ is a prime in Hnot dividing $\mathfrak{m}$, then*

$$v_\lambda(\kappa(\mathfrak{m})) = 0 \quad (mod\ n(\mathfrak{m})).$$

Proof. If $\lambda \nmid \mathfrak{m}$ then λ is unramified in $H(\mathfrak{m})$ and the valuation extends from $H^*/(H)^{*n(\mathfrak{m})}$ to $H(\mathfrak{m})^*/(H(\mathfrak{m}))^{*n(\mathfrak{m})}$. But $v_\lambda(\alpha(\mathfrak{m})) = 0$, since $\alpha(\mathfrak{m})$ is an unit in $H(\mathfrak{m})$ by Proposition 1.3.4. □

The rest of the section is devoted to the relation between $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$ and $\kappa(\mathfrak{m})$.

Lemma 1.9.6. *Consider the prime decomposition of $\mathfrak{m} = \prod_i \mathfrak{l}_i$, then*

$$n(\mathfrak{m})(\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_{r(\mathfrak{m}^+)}} - 1) = 0 \in I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6].$$

Proof. The elements $\gamma_{\mathfrak{l}}$ have orders exactly $N_{K/\mathbb{Q}}\mathfrak{l} - 1$.

Write $\gamma_{\mathfrak{l}_i} - 1 = \sum_l (\gamma_{\mathfrak{l}_i}^{(l)} - 1) \in I_{\mathfrak{m}}/I_{\mathfrak{m}}^2$ where the $\gamma_{\mathfrak{l}_i}^{(l)}$ have order a power of l.

We can write, $(\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_{r(\mathfrak{m}^+)}} - 1)$ has a sum of the following elements $(\gamma_{\mathfrak{l}_1}^{(l)} - 1)...(\gamma_{\mathfrak{l}_{r(\mathfrak{m}^+)}}^{(l)} - 1)$.

If l is prime to 6, by definition of $n(\mathfrak{m})$, one of the $\gamma_{\mathfrak{l}_i}^{(l)}$ has order exactly $v_l(n(\mathfrak{m}))$.

Hence, it suffices to prove the lemma when $n(\mathfrak{m})$ is a power of a prime $q = l^r$.

But then, choosing $\gamma_{\mathfrak{l}_i}^{(l)}$ with order exactly q, we have

$$1 = (\gamma_{\mathfrak{l}_i}^{(l)} - 1 + 1)^q = \sum_{i=0}^{q} \binom{q}{i} (\gamma_{\mathfrak{l}_i}^{(l)} - 1)^i$$

and

$$q(\gamma_{\mathfrak{l}_i}^{(l)} - 1) = \sum_{i=2}^{q} \binom{q}{i} (\gamma_{\mathfrak{l}_i}^{(l)} - 1)^i \in I_{\mathfrak{m}}^2.$$

□

Proposition 1.9.7. *Write* $\mathfrak{m}^+ = \prod_{i=1}^{s} \mathfrak{l}_i$.

We have the equality in $H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6]$:

$$\sum_{\mathfrak{n}|\mathfrak{m}^+} \tilde{\theta}'(\psi, \mathfrak{m}/\mathfrak{n}, \mathfrak{a}) \prod_{\mathfrak{l}|\mathfrak{n}} P_{\mathfrak{m}/\mathfrak{n}}(Frob_{\mathfrak{l}} - 1) = 2^{r(\mathfrak{m}^-)} \kappa(\mathfrak{m}^+) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1).$$

Proof.

$$\begin{aligned}
&\sum_{\mathfrak{n}|\mathfrak{m}^+} \tilde{\theta}'(\psi, \mathfrak{m}/\mathfrak{n}, \mathfrak{a}) \prod_{\mathfrak{l}|\mathfrak{n}} P_{\mathfrak{m}/\mathfrak{n}}(\mathrm{Frob}_{\mathfrak{l}} - 1) \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}}} \sigma(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1).P_{\mathfrak{m}^-}(\sigma) \text{ (Lemma 1.8.3)} \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sum_{\sigma' \in \Gamma_{\mathfrak{m}^-}} \sigma'\sigma(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1).\sigma' \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sum_{\sigma' \in \Gamma_{\mathfrak{m}^-}} \sigma'\sigma(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1) \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sigma N_{\mathfrak{m}^-}(\alpha(\mathfrak{m})) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1) \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sigma \prod_{\mathfrak{q}|\mathfrak{m}^-} (1 - \mathrm{Frob}_q^{-1})(\alpha(\mathfrak{m}^+)) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1) \text{ (Proposition 1.3.5)} \\
&= \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sigma(\alpha(\mathfrak{m}^+)) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1) \prod_{\mathfrak{q}|\mathfrak{m}^-} (1 + \psi(\mathfrak{q})\mathrm{Frob}_q) \text{ (Lemma 1.8.1)} \\
&= 2^{r(\mathfrak{m}^-)} \sum_{\sigma \in \Gamma_{\mathfrak{m}^+}} \sigma(\alpha(\mathfrak{m}^+)) \otimes \prod_{\mathfrak{l}|\mathfrak{m}^+} (P_{\mathfrak{l}}(\sigma) - 1) \\
&= 2^{r(\mathfrak{m}^-)} \sum_{i_i \in \{1...N_{\mathfrak{l}i}-1\}} \gamma_{\mathfrak{l}1}^{i_1}...\gamma_{\mathfrak{l}s}^{i_s}(\alpha(\mathfrak{m}^+)) \otimes (\gamma_{\mathfrak{l}_1}^{i_1} - 1)...(\gamma_{\mathfrak{l}_s}^{i_s} - 1) \\
&= 2^{r(\mathfrak{m}^-)} D(\mathfrak{m}^+)(\alpha(\mathfrak{m}^+)) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1) \\
&= 2^{r(\mathfrak{m}^-)} (\beta(\mathfrak{m}^+)) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1) \\
&= 2^{r(\mathfrak{m}^-)} (\kappa(\mathfrak{m}^+)) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1) \text{ (Lemma 1.9.6) .}
\end{aligned}$$

□

The previous proposition allows us to see $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$ as an element in $H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1}$. It is a key fact in our purpose since a Kolyvagin system for $\mathbb{Z}_p \otimes \psi$ is a collection of elements in $H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}_p$.

As in Proposition 1.9.3, the map

$$H^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \to (H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}[1/6])^{\Gamma_{\mathfrak{m}}}$$

doesn't need to be an isomorphism. Nevertheless, $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$ has a canonical inverse through this map which will be enough for our purpose. (Here, canonical means compatible for all the cohomology maps that we consider.)

1.10 Proof of the Theorem 1.4.1 for $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$

We have now all the tools needed to conclude the proof of Theorem 1.4.1.

Proposition 1.10.1. *For any prime $p \neq 2$, the collection*

$$\{2^{-r(\mathfrak{m}^-)}\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})\}$$

is a pre-Kolyvagin system for $(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_{can}, \mathcal{P})$.

Proof. We need to check the five properties of Proposition 1.6.2.

Proposition 1.9.7 is a key fact for the proof. The formula relates $\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})$ to $\kappa(\mathfrak{m}^+)$ for which we know all the useful properties.

• Property (i):

By induction on $r(\mathfrak{m})$, using Propositions 1.9.7, 1.9.5 and [16] Theorem IV.5.1.

• Property (ii) is Lemma 1.8.2.

Projecting the formula in Proposition 1.9.7 into $H^1(K, T/I_{\mathfrak{m}}T) \otimes \mathcal{I}_{\mathfrak{m}}^{new}$ gives

$$\langle 2^{-r(\mathfrak{m}^-)}\tilde{\theta}'(\psi, \mathfrak{m}, \mathfrak{a})\rangle_{\mathfrak{m}}^{new} = \langle \kappa(\mathfrak{m}^+) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1)\rangle_{\mathfrak{m}}^{new}.$$

Properties (ii),(iv)' and (v) follow from the corresponding properties of $\kappa(\mathfrak{m}^+) \otimes (\gamma_{\mathfrak{l}_1} - 1)...(\gamma_{\mathfrak{l}_s} - 1)$. More precisely, (iii) is [16] Theorem IV.5.4, (iv)' is Theorem A.4 in [12] adapted to the case of quadratic imaginary fields, and (v) is immediate. □

Proposition 1.10.2. *For any prime $p \neq 2$, the collection $\{h_{\mathfrak{m}}R_{\mathfrak{m}}\}$ is a pre-Kolyvagin system for $(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_{can}, \mathcal{P})$.*

Proof. This is the same as [13] section 8, adapted to ideals in K (the finite singular morphism has been explicited in 1.7.1). □

For simplicity, let's denote $\mathbf{PKS}(p) :=\mathbf{PKS}(K, \mathbb{Z}_p(1) \otimes \psi, \mathcal{F}_f, \mathcal{P})$.

By Propositions 1.7.4,1.6.3 and the remark at the end of section 1.6, for all $p \neq 2$, $\mathbf{PKS}(p)$ has rank one.

Lemma 1.10.3. *For all $p \neq 2$, suppose that $\kappa_{\mathfrak{m}}$ and $\kappa'_{\mathfrak{m}} \in \boldsymbol{PKS}(p)$ that agree at first step (ie. $\kappa_{\mathfrak{l}} = \kappa'_{\mathfrak{l}}$) then $\kappa_{\mathfrak{m}} = \kappa'_{\mathfrak{m}}$.*

1.10 Proof of the Theorem 1.4.1 for $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$

Proof. If both are zero, then there is nothing to prove.

Suppose $\kappa'_{\mathfrak{m}} \neq 0$, then since $\mathbf{PKS}(p)$ has rank one, we may suppose (by switching $\kappa_{\mathfrak{m}}$ and $\kappa'_{\mathfrak{m}}$ if necessary) $\kappa_{\mathfrak{m}} = a\kappa'_{\mathfrak{m}}$ for some $a \in \mathbb{Z}_p$. By Theorem 1.5.3, Proposition 1.7.5 and 1.6.3, $\kappa'_{\mathfrak{1}} \neq 0$ and $a = 1$. □

Proof of the theorem 1.4.1 when $\mathfrak{m} \in \mathcal{N}_{\mathfrak{af}}$:

By Propositions 1.10.1 and 1.10.2, the two sides of Theorem 1.4.1 are elements in $\mathbf{PKS}(p)$ for $p \neq 2$ and by section 1.3, they agree at the first step for $p \neq 2, 3$. Using Lemma 1.10.3, we have the equality in

$$H(\mathfrak{m})^* \otimes I_{\mathfrak{m}}^{r(\mathfrak{m}^+)}/I_{\mathfrak{m}}^{r(\mathfrak{m}^+)+1} \otimes \mathbb{Z}_p$$

for all $p \neq 2, 3$, which finishes the proof.

Appendix

1.A About the augmentation quotient

Let $\mathcal{I}_{\mathfrak{m}}^{new}$ be the subgroup generated by the elements of the form $\prod_{\mathfrak{l}|\mathfrak{m}^+}(g_{\mathfrak{l}}-1)$ where $g_{\mathfrak{l}} \in \Gamma_{\mathfrak{l}}$.

Denote also $P_{\mathfrak{n}}$, the composition $\mathbb{Z}[\Gamma_{\mathfrak{m}}] \to \mathbb{Z}[\Gamma_{\mathfrak{n}}] \to \mathbb{Z}[\Gamma_{\mathfrak{m}}]$.

To simplify the notation denote $r := r(\mathfrak{m}^+)$.

We have the following statement:

Proposition 1.A.1. *For any abelian group A, if $x \in A \otimes I^r/I^{r+1}$ is such that $P_{\mathfrak{m}/\mathfrak{l}}(x) = 0$ for all $\mathfrak{l}|\mathfrak{m}^+$ then $x \in A \otimes \mathcal{I}_{\mathfrak{m}}^{new}$.*

Proof. • As a first remark, since $P_{\mathfrak{m}/\mathfrak{l}_1} \circ P_{\mathfrak{m}/\mathfrak{l}_2} = P_{\mathfrak{m}/(\mathfrak{l}_1\mathfrak{l}_2)}$, we have:

$$P_{\mathfrak{m}^-\mathfrak{d}}(x) = 0 \quad \forall \mathfrak{d}|\mathfrak{m}^+.$$

• For any $\mathfrak{l}|\mathfrak{m}$ choose a generator $\gamma_{\mathfrak{l}}$ of $\Gamma_{\mathfrak{l}}$.

Then the elements of the form $\prod(\gamma_{\mathfrak{l}} - 1)$ generate I^r/I^{r+1}.

Indeed for any $\prod_j(g_j - 1) \in I^r/I^{r+1}$ we have:

$$\begin{aligned}\prod_j(g_j-1) &= \prod_j(\prod_{\mathfrak{l}}\gamma_{\mathfrak{l}}^{n_{\mathfrak{l},j}} - 1)\\ &= \prod_j(\sum_{\mathfrak{l}} n_{\mathfrak{l},j}(\gamma_{\mathfrak{l}}-1) \text{ since } g_1g_2 - 1 = g_1 - 1 + g_2 - 1 \in I_{\mathfrak{m}}/I_{\mathfrak{m}}^2\\ &= \sum_I n_I \prod_{\mathfrak{l}\in I}(\gamma_{\mathfrak{l}}-1).\end{aligned}$$

• Using the previous fact and using the notations $\mathfrak{m}^+ = \prod_{i=1}^r \mathfrak{l}_i$ and $\mathcal{J}_r^- := \{\{\mathfrak{l}_1, .., \mathfrak{l}_r\}$ such that $\forall i, \mathfrak{l}_i|\mathfrak{m}^-\}$, any element $x \in A \otimes I^r/I^{r+1}$ can be written :

$$
\begin{aligned}
x = x_{new} \otimes \prod_{i=1}^{r} (\gamma_{\mathfrak{l}_i} - 1) \\
+ \sum_{J \in \mathcal{J}_r^-} x_J \otimes \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) \\
+ \sum_{a_1=1}^{r} \Big(\sum_{J \in \mathcal{J}_{r-a_1}} x_{J,1} \otimes (\gamma_{\mathfrak{l}_1} - 1)^{a_1} \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) \Big) + ... \\
... + \sum_{a_r=1}^{r} \Big(\sum_{J \in \mathcal{J}_{r-a_r}} x_{J,r} \otimes (\gamma_{\mathfrak{l}_r} - 1)^{a_r} \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) \Big) \\
+ \sum_{a_1+a_2=2, a_1, a_2 \neq 0}^{r} \Big(\sum_{J \in \mathcal{J}_{r-a_1-a_2}} x_{J,1,2} \otimes (\gamma_{\mathfrak{l}_1} - 1)^{a_1} (\gamma_{\mathfrak{l}_2} - 1)^{a_2} \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) \Big) + ... \\
\vdots \\
+ \sum_{\mathfrak{l} | \mathfrak{m}^-} x_{\mathfrak{l}, \mathfrak{l}_r} \otimes (\gamma_{\mathfrak{l}_1} - 1) ... (\gamma_{\mathfrak{l}_{r-1}} - 1)(\gamma_{\mathfrak{l}} - 1) + ... \\
... + \sum_{\mathfrak{l} | \mathfrak{m}^-} x_{\mathfrak{l}, \mathfrak{l}_1} \otimes (\gamma_{\mathfrak{l}_2} - 1) ... (\gamma_{\mathfrak{l}_r} - 1)(\gamma_{\mathfrak{l}} - 1).
\end{aligned}
$$

To finish the proof, we have to show that $x = x_{new} \otimes \prod_{\mathfrak{l} | \mathfrak{m}^+} (\gamma_{\mathfrak{l}} - 1)$ and we prove it by induction:

By applying $P_{\mathfrak{m}^-}$, we see that:

$$\sum_{J \in \mathcal{J}_r^-} x_J \otimes \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) = 0$$

and the second row is zero.

Then applying $P_{\mathfrak{m}^- \mathfrak{l}_i}$, we have:

$$\sum_{a_i=1}^{r} \Big(\sum_{J \in \mathcal{J}_{r-a_i}} x_{J,i} \otimes (\gamma_{\mathfrak{l}_i} - 1)^{a_i} \prod_{\mathfrak{l} \in J} (\gamma_{\mathfrak{l}} - 1) \Big) = 0.$$

Applying it for all i we see that the third row is zero.

Then, by induction on the row, we apply $P_{\mathfrak{m}^- \mathfrak{l}_{i_1} ... \mathfrak{l}_{i_n}}$ for all $n-$uple $(i_1, ...i_n)$, we see that the $n+2$th row is zero.

□

1.B On a technical hypothesis in [12]

We end this paper with a small erratum in [12]. Stated as they are, Lemma 2.1.4 and Lemma 3.5.2 are wrong and we sate here a "good version" of

1.B On a technical hypothesis in [12]

Lemma 3.5.2. It doesn't change anything in [12], since Lemma 3.5.2 is only used in a special case where it is actually true. We suggest here a new formulation of this lemma with its proof. We follow the notation of [12].

