Algebraic cycles and Diophantine geometry

Generalised Heegner cycles, quadratic Chabauty & diagonal cycles

David Ter-Borch Gram Lilienfeldt

Department of Mathematics and Statistics
McGill University, Montreal

March, 2021

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

Contents

Abstract

This thesis studies three distinct but interrelated topics revolving around the theme of rational points on curves defined over number fields. The guiding questions differ depending on the genus of the curves under investigation: we distinguish between the case of elliptic curves (genus one case) and the case of higher genus curves.

In the context of elliptic curves, the difficulty lies in constructing interesting rational points in view of shedding light on the famous Birch and Swinnerton-Dyer conjecture. A possible direction is the study of algebraic cycles and their resulting Chow–Heegner points.

Chapter 2, which is joint work with Henri Darmon, Massimo Bertolini and Kartik Prasanna, explores questions related to generalised Heegner cycles on products of Kuga–Sato varieties with powers of a CM elliptic curve. The first main result is a formula for the image of these cycles under the complex Abel–Jacobi map in terms of explicit line integrals of modular forms on the complex upper half-plane. Such a formula has implications for the corresponding Chow–Heegner points on the CM elliptic curve. The second main theorem uses this formula to show that the Chow group and the Griffiths group of the relevant product varieties are not finitely generated. More precisely, it is shown that the subgroup generated by the images of generalised Heegner cycles has infinite rank in the group of null-homologous cycles modulo both rational and algebraic equivalence.

Chapter 4 focuses on the setting of diagonal type cycles on the triple product of the modular curve $X_0(p)$ of prime level p. The main motivation stems from the Beilinson–Bloch conjecture in this particular setting. This conjecture predicts the equality between the central order of vanishing of the triple product L-function associated to three normalised newforms in $S_2(\Gamma_0(p))$ on the one hand, and the rank of the (f_1, f_2, f_3)-isotypic component of the null-homologous Chow group of $X_0(p)^3$ of codimension two on the other hand. One of the main results asserts that the global root number of the triple product L-function of (f_1, f_2, f_3) twisted by the Legendre symbol χ at p is always -1. In parallel, we construct a canonical null-homologous cycle on $X_0(p)^3$ of codimension 2 which lies in the (-1)-eigenspace of the Chow group for the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{\chi(-1)p})/\mathbb{Q})$. This leads us to formulate refinements of the Beilinson–Bloch conjecture in a setting which has not been considered before. Specialising to the case where f_3 has rational coefficients and $f_1 = f_2$, we formulate further refined conjectures concerning the associated Chow–Heegner points on the elliptic curve associated with f_3. When the global root number of the triple product (f_1, f_2, f_3) is $+1$, we prove that the image of the Gross–Kudla–Schoen cycle under the complex Abel–Jacobi map is torsion in the (f_1, f_2, f_3)-isotypic component of the second intermediate Jacobian of $X_0(p)^3$, and deduce torsion properties of the related Chow–Heegner points, which had originally been studied by Darmon, Rotger and Sols in the case where the root number is

-1. Moreover, we prove that the Chow–Heegner points associated to the special cycle defined over $\mathbb{Q}(\sqrt{-p})$ are torsion whenever $p \equiv 3 \pmod 4$. Such torsion properties fit nicely with the proposed conjectures, and are in line with the Beilinson–Bloch and Birch–Swinnerton-Dyer conjectures.

In the context of higher genus curves, it is known by Faltings' famous proof of Mordell's conjecture that any smooth, projective, geometrically irreducible curve of genus greater than one over a number field has only finitely many rational points. However, this does not allow for the explicit determination of this finite set, given that Faltings' proof is not effective. Chapter 3, which is joint work with Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao, generalises the geometric quadratic Chabauty method, initiated over $\mathbb{Q}$ by Edixhoven and Lido, to higher genus curves defined over arbitrary number fields. This results in a conditional bound on the number of rational points on curves that satisfy an additional Chabauty type condition on the rank of the Jacobian of the curve. The method gives a more direct approach to the generalisation by Dogra of the quadratic Chabauty method to arbitrary number fields. As such, this work can be viewed as part of the non-abelian Chabauty program initiated by Kim.

Résumé

Cette thèse traite de trois sujets distincts quoique liés autour du thème des points rationnels sur les courbes algébriques définies sur des corps de nombres. Les questions directrices varient selon le genre des courbes considérées: nous distinguerons entre le cas des courbes elliptiques (de genre égal à un) et celui des courbes de genre supérieur ou égal à deux.

La problématique principale dans le contexte des courbes elliptiques provient du fait qu'il est difficile de construire des points rationnels interéssants sur de telles courbes. Ceci est formulé plus précisément dans la fameuse conjecture de Birch et Swinnerton-Dyer. Une approche possible de ce problème est l'étude de cycles algébriques et des points dits de Chow–Heegner qui en découlent.

Le Chapitre 2, qui est un travail en commun avec Henri Darmon, Massimo Bertolini et Kartik Prasanna, traite des cycles de Heegner généralisés sur le produit d'une variété de Kuga–Sato avec une puissance d'une courbe elliptique à multiplication complexe. Le premier résultat principal est une formule pour l'image de ces cycles par l'application d'Abel–Jacobi complexe en termes d'intégrales explicites de formes modulaires sur le demi-plan supérieur de Poincaré. Une telle formule peut être utilisée pour déduire des propriétés des points de Chow–Heegner associés. Le second résultat principal se sert de cette formule pour démontrer que le groupe de Chow ainsi que le groupe de Griffiths des variétés produits ci-dessus ne sont pas de type fini. Plus précisément, il est démontré que le sous-groupe engendré par les cycles de Heegner généralisés est de rang infini dans le groupe des cycles homologues à zéro modulo l'équivalence rationnelle ainsi qu'algébrique.

Le Chapitre 4 porte sur les cycles diagonaux sur le produit triple de la courbe modulaire $X_0(p)$ où p est un nombre premier. La motivation principale provient de la conjecture de Beilinson–Bloch dans le contexte particulier du produit triple. Celle-ci prédit l'égalité entre, d'une part, l'ordre d'annulation de la fonction L associée à un triplet de formes modulaires paraboliques $f_1, f_2, f_3 \in S_2(\Gamma_0(p))$ en son centre $s = 2$ et, d'autre part, le rang de la composante (f_1, f_2, f_3)-isotypique du groupe de Chow des cycles homologues à zéro et de codimension 2 sur $X_0(p)^3$. Le premier résultat dit la chose suivante: si χ désigne le symbole de Legendre en p, alors le signe de l'équation fonctionnelle de $L(f_1 \otimes f_2 \otimes f_3 \otimes \chi, s)$ est négatif. En parallèle, on construit sur $X_0(p)^3$ un cycle canonique, homologue à zéro, de codimension 2 et défini sur $\mathbb{Q}(\sqrt{\chi(-1)p})$ (i.e., l'extension quadratique de $\mathbb{Q}$ associée au caractère χ). De plus, l'automorphisme non trivial de cette extension agit sur le cycle avec valeur propre égale à -1. Ceci nous amène à formuler un raffinement de la conjecture de Beilinson–Bloch dans un contexte nouveau. En spécialisant au cas où f_3 est à coefficients de Fourier rationnels et $f_1 = f_2$, nous formulons des raffinements de la conjecture de Birch et Swinnerton-Dyer concernant les points de Chow–Heegner sur la courbe elliptique correspondant à f_3 associés

au cycle spécial. Lorsque le signe de l'équation fonctionnelle de $L(f_1 \otimes f_2 \otimes f_3, s)$ est positif, nous démontrons que l'image du cycle de Gross–Kudla–Schoen par l'application d'Abel–Jacobi complexe est de torsion dans la composante (f_1, f_2, f_3)-isotypique de la Jacobienne intermédiaire de $X_0(p)^3$, et nous déduisons les propriétés de torsion des points de Chow–Heegner associés à ce cycle. Ces derniers ont fait l'objet d'étude dans le travail de Darmon, Rotger et Sols lorsque le signe de l'équation fonctionnelle est négatif. De plus, nous prouvons que les points de Chow–Heegner associés au cycle spécial défini sur $\mathbb{Q}(\sqrt{-p})$ sont de torsion lorsque $p \equiv 3 \pmod 4$. Ces propriétés de torsion s'accordent bien avec les conjectures proposées, ainsi que les conjectures de Beilinson–Bloch et de Birch et Swinnerton-Dyer.

Dans le contexte des courbes de genre supérieur, il est bien connu depuis la fameuse preuve de Faltings de la conjecture de Mordell que toute courbe lisse, projective et géométriquement irréductible de genre supérieur ou égal à deux définie sur un corps de nombres n'admet qu'un nombre fini de points rationnels. Du fait que la preuve de Faltings n'est pas effective, la détermination explicite de cet ensemble fini pour une courbe donnée demeure aujourd'hui un problème difficile. Le Chapitre 3, qui est un travail en commun avec Pavel Čoupek, Luciena Xiao Xiao, et Zijian Yao, généralise la méthode de Chabauty quadratique géométrique, due à Edixhoven et Lido sur $\mathbb{Q}$, aux courbes de genre supérieur définies sur des corps de nombres arbitraires. Ceci fournit une borne conditionnelle sur le nombre de points rationnels sur de telles courbes satisfaisant de plus à une condition de type Chabauty sur le rang de la Jacobienne de la courbe en question. Cette méthode peut être interprétée comme une approche plus directe à la généralisation de Dogra de la méthode de Chabauty quadratique aux corps des nombres arbitraires. Ainsi, ce travail s'insère naturellement dans le cadre plus général du programme de Chabauty non-abélien initié par Kim.

Acknowledgements

First of all, I wish to thank my supervisor, Henri Darmon, for his invaluable advice and guidance from the beginning until the end of my doctoral degree. I have benefitted not only from his vast knowledge of mathematics, but also from his skills as an excellent teacher and communicator of mathematics; he has been, and continues to be, a role model for me as a mathematician. He has guided me through the beginning steps of my career, from my first research talk, to writing my first paper, and finally to doing my job applications. Thanks to him, I feel ready for the next exciting step in my career as a mathematician. I am very grateful and proud to say that I have been his student.

Going back to my days at the École Polytechnique Fédérale de Lausanne, I wish to thank Eva Bayer–Fluckiger for introducing me to the theory of algebraic number theory and arithmetic geometry. She opened a lot of doors for me by giving me the opportunity to be a member of her research group. I extend my thanks to Peter Jossen and Mathieu Huruguen, both postdocs during my time at the EPFL, who supervised my Bachelor and Master semester projects within Eva Bayer–Fluckiger's group, and who both taught me a lot. Finally, I thank Benedict Gross who accepted to host and supervise my stay at Harvard where I wrote my Master thesis; the lessons learned about mathematics and life remain invaluable. Je remercie tous les amis de Lausanne et spécialement Marco Biemann, Hadrien Espic, Quentin Le Moal, Jonathan Moustakis et Raphaël Zacharias: sans vous ces années passées dans le couloir de la mort (et à SAT) n'auraient pas été les mêmes !

Back to the present day, I want to thank all the members of the Montréal Number Theory group who have made this city a vibrant and exciting place to study mathematics. In particular, I thank my fellow students Michele Fornea, Alice Pozzi, Isabella Negrini, James Rickards, Nicolas Simard and Peter Xu who were/are also advised by Henri Darmon. I also thank Óscar Rivero, Ricardo Toso and Francesc Gispert Sánchez for stimulating conversations. James, thanks for sharing both office and advisor with me during all these years, and for all the interesting conversations, card-throwing games, and winter camping ! Michele, thank you for your important role as a friend and mentor, your advice has always been, and continues to be, very dear to me ! My sincere thanks go to Jan Vonk, who was a postdoc at McGill during my first years of study, and who was and is still a great support for me, both as a friend and mentor. I thank Eyal Goren for his helpfulness and guidance. I thank Adrian Iovita for stimulating conversations, great teaching, and his help with my job applications. I also thank Daniel Wise for his mentorship in teaching mathematics and his help with my job applications. Finally, I thank all my fellow students at McGill who have made these past years (and our lunch discussions) exciting and stimulating.

Including my advisor Henri Darmon, my special thanks go to my collaborators Massimo

Bertolini, Kartik Prasanna, Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao, who generously agreed to let me include our joint works in this thesis.

I take the opportunity to thank the organisers of the Arizona Winter School 2020, where my collaboration with Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao started, resulting in our preprint [41]. I thank Bas Edixhoven, Guido Lido and Jan Vonk for suggesting this project and guiding us through the early stages.

During my doctoral studies I have benefitted from the following scholarships and awards: the Alexis and Charles Pelletier Fellowship, the ISM Graduate Scholarship, the ISM Scholarship for Outstanding PhD Candidates, as well as the ISM and GREAT travel awards. I acknowledge this funding support and am grateful to the Institut de Sciences Mathématiques au Québec (ISM), the McGill Faculty of Science, and the Pelletier family.

I thank the members and staff of the Department of Mathematics and Statistics at McGill University for their guidance, patience and helpfulness.

I am grateful to Benedict Gross for pointing out a mistake in a preliminary version of this thesis.

I defended my thesis on May 20, 2021 remotely on Zoom. I thank the members of my doctoral oral defence committee: Jacques Hurtubise (Chair), Henri Darmon (Supervisor), Eyal Goren (Internal Examiner), Patrick Allen (Internal Member), Netan Dogra (External Examiner), and Christoph Neidhöfer (Pro-Dean). I am grateful to my examiners, Eyal Goren and Netan Dogran, for their valuable feedback which helped to improve the quality of the exposition and the mathematics of this thesis.

To my friends from all around the world: your support and friendship mean so much to me – tak, merci, thank you ! Thanks in particular to all of you who are based in Montréal – you have made my stay at rue Bagg incredible and I will forever miss the park hangs in Jeanne–Mance !

Sidst men ikke mindst, går den største tak til min familie. Far og mor, tak for jeres konstante støtte og kærlighed. Rachel og Noah, det har været så skønt at have jer i Montréal, og så endda som roommates ! Jeres opbakning og kærlighed er min største styrke i denne verden; jeg elsker jer alle fire højere end alt ! Estelle, merci pour tout ♡

Contribution to original knowledge

Chapters 2, 3 and 4 constitute the main body of this thesis and are considered original scholarship and distinct contributions to knowledge. Chapter 1 collects the background material necessary to understand the main body of the thesis: the covered material does not contain any new contributions to knowledge and does not constitute original scholarship. All sources of the included material are clearly cited and referenced. Chapter 5 outlines possible future directions of research of the author. The ideas and projects proposed are, to the best of the authors knowledge, new and unexplored.

Chapter 3 is a reformatted and slightly modified version of the preprint article [41] available on the author's website.

Chapter 2 is a reformatted and slightly modified version of the article [11] first published in *Mathematische Zeitschrift*. By clause 4.*c*. of the Copyright Transfer Statement for the article [11] to Springer-Verlag GmbH Germany, part of Springer Nature, the author of the present thesis, David Ter-Borch Gram Lilienfeldt, retains the right to reproduce the article [11] in whole or in part in any printed volume (book or thesis) written by him.

Contribution of Authors

The author, David Ter-Borch Gram Lilienfeldt, has written this whole thesis alone. His supervisor, Henri Darmon, has proofread the thesis and helped with the editing.

The introduction is written by the author alone. The only originality lies in the way the material is presented and in Section 0.4 outlining the contributions of this thesis.

Chapter 1 is written by the author alone and collects background material for the main body of the thesis: as such, it does not contain any original ideas by the author. The only originality lies in the way the material is organised.

Chapters 2, 3 and 4 constitute the main body of this thesis and are considered original scholarship and distinct contributions to knowledge.

Chapter 2 is a reformatted and slightly modified version of the article [11] first published in *Mathematische Zeitschrift*. In particular, all results presented in this chapter are joint work with Henri Darmon, Massimo Bertolini and Kartik Prasanna. The reformatting and modifications compared to [11] are due to the author of this thesis, and any errors introduced through this process are solely his responsibility. By clause 4.*c*. of the Copyright Transfer Statement for the article [11] to Springer-Verlag GmbH Germany, part of Springer Nature, the author of the present thesis, David Ter-Borch Gram Lilienfeldt, retains the right to reproduce the article [11] in whole or in part in any printed volume (book or thesis) written by him. Moreover, he has obtained written consent from his co-authors Henri Darmon, Massimo Bertolini and Kartik Prasanna to include their joint work [11] in this thesis.

Chapter 3 is a reformatted and slightly modified version of the preprint article [41] available on the author's website. In particular, all results presented in this chapter are joint work with Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao. The reformatting and modifications compared to [41] are due to the author of this thesis, and any errors introduced through this process are solely his responsibility. The author, David Ter-Borch Gram Lilienfeldt, has obtained written consent from his co-authors Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao to include their joint work [41] in this thesis.

Chapter 4 is written by the author based on his work alone. The author acknowledges that the ideas behind this project stem from discussions with his supervisor Henri Darmon.

Chapter 5 is written by the author, and represents his ideas alone, unless otherwise stated.

Introduction

The unifying theme of the present thesis is the study of rational points on curves, using methods and tools from algebraic geometry. The types of questions that arise depend on the nature of the curves of interest: we will distinguish between two classes of curves, namely elliptic curves and higher genus curves.

In the case of elliptic curves, the main motivation stems from the conjecture of Birch and Swinnerton-Dyer and the inherent difficulty of constructing interesting rational points on such curves. In particular, we will focus on the construction and properties of so-called Chow–Heegner points, which arise as images of algebraic cycles under certain generalised modular parametrisations. This construction generalises the one of the more classic Heegner points, which account for the most significant progress towards the Birch and Swinnerton-Dyer conjecture to date. Two different settings, along with their associated Chow–Heegner points, will be considered in this thesis, namely the one of generalised Heegner cycles and the one of diagonal type cycles on triple products of modular curves.

In the case of higher genus curves, it is known since Faltings' proof of Mordell's conjecture that the set of rational points is finite. However, the available proofs of this result are not effective, which prompts the question of the explicit determination of rational points on such curves. To this end, many methods have been developed recently, originating in the Chabauty–Coleman method. This method allows for the explicit determination of the set of rational points of higher genus curves satisfying an additional so-called Chabauty condition. The Chabauty–Kim method is a far-reaching non-abelian generalisation of the ideas of Chabauty, which aims to relax the original Chabauty condition, and thus to allow for the determination of rational points on more general curves. The first non-abelian instance of this program is known as the quadratic Chabauty method. Recently, Edixhoven and Lido have found an approach to quadratic Chabauty which replaces Kim's language of non-abelian p-adic Hodge theory with the more geometric one of Jacobians and line bundles on curves. Part of this thesis is concerned with the generalisation of the work of Edixhoven and Lido to the case of arbitrary number fields.

0.1 Diophantine geometry

The study of Diophantine equations, named after the 3rd century greek mathematician Diophantus of Alexandria, consists in finding integer or rational solutions to systems of polynomials in several variables with rational coefficients. Individual Diophantine problems are akin to puzzles and have been the objects of mathematical interest throughout history. For instance, consider the Diophantine problem which asks for all the integer solutions to the three variable equation

$$x^2 + y^2 = z^2.$$

Equivalently, this problem is asking for the points with rational coordinates on the unit circle. There are infinitely many solutions, the so-called Pythagorean triples, which, as their name indicates, were considered by Pythagoras and his school.

Perhaps one of the most famous Diophantine problems is a variant of the above, originally formulated by Pierre de Fermat and known as Fermat's Last Theorem. In 1637 he claimed, in the form of a scribbled note in the margin of his copy of the *Arithmetica*, that the equation

$$x^n + y^n = z^n, \qquad \text{with } n \geq 3,$$

has no integer solutions satisfying $xyz \neq 0$. This was proved, possibly even more famously, in 1995 by Sir Andrew Wiles. His proof is truly a 20th century proof, putting to use deep tools from modern algebraic geometry, which were unavailable at the time of Fermat.

Modern day research in Diophantine problems has departed from individual equations and seeks the formulation of more general theories of Diophantine equations. The systems of equations of a Diophantine problem define algebraic varieties, and from this perspective the problem becomes the one of finding rational or integral points on these varieties. It is then natural to attempt to solve such problems by importing tools and techniques from the world of algebraic geometry; this train of thought leads to a field of study known today as Diophantine geometry.

The modern development of Diophantine geometry can provide answers to a variety of geometric questions, ranging from Greek geometry to modern algebraic geometry. Vice-versa, insights into the field of algebraic geometry can lead to solutions to previously unsolved Diophantine problems, as in the case of Wiles' proof of Fermat's Last Theorem.

As an example of a piece of Greek mathematics that was only fully answered by modern techniques, consider Problem 17 of Book VI of Diophantus' *Arithmetica*:

> *Find three squares which when added give a square, and such that the first one is the square-root of the second, and the second is the square-root of the third.*

Solutions here are implicitly assumed to be positive rational numbers. In modern language, the problem is therefore to find positive rational solutions to the equation

$$y^2 = x^8 + x^6 + x^2. \tag{1}$$

Diophantus himself found that $(x, y) = (1/2, 9/16)$ is a solution, and from his perspective that solved the problem (as was the custom at his time). This is unsatisfactory from a modern point of view, in that we wish to know all the solutions. The answer to this came in the form of Wetherell's thesis [152] in 1997: using a modern technique, known as the Chabauty–Coleman method, he established that the only positive rational solution to (1) is the one discovered by Diophantus himself.

Another source of motivation for studying Diophantine geometry comes from the theory of moduli spaces – algebraic varieties whose algebraic points represent certain geometric objects. Via moduli spaces, questions that seemingly have nothing to do with finding solutions to polynomial equations can be interpreted as Diophantine problems, and can thus be solved using methods from Diophantine geometry. As an example, consider the following question raised by Serre [132], known today as Serre's Uniformity Question:

Question 0.1. *Does there exist a constant N such that, for any prime $\ell \geq N$ and any non-CM elliptic curve E over $\mathbb{Q}$, the Galois representation $\bar{\rho}_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\ell](\bar{\mathbb{Q}})) \simeq \mathbf{GL}_2(\mathbb{F}_\ell)$ of E at ℓ is surjective ?*

This question is still open in general but has seen significant recent progress – it is expected to be true for $N = 37$. One can turn the question around and try to establish which elliptic curves have the property that the image of $\bar{\rho}_{E,\ell}$ is contained in a maximal subgroup of $\mathbf{GL}_2(\mathbb{F}_\ell)$. These maximal subgroups are categorised as Borel subgroups, exceptional subgroups, normalisers of split Cartan subgroups and normalisers of non-split Cartan subgroups. Serre [133] classified elliptic curves with residual Galois image in exceptional subgroups. The set of elliptic curves whose residual Galois image modulo ℓ is contained in a Borel subgroup (resp. normaliser of split/non-split Cartan subgroup) defines a moduli problem which is representable by the modular curve $X_0(\ell)$ over $\mathbb{Q}$ of level $\Gamma_0(\ell)$ (resp. the split/non-split Cartan modular curves $X_s(\ell)$ and $X_{ns}(\ell)$ of level ℓ). Serre's Uniformity Question can now be restated in terms of finding $\mathbb{Q}$-rational points on these modular curves. Mazur [113] classified the rational points on $X_0(\ell)$, thereby disposing of the Borel case. Bilu, Parent and Rebolledo [21, 22] classified the rational points of $X_s(\ell)$ for $\ell \geq 11$ different from 13. This classification was completed recently, in a striking application of the quadratic Chabauty method, when Balakrishnan, Dogra, Müller, Tuitman and Vonk [8] determined the rational points of $X_s(13)$ in the elusive case $\ell = 13$. The case of non-split Cartan subgroups remains open today. However, Dogra and Le Fourn [61] have recently developed a "quadratic Chabauty for quotients" method for modular curves, which notably enables them to effectively bound the size of the set of rational points $X_{ns}(\ell)(\mathbb{Q})$.