Lemma 1.B.1. *Suppose that (H.0),(H.1) and (H.3) hold, then for any ideal J of R, and any submodule S of T and S' of T^* we have:*

$$(S/JT)^{G_{\mathbb{Q}}} = (S'/JT^*)^{G_{\mathbb{Q}}} = 0.$$

Proof. By (H.1), if $(T/\mathfrak{m}T)^{G_{\mathbb{Q}}} \neq 0$ then $G_{\mathbb{Q}}$ acts trivially on T. In this case we can find a non zero element in $H^1(\mathbb{Q}(T,\mu_{p^\infty})/\mathbb{Q}, T/\mathfrak{m}T)$ since $\mathrm{Gal}(\mathbb{Q}(T,\mu_{p^\infty})/\mathbb{Q})$ has a quotient isomorphic to Z/pZ and $T/\mathfrak{m}T \simeq Z/pZ$.

By (H.3), this shows $(T/\mathfrak{m}T)^{G_{\mathbb{Q}}} = 0$.

For any submodule S of T, and any ideal $J \subseteq R$, $(S/JT)^{G_{\mathbb{Q}}}$ injects in $(T/JT)^{G_{\mathbb{Q}}}$, so we have to show that $(T/JT)^{G_{\mathbb{Q}}} = 0$.

Suppose $\mathfrak{m}^{i+1} \subsetneq J \subseteq \mathfrak{m}^i$ and let $\overline{x} \in (T/JT)^{G_{\mathbb{Q}}}$ with antecedent x in T.

By definition, $x \in (T/\mathfrak{m}T)^{G_{\mathbb{Q}}} = 0$ and $x \in \mathfrak{m}T$. Write $x = a_1 x_1$.

We have $a_1 x_1 \in\in (T/JT)^{G_{\mathbb{Q}}}$. If $a_1 \in J$, $\overline{x} = 0$ and we're done. If not, by (H.0), $x_1 \in \mathfrak{m}T$ and we can write $x_1 = a_2 x_2$ with $a_2 \in \mathfrak{m}$.

By induction, $x = a_1 .....a_{i+1} x_{i+1}$ with $a_k \in \mathfrak{m}$ and $\overline{x} = 0$.

The proof for T^* is similar.

□

Further directions

The "refined class number formulas" that we prove beg for generalization. There are here two natural generalizations, either by taking H to be any finite abelian extension of K or by taking K to be any any number field.

Changing H shouldn't be a major difficulty, since we could define the elliptic units and the regulators in a similar way by considering the characters corresponding to H/K.

If we consider K to be any quadratic imaginary field of arbitrary class number, the construction of elliptic units is the same but gives units defined over extensions of the Hilbert class field of K (instead of extensions of K). We then face the difficulty of defining the regulators in this case but this seems more technical than conceptual.

In the other hand, considering K to be any number field is a much deeper question since we don't know how to construct special units for arbitrary number fields. In a forthcoming paper, Mazur and Rubin explain how to generalize Darmon's formula as well as ours by considering the conjectured Stark units ([14]). The present work fits in the general picture since this case of quadratic imaginary field is the second case after the rational numbers where the Stark conjectures are well known.

Chapter 2

Mazur-Tate type conjectures for elliptic curve over finite anticyclotomic extensions

Summary

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, let K be a quadratic imaginary field and let $\mathcal{O}$ be an order in K. To this triple is attached a theta element $\Theta(E, K, \mathcal{O})$ that is conjectured to interpolate the special values of the Hasse Weil L-function $L(E/K, s)$ twisted by characters of $Pic(\mathcal{O})$. Following the ideas in [1], we give conjectures of the order of vanishing of $\Theta(E, K, \mathcal{O})$ that we prove in some special cases.

2.1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$ with associated Dirichlet character ϵ. For simplicity, we assume that $D \neq 2, 3$ so that the ring of integers $\mathcal{O}_K$ has unit group $\mathcal{O}_K^* =< \pm 1 >$. Throughout the paper, we make the following assumption on the pair (N, K):

Assumption 2.1.1. *1. N and D are coprime.*

2. The field K induces a decomposition of $N = N^+N^-$, where N^+ (resp. N^-) is the product of the primes dividing N that are split (resp. inert) in K. We suppose that N^- is the squarefree product of an odd number of primes.

For any order $\mathcal{O}$ in K, we construct in section 2.2.4 a theta element $\Theta(E, K, \mathcal{O})$ in the group ring $\mathbb{Z}[\frac{1}{d}][Pic(\mathcal{O})]$, where d is an integer that depends only on K and E but not on $\mathcal{O}$. The element $\Theta(E, K, \mathcal{O})$ is conjectured to interpolate the special values of the Hasse Weil L-function $L(E/K, s)$ twisted by characters of $Pic(\mathcal{O})$.

The existence of such interpolation properties yields to conjectures à la Mazur-Tate, conjectures that relate the order of vanishing of $\Theta(E, K, \mathcal{O})$ and the rank r_E of E over K. For any group ring $A[G]$, recall that an element f in $A[G]$ has order of vanishing greater than r if it belongs to the r-th power of the augmentation ideal:

Definition 2.1.2. *For any group ring $A[G]$, the augmentation ideal $I_G \subset A[G]$ is defined as the kernel of the augmentation map:*

$$\psi : \begin{array}{ccc} A[G] & \to & A, \\ g & \mapsto & 1. \end{array}$$

The order of vanishing $r_f \in \mathbb{N} \cup \{\infty\}$ of $f \in A[G]$ is defined to be:

$$ord_{I_G}(f) := sup_{i \in \mathbb{N}}\{i | f \in I_G^i \subset A[G]\}.$$

Here is a short motivation to understand why the order of vanishing corresponds to powers of the augmentation ideal. When L is a complex analytic function with analytic expansion around 0 given by $L(s) = \sum_{i \geqslant 0} a_i s^i$, the order of vanishing of L is the integer r such that $a_i = 0$ for $i < r$ and $a_r \neq 0$. For the p-adic counterpart, when L is an element of the Iwasawa algebra Λ_p, the order of vanishing of L is the T-valuation when we consider the isomorphism $\Lambda_p \simeq \mathbb{Z}_p[[T]]$. Now, the Iwasawa algebra is the completion of a group ring and the isomorphism $\Lambda_p \simeq \mathbb{Z}_p[[T]]$ is made by sending T to $g-1$, where g is a topological generator of $\mathbb{Z}_p$. The group ring counterpart of the order of vanishing is then to understand the divisibility of $f \in A[G]$ by elements of the form $g-1$ or in other word in which power of the augmentation ideal f belongs.

Following theses ideas, we make the following conjecture:

Conjecture 2.1.1. *For any order $\mathcal{O}$, we have:*

$$ord_{\mathbb{Z}[\frac{1}{d}][Pic(\mathcal{O})]}(\Theta(E,K,\mathcal{O})) \geqslant r_E.$$

For technical reasons arising from the geometry of the elliptic curve and from the structure of the group ring $\mathbb{Z}[\frac{1}{d}][Pic(\mathcal{O})]$, we prove the weaker theorem:

Theorem 2.1.3. *For any order $\mathcal{O}$, there exists an integer M that depends on $\mathcal{O}$ such that:*

1. If $Pic(\mathcal{O})^{(p)} \simeq (\mathbb{Z}/p\mathbb{Z})^{n_p}$ ($Pic(\mathcal{O})^{(p)}$ is the p-part of $Pic(\mathcal{O})$) whenever $p \nmid M$, then:

$$ord_{\mathbb{Z}[\frac{1}{M}][Pic(\mathcal{O})]}(\Theta(E,K,\mathcal{O})) \geqslant r_E.$$

2. If $r \leqslant 2$ then:

$$ord_{\mathbb{Z}[\frac{1}{M}][Pic(\mathcal{O})]}(\Theta(E,K,\mathcal{O})) \geqslant r_E.$$

3. If p doesn't divide M then:

$$ord_{\mathbb{F}_p[Pic(\mathcal{O})]}(\Theta(E,K,\mathcal{O})) \geqslant r_E.$$

For this article, the author is inspired by the work of Bertolini and Darmon. In [1], they present a similar construction in a purely p-adic setting: They choose from the beginning an ordinary prine p relative to E and construct theta elements $\mathcal{L}_{E,n} \in \mathbb{Z}_p[Pic(\mathcal{O}_{p^n})]$[1]. The elements $\mathcal{L}_{f,n}$ are compatible with the natural surjection map

$$\mathbb{Z}_p[Pic(\mathcal{O}_{p^n})] \to \mathbb{Z}_p[Pic(\mathcal{O}_{p^{n-1}})],$$

which allows to consider an element $L_p(E,K)$ in the Iwasawa algebra Λ_p. If we deonte $I_p \subset \Lambda_p$ the augmentation ideal in Λ_p, they prove the following theorem under certain technical assumption on p:

Theorem 2.1.4. $ord_{I_p} L_p(E,K) \geqslant r_E$.

The differences between the present article and the work of Bertolini and Darmon are of two natures. First, the construction of the theta elements is purely integral and all the primes are treated indifferently. Secondly, the structures of the group rings $\mathbb{Z}[Pic(\mathcal{O})]$ are more complicated than the Iwasawa algebra Λ_p and the difficulty is to understand the conditions that an element in $\mathbb{Z}[Pic(\mathcal{O})]$ should satisfy in order to ensure that it belongs to the rth-power of the augmentation ideal.

[1] To be precise with the notation, they denote their element $\mathcal{L}_{f,n}$ where f is an eigenform with the same eigenvalues at $\ell \neq p$ as the eigenform attached to E by Eichler-Shimura correspondence and such that f is an eigenvector for the U_p operator.

2.2 The theta elements

For this section let f be a newform on $X_0(N)$ and let $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$ be an order in K of conductor c. To the pair $(f, \mathcal{O})$, we associate a *theta element* $\Theta(f, \mathcal{O})$ in an appropriate Group ring (section 2.2.4) and $L-$functions that vary with characters of $Pic(\mathcal{O})$ (section 2.2.6). The two constructions are closely related since the theta element should interpolate the special values of the $L-$functions (see Conjectures and Theorems 2.2.16). The newform f is later specialized to be the newform associated to an elliptic curve E defined over $\mathbb{Q}$ so that we can give a precise conjectures of the order of vanishing of the theta element that involves the rank of the Mordell-Weil group $E(K)$.

2.2.1 Definite Shimura curves

We start by describing quickly the geometry of "definite Shimura curves" which is the main tool in the construction of the theta element. The material described here is studied in more detail in [2] and [9].

Let B be the definite quaternion algebra ramified at all primes dividing N^- and let R_{N^+,N^-} be an Eichler order of level N^+. Such a quaternion algebra is defined up to isomorphisms whereas the Eichler order is defined up to conjugation by an element of B^* (see [23] for more details about quaternion algebras). Let $\hat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$. For any $\mathbb{Z}$-module M, we denote $\hat{M} := M \otimes \hat{\mathbb{Z}}$.

Let $\mathbb{P}$ denote the conic (curve of genus 0) defined over $\mathbb{Q}$ by:

$$\mathbb{P}(K) = \{x \in B \otimes K | Norm(x) = trace(x) = 0\},$$

for all $\mathbb{Q}$-algebras K. The group B^* acts naturally on $\mathbb{P}$ by conjugation. When $K = \mathbb{C}$ (resp. K is a quadratic field), $P(\mathbb{C})$ (resp. $P(K)$) is identified with $Hom(\mathbb{C}, B \otimes \mathbb{R})$ (resp. $Hom(K, B)$).

Consider the definite Shimura curve

$$X_{N^+,N^-} := \hat{R}^*_{N^+,N^-} \setminus (\hat{B}^* \times \mathbb{P})/B^*.$$

It is the disjoint union of $n := h(R_{N^+,N^-})$ (the class number of R_{N^+,N^-}) curves of genus 0 that we denote X_i and that correspond to the n different elements I_i of the ideal class group of R_{N^+,N^-}. To each element I_i correspond an element g_i of $\hat{R^*_{N^+,N^-}} \setminus \hat{B}^*/B^*$ and an Eichler order of level N^+ that we denote R_i. Denote $w_i := |R_i^*/\{\pm 1\}|$.

Denote J_{N^+,N^-} its Jacobian. It is a free $\mathbb{Z}$-module of rank n and let $(e_i)_{1 \leq i \leq n}$ be a base of J_{N^+,N^-} where e_i corresponds to the component X_i.

Definition 2.2.1. *Following [9], we define a height pairing on J_{N^+,N^-} with basis given by $(e_i)_{1 \leq i \leq n}$, by:*

$$< e_i, e_j >:= w_i \delta_{i,j}.$$

Since $\mathbb{Q}$ has class number one, we have $\hat{\mathbb{Q}}^* = \mathbb{Q}^*\hat{\mathbb{Z}}^*$ and

$$X_{N^+,N^-} = (\hat{R}^*_{N^+,N^-} \setminus \hat{B}^*/\hat{\mathbb{Q}}^*) \times \mathbb{P}/(B^*/\mathbb{Q}^*).$$

The Hecke algebra T_N acting on J_{N^+,N^-}:

When $p \nmid N$, the space $R_p^* \setminus B_p^*/\mathbb{Q}_p^* \simeq PGL_2(\mathbb{Z}_p)/PGL_2(\mathbb{Q}_p)$ has the structure of the set of vertices in a homogeneous tree of degree $p+1$ ([19] p.70). Let δ_p denote the distance function on the trees at the place p. For m and N coprime, we define a correspondence T_m on the product of the trees given on an element g in $(\hat{R}^*_{N^+,N^-} \setminus \hat{B}^*/\hat{\mathbb{Q}}^*)$ by:

$$T_m(g) = \sum_{\substack{\delta_p(g_p,h_p)\leq v_p(m) \\ \delta_p(g_p,h_p)\equiv v_p(m) \bmod 2}} (h).$$

Since right multiplication by B acts by isometries on the tree, T_m naturally gives rise to a well-defined correspondence on the curve X_{N^+,N^-} and an endomorphism on its Jacobian J_{N^+,N^-}. The ring of endomorphism generated by the T_m for m and N coprime acting on J_{N^+,N^-} is the Hecke algebra $\mathbb{T}_N$.

The Atkin-Lehner involutions $\mathcal{W}_N$.

When $p|N^-$, the space $R_p^* \setminus B_p^*/\mathbb{Q}_p^*$ has two elements. We denote W_p the non trivial involution on this set and also denote W_p the corresponding involution on X_{N^+,N^-} and J_{N^+,N^-}.

When $p||N^+$, the space $R_p^* \setminus B_p^*/\mathbb{Q}_p^* \simeq \Gamma_0(p)/PGL_2(\mathbb{Q}_p)$ is equipped with a non trivial involution given by the action of

$$\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}.$$

We denote W_p the corresponding involution on X_{N^+,N^-} and J_{N^+,N^-}.

Proposition 2.2.2. *The operatosr $T_m \in \mathbb{T}_N$ are autoadjoint with respect to the height pairing defined in 2.2.1.*

Proof. The proof follows from a deep study of the so-called Brand matrices. The reader is referred to [9] for a nice exposition in the case where N is prime. □

Remark: For N^- squarefree product of an even number of primes, the indefinite Shimura curve X_{N^+,N^-} has a totally different shape (its genus is greater than 0 to begin with) and doesn't allow us to construct our theta element. Actually, the case where N^- is the squarefree product of an even number of primes will be used later in Theorem 2.3.26 to build classes in Galois cohomology.

2.2.2 The projection map associated to a newform f

To a newform f of conductor N is associated a ring homomorphism of the Hecke algebra :

$$\phi_f : \mathbb{T}_N \to \mathcal{O}_f,$$

where $\mathcal{O}_f$ is the ring of integer of K_f where K_f is the field generated by the Fourier coefficients of f. When f is associated to an elliptic curve by Eichler-Shimura theory over $\mathbb{Q}$, the ring $\mathcal{O}_f$ is simply $\mathbb{Z}$.

Consider a prime λ of $\mathcal{O}_f$ and the discrete valuation ring $\mathcal{O}_{f,\lambda}$. It is a theorem that the component of $J_{N^+,N^-} \otimes \mathcal{O}_{f,\lambda}$ on which the Hecke algebra acts by ϕ_f is a free $\mathcal{O}_{f,\lambda}$-module of rank 1. Denote D_f a generator of this module. (D_f is only defined up to $\mathcal{O}_{f,\lambda}^*$.)

Definition 2.2.3. *We define a projection map on J_{N^+,N^-}, by*

$$x \mapsto v_f(x) := \frac{< x, D_f >}{< D_f, D_f >} \in \mathcal{O}_{f,\lambda}[\frac{1}{< D_f, D_f >}].$$

(The projection map is defined up to $\mathcal{O}_{f,\lambda}^*$.)

There is another interpretation of the projection map in terms of double cosets.

Definition 2.2.4. *Suppose given a function $f : \widehat{R^*_{N^+,N^-}} \setminus \widehat{B^*}/B^* \to \mathcal{O}_{f,\lambda}$, then we may associate to it a projection map on the J_{N^+,N^-} as follow. Take a element $g_i \times \varphi$ in the component X_i. We define*

$$e_i \mapsto v_f(ei) := f(g_i),$$

and extend it by linearity to J_{N^+,N^-}.

Both constructions are closely related. By the Jacquet-Langlands correspondence, to a newform f corresponds a unique (up to a non zero scalar) function $g_f : \widehat{R^*_{N^+,N^-}} \setminus \widehat{B^*}/B^* \to \mathcal{O}_{f,\lambda}$ such that $T_l g_f = a_l g_f$. The projection maps v_f and v_{g_f} are then equal up to a multiplication by a non zero scalar.

Behaviour of v_f under the Atkin-Lehner involutions:
By Proposition 2.2.2, the projection maps v_f satisfy

$$v_f(T_m.x) = \phi_f(T_m) v_f(x)$$

for any $T_m \in \mathbb{T}_N$. A similar result is true for the Atkin-Lehner involutions. By definition, the involutions $\mathcal{W}_N$ commute with the Hecke operators . Let $\ell | N$. If f is a newform of $\widehat{R^*_{N^+,N^-}} \setminus \widehat{B^*}/B^*$ then $W_\ell.f$ is also a newform of $\widehat{R^*_{N^+,N^-}} \setminus \widehat{B^*}/B^*$ with the same eigenvalues since the actions of $\mathcal{W}_N$ commutes with the ones of $\mathbb{T}_N$. By multiplicity one, $W_\ell.f$ is a multiple

of f and since $W_\ell^2 = 1$, we must have $W_\ell.f = \epsilon_{\ell,f}$, where $\epsilon_{\ell,f} = \pm 1$. In particular, it means that the projection maps satisfy $v_f(W_\ell.x) = \epsilon_{\ell,f} v_f(x)$.

Case when $\mathcal{O}_f$ is a principal ring:

For $\mathcal{O}_f$ a principal ring, we can define the projection map associated to the newform f but this time with values in $\mathcal{O}_f$: Indeed, the component of $J_{N^+,N^-} \otimes \mathcal{O}_f$ on which the Hecke algebra acts by ϕ_f is also a free $\mathcal{O}_f$-module of rank 1 and we can consider D_f a generator of this module. By abuse of notation, we still denote v_f for the projection map with values in $\mathcal{O}_f[\frac{1}{< D_f, D_f >}]$.

The obstruction when $\mathcal{O}_f$ is not principal comes from the fact that the component of $J_{N^+,N^-} \otimes \mathcal{O}_f$ on which the Hecke algebra acts by ϕ_f is not necessarily a free $\mathcal{O}_f$-module of rank 1 but only a projective module of rank 1 and we can't guarantee to find any global generator D_f.

2.2.3 Heegner points on X_{N^+,N^-}

We return to the notations and settings made in the introduction where K is a quadratic field. We say that $x \in X_{N^+,N^-}$ is a Heegner point relative to K if it belongs to $X_{N^+,N^-}(K)$. We write $x = g \times f$ for $g \times f$ representative of x in $\hat{B}^* \times Hom(K, B)$. To be more precise, x is a Heegner point of conductor $\mathcal{O}$ for $\mathcal{O}$ an order of K when

$$f(K) \bigcap g^{-1} R_{N^+,N^-} g = f(\mathcal{O}).$$

Since all orders of K can be written as $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$, a Heegner points x of conductor $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$ is sometimes called a Heegner point of conductor c, the context making clear that x is a Heegner point relative to K. All the following results follow from [2] section 1 and 2.

Theorem 2.2.5. *Fix a quadratic field K, an integer N and a decomposition $N := N^+N^-$ such that N^- is squarefree product of an odd number of primes. Suppose that $disc(K)$ and N are coprime. For any integer c prime to N, the set $H_{N^+,N^-}(K, c)$ of Heegner points of conductor c relative to K in X_{N^+,N^-} is non empty if the decomposition N^+N^- satisfies:*

For all ℓ dividing N^+, ℓ is split in K.
For all ℓ dividing N^-, ℓ is inert in K.

Proof. This is Lemma 2.1 in [2]. □

The assumption 2.1.1 assures us that we can find Heegner points relative to a Shimura curve hence the quadratic field K and the level N are fixed.

Action of $Pic(\mathcal{O})$ on the Heegner points of conductor $\mathcal{O}$:

$Pic(\mathcal{O})$ has an adelic description $Pic(\mathcal{O}) = \hat{\mathcal{O}}^+ \setminus \hat{K}^*/K^*$. If f belongs to $Hom(K, B)$, let denote $\hat{f}$ in $Hom(\hat{K}, \hat{B})$ to be the homomorphism deduced

by extension of scalars. Define an action of σ in $Pic(\mathcal{O})$ on $x = g \times f$ by the formula

$$\sigma(g \times f) = (g\hat{f}(\sigma) \times f).$$

One can check that the action is well-defined and free ([9] section 3). By considering the action of the Atkin-Lehner involutions, the product $Pic(\mathcal{O}) \times \mathcal{W}_N$ acts simply transitively on the Heegner points of a given conductor ([2] proof of Lemma 2.5,[9] and [23]).

Theorem 2.2.6. *The action of $\mathcal{W}_N$ on X_{N^+,N^-} preserves the set of Heegner points $H_{N^+,N^-}(K,c)$ for any conductor c. Furthermore, if N is a squarefree integer, the group $\mathcal{W}_N \times Pic(\mathcal{O})$ acts simply transitively on $H_{N^+,N^-}(K,c)$.*

This action could also allow us to compute exactly the (finite) number of Heegner points of a given conductor ([2] lemma 2.5).

Heegner points and homogeneous trees:

Suppose that the assumption of Theorem 2.2.5 are satisfied. We want now to understand the value c of the conductor of an Heegner point x with representatives $g \times f \in (\hat{R}^*_{N^+,N^-} \setminus \hat{B}^*/\hat{\mathbb{Q}}^*) \times Hom(K,B)$ when c and N are coprime. By the Skolen-Noether theorem, up to conjugation there is only one embedding $K \hookrightarrow B$ and the Heegner points x_i of conductor 1 can be written $x_i = g^{(i)} \times f$ with $g^{(i)} \times f$ representatives of x in

$$(\hat{R}^*_{N^+,N^-} \setminus \hat{B}^*/\hat{\mathbb{Q}}^*) \times Hom(K,B).$$

For p and N coprime, the $p-$valuation of c can be seen locally by looking at the distance of g_p and the $g_p^{(i)}$ in the tree $R_p^* \backslash B_p^*/\mathbb{Q}_p^* \simeq PGL_2(\mathbb{Z}_p)/PGL_2(\mathbb{Q}_p)$.

Suppose that p is inert in K:

Proposition 2.2.7. *All the $g_p^{(i)}$ have the same values $g_p^{(0)}$ and we have the equality:*

$$v_p(c) = \delta_p(g_p, g_p^{(0)}),$$

where δ_p is the natural distance of the homogeneous tree

$$PGL_2(\mathbb{Z}_p)/PGL_2(\mathbb{Q}_p)$$

of degree $p+1$.

The reader could have the following local picture in mind, where the prime 3 is inert in K: The point at the center represents the element $g_3^{(0)}$ hence f is chosen and the circles represent Heegner point whose conductors have same 3 valuation. The 4 neighboors of any point are the points given by the Hecke operator T_3:

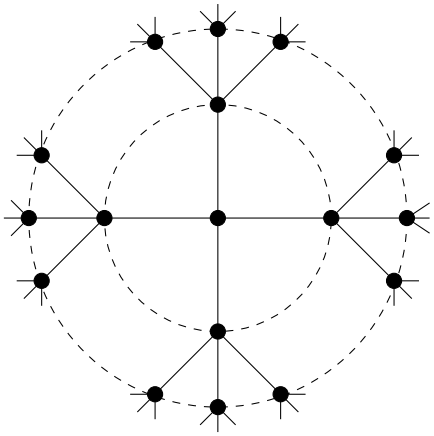


Fig.1 Diagramm of the tree $PGL_2(\mathbb{Z}_3)/PGL_2(\mathbb{Q}_3)$ considered with the conductor's valuation of the corresponding Heegner point when 3 is inert in K.

Suppose that p is split in K:

In this case, the local picture is slightly more complicated and the elements $g_p^{(i)}$ can take an infinite number of values.

Proposition 2.2.8. *The p-valuation of the conductor satisfies the formula:*

$$v_p(c) = min_{h|(h\times f \text{ has conductor } 1)}(\delta_p(g_p, h_p)),$$

where δ_p is the natural distance of the homogeneous tree

$$PGL_2(\mathbb{Z}_p)/PGL_2(\mathbb{Q}_p)$$

of degree $p+1$.

The reader could have the following local picture in mind, where the prime 3 is split in K: The horizontal lines correspond to Heegner points whose conductors have same 3-adic valuation. The bottom line correspond to Hegnneer points with trivial 3-adic valuation. The 4 neighboors of any point are the points given by the Hecke operator T_3:

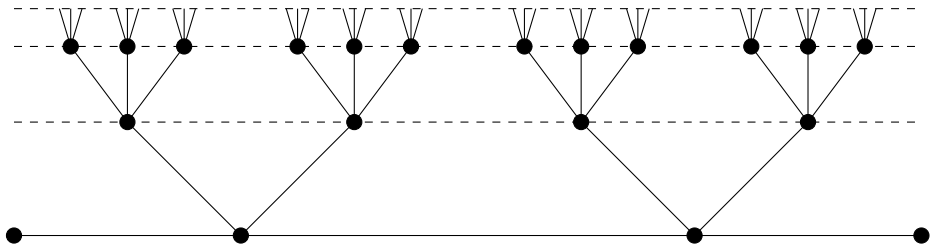


Fig.2 Diagramm of the tree $PGL_2(\mathbb{Z}_3)/PGL_2(\mathbb{Q}_3)$ considered with the conductor's valuation of the corresponding Heegner point when 3 is split in K.

2.2.4 Construction of the theta element $\Theta(\mathcal{O}, f)$

Fix a newform f of level N with values in a principal ring A. For our purpose, A is either a ring of integers of class number one $\mathcal{O}_f$ or a localization of a ring of integers $\mathcal{O}_{f,\lambda}$. Fix also an order $\mathcal{O}$ of K of conductor c prime to $Disc(K).N$ (Recall that K and N satisfy the decomposition relation in 2.1.1). Let x be an Heegner point on X_{N^+,N^-} and for any element of $g \in Pic(\mathcal{O})$, denote x_g the element $g(x)$ where the action is given as in subsection 2.2.3. As an abuse of notation, we'll also denote x the image of X_{N^+,N^-} in J_{N^+,N^-}. The context is generally clear whereas we consider x as in X_{N^+,N^-} or in J_{N^+,N^-}

Definition 2.2.9. *The square root theta element attached to $(x, \mathcal{O}, D_f)$ is*

$$\mathcal{L}_f(x, \mathcal{O}, D_f) := \sum_{g \in Pic(\mathcal{O})} v_f(x_g) g^{-1} \in A[\frac{1}{< D_f, D_f >}][Pic(\mathcal{O})].$$

The group ring is equipped with an involution $\mathcal{L} \to \mathcal{L}^*$ sending $g \in Pic(\mathcal{O})$ to g^{-1}.

Definition 2.2.10. *The theta element is defined to be:*

$$\Theta(\mathcal{O}, f, x, D_f) := \mathcal{L}_f \mathcal{L}_f^*.$$

Proposition 2.2.11. *If $A = \mathbb{Z}$ and N is squarefree, then the theta element $\Theta(\mathcal{O}, f, x, D_f)$ doesn't depend on any choice of generator D_f nor on any choice of Heegner point x and we denote it $\Theta(\mathcal{O}, f)$.*

Proof. We may write $\Theta(\mathcal{O}, f)$ as following:

$$\Theta(\mathcal{O}, f, x, D_f) = \sum_{g \in Pic(\mathcal{O})} (\sum_{g_1 \in Pic(\mathcal{O})} v_f(x_{g_1}) v_f(x_{gg_1})) g.$$

Taking another generator D_f is the same as replacing v_f by $-v_f$, and the formula shows that $\Theta(\mathcal{O}, f)$ doesn't depend on the sign of v_f.

If $x' = x_g$ is another Heegner point, then the formula also shows that $\Theta(\mathcal{O}, f, x, D_f) = \Theta(\mathcal{O}, f, x_g, D_f)$.

If $x' = w(x)$ is another Heegner point where $w \in \mathcal{W}$ the Atkin-Lehner group then as since $v_f(w(x)) = \epsilon v_f$ where $\epsilon = \pm 1$ only depends on w and not on x one has

$$\Theta(\mathcal{O}, f, w(x), D_f) = \Theta(\mathcal{O}, f, x, \epsilon D_f)$$

and

$$\Theta(\mathcal{O}, f, w(x), D_f) = \Theta(\mathcal{O}, f, x, D_f)$$

by the first result.

Finally, since $Pic(\mathcal{O}) \times \mathcal{W}$ acts (simply) transitively on the set Heegner points (Proposition 2.2.6), the proposition follows.

□

2.2.5 On the relations between the theta elements

Let $\mathcal{O}_n$ denote the order of conductor n for any n prime to $N.disc(K)$. We always have a map, $Pic(\mathcal{O}_{n\ell}) \to Pic(\mathcal{O}_n)$ and we can ask for the relations that it induces for the elements $\Theta(\mathcal{O}_{nl}, f)$ and $\Theta(\mathcal{O}_n, f)$. When we consider the tower of group $Pic(\mathcal{O}_{p^n})$ for a fix prime p, one can hope to get compatibilities that would allow to consider a theta element in the Iwasawa algebra $\Lambda_p := \varprojlim_i \mathbb{Z}_p[\mathbb{Z}/p^i\mathbb{Z}]$. This point of view is deeply treated in [1].

The relations property are not only at the level of the theta elements $\Theta(f, \mathcal{O}_n)$ but directly at the level of the elements $\mathcal{L}_f(x, \mathcal{O}, D_f)$. Nevertheless, unlike the theta elements which don't depend on any choice when f is rational (propsoition 2.2.11), the elements $\mathcal{L}_f(x, \mathcal{O}, D_f)$ always depend (up to a unit) on the choices (x, D_f). To understand the relation properties, we fix for this subsection a generator D_f and a compatible family of Heegner points x_n of conductor $\mathcal{O}_n$ for n and $N.disc(K)$ coprime.

By compatible, we mean that the Heegner points $x_n = g_n \times f$ and $x_{n\ell} = g_{nl} \times f$ are such that $\delta_\ell((g_n)_\ell, (g_{n\ell})_\ell) = 1$.

Let denote $\mathcal{L}_f(x_n) := \mathcal{L}_f(x_n, \mathcal{O}_n, D_f)$.

Theorem 2.2.12. *The following relations hold in* $A[\frac{1}{< D_f, D_f >}][Pic(\mathcal{O}_n)]$.

1.For ℓ is inert in K, and $\ell \nmid n$, then

$$\overline{\mathcal{L}_f(x_{n\ell})} = a_\ell \mathcal{L}_f(x_n).$$

2.For $\ell = \lambda_1\lambda_2$ is split in K, and $\ell \nmid n$, then

$$\overline{\mathcal{L}_f(x_{n\ell})} = a_\ell \mathcal{L}_f(x_n) - \mathcal{L}_f(Frob_{\lambda_1}(x_n)) - \mathcal{L}_f(Frob_{\lambda_2}(x_n)),$$

where $Frob_{\lambda_i}$ is the Frobenius element in $Pic(\mathcal{O}_n)$ corresponding to λ_i.

3. Suppose that $\ell | n$ then

$$\overline{\mathcal{L}_f(x_{n\ell})} = a_\ell \mathcal{L}_f(x_n) - \hat{\mathcal{L}}_f(x_{n/\ell}) \sum_{g \in ker: Pic(\mathcal{O}_n) \to Pic(\mathcal{O}_{n/\ell})} g,$$

where $\hat{\mathcal{L}}_f(x_{n/\ell}) := \sum_{\overline{g} \in Pic(\mathcal{O}_{n/\ell})} v_f(g(x_{n/\ell}))g^{-1}$.