0.1.1 Rational points on curves

Let K denote a number field and let C be a "nice" curve (smooth, projective, geometrically irreducible) defined over K. The main object of interest in this thesis is the set of rational points $C(K)$. Among the natural questions one might ask are the following:

1. Is $C(K)$ empty ?
2. If not, then what is the cardinality of $C(K)$?
3. If finite, can we find all the rational points explicitly ?
4. If infinite, can we generate all solutions using only finitely many of them ?

Let us suppose from the onset that $C(K) \neq \emptyset$, which effectively rules out the first question. Associated to the curve C is a numerical invariant g called its genus. It is defined as the dimension of the space of regular differential 1-forms on C, namely $g := \dim_K H^0(C, \Omega^1_C)$. The size of the set $C(K)$, i.e., the answer to the second question above, is dictated by the genus of the curve:

- When $g = 0$, the curve C is either a conic or the projective line. In any case, the set $C(K)$ is infinite and well understood, as established by Hilbert and Hurwitz [84]. Moreover, one obtains all solutions using a single rational point via a geometric recipe, in answer to question 4 above.

- When $g = 1$, the curve C is an elliptic curve and the Mordell–Weil theorem [118, 151] asserts that $C(K)$ has the structure of a finitely generated abelian group. As a consequence, $C(K)$ can be either finite or infinite, depending on whether its algebraic rank is zero or positive.

- When $g \geq 2$, it was conjectured by Mordell [118] and proved by Faltings [68] in 1983, that $C(K)$ is finite. Subsequent proofs include the one by Vojta [148] and the recent proof by Lawrence and Venkatesh [106].

We summarise this discussion about the cardinality of $C(K)$ in the following table:

g	$\#C(K)$
0	infinite
1	finite or infinite
≥ 2	finite

As is clear, the situation of genus zero curves is fully understood, and the focus from now on will be on the remaining two cases, namely elliptic curves and higher genus curves.

0.1.2 Questions in genus one

Let E denote a smooth projective genus one curve defined over some number field K and assume that $E(K) \neq \emptyset$. After fixing a rational point $O_E \in E(K)$, the pair (E, O_E) is an elliptic curve. In the special case of elliptic curves, the set $E(K)$ can be endowed with the structure of an abelian group with identity element O_E, and $E(K)$ is in fact finitely generated by the Mordell–Weil theorem. In particular, we have an identification

$$E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^{r_{\text{alg}}(E/K)},$$

where $E(K)_{\text{tors}}$ is the finite subgroup of torsion points, and $r_{\text{alg}}(E/K)$ is called the Mordell–Weil rank of E. When $K = \mathbb{Q}$, Mazur [112] established which abstract finite groups could occur as $E(\mathbb{Q})_{\text{tors}}$. The case of general number fields was settled by Merel [115].

Central to the theory of elliptic curves remains the unsolved problem of determining the algebraic rank $r_{\text{alg}}(E/K)$. This quantity appears to be quite intractable as, for instance, it is still unknown if there exist elliptic curves with arbitrarily large rank.

During the 1960's, Birch and Swinnerton-Dyer [23, 24] observed, after conducting extensive computations, the following experimental relation for an elliptic curve $E/\mathbb{Q}$:

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \overset{?}{\sim} C_E \log(X)^{r_{\mathrm{alg}}(E/\mathbb{Q})}, \qquad \text{as } X \to +\infty,$$

where the product ranges over (all but finitely many) prime numbers, and C_E is some constant depending on E. Associated to E is a complex function $L(E/\mathbb{Q}, s)$ called the Hasse–Weil L-function of E. It is given, except for finitely many primes p, by the product

$$\prod_p (1 - (p + 1 - \#E(\mathbb{F}_p))p^{-s} + p^{1-2s})^{-1}$$

which converges to a holomorphic function for all $\Re(s) > 3/2$. Thus, formally we have $L(E/\mathbb{Q}, 1) = \prod_p \left(\frac{\#E(\mathbb{F}_p)}{p}\right)^{-1}$, although the convergence of this product was unknown at the time. Hasse conjectured that $L(E/\mathbb{Q}, s)$ admits analytic continuation to the whole complex plane via a functional equation centred at $s = 1$. Motivated by their observations and this conjecture, Birch and Swinnerton-Dyer were led to define the analytic rank of E as $r_{\mathrm{an}}(E/\mathbb{Q}) := \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$, and to conjecture the equality $r_{\mathrm{an}}(E/\mathbb{Q}) = r_{\mathrm{alg}}(E/\mathbb{Q})$.

One can formulate a similar conjecture for elliptic curves over a general number field K. The Hasse–Weil L-function $L(E/K, s)$ can be defined by a similar convergent product formula as above and one conjectures that it admits analytic continuation to the complex plane along with a functional equation centred at $s = 1$, hence (conjecturally) the analytic rank $r_{\mathrm{an}}(E/K) := \mathrm{ord}_{s=1} L(E/K, s)$ is well-defined. The famous Birch and Swinnerton-Dyer conjecture, now one of the seven Clay Millennium Prize Problems, predicts the following:

Conjecture 0.1 (weak BSD)**.**

$$r_{\mathrm{an}}(E/K) = r_{\mathrm{alg}}(E/K).$$

When $K = \mathbb{Q}$, the good analytic properties of $L(E/\mathbb{Q}, s)$, originally conjectured by

Hasse, are known today as a consequence of the Modularity Theorem of Wiles [153], Taylor and Wiles [145], and Breuil, Conrad, Diamond and Taylor [31]. Note that the Modularity Theorem for semistable elliptic curves was the key ingredient in Wiles' proof of Fermat's Last Theorem. As a consequence of these analytic properties, it makes sense to consider the equality of ranks predicted by the BSD conjecture. The most significant progress to date towards the Birch and Swinnerton-Dyer conjecture is due to the method of Gross and Zagier [78], and Kolyvagin [75, 103], which rests on the construction of Heegner points, and yields the implication

$$r_{\mathrm{an}}(E/\mathbb{Q}) \in \{0,1\} \implies r_{\mathrm{alg}}(E/\mathbb{Q}) = r_{\mathrm{an}}(E/\mathbb{Q}). \tag{2}$$

Their strategy has been generalised to the case of totally real number fields by S. Zhang [156]. The work of Skinner and Urban [141], and Skinner [140], uses p-adic methods, and more specifically Iwasawa theory, to produce the first instances of the opposite implication of (2)

$$r_{\mathrm{alg}}(E/\mathbb{Q}) \in \{0,1\} \implies r_{\mathrm{alg}}(E/\mathbb{Q}) = r_{\mathrm{an}}(E/\mathbb{Q}), \tag{3}$$

under certain technical assumptions.

The Birch and Swinnerton-Dyer conjecture remains open in higher rank situations, as well as for elliptic curves over general number fields in any rank. The key obstacle to further progress is the construction of non-torsion rational points on elliptic curves that go beyond the setting of Heegner points. We will elaborate more on this point in Section 0.2.

0.1.3 Questions in higher genus

Let us go back to the original notation of this introduction and let C denote a smooth, projective, geometrically irreducible curve of genus $g \geq 2$ defined over a number field K. Recall that Faltings' theorem [68] implies that $C(K)$ is a finite set. However, none of the currently available proofs of this theorem are effective: they do not give a way, for a given curve, to determine the set $C(K)$ explicitly. The effective determination of the set of rational points of higher genus curves is one of the key problems of modern Diophantine geometry. Several recent methods attempt to address this question.

The first partial result towards Mordell's conjecture [118] came in the form of the pioneering work of Chabauty [35] in 1941. He managed to prove finiteness of the set of rational points under an additional constraint, known as the Chabauty condition – namely, the rank r of the Mordell–Weil group of the Jacobian J of C is less than the genus g. In 1985, Coleman [36] succeeded in making Chabauty's method effective, resulting in explicit upper bounds for the number of rational points on curves satisfying the Chabauty condition. Using this bound and further refinements of the method, it is possible in many cases to determine $C(K)$ completely. The resulting method is known as the Chabauty–Coleman method. This is the method used by Wetherell [152] in order to complete the solution of Problem 17 of Book VI in Diophantus' *Arithmetica*. More precisely, by removing the singularity of equation (1) at $(0,0)$, Wetherell reduced the question to finding all the rational points on the genus 2 bielliptic curve given by the affine model

$$Y : y^2 = x^6 + x^2 + 1. \tag{4}$$

The Jacobian of this curve has rank 2, so we are in the case $r = g = 2$, and a priori the Chabauty–Coleman method does not apply. However, the main innovation of Wetherell was to consider a collection of covering curves of Y and apply Chabauty–Coleman succesfully to these.

In the mid 2000's, Kim [101, 102] initiated a fascinating non-abelian Chabauty program, known as the Chabauty–Kim method, which aims to relax the restrictive Chabauty condition $r < g$. The first non-abelian instance of the program is called the quadratic Chabauty method. It has recently been made effective over $\mathbb{Q}$ in [8]; the method is successfully applied to determine all rational points on the "cursed" split Cartan modular curve $X_s(13)$ of level

13 (which satisfies $r = g = 3$, so not in range for Chabauty–Coleman), thereby settling the classification of non-CM elliptic curves over $\mathbb{Q}$ of split Cartan type, which relates to Serre's Uniformity Question 0.1. Let us mention here that Bianchi [20] has recently revisited Problem 17 of Book VI in Diophantus' *Arithmetica*, obtaining a new proof of Wetherell's theorem using the quadratic Chabauty method.

Recently, Edixhoven and Lido [62] have found a different approach to quadratic Chabauty over $\mathbb{Q}$, which replaces Kim's language of non-abelian p-adic Hodge theory with the more geometric language of Jacobians and line bundles on curves. This method is therefore referred to as the geometric quadratic Chabauty method. It is expected to work under the so-called quadratic Chabauty condition $r < g + \rho - 1$, where ρ is the rank of the Néron–Severi group of J. As we will see, it lies close in spirit to the original method of Chabauty.

0.2 Algebraic cycles and the arithmetic of elliptic curves

We review the construction of Heegner points and their role in the Gross–Zagier–Kolyvagin strategy towards the Birch and Swinnerton-Dyer conjecture. This motivates a generalisation of such points, known as Chow–Heegner points.

0.2.1 The three pillars of the BSD strategy over $\mathbb{Q}$

The strategy of Gross, Zagier and Kolyvagin towards the BSD conjecture over $\mathbb{Q}$ relies, in an essential way, on the construction of certain rational points on elliptic curves – the so-called Heegner points. These arise, via a modular parametrisation, from special points on certain modular curves, and are linked to the behaviour of the Hasse–Weil L-function via the famous Gross–Zagier formula.

Modular parametrisations

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N – a positive integer which contains the information about the places of bad reduction of E. The Modularity Theorem [31, 145, 153] associates to E a weight 2 normalised Hecke newform $f \in S_2(\Gamma_0(N))^{\mathrm{new}}$ of level $\Gamma_0(N)$ such that we have an equality of L-functions

$$L(E/\mathbb{Q}, s) = L(f, s) := \sum_{n \geq 1} \frac{a_n(f)}{n^s},$$

where f is given by the Fourier expansion $f(z) = \sum_{n \geq 1} a_n(f) e^{2\pi i z}$ around the cusp at infinity. It follows that the Hasse–Weil L-function of E inherits the good analytic properties of the L-function of f; namely, $L(E/\mathbb{Q}, s)$ admits analytic continuation to the whole complex plane via a functional equation centred at $s = 1$. In other words, Hasse's conjecture is true. Note that these properties were not known before the proof of modularity for all rational elliptic curves over $\mathbb{Q}$, and modularity type statements are the only way to access such analytic properties of L-functions of algebraic varieties.

The Eichler–Shimura construction [64, 135] associates to f an elliptic curve E_f over $\mathbb{Q}$, which is a quotient of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ over $\mathbb{Q}$ (which coarsely represents pairs of elliptic curves related by a cyclic N-isogeny), in a way such that

$$L(f, s) = L(E_f/\mathbb{Q}, s).$$

In particular, we have the equality

$$L(E/\mathbb{Q}, s) = L(E_f/\mathbb{Q}, s),$$

and it follows from Faltings' proof [68] of the Tate conjecture for abelian varieties over number fields, that the elliptic curves E and E_f are isogenous. As a consequence, there is a non-constant morphism of algebraic varieties over $\mathbb{Q}$

$$\pi_E : J_0(N) \longrightarrow E. \tag{5}$$

Such a morphism is called a modular parametrisation of E. Note that the statement that all elliptic curves over $\mathbb{Q}$ admit a modular parametrisation is equivalent to the Modularity Theorem.

Heegner points

The key observation is that the modular curve $X_0(N)$ comes equipped, via the theory of complex multiplication, with a special supply of rational points.

The set of complex points $X_0(N)(\mathbb{C})$ is a Riemann surface, and admits a uniformisation by the extended Poincaré upper half-plane given by

$$\mathcal{H}^* \longrightarrow X_0(N)(\mathbb{C}), \qquad \tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, \langle 1/N + \mathbb{Z} \oplus \tau\mathbb{Z} \rangle)$$

which identifies $X_0(N)(\mathbb{C})$ with the quotient $\Gamma_0(N) \setminus \mathcal{H}^*$ where $\Gamma_0(N) \subset \mathbf{SL}_2(\mathbb{Z})$ is the standard congruence subgroup. Let K be an imaginary quadratic field embedded in $\mathbb{C}$, of discriminant $-d_K$, and let $\mathcal{O}_K$ denote its ring of integers. Let $\mathcal{O}_c$ denote the unique order of K of conductor c. One may consider on $X_0(N)(\mathbb{C})$ the following set of complex multiplication (CM) points

$$\mathrm{CM}_{\mathbb{C}}(\mathcal{O}_c) = \{[\tau] \in \Gamma_0(N) \setminus \mathcal{H} \mid a\tau^2 + b\tau + d = 0, \gcd(a, b, d) = 1, b^2 - 4ad = -c^2 d_K\}.$$

These points are so named because they correspond, via the moduli description, to elliptic curves $E/\mathbb{C}$ with complex multiplication by $\mathcal{O}_c$ (i.e., $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}_c$) together with a $\Gamma_0(N)$-level structure. There is a subset $\mathrm{CM}_{\mathbb{C}}(\mathcal{O}_c)_{\mathrm{heeg}} \subset \mathrm{CM}_{\mathbb{C}}(\mathcal{O}_c)$ consisting of special points that correspond via moduli to cyclic N-isogenies of elliptic curves $E \longrightarrow E'$ where E and E' both admit complex multiplication by the same order $\mathcal{O}_c$.

Given $x \in \mathrm{CM}_{\mathbb{C}}(\mathcal{O}_c)_{\mathrm{heeg}}$, we define the corresponding Heegner point by applying the modular parametrisation π_E to the class of the degree zero divisor $(x) - (\infty)$, where ∞ denotes the cusp at infinity of $X_0(N)$:

$$P_{c,x} := \pi_E([x] - [\infty]) \in E(\mathbb{C}).$$

By the theory of complex multiplication, this point is defined over an abelian extension of K, and more precisely, over the ring class field H_c of K of conductor c. It can be shown that the collection of all Heegner points, with imaginary quadratic field K and conductor c varying, generates a subgroup of $E(\bar{\mathbb{Q}})$ of infinite rank.

The Gross–Zagier formula

In 1986, Gross and Zagier proved a now famous formula relating the behaviour of Heegner points to the derivative of a Hasse–Weil L-function. Let us assume that the conductor N of the elliptic curve is square-free and fix an imaginary quadratic field K. We need to assume the so-called Heegner hypothesis:

Assumption 0.1. *All primes dividing N are split in K.*

As a consequence of this assumption, the sign of the functional equation of the Hasse–Weil L-function $L(E/K, s)$ of E base-changed to K is -1, hence the analytic rank $r_{\mathrm{an}}(E/K)$ is odd, and in particular greater or equal to 1. Let $P_{1,x} \in E(H)$ be a Heegner point associated with the maximal order of K, and thus defined over the Hilbert class field H of K, and consider its trace

$$P_K := \mathrm{Tr}_{H/K}(P_{1,x}) \in E(K).$$

The Gross–Zagier formula [78] gives an equality (up to multiplication by some explicit non-zero complex number)

$$L'(E/K, 1) \doteq h(P_K),$$

where h denotes the canonical Néron–Tate height on E.

By the properties of the canonical height, we get, as an immediate consequence, that the Heegner point P_K has infinite order in $E(K)$ if and only if $L'(E/K,1) \neq 0$, and we have the implication

$$r_{\mathrm{an}}(E/K) = 1 \implies r_{\mathrm{alg}}(E/K) \geq 1.$$

By combining this result with techniques exploiting the full Euler system of Heegner points, Kolyvagin [75, 103] was able to deduce the following implication:

$$r_{\mathrm{an}}(E/\mathbb{Q}) \in \{0,1\} \implies r_{\mathrm{an}}(E/\mathbb{Q}) = r_{\mathrm{alg}}(E/\mathbb{Q}) \qquad \& \qquad |Ш(E/\mathbb{Q})| < \infty. \tag{6}$$

This remains to date the strongest implication towards the BSD conjecture.

Further progress and obstacles

The above described Gross–Zagier–Kolyvagin strategy towards the BSD conjecture has been generalised by S. Zhang [156] to the case of elliptic curves defined over totally real number fields; given a modular elliptic curve E/F, where F is a totally real field such that either $[F:\mathbb{Q}]$ is odd or E/F has at least one prime of multiplicative reduction, we have

$$r_{\mathrm{an}}(E/F) \in \{0,1\} \implies r_{\mathrm{an}}(E/F) = r_{\mathrm{alg}}(E/F).$$

The work of Skinner and Urban [140, 141] uses p-adic methods, and more specifically Iwasawa theory, to produce the first instances of the opposite implication (3).

The three key ingredients of the Gross–Zagier–Kolyvagin approach to the BSD conjecture over $\mathbb{Q}$ that we have seen are:

1. A *modular parametrisation* $\pi_E : J_X \longrightarrow E$, where J_X is the Jacobian of a modular curve X (or more generally a Shimura curve).

2. A *special supply of rational points* on X – the so-called CM points – which gives rise

to Heegner points on E via the modular parametrisation.

3. The *Gross–Zagier formula* relating the height of Heegner points to the central derivative of certain base-changes of the Hasse–Weil L-function of E.

Suppose that we wish to understand the higher rank situation when $r_{\mathrm{an}}(E/\mathbb{Q}) > 1$. Suppose that K is an imaginary quadratic field satisfying the Heegner hypothesis (Assumption 0.1), so that $r_{\mathrm{an}}(E/K)$ is odd. It is clear that we also have $r_{\mathrm{an}}(E/K) > 1$, thus the Gross–Zagier formula implies that the Heegner point $P_K \in E(K)$ is torsion. Even though we expect, by the BSD conjecture, to have $r_{\mathrm{alg}}(E/K) \geq 3$, we can currently not produce a point of infinite order. This highlights the limitations of Heegner points: they can only know about rank 1 situations. In the higher rank case, we need a construction of interesting rational points that goes beyond the setting of Heegner points.

Given an elliptic curve E over $\mathbb{Q}$, even of small rank, we may wonder whether we can say anything about the BSD conjecture for the base-change of E to some number field F. But again we are limited: the Heegner point construction only yields rational points defined over abelian extensions of imaginary quadratic fields which are generalised dihedral over $\mathbb{Q}$. Therefore, the Heegner point construction is insufficient to deal with the BSD conjecture over arbitrary number fields.

Given the shortcomings of the Heegner point construction, a central obstacle to further progress on the BSD conjecture is the construction of rational points on elliptic curves which may account for higher rank situations, and which can be defined over arbitrary number fields.

0.2.2 The construction of Chow–Heegner points

A generalisation of the Heegner point construction exists. The idea is to consider points on elliptic curves arising as images of algebraic cycles under certain generalised modular parametrisation maps. The name of Chow–Heegner points was coined by Bertolini, Darmon and Prasanna when they first envisioned such constructions in [13].

Algebraic cycles

Let X denote a smooth projective variety of dimension d defined over some number field K. An algebraic cycle on X is a formal $\mathbb{Z}$-linear combination of subvarieties of $X_{\bar{K}}$. Hence, an algebraic cycle can be written as a finite sum $Z = \sum_{i=1}^{t} n_i \cdot V_i$, where the coefficients n_i are integers, and the V_i are subvarieties. These form a group under addition, and if all the V_i's have codimension j, then the algebraic cycle Z is said to be of codimension j.

The Chow group of X is obtained by considering the group of algebraic cycles modulo rational equivalence (i.e., by taking the quotient of the subgroup generated by cycles arising as divisors of functions on subvarieties). The Chow group has the structure of a ring under the intersection product, and the additive subgroup generated by cycles of codimension j is denoted $\mathrm{CH}^j(X)$. There is also a notion of an algebraic cycle being null-homologous (i.e., having image in cohomology equal to zero), and the subgroup generated by such cycles will be denoted by $\mathrm{CH}^j(X)_0$.

As an example, let us consider the case when $d = 1$, i.e., the variety X is a curve. In this case, algebraic cycles of codimension 1 are given by formal sums of points in $X(\bar{K})$, so the group of codimension 1 cycles is the familiar divisor group $\mathrm{Div}(X)$. Rational equivalence in this case is the perhaps more familiar relation of linear equivalence on divisors, hence $\mathrm{CH}^1(X) = \mathrm{Pic}(X)$ is the Picard group of X. Finally, null-homologous divisors correspond to degree zero divisors, so that the null-homologous Chow group is $\mathrm{CH}^1(X)_0 = \mathrm{Pic}^0(X) = J_X$, i.e., the Jacobian of X.

The three pillars of BSD revisited

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. The language of algebraic cycles allows us to recast the modular parametrisation (5) as a natural transformation

$$\pi_E : \mathrm{CH}^1(X_0(N))_0 \longrightarrow E.$$

As explained in [13], it is tempting to define generalisations of modular parametrisations by replacing the domain $\mathrm{CH}^1(X_0(N))_0$ with $\mathrm{CH}^j(X)_0$ for some algebraic variety of higher dimension, as natural transformations

$$\Pi_E : \mathrm{CH}^j(X)_0 \longrightarrow E.$$

Such a generalised modular parametrisation then gives rise to rational points on E – namely, Chow–Heegner points – by evaluating at suitable rational null-homologous algebraic cycles of codimension j. Note that the use of the word "parametrisation" is a slight abuse of language, since the natural transformations Π_E are in general not surjective.

From this perspective, one can devise a new strategy towards the BSD conjecture based on three ingredients, generalising the Gross–Zagier–Kolyvagin picture:

1. A *generalised modular parametrisation* $\Pi_E : \mathrm{CH}^j(X)_0 \longrightarrow E$, where X is an algebraic variety.

2. A *special supply of algebraic cycles* on X (null-homologous of codimension j) which gives rise to Chow–Heegner points on E via Π_E.

3. A *Gross–Zagier type formula* relating the height of Chow–Heegner points to the central derivative of certain base-changes of the Hasse–Weil L-function of E.