Proof. Everything follows from the choice of a compatible system of Heegner point, from the equality

$$v_f(T_\ell(x)) = a_\ell v_f(x)$$

and from the fact that, when p is split in K, the 2 p-neighbors of a Heegner point x of conductor prime to p that have also conductor prime to p are given by $Frob_{\lambda_i}(x)$. Fig. 1 and Fig.2 are here quite useful to visualize the proof.

□

This theorem shows us that the square root theta elements and the theta elements are not directly compatible under the natural group maps and we can't define directly any element in $\varprojlim_n A[\mathcal{O}_n]$ or even in Λ_p for a well chosen p. The way to work in the Iwasawa algebra Λ_p is to ask the eigenform f to be an eigenvector for the operator U_p instead of the Hecke operator T_p. As mentioned in the beginning of the subsection, it is the point of view adopted in [1]. Here, we want to consider all the primes indifferently and we have to "loosen" the strict compatibility between the theta elements. This loss isn't problematic but we mention it to compare our elements with the ones in [1].

2.2.6 Interpolation properties and conjectures

This section is devoted to the relations between the theta elements and the special values of a L-functions that we exhibit. In particular, we explicit here the meaning of the sentence made in the introduction: "The element $\Theta(E, K, \mathcal{O})$ is conjectured to interpolate the special values of the Hasse Weil L-function $L(E/K, s)$ twisted by characters of $Pic(\mathcal{O})$." We start by defining $L(K, f, \chi, s)$.[2]

For the rest of the section, the order $\mathcal{O}$ is fixed.

Definition 2.2.13. *For any element A of $Pic(\mathcal{O})$ with representative $\mathfrak{a} \subset \mathcal{O}$, let E_A be the theta series of weight 1 for $\Gamma_0(D)$ with character ϵ which is determined by the ideal class of A:*

$$\begin{aligned} E_A(z) &:= \frac{1}{2u} \sum_{\lambda \in \mathfrak{a}} q^{\boldsymbol{N}\lambda/\boldsymbol{N}\mathfrak{a}} \\ &:= \frac{1}{2u} + \sum_{m \geq 1} r_A(m) q^m, \end{aligned}$$

where $\mathfrak{a}$ is any ideal in the class A.

Definition 2.2.14. *We define the L-function $L(K, f, A, s)$ as the product of the two Dirichlet series:*

$$L(K, f, A, s) := \sum_{m=1,(m,N)=1}^{\infty} \frac{\epsilon(m)}{m^{2s-1}} \sum_{m=1}^{\infty} \frac{a_m r_A(m)}{m^s},$$

where the coefficients a_m are the Fourrier coefficients of f.

Definition 2.2.15. *For any character χ in $Hom(Pic(\mathcal{O}), \mathbb{C})$, denote:*

$$L(K, f, \chi, s) = \sum_A \chi(A) L(K, f, A, s).$$

[2] When f is a newform attached to an elliptic curve E, we could also write $L(K, E, \chi, s)$ instead of $L(K, f, \chi, s)$. Both notation refer to the same object.

Relation between $\Theta(\mathcal{O}, f)$ and the $L(f, \chi, 1)$:

Theorem 2.2.16. *For all characters χ of $Pic(\mathcal{O})$, we have:*

$$\chi(\Theta(\mathcal{O}, f)) \doteq L(f, \chi, 1)\sqrt{D}/(f, f),$$

where (f, g) is the Peterson product of f with g (the element (f, f) is sometimes called the complex period of f and is denoted Ω_f). The symbol $\doteq$ indicates an equality up to a simple algebraic fudge factor expressed as the product of terms comparatively less important than the quantities explicitely described in the formulas. In particular, dividing $L(f, \chi, 1)$ by the complex period Ω_f yields an algebraic number.

The conjecture has been first proven for the case $N = N^-$ is a prime number and $\mathcal{O} = \mathcal{O}_K$ in [9] and was then generalized in [24] and in [25].

By the previous statement, the formulas relating the theta elements and the $L-$function yield to conjectures a la Mazur-Tate. The spirit of Mazur-Tate types of conjectures is to relate the order of vanishing of $\Theta(\mathcal{O}, f)$ and the rank of $E(K)$.

Conjecture 2.2.1. *Suppose that the Fourrier coefficients of f are rational (ie. $\mathcal{O}_f = \mathbb{Z}$). Let E be the elliptic curve defined over $\mathbb{Q}$ attached to f by Eichler-Shimura theory. Denote r the rank of $E(K)$, then:*

$$\Theta(\mathcal{O}, f) \in I^r_{Pic(\mathcal{O})} \subset \mathbb{Z}[\frac{1}{< D_f, D_f >}][Pic(\mathcal{O})].$$

2.2.7 Remarks on the augmentation ideal

For all this section, let G be a finite abelian group of order n_G. The augmentation ideal and especially its powers are quite subtle ideals and it's a tough question to understand if an element in the group ring belongs to a given power of the augmentation ideal. Here, we start by decomposing the study of $f \in \mathbb{Z}[G]$ into the studies of all its images in $\mathbb{Z}_{p_i}[G_i]$, where G_i is the p_i part of G. Finally, at the end of the section, we state theorems which relate the properties of the image $\varphi(f)$ of f under surjective morphisms φ from $\mathbb{Z}[G]$ into principal local rings $\mathcal{R}$ and the properties of f itself.

Lemma 2.2.17. *Suppose that $G \simeq \mathbb{Z}/p^n\mathbb{Z}$ then for all $g \in G$,*

$$p^n.(g - 1) \in I^p_G$$

.

Furthermore, if $n = 1$,

$$p.(g-1) = (g-1)^p.h \in \mathbb{Z}_p[G],$$

where h *is an element of* $\mathbb{Z}_p[G]^*$.

Proof. Denote $q = p^n$. We have:

$$g^q - 1 = 0 = \sum_{i=1}^{q} \binom{q}{i} (g-1)^i,$$

which leads to

$$q(g-1) = -\sum_{i=2}^{q} \binom{q}{i} (g-1)^i.$$

Since $q|\binom{q}{i}$ for $i < p$, we may repeat the argument and write:

$$q(g-1) = -(g-1)^p \left[\binom{q}{p} + (g-1)f(g) \right],$$

where $f(g)$ is an element of $\mathbb{Z}[G]$.

To prove the statement for $n = 1$, we notice that since $\mathbb{Z}_p[G]$ is a local ring with maximal ideal generated by p and I_G, an element is invertible iff its valuation is prime to p. □

The next example is an example of "funny" behavior and illustrates the difficulties one may have to deal with augmentation ideals.

Example 2.2.18. *Consider the group ring* $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}]$ *and the element*

$$h := (1-\alpha)(1-\beta) \in \mathbb{Z}[\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}],$$

where $\alpha = (1,0)$ *and* $\beta = (0,1)$ *as elements of* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. *Then, writing* $h = (u.2^n + v.3^m)h$ *and using Lemma 2.2.17 shows that*

$$\forall r, h \in I^r_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}} \subseteq \mathbb{Z}[\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}].$$

Decomposition of the structure of the group rings into "elementary" pieces:

Proposition 2.2.19. *Let* A *be a ring and* G *a commutative group,* f *an element of* $A[G]$ *and* r *an integer. Suppose that* $G \simeq G_1 \times G_2$ *with* $\#G_i = n_i$ *and suppose that* $(n_1, n_2) = 1$, *then the following propositions are equivalent:*

(i) $f \in I^r_G \subset A[G]$.

(ii) $f \in I^r_{G_1} \subset A[G_1]$ *and* $f \in I^r_{G_2} \subset A[G_2]$, *where by abuse of notation, we still denote* f *the image of* f *by the surjection maps* $A[G] \to A[G_i]$.

Proof. The case $r \leqslant 1$ is immediate, so we may suppose $r > 1$.

(i) implies (ii) is clear.

(ii) implies (i):

Suppose that f satisfies condition (ii). It is straightforward that f can be written:

$$f = f_1 + f_2 + \sum_{g_1 \in G_1, g_2 \in G_2} (g_1 - 1)(g_2 - 1) f_{g_1,g_2},$$

where $f_i \in I^r_{G_1} \subset A[G_i] \subset A[G]$ and $f_{g_1,g_2} \in A[G]$.

We need to show that for any $g_1 \in G_1$ and $g_2 \in G_2$, we have

$$(g_1 - 1)(g_2 - 1) \in I^r_G.$$

By using the computation

$$(g-1)(h-1) + (g-1) + (h-1) = (gh-1),$$

we may suppose that the order of g_1 (resp. g_2) is a power of a prime q_1 (resp. q_2). By hypothesis on $\#G_i$, we know that q_1 and q_2 are coprime. Writing

$$uq_1^m + vq_2^m = 1,$$

for any choice of m and using Lemma 2.2.17 finishes the proof.

□

Lemma 2.2.20. *Let A be a ring and G be an abelian finite group of order a power of p. Write $G = \oplus_{i=1}^k G_i$ with G_i cyclic of order n_i generated by g_i and suppose that:*

$$f = (g_k - 1)F \in I^r_G \subset A[G],$$

then we may write

$$f = (g_k - 1)\tilde{F} \text{ with } \tilde{F} \in I^{r-1}_G \subset A[G].$$

Proof. By hypothesis, we have:

$$(g_k - 1)F = \sum_{i_1 + \ldots + i_k = r, i_k \neq 0} (g_i - 1)^{i_i} F_{i_1,..,i_k} + \sum_{i_1 + \ldots + i_{k-1} = r} (g_i - 1)^{i_i} f_{i_1,..,i_{k-1}}, \tag{2.1}$$

where the $f_{i_1,..,i_{k-1}}, F_{i_1,..,i_k}$ belong to $A[G]$.

By the Taylor expansion, we may write

$$f_{i_1,..,i_{k-1}} = (g_k - 1)F'_{i_1,..,i_{k-1}} + R_{i_1,..,i_{k-1}},$$

where $R_{i_1,..,i_{k-1}}$ belongs to $A[\bigoplus_{i=1}^{k-1} G_i]$. Without a loss of generalities, we may assume that:

$f_{i_1,..,i_{k-1}}$ belong to $A[\bigoplus_{i=1}^{k-1} G_i]$.

Evaluating equation 2.1 at $g_k = 1$ shows that in this case $f_{i_1,..,i_{k-1}} = 0$ for all $(k-1)$-uples and show that we may write:

$$f = (g_k - 1)\tilde{F} \text{ with } \tilde{F} \in I_G^{r-1} \subset A[G].$$

□

Proposition 2.2.21. *Let $f \in \mathbb{Z}[\frac{1}{D}][G]$ and suppose that G has order $q = p^n$. The following propositions are equivalent:*

(i) f belongs to $I_G^r \subset \mathbb{Z}[\frac{1}{D}][G]$.

(ii)f belongs to $I_{G_i}^r \subset \mathbb{Z}_p[\frac{1}{D}][G]$.

Proof. (i) implies (ii) is immediate.

(ii) implies (i): The case $r \leqslant 1$ is clear. When p divides D, Lemma 2.2.17 shows that $I_G^r = I_G \subset \mathbb{Z}[\frac{1}{D}][G]$ and $I_G^r = I_G \subset \mathbb{Z}_p[\frac{1}{D}][G]$ and we may assume that D and p are coprime and $\mathbb{Z}_p[\frac{1}{D}] = \mathbb{Z}_p$.

• Suppose first that G is cyclic of order p^n with generator g, we prove the proposition by induction on r:

Consider $f \in \mathbb{Z}[\frac{1}{D}][G]$ such that $f \in I_G^r \subset \mathbb{Z}_p[G]$, and we want to prove that $f \in I_G^r \subset \mathbb{Z}[\frac{1}{D}][G]$.

By the Taylor expansion, we may write

$$f = \sum_{i=0}^{r} (g-1)^i a_i \in \mathbb{Z}[\frac{1}{D}][G],$$

with $a_i \in \mathbb{Z}[\frac{1}{D}]$ for $i < r$ and $a_r \in \mathbb{Z}[\frac{1}{D}][G]$. By replacing if necessary f by $f - (g-1)^r a_r$ we may assume that f can be written

$$f = \sum_{i=0}^{r-1} (g-1)^i a_i \in \mathbb{Z}[\frac{1}{D}][G],$$

with $a_i \in \mathbb{Z}[\frac{1}{D}]$.

By Lemma 2.2.17, we may also assume that either $v_p(a_i) < n$ or $a_i = 0$.

By evaluating f at $g = 1$, we see that $a_0 = 0$. By recurrence, suppose that $a_i = 0$ for $i < t$, then:

$$f = (g-1)^t \sum_{i=0}^{r-t} (g-1)^i a_{i+t}.$$

Over $\mathbb{Z}_p[G]$, we have $f = (g-1)^r h$ for some $h \in \mathbb{Z}_p[G]$.

Comparing the formulas, we have:

$$(g-1)\left[\sum_{i=0}^{r-t}(g-1)^i a_{i+t} - (g-1)^{r-t}h\right] = 0,$$

which shows that

$$\sum_{i=0}^{r-t}(g-1)^i a_{i+t} = (g-1)^{r-t}h + (\sum_{j=0}^{p^n-1} g^j)h_2, \tag{2.2}$$

for some $h_2 \in \mathbb{Z}_p[G]$.

Evaluating 2.2 at $g = 1$ shows that $v_p(a_i) \geqslant n$ and hence that $a_i = 0$.

• Suppose now that $G \simeq \bigoplus_{i=1}^{k} G_i$, where the G_k are cyclic of order p^{n_k} with generator g_k, we prove the proposition by induction on r and k:

By the Taylor expansion, we have:

$$f = (g_k - 1)f_1 + f_2,$$

where f_2 belongs to $\mathbb{Z}[\frac{1}{D}][\bigoplus_{i=1}^{k-1}]$.

f_2 belongs to $I_G^r \subset \mathbb{Z}[\frac{1}{D}][G]$ by induction on k and we may suppose that $f = (g_k - 1)f_1$.

Now, $f = (g_k - 1)f_1$ and by Lemma 2.2.20, we may assume that f_1 satisfies the hypothesis for $r-1$ which concludes the proof by induction on r. (Notice here, that the transformation from F to $\tilde{F}$ leaves stable the subspace $\mathbb{Z}[\frac{1}{D}][G]$ of $\mathbb{Z}_p[G]$ so we can really use induction.)

□

If we combine Propositions 2.2.21 and 2.2.19, we get the following theorem:

Theorem 2.2.22. *Let G be an abelian group and f be an element of $\mathbb{Z}[\frac{1}{D}][G]$. Decompose $G \simeq \bigoplus G_i$ where $\#G_i = p_i^{n_i}$ and $p_i \neq p_j$ for $i \neq j$. Then the following propositions are equivalent:*

(i) f belongs to $I_G^r \subset \mathbb{Z}[\frac{1}{D}][G]$.

(ii) For all i, f belongs to $I_{G_i}^r \subset \mathbb{Z}_{p_i}[\frac{1}{D}][G_i]$.

This theorem shows us that it is enough to understand what happens at each prime p separately in order to understand the properties in the global group ring. The first advantage of this point of view is the fact that the group rings $\mathbb{Z}_{p_i}[G_i]$ are local rings with maximal ideal generated by the elements $\langle (g-1)_{g\in G}, p\rangle$.

The ring that we consider are then easier but are still not principal. To avoid this difficulty, one may work on the images of elements f in $\mathbb{Z}_p[G]$ in principal rings $\mathcal{R}$.

Study of morphisms $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}$:

For the rest of the section, p is a fixed prime. We mention here the three kind of surjective morphisms $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}$ that appear later. For this purpose, denote ϵ_n a choice of a p^n-roots of unity in an extension of $\mathbb{Q}_p$ for any n. Denote also $\mathcal{R}_n$ the discrete valuation ring $\mathbb{Z}_p[\epsilon_n]$. As a remark, $\pi_n := (\epsilon_n - 1)$ is an uniformizer of $\mathcal{R}_n$ with p-valuation equal to $\frac{1}{(p-1)p^{n-1}}$. The reader may keep in mind the following surjective morphisms when G is cyclic of order p^n with generator g.

$$\varphi_1 : \begin{cases} \mathbb{Z}_p[G] \to \mathbb{Z}_p \\ g \mapsto 1 \end{cases}, \quad \varphi_2 : \begin{cases} \mathbb{Z}_p[G] \to \mathbb{Z}/p^{2n+1} \\ g \mapsto 1 + p^n \end{cases} \quad \text{and} \quad \varphi_3 : \begin{cases} \mathbb{Z}_p[G] \to \mathcal{R}_n \\ g \mapsto \epsilon_n. \end{cases}$$

Result when all elements of G have order p:

Theorem 2.2.23. *Suppose $G = \bigoplus_{i=1}^t G_i$, where $G_i \simeq \mathbb{Z}/p\mathbb{Z}$ with generators g_i. Let f be an element in $\mathbb{Z}_p[G]$:*

1. If f can be written $F(g_1, ..., g_n)(g_1 - 1)$ with $\varphi(f) \in \varphi(I_G)^r$ for any morphism $\varphi : \mathbb{Z}_p[\bigoplus_{i=1}^t G_i] \to \mathcal{R}_1$ such that $\varphi(g_1) \neq 1$ then f can also be written

$$f = f_1 + \sum_{i<j} \left[(g_i - 1)(g_j - 1) \prod_{k=1}^{p-1} (g_i - g_j^k) f_{i,j} \right],$$

where $f_1 \in I_G^r$ and $f_{i,j} \in \mathbb{Z}_p[G]$.

2. If for any morphism $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}_1$ (including the trivial one) we have $\varphi(f) \in \varphi(I_G)^r$ then, we can write:

$$f = f_1 + \sum_{i<j} \left[(g_i - 1)(g_j - 1) \prod_{k=1}^{p-1} (g_i - g_j^k) f_{i,j} \right],$$

where $f_1 \in I_G^r$ and $f_{i,j} \in \mathbb{Z}_p[G]$.

Proof. We prove the proposition by induction on t:

Case $t = 1$ for 1.

By the Taylor expansion, F may be written

$$F = (g_1 - 1)(a_0 + a_1(g_1 - 1) + ... + a_n(g_1 - 1)^n),$$

for some n with $a_i \in \mathbb{Z}_p$. By Lemma 2.2.17, we can even suppose that $a_i \in \mathbb{Z}_p^*$. Applying now φ defined by $\varphi(g) = \epsilon_1$ shows that $a_i = 0$ for $i < r$.

General case for 1. by induction on t:

By the Taylor expansion, f may be written:

$$\begin{aligned} f &= (g_1-1)f_0(g_1,g_3,...,g_n) + (g_2-1)(g_1-1)f_1(g_1,g_3,...,g_n) \\ &+ (g_1-1)(g_2-1)(g_1-g_2)f_1(g_2,g_3,...,g_n) + ... \\ &+ (g_1-1)(g_2-1)(g_1-g_2)...(g_1-g_2^{p-2})f_{p-2}(g_2,g_3,...,g_n) \\ &+ (g_1-1)(g_2-1)(g_1-g_2)...(g_1-g_2^{p-1})f_{p-1}(g_1,g_2,g_3,...,g_n). \end{aligned}$$

The last component has the desired form so we may assume $f_{p-1}=0$. Applying the natural map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/G_2]$ shows that the component $(g_1-1)f_0(g_1,g_3,...,g_n)$ satisfies the hypothesis for $t'=t-1$. By induction, we may suppose that $f_0=0$.

Applying the maps $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}_1$, with $\varphi(g_1)=\varphi(g_2)\neq 1$ shows that $\varphi((g_1-1)f_1(g_1,g_3,...,g_n)) \in \varphi(I_G)^{r-1}$ for all morphsims with $\varphi(g_1)\neq 1$. By induction on t, $(g_1-1)f_1(g_1,g_3,...,g_n)$ has the desired form and we may assume that $f_1=0$.

Repeating the argument for $i<p$, by using the maps $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}_1$, with $\varphi(g_1)=\varphi(g_2)^i \neq 1$ proves that the component

$$(g_1-1)(g_2-1)(g_1-g_2)...(g_1-g_2^{i-1})f_{p-1}(g_1,g_2,g_3,...,g_n)$$

has the desired form, which finishes the proof of 1/.

Case $t=1$ for 2.

Let $f \in \mathbb{Z}_p[G]$ with $G \simeq \mathbb{Z}/p\mathbb{Z}$. Consider g a generator of G. By the Taylor expansion, we have

$$f = a_0 + a_1(g-1) + ... + a_n(g-1)^n,$$

for some n with $a_i \in \mathbb{Z}_p$. By applying, the trivial morphism, we have $a_0=0$. f satisfies then the hypothesis of 1. and the result follows.

General case for 2. by induction on t:

By the Taylor expansion we may write:

$$f = F(g_1,...,g_n)(g_1-1) + f_0(g_2,g_3...,g_n).$$

By taking the natural map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/G_1]$, we see that the component $f_0(g_2,...,g_n)$ satisfy the hypothesis of 2/ for $t'=t-1$. By induction, f_0 has the desired form and we may assume $f_0=0$.

Now, the component $F(g_1,...,g_n)(g_1-1)$, satisfies the hypothesis of 1/. which proves that it has the desired form.

□

Results without assumption on the order:

When G is any finite ring with order a power of p, the result of Theorem 2.2.23 doesn't stand anymore. The obstruction already appears when we consider cyclic group of order p^n for $n>1$:

Example 2.2.24. *Let $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ with generator g, and consider the element*

$$f := p(g-1)^2.$$

Then for the surjective morphism φ_i considered earlier, we have

$$\varphi_i(p(g-1)^2) \subset \varphi_i(I_G^3).$$

On the other hand $p(g-1)^2$ doesn't seem to belong to I_G^3. Unlike the case of $n = 1$, it is not clear if the element $p(g-1)$ belongs to I_G^2 or not.

As a remark, this obstruction disappears in the case of the Iwasawa algebra Λ_p by using the morphism

$$\psi : \begin{cases} \Lambda_p \to \mathbb{Z}_p \\ g \mapsto 1 + p^2 \end{cases},$$

which has not counterpart when G is finite.

To avoid dealing with elements of the form $p(g-1)^2$, one may assume that r is smaller than 3 or one may work over $\mathbb{F}_p$.

Theorem 2.2.25. *Consider $G \simeq \oplus_{i=1}^t G_i$ with G_i cyclic of order p^{n_i}. Let $f \in \mathbb{Z}_p[G]$ be such that for all surjective morphisms*

$$\varphi : \mathbb{Z}_p[G] \to \mathcal{R},$$

where $\mathcal{R}$ is a principal local ring, we have

$$\varphi(f) \in (\varphi(g-1)^r)$$

with $r < 3$ then:

$$f \in I_G^r.$$

Proof. The theorem is proven by induction on t.

Case $t = 1$:

By the Taylor expansion, we can write:

$$f = A_0 + \sum_{i=1}^{t} a_i (g-1)^i$$

with $v_p(a_i) < n$ by Lemma 2.2.17. By subtracting $\sum_{i=r}^t a_i(g-1)^i$, we may assume that $a_i = 0$ for $i \geqslant r$.

By taking $\varphi(g) = 1$, we see directly that $A_0 = 0$.

Now consider the morphism:

$$\begin{aligned} \varphi : &\mathbb{Z}_p[G] \to \mathbb{Z}/p^{2n+1}\mathbb{Z} \\ &g \mapsto 1 + p^n. \end{aligned}$$

Then,

$$\sum_{i=1}^{r-1} a_i p^{in} \in (p^{rn})$$

which shows that $a_i = 0$ since $n - 1 + (r-1)n < 2n + 1$.

Case $t \geqslant 1$:

By the Taylor expansion, f can be written

$$f(g_1, ..., g_t) = (g_1 - 1)(g_2 - 1)f_1 + (g_1 - 1)f_2(g_1, g_3, ..., g_t) + f_3(g_2, ..., g_t).$$

Using the natural projection maps $\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/G_i]$ for $i = 1$ and 2 shows that $(g_1 - 1)f_2(g_1, g_3, ..., g_t)$ and $f_3(g_2, ..., g_t)$ satisfy the induction hypothesis.

□

Theorem 2.2.26. *Let $r \in \mathbb{N}$ such that $r \leqslant p + 1$. Suppose that $p \neq 2$ and that $G \simeq \oplus_{i=1}^{t} G_i$ with G_i cyclic of order p^{n_i}.. Let $f \in \mathbb{Z}_p[G]$ be such that for all surjective morphisms*

$$\varphi : \mathbb{Z}_p[G] \to \mathcal{R},$$

where $\mathcal{R}$ is a principal local ring, we have

$$\varphi(f) \in (\varphi(g - 1)^r)$$

then:

$$\overline{f} \in I_G^r \subset \mathbb{F}_p[G].$$

Proof. The theorem is (once again) proven by induction on t:

Case $t = 1$:

The case $n_1 = 1$ has been treated in Theorem 2.2.23. Suppose that $n > 1$. By the same argument as before, we may assume that:

$$f = \sum_{i=1}^{r-1} a_i (g - 1)^i.$$

Now consider the morphism:

$$\begin{aligned} \varphi :& \mathbb{Z}_p[G] \to \mathcal{O}_{\epsilon_{p^n}}/p \\ & g \mapsto 1 + \epsilon_{p^n}. \end{aligned}$$

Then,

$$\sum_{i=1}^{r-1} \overline{a_i} (\epsilon_{p^n} - 1)^i \in ((\epsilon_{p^n} - 1)^r) \subset \mathcal{O}_{\epsilon_{p^n}}/p,$$

which shows that $a_i = 0$ since by hypothesis $r \leqslant (p-1)p^n$.

Case $t > 1$:

The general case is proven by induction as in the proof of Theorem 2.2.23.

□

2.3 The Euler system argument

2.3.1 Settings and structure of the proof

For this section, let fix an eigenform f of weight 2 of level N with values in $\mathbb{Z}_p$ where we suppose that p doesn't divide $D.N$.

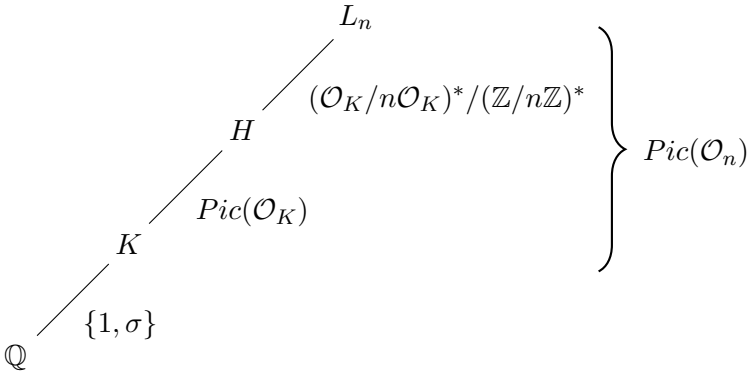
To this eigenform is attached a continuous representation of the Galois group $G_{\mathbb{Q}}$:

$$V_f \simeq \mathbb{Q}_p^2.$$

The representation V_f arises in the Jacobian $J_0(N)$ using the construction of Eichler and Shimura (the reader can find all the basis properties of V_f in [8]).

Since the action of $G_{\mathbb{Q}}$ is continuous, it preserves a $\mathbb{Z}_p$ lattice T_f of V_f and we denote $T_{f,n} := T_f/p^n T_f$. In this section, we use deeply the Group cohomology of $T_{f,n}$ to understand the vanishing properties of the theta elements $\Theta(K, f, \mathcal{O})$. As a remark and to fix the ideas, when f has values in $\mathbb{Z}$, then T_f is isomorphic as $G_{\mathbb{Q}}$-module to the Tate module of the elliptic curve E_f over $\mathbb{Q}$ associated to f and in this case $T_{f,n}$ is $E_f[p^n]$ the group of p^n torsion points of E_f.

For any n, let L_n be the ray class field of K associated to $\mathcal{O}_n$. It is an abelian extension, ramified only at primes dividing n, and such that $Gal(L_n/K) \simeq Pic(\mathcal{O}_n)$. When m and n are coprime, L_{nm} is the compositum of L_m and L_n with L_m and L_n linearly disjoint. This is summarized in the following diagram of Galois extensions:



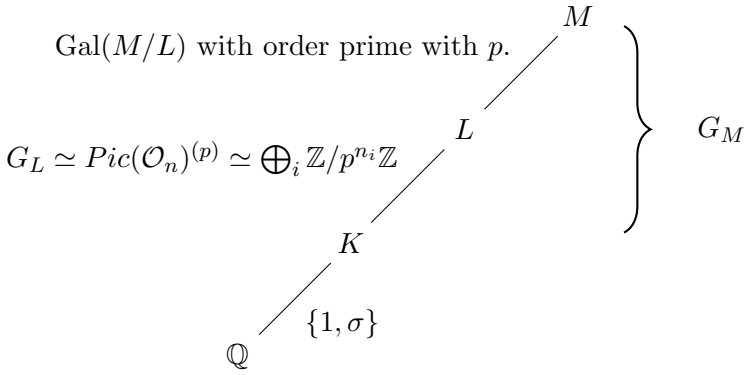
Here, σ denotes the complex conjugation. It acts on $g \in \mathrm{Gal}(L_n/K)$ as an involution by the formula $\sigma g \sigma = g^{-1}$. (That's where the term anticyclotomic or dihedral comes from.)

For all n coprime with $N.D$, let x_n a Heegner point of conductor $\mathcal{O}_n$ in the Shimura curve X_{N^+,N^-}. By section 2.2.4, we associate to the quadruple $(K, \mathcal{O}_n, f, x_n)$ an element

$$\mathcal{L}_{f,n} \in \mathbb{Z}_p[\frac{1}{< D_f, D_f >}][Pic(\mathcal{O}_n)].$$

We fix now the settings to simplify the notations:

Fix a conductor n prime to $N.D$. Let $M := L_n$ and denote L to be the subfield of M such that $G_L := \mathrm{Gal}(L/K) \simeq Pic(\mathcal{O}_n)^{(p)}$ where $Pic(\mathcal{O}_n)^{(p)}$ is the p-part of $Pic(\mathcal{O}_n)$. By definition the order of $\mathrm{Gal}(M/L)$ is prime with p. Denote also $G_M := \mathrm{Gal}(M/K)$:



The advantage of using this subextension L follows from the fact that $\mathbb{Z}_p[G_L]$ is now a local ring with maximal ideal (p, I_{G_L}).

Denote $\tilde{\mathcal{L}_f}$ to be the image of $\mathcal{L}_f$ in $\mathbb{Z}_p[G_L]$. The aim is to prove the following theorem:

Theorem 2.3.1. *Under assumption 2.3.2 on p, for any surjective morphism*

$$\varphi : \mathbb{Z}_p[G_L] \to \mathcal{R},$$

where $\mathcal{R}$ is a principal local ring, we have:

$$\varphi(\tilde{\mathcal{L}_f})^2 \in Fitt_{\mathcal{R}}(Sel_{f,n}^{\vee} \otimes_{\varphi} \mathcal{R}),$$

where Fitt denotes the Fitting ideal, $Sel_{f,n}$ the Selmer group of f at n defined in 2.3.9 and where the noatation $A^{\vee}$ denotes the Pontryagin dual of A.

Using this theorem and standard techniques in the study of modules over local rings allow us to link the p-valuation of $\varphi(\tilde{\mathcal{L}_f})$ and the rank of E_f over K when f is a eigenform with values in $\mathbb{Z}$. This is done in section 2.4.

The main idea in the proof of Theorem 2.3.1 is to construct global classes $\kappa(\ell)$ in $H^1(G_L, T_{f,n})$ that look locally like $\tilde{\mathcal{L}_f}$ and that are almost orthogonal with the elements in the usual Selmer group of our elliptic curve with respect to the Tate global pairing. The "almost" orthogonality is precisely what allows us to link the order of vanishing of $\tilde{\mathcal{L}_f}$ and the rank of the elliptic curve E_f.

We make now the following assumptions:

Assumption 2.3.2. *1. The prime p is $\geqslant 5$.*

2.For all prime ℓ such that ℓ^2 divide N, and p divides $\ell + 1$, the module $T_{f,1}$ is an irreducible I_ℓ-module.

3.The eigenform f is p-isolated (Definition 1.2 [1]).

4. The Galois representation attached to $T_{f,1}$ has image isomorphic to $\boldsymbol{GL}_2(\mathbb{F}_p)$.

5.For all ℓ dividing pN exactly, the Galois representation $T_{f,n}$ has a unique one dimensional subspace $T_{f,n}^{(\ell)}$ on which $Gal(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ acts via ϵ or $-\epsilon$.

Remarks: 1. Part 3. of the assumptions is a key assumption that will allows to prove Theorem 2.3.1 by induction.

2. Suppose that f has values in $\mathbb{Z}$ and consider E the elliptic curve attached to f. In this case, the previous assumptions are satisfied for all but finitely many ordinary prime.

It is clear for parts 1,2.

Part 3 is in this case equivalent to:

The prime p doesn't divide the minimal degree of a parametrisation
$$X_0(N) \to E.$$

It is satisfied for all but finitely many primes.

It is also a well known result that part 4 is satisfied for all but finitely many primes when E doesn't have complex multiplication. (See theorem 2 in [20]).

When E has multiplicative reduction at ℓ and ordinary reduction at p, then assumption 5 is automatically satisfied. (See Propositions 2.11 and 2.12 of [8]).