Chow–Heegner points

Let E denote an elliptic curve defined over a number field K, and let X denote a smooth projective variety over K of dimension d. Any element Π of $\mathrm{CH}^{d-j+1}(X \times E)(K)$ gives rise, via push-forward of correspondences, to a natural transformation

$$\Pi_* : \mathrm{CH}^j(X)_0 \longrightarrow \mathrm{CH}^1(E)_0, \qquad \Delta \mapsto \mathrm{pr}_{E,*}(\Pi \cdot \mathrm{pr}_X^*(\Delta)),$$

where $\mathrm{pr}_E : X \times E \longrightarrow E$ and $\mathrm{pr}_X : X \times E \longrightarrow X$ denote the natural projections, and the product is the intersection product in Chow groups. Note that $\mathrm{CH}^1(E)_0 = J_E$ is the Jacobian of E, which in the case of elliptic curves is simply E. Hence the push-forward of Π gives rise to a generalised modular parametrisation

$$\Pi_E := \Pi_* : \mathrm{CH}^j(X)_0 \longrightarrow E.$$

For any field extension F of K, it induces homomorphisms

$$\Pi_E : \mathrm{CH}^j(X)_0(F) \longrightarrow E(F),$$

hence it can be used to produce rational points on E.

Definition 0.1. Given an algebraic cycle $\Delta \in \mathrm{CH}^j(X)_0(F)$ defined over some extension F of K, we define the associated Chow–Heegner point by

$$P(X, \Pi, \Delta) := \Pi_E(\Delta) = \Pi_*(\Delta) \in E(F).$$

As an example, let us consider the case where $K = \mathbb{Q}$ and $X = X_0(N)$ is the modular curve over $\mathbb{Q}$ of level $\Gamma_0(N)$ with N the conductor of E. Consider the graph of the modular parametrisation $\Pi := \Gamma_{\pi_E} \in \mathrm{CH}^1(X_0(N) \times E)(\mathbb{Q})$ arising from the Modularity Theorem. If

$x \in \mathrm{CM}_{\mathbb{C}}(\mathcal{O}_K)_{\mathrm{heeg}}$ is a special CM point of $X_0(N)$, then the Chow–Heegner point

$$P(X_0(N), \Gamma_{\pi_E}, [x] - [\infty]) = \pi_E([x] - [\infty]) = P_{1,x} \in E(H)$$

is the corresponding Heegner point of conductor 1. In particular, the Chow–Heegner construction can be seen as a vast generalisation of the original construction of Heegner points. Because it involves modular parametrisations whose domains are Chow groups, the name of Chow–Heegner point was suitably chosen.

0.2.3 Complex Abel–Jacobi maps

Recall the Abel–Jacobi map of the elliptic curve E,

$$\mathrm{AJ}_E : E(\mathbb{C}) \xrightarrow{\sim} J^1(E)(\mathbb{C}) := \frac{H^0(E(\mathbb{C}), \Omega^1_E)^\vee}{\operatorname{Im} H_1(E(\mathbb{C}), \mathbb{Z})}.$$

Here $J^1(E/\mathbb{C})$ denotes the complex points of the Jacobian of E, viewed as a complex torus by taking the quotient of the dual of the 1-dimensional $\mathbb{C}$-vector space of global regular differentials by the lattice coming from the singular homology of the Riemann surface $E(\mathbb{C})$ (viewed inside $H^0(E(\mathbb{C}), \Omega^1_E)^\vee$ by integration of differential forms on topological 1-chains). The map is defined, using as base point the origin $O_E \in E(\mathbb{C})$, by the integration formula

$$\mathrm{AJ}_E(P)(\omega) = \int_{O_E}^{P} \omega, \qquad \text{for all } \omega \in H^0(E(\mathbb{C}), \Omega^1),$$

and it is an isomorphism by a classic result of Abel.

It admits a higher dimensional analogue for the variety X in form of a homomorphism

$$\mathrm{AJ}_X : \mathrm{CH}^j(X)_0(\mathbb{C}) \longrightarrow J^j(X/\mathbb{C}) := \frac{\mathrm{Fil}^{d-j+1} H^{2d-2j+1}_{\mathrm{dR}}(X/\mathbb{C})^\vee}{\operatorname{Im} H_{2d-2j+1}(X(\mathbb{C}), \mathbb{Z})}, \tag{7}$$

where $J^j(X/\mathbb{C})$ is the j-th intermediate Jacobian of X first studied by Griffiths and Weil. It is a complex torus realised by taking the dual of the $(d-j+1)$-th step in the Hodge filtration of the de Rham cohomology of $X/\mathbb{C}$ in degree $2d-2j+1$ modulo the lattice coming from the singular homology of the complex manifold $X(\mathbb{C})$ (viewed inside $\mathrm{Fil}^{d-j+1} H_{\mathrm{dR}}^{2d-2j+1}(X/\mathbb{C})^\vee$ by integration of differential forms on topological $(2d-2j+1)$-chains). This map is similarly defined by an integration formula

$$\mathrm{AJ}_X(Z)(\alpha) = \int_{\partial^{-1}(Z)} \alpha, \qquad \text{for all } \alpha \in \mathrm{Fil}^{d-j+1} H_{\mathrm{dR}}^{2d-2j+1}(X/\mathbb{C}),$$

where $\partial^{-1}(Z)$ denotes any topological $(2d-2j+1)$-chain whose boundary is the homology class of Z. Note that AJ_X is no longer an isomorphism in general, and $J^j(X)$ does not carry an algebraic structure.

Functoriality properties of these complex Abel–Jacobi maps with respect to correspondences [65] yield a commutative diagram

$$\begin{array}{ccc} \mathrm{CH}^j(X)_0(\mathbb{C}) & \xrightarrow{\mathrm{AJ}_X} & J^j(X/\mathbb{C}) \\ \downarrow{\scriptstyle \Pi_*} & & \downarrow{\scriptstyle (\Pi_{\mathrm{dR}}^*)^\vee} \\ E(\mathbb{C}) & \xrightarrow[\mathrm{AJ}_E]{\sim} & J^1(E/\mathbb{C}), \end{array}$$

where Π_{dR}^* denotes the pull-back of the correspondence Π on de Rham cohomology groups. Since AJ_E is an isomorphism, studying the Chow–Heegner point $P(X,\Pi,\Delta)$ in $E(\mathbb{C})$ amounts to studying its image via AJ_E. We have the following formula, for all $\omega \in H^0(E(\mathbb{C}),\Omega^1)$,

$$\mathrm{AJ}_E(P(X,\Pi,\Delta))(\omega) = \mathrm{AJ}_E(\Pi_*(\Delta))(\omega) = \mathrm{AJ}_X(\Delta)(\Pi_{\mathrm{dR}}^*(\omega)).$$

In conclusion, the computation of the image of algebraic cycles under complex Abel–Jacobi maps can be used as a tool in the study of the associated Chow–Heegner points.

0.3 Rational points on higher genus curves

Let C be a smooth, projective, geometrically irreducible curve of genus $g \geq 2$ defined over a number field K. The theorem of Faltings states that the set of rational points on C is finite. Faltings' spectacular proof, however, cannot be made effective and there is no general algorithm for determining the set $C(K)$ at present. (This is not quite true: there is an algorithm by Alpöge and Lawrence that terminates assuming standard conjectures. We refer to Chapters 7-9 of [2]). Let J denote the Jacobian of C, which is an abelian variety over K of dimension g. By the Mordell–Weil theorem for abelian varieties [151], the abelian group of rational points $J(K)$ is finitely generated and thus has a well defined rank $r := \operatorname{rank}_{\mathbb{Z}} J(K)$. In recent years, starting with the groundbreaking work of Chabauty in 1941, methods have been invented which lead, in many cases, to the explicit determination of rational points on curves satisfying certain rank inequality conditions on r, commonly referred to as Chabauty type conditions. In this introduction, we will restrict the attention to the setting where $K = \mathbb{Q}$.

0.3.1 Chabauty–Coleman

If the Mordell–Weil rank r of the Jacobian J of C satisfies the inequality $r := \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) < g$, the pioneering work of Chabauty [35] and Coleman [36] can be used to give upper bounds for the size of $C(\mathbb{Q})$, and in many cases, to explicitly compute the set of rational points.

Upon choosing a prime p of good reduction, one obtains a homomorphism

$$\log_p : J(\mathbb{Q}_p) \longrightarrow H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee \simeq H^0(J_{\mathbb{Q}_p}, \Omega^1)^\vee$$

induced from a linear pairing $J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \longrightarrow \mathbb{Q}_p$ which sends (P, ω) to the Coleman integral $\int_0^P \omega$. We refer to [37] for details about Coleman integration. This map is the p-adic syntomic Abel–Jacobi map

$$\mathrm{AJ}_p : \mathrm{CH}^1(X)_0(\mathbb{C}_p) \longrightarrow \mathrm{Fil}^1 H^1_{\mathrm{dR}}(X/\mathbb{C}_p)^\vee,$$

a p-adic avatar of the complex Abel–Jacobi map introduced earlier.

The Abel–Jacobi embedding $j_b : C \hookrightarrow J$ (relying on a fixed base point $b \in C(\mathbb{Q})$) leads to the following diagram, which is central to the method:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) & \overset{\int}{\searrow} & \\ \downarrow j_b & & \downarrow j_b & & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow[\log_p]{} & H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee. \end{array} \tag{8}$$

The Chabauty condition $r < g$ guarantees that the closure $\overline{J(\mathbb{Q})}^p$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with respect to the p-adic topology has positive codimension. In particular, there exists a nontrivial differential form ω which is annihilated by $\log_p(\overline{J(\mathbb{Q})}^p)$, and thus

$$C(\mathbb{Q}) \subset j_b^{-1}(\overline{J(\mathbb{Q})}^p \cap j_b(C(\mathbb{Q}_p))) \subset \left\{ x \in C(\mathbb{Q}_p) \ : \ \int_b^x \omega = 0 \right\}.$$

The Coleman function $\int_b^x \omega$ of x is given by a converging p-adic power series on each residue disk of the curve C, and in particular has only finitely many zeros. It follows that $C(\mathbb{Q})$ is finite. Coleman [36] was able, using Newton polygons, to count the number of zeros of converging p-adic power series on residue disks, and prove the following bound

$$|C(\mathbb{Q})| \leq |C(\mathbb{F}_p)| + (2g-2)$$

when $r < g$ and $p > 2g$ is a prime of good reduction for C.

The question of the uniformity of the bound on the number of rational points on higher genus curves has been explored in the work of Stoll [143], Katz and Zureick-Brown [97], and Katz, Rabinoff and Zureick-Brown [96]. They notably extend the ideas of Chabauty–

Coleman to the setting of primes of bad reduction.

0.3.2 Quadratic Chabauty

The tantalising non-abelian Chabauty program, initiated by Kim [101,102], aims to relax the Chabauty condition $r < g$ by considering non-abelian variants of the objects in (8). To this end, we first reinterpret the diagram above using the Bloch–Kato Selmer groups $H^1_f(\mathbb{Q}, V)$ (resp. $H^1_f(\mathbb{Q}_p, V)$) in place of $J(\mathbb{Q})$ (resp. $J(\mathbb{Q}_p)$) via the Kummer maps, where $V := V_pJ$ is the p-adic Tate module of J with its canonical Galois action. The logarithm map above is essentially the inverse of the Bloch–Kato exponential

$$H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee \simeq \mathrm{D}_{\mathrm{dR}}(V)/\mathrm{D}^+_{\mathrm{dR}}(V) \xrightarrow{\exp} H^1_f(\mathbb{Q}_p, V).$$

Next, we replace V by certain pro-unipotent quotients U_n of the étale fundamental group $\pi_1^{\text{ét}}(C_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, one for each $n \geq 1$, which again carries a continuous Galois action. Kim defines a certain Selmer subgroup $\mathrm{Sel}(U_n) \subset H^1_f(\mathbb{Q}, U_n)$, and upgrades the previous diagram to

$$\begin{array}{ccccc} C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) & \overset{\int}{\searrow} & \\ \downarrow{\scriptstyle j_n} & & \downarrow{\scriptstyle j_{n,p}} & & \\ \mathrm{Sel}(U_n) & \xrightarrow[\mathrm{loc}_p]{} & H^1_f(\mathbb{Q}_p, U_n) & \xrightarrow[\mathrm{loc}_n]{} & \pi_1^{\mathrm{dR}}(C_{\mathbb{Q}_p})_n/\mathrm{Fil}^0. \end{array}$$

Here the vertical maps j_n and $j_{n,p}$ are Kim's unipotent Kummer maps. Define the sets

$$C(\mathbb{Q}_p)_n := j_{n,p}^{-1}\big(\mathrm{loc}_p(\mathrm{Sel}(U_n))\big),$$

which give rise to an infinite nested sequence of sets

$$C(\mathbb{Q}) \subset \ldots \subset C(\mathbb{Q}_p)_{n+1} \subset C(\mathbb{Q}_p)_n \subset \ldots \subset C(\mathbb{Q}_p)_2 \subset C(\mathbb{Q}_p)_1 \subset C(\mathbb{Q}_p).$$

For sufficiently large n, Kim conjectures that $C(\mathbb{Q}_p)_n$ is finite, and even coincides with $C(\mathbb{Q})$.

Here $C(\mathbb{Q}_p)_1$ is the set studied in the Chabauty–Coleman method. It is the pre-image in $C(\mathbb{Q}_p)$ of the p-saturation of the rational points of J inside the p-adic points. More precisely, it consists of those $x \in C(\mathbb{Q}_p)$ such that $n \cdot j_b(x) \in \overline{J(\mathbb{Q})}^p$ for some rational integer n. In particular, $C(\mathbb{Q}_p)_1$ contains $j_b^{-1}(\overline{J(\mathbb{Q})}^p \cap j_b(C(\mathbb{Q}_p)))$, as well as $j_b^{-1}(J(\mathbb{Q}_p)_{\mathrm{tors}} \cap j_b(C(\mathbb{Q}_p)))$.

The first non-abelian instance of Kim's program is known as the quadratic Chabauty method – it consists of establishing the finiteness of $C(\mathbb{Q}_p)_2$ under some quadratic Chabauty condition on the rank r. This particular method has been developed by Balakrishnan and Dogra in a series of papers [5–7]. In particular, they show that if the Mordell–Weil rank r satisfies $r < g + \rho - 1$ (where ρ is the rank of the Néron–Severi group of J), then $C(\mathbb{Q}_p)_2$ is finite. This method has been made effective by Balakrishnan, Dogra, Müller, Tuitman and Vonk [8], and applied to determine the rational points on the "cursed curve" $X_s(13)$. This work has been extended by the same authors in [9].

Dogra and Le Fourn [61] have recently developed a "quadratic Chabauty for quotients" method that works well for modular curves; the quadratic Chabauty condition is replaced by a condition on the rank of a quotient of the Jacobian plus an associated space of Chow–Heegner points. This enables them to effectively bound the size of the rational points of the modular curves $X_0^+(\ell)$ and $X_{ns}(\ell)$ of prime level. We highlight the fact that their work combines ideas from the two main themes of the present thesis: the quadratic Chabauty method and the theory of Chow–Heegner points.

0.3.3 Geometric quadratic Chabauty

Recently, Edixhoven and Lido [62] have explored a different, less cohomological but arguably more direct approach to quadratic Chabauty. Their method, known as the geometric quadratic Chabauty method, proves finiteness of the set of rational points $C(\mathbb{Q})$ under the same quadratic Chabauty condition $r < g + \rho - 1$ as in the previous section. It has the advantage of avoiding the consideration of iterated Coleman integrals and the analysis of certain complicated p-adic heights. In fact, this method is rather geometric and elementary, and even eliminates the language of non-abelian p-adic Hodge theory used by Kim.

The strategy of Edixhoven and Lido is close in spirit to the original idea of Chabauty from 1941. However, in order to relax the condition $r < g$, they replace the Jacobian J in (8) by something bigger – namely, a certain $\mathbb{G}_m^{\rho-1}$-torsor T over J, which they construct. This torsor comes equipped, by construction, with a lift $\tilde{j}_b : C \longrightarrow T$ of the Abel–Jacobi embedding of C in J. Letting p denote a prime of good reduction for the curve C, one may then consider the diagram

$$\begin{array}{ccccc} C(\mathbb{Q}) & \longrightarrow & & \longrightarrow & C(\mathbb{Q}_p) \\ \downarrow \tilde{j}_b & & & & \downarrow \tilde{j}_b \\ T(\mathbb{Q}) & \longrightarrow & \overline{T(\mathbb{Q})}^p & \longrightarrow & T(\mathbb{Q}_p), \end{array} \tag{9}$$

where $\overline{T(\mathbb{Q})}^p$ denotes the closure of $T(\mathbb{Q})$ in $T(\mathbb{Q}_p)$ with respect to the p-adic topology. The method now consists in bounding the size of the intersection

$$\tilde{j}_b^{-1}(\overline{T(\mathbb{Q})}^p \cap \tilde{j}_b(C(\mathbb{Q}_p))), \tag{10}$$

which contains $C(\mathbb{Q})$.

Note, however, that the torsor T has "too many rational points" as its fibre over J is $\mathbb{G}_m^{\rho-1}$ and $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$ is not finitely generated. In fact, this brief overview of the method is too simplified and it becomes necessary to work with (residue disks of) a regular, proper, integral model $\mathbf{C}$ of C over $\mathbb{Z}$ and the corresponding diagram (9) over $\mathbb{Z}$.

Their method allows Edixhoven and Lido to reprove Faltings' theorem for curves satisfying the quadratic Chabauty condition $r < g + \rho - 1$. Furthermore, they have made their method effective and have successfully used it to compute the rational points on the quotient of the modular curve $X_0(129)$ by the Atkin–Lehner group $\langle w_3, w_{43} \rangle$ – a genus 2 curve with Mordell–Weil rank 2, hence lying outside the Chabauty–Coleman range.

0.4 Contributions of this thesis

This thesis explores several topics related to the themes described so far. We now introduce each topic and outline the main contributions to be found in this thesis.

0.4.1 Generalised Heegner cycles

The first contribution of this thesis pertains to the study of certain algebraic cycles, known as generalised Heegner cycles, with applications towards the study of their associated Chow–Heegner points. This work is joint with Massimo Bertolini, Henri Darmon and Kartik Prasanna, and has resulted in the published article [11].

Preliminaries

Let r and N be positive integers with $N \geq 5$. Let $X_1(N)$ denote the modular curve over $\mathbb{Q}$ of level $\Gamma_1(N)$ which classifies elliptic curves together with a point of order N. This moduli problem admits a universal object $\pi : \mathcal{E} \longrightarrow X_1(N)$ known as the universal (generalised) elliptic curve over $X_1(N)$. Let W_r denote the r-th Kuga–Sato variety of level $\Gamma_1(N)$, which is the canonical proper desingularisation of the r-fold self-fibre product of $\mathcal{E}$ over $X_1(N)$. Let A be an elliptic curve with complex multiplication by $\mathcal{O}_K$, the ring of integers of some imaginary quadratic field K. We can then consider the smooth projective $(2r+1)$-dimensional variety

$$X_r := W_r \times A^r$$

defined over the Hilbert class field H of K. It comes equipped with a natural projection map $\pi_r : X_r \longrightarrow X_1(N)$, whose fibre over a non-cuspidal point corresponding to an elliptic curve E is $\pi_r^{-1}(E) = E^r \times A^r$.

Let ω_A be a Néron differential of A and let $\eta_A \in H^{0,1}(A/H)$ such that $\langle \omega_A, \eta_A \rangle = 1$. In particular, $\{\omega_A, \eta_A\}$ is then a basis of $H^1_{\mathrm{dR}}(A/H)$. Let θ_A be the theta series associated to the Hecke character ψ of K of infinity type $(r+1, 0)$ satisfying $\psi_H = \psi_A^{r+1}$, where ψ_A is the

Hecke character of H of infinity type $(1,0)$ corresponding to A. The Fourier coefficients of this cusp form generate a finite extension E_{θ_A} of $\mathbb{Q}$ and we let ω_{θ_A} denote the associated class in $H^{r+1}_{\mathrm{dR}}(W_r/E_{\theta_A})$. Assuming the Tate conjecture for the variety $X_r \times A$, there exists a correspondence $\Pi^? \in \mathrm{CH}^{r+1}(X_r \times A)(H) \otimes E_{\theta_A}$ such that

$$\Pi^{?,*}_{\mathrm{dR}}(\omega_A) = c_A \cdot (\omega_{\theta_A} \wedge \eta_A^r),$$

where $c_A \in (H \otimes E_{\theta_A})^\times$ is some constant. This gives rise, as in Section 0.2.2, to a modular parametrisation

$$\Pi^?_* : \mathrm{CH}^{r+1}(X_r)_0 \otimes E_{\theta_A} \longrightarrow A \otimes E_{\theta_A}.$$

In order to construct Chow–Heegner points on A, we need a supply of special cycles in the domain of this natural transformation. A distinguished collection of algebraic cycles in $\mathrm{CH}^{r+1}(X_r)_0$ was first introduced by Bertolini, Darmon and Prasanna [12]. These so-called generalised Heegner cycles are naturally indexed by isogenies of elliptic curves with $\Gamma_1(N)$-level structure. If $\varphi : A \longrightarrow A'$ is such an isogeny, the generalised Heegner cycle Δ_φ is a codimension $r+1$ cycle that lives in the CM fibre of π_r over A' and is essentially given by the r-fold self-product of the graph of φ.

The main result in *loc. cit.* is a p-adic Gross–Zagier formula that relates the images of such cycles under the p-adic syntomic Abel–Jacobi map to special values of certain p-adic Rankin L-series outside the range of classic interpolation.

We now have in hand the three ingredients of the BSD strategy outlined in Section 0.2.2, namely:

1. A generalised modular parametrisation $\Pi^? : \mathrm{CH}^{r+1}(X_r)_0 \longrightarrow A$.

2. A special supply of generalised Heegner cycles, which give rise to Chow–Heegner points $P(X_r, \Pi^?, \Delta_\varphi) \in A \otimes E_{\theta_A}$.

3. The p-adic Gross–Zagier formula of [12].

The difficulty in this situation stems from the fact that it is necessary to assume the Tate conjecture in order to define the modular parametrisation $\Pi^?$. In [13, Theorem 3.3], Bertolini, Darmon and Prasanna manage to construct certain p-adic avatars of these Chow–Heegner points unconditionally and relate them to global points with the expected field of rationality. Moreover, the global point is of infinite order if certain related L-functions have the expected orders of vanishing.

Contributions

In their series of papers [12–14], Bertolini, Darmon and Prasanna initiated a deeper study of their generalised Heegner cycles – a study since then taken up by many authors including Brooks [89], Burungale [33, 34], Elias [66, 67], Kriz [104], Longo and Pati [109], Longo and Vigni [110], Ota [122] and Shnidman [137]. A possible direction, left unexplored, was to consider their algebraic geometric, or even Hodge theoretic, incarnation: a study of the complex Abel–Jacobi images of the cycles, and consequences for Chow and Griffiths groups. The joint work [11], with Bertolini, Darmon and Prasanna, fills this gap.

The first main result is a formula for the image of Δ_φ under the complex Abel–Jacobi map

$$\mathrm{AJ}_{X_r} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow J^{r+1}(X_r/\mathbb{C}) := \frac{\mathrm{Fil}^{r+1} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C})^\vee}{\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})},$$

which is defined in terms of complex integration of differential forms, as in (7).