Finally, part 5 is also satisfied for $\ell | N$, such that $T_{f,n}$ is unramified at ℓ and p doesn't divide $\ell^2 - 1$. Indeed, in this case, the Frobenius element acts on $T_{f,n}$ with eigenvalues ℓ and 1 and assumption 5 follows then from the congruence $p \nmid \ell^2 - 1$.

2.3.2 Local/global structures

This subsection is devoted to the study of submodules in the Galos cohomology of $T_{f,n}$ for a number field H such that $H = K, L$ or M.

Let λ be a prime of H. There is always a restriction map
$$H^i(H, T_{f,n}) \to H^i(H_\lambda, T_{f,n})$$
and by abuse of notation let still denote $s \in H^i(H_\lambda, T_{f,n})$ the image of an element $s \in H^i(H, T_{f,n})$.

Definition 2.3.3. *Suppose that $\lambda \nmid N$. The singular part of $H^1(H_\lambda, T_{f,n})$ is the group*
$$H^1_{sing}(L_\lambda, T_{f,n}) := H^1(I_\lambda, T_{f,n})^{G_{H_\lambda}},$$
where I_λ is the inertia group associated to an embedding $H \subset H_\lambda$.

The natural map arising from restriction is called the residue map and is denoted

$$\delta_\lambda : H^1(H_\lambda, T_{f,n}) \to H^1_{sing}(H_l, T_{f,n}).$$

Definition 2.3.4. *Let $H^1_{fin}(H_\lambda, T_{f,n})$ denote the kernel of δ_λ. The classes in $H^1_{fin}(H_\lambda, T_{f,n})$ are called the finite or unramified classes.*

For each rational prime ℓ, set $H_\ell := H \otimes \mathbb{Q}_\ell = \oplus_{\lambda|\ell} H_\lambda$, where the direct sum is taken over all the primes λ of H dividing ℓ, and write:

$$H^1(H_\ell, T_{f,n}) := \oplus_{\lambda|\ell} H^1(H_\lambda, T_{f,n}).$$

Definition 2.3.5. *Let denote*

$$H^1_{sing}(H_\ell, T_{f,n}) := \oplus_{\lambda|\ell} H^1_{sing}(H_\lambda, T_{f,n}) \subset H^1(H_\ell, T_{f,n}).$$

The map $\delta_\ell := \oplus \delta_\lambda$ is the residue map at ℓ, and the kernel of δ_ℓ, denoted $H^1_{fin}(H_\ell, T_{f,n})$ is the finite part of $H^1(H_\ell, T_{f,n})$.

Definition 2.3.6. *Let ℓ be a prime dividing N exactly. The ordinary part of $H^1(H_\ell, T_{f,n})$ is defined to be the group*

$$H^1_{ord}(H_\ell, T_{f,n}) := H^1(H_\ell, T^{(\ell)}_{f,n}).$$

Definition 2.3.7. *At prime p, the ordinary part of $H^1(H_p, T_{f,n})$ is defined to be the group*

$$H^1_{ord}(L_p, T_{f,n}) := res_p^{-1}(H^1_{sing}(H_p, T^{(p)}_{f,n})).$$

Tate duality: The Weil pairing gives rise to a canonical $G_{\mathbb{Q}}$-equivariant pairing:

$$T_{f,n} \times T_{f,n} \to \mu_{p^n}.$$

Combining this pairing with the cup product pairing in cohomology gives rise for all ℓ to the perfect local Tate pairing :

$$<,>_\ell : H^1(H_\ell, T_{f,n}) \times H^1(H_\ell, T_{f,n}) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Proposition 2.3.8. *1. If ℓ is a prime not dividing pN, then the groups $H^1_{fin}(H_\ell, T_{f,n})$ and $H^1_{sing}(H_\ell, T_{f,n})$ are annihilators of each other under the local Tate pairing $<,>_\ell$.*

2. If ℓ is a prime dividing pN exactly, the groups $H^1_{ord}(H_\ell, T_{f,n})$ and $H^1_{ord}(H_\ell, T_{f,n})$ are annihilators of each other under the local Tate pairing $<,>_\ell$.

Proof. This is Proposition 2.3 of [1]. □

Definition 2.3.9. *The Selmer group $Sel_{f,n}(H)$ attached to f, n and H is the group of elements s in $H^1(H, T_{f,n})$ satisfying:*

1. *$\delta_\ell(s) = 0$ for all primes ℓ not dividing Np.*
2. *The class s is ordinary at primes $\ell \mid N^-p$.*
3. *The class s is trivial at primes $\ell \mid N^+$.*

Definition 2.3.10. *Let S be a squarefree integer which is relatively prime to pN. The Selmer group $H^1_S(H, T_{f,n})$ attached to f, S, and H is the group of elements κ in $H^1(H, T_{f,n})$ satisfying:*

1. *$\delta_\ell(\kappa) = 0$ for all primes ℓ not dividing SNp.*
2. *The class s is ordinary at primes $\ell \mid N^-p$.*
3. *The class s is arbitrary at primes $\ell \mid N^+$, and at the primes $\ell \mid S$.*

Proposition 2.3.11. *Let $s \in Sel_{f,n}(H)$ and $\kappa \in H^1_S(H, T_{f,n})$, we have the equality:*

$$\sum_{\ell|S} < s_\ell, \kappa_\ell >_\ell = 0.$$

Proof. This follows from global reciprocity laws in class field theory and Proposition 2.3.8. □

2.3.3 Construction of derivative classes

Lemma 2.3.12. *We have:*

$$H^1_{sing}(K_\ell, T_{f,n}) \simeq \begin{cases} 0 & \text{if } p^n \nmid \ell + 1 \pm a_\ell \\ \mathbb{Z}/p^n\mathbb{Z} & \text{if } p^n \mid \ell + 1 \pm a_\ell \quad \text{and } p \nmid \ell^2 - 1 \\ (\mathbb{Z}/p^n\mathbb{Z})^2 & \text{if } p^n \mid \ell + 1 \pm a_\ell \quad \text{and } \ell \mid \ell^2 - 1. \end{cases}$$

Proof. By definition $H^1_{sing}(K_\ell, T_{f,n}) := H^1(I_\ell, T_{f,n})^{G_{K_\ell}}$. Since $T_{f,n}$ is unramified at ℓ, the group is identified with the group of homomorphisms

$$Hom(I_\ell, T_{f,n})^{G_{K_\ell}} = Hom(I_\ell/p^n I_\ell, T_{f,n})^{G_{K_l}} = Hom(I_\ell/p^n I_\ell, T_{f,n}^{frob_\ell^2 = \ell^2}).$$

The characteristic polynomial of $Frob_\ell$ acting on $T_{f,n}$ is known to be $x^2 - a_\ell x + \ell$ and the result follows from the study of the eigenvalues. □

Lemma 2.3.13. *The natural maps*

$$H^1_{sing}(K_\ell, T_{f,n}) \to H^1_{sing}(K_\ell, T_{f,n-m})$$

are given by reduction modulo p^{n-m}.

Proof. This follows from the proof of Lemma 2.3.12. □

Lemma 2.3.14. *We have:*

$$H^1_{fin}(K_\ell, T_{f,n}) \simeq \begin{cases} 0 & \text{if } p^n \nmid \ell + 1 \pm a_\ell \\ \mathbb{Z}/p^n\mathbb{Z} & \text{if } p^n \mid \ell + 1 \pm a_\ell \quad \text{and } p \nmid \ell^2 - 1 \\ (\mathbb{Z}/p^n\mathbb{Z})^2 & \text{if } p^n \mid \ell + 1 \pm a_\ell \quad \text{and } p \mid \ell^2 - 1. \end{cases}$$

Proof. It follows from Lemma 2.3.12 and perfect local Tate duality. □

Lemma 2.3.15. *Suppose ℓ is inert in K, and ℓ doesn't divide the conductor of $\mathcal{O}$. We have $H^1(H_\ell, T_{f,n}) \simeq H^1(K_\ell, T_{f,n}) \otimes \mathbb{Z}[G_H]$. Furthermore, the action of G_H on $H^1(H, T_{f,n})$ commutes with the reduction*

$$H^1(H, T_{f,n}) \to H^1(H_\ell, T_{f,n}).$$

Proof. Since ℓ is inert in K and unramified in H, ℓ splits completely in H. The choice of a prime λ above ℓ determines an isomorphism

$$H^1(H_\ell, T_{f,n}) \simeq H^1(H_\ell, T_{f,n}) \otimes \mathbb{Z}[G_H].$$

The part about the action of G_H can be seen using the description of the cohomology groups as cocyles. □

Lemma 2.3.16. *Suppose that p doesn't divide $\ell^2 - 1$, then the local cohomology groups $H^1(K_\ell, T_{f,n})$ decompose as the direct sums:*

$$H^1_{sing}(K_\ell, T_{f,n}) \oplus H^1_{fin}(K_\ell, T_{f,n}) \text{ when } \ell \text{ doesn't divide } N,$$

$$H^1_{ord}(K_\ell, T_{f,n}) \oplus H^1_{fin}(K_\ell, T_{f,n}) \text{ when } \ell \text{ divides } N.$$

Proof. When $p^n \nmid \ell + 1 \pm a_\ell$, all the groups are trivial and there is nothing to prove. When p^n divides $\ell + 1 \pm a_\ell$, the module $T_{f,n}$ is the direct sums of two eigenspaces for the action of $Frob_\ell^2$ with eigenvalues 1 and ℓ^2. Since $p \nmid \ell^2 - 1$, the two eigenvalues are different mod p^n. Now, the finite part corresponds to the eigenvalue 1 whereas the singular or ordinary part corresponds to the eigenvalue ℓ^2. □

Definition 2.3.17. *A rational prime ℓ is said to be n-admissible relative to f if it satisfies:*

1. *ℓ does not divide N.*
2. *ℓ is inert in $K/\mathbb{Q}$.*
3. *p does not divide $\ell^2 - 1$.*
4. *p^n divides $\ell + 1 - a_l$ or $\ell + 1 + a_l$.*

Proposition 2.3.18. *Ler ℓ be an n-admissible prime and denote by $\overline{g}$ the natural projection of $g \in G_M$ into G_H. We have the following commutative diagram.*

$$\begin{array}{ccccc}
H^1(H, T_{f,n}) & \xrightarrow{Res} & H^1(M, T_{f,n}) & \xrightarrow{Cores} & H^1(H, T_{f,n}) \\
\downarrow Res & & \downarrow Res & & \downarrow Res \\
H^1(H_\ell, T_{f,n}) & \xrightarrow{Res} & H^1(M_\ell, T_{f,n}) & \longrightarrow & H^1(H_\ell, T_{f,n}) \\
\downarrow \sim & & \downarrow \sim & & \downarrow \sim \\
(\mathbb{Z}/p^n\mathbb{Z}[G_H])^2 & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z}[G_M])^2 & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z}[G_H])^2
\end{array}$$

$$h \longmapsto \sum_{g|\overline{g}=h} g$$

$$g \longmapsto \overline{g}$$

Proof. This follows from Lemma 2.3.16, Lemma 2.3.15 and the definition of the corestriction map. □

Definition 2.3.19. *A finite set S of primes is said to be an n-admissible set relative to f if:*

1. *All $\ell \in S$ are n-admissible primes relative to f.*
2. *The map $Sel_{n,f}(K) \to \bigoplus_{\ell \in S} H^1_f(K_\ell, T_{f,n})$ is injective.*

Proposition 2.3.20. *Any collection of n-admissible primes can be enlarged to an n-admissible set. In particular, n-admissible sets exist.*

Proof. This is explained in the discussion preceding Proposition 3.3 of [1]. □

Proposition 2.3.21. *If S is an $n-$admissible set, then the group $H^1(L, T_{f,n})$ is free of rank $\#S$ over $\mathbb{Z}/p^n\mathbb{Z}[G_L]$.*

Proof. It is Proposition 3.3 of [1]. □

Proposition 2.3.22. *The natural restriction map*

$$H^1(K, T_{f,n}) \to H^1(L, T_{f,n})^{G_L}$$

is an isomorphism.

Proof. The inflation-reduction exact sequence is:

$$H^1(L/K, T_{f,n}^{G_{\overline{L}/L}}) \to H^1(K, T_{f,n}) \to H^1(L, T_{f,n})^{G_L} \to H^2(L/K, T_{f,n}^{G_{\overline{L}/L}}),$$

and the result from $T_{f,n}^{G_{\overline{M}/M}} = 0$. □

Proposition 2.3.23. *Suppose that $m \leqslant n$, the natural map*

$$H^1(H, T_{f,m}) \to H^1(H, T_{f,n})[p^m]$$

is an isomorphism.

Proof. The surjectivity follows directly from the short exact sequence:

$$0 \to T_{f,m} \to T_{f,n} \to^{p^m} T_{f,n} \to 0.$$

The injectivity follows from $T_{f,n}^{G_{\overline{M}/M}} = 0$. □

Theorem 2.3.24. *Let s be a non-zero element of $H^1(K, T_{f,1})$. There exists infinitely many n-admissible primes ℓ relative to f and p such that $\delta_\ell(s) = 0$ and $v_\ell(s) \neq 0$.*

Proof. It is Theorem 3.2 in [1]. □

Theorem 2.3.25. *$Sel_{n,f}(L)$ is trivial iff $Sel_{n,f}(K)$ is trivial*

Proof. We have a natural injection $Sel_{n,f}(K) \subset Sel_{n,f}(L)$ which proves the implication.

Now suppose that $x \neq 0 \in Sel_{n,f}(L)$. The group G_L is the direct product of G_i where $G_i \simeq \mathbb{Z}/p^{k_i}\mathbb{Z}$.

Consider g_1 a generator of G_1. By the same reasoning as in the proof of Lemma 2.2.17, $(g_1 - 1)^{p^{k_1}} = p(g_1 - 1)h$ where h is an element in $\mathbb{Z}/p^n\mathbb{Z}[G_1]$ (here h is not necessarily invertible). Since $p^n.x = 0$, there exists $i_1 \geqslant 0$ such that $(g_1 - 1)^{i_1} \neq 0$ and $(g_1 - 1)^{i_1+1} = 0$. By induction, there exists an element $y \neq 0 \in Sel_{n,f}(L)$ such that y is invariant by G_L. By Proposition 2.3.22, the class y belongs to $Sel_{n,f}(K)$. □

Theorem 2.3.26. *For ℓ an admissible prime relative to p and f, there exist classes $\kappa(\ell) \in H^1_\ell(M, T_{f,n})$ such that:*

$$\delta_\ell(\kappa(\ell)) = \mathcal{L}_f \text{ (up to an element of } (\mathbb{Z}/p^n\mathbb{Z})^* \text{ and of } G_M),$$

$$v_\ell(\kappa(\ell)) = 0.$$

Using a Heegner point of conductor $\mathcal{O}$ on the indefinite $X_{N^+,N^-\ell}$

This theorem is key in all the proof and allow us to consider the $\mathcal{L}_f$ as localization of well chosen global cohomology classes. The proof is geometric and is far from being immediate. The way to construct the classes is the following: Let $X_{N^+,N^-\ell}$ be an "indefinite Shimura curve" associated to the couple $(N^+, N^-\ell)$. If we consider a Heegner point P_ℓ of conductor $\mathcal{O}$ which is defined over M, its image by the Kummer map is a class in $H^1_\ell(M, T_{f,n})$ that satisfies the desired properties. (See [1] section 5 to 8 for a deeper study of the construction.)

Corollary 2.3.27. *For ℓ an admissible prime relative to p and f, there is a class in $H^1_\ell(L, T_{f,n})$ still denoted $\kappa(\ell)$ by abuse of notation, satisfying:*

$$\delta_\ell(\kappa(\ell)) = \tilde{\mathcal{L}}_f \text{ (up to an element of } (\mathbb{Z}/p^n\mathbb{Z})^* \text{ and of } G_L),$$

$$v_\ell(\kappa(\ell)) = 0.$$

Proof. This follows for the previous Lemma and Proposition 2.3.18. □

Congruences between modular forms: Let ℓ_1 and ℓ_2 be n-admissible primes relative to f and such that p^n divides both $\ell_1 + 1 - \epsilon_1 a_{\ell_1}(f)$ and $\ell_2 + 1 - \epsilon_2 a_{\ell_2}(f)$ where ϵ_1 and ϵ_2 are equal to ± 1.