Theorem A (Bertolini–Darmon–Lilienfeldt–Prasanna)**.** *Let $\varphi : A \longrightarrow \mathbb{C}/\langle 1, \tau\rangle$ be an isogeny of degree $d_\varphi = \deg(\varphi)$, satisfying $\varphi(t_A) = \frac{1}{N}$ and $\varphi^*(2\pi i dw) = \omega_A$. Let $\Lambda_{r,r}$ denote the lattice in $(S_{r+2}(\Gamma_1(N)) \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C}))^\vee$ defined in Section 2.2.4. For all $f \in S_{r+2}(\Gamma_1(N))$ and $0 \leq j \leq r$, we have*

$$\mathrm{AJ}_{X_r}(\Delta_\varphi)(\omega_f \wedge \omega_A^j \eta_A^{r-j}) = \frac{(-d_\varphi)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{i\infty}^{\tau} (z-\tau)^j (z - \bar{\tau})^{r-j} f(z) dz \pmod{\Lambda_{r,r}}.$$

This formula forms the basis of the numerical calculations of Chow–Heegner points carried out by Bertolini, Darmon and Prasanna [13], as we will now explain. Suppose, following *loc. cit.* that K has class number one, odd discriminant and $\mathcal{O}_K^\times = \{\pm 1\}$. Moreover, let ψ_0 be the canonical Hecke character of K of infinity type $(1,0)$, which corresponds (up to isogeny) to an elliptic curve $A/\mathbb{Q}$ with $\mathrm{End}_K(A) \simeq \mathcal{O}_K$ satisfying $L(A/\mathbb{Q}, s) = L(\psi_0, s)$. Now, θ_A is the theta series associated to the Hecke character ψ_0^{r+1}, hence $E_{\theta_A} = \mathbb{Q}$. By clearing denominators, we may then suppose that $\Pi^? \in \mathrm{CH}^{r+1}(X_r \times A)(K)$ and thus it induces a modular parametrisation

$$\Pi^?_* : \mathrm{CH}^{r+1}(X_r)_0 \longrightarrow A.$$

Note, moreover, that $\Pi^{?,*}_{\mathrm{dR}}(\omega_A) = c_A \cdot (\omega_{\theta_A} \wedge \eta_A^r)$ with $c_A \in K^\times$. It is possible to show [127, Ch. 5, Theorem 2.4] that there exists a non-zero scalar $c_r \in \mathcal{O}_K$ such that $c_r \cdot (\omega_{\theta_A} \wedge \eta_A^{r+1})$ is an integral Hodge class on $X_r \times A$. This implies that one can define a map

$$(\Phi^*_{\mathrm{dR}})^\vee : J^{r+1}(X_r/\mathbb{C}) \longrightarrow J^1(A/\mathbb{C})$$

of intermediate Jacobians, which satisfies $\Phi^*_{\mathrm{dR}}(\omega_A) = c_r \cdot (\omega_{\theta_A} \wedge \eta_A^r)$ and thus coincides with the conjectural map $(\Pi^{?,*}_{\mathrm{dR}})^\vee$ (if it exists) up to a constant in $K^\times$. Since AJ_A is an isomorphism, one can define complex avatars of Chow–Heegner points

$$P(X_r, \Delta_\varphi) := \mathrm{AJ}_A^{-1}((\Phi^*_{\mathrm{dR}})^\vee(\mathrm{AJ}_{X_r}(\Delta_\varphi))) \in A(\mathbb{C}).$$

This definition does not require the Tate (or Hodge) conjecture, but the price to pay is that the rationality properties of these points are unknown and mysterious. Conjecturally, the field of rationality is some abelian extension of K (a compositum of a ray class field and a ring class field of K). One can access the point $P(X_r, \Delta_\varphi)$ via the formula

$$\mathrm{AJ}_A(P(X_r, \Delta_\varphi))(\omega_A) = \mathrm{AJ}_{X_r}(\Phi^*_{\mathrm{dR}}(\omega_A)) = c_r \cdot \mathrm{AJ}_{X_r}(\omega_{\theta_A} \wedge \eta_A^r)$$

by functoriality of Abel–Jacobi maps. Thus, Theorem A (with $j = 0$) gives an explicit formula for the point $P(X_r, \Delta_\varphi)$ viewed inside the complex torus $\mathbb{C}/\Lambda_A$ which uniformises $A(\mathbb{C})$, where Λ_A is the period lattice of A. This is used by Bertolini, Darmon and Prasanna in [13, Section 4] to numerically compute the points $P(X_r, \Delta_\varphi)$ and experimentally verify their expected field of definition in many cases. Their calculations can be seen as providing indirect evidence for the Tate and Hodge conjectures in this specific setup.

Another application of Theorem A is the second main theorem of the paper [11].

Theorem B (Bertolini–Darmon–Lilienfeldt–Prasanna)**.** *The subgroup generated by the collection of generalised Heegner cycles in the group of null-homologous codimension $r+1$ cycles of X_r modulo both rational and algebraic (assuming $r \geq 2$) equivalence has infinite rank.*

The proof makes up the technical core of the article, and the result can be viewed as a generalisation of [128, Thm 4.7], which treats classic Heegner cycles on a Kuga–Sato threefold.

The method uses purely transcendental, or Hodge theoretic, arguments coupled with specific properties of modular forms to prove Theorem A. Analytic estimates of the explicit line integrals appearing in the Abel–Jacobi formula are then used in order to determine their vanishing (or not), and consequences for the order of the cycles in the relevant groups. Class field theory, étale ℓ-adic variants of Abel–Jacobi maps and fundamental properties of étale cohomology are employed to upgrade the previous order estimates and show that infinitely many of the cycles have infinite order. Finally, complex multiplication theory as formulated by Shimura is key to understanding the Galois action on these cycles, which allows us to prove that they generate a subgroup of infinite rank.

It is natural to expect the collection of (conjectural) Chow–Heegner points $P(X_r, \Pi^?, \Delta_\varphi)$ to behave similarly to Heegner points – namely, to satisfy the properties of an Euler system and to generate a subgroup of $A(\bar{H})$ of infinite rank. While the latter would imply Theorem B (at least the statement about rational equivalence), it is not implied by Theorem B, as the injectivity properties of the modular parametrisation $\Pi^?_*$ are unknown. Theorem B can be seen as lending support to the statement that the Chow–Heegner points generate a subgroup of infinite rank.

0.4.2 Geometric quadratic Chabauty over number fields

The second contribution of this thesis pertains to the question of the explicit determination of rational points on higher genus curves. The work presented is joint with Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao, and has resulted in the preprint article [41].

Preliminaries

Recall from Section 0.3 the effective methods of Chabauty–Coleman, quadratic Chabauty, and geometric quadratic Chabauty that were introduced. These are tools for the explicit determination of rational points on higher genus curves defined over $\mathbb{Q}$ satisfying certain rank conditions on their Jacobians:

$$\begin{cases} r < g & \text{(Chabauty condition)} \\ r < g + \rho - 1 & \text{(quadratic Chabauty condition),} \end{cases}$$

where we recall that ρ denotes the rank of the Néron–Severi group of the Jacobian. A natural question is the generalisation of these methods to the case of curves C defined over arbitrary number fields K. This has been the subject of recent developments in the field, which we briefly review.

The Chabauty–Coleman method naturally generalises over K. In fact, Coleman in his original paper [36] directly considers this setup. Given an unramified prime $\mathfrak{p}$ of K of good reduction for C, he considers the diagram

$$\begin{array}{ccccc} C(K) & \longrightarrow & C(K_{\mathfrak{p}}) & \overset{\int}{\searrow} & \\ \downarrow{\scriptstyle j_b} & & \downarrow{\scriptstyle j_b} & & \\ J(K) & \longrightarrow & J(K_{\mathfrak{p}}) & \xrightarrow{\log_{\mathfrak{p}}} & H^0(C_{K_{\mathfrak{p}}}, \Omega^1)^\vee, \end{array} \tag{11}$$

and, using his theory of $\mathfrak{p}$-adic integration, proves the following upper bound on the number of rational points

$$|C(K)| \leq N(\mathfrak{p}) + 2g(\sqrt{N(\mathfrak{p})} + 1) - 1,$$

assuming that $r < g$ and $p > 2g$ where $\mathfrak{p}$ lies above the prime p.

Siksek [138] extends the ideas of Chabauty–Coleman by studying all primes of K above p simultaneously, instead of restricting to a single prime as above. This is achieved by considered the Weil restrictions from K to $\mathbb{Q}$ of both the curve C and its Jacobian J in the above picture. In this way, Siksek reduces the geometric situation to working entirely over $\mathbb{Q}$, but the price to pay is that it becomes necessary to work with higher dimensional (hence more complicated) varieties. He successfully generalises the theory of Coleman integration to the setting of the Weil restriction of the Jacobian. Siksek's method, known as Restriction of Scalars (RoS) Chabauty, results in a bound on the number of rational points on curves over K satisfying the RoS Chabauty condition

$$r \leq (g - 1)d, \tag{12}$$

where d is the degree of K. Note, however, that the method can fail to produce a bound on the number of rational points even when (12) is satisfied; examples include the case where the curve C is the base change of a curve C' defined over $\mathbb{Q}$ which does not satisfy the Chabauty condition $\operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}(C') < g$. Aware of this, Siksek in his article asked whether a sufficient condition for his method to prove finiteness is that for all extensions $\mathbb{Q} \subset L \subset K$ over which C admits a good model C_L we have

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}(C_L) \leq (g - 1)[L : \mathbb{Q}].$$

Failures of the method of RoS Chabauty have been studied by Triantafillou [146] who introduces Base-Change-Prym (BCP) obstructions, which account for all known failures to date.

Dogra [60] has recently combined ideas of the RoS Chabauty method with Kim's non-abelian Chabauty program, which has led to the generalisation of the Chabauty–Kim program to arbitrary number fields. He obtains, as in Section 0.3.2, an infinite nested sequence of Chabauty–Kim sets

$$C(K) \subset \ldots \subset C(K \otimes \mathbb{Q}_p)_{n+1} \subset C(K \otimes \mathbb{Q}_p)_n \subset \ldots \subset C(K \otimes \mathbb{Q}_p)_2 \subset C(K \otimes \mathbb{Q}_p)_1 \subset C(K \otimes \mathbb{Q}_p)$$

where $C(K \otimes \mathbb{Q}_p)_1$ is the RoS Chabauty set studied by Siksek. Dogra provides a negative answer to Siksek's question using a BCP-obstruction, but also gives a sufficient condition for RoS Chabauty to prove finiteness of $C(K \otimes \mathbb{Q}_p)_1$ when $r \leq (g-1)d$, namely that

$$\mathrm{Hom}(J_{\bar{\mathbb{Q}},\sigma_1}, J_{\bar{\mathbb{Q}},\sigma_2}) = 0 \text{ for any two distinct embeddings } \sigma_1, \sigma_2 : K \hookrightarrow \bar{\mathbb{Q}}. \tag{13}$$

Moreover, he proves [60, Proposition 1.1], under the same condition (13), that the second Chabauty–Kim set $C(K \otimes \mathbb{Q}_p)_2$ is finite whenever the following quadratic RoS Chabauty condition is satisfied:

$$r + \delta(\rho - 1) \leq (g + \rho - 2)d, \tag{14}$$

where $\delta := \mathrm{rank}_{\mathbb{Z}}\, \mathcal{O}_K^{\times}$.

By the work of Dogra, the theoretical stage is set for the quadratic RoS Chabauty method. It has been made effective recently by Balakrishnan, Besser, Bianchi and Müller [4] in the case of odd degree hyperelliptic curves and genus 2 bielliptic curves. This allows them to determine for example the $\mathbb{Q}(i)$-rational points on the bielliptic modular curve $X_0(91)^+$ defined over $\mathbb{Q}$, and also the $\mathbb{Q}(\sqrt{34})$-rational points on the bielliptic curve (4) defined over $\mathbb{Q}$ studied by Diophantus, Wetherell [152] and Bianchi [20].

Contributions

In the joint work [41] with Čoupek, Xiao and Yao, we generalise the recent geometric quadratic Chabauty method, originally due to Edixhoven and Lido [62] over $\mathbb{Q}$, to the case of higher genus curves defined over arbitrary number fields. Assume that p is a prime such that C admits good reduction at all the primes of K lying above p. We also assume some mild additional ramification conditions on p, the details of which are spelled out in Assumption 3.1. The main theoretical result is roughly the following.

Theorem C (Čoupek–Lilienfeldt–Xiao–Yao)**.** *Let K be a number field of degree d. Let C/K be a smooth, proper, geometrically connected curve of genus $g \geq 2$ with Mordell–Weil rank $r = \operatorname{rank}_{\mathbb{Z}} J(K)$ satisfying condition (14). Let $R := \mathbb{Z}_p\langle z_1, ..., z_{r+\delta(\rho-1)}\rangle$ be the p-adically completed polynomial algebra over $\mathbb{Z}_p$. There exists an ideal I of R, which is explicitly computable modulo p, such that if $\overline{A} := (R/I) \otimes \mathbb{F}_p$ is a finite dimensional $\mathbb{F}_p$-vector space, then the set of rational points $C(K)$ is finite, of size bounded above by $\dim_{\mathbb{F}_p} \overline{A}$.*

The precise form of this theorem is slightly more involved than what is stated above. We need to work integrally with a regular proper model $\mathbf{C}$ of C over $\mathcal{O}_K$, and in order for the method to work, we need to cover $\mathbf{C}^{\mathrm{sm}}$ by certain open subschemes $\mathbf{U}_i$ and work with one $\mathbf{U}_i$ at a time. Moreover, we work separately on each residue disk $\mathbf{U}_{i,u}$ at p of $\mathbf{U}_i$ and produce a bound on the size of $\mathbf{U}_{i,u}(\mathcal{O}_K)$ by constructing an ideal $I_{i,u} \subset R$ for each i, u. The bound on the size of $C(K)$ is then obtained by summing the bounds for each i and u. This is made precise in Corollary 3.2.

If we were to work with a single fixed prime over p, the method would only have a chance of working if the following condition is satisfied

$$r + \delta(\rho - 1) < g + \rho - 1.$$

When K is imaginary quadratic, this amounts to the same quadratic Chabauty condition as over $\mathbb{Q}$ and could still be useful. However, if K is real quadratic, the condition becomes $r < g$

and the Chabauty–Coleman method can already be applied. When considering higher degree number fields, the above condition is more restrictive than the classic Chabauty condition.

As a consequence, it is necessary to work with all primes above p simultaneously in order to have a chance to bound the rational points on curves satisfying (14). This comes as no surprise, as condition (14) stems from Dogra's quadratic RoS Chabauty method, which by definition involves all primes above p. However, the generalisation of the geometric quadratic Chabauty method does not make use of restriction of scalars in the same way as the RoS methods of Siksek, Dogra, and Balakrishnan, Besser, Bianchi and Müller. Where they use Weil restriction to reduce the geometric situation to working over $\mathbb{Q}$, we work directly over K (and even integrally over $\mathcal{O}_K$). Only at the end of the argument do we apply a restriction of scalars and work with all primes above p simultaneously, a step which is crucial.

Note that the bound produced in Theorem C depends on the choice of a prime p and is conditional on a certain $\mathbb{F}_p$-vector space $\bar{A}$ being finite dimensional. Hence one may ask when is the method expected to work ? Edixhoven and Lido in their paper have given a new proof of Faltings' theorem, using their method, in the case of higher genus curves defined over $\mathbb{Q}$ and satisfying $r < g+\rho-1$. Their argument is quite elegant: it uses complex analytic methods to prove a Zariski density statement, which can then be bridged with their p-adic geometric situation using formal geometry. This proves finiteness of the intersection (10) and thus finiteness of $C(\mathbb{Q})$. However, in order to extract an explicit bound for $|C(\mathbb{Q})|$, they similarly rely on some $\mathbb{F}_p$-vector space being finite dimensional. They conjecture [62, Section 4] that it is always possible in practice to choose p such that their condition is satisfied.

The setting over arbitrary number fields is more complicated. Reminiscent of the failures of Siksek's method, there are examples of curves satisfying (14) for which the analogous intersection (10) over K is not finite. Examples include curves base changed from $\mathbb{Q}$ which do not satisfy the quadratic Chabauty condition over $\mathbb{Q}$. Based on Dogra's results, we expect the intersection to be finite whenever conditions (14) and (13) are both satisfied. However, the proof of this still eludes us. Concerning the finite $\mathbb{F}_p$-dimensionality criterion, we expect, following Edixhoven and Lido, that for curves satisfying (14) and (13), there always exists a prime p such that the conditions of Theorem C are satisfied.

0.4.3 Triple product diagonal cycles on $X_0(p)$

The third contribution of this thesis is concerned with algebraic cycles of diagonal type on the triple product of the modular curve $X_0(p)$ of prime level, and associated Chow–Heegner points. This project is the fruit of the author's work alone. It is open-ended as it explores certain algebraic cycle and Chow–Heegner point constructions, providing theoretical evidence that suggests their non-triviality, but failing to prove so. Questions and conjectures are formulated, which will be the subject of future work by the author.

Preliminaries

The study of the diagonal cycle on the triple product of modular curves originates in the work of Gross and Kudla [76], and Gross and Schoen [77] – more precisely, they study a null-homologous modification of the diagonal embedding of the curve in its triple product, known today as the Gross–Kudla–Schoen cycle. Given three modular newforms of weight 2 and square-free level N such that the sign of the functional equation of the associated triple product L-function is -1, Gross and Kudla [76] conjectured that the central value at $s = 2$ of the derivative of this L-function is given by the Beilinson–Bloch height of this cycle. A proof of this conjecture due to Yuan, Zhang and Zhang is expected to appear in [154].

Around 2014, Darmon and Rotger [48–50] initiated a study of the Euler system properties of diagonal cycles in products of Kuga–Sato varieties, which led to new instances of the equivariant Birch and Swinnerton-Dyer conjecture. The study of diagonal cycles is today an active area of research as evidenced by the work of many authors including Bertolini, Seveso and Venerucci [15–17], Buhler, Schoen and Top [32], Blanco-Chacón and Fornea [26], Darmon, Lauder and Rotger [46, 47], Darmon, Rotger and Sols [51], Fornea [69, 70], Fornea and Jin [71], Gatti, Guitart, Masdeu and Rotger [73], Liu [107, 108], and Wang [149, 150].

Let $f \in S_2(\Gamma_0(p))$ be a normalised newform of prime level p, and denote by E_f the elliptic curve over $\mathbb{Q}$ associated to f by the Eichler–Shimura construction described in Section 0.2. Using an auxiliary normalised newform $g \in S_2(\Gamma_0(p))$ (not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f), it is possible to construct a correspondence $\Pi_{g,f} \in \mathrm{CH}^2(X_0(p)^3 \times E_f)(\mathbb{Q})$, which gives rise, as in Section 0.2.2, to a generalised modular parametrisation of E_f

$$\Pi_{g,f,*} : \mathrm{CH}^2(X_0(p)^3)_0 \longrightarrow E_f.$$

Let Δ denote the image of $X_0(p)$ under the diagonal embedding $X_0(p) \longrightarrow X_0(p)^3$, i.e.,

$$\Delta = \{(x, x, x) \mid x \in X_0(p)\} \subset X_0(p)^3.$$

The Gross–Kudla–Schoen cycle arises from Δ by applying a certain correspondence P_{GKS} due to Gross and Schoen [77]. The resulting cycle

$$\Delta_{\mathrm{GKS}} := (P_{\mathrm{GKS}})_*(\Delta) \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$$

then lies in the domain of the modular parametrisation $\Pi_{g,f,*}$. Note that the definition of the projector P_{GKS} depends on a choice of a rational point of $X_0(p)$, which we take to be the cusp at infinity. More generally, we denote by $\Delta_{\mathrm{GKS}}(e)$ the cycle based at $e \in X_0(p)(\mathbb{Q})$.

Darmon, Rotger and Sols [51] have studied, in the broader context of Shimura curves over totally real fields, the Chow–Heegner point

$$P(X_0(p)^3, \Pi_{g,f}, \Delta_{\mathrm{GKS}}) \in E(\mathbb{Q}), \tag{15}$$

notably by computing the image of Δ_{GKS} under the complex Abel–Jacobi map $\mathrm{AJ}_{X_0(p)^3}$ in terms of iterated integrals. Methods have been developed by Darmon, Daub, Lichtenstein and Rotger [44] to numerically calculate such points.

In this setting, the three ingredients of the BSD strategy outlined in Section 0.2.2 are:

1. The generalised modular parametrisation $\Pi_{g,f,*} : \mathrm{CH}^2(X_0(p)^3)_0 \longrightarrow E_f$.

2. The Gross–Kudla–Schoen cycle Δ_{GKS} which gives rise to the Chow–Heegner point $P(X_0(p)^3, \Pi_{g,f}, \Delta_{\mathrm{GKS}}) \in E_f(\mathbb{Q})$.

3. The conjectural Gross–Kudla formula relating the first central derivative of the triple product L-functions $L(g^\sigma, g^\sigma, f, s)$ at $s = 2$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$ to the behaviour of Δ_{GKS}.

Armed with these ingredients, Darmon, Rotger and Sols [51, Theorem 3.7] have given a criterion for $P(X_0(p)^3, \Pi_{g,f}, \Delta_{\mathrm{GKS}})$ to have infinite order in $E(\mathbb{Q})$ based on certain orders of vanishing of L-functions. More precisely, observe that the triple product L-function decomposes as

$$L(g, g, f, s) = L(f, s-1)L(\mathrm{Sym}^2(g) \otimes f, s).$$

Now, assuming that the global root numbers are $W(f) = -1$ and $W(\mathrm{Sym}^2(g) \otimes f) = +1$, they establish that $P(X_0(p)^3, \Pi_{g,f}, \Delta_{\mathrm{GKS}})$ has infinite order if and only if

$$\mathrm{ord}_{s=1} L(f, s) = 1 \qquad \text{and} \qquad \mathrm{ord}_{s=2} L(\mathrm{Sym}^2(g^\sigma) \otimes f, s) = 0, \ \forall \sigma : K_g \hookrightarrow \mathbb{C}.$$

Contributions

We are mainly motivated by the important theme of detecting the position of algebraic cycles in Chow groups via analytic or transcendental invariants such as L-functions. This problem has been formulated more precisely in the Beilinson–Bloch conjecture (a generalisation of the Birch and Swinnerton-Dyer conjecture 0.1 to higher dimensional varieties and algebraic cycles). Let f_1, f_2, f_3 be three newforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$ denote their triple tensor product. Associated to F is the Garrett–Rankin triple product L-function $L(F, s)$ (sometimes also denoted $L(f_1, f_2, f_3, s)$). The Beilinson–Bloch conjecture in this setting predicts that the central order of vanishing $\mathrm{ord}_{s=2} L(F, s)$ is equal to the rank of the F-isotypic component of the Chow group $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ of null-homologous cycles of codimension 2 on $X_0(p)^3$. The first main result is a global root number calculation.

Theorem D (Lilienfeldt)**.** *Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$. If χ denotes the Legendre symbol at p, then the global root number of the twisted triple product L-function $L(F \otimes \chi, s)$ is equal to -1.*

The Legendre symbol χ is the character of the unique quadratic extension of $\mathbb{Q}$ which ramifies only at p, namely $K = \mathbb{Q}(\sqrt{\chi(-1)p})$. Let τ denote the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Guided by the Beilinson–Bloch conjecture, we expect by Theorem D the existence of a non-torsion algebraic cycle in the F-isotypic component of $\mathrm{CH}^2(X_0(p)^3)_0(K)$ which lies in the (-1)-eigenspace for τ. In parallel, we construct a canonical cycle

$$\Xi := \Delta_+ - \Delta_- \in \mathrm{CH}^2(X_0(p)^3), \tag{16}$$

where the cycles Δ_+ and Δ_- arise as images of maps $\varphi_+, \varphi_- : X(p) \longrightarrow X_0(p)^3$ respectively. Here $X(p)$ denotes the modular curve of full level p-structure over the cyclotomic field $\mathbb{Q}(\zeta_p)$.

Theorem E (Lilienfeldt)**.** *The cycle Ξ belongs to $\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}$.*

The maps φ_+ and φ_- are defined using the moduli interpretation of $X_0(p)$ in an essential way. Therefore, this construction is not available for the triple product of a generic curve, as opposed to the Gross–Kudla–Schoen cycle described above. The cycle Ξ is canonical in the sense that it does not depend on the choice of a base-point, and does not require a projector to render it null-homologous (again, as opposed to $\Delta_{\mathrm{GKS}}(e)$). Moreover, there are no apparent geometric phenomena that suggest that the construction yields a torsion element in the Chow group. Guided by the Beilinson–Bloch conjecture, we are led to formulate refined conjectures in a context that has never been explored before. In particular, we conjecture the following (Conjecture 4.1).

Conjecture (Lilienfeldt). *Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$ denote the associated triple product. The cycle*

$$(t_F)_*(\Xi) \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star}))^{\tau=-1} \otimes K_F$$

is non-zero if and only if $\mathrm{ord}_{s=2} L(F \otimes \chi, s) = 1$. Here $t_F \in \mathrm{CH}^3(X_0(p)^6)$ is the F-isotypic projector which cuts out the motive of F.

We further refine this by distinguishing between the situations where $W(F) = +1$ and $W(F) = -1$ (Conjectures 4.2 and 4.3), bringing into play the interaction with the Gross–Kudla–Schoen cycle. Another main result concerns the latter cycle when the global root number of F is assumed to be $+1$, and is consistent with Conjecture 4.2.

Theorem F (Lilienfeldt). *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(p))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies $W(F)=+1$. Then $\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e)))$ is torsion in $J^2(X_0(p)^3/\mathbb{C})$ for any base point $e \in X_0(p)(\mathbb{Q})$.*

Here $\mathrm{AJ}_{X_0(p)^3}$ denotes the complex Abel–Jacobi map of codimension 2 for $X_0(p)^3$ and $J^2(X_0(p)^3/\mathbb{C})$ is the second intermediate Jacobian. See Section 0.2.3.

Specialising now to the case where one of the three forms, say f, has rational Fourier coefficients and the other two forms are equal to some g (not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f), we may consider the generalised modular parametrisation described above, namely

$$\Pi_{g,f,*} : \mathrm{CH}^2(X_0(p)^3)_0 \longrightarrow E_f,$$

where E_f is the elliptic curve over $\mathbb{Q}$ attached to f by the Eichler–Shimura construction. Applying this map to the cycle (16) yields a Chow–Heegner point

$$P(X_0(p)^3, \Pi_{g,f}, \Xi) \in E_f(K)^{\tau=-1}.$$

If we assume that $p \equiv 3 \pmod 4$, then $K = \mathbb{Q}(\sqrt{-p})$ and the global root number of the quadratic twist E^χ of E by χ is $W(E^\chi) = +1$. In line with the Birch and Swinnerton-Dyer conjecture 0.1, we prove the following.

Theorem G (Lilienfeldt)**.** *Let f and g be two normalised newforms in $S_2(\Gamma_0(p))$ as above. If we assume $p \equiv 3 \pmod 4$, then the Chow–Heegner point $P(X_0(p)^3, \Pi_{g,f}, \Xi)$ is torsion in $E_f(\mathbb{Q}(\sqrt{-p}))$.*

If we assume that $p \equiv 1 \pmod 4$, then $K = \mathbb{Q}(\sqrt{p})$ and the global root number of the quadratic twist E^χ of E by χ is $W(E^\chi) = -1$. Guided by the Birch and Swinnerton-Dyer conjecture 0.1, the proposed conjectures about the cycle Ξ lead us to make analogous conjectures about $P(X_0(p)^3, \Pi_{g,f}, \Xi)$. In particular, we conjecture (Conjecture 4.4) the following.

Conjecture (Lilienfeldt)**.** *Let f and g be normalised newforms in $S_2(\Gamma_0(p))$ as above. If $p \equiv 1 \pmod 4$, then the point $P(X_0(p)^3, \Pi_{g,f}, \Xi) \in E_f(\mathbb{Q}(\sqrt{p}))^{\tau=-1}$ has infinite order if and only if $\mathrm{ord}_{s=1} L(E_f^\chi/\mathbb{Q}, s) = 1$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f \otimes \chi, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$.*

We further refine this depending on whether $W(E/\mathbb{Q}) = +1$ or $W(E/\mathbb{Q}) = -1$ in Conjectures 4.5 and 4.6, bringing into play the interaction with the Chow–Heegner point (15). Using Theorem F, we prove the following.

Theorem H (Lilienfeldt)**.** *If E_f admits split multiplicative reduction at p, then the Chow–Heegner point $P(X_0(p)^3, \Pi_{g,f}, \Delta_{\mathrm{GKS}}(e))$ is torsion in $E_f(\mathbb{Q})$ for all $e \in X_0(p)(\mathbb{Q})$.*

This is a particular case of a more general result obtained by Daub [53], but the proof differs as Daub relies on a comparison with Zhang points. Theorem H is consistent with Conjecture 4.5.

Following Section 0.2.3, one strategy for addressing the conjecture above is to compute the image of the Chow–Heegner point under the complex Abel–Jacobi isomorphism AJ_{E_f}, which is given by the formula

$$\mathrm{AJ}_{E_f}(P(X_0(p)^3, \Pi_{g,f}, \Xi))(\omega_f) = \mathrm{AJ}_{X_0(p)^3}(\Xi)((\Pi_{g,f})^*_{\mathrm{dR}}(\omega_f)).$$

The computation of $\mathrm{AJ}_{X_0(p)^3}(\Xi)$ will be addressed in future work. We note that the techniques developed in [51] to compute $\mathrm{AJ}_{X_0(p)^3}(\Delta_{\mathrm{GKS}})$ do not seem to carry over to the present setting. See Section 5.1 for a more detailed discussion of possible strategies to tackle the above conjectures.

0.5 Outline

We end the introduction with an outline of the contents of the thesis. We have attempted to keep this document reasonably self-contained; where details are insufficient, we provide references for the interested reader.

Chapter 1 reviews the background material necessary for the main body of the thesis. The concepts of elliptic curves, modular forms and their L-functions are recalled, as well as the theory of complex multiplication. The topic of algebraic cycles and associated Abel–Jacobi maps is surveyed. This chapter is meant to be concise and precise, and as a result it is non-exhaustive: only themes relevant for this thesis are covered.

Chapter 2 pertains to the author's joint work on generalised Heegner cycles with Bertolini, Darmon and Prasanna. As such, this chapter is a reformatted version of the article [11]. In particular, all results presented are joint and taken from *loc. cit.*

Chapter 3 contains the author's joint work with Čoupek, Xiao and Yao on the geometric quadratic Chabauty method over arbitrary number fields. The content is based on the preprint article [41] and is reformatted to fit this thesis.

Chapter 4 presents the author's work on triple diagonal cycles on $X_0(p)$. As mentioned previously, this is the result of the author's sole work, and remains open-ended as questions and conjectures are formulated, without full answers being given.

Chapter 5 concludes this thesis by briefly introducing open projects and questions that the author plans to address in the future. Concerning the diagonal cycles introduced in Chapter 4, we discuss the complex Abel–Jacobi map and the p-adic Abel–Jacobi map, as well as comparisons of Chow–Heegner points with Heegner points or Stark–Heegner points. Concerning the method of Chapter 3, we would like to establish precise conditions that guarantee that the method works, as well as apply the method to explicit examples in order to test the sharpness of the bound. We also outline a project concerned with new examples of curves whose Ceresa class is torsion.

Chapter 1

Preliminaries

The goal of this first chapter is to lay the groundwork for the main body of the thesis. As such, it is solely expository and contains almost no proofs. The exposition is kept brief and references are provided to fill gaps where proofs are lacking, and also to supplement material for the various themes covered.

We begin in Section 1.1 by reviewing how to attach L-functions to smooth algebraic varieties, or more generally to pure motives, using Weil–Deligne representations. This approach allows us to define ϵ-factors and global root numbers in order to state the conjectural functional equation of such L-functions. This material will become handy in Chapter 4 when proving Theorem D.

Section 1.2 introduces elliptic curves and modular forms with focus on the key properties relevant for us. These are central concepts throughout Chapters 2 and 4. After a brief introduction to elliptic curves and modular curves, we review the Modularity Theorem and recall that the motive associated to higher weight modular forms can be realised in certain Kuga–Sato varieties.

Section 1.3 surveys the theory of elliptic curves with complex multiplication and how this relates to the class field theory of quadratic imaginary fields. This plays an important role in Chapter 2.

Section 1.4 defines algebraic cycles along with three equivalence relations: rational, algebraic and homological equivalence. This leads to the definition of the Chow group of a smooth projective variety and we formulate the Beilinson–Bloch conjecture, which generalises the Birch and Swinnerton-Dyer conjecture to higher dimensions.

Section 1.5 introduces three types of so-called Abel–Jacobi maps: the complex Abel–Jacobi map, the Bloch map, and the ℓ-adic étale Abel–Jacobi map. The main properties are reviewed and the existing comparison theorems between these maps are explained.

Notation 1.1. All number fields arising in this chapter are viewed as embedded in a fixed algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Moreover, we fix a complex embedding $\sigma : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, as well as a p-adic embeddings $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ for each rational prime p. In this way, all finite extensions of $\mathbb{Q}$ are viewed simultaneously as subfields of $\mathbb{C}$ and $\mathbb{C}_p$.

1.1 Weil–Deligne representations and L-functions

This section introduces the background material on Weil–Deligne representations, selecting only the results relevant for our setup. The reader is referred to [56, 126] for more details.

1.1.1 The Weil–Deligne group

Let q denote a prime number. The embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_q$ fixed in Notation 1.1 realises $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ as the decomposition subgroup at q of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. It sits in the short exact sequence

$$1 \longrightarrow I_q \longrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q) \xrightarrow{r} \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow 1$$

where I_q denotes the inertia subgroup at q and r denotes the natural reduction map. The group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by the Frobenius automorphism $\phi : x \mapsto x^q$ and is isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$. We denote by φ the inverse of the Frobenius automorphism ϕ.

Definition 1.1. The Weil group at q, denoted $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$, is defined as the pre-image under r of the infinite cyclic subgroup of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ generated by ϕ. We endow it with the coarsest topology for which $r : W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow \langle\phi\rangle$ and $I_q \hookrightarrow W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ are both continuous and for which $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ is a topological group.

By a representation of the Weil group we mean a continuous homomorphism of groups

$$\sigma_q : W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow \mathbf{GL}(V)$$

where V is a finite dimensional complex vector space. The continuity condition is equivalent to asking that the homomorphism σ_q is trivial on an open subgroup of I_q.

Examples of Weil representations include all finite dimensional complex representations of Galois groups of finite extensions of $\mathbb{Q}$. Also, we identify all characters of $\mathbb{Q}_q^\times$ with characters of $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ via the Artin isomorphism

$$\mathbb{Q}_q^\times \simeq W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)^{\mathrm{ab}} \tag{1.1}$$

normalised so that it maps q to the image in $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)^{\mathrm{ab}}$ of an inverse Frobenius element of $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$.

Definition 1.2. Another example of a Weil representation is given by the character

$$\omega_q : W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow \mathbb{C}^\times$$

defined by $\omega_q(I_q) = 1$ (i.e., it is unramified) and $\omega_q(\Phi) = q^{-1}$ where Φ is an inverse Frobenius element of $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ (i.e., an element satisfying $r(\Phi) = \varphi$). Under the isomorphism (1.1) the character ω_q corresponds to the q-adic norm character $\|\cdot\|_q : \mathbb{Q}_q^\times \longrightarrow \mathbb{C}^\times$ normalised such that $\|q\|_q = q^{-1}$.

We let $W'(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ denote the Weil–Deligne group at q and we refer to [126, §3] for its definition. We do not need the precise definition of this group as its continuous finite dimensional complex representations admit a very nice description in terms of Weil representations.

Definition 1.3. A Weil–Deligne representation is a pair $\sigma_q' = (\sigma_q, N_q)$ where σ_q is a Weil representation on a finite dimensional complex vector space V and N_q is a nilpotent endomorphism of V satisfying

$$\sigma_q(g) \circ N_q \circ \sigma_q(g)^{-1} = \omega_q(g) N_q \qquad \text{for all } g \in W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q). \tag{1.2}$$

For ℓ a prime distinct from q, it is possible to associate to an ℓ-adic Galois representation $\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_d(\mathbb{Q}_\ell)$ a Weil–Deligne representation of $W'(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$. This procedure is due to Grothendieck and Deligne. Let $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ denote a fixed embedding. One can restrict ρ_ℓ to the Weil group $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ and compose with ι to obtain a complex representation

$$\sigma_{\ell,\iota} : W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow \mathbf{GL}_d(\mathbb{C}).$$

If ρ_ℓ is trivial on an open subgroup of the inertia group I_q, then $\sigma_{\ell,\iota}$ is a Weil representation and the associated Weil–Deligne representation is $\sigma_{\ell,\iota}' = (\sigma_{\ell,\iota}, 0)$. However, if ρ_ℓ is not trivial on an open subgroup of I_q, then $\sigma_{\ell,\iota}'$ has non-trivial monodromy and the precise recipe is given in [126, §4].

Example 1.1. Consider the ℓ-adic cyclotomic character

$$\omega_{\mathrm{cyc},\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}) \longrightarrow \mathbb{Z}_\ell^\times$$

where ζ_{ℓ^∞} denotes a compatible system $(\zeta_{\ell^n})_n$ of primitive ℓ^n-th roots of unity. If σ is an element in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then $\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{m_n}$ for some compatible $m_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ and $\omega_{\mathrm{cyc},\ell}(\sigma) = (m_n)_n \in \mathbb{Z}_\ell^\times$. This character is unramified at q since the extension $\mathbb{Q}(\zeta_{\ell^\infty})$ of $\mathbb{Q}$ is ramified only at ℓ. Hence the Weil–Deligne representation at q of $\omega_{\mathrm{cyc},\ell}$ is the Weil representation $\iota \circ \omega_{\mathrm{cyc},\ell}|_{W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)}$. If Φ is a geometric Frobenius element of $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$, then $\omega_{\mathrm{cyc},\ell}(\Phi) = q^{-1} \in \mathbb{Z}_\ell^\times$ and thus $\iota \circ \omega_{\mathrm{cyc},\ell}|_{W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)} = \omega_q$ of Definition 1.2. In particular, the

Weil–Deligne representation of $\omega_{\mathrm{cyc},\ell}$ at q is independent of ι and ℓ.

There is also a theory of Weil–Deligne representations at archimedean places. In this case the Weil–Deligne group and the Weil group are equal. We have the following two situations:

- Over the field $\mathbb{C}$, the Weil group is $W(\mathbb{C}/\mathbb{C}) = \mathbb{C}^\times$. We consider on $\mathbb{C}$ the Haar measure $\mathbf{d}x = |\mathbf{d}z \wedge \mathbf{d}\bar{z}| = 2\mathbf{d}a\mathbf{d}b$ where $z = a + ib$ such that $\mathbf{d}(\lambda x) = |\lambda|^2 \mathbf{d}x$ for all $\lambda \in \mathbb{C}$ and $|\cdot|$ is the complex modulus. This is twice the Lebesgue measure. The irreducible Weil representations of $\mathbb{C}$ are given by quasi-character $\chi : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$. These take on the form $z^{-N}\omega_s(z)$ or $\bar{z}^{-N}\omega_s(z)$ for $n \in \mathbb{N}$ and $s \in \mathbb{C}$ where $\omega_s = |\cdot|^{2s}$.

- Over the field $\mathbb{R}$, the Weil group is $W(\mathbb{C}/\mathbb{R}) = \mathbb{C}^\times \cup J\mathbb{C}^\times$ where $J^2 = -1$ and $JzJ^{-1} = \bar{z}$ for $z \in \mathbb{C}^\times$. We consider on $\mathbb{R}$ the Lebesgue measure $\mathbf{d}x$ such that $\mathbf{d}(\lambda x) = |\lambda|\mathbf{d}x$ for all $\lambda \in \mathbb{R}$ where $|\cdot|$ denotes the absolute value. The irreducible Weil representations of $\mathbb{R}$ are given by quasi-character $\chi : \mathbb{C}^\times \cup J\mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ or $\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\,\chi := \mathrm{ind}_{W(\mathbb{C}/\mathbb{C})}^{W(\mathbb{C}/\mathbb{R})}\,\chi$ for quasi-characters $\chi : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ with $\chi \neq \chi \circ c$. The quasi-characters of $W(\mathbb{C}/\mathbb{R})$ take on the form $\mathrm{sign}(x)^{-N}\omega_s(x)$ for $n \in \{0, 1\}$ and $s \in \mathbb{C}$, where $\mathrm{sign} : W(\mathbb{C}/\mathbb{R}) \longrightarrow \mathbb{C}^\times$ is the quadratic character with kernel $W(\mathbb{C}/\mathbb{C})$, i.e., $\mathrm{sign}(z) = 1$ and $\mathrm{sign}(Jz) = -1$ for all $z \in \mathbb{C}^\times$.

1.1.2 Local ε-factors

Epsilon factors were first introduced by Deligne [56] and their properties are summarised in section 5 of *loc. cit.*. We will follow the exposition of [126] to collect the essential properties needed for the purposes of this thesis. We begin by defining the epsilon factor of a Weil–Deligne representation in terms of the epsilon factor of the corresponding Weil representation. We then give the definition of the epsilon factor of a Weil representation.

At the infinite place ∞, let σ'_∞ denote a representation of the Weil–Deligne group $W(\mathbb{C}/\mathbb{R})$, let $\psi : \mathbb{R} \longrightarrow \mathbb{C}^\times$ denote a non-trivial addiditive character and $\mathbf{d}x$ the choice of a Haar measure on $\mathbb{R}$. The epsilon factor depends on these choices and is given by

$$\epsilon'(\sigma'_\infty, \psi, \mathbf{d}x) = \epsilon(\sigma_\infty, \psi, \mathbf{d}x) \in \mathbb{C}^\times.$$

If q is a finite place, let $\sigma'_q = (\sigma_q, N_q)$ be a Weil–Deligne representation with associated finite dimensional complex vector space V. Let $\psi_q : \mathbb{Q}_q \longrightarrow \mathbb{C}^\times$ denote an additive character and let $\mathbf{d}x_q$ denote the choice of a Haar measure on $\mathbb{Q}_p$. The epsilon factor associated to σ'_q depends on ψ_q and $\mathbf{d}x_q$ and is given by

$$\epsilon'(\sigma'_q, \psi_q, \mathbf{d}x_q) := \epsilon(\sigma_q, \psi_q, \mathbf{d}x_q)\delta(\sigma'_q) \in \mathbb{C}^\times, \tag{1.3}$$

where

$$\delta(\sigma'_q) := \det(-\Phi \mid V^{I_q}/(V^{I_q} \cap \ker N_q)). \tag{1.4}$$

In the case where the Weil–Deligne representation at a place v is a character, the epsilon factor above is defined via Tate's local functional equation. It satisfies

$$\epsilon(\chi, \psi, a\mathbf{d}x) = a\epsilon(\chi, \psi, \mathbf{d}x) \qquad \text{and} \qquad \epsilon(\chi, \psi(ax), \mathbf{d}x) = \chi(a)\omega^{-1}(a)\epsilon(\chi, \psi, \mathbf{d}x).$$

Explicit formulas for the epsilon factor of a character are given as follows.

- Over $\mathbb{C}$, take the additive character $\psi_\mathbb{C} : \mathbb{C} \longrightarrow \mathbb{C}^\times$ to be $\psi_\mathbb{C}(z) = \exp(2\pi i \, \mathrm{t}_{\mathbb{C}/\mathbb{R}}(z))$ and the Haar measure to be $\mathbf{d}x_\mathbb{C} = |\mathbf{d}z \wedge \mathbf{d}\bar{z}|$. Given a quasi-character $\chi : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ of the form $z \mapsto z^{-N}\omega_s(z)$ or $z \mapsto \bar{z}^{-N}\omega_s(z)$ with $N \in \mathbb{N}$ and $s \in \mathbb{C}$,

$$\epsilon(\chi, \psi_\mathbb{C}, \mathbf{d}x_\mathbb{C}) := i^N. \tag{1.5}$$

- Over $\mathbb{R}$, take the additive character $\psi_\mathbb{R} : \mathbb{R} \longrightarrow \mathbb{C}^\times$ to be $\psi_\mathbb{R}(x) = \exp(2\pi i x)$ and the Haar measure $\mathbf{d}x_\mathbb{R}$ to be the Lebesgue measure. If $\chi : W(\mathbb{C}/\mathbb{R}) \longrightarrow \mathbb{C}^\times$ is a quasi-character of the form $x \mapsto \mathrm{sign}(x)^{-N}\omega_s(x)$ with $N \in \{0,1\}$ and $s \in \mathbb{C}$, then

$$\epsilon(\chi, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) := i^N. \tag{1.6}$$

- Let χ be a character of $\mathbb{Q}_p^\times$ identified with a one-dimensional representation of the Weil group. Let $n(\psi_q)$ denote the largest integer n such that ψ_q is trivial on $q^{-n}\mathbb{Z}_q$. Let $a(\chi)$ denote the conductor of χ, i.e., $a(\chi) = 0$ is χ is unramified and otherwise $a(\chi)$ is the smallest positive integer m such that χ is trivial on $1 + q^m\mathbb{Z}_q$. Then

$$\epsilon(\chi, \psi_q, \mathbf{d}x_q) = \begin{cases} \int_{q^{-(n(\psi_q)+a(\chi))}\mathbb{Z}_q^\times} \chi^{-1}(x)\psi_q(x)\mathbf{d}x_q & \text{if } \chi \text{ is ramified} \\ \chi\omega_q^{-1}(q^{n(\psi_q)}) \int_{\mathbb{Z}_q} \mathbf{d}x_q & \text{if } \chi \text{ is unramified.} \end{cases} \tag{1.7}$$

The epsilon factor of a Weil representation is completely determined by the following result.

Theorem 1.1. *Let K be either $\mathbb{R}, \mathbb{C}$ or $\mathbb{Q}_q$ for some finite place q. There is a unique function ϵ, which to any Weil representation σ, any non-trivial additive character $\psi : K \longrightarrow \mathbb{C}^\times$ and any choice of a Haar measure $\mathbf{d}x$ on K, associates a complex number $\epsilon(\sigma, \psi, \mathbf{d}x) \in \mathbb{C}^\times$ satisfying:*

i) $\epsilon(*, \psi, \mathbf{d}x)$ is multiplicative in short exact sequences.

ii) If L/K is any finite extension of K in $\bar{K}$ and σ_L is a Weil representation of L, then for any choice of Haar measure $\mathbf{d}x_L$ on L, we have

$$\epsilon(\mathrm{ind}_{W(\bar{K}/L)}^{W(\bar{K}/K)} \sigma_L, \psi, \mathbf{d}x) = \epsilon(\sigma_L, \psi \circ \mathrm{t}_{L/K}, \mathbf{d}x_L) \left(\frac{\epsilon(\mathrm{ind}_{W(\bar{K}/L)}^{W(\bar{K}/K)} 1_L, \psi, \mathbf{d}x)}{\epsilon(1_L, \psi \circ \mathrm{t}_{L/K}, \mathbf{d}x_L)} \right)^{\dim \sigma_L}.$$

iii) If $\dim \sigma = 1$, then $\epsilon(\sigma, \psi, \mathbf{d}x)$ is given by the above formulas (1.5), (1.6), (1.7).