Let B' be the definite quaternion algebra of discriminant $Disc(B)\ell_1\ell_2$ and $R'_{N^+,N^-\ell_1\ell_2}$ be an Eichler order of level N^+ in B'. The theory of congruences between modular form yields to the following statement:

Proposition 2.3.28. *There exists a unique (up to an invertible scalar) eigenform $g : \widehat{R^*_{N^+,N^-\ell_1\ell_2}} \setminus \widehat{B^*}/B^* \to \mathbb{Z}/p^n\mathbb{Z}$, such that the equalities modulo p^n hold:*

$$T_q g = a_q(f) g \quad (q \nmid N\ell_1\ell_2), \quad W_q g = a_q(f) g \quad (q|N),$$

$$W_{\ell_1}(g) = \epsilon_1 g, \quad W_{\ell_2}(g) = \epsilon_2 g.$$

Proof. It is Theorem 3.10 of [1]. □

By Definition 2.2.4, for any order $\mathcal{O}$, we may associate to g and element $\tilde{\mathcal{L}}_g$. This element $\tilde{\mathcal{L}}_g$ appears as the finite localization of $\kappa(\ell)$ at n-admissible prime:

Theorem 2.3.29. *The equality*

$$v_{\ell_2}(\kappa(\ell_1)) = \tilde{\mathcal{L}}_g$$

hold in $H^1_{fin}(L_{\ell_2}, T_{f,n})$ up to multiplication by elements of $(\mathbb{Z}/p^n\mathbb{Z})^*$ and G_L.

Proof. It is Theorem 4.2 of [1]. □

The key point of the proof of Theorem 2.3.1 is to use the eigenform g associated to a pair (ℓ_1, ℓ_2) for an argument by induction. In order to do so, we need eigenforms with values in $\mathbb{Z}_p$ and not only in $\mathbb{Z}/p^n\mathbb{Z}$. The question is to be able to lift g. It is not possible for all pair (ℓ_1, ℓ_2) and consider now the cases for which such a lift exists:

Definition 2.3.30. *We say that a pair of n-admissible primes (ℓ_1, ℓ_2) is a rigid pair when the eigenform g associated to (ℓ_1, ℓ_2) can be lifted to an eigenform $\tilde{g}$ with values in $\mathbb{Z}_p$.*

Proposition 2.3.31. *Suppose that (ℓ_1, ℓ_2) is a rigid pair and that f is p-isolated then $\tilde{g}$ is p-isolated.*

Proof. It is Theorem 3.10 of [1]. □

The definition that we give here of a rigid pair is an ad hoc definition and a working definition can be found in [1] section 3. In particular, the authors of [1] prove that we can find sufficiently many rigid pair with properties analogous to Theorem 2.3.24. (See Theorem 3.10 and Theorem 3.11 in [1].)

2.3.4 A first general result

Theorem 2.3.32. *If $\tilde{\mathcal{L}_f}$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[G_L]$ then $Sel_{f,n}(L)^\vee$ is trivial.*

Proof. Since $\tilde{\mathcal{L}_f}$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[G_L]$ then for all n-admissible prime ℓ the class $\delta_\ell(\kappa(\ell))$ generates $H^1_{sing}(L_\ell, T_{f,n})$. By proposition 2.3.11 the maps

$$\eta_\ell : H^1_{sing}(L_\ell, T_{f,n}) \to Sel_{f,n}(L)^\vee$$

are trivial for all n-admissible primes.

Suppose that $Sel_{f,n}(L)$ is not trivial. By Propositions 2.3.23 and 2.3.25, we may find an element x of

$$Sel_{f,n}(L) \cap H^1(K, T_{f,1}).$$

By Proposition 2.3.24, there exists an n-admissible prime ℓ such that $v_\ell(x) \neq 0$ and $\delta_\ell(x) = 0$. Let $x_\vee$ be a generator of $H^1_{sing}(K_\ell, T_{f,n})$ that we see as $(x_\vee, 0..., 0)$ inside $H^1_{sing}(L_\ell, T_{f,n})$. By the choice of ℓ, we have $\eta_\ell(x_\vee)(x) =< x_\vee, x >_\ell \neq 0$, a contradiction with $\eta_\ell = 0$. □

2.3.5 Results in the tensor product with principal local rings

In this subsection we prove the following theorem:

Theorem 2.3.33. *For all n and all surjective morphisms $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}$, where $\mathcal{R}$ is a local principal ring, $\tilde{\mathcal{L}_f}$ satisfies:*

$$\varphi(\tilde{\mathcal{L}_f})^2 \text{ belongs to } Fitt_{\mathcal{R}}(Sel_{f,n}(L) \otimes_\varphi \mathcal{R}).$$

For now one, fix such a surjective morphism $\varphi : \mathbb{Z}_p[G] \to \mathcal{R}$, let π be a uniformizer of $\mathcal{R}$. Let denote $e = ord_\pi(p)$ and

$$t_f = ord_\pi(\varphi(\tilde{\mathcal{L}_f})).$$

We prove the Theorem 2.3.33 by induction on t_f and on the size of

$$Sel_{f,n,\varphi} := Sel_{f,n}(L) \otimes_\varphi \mathcal{R}.$$

Proposition 2.3.34. *If $t_f = 0$ then $Sel_{f,n,\varphi}$ is trivial*

Proof. Write $\tilde{\mathcal{L}_f} = h(g)(g-1) + val(f)$. Since φ sends I_G to $(\pi) \subset \mathcal{R}$, the nullity of t_f implies that $val(f) \neq 0 \pmod p$ and that $\tilde{\mathcal{L}_f}$ is a unit. The proposition follows then from Proposition 2.3.32. □

For the general case, let ℓ be any $n + t_f$-admissible prime and enlarge $\{\ell\}$ to an n-admissible set. By corollary 2.3.27, we can consider the class

$$\kappa(\ell) \in H^1_\ell(L, T_{f,n+t_f}) \subset H^1_S(L, T_{f,n}).$$

By Proposition 2.3.21, $\mathcal{M} := H^1_S(L, T_{f,n+t_f}) \otimes_\varphi \mathcal{R}$ is a free module over $\mathcal{R}/\pi^m$ for some m. Consider $\kappa_\varphi(\ell)$ the image of $\kappa(\ell) \in \mathcal{M}$. By construction,

$$ord_\pi(\kappa_\varphi(\ell)) \leqslant ord_\pi(\delta_\ell(\kappa_\varphi(\ell)) = ord_\pi(\tilde{\mathcal{L}_f}),$$

so that $t := ord_\pi(\kappa_\varphi(\ell)) \leqslant t_f$. Choose an element $\tilde{\kappa}_\varphi(\ell) \in \mathcal{M}$ such that

$$\pi^t \tilde{\kappa}_\varphi(\ell) = \kappa_\varphi(\ell).$$

The element $\tilde{\kappa}_\varphi(\ell)$ is only defined up to π^t torsion. To remove this ambiguity, we consider $\kappa'_\varphi(\ell)$ under the natural homomorphism:

$$H^1_S(L, T_{f,n+t_f}) \otimes_\varphi \mathcal{R} \to H^1_S(L, T_{f,n}) \otimes_\varphi \mathcal{R}.$$

Lemma 2.3.35. *The class $\kappa'_\varphi(\ell)$ enjoys the following properties:*

1. $ord_\pi(\kappa'_\varphi(\ell)) = 0$.
2. $\delta_q(\kappa'_\varphi(\ell)) = 0$, *for all* $q \nmid \ell N$.
3. $v_\ell(\kappa'_\varphi(\ell)) = 0$.
4. $ord_\pi(\delta_\ell(\kappa'_\varphi(\ell))) = t_f - t$.

Let Π be the set of rational primes ℓ that satisfy:

1. ℓ is an $n + t_f$ admissible prime.

2. The quantity $t = ord_\pi(\kappa_\varphi(\ell))$ is minimal among the primes satisfying condiction 1.

Lemma 2.3.36. *If $Sel_{f,n}(L)$ is not trivial, one has $t < t_f$.*

Proof. By Propositions 2.3.23 and 2.3.25, we may find an element x of

$$Sel_{f,n}(L) \cap H^1(K, T_{f,1}).$$

By Proposition 2.3.24, let ℓ be an $n-$admissible prime such that $v_\ell(x) \neq 0$ and $\delta_\ell(x) = 0$. Recall that under theses identifications, for all n-admissible prime q, x_q can be written

$$p^{n-1}(\sum_{g \in G} g)s_q$$

where s_q is an element of $H^1(L_q, T_{f,n})$ and by the choice of ℓ then s_ℓ can be taken as a generator of $H^1_f(L_\lambda, T_{f,n}) \subset H^1_f(L_\ell, T_{f,n})$ when $\lambda|\ell$.

We remark now that for any n-admissible prime q, if

$$y \in ker(H^1(L_q, T_{f,n}) \to H^1(L_q, T_{f,n}) \otimes \mathcal{R}),$$

then

$$< x_q, y >_q = 0.$$

Indeed $ker(\varphi)$ is contained in the maximal ideal $< I_{G_L}, p >$. So y is the sum $\sum_{g \in G_L}(g-1)y_g + py_0$ where y_g, y_0 are elements of $H^1(L_q, T_{f,n})$. By summing all the elements together:

$$\begin{aligned} < x_q, y >_q &= < x_q, \sum_{g \in G_L} (g-1)y_g + py_0 >_q \\ &= \sum_{g \in G_L} < (g-1)x_q, y_g) >_q + p^n < x_q, y_0 >_q \\ &= 0. \end{aligned}$$

Suppose that $t = t_f$:
Let $r \in \mathbb{Z}[G_L]$ such that

$$r.\delta_\ell(\kappa_\varphi(\ell)) = s_\ell^\vee \subset H^1_f(L_\ell, T_{f,n}) \otimes \mathcal{R},$$

where

$$s_\ell^\vee \text{ satisfies } < s_\ell^\vee, s_\ell >= 1.$$

Denote $y := r.\kappa_\varphi(\ell)$ and let $\tilde{y}$ be a preimage of x in $H^1_S(L, t_{f,n})$. We have $< x, \tilde{y} >= 0$ by global Tate duality. On the other hand, by the previous remark $< x, \tilde{y} >= < x_\ell, \tilde{y}_\ell >_\ell = 1$ a contradiction.

□

Lemma 2.3.37. *For all $\ell_1 \in \Pi$, there exists ℓ_2 in Π such that:*

$$ord_\pi(v_{\ell_2}(\kappa_\varphi(\ell_1))) = ord_\pi(v_{\ell_1}(\kappa_\varphi(\ell_2))) = ord_\pi(\varphi(\mathcal{L}_g)) = t,$$

where g is the eigenform associated to the pair (ℓ_1, ℓ_2) in Theorem 2.3.28.

Proof. Consider s the image of $\kappa'(\ell_1)$ in $H^1_S(K, T_{f,1}) \otimes_\varphi \mathcal{R}/(\pi)$. By Lemma 2.3.35, this image is non zero. Let $\tilde{s}$ be a preimage of s in $H^1_S(K, T_{f,1})$ and by Theorem 2.3.24, let ℓ_2 be a $n-$admissible prime such that $v_{\ell_2}(\tilde{s}) \neq 0$. We prove now that ℓ_2 satisfies the condictions of Lemma 2.3.38.

The three first equalities follow from the symmetry in Theorem 2.3.29. We need to prove the last equality relative to t.

Denote $\mathbf{F} = \mathcal{R}/(\pi)$ and consider the following diagram:

$$\begin{array}{ccccc} H^1_S(L,T_{f,n+t_f})\otimes_\varphi \mathcal{R} & \longrightarrow & H^1_S(L,T_{f,1})\otimes_\varphi \mathbf{F} & \xrightarrow{Cores} & H^1_S(K,T_{f,1})\otimes_\varphi \mathbf{F} \\ \downarrow v_{\ell_2} & & & & \downarrow v_{\ell_2} \\ H^1_f(L_{\ell_2}T_{f,n+t_f})\otimes_\varphi \mathcal{R} & \longrightarrow & H^1_f(L_{\ell_2}T_{f,n})\otimes_\varphi \mathcal{R} & \xrightarrow{Res} & H^1_f(K_{\ell_2},T_{f,1})\otimes_\varphi \mathbf{F} \end{array}$$

$$\begin{array}{ccccc} \tilde{\kappa}_\varphi(\ell_1) & \longrightarrow & \kappa'_\varphi(\ell_1) \pmod{\pi} & \longrightarrow & s \\ \downarrow v_{\ell_2} & & & & \downarrow v_{\ell_2} \\ v_{\ell_2}(\tilde{\kappa}_\varphi(\ell_1)) & \longrightarrow & v_{\ell_2}(\kappa'_\varphi(\ell_1)) & \longrightarrow & val(\kappa'_\varphi(\ell_1))\neq 0 \end{array}$$

The fact that $val(\kappa'_\varphi(\ell_1))\neq 0$ follows directly from the choice of ℓ_2 and it shows that $ord_\pi(v_{\ell_2}(\kappa'_\varphi(\ell_1)))=0$ and $ord_\pi(v_{\ell_2}(\kappa_\varphi(\ell_1)))=t$.

□

As mentioned earlier, in order to use induction, one needs a rigid pair (ℓ_1,ℓ_2) satisfying the previous lemma. The existence of such pairs is given by the following lemma:

Lemma 2.3.38. *There exist a rigid pair (ℓ_1,ℓ_2) satisfying the relations of Lemma 2.3.37*

Proof. This is Lemma 4.9 in [1]. The proof follows from the fact that we can find sufficiently many rigid pair as mentioned in the discussion after the Proposition 2.3.31. □

Let (ℓ_1,ℓ_2) be a rigid pair of elements in Π that satisfies

$$ord_\pi(v_{\ell_2}(\kappa_\varphi(\ell_1)))=ord_\pi(v_{\ell_1}(\kappa_\varphi(\ell_2)))=ord_\pi(\varphi(\mathcal{L}_g))=t,$$

where g is the modular form attached to the pair (ℓ_1,ℓ_2) in Proposition 2.3.28. By construction, we have $t_g=t<t_f$.

Consider the exact sequence:

$$0\to Sel_{f,n,[\ell_1,\ell_2]}(L)^\vee\to Sel_{f,n}(L)^\vee\to S^f_{\ell_1,\ell_2}\to 0,$$

where $Sel_{f,n,[\ell_1,\ell_2]}(L)$ is the set of element x in $Sel_{f,n}(L)$ satisfying:

$$x_{\ell_1}=x_{\ell_2}=0.$$

Locale Tate duality gives a surjection:

$$\eta_{\ell_1,\ell_2}: H^1_{sing}(L_{\ell_1},T_{f,n})\oplus H^1_{sing}(L_{\ell_2},T_{f,n})\to S^f_{\ell_1,\ell_2}.$$

By hypothesis, the map

$$H^1_{\ell_1}(L,T_{f,n})\to H^1_{\ell_1}(L,T_{f,n})\otimes_\varphi \mathcal{R}$$

is surjective and let s be a preimage of $\kappa'_\varphi(\ell_1)$ in $H^1_S(L,T_{f,n})$.

Considering the following diagram

$$\begin{array}{ccc} H^1_S(L,T_{f,n}) & \xrightarrow{0} & Sel_{f,n}(L)^\vee \\ \downarrow & & \downarrow \\ H^1_S(L,T_{f,n})\otimes_\varphi \mathcal{R} & \xrightarrow{0} & Sel_{f,n}(L)^\vee \otimes_\varphi \mathcal{R} \\ \downarrow & & \downarrow \\ \bigoplus_{q|S}(H^1_{sing}(L_q,T_{f,n})\otimes_\varphi \mathcal{R}) & \longrightarrow & Sel_{f,n}(L)^\vee \otimes_\varphi \mathcal{R}, \end{array}$$

shows that the element $(\delta_{\ell_1}(\kappa'_\varphi(\ell_1)),0)$ is in the kernel of $\eta_{\ell_1,\ell_2}\otimes\mathcal{R}$.

By symmetry, the same is true for ℓ_2 instead of ℓ_1. Using

$$ord_\pi(\delta_{\ell_i}(\kappa_{\ell_i})) = t_f - t,$$

leads to:

$$\pi^{2(t_f-t)}\text{belongs to the Fitting ideal of } S^f_{\ell_1,\ell_2}\otimes\mathcal{R}.$$

To finish the proof, we show that π^{2t} belongs to the Fitting ideal of $Sel_{f,n,[\ell_1,\ell_2]}(L)\otimes\mathcal{R}$.