Proof. This is [56, Theorem 4.1]. □

Definition 1.4. Let K be either $\mathbb{R}, \mathbb{C}$ or $\mathbb{Q}_q$ for some finite place q. Given a Weil–Deligne representation $\sigma' = (\sigma, N)$ of K, the choice of an additive character $\psi : K \longrightarrow \mathbb{C}^\times$ and a Haar measure $\mathbf{d}x$ on K, we define the root number

$$W(\sigma', \psi) = \frac{\epsilon'(\sigma', \psi, \mathbf{d}x)}{|\epsilon'(\sigma', \psi, \mathbf{d}x)|}.$$

Remark 1.1. As the notation suggests, the root number is independent of the choice of a Haar measure $\mathbf{d}x$, as can be seen from [126, §11 Proposition (ii)]. Moreover, if the Weil–Deligne representation σ'_q at a finite prime q is essentially symplectic, then the local root number at q is independent of the additive character ψ and belongs to $\{\pm 1\}$ by [126, §12]. We shall simply write $W(\sigma'_q)$ in this case.

We end this section with a few results concerning epsilon factors of Weil–Deligne representations at finite places.

Proposition 1.1. *If χ is an unramified character of $\mathbb{Q}_q^\times$, $\psi : \mathbb{Q}_q \longrightarrow \mathbb{C}^\times$ is a non-trivial additive character and $\mathbf{d}x$ is Haar measure on $\mathbb{Q}_q$, then*

$$\epsilon(\sigma_q \otimes \chi, \psi, \mathbf{d}x) = \chi(q^{n(\psi)\dim(\sigma_q) + a(\sigma_q)})\epsilon(\sigma_q, \psi, \mathbf{d}x).$$

Here $a(\sigma_q)$ is the conductor of σ_q defined in [126, §10].

Proof. This is [126, §11 Proposition (iii)]. □

The following proposition gives an explicit formula for the epsilon factor of a ramified character of conductor 1. Note that if $\psi : \mathbb{Q}_q \longrightarrow \mathbb{C}^\times$ is an additive character with $n(\psi_q) = 0$, then $\psi|_{\mathbb{Z}_q^\times} = 1$ but $\psi|_{q^{-1}\mathbb{Z}_q^\times} \neq 1$. Thus there exists $c \in \mathbb{F}_q^\times$ such that $\psi(1/q) = \exp((2\pi i c)/q)$. In this case, we write ψ_c for ψ. The proof of the following proposition is part of the proof of [123, Theorem 3.2 (2)], but we choose to include it here for the convenience of the reader.

Proposition 1.2. *Let χ be a ramified character of $\mathbb{Q}_q^\times$ identified with a one-dimensional representation of the Weil group. Let $\psi : \mathbb{Q}_q \longrightarrow \mathbb{C}^\times$ denote an unramified additive character,* *i.e.,* $n(\psi) = 0$, *and* $\mathbf{d}x$ *denote the Haar measure on* $\mathbb{Q}_p$ *such that* $\int_{\mathbb{Z}_p} \mathbf{d}x = 1$. *Suppose that* $a(\chi) = 1$. *Let* $c \in \mathbb{F}_q^\times$ *such that* $\psi = \psi_c$. *Then the following formula holds:*

$$\epsilon(\chi, \psi, \mathbf{d}x) = \chi(c)\chi(q)G(\chi^{-1})$$

where $G(\chi^{-1}) = \sum_{b \in \mathbb{F}_q^\times} \chi^{-1}(b) e^{\frac{2\pi i b}{q}}$ *is the Gauss sum of the character* χ^{-1}.

Proof. Since $a(\chi) = 1$ we have $\chi|_{\mathbb{Z}_q^\times} \neq 1$ but $\chi|_{1+q\mathbb{Z}_q} = 1$ (i.e., χ is tamely ramified). So when restricted to $\mathbb{Z}_q^\times$, the character χ factors through the quotient $\mathbb{Z}_q^\times/(1 + q\mathbb{Z}_q) \simeq \mathbb{F}_q^\times$ and can be seen as a Dirichlet character modulo q. Thus the expression defining the Gauss sum makes sense. By Theorem 1.1 *iii*) we have the following formula for the epsilon factor:

$$\epsilon(\chi, \psi, \mathbf{d}x) = \int_{q^{-1}\mathbb{Z}_q^\times} \chi^{-1}(x)\psi(x)\mathbf{d}x.$$

The normalisation of the Haar measure implies that for all $a \in \mathbb{Z}_q$ we have the identity $\mathbf{d}(ax) = \|a\|_q \mathbf{d}x$, where the q-adic norm is the one in Definition 1.2. Taking this into account, a simple change of variables yields the following expression:

$$\epsilon(\chi, \psi, \mathbf{d}x) = q \int_{\mathbb{Z}_q^\times} \chi^{-1}\left(\frac{x}{q}\right) \psi\left(\frac{x}{q}\right) \mathbf{d}x.$$

Recall that $\mathbb{Z}_q^\times \simeq \mathbb{F}_q^\times \times (1 + q\mathbb{Z}_q)$ and thus we have $\mathbb{Z}_q^\times = \bigcup_{b \in \mathbb{F}_q^\times} (b + q\mathbb{Z}_q)$ where the union is disjoint. We decompose the above integral accordingly to get

$$\epsilon(\chi, \psi, \mathbf{d}x) = q \sum_{b \in \mathbb{F}_q^\times} \int_{b+q\mathbb{Z}_q} \chi^{-1}\left(\frac{x}{q}\right) \psi\left(\frac{x}{q}\right) \mathbf{d}x = q\chi(q) \sum_{b \in \mathbb{F}_q^\times} \int_{b+q\mathbb{Z}_q} \chi^{-1}(x) \psi\left(\frac{x}{q}\right) \mathbf{d}x.$$

Making the change of variables $x = b + qy$, we obtain

$$\epsilon(\chi, \psi, \mathbf{d}x) = q\chi(q) \sum_{b \in \mathbb{F}_q^\times} \int_{\mathbb{Z}_q} \chi^{-1}(b + qy) \psi\left(\frac{b}{q} + y\right) \mathbf{d}(b + qy).$$

Since χ is trivial on $1 + q\mathbb{Z}_q$, we have $\chi^{-1}(b + qy) = \chi^{-1}(b)$ whenever $y \in \mathbb{Z}_q$. Since ψ is an additive character, we have $\psi\left(\frac{b}{q} + y\right) = \psi\left(\frac{b}{q}\right)\psi(y)$. But ψ is trivial on $\mathbb{Z}_q^\times$, whence $\psi(y) = 1$ for $y \in \mathbb{Z}_q$. We therefore arrive at the formula

$$\epsilon(\chi, \psi, \mathbf{d}x) = q\chi(q) \sum_{b \in \mathbb{F}_q^\times} \chi^{-1}(b)\psi\left(\frac{b}{q}\right) \int_{\mathbb{Z}_q} \mathbf{d}(b + qy) = \chi(q) \sum_{b \in \mathbb{F}_q^\times} \chi^{-1}(b)\psi\left(\frac{b}{q}\right)$$

since $\int_{\mathbb{Z}_q} \mathbf{d}(b + qy) = \int_{\mathbb{Z}_q} \mathbf{d}(qy) = \frac{1}{q}\int_{\mathbb{Z}_q} \mathbf{d}y = \frac{1}{q}$ by the normalisation of the Haar measure. Finally, we assumed that $\psi = \psi_c$, and therefore

$$\sum_{b \in \mathbb{F}_q^\times} \chi^{-1}(b)\psi\left(\frac{b}{q}\right) = \sum_{b \in \mathbb{F}_q^\times} \chi^{-1}(b)e^{\frac{2\pi ibc}{q}} = \chi(c)G(\chi^{-1})$$

and the proof is complete. □

Corollary 1.1. *With the same notations and assumptions as in Proposition 1.2, we have the formula*

$$\epsilon(\chi, \psi, \mathbf{d}x)\epsilon(\chi^{-1}, \psi, \mathbf{d}x) = q\chi(-1).$$

Proof. Applying the result of the proposition to χ and χ^{-1} leads to

$$\epsilon(\chi, \psi, \mathbf{d}x)\epsilon(\chi^{-1}, \psi, \mathbf{d}x) = G(\chi^{-1})G(\chi).$$

By standard properties of Gauss sums, we have $G(\chi^{-1}) = \chi(-1)\overline{G(\chi)}$. Using the fact that $|G(\chi)|^2 = q$ we obtain the desired result. □

1.1.3 Local L-factors

Given a prime q, let V denote the finite dimensional complex vector space associated with the Weil–Deligne representation σ'_q. Let V^{I_q} denote the subspace of vectors invariant under the action of inertia and let $V_{N_q}^{I_q} = V^{I_q} \cap \ker N_q$. Define the local L-factor at q to be

$$L(\sigma_q', s) = \det(1 - q^{-s}\Phi \mid V^{I_q}/V_{N_q}^{I_q})^{-1}.$$

We also define local L-factors (also known as gamma factors) at the archimedean places:

- Over $\mathbb{C}$, define $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$. If $\chi = z^{-N}\omega_t : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ for $N \in \mathbb{N}$ and $t \in \mathbb{C}$, then define

  $$L_{\mathbb{C}}(\chi, s) = \Gamma_{\mathbb{C}}(s+t).$$

  For any finite dimensional complex representation V of $\mathbb{C}^\times$, decompose it into a sum of quasi-characters $V = \bigoplus_i \chi_i$ and define

  $$L(V, s) = \prod_i L_{\mathbb{C}}(\chi_i, s).$$

- Over $\mathbb{R}$, define $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$. If $\chi = \operatorname{sign}^{-N}\omega_t : \mathbb{R}^\times \longrightarrow \mathbb{C}^\times$ for $N \in \{0,1\}$ and $t \in \mathbb{C}$, then define

  $$L_{\mathbb{R}}(\chi, s) = \Gamma_{\mathbb{R}}(s+t).$$

  For any finite dimensional complex representation V of $W(\mathbb{C}/\mathbb{R})$, decompose it into a sum of quasi-characters and induced characters in the Grothendieck group of representations of $W(\mathbb{C}/\mathbb{R})$, $[V] = \sum_i [\chi_i] + \sum_j [\operatorname{ind}_{\mathbb{C}/\mathbb{R}} \chi_j]$, and define

  $$L(V, s) = \prod_i L_{\mathbb{R}}(\chi_i, s) \prod_j L_{\mathbb{C}}(\chi_j).$$

1.1.4 Motivic L-functions

Suppose now that M is a pure motive over $\mathbb{Q}$. We refer to Section 1.4.2 below for the definition. Its ℓ-adic realisations give rise to a compatible family of ℓ-adic Galois representations by considering the Galois action on ℓ-adic étale cohomology. Given a prime q, choose a prime ℓ distinct from q and an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. Then the ℓ-adic representation gives rise to a Weil–Deligne representation $\sigma'_{M,q,\iota,\ell} = (\sigma_{M,q,\iota,\ell}, N_{M,q,\iota,\ell})$. A priori, this construction depends on ℓ and the embedding ι, but it can be shown that it is in fact independent of these choices. Hence we write $\sigma'_{M,q} = (\sigma_{M,q}, N_{M,q})$. One defines the L-function of the motive M by

$$L(M/\mathbb{Q}, s) := \prod_q L(\sigma'_{M,q}, s).$$

This function converges on some right half-plane $\Re(s) \gg 0$.

We can also consider the Betti realisation of M which is a pure rational Hodge structure of weight n for some $n \in \mathbb{N}$. For the sake of simplicity and because this is the case we will be interested in, let us assume that n is odd. Consider the Hodge decomposition

$$H_B(M) \otimes \mathbb{C} = \bigoplus_{p+q=n} H^{p,q}(M)$$

and let $h^{p,q}(M) = \dim_{\mathbb{C}} H^{p,q}(M)$ denote the corresponding Hodge numbers. For $p, q \in \mathbb{Z}$, consider the quasi-character $\varphi_{p,q} : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ given by $\varphi_{p,q}(z) = z^{-p}\bar{z}^{-q}$. Since n is odd, we have $\varphi_{p,q} \neq \varphi_{p,q} \circ c$ and thus $\operatorname{ind}_{\mathbb{C}/\mathbb{R}} \varphi_{p,q} = \operatorname{ind}_{\mathbb{C}/\mathbb{R}} \varphi_{q,p}$ is an irreducible representation of $W(\mathbb{C}/\mathbb{R})$. We define the Weil–Deligne representation of M at the infinite place by

$$\sigma'_{M,\infty} = \bigoplus_{\substack{p+q=n \\ p<q}} (\operatorname{ind}_{\mathbb{C}/\mathbb{R}} \varphi_{p,q}) \otimes H^{p,q}(M)$$

where $H^{p,q}(M)$ is given the trivial action. If $p < q$, then

$$\varphi_{p,q}(z) = \bar{z}^{-(q-p)}|z|^{-2p} = \bar{z}^{-(q-p)}\omega_{-p}(z).$$

It follows that the L-factor at infinity is given by

$$L(\sigma'_{M,\infty}, s) = \prod_{\substack{p+q=n \\ p<q}} L_{\mathbb{C}}(\varphi_{p,q}, s)^{h^{p,q}(M)} = \prod_{\substack{p+q=n \\ p<q}} \Gamma_{\mathbb{C}}(s-p)^{h^{p,q}(M)}.$$

One can now form the completed L-function of M

$$\Lambda(M/\mathbb{Q},s) := \prod_v L(\sigma'_{M,v},s) = L(\sigma'_{M,\infty},s)L(M/\mathbb{Q},s),$$

where the product runs over all places v of $\mathbb{Q}$.

The conductor of M is defined to be

$$\mathrm{cond}(M/\mathbb{Q}) := \prod_q q^{a(\sigma'_{M,q})} \in \mathbb{N} \tag{1.8}$$

where the product is over all finite places q.

Consider $\psi = \prod_v \psi_v : \mathbb{A}_\mathbb{Q}/\mathbb{Q} \longrightarrow \mathbb{C}$ an additive character of the adèles and let $\mathbf{d}x$ denote the normalised Haar measure on the adèles such that $\int_{\mathbb{A}_\mathbb{Q}/\mathbb{Q}} \mathbf{d}x = 1$. It decomposes as a product of local Haar measures $\mathbf{d}x_v$ which satisfy $\int_{\mathbb{Z}_v} \mathbf{d}x_v = 1$ for almost all finite places v. We can then define the global epsilon factor of M to be

$$\epsilon(M/\mathbb{Q}) = \prod_v \epsilon'(\sigma'_{M,v},\psi_v,\mathbf{d}x_v)$$

which is independent of the choice of ψ and $\mathbf{d}x$. Moreover, $\epsilon(\sigma'_{M,v},\psi_v,\mathbf{d}x_v) = 1$ for almost all v.

The global root number is similarly defined as

$$W(M/\mathbb{Q}) = \prod_v W(\sigma'_{M,v},\psi_v,\mathbf{d}x_v).$$

Conjecture 1.1. *The completed L-function $\Lambda^*(M/\mathbb{Q},s) := \mathrm{cond}(M/\mathbb{Q})^{\frac{s}{2}}\Lambda(M/\mathbb{Q},s)$ can be continued meromorphically to the whole complex plane and satisfies the functional equation*

$$\Lambda^*(M/\mathbb{Q},s) = W(M/\mathbb{Q})\Lambda^*(M^\vee/\mathbb{Q},1-s) \tag{1.9}$$

where $M^\vee$ is the dual of the motive M.

1.2 Elliptic curves and modular forms

We review the necessary background on elliptic curves and modular forms. In particular, we cover the Modularity Theorem relating elliptic curves over $\mathbb{Q}$ with cusp forms of weight 2 for $\Gamma_0(N)$. Concerning modular forms on $\Gamma_1(N)$, we recall that the space of cusp forms of weight ≥ 2 can be realised inside the de Rham cohomology of suitable Kuga–Sato varieties.

1.2.1 Elliptic curves

An elliptic curve over a scheme S is a proper smooth morphism $E \longrightarrow S$, whose geometric fibres are connected curves of genus 1, together with a section $e : S \longrightarrow E$. In particular, an elliptic curve over a field K, i.e., over $\mathrm{Spec}(K)$, is a smooth proper curve over K of genus 1, together with a prescribed K-rational point $O_E \in E(K)$. Consequently, an elliptic curve over a scheme S can be seen as a family of (classic) elliptic curves defined over fields parametrised by the scheme S.

Any smooth proper curve is projective, and thus an elliptic curve E/K is a smooth projective curve of genus 1 with a K-rational point. The Riemann–Roch theorem [139, Theorem 5.4] implies that any such curve is isomorphic to a smooth plane projective curve given by a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.10}$$

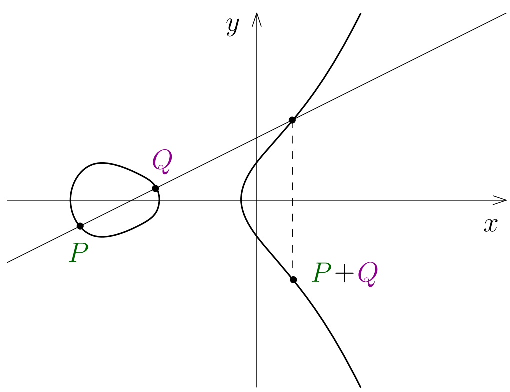
with coefficients $a_1, \dots, a_6 \in K$ satisfying the smoothness criterion that the discriminant $\Delta(a_1, \dots, a_6)$ is non-zero. See [139, §III.1]. This isomorphism maps the point $O_E \in E(K)$ to the point at infinity $[0, 1, 0] \in \mathbb{P}_2$.

Commutative group scheme structure

An elliptic curve $p : E \longrightarrow S$ has a natural structure of commutative group scheme over S as explained in [100]. Any point $P \in E(S)$, i.e., a section $P : S \longrightarrow E$, determines an effective

Cartier divisor on E with sheaf of ideals denoted $I(P)$. Let $I^{-1}(P)$ denote the inverse of this ideal sheaf as an invertible $\mathcal{O}_E$-module. For any S-scheme T, there is a bijection $E(T) \longrightarrow \mathrm{Pic}^0_{E/S}(T)$ given by sending a point $P \in E(T) = E_T(T)$ to the invertible $\mathcal{O}_{E_T}$-module $I^{-1}(P) \otimes I(e_T)$, where e_T denotes the base change of the trivial section e to T. Here $\mathrm{Pic}^0_{E/S}(T)$ denotes the abelian group of isomorphism classes of degree 0 invertible sheaves on E_T modulo the subgroup of those of the form $p_T^*(\mathcal{L})$, where $\mathcal{L}$ any invertible sheaf on T. By transfer of group structure, E/S represents a functor from S-schemes to the category of abelian groups, hence acquires the structure of a commutative group scheme over S.

When $S = \mathrm{Spec}(K)$, the natural bijection $E \simeq \mathrm{Pic}^0_{E/K}$ is given by mapping a point P to the divisor class of $(P) - (O_E)$ and identifies E with its Jacobian. If E is described in the projective plane by a Weierstrass equation, the classic geometric chord-and-tangent recipe endows E with the structure of an algebraic group, as illustrated in the following figure:



These two group structures, the one coming the Jacobian of E and the other coming from the description of E as a plane projective curve, coincide.

In this thesis, we will mostly focus on elliptic curves defined over a number field K, in which case the Mordell–Weil theorem asserts that the abelian group $E(K)$ is finitely generated. As a consequence, there is an isomorphism

$$E(K) \simeq E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^{r_{\mathrm{alg}}(E/K)}, \tag{1.11}$$

where $E(K)_{\mathrm{tors}}$ denotes the finite subgroup of torsion points and $r_{\mathrm{alg}}(E/K) \in \mathbb{Z}_{\geq 0}$ is the algebraic rank of E, also referred to as the Mordell–Weil rank of E.

The Weil–Deligne representations of an elliptic curve

Let E be an elliptic curve defined over $\mathbb{Q}$. Associated to E is a family of compatible 2-dimensional ℓ-adic Galois representations $\rho_{E,\ell}$ for each prime ℓ coming from the ℓ-adic étale cohomology groups $H^1_{\text{et}}(\bar{E}, \mathbb{Q}_\ell)$. This is the contragredient of the representation arising from the action of the Galois group on the ℓ-adic Tate module

$$V_\ell(E) := \varprojlim E[\ell^n](\bar{\mathbb{Q}}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let q be a prime, ℓ a prime distinct from q, and choose an embedding $\iota_\ell : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. Following [126, §4], one may associate to $\rho_{E,\ell}$ a complex representation $\sigma'_{E,\ell,\iota_\ell,q} = (\sigma_{E,\ell,\iota_\ell,q}, N_{E,\ell,\iota_\ell,q})$ of the Weil–Deligne group $W'(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$. It turns out that the isomorphism class of the Weil–Deligne representation $\sigma'_{E,\ell,\iota_\ell,q}$ is independent of ℓ and ι_ℓ, as follows from the two propositions below, and we shall simply write $\sigma'_{E,q} = (\sigma_{E,q}, N_{E,q})$. This is the Weil–Deligne representation of E at q.

Proposition 1.3. *If E has potential good reduction at q, then $N_{E,q} = 0$ and $\sigma_{E,q}$ is semisimple. Furthermore, E has good reduction if and only if $\sigma_{E,q}$ is unramified, in which case*

$$\sigma_{E,q} \simeq \xi_q \oplus \xi_q^{-1}\omega_q^{-1}$$

for some unramified character ξ_q. Here ω_q is the Weil–Deligne representation of the ℓ-adic cyclotomic character of Definition 1.2 and Example 1.1.

Proof. This is [126, §14 Proposition]. □

Definition 1.5. Let (e_0, e_1) denote the standard basis of $\mathbb{C}^2$. The special representation of the Weil–Deligne group at q of dimension 2, denoted $\mathrm{sp}(2)$, is the representation (σ_q, N)

defined by the matrices

$$\sigma_q := \begin{pmatrix} 1 & 0 \\ 0 & \omega_q \end{pmatrix} \qquad \text{and} \qquad N := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

It is an admissible, indecomposable, reducible 2-dimensional representation of $W'(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$.

Proposition 1.4. *Suppose that E has potential multiplicative reduction at q and let λ be a character of $W(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ such that $\lambda^2 = 1$ and the twist E^λ of E by λ has split multiplicative reduction at q. Then*

$$\sigma'_{E,q} \simeq \lambda\omega_q^{-1} \otimes \mathrm{sp}(2),$$

so that, in particular, $N_{E,q} \neq 0$ and $\sigma'_{E,q}$ is ramified. Moreover, λ is trivial, unramified but nontrivial, or ramified according as E has split multiplicative, non-split multiplicative reduction, or additive reduction at q.

Proof. This is [126, §15 Proposition]. □

Finally, we describe the Weil–Deligne representation of E at the infinite place. The rational Hodge structure $H^1_B(E(\mathbb{C}), \mathbb{Q})$ is of weight 1 and admits the Hodge decomposition

$$H^1_B(E(\mathbb{C}), \mathbb{C}) = H^{1,0}(E) \oplus H^{0,1}(E)$$

with Hodge numbers $h^{1,0}(E) = h^{0,1}(E) = 1$. Therefore the Weil–Deligne representation at infinity is given by

$$\sigma'_{E,\infty} = \mathrm{ind}_{\mathbb{C}/\mathbb{R}}\, \varphi_{0,1} \otimes H^{0,1}(E). \tag{1.12}$$

The root number of an elliptic curve

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Having described the Weil–Deligne representations of E, one can define the global root number $W(E/\mathbb{Q})$ following Section 1.1.4.

Remark 1.2. Note that for finite primes q, the Weil–Deligne representation $\sigma'_{E,q} \otimes \omega_q^{1/2}$ is symplectic due to the existence of the Weil pairing for elliptic curves. In other words, $\sigma'_{E,q}$ is essentially symplectic of weight 1. By Remark 1.1, the local root number $W(\sigma'_{E,q})$ belongs to $\{\pm 1\}$ and does not depend on the choice of additive characters or Haar measures. In particular, the global root number of E belongs to $\{\pm 1\}$.

We proceed to compute $W(E/\mathbb{Q})$ in the case where the conductor N is square-free; E admits good reduction at all primes not dividing N, and either split or non-split multiplicative reduction at the primes dividing N. For primes $p \mid N$, we define

$$a_p(E) = \begin{cases} +1 & \text{if } E \text{ admits split multiplicative reduction at } p \\ -1 & \text{if } E \text{ admits non-split multiplicative reduction at } p. \end{cases} \tag{1.13}$$

Proposition 1.5. *Suppose that the conductor N of E is square-free. The local root numbers of E are given by the following:*

$$\begin{cases} W(\sigma'_{E,q}) = 1, & \textit{for } q \nmid N \\ W(\sigma'_{E,p}) = -a_p(E), & \textit{for } p \mid N \\ W(\sigma'_{E,\infty}) = -1. \end{cases}$$

In particular, the global root number is given by

$$W(E/\mathbb{Q}) = -(-1)^{\omega(N)} \prod_{p \mid N} a_p(E),$$

where $\omega(N)$ denote the number of distinct prime divisors of N.

Remark 1.3. For the general case, we refer to [126, §19 Proposition]. We choose to include a detailed proof here as the local epsilon factor computations will be useful when dealing with more difficult situations as in Section 4.4. Moreover, this is a nice concrete application of the theory outlined in Section 1.1. Note that $W(E/\mathbb{Q})$ is the negative of the eigenvalue of the Atkin–Lehner [3] operator w_N acting on the newform in $S_2(\Gamma_0(N))$ associated to E. See Section 1.2.3.

Proof. Let q denote a prime not dividing N and choose an additive character ψ_q of $\mathbb{Q}_q$ with $n(\psi_q) = 0$ as well as the Haar measure $\mathbf{d}x_q$ on $\mathbb{Q}_q$ normalised such that $\int_{\mathbb{Z}_q} \mathbf{d}x_q = 1$. By Proposition 1.3, the Weil–Deligne representation of E at q is given by

$$\sigma'_{E,q} = \sigma_{E,q} \simeq \xi_q \oplus \xi_q^{-1}\omega_q^{-1}$$

for some unramified character ξ_q. In particular, since $N_{E,q} = 0$, we have

$$\epsilon'(\sigma'_{E,q}, \psi_q, \mathbf{d}x_q) = \epsilon(\sigma_{E,q}, \psi_q, \mathbf{d}x_q)$$

and by Theorem 1.1 *i*) we find that

$$\epsilon(\sigma_{E,q}, \psi_q, \mathbf{d}x_q) = \epsilon(\xi_q, \psi_q, \mathbf{d}x_q)\epsilon(\xi_q^{-1}\omega_q^{-1}, \psi_q, \mathbf{d}x_q).$$

By Proposition 1.1 applied to the unramified characters ξ_q and $\xi_q^{-1}\omega_q^{-1}$, we find that

$$\epsilon(\sigma_{E,q}, \psi_q, \mathbf{d}x_q) = \xi_q\xi_q^{-1}\omega_q^{-1}(q)^{n(\psi_q)+a(1)}\epsilon(1, \psi_q, \mathbf{d}x_q)^2.$$

But $n(\psi_q) = 0$ and the trivial character is unramified so $a(1) = 0$. Moreover, $\epsilon(1, \psi_q, \mathbf{d}x_q) = 1$ by (1.7) and the normalisation of the Haar measure. It follows that $W(\sigma'_{E,q}) = 1$.

We now deal with the local root number at a prime $p \mid N$. Choose an additive character ψ_p of $\mathbb{Q}_p$ with $n(\psi_p) = 0$ as well as the Haar measure $\mathbf{d}x_p$ on $\mathbb{Q}_p$ normalised such that $\int_{\mathbb{Z}_p} \mathbf{d}x_p = 1$. Let λ_p be an unramified character of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\lambda_p^2 = 1$ and the twist E^{λ_p} of E by λ_p has split multiplicative reduction at p. By Proposition 1.4 we have

$$\sigma'_{E,p} \simeq \lambda_p\omega_p^{-1} \otimes \mathrm{sp}(2).$$

Let $V = \mathbb{C}(\lambda_p \omega_p^{-1}) \otimes \mathbb{C}^2$ denote the complex vector space associated to this representation. Let (e_0, e_1) denote the standard basis of $\mathbb{C}^2$ as in Definition 1.5. Since the characters λ_p and ω_p are unramified, we have $V^{I_p} = V$ and thus $V_{N_{E,p}}^{I_p} = \ker N_{E,p} = \mathbb{C}e_1$ and $V^{I_p}/V_{N_{E,p}}^{I_p} = \mathbb{C}e_0$. We deduce that

$$\delta(\sigma'_{E,p}) = \det(-\Phi \mid \mathbb{C}e_0) = -\lambda_p(\Phi)p$$

since $\sigma'_{E,p}$ acts as $\lambda_p \omega_p^{-1}$ on e_0 and $\omega_p^{-1}(\Phi) = p$. So far, we see that

$$\epsilon'(\sigma'_{E,p}, \psi_p, \mathbf{d}x_p) = -\lambda_p(\Phi)p \cdot \epsilon(\sigma_{E,p}, \psi_p, \mathbf{d}x_p).$$

However, $\sigma_{E,p} = \lambda_p \omega_p^{-1} \oplus \lambda_p$ and thus, by Theorem 1.1 *i)* and (1.7), we have

$$\epsilon(\sigma_{E,p}, \psi_p, \mathbf{d}x_p) = \epsilon(\lambda_p \omega_p^{-1}, \psi_p, \mathbf{d}x_p)\epsilon(\lambda_p, \psi_p, \mathbf{d}x_p) = 1.$$

In conclusion, we have established that $\epsilon'(\sigma'_{E,p}, \psi_p, \mathbf{d}x_p) = -\lambda_p(\Phi)p$. Note that the quadratic character λ_p is trivial or non-trivial, i.e., $\lambda_p(\Phi) = +1$ or -1, according as E has split or non-split multiplicative reduction at p. In other words, we have $\lambda_p(\Phi) = a_p(E)$, and we have proved that $W(\sigma'_{E,p}) = -a_p(E)$.

Finally, we take care of the infinite place. Recall from (1.12) that

$$\sigma'_{E,\infty} = \operatorname{ind}_{\mathbb{C}/\mathbb{R}} \varphi_{0,1} : W(\mathbb{C}/\mathbb{R}) \longrightarrow \mathbf{GL}_2(\mathbb{C}).$$

By Theorem 1.1 *ii)* we have

$$\epsilon(\sigma'_{E,\infty}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = \epsilon(\varphi_{0,1}, \psi_{\mathbb{C}}, \mathbf{d}x_{\mathbb{C}}) \frac{\epsilon(\operatorname{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}})}{\epsilon(1_{\mathbb{C}}, \psi_{\mathbb{C}}, \mathbf{d}x_{\mathbb{C}})}.$$

A set of representatives for the left cosets $W(\mathbb{C}/\mathbb{R})/W(\mathbb{C}/\mathbb{C})$ is given by $\{1, J\}$. The induced representation $\operatorname{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}$ is the permutation representation associated to this set. If we let (e_1, e_J) denote a basis for the space of $\operatorname{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}$, then $\alpha \in W(\mathbb{C}/\mathbb{R})$ maps e_1 to e_α and e_J

to $e_{\alpha \cdot J}$. If α belongs to $J^N\mathbb{C}^\times$ with $N \in \{0,1\}$, then α acts on $\mathbb{C}e_1 \oplus \mathbb{C}e_J$ via the matrix $\left(\begin{smallmatrix} 1-N & N \\ N & 1-N \end{smallmatrix}\right)$. By conjugating with respect to the matrix $\left(\begin{smallmatrix} 1 & 1 \\ -1/2 & 1/2 \end{smallmatrix}\right)$ we obtain the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mathrm{sign} \end{smallmatrix}\right)$. We conclude that $\mathrm{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}} = 1_{\mathbb{R}} \oplus \mathrm{sign}$, and by Theorem 1.1 i), we have

$$\epsilon(\mathrm{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = \epsilon(1_{\mathbb{R}}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}})\epsilon(\mathrm{sign}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}).$$

Finally, using the defining formulas (1.5) and (1.6), we obtain

$$\epsilon(\sigma'_{E,\infty}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = i\frac{1 \cdot i}{1} = i^2 = -1.$$

□

Remark 1.4. In the course of the proof, we have seen that for primes $p \mid N$,

$$a(\sigma'_{E,p}) = a(\sigma_{E,p}) + \dim V^{I_p}/V^{I_p}_{N_{E,p}} = 1$$

since $\sigma_{E,p}$ is unramified. At primes q not dividing N, $\sigma'_{E,q}$ is unramified and thus $a'(\sigma'_{E,q}) = 0$. In particular, we recover the fact that $\mathrm{cond}(E/\mathbb{Q}) = \prod_\ell \ell^{a'(\sigma'_{E,\ell})} = N$.

The L-function of an elliptic curve

Recall from Section 1.1.3 that for each finite prime q, the local L-factor associated to the Weil–Deligne representation of E is

$$L(\sigma'_{E,q}, s) = \det(1 - q^{-s}\Phi \mid V^{I_q}_{q,N_{E,q}})^{-1}$$

where V_q is the underlying complex vector space of $\sigma'_{E,q}$ and $V^{I_q}_{q,N_{E,q}} := V_q^{I_q} \cap \ker N_{E,q}$.

At the infinite prime, we have

$$L(\sigma'_{E,\infty}, s) = L_{\mathbb{C}}(\varphi_{0,1}, s)^{h^{0,1}(E)} = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Having described the Weil–Deligne representations of E at the finite places in Propositions 1.3 and 1.4, one can work out explicit formulas for the corresponding local L-factors, as done in [126, §17 Proposition]. We content ourselves with stating the formulas. We have

$$\Lambda(E/\mathbb{Q}, s) = \prod_v L(\sigma'_{E,v}, s) = 2(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s)$$

where v runs over all places and $L(E/\mathbb{Q}, s)$ denotes the Hasse–Weil L-function. If N denotes the conductor of E, then we have the explicit formula

$$L(E/\mathbb{Q}, s) = \prod_{p\nmid N}(1 - a_p(E)p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p(E)p^{-s})^{-1} \tag{1.14}$$

where

$$a_p(E) = \begin{cases} p + 1 - |E(\mathbb{F}_p)| & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

It can be shown to converge absolutely on the right half-plane $\Re(s) > 3/2$.

We have $\mathrm{cond}(E/\mathbb{Q}) = N$ and

$$\Lambda^*(E/\mathbb{Q}, s) := N^{\frac{s}{2}} 2(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s).$$

For ℓ a prime, the dual of $H^1_{\text{et}}(\bar{E}, \mathbb{Q}_\ell)$ is $H^1_{\text{et}}(\bar{E}, \mathbb{Q}_\ell)(1) = H^1_{\text{et}}(\bar{E}, \mathbb{Q}_\ell) \otimes \omega_{\text{cyc},\ell}$. It follows that $\Lambda^*(E^\vee/\mathbb{Q}, s) = \Lambda^*(E/\mathbb{Q}, s + 1)$, and thus the conjectural functional equation (1.9) for $\Lambda^*(E/\mathbb{Q}, s)$ reads

$$\Lambda^*(E/\mathbb{Q}, s) = W(E/\mathbb{Q})\Lambda^*(E/\mathbb{Q}, 2 - s). \tag{1.15}$$

This conjecture is a corollary of the Modularity Theorem as we will explain in Section 1.2.3.

Remark 1.5. One can also define the Hasse–Weil L-function of an elliptic curve defined over more general number fields and describe its local factors explicitly. We content ourselves with the description given over $\mathbb{Q}$ for the purposes of this thesis.

The Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve defined over a number field K. The famous conjecture of Birch and Swinnerton-Dyer, now one of the Clay Millennium Prize Problems, relates the algebraic rank $r_{\mathrm{alg}}(E/K)$ to the behaviour of the Hasse–Weil L-function of the curve.

Conjecture 1.2 (Birch–Swinnerton-Dyer)**.** *Let E be an elliptic curve over a number field K. The Hasse–Weil L-function $L(E/K,s)$ admits analytic continuation to the whole complex plane via a functional equation centred at $s=1$, and the rank $r_{\mathrm{alg}}(E/K) := \mathrm{rank}_{\mathbb{Z}}(E(K))$ is given by $r_{\mathrm{alg}}(E/K) = \mathrm{ord}_{s=1} L(E/K,s)$.*

By the pioneering work of Wiles [153], Taylor and Wiles [145], and Breuil, Conrad, Diamond and Taylor [31], it is known, for $K=\mathbb{Q}$, that $L(E/\mathbb{Q},s)$ admits analytic continuation and a functional equation centred at $s=1$. The most significant progress to date towards the Birch and Swinnerton-Dyer conjecture is due to the method of Gross, Zagier and Kolyvagin [75,78,103], which rests on the construction of Heegner points, and yields the implication

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q},s) \in \{0,1\} \implies r_{\mathrm{alg}}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q},s). \tag{1.16}$$

Their strategy has been generalised to the case of totally real number fields by S. Zhang [156]. The work of Skinner and Urban [140,141], uses p-adic methods, and more specifically Iwasawa theory, to produce the first instances of the opposite implication (3). The Birch and Swinnerton-Dyer conjecture remains open in higher rank situations, as well as for elliptic curves over general number fields in any rank. More details about this can be found in Section 0.2.1.

1.2.2 Modular curves

We recall the definitions and introduce the notation for the various modular curves that we will be working with. Throughout we fix an integer $N \geq 3$ and work with level N structures. For more details we refer to [59, 98].

$\Gamma(N)$-level structure

Let $\bar{M}_N$ denote the fine moduli scheme representing pairs (E, α_N) consisting of a generalised elliptic curve E over a $\mathbb{Z}[1/N]$-scheme S together with a full level N structure, that is, an isomorphism $\alpha_N : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})_S$ of group schemes over S. The scheme $\bar{M}_N$ is a smooth proper curve over $\mathbb{Z}[1/N]$ and we will mostly work with its base-change to $\mathbb{Q}$ which we, by abuse of notation, denote again by $\bar{M}_N$. Let ζ_N denote a choice of a primitive N-th root of unity. The base-change $\bar{M}_N \otimes \mathbb{Q}(\zeta_N)$ of this curve to the cyclotomic extension $\mathbb{Q}(\zeta_N)$ is the disjoint union of $\varphi(N)$ geometrically connected smooth proper curves $X^n(N)$ over $\mathbb{Q}(\zeta_N)$ indexed by $n \in (\mathbb{Z}/N\mathbb{Z})^\times$. The curve $X^n(N)$ is the fine moduli scheme classifying pairs $(E, (P, Q))$ consisting of a generalised elliptic curve over a $\mathbb{Q}(\zeta_N)$-scheme S together with the choice of a basis $\{P, Q\}$ for the N-torsion group $E[N]$ satisfying $e_N(P, Q) = \zeta_N^n$, where e_N denotes the Weil pairing on the N-torsion. We will often write $X(N)$ for the curve $X^1(N)$. Taking ζ_N to be $e^{\frac{2\pi i}{N}}$ over $\mathbb{C}$, there is a uniformisation of $X(N)$ by the extended complex upper half-plane $\mathcal{H}^*$ given by

$$\mathcal{H}^* \longrightarrow X(N)(\mathbb{C}), \qquad \tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, (1/N + \mathbb{Z} \oplus \tau\mathbb{Z}, \tau/N + \mathbb{Z} \oplus \tau\mathbb{Z}))$$

which identifies $X(N)(\mathbb{C})$ with the quotient $\Gamma(N) \setminus \mathcal{H}^*$ where $\Gamma(N)$ denotes the full level N congruence subgroup of $\mathbf{SL}_2(\mathbb{Z})$ acting on $\mathcal{H}^*$ by Möbius transformations. More precisely,

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

There is a natural projection map $X(N) \longrightarrow \mathbf{SL}_2(\mathbb{Z}) \setminus \mathcal{H}^*$ over $\mathbb{C}$ which has degree equal to $\frac{N^3}{2} \prod_{p|N}(1-\frac{1}{p^2})$.

When $N = p$ is prime, the curve $X(p)$ has $\frac{p^2-1}{2}$ cusps and its genus is given by

$$g(X(p)) = 1 + \frac{(p^2-1)(p-6)}{24} \qquad \text{for } p > 2 \qquad \text{and} \qquad g(X(2)) = 0.$$

$\Gamma_1(N)$-level structure

If $N \geq 5$, let $X_1(N)$ denote the fine moduli scheme representing pairs (E, P) consisting of a generalised elliptic curve E over a $\mathbb{Q}$-scheme S together with the choice of a point P on E of exact order N. Then $X_1(N)$ is a geometrically connected smooth proper curve over $\mathbb{Q}$. It admits a uniformisation by the extended complex upper half-plane given by

$$\mathcal{H}^* \longrightarrow X(N)(\mathbb{C}), \qquad \tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, 1/N + \mathbb{Z} \oplus \tau\mathbb{Z})$$

which identifies $X_1(N)(\mathbb{C})$ with the quotient $\Gamma_1(N) \setminus \mathcal{H}^*$ where $\Gamma_1(N) \subset \mathbf{SL}_2(\mathbb{Z})$ is the congruence subgroup defined by

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}. \tag{1.17}$$

There is a natural projection map $X(N) \longrightarrow X_1(N)$ over $\mathbb{C}$ of degree N.

When $N = p$ is prime, the curve $X_1(p)$ has $p-1$ cusps and its genus is given by

$$g(X_1(p)) = 1 + \frac{(p-1)(p-11)}{24} \qquad \text{for } p > 3 \qquad \text{and} \qquad g(X_1(2)) = g(X_1(3)) = 0.$$

$\Gamma_0(N)$-level structure

If $N \geq 5$, let $X_0(N)$ denote the coarse moduli scheme representing pairs (E, H) consisting of a generalised elliptic curve E defined over a $\mathbb{Q}$-scheme S together with a cyclic subgroup scheme H of order N. Then $X_0(N)$ is a geometrically connected smooth proper curve over $\mathbb{Q}$. It admits a uniformisation by the extended complex upper half-plane given by

$$\mathcal{H}^* \longrightarrow X_0(N)(\mathbb{C}), \qquad \tau \mapsto (\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, \langle 1/N + \mathbb{Z} \oplus \tau\mathbb{Z} \rangle)$$

which identifies $X_0(N)(\mathbb{C})$ with the quotient $\Gamma_0(N) \setminus \mathcal{H}^*$ where $\Gamma_0(N) \subset \mathbf{SL}_2(\mathbb{Z})$ is the congruence subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}.$$

The natural projection $X_1(N) \longrightarrow X_0(N)$ over $\mathbb{C}$ descends to a morphism of curves over $\mathbb{Q}$ and has degree $\frac{\varphi(N)}{2} = [\Gamma_0(N) : \pm\Gamma_1(N)]$. In fact, $X_0(N)$ classifies elliptic curves with $\Gamma_0(N)$-structures up to isomorphism. Hence the two distinct elements (E, P) and $(E, -P)$ of $X_1(N)$ both map to $(E, \langle P \rangle)$ of $X_0(N)$, as $[-1] : (E, \langle P \rangle) \simeq (E, \langle -P \rangle)$ is an automorphism of elliptic curves with $\Gamma_0(N)$-structure.

When $N = p$ is prime, the curve $X_0(p)$ has two cusps ξ_∞ and ξ_0 corresponding via the complex uniformisation to the points $i\infty$ and 0 respectively. The genus of $X_0(p)$ is given by the formula

$$g(X_0(p)) = \begin{cases} \lfloor \frac{p+1}{12} \rfloor - 1 & \text{if } p \equiv 1 \pmod{12} \\ \lfloor \frac{p+1}{12} \rfloor & \text{otherwise.} \end{cases} \tag{1.18}$$

1.2.3 Weight 2 modular forms of level $\Gamma_0(N)$

A modular form of weight 2 for the congruence subgroup $\Gamma_0(N)$ is a holomorphic function on the complex upper half-plane $f : \mathcal{H} \longrightarrow \mathbb{C}$ satisfying the transformation property

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau), \qquad \forall \tau \in \mathcal{H}, \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

and which is holomorphic at the cusps of $X_0(N)$. The space of such modular forms is denoted $M_2(\Gamma_0(N))$. Note that $\Gamma_0(N)$ contains the matrix $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so that we have $f(\tau+1) = f(\tau)$ for all $\tau \in \mathcal{H}$. It follows that f admits a Fourier expansion around the cusp at infinity

$$f(q) = \sum_{n \geq 0} a_n(f) q^n, \qquad q = e^{2\pi i \tau}.$$

In fact, f admits a Fourier expansion around each cusp, and if the constant term of all these expansions is zero, we say that f is a cusp form. We denote by $S_2(\Gamma_0(N))$ the subspace of cusp forms of weight 2 and level $\Gamma_0(N)$. One can identify $S_2(\Gamma_0(N))$ with the space of global sections of the sheaf of regular differential 1-forms on the modular curve $X_0(N)$

$$S_2(\Gamma_0(N)) \xrightarrow{\sim} H^0(X_0(N), \Omega^1_{X_0(N)}), \qquad f \mapsto \omega_f := 2\pi i f(\tau) d\tau. \tag{1.19}$$

In particular, the dimension of $S_2(\Gamma_0(N))$ is equal to the genus of $X_0(N)$. Let K_f be the field generated by the Fourier coefficients of the cuspform f. As $X_0(N)$ admits a rational structure as an algebraic curve over $\mathbb{Q}$, the space of differential 1-forms admits a basis consisting of differentials defined over $\mathbb{Q}$. By (1.19), the space $S_2(\Gamma_0(N))$ similarly admits a basis of cuspforms defined over $\mathbb{Q}$, i.e., with Fourier coefficients in $\mathbb{Q}$. It follows that the extension $K_f/\mathbb{Q}$ is finite. We will denote by d_f the degree of this extension.

Hecke operators

The curve $X_0(N)$ is equipped with a collection of Hecke correspondences, which act on cohomology and give rise to operators on $S_2(\Gamma_0(N))$ via (1.19). These correspondences and their induced operators are traditionally denoted by T_n for integers $n \geq 1$ coprime to the level N, and by U_q for primes q that divide N. Defining formulas for these operators on the Fourier expansions of cusp forms can be found in [3, (3.1)]. For integers $d \parallel N$, there are Atkin–Lehner operators w_d acting on $S_2(\Gamma_0(N))$. See [3, p. 138] for their definition. The operators T_m with $(m, N) = 1$ commute with the operators T_n, U_q and w_d, but the operators

U_q and w_d do not commute with each other. See for instance [3, Lemma 17].

Let $\mathbb{T} := \mathbb{T}(N)$ denote the full commutative Hecke $\mathbb{Q}$-algebra generated by the Hecke operators T_n with $(n, N) = 1$ and U_q with $q \mid N$ acting on $S_2(\Gamma_0(N))$. Let $\mathbb{T}_0 := \mathbb{T}_0(N)$ denote the subalgebra generated only by the operators T_n with $(n, N) = 1$. The space of cusp forms $S_2(\Gamma_0(N))$ admits a basis of eigenfunctions for $\mathbb{T}_0$. Essentially, the operators T_n commute and are Hermitian with respect to the Petersson inner product [3, (1.3)], and they can therefore be simultaneously diagonalised. For the full proof we refer to [3, Theorem 2] which is attributed to Hecke and Petersson. We refer to eigenfunctions for $\mathbb{T}_0$ as eigenforms.