Let consider the exact sequence:

$$0\to Sel_{g,n,[\ell_1,\ell_2]}(L)^\vee \to Sel_{g,n}(L)^\vee \to S^g_{\ell_1,\ell_2}\to 0,$$

where f has been replaced by g. The following isomorphism holds naturally:

$$Sel_{g,n,[\ell_1,\ell_2]}(L)^\vee \simeq Sel_{f,n,[\ell_1,\ell_2]}(L)^\vee.$$

Locale Tate duality gives a surjection:

$$\eta'_{\ell_1,\ell_2} : H^1_{fin}(L_{\ell_1},T_{f,n})\oplus H^1_{fin}(L_{\ell_2},T_{f,n})\to S^g_{\ell_1,\ell_2}$$

and by the same reasoning as before, the elements

$$x_1 := (v_{\ell_1}(\kappa'_\varphi(\ell_2)),0) \text{ and } x_2 := (0, v_{\ell_2}(\kappa'_\varphi(\ell_1)))$$

belong to the kernel of $\eta'_{\ell_1,\ell_2}\otimes\mathcal{R}$. But since x_1 and x_2 generate

$$(H^1_{fin}(L_{\ell_1},T_{f,n})\oplus H^1_{fin}(L_{\ell_2},T_{f,n}))\otimes_\varphi\mathcal{R},$$

we have

$$S^g_{\ell_1,\ell_2}\otimes\mathcal{R}\text{ is trivial}$$

and

$$Sel_{g,n,[\ell_1,\ell_2]}(L)^\vee\otimes\mathcal{R} = Sel_{g,n}(L)^\vee\otimes\mathcal{R}.$$

By induction (the justification for using induction is explained at the end of the proof in Proposition 2.3.39)

$$\pi^{2t_g}\text{ belongs to the Fitting ideal of } Sel_{g,n}(L)^\vee\otimes\mathcal{R}.$$

Finally,

$$\begin{aligned}\pi^{2t_f} &= \pi^{2(t_f-t_g)}\pi^{2t_g} \\ &\in Fitt_{\mathcal{R}}(S^f_{\ell_1\ell_2})Fitt_{\mathcal{R}}(Sel^{\vee}_{g,n}\otimes\mathcal{R}) \\ &= Fitt_{\mathcal{R}}(S^f_{\ell_1\ell_2})Fitt_{\mathcal{R}}(Sel^{\vee}_{g,n,[\ell_1\ell_2]}\otimes\mathcal{R}) \\ &\subseteq Fitt_{\mathcal{R}}(Sel^{\vee}_{f,n}\otimes\mathcal{R}),\end{aligned}$$

where the last equality comes from the well-known properties of the Fitting ideal towards short exact sequence. (The definition and some basic properties of Fitting ideals can be found in [10] XIX §2.)

□

Proposition 2.3.39. *The lift $\tilde{g}$ of g satisfies assumptions 2.3.2.*

Proof. Assumption 1. is trivially satisfied. By Theorem 5.17 in [1], the Galois representations $T_{f,n}$ and $T_{g,n}$ are isomorphic. From this, assumption 4. is immediate. Assumptions 2. and 5. also follow from this isomorphism and the fact that p doesn't divide ℓ_i+1 (see in addition the discussion after the assumptions 2.3.2 for 5.) Finally assumption 3. follows from Proposition 2.3.31. □

2.4 The case of elliptic curves over $\mathbb{Q}$

For this section, fix E an elliptic curve over $\mathbb{Q}$ without complex multiplication and with associated eigenform f. We put all the pieces together of section 1 and 2 to formulate a theorem that relates the rank r_E of E over K and the order of vanishing of the theta elements. For the notation, denote $d :=< D_f, D_f >$, where $< D_f, D_f >$ is defined in subsection 2.2.2.

Let fix an order $\mathcal{O}_c$ of conductor c prime to $N.D$ and let denote

$$G = Pic(\mathcal{O}_c).$$

Let M_c be the product of all primes dividing $\#G$ that don't satisfy assumption 2.3.2. As a remark, if

$$c = \prod_i \ell_i^{n_i},$$

then

$$\#G = \prod_i (\ell_i - \epsilon(\ell_i))\ell_i^{n_i-1}\#Pic(\mathcal{O}_K).$$

The fact that almost all ordinary primes satisfy assumption 2.3.2 assure that we can find c such that M is not too "big".

Theorem 2.4.1. *For all $p \nmid M_c d$ and all surjective morphisms*

$$\varphi : \mathbb{Z}_p[G] \to \mathcal{R},$$

where $\mathcal{R}$ is a principal local ring with uniformizer π,

$$\varphi(\Theta(\mathcal{O}_c, E)) \text{ belongs to } (\varphi(I_G))^{r_E}.$$

Proof. Fix a prime p that doesn't divide $M_c.d$ and a surjective morphism

$$\varphi : \mathbb{Z}[\frac{1}{D_f}][G] \to \mathcal{R},$$

where $\mathcal{R}$ is a principal local ring with uniformizer π.

By Theorem 2.3.33, we have:

$$\varphi(\Theta(\mathcal{O}_c, E)) \text{ belongs to } Fitt_{\mathcal{R}}(Sel_{f,n}(L)^\vee \otimes_\varphi \mathcal{R}),$$

and we want to prove that

$$Fitt_{\mathcal{R}}(Sel_{f,n}(L)^\vee \otimes_\varphi \mathcal{R}) \subset (\pi)^{r_E}.$$

The Kummer map gives an injection:

$$E(K)/p^n E(K) \hookrightarrow Sel_{f,n}(L).$$

Since $\mathbb{Z}/p^n\mathbb{Z}$ is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module, the injection gives a surjection for the duals:

$$Sel_{f,n}(L)^\vee \twoheadrightarrow E(K)/p^n E(K),$$

that we can tensor by $\mathcal{R}$ over $\mathbb{Z}/p^n\mathbb{Z}[G]$ to get:

$$Sel_{f,n}(L)^\vee \otimes_\varphi \mathcal{R} \twoheadrightarrow E(K)/p^n E(K) \otimes_\varphi \mathcal{R}.$$

By the usual properties of Fitting ideals, we have

$$Fitt_{\mathcal{R}}(Sel_{f,n}(L) \otimes_\varphi \mathcal{R}) \subset Fitt_{\mathcal{R}}(E(K)/p^n E(K) \otimes_\varphi \mathcal{R}).$$

Finally, we have:

$$\begin{aligned} Fitt_{\mathcal{R}}(E(K)/p^n E(K) \otimes_\varphi \mathcal{R}) &= Fitt_{\mathcal{R}}((\mathbb{Z}/p^n\mathbb{Z}))^{r_E} \otimes_\varphi \mathcal{R}) \\ &= Fitt_{\mathcal{R}}((\mathbb{Z}/p^n\mathbb{Z})) \otimes_\varphi \mathcal{R})^{r_E} \\ &= Fitt_{\mathcal{R}}(\mathcal{R}/(\varphi(I_G)))^{r_E} \\ &= (\varphi(I_G))^{r_E}. \end{aligned}$$

The equality at all levels n, shows the equality in $\mathbb{Z}_p[G]$. □

Theorem 2.4.2. *1. If $Pic(\mathcal{O}_c)^{(p)} \simeq (\mathbb{Z}/p\mathbb{Z})^{n_p}$ (recall that $Pic(\mathcal{O}_c)^{(p)}$ is the p-part of $Pic(\mathcal{O}_c)$) whenever $p \nmid M_c$, then:*

$$ord_{\mathbb{Z}[\frac{1}{M_c(r_E-2)!}][Pic(\mathcal{O}_c)]}(\Theta(E,K,\mathcal{O}_c)) \geqslant r_E.$$

2. If $r_E \leqslant 2$ then:

$$ord_{\mathbb{Z}[\frac{1}{M_c}][Pic(\mathcal{O}_c)]}(\Theta(E,K,\mathcal{O}_c)) \geqslant r_E.$$

3. If p doesn't divide M_c then:

$$ord_{\mathbb{F}_p[Pic(\mathcal{O}_c)]}(\Theta(E,K,\mathcal{O}_c)) \geqslant r_E.$$

Proof. This follows by combining Theorem 2.4.1, Theorem 2.2.22, Theorem 2.2.23, Theorem 2.2.25 and Theorem 2.2.26. □

Appendix

2.A A special case of Theorem 2.4.2

We keep the notation of section 2.3. In this appendix, we deal with the special case of $r_E \geqslant 1$ and we prove that $\tilde{\mathcal{L}}_f$ belongs to $I_{G_L} \subset \mathbb{Z}_p[G_L]$. It is a special case of Theorem 2.4.2 but the following proof doesn't use any induction argument, or any morphism φ so that the Euler system argument appears clearer.

Lemma 2.A.1. *Suppose that $rk(E(K)) \geqslant 1$, then for all n, there exists $s \in Sel_{f,n}(K)$ such that s has order exactly p^n.*

Proof. We use the short exact sequence

$$0 \to E(\overline{K})[p^n] \to E(\overline{K}) \to E(\overline{K}) \to 0.$$

Taking the associated exact sequence in cohomology leads to the injection

$$E(K)/p^n E(K) \hookrightarrow Sel_{f,n}(K).$$

If $rk(E(K)) \geqslant 1$, then we have at least one element of order exactly p^n in $E(K)/p^n E(K)$ and the result follows. □

Theorem 2.A.2. *Suppose that the rank of $E(K)$ is greater than one, then $\tilde{\mathcal{L}}_f$ belongs to $I_{G_L} \subset \mathbb{Z}_p[G_L]$.*

Proof. Fix $n > 0$. By Lemma 2.A.1, we take $x \in Sel_{f,n}(K)$ with order exactly p^n.Choose S an n-admissible set and $\ell \in S$ such that $x_\ell \in H^1_f(K_\ell, T_{f,n})$ has order exactly p^n. Such an ℓ exists by part 2. of Definition 2.3.19 and Proposition 2.3.20. Denote s the image of x in $Sel_{f,n}(L)$. By Proposition 2.3.22, it has order exactly p^n and is invariant by G_L. By Lemma 2.3.15 and local Tate duality, we have for all $\kappa \in H^1_{sing}(L_\ell, T_{f,n})$:

$$< \kappa, s >_\ell \equiv val(\kappa)[p^n] \text{ up to multiplication by an element of } (\mathbb{Z}/p^n\mathbb{Z})^*,$$

where κ is seen as an element of $\mathbb{Z}/p^n\mathbb{Z}[G_L]$.

Let $\kappa(\ell)$ be the class constructed in Theorem 2.3.27, then by global Tate duality:

$$\sum_q < \kappa(\ell)_q, s_q >_q = 0.$$

By construction,

$$\sum_q < \kappa(\ell)_q, s_l >_q = < \kappa(\ell)_l, s_\ell >_\ell = val(\tilde{\mathcal{L}}_f) \equiv 0[p^n].$$

Finally, $val(\tilde{\mathcal{L}}_f) \equiv 0[p^n]$ for all $n \geq 1$, which shows that $val(\tilde{\mathcal{L}}_f) = 0$ and that $\tilde{\mathcal{L}}_f$ belongs to $I_{G_L} \subset \mathbb{Z}_p[G_L]$.

□

Further directions

This work raises as many (and perhaps, more) questions as it settles, of which we now describe a few.

At first, one could try to develop tools to understand objects in the group rings $\mathbb{Z}[G]$. In our case, we are able to understand the properties of the image of the theta elements in principal local ring but we fail to transpose all these properties for the initial theta elements in the group ring $\mathbb{Z}[G]$. To overcome this difficulty, one could maybe work directly with the modules over the group rings (and not with the tensorisation with the rings $\mathcal{R}$) and use the induction directly at this level. One could also try to use a Iwasawa type argument adapted to the case of group ring. This last idea is still very vague but echoes with the now famous patching technique of Taylor-Wiles.

A second and natural continuation would be to try to treat all the primes p indifferently and not only almost all ordinary primes. The case of ordinary primes that do not satisfy assumption 2.3.2 seems to be purely technical. The same arguments seem to be doable in this case but at the price of more complicated and tedious proofs. The case of supersingular primes raises a more conceptual question. The problem here is to define an appropriate local condition at p for $H^1(L_p, T_{f,n})$ such that the resulting subgroup is selfdual with respect to the local Tate pairing and such that it contains the p-localization of the classes $\kappa(\ell)$ defined in Theorem 2.3.26. A definition of such a local condition using Dieudonné modules and Fontaine's theory can be found in [6] for special cases of supersingular prime. To be precise, a key argument would be to generalize the Theorem 3.10 of [6]. As a final remark on this specific topic, there is no need to define a local condition for all the n-admissible primes but for sufficiently many n-admissible primes where the word "sufficiently" has to be taken as in Theorem 2.3.24.

Thirdly, one may try to refine the lower bound r_Θ of the order

of vanishing of our theta elements. The question is to understand if our lower bound is sharp. It seems that it isn't and that we can refine Conjecture 2.1.1 to incorporate the rank of E twisted by K. The construction of $\Theta(E, K, \mathcal{O})$ (as the construction of the L-function that it interpolates) really depends on the field K and it would be surprising indeed that its order of vanishing only depends on E. The refinement is for instance treated for ordinary primes in the setting of Iwasawa algebras in section 4 of [2], or also in [3] and [4]. The present author thinks that such a refinement shouldn't raise any major issues in the settings of ordinary primes but it still needs to be done.

The conjectures and theorems given in this paper deal with lower bound of the order of vanishing r_Θ of our theta elements. Ultimately, one could wish to understand precisely the value of r_Θ. In order to do so, one could try to give the reverse inequality and study upper bounds of r_Θ. The use of Euler system argument would be useless there since Euler system arguments can only be used to bound the size of modules from above and not the opposite. Nevertheless, recent works of W.Zhang and Skinner-Urban seem to be fruitful for this kind of questions and give hope to formulate a precise theorem for the values of r_Θ ([22],[26]). One may try in particular to adapt the methods of W.Zhang in [27] where the converse equality seems to be treated in the case where N^- is the squarefree product of an even number of primes. An even further step would be then interesting to understand the image of our theta elements in $I_G^{r_\Theta}/I_G^{r_\Theta+1}$ (the so-called leading terms).

Bibliography

[1] M. Bertolini and H. Darmon, *Iwasawa's Main Conjecture for Elliptic Curves over Anticyclotomic $\mathbb{Z}_p$-extensions* In: Annals of Mathematics, **162** (2005) 1-64.

[2] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves* In: Inventiones Math **126** (1996) 413-456.

[3] M. Bertolini and H. Darmon, *Derived p-adic heights* In: Amer. J. Math. **117** (1995), no 6, 1517-1554.

[4] M. Bertolini and H. Darmon, *Derived heights and generalized Mazur-Tate regulators* In: Duke Math. J. **76** (1994),no 1, 75-111.

[5] H. Darmon, *Thaine's method for circular units and a conjecture of Gross.* In: Canad. J. Math. **47** (1995) 302-317.

[6] H. Darmon and A. Iovita, *The anticyclotomic main conjecture for supersingular elliptic curves.* In: Journal de l'Institut Mathématique de Jussieu, **7** Issue 2 (2008) 291-325.

[7] M. Flach, *Iwasawa theory and motivic L-functions.* In: Pure Appl. Math. Q. **5** (1, Sp.). pp. 255-294.

[8] H. Darmon, F. Diamond and R. Taylor, *Fermat's Last Theorem* In: Current Developments in Mathematics **1** (1995) International Press, pp. 1-157.

[9] B. Gross, *Heights and the Special values of L-series* In: Canad. Math. Soc. **Volume 7** (1987)

[10] S. Lang, *Algebra* Springer-Verlag (1965)

[11] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms.* In: Astérisque 295 (2004), 117-290

[12] B. Mazur and K. Rubin, *Kolyvagin systems.* Mem. Amer. Math. Soc. **799** (2004).

[13] B. Mazur and K. Rubin, *Refined class number formulas and Kolyvagin systems.* In: Compos. Math. **147** (2011), pp. 56-74.

[14] B. Mazur and K. Rubin, *Refined class number formulas for $\mathbb{G}_m$. Preprint.*

[15] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*. In: Duke Math. J. **54**, No. 2, (1987), pp. 711.

[16] K. Rubin, *Euler System.* Ann. of Math. Stud. **147** (2000)

[17] K. Rubin, *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer in Arithmetic Theory of Elliptic Curves.* In: Lectures Notes in Mathematics **1716** (1997), pp. 167-234.

[18] J-P. Serre, *Corps locaux.* 4e édition Hermann, Paris (1968).

[19] J-P. Serre, *Trees*, Springer-Verlag (1980)

[20] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, In: Inventiones Math **volume 15** (1972) pp. 259 - 331

[21] C L. Siegel *Advanced Analytic Number Theory* Tata Inst. Fund. Res. Stud. Math. (1965)

[22] C. Skinner and E. Urban *The Iwasawa main conjecture for GL_2* To appear in Inventiones Math.

[23] M-F. Vignéras, *Arithmétique des algèbres de quaternions* In: Lecture Notes in Math. **800**, Springer Verlag.

[24] X. Yuan, S. Zhang and W.Zhang *The Gross-Zagier Formula on Shimura Curves* In: Annals of Nathematics Studies.

[25] S. Zhang, *Gross-Zagier formula for GL_2* In: Asian J. Math. **5**, (2001), no.2, pp. 183 - 290.

[26] W. Zhang, *Selmer groups amd divisibility of Heegner points* Preprint (2013)

[27] W. Zhang, *A Birch-Swinnerton-Dyer type conjecture for Selmer groups* Preprint (2013)