There is a theory of oldforms and newforms developed in [3, §4]. Briefly, oldforms are elements of $S_2(\Gamma_0(N))$ that arise from modular forms in $S_2(\Gamma_0(d))$ for $d \mid N$. The space $S_2(\Gamma_0(N))^{\text{new}}$ is the orthogonal complement of the space of oldforms with respect to the Petersson inner product. As in the previous paragraph, $S_2(\Gamma_0(N))^{\text{new}}$ also admits a basis consisting of eigenforms for $\mathbb{T}_0$. Such a basis element will be called a newform. The first Fourier coefficient of a newform f is necessarily nonzero by [3, Lemma 19] and such forms can thus be rescaled so that $a_1(f) = 1$. A newform f with the property that $a_1(f) = 1$ is called a normalised newform. Normalised newforms satisfy the theorem of mulitplicity one [3, Lemmas 20 and 21]: any two normalised newforms that have the same eigenvalues for the operators T_p with $p \nmid N$ must be equal, and any form in $S_2(\Gamma_0(N))^{\text{new}}$ which is an eigenform for $\mathbb{T}_0$ is a constant multiple of some normalised newform. Note that a normalised newform is also an eigenvector for the Atkin–Lehner involutions w_d with $d \| N$: indeed, $w_d(f) \in S_2(\Gamma_0(N))^{\text{new}}$ and by commutativity of w_d with the operators T_p for $p \nmid N$, $w_d(f)$ and f share the same eigenvalues for T_p. By multiplicity one, we necessarily have $w_d(f) = \lambda(d) f$. Moreover, since w_d is an involution, we have $\lambda(d) \in \{\pm 1\}$. More is true, as $U_q(f) = a_q(f) f$ for any prime $q \mid N$. Let $d = q^\alpha \| N$ with q prime. If $\alpha \geq 2$, then $U_q(f) = 0$ and in particular $a_q(f) = 0$. If $\alpha = 1$, it is possible to read off the Atkin–Lehner eigenvalue $\lambda(q)$ from the Fourier coefficient $a_q(f)$: indeed, $\lambda(q) = -a_q(f)$, and in particular $a_q(f) \in \{\pm 1\}$. This follows from the fact that in this case $U_q(f) + w_q(f)$ is an oldform [3, Lemma 17 (iii)]. The detailed proofs of these facts along with additional basic properties of newforms can be found in [3, Theorem 3].

Eichler–Shimura theory

The Eichler–Shimura construction [64, 135] associates to the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugacy class $[f]$ of any normalised newform $f \in S_2(\Gamma_0(N))$ a simple abelian variety $A_{[f]}$ defined over $\mathbb{Q}$ as a quotient of $J_0(N) := \mathrm{Pic}^0_{X_0(N)/\mathbb{Q}}$, the Jacobian of $X_0(N)$. The quotient map $J_0(N) \longrightarrow A_{[f]}$ is defined over $\mathbb{Q}$ and its kernel is stable under the action of $\mathbb{T}_0(N)$. Moreover, we have $\mathrm{End}_{\mathbb{Q}}(A_{[f]}) \otimes \mathbb{Q} = K_f$ and the dimension of A_f is $d_f = [K_f : \mathbb{Q}]$. The association $[f] \mapsto A_{[f]}$ is unique up to isogeny.

In particular, if f is a normalised newform in $S_2(\Gamma_0(N))$ with Fourier coeffecients in $\mathbb{Q}$, then the Eichler–Shimura construction associates to f and elliptic curve E_f over $\mathbb{Q}$ (up to isogeny), which is a quotient of $J_0(N)$. The association is such that we have an equality of L-functions $L(f, s) = L(E_f/\mathbb{Q}, s)$, where

$$L(f, s) := \sum_{n \geq 1} \frac{a_n(f)}{n^s}$$

is the L-function associated to f, and $L(E_f/\mathbb{Q}, s)$ is the Hasse–Weil L-function (1.14) of E_f.

The Modularity Theorem

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. The Modularity Theorem [31, 145, 153] is a converse to the Eichler–Shimura construction; it associates to E a normalised newform $f \in S_2(\Gamma_0(N))$ such that

$$L(E/\mathbb{Q}, s) = L(f, s).$$

As a consequence, $L(E/\mathbb{Q}, s)$ admits analytic continuation to the whole complex plane and satisfies a functional equation centred at $s = 1$. These analytic properties of the Hasse–Weil L-function were not known before the proof of the Modularity Theorem.

By the Eichler–Shimura construction, there is an elliptic curve E_f, which is a quotient of $J_0(N)$ and satisfies $L(f,s) = L(E_f/\mathbb{Q}, s)$, hence we obtain the equality of L-functions

$$L(E/\mathbb{Q}, s) = L(E_f/\mathbb{Q}, s).$$

By Faltings' proof of the Tate conjecture for abelian varieties defined over number fields, this equality implies that the elliptic curves E and E_f are isogenous. Since E_f arises as a quotient of $J_0(N)$, we deduce that there exists a non-constant morphism of abelian varieties over $\mathbb{Q}$

$$\pi_E : J_0(N) \longrightarrow E. \tag{1.20}$$

By fixing an embedding of $X_0(N)$ into its Jacobian using the base point ξ_∞, we obtain a non-constant morphism of algebraic curves over $\mathbb{Q}$

$$\pi_E : X_0(N) \longrightarrow E, \tag{1.21}$$

which we still denote by π_E, by slight abuse of notation. Any of the two morphisms (1.20) and (1.21) will be called a modular parametrisation of E. Note that the existence of a modular parametrisation of E is equivalent to the Modularity Theorem.

There is a unique invariant differential ω of E such that $\pi_E^*(\omega) = \omega_f := 2\pi i f(z)dz$. Write $\omega = c\omega_E$, where ω_E is a Néron differential of E. Then c is an integer known as the Manin constant of the modular parametrisation π_E.

1.2.4 Higher weight modular forms for $\Gamma_1(N)$

This section is derived from [11, §3]. Let $N \geq 5$ and consider the open modular curve $Y_1(N)$ which is the fine moduli space representing pairs (E, P) consisting of an elliptic curve E over a $\mathbb{Q}$-scheme S together with the choice of a point P of E of exact order N. It is a geometrically connected smooth affine curve over $\mathbb{Q}$ and it is the complement of the set of cusps in the curve $X_1(N)$ described in Section 1.2.2.

Let $\pi : \mathcal{E} \longrightarrow Y_1(N)$ be the universal elliptic curve with $\Gamma_1(N)$-level structure over $Y_1(N)$, and let $\underline{\omega} := \pi_* \Omega^1_{\mathcal{E}/Y_1(N)}$ be the coherent sheaf of relative differentials on $\mathcal{E}/Y_1(N)$, extended to a coherent sheaf on $X_1(N)$ in the standard way. See [12, §1.1]. Let $\underline{\omega}^r$ be the r-th tensor power of this line bundle. The sheaf $\underline{\omega}^2$ is related to the sheaf $\Omega^1_{X_1(N)}(\log \text{cusps})$ of regular differentials on $X_1(N)$ with logarithmic poles at the cusps by the Kodaira–Spencer isomorphism

$$\sigma : \underline{\omega}^2 \xrightarrow{\sim} \Omega^1_{X_1(N)}(\log \text{cusps}), \tag{1.22}$$

as described for instance in [12, §1.1].

Definition 1.6. Let r denote a non-negative integer. A (holomorphic) modular form of weight $k = r + 2$ is a global section of the sheaf $\underline{\omega}^k$, or – equivalently, by (1.22) – of $\underline{\omega}^r \otimes \Omega^1_{X_1(N)}(\log \text{cusps})$ over $X_1(N)$. The global sections of $\underline{\omega}^r \otimes \Omega^1_{X_1(N)}$ are called cusp forms. Let $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ denote the complex vector spaces of modular forms and cusp forms on $\Gamma_1(N)$, respectively.

When working over the field of complex numbers, the set $X_1(N)(\mathbb{C})$ of complex points of $X_1(N)$ is a compact Riemann surface, and the analytic map

$$\text{pr} : \mathcal{H} \longrightarrow Y_1(N)(\mathbb{C}), \qquad \text{pr}(\tau) := \left(\mathbb{C}/\langle 1, \tau \rangle, \frac{1}{N}\right)$$

identifies $Y_1(N)(\mathbb{C})$ with the quotient $\Gamma_1(N)\backslash\mathcal{H}$. Let τ denote a point of $\mathcal{H}$ and let w be the standard complex coordinate on the elliptic curve $\mathbb{C}/\langle 1, \tau \rangle$. The Hodge filtration on $H^1_{\text{dR}}(\mathbb{C}/\langle 1, \tau \rangle)$ admits a canonical, functorial (but not holomorphic) splitting

$$H^1_{\text{dR}}(\mathbb{C}/\langle 1, \tau \rangle) := \mathbb{C}dw \oplus \mathbb{C}d\bar{w}. \tag{1.23}$$

This is the Hodge decomposition of the elliptic curve. In terms of the coordinates τ, dw, and $d\bar{w}$, one has [12, §1.2]

$$\sigma((2\pi i dw)^2) = 2\pi i d\tau, \tag{1.24}$$

and a modular form $\omega_f \in M_k(\Gamma_1(N))$ gives rise to a holomorphic function on the upper half plane $\mathcal{H}$ by the rule

$$\omega_f(\tau) = f(\tau)(2\pi i dw)^{r+2} = f(\tau)(2\pi i dw)^r \otimes (2\pi i d\tau). \tag{1.25}$$

This function obeys the familiar transformation rule

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N), \tag{1.26}$$

and the modular form ω_f is completely determined by the associated function $f(\tau)$.

Modular forms and Kuga–Sato varieties

We retain the assumptions that $N \geq 5$ and $r \geq 0$. Let $\pi : \bar{\mathcal{E}} \longrightarrow X_1(N)$ denote the universal generalised elliptic curve over $X_1(N)$ that extends the universal elliptic curve $\mathcal{E}$ over $Y_1(N)$ introduced in Section 1.2.4. This is a smooth and proper variety over $\mathbb{Q}$, and the geometric fibres over a closed point $x \in X_1(N)$ are singular precisely when x is a cusp. Let

$$W_r^\# := \bar{\mathcal{E}} \times_{X_1(N)} \bar{\mathcal{E}} \times_{X_1(N)} \ldots \times_{X_1(N)} \bar{\mathcal{E}} \tag{1.27}$$

denote the r-fold self-product of $\bar{\mathcal{E}}$ over $X_1(N)$.

Definition 1.7. The canonical desingularisation, described for instance in [12, Appendix]), of $W_r^\#$ is denoted W_r and called the r-th Kuga–Sato variety with $\Gamma_1(N)$-level structure.

The variety W_r is smooth and proper over $\mathbb{Q}$ of dimension $r + 1$ and it is fibred over $X_1(N)$ via the natural projection $\pi_r : W_r \longrightarrow X_1(N)$. If $x \in X_1(N)$ is a closed non-cuspidal point corresponding to an elliptic curve E with $\Gamma_1(N)$-structure, then the fibre $\pi_r^{-1}(x)$ is E^r, the r-fold self-product of E.

Following [12], we now introduce an idempotent in the ring of automorphism of $W_r/X_1(N)$ which will enable us to identify the space of cusp forms $S_{r+2}(\Gamma_1(N))$ with a piece of the de Rham cohomology of W_r.

The generalised elliptic curve $\pi : \bar{\mathcal{E}} \longrightarrow X_1(N)$ is equipped with a $\Gamma_1(N)$-level structure, i.e., with a section $s : X_1(N) \longrightarrow \bar{\mathcal{E}}$ of order N. Translation by this section gives rise to an action of $\mathbb{Z}/N\mathbb{Z}$ on $\bar{\mathcal{E}}$; if $a \in \mathbb{Z}/N\mathbb{Z}$ and $x \in \bar{\mathcal{E}}$ lies over $(E, P) \in X_1(N)$, then we let $a \cdot x = x + a \cdot s(E, P)$, where the addition is the group structure on E. The variety $W_r^{\#} \longrightarrow X_1(N)$ is the r-fold fibre product of $\bar{\mathcal{E}}$, and therefore there is a natural action of $(\mathbb{Z}/N\mathbb{Z})^r$ on $W_r^{\#}$. By the canonical nature of the desingularisation of $W_r^{\#}$, this action extends to W_r. Let σ_a denote the automorphism of $W_r/X_1(N)$ associated to $a \in (\mathbb{Z}/N\mathbb{Z})^r$ and define

$$\epsilon_{W_r}^{(1)} := \frac{1}{N^r} \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^r} \sigma_a, \tag{1.28}$$

which is an idempotent in the group ring $\mathbb{Z}[1/N][\mathrm{Aut}(W_r/X_1(N))]$.

Let S_r denote the symmetric group on r letters. Multiplication by -1 on the generalised elliptic curve $\bar{\mathcal{E}}/X_1(N)$ together with the natural action of S_r on $W_r^{\#}$ gives rise to an action of the semidirect product $(\mu_2)^r \rtimes S_r$ on $W_r^{\#}$, which extends to an action on W_r by the canonical nature of the desingularisation. Let $j : (\mu_2)^r \rtimes S_r \longrightarrow \mu_2$ be the homomorphism which is the identity on μ_2 and the sign character on S_r and define

$$\epsilon_{W_r}^{(2)} := \frac{1}{2^r r!} \sum_{\sigma \in (\mu_2)^r \rtimes S_r} j(\sigma)\sigma, \tag{1.29}$$

which is an idempotent in the group ring $\mathbb{Z}[1/2r!][\mathrm{Aut}(W_r/X_1(N))]$.

Definition 1.8. The two idempotents $\epsilon_{W_r}^{(1)}$ and $\epsilon_{W_r}^{(2)}$ commute and hence define an idempotent

$$\epsilon_{W_r} := \epsilon_{W_r}^{(1)} \circ \epsilon_{W_r}^{(2)} \in \mathbb{Q}[\mathrm{Aut}(W_r/X_1(N))].$$

Most useful for us is the following result.

Proposition 1.6. *For any field F of characteristic zero, we have an identification*

$$S_{r+2}(\Gamma_1(N), F) \simeq \mathrm{Fil}^{r+1}\, \epsilon_{W_r} H^{r+1}_{\mathrm{dR}}(W_r/F),$$

via the association $f \mapsto \omega_f := f(E,t,\omega)\omega^r \otimes \sigma(\omega^2)$, for an elliptic curve with $\Gamma_1(N)$-structure (E,t) and an invariant differential ω of E.

Proof. This is [12, Lemma 2.2, Corollary 2.3]. □

1.3 Complex multiplication theory

We review the theory of elliptic curves with complex multiplication and its relation to the explicit class field theory of imaginary quadratic fields. A complete reference is [136], but we mainly follow [42, 131].

1.3.1 Class field theory for imaginary quadratic fields

Let K be an imaginary quadratic field of discriminant $-d_K$ where $d_K > 0$, and let $\mathcal{O}_K$ denote its ring of integers. Recall from Notation 1.1 the fixed embedding $\bar{K} \hookrightarrow \mathbb{C}$. For simplicity, we assume that $d_K \neq 3, 4$, so that $\mathcal{O}_K^\times = \{\pm 1\}$.

Orders in quadratic imaginary fields

Let $\tau := (-d_K + \sqrt{-d_K})/2$ be the standard generator of $\mathcal{O}_K = \langle 1, \tau\rangle := \mathbb{Z} \oplus \tau\mathbb{Z}$. Any order $\mathcal{O}$ in K is uniquely determined by its conductor $c := [\mathcal{O}_K : \mathcal{O}]$. The unique order of conductor c will be denoted $\mathcal{O}_c = \langle 1, c\tau\rangle$ and its discriminant is equal to $-c^2 d_K$.

Given an order $\mathcal{O}$, its class group is defined as $\mathrm{Cl}(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$, where $I(\mathcal{O})$ denotes the multiplicative group of proper fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ is the subgroup of principal

$\mathcal{O}$-ideals. The size of this class group will be denoted $h(\mathcal{O})$. We will write $I_K = I(\mathcal{O}_K)$, $P_K = P(\mathcal{O}_K)$, $\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K)$ and $h_K = h(\mathcal{O}_K)$ in the case of the maximal order.

We denote by $I(\mathcal{O}_c, c)$ the subgroup of fractional ideals relatively prime to the conductor c and let $P(\mathcal{O}_c, c) = P(\mathcal{O}_c) \cap I(\mathcal{O}_c, c)$. Similarly, we write $I_K(c)$ for the group of fractional $\mathcal{O}_K$-ideals relatively prime to c and we define $P_{K,\mathbb{Z}}(c)$ to be the subgroup generated by principal $\mathcal{O}_K$-ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \pmod{c\mathcal{O}_K}$ for some integer a relatively prime to c. We then have [42, Proposition 7.22]

$$\mathrm{Cl}(\mathcal{O}_c) \simeq I(\mathcal{O}_c, c)/P(\mathcal{O}_c, c) \simeq I_K(c)/P_{K,\mathbb{Z}}(c). \tag{1.30}$$

From this isomorphism and the exact sequence

$$1 \longrightarrow (\mathbb{Z}/c\mathbb{Z})^\times \longrightarrow (\mathcal{O}_K/c\mathcal{O}_K)^\times \longrightarrow (I_K(c) \cap P_K)/P_{K,\mathbb{Z}}(c) \longrightarrow 1, \tag{1.31}$$

one can deduce the formula [42, Theorem 7.24]

$$\frac{h(\mathcal{O}_c)}{h(\mathcal{O}_K)} = |(I_K(c) \cap P_K)/P_{K,\mathbb{Z}}(c)| = c \prod_{p|c} \left(1 - \left(\frac{-d_K}{p}\right) \frac{1}{p}\right). \tag{1.32}$$

Ray class fields and ring class fields

Given an ideal $\mathfrak{N}$ of $\mathcal{O}_K$, we define $I_K(\mathfrak{N})$ to be the group of fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{N}$ and $P_K(\mathfrak{N}) = P_K \cap I_K(\mathfrak{N})$. We also define $P_{K,1}(\mathfrak{N})$ as the subgroup generated by principal ideals $\alpha\mathcal{O}_K$ where $\alpha \equiv 1 \pmod{\mathfrak{N}}$.

Given a finite abelian extension L/K, let $\mathfrak{N}$ denote an ideal of $\mathcal{O}_K$ divisible by all primes that ramify in L. The Artin reciprocity map

$$\phi_{L/K,\mathfrak{N}} : I_K(\mathfrak{N}) \longrightarrow \mathrm{Gal}(L/K)$$

is then defined by mapping a prime ideal $\mathfrak{p}$ to the Frobenius element $\sigma_\mathfrak{p} \in \mathrm{Gal}(L/K)$. This map is surjective by the Cebotarev Density Theorem [42, Theorem 8.17].

Definition 1.9. Let $\mathfrak{N}$ be an ideal of $\mathcal{O}_K$. By the Existence Theorem of class field theory [42, Theorem 8.6], there exists a unique abelian extension $K_{\mathfrak{N}}$ of K, ramified only at primes dividing $\mathfrak{N}$, such that the Artin reciprocity map induces an isomorphism

$$\phi_{K_{\mathfrak{N}}/K,\mathfrak{N}} : I_K(\mathfrak{N})/P_{K,1}(\mathfrak{N}) \xrightarrow{\sim} \mathrm{Gal}(K_{\mathfrak{N}}/K).$$

The field $K_{\mathfrak{N}}$ is called the ray class field of K of conductor $\mathfrak{N}$.

Any finite abelian extension L of K has a conductor $\mathfrak{f}$ [42, Theorem 8.5], which is an ideal of $\mathcal{O}_K$, such that a prime in K ramifies in L if and only if the prime divides $\mathfrak{f}$ and such that L is contained in the ray class field $K_{\mathfrak{f}}$ [42, Theorem 8.2].

Definition 1.10. In the special case when $\mathfrak{N} = 1$, the ray class field is denoted H and called the Hilbert class field of K. In this case the Artin reciprocity map induces an isomorphism

$$\phi_{H/K,1} : \mathrm{Cl}_K = I_K/P_K \xrightarrow{\sim} \mathrm{Gal}(H/K)$$

and H is the maximal unramified abelian extension of K.

Definition 1.11. Let c be a positive integer. By the Existence Theorem of class field theory [42, Theorem 8.6], there exists a unique abelian extension $H_{\mathcal{O}_c} = H_c$ of K, ramified only at primes dividing $c\mathcal{O}_K$, such that the Artin reciprocity map induces an isomorphism

$$\phi_{H_c/K,c\mathcal{O}_K} : \mathrm{Cl}(\mathcal{O}_c) = I_K(c)/P_{K,\mathbb{Z}}(c) \xrightarrow{\sim} \mathrm{Gal}(H_c/K). \tag{1.33}$$

The field H_c is called the ring class field of K of conductor c and is contained in the ray class field $K_{c\mathcal{O}_K}$.

The ring class field H_c is fixed by complex conjugation and is therefore a Galois extension over $\mathbb{Q}$. In fact, it is a generalised dihedral extension of $\mathbb{Q}$, meaning that its Galois group can be written as a semi-direct product

$$\mathrm{Gal}(H_c/\mathbb{Q}) \simeq \mathrm{Gal}(H_c/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where the non-trivial element τ of $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(H_c/K)$ by inversion [42, Lemma 9.3], i.e., $\tau\sigma\tau^{-1} = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(H_c/K)$. Any abelian extension of K is generalised dihedral over $\mathbb{Q}$ if and only it is contained in a ring class field of K [42, Theorem 9.18].

The following properties concern the behaviour of primes in ring class fields and will be particularly useful in Section 2.3.3 of Chapter 2. Let n be a square-free integer and let $q \mid n$ denote a rational prime. Write $n = qm$ with $(q, m) = 1$. We begin with the following simple observation.

Proposition 1.7. *The intersection $H_q \cap H_m$ is the Hilbert class field H of K, and the ring class field H_n is the compositum of H_q and H_m.*

Proof. Let $\mathfrak{p}$ denote a prime of K. If $\mathfrak{p}$ ramifies in $H_q \cap H_m$, then $\mathfrak{p}$ ramifies both in H_q and in H_m. By Definition 1.11, this implies that $\mathfrak{p}$ divides q and m, respectively. But q and m are coprime, so this is not possible. As a consequence, $H_q \cap H_m$ is an unramified abelian extension of K, hence contained in H by Definition 1.10.

For the second statement, observe that for any $k \mid n$, H_n contains the ring class field H_k. This follows from [42, Corollary 8.7] after noting the inclusion

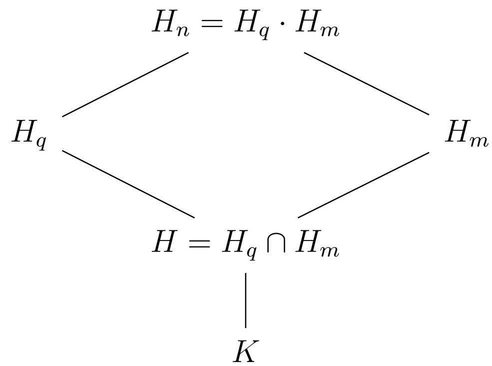
$$P_{K,1}(n) \subset P_{K,\mathbb{Z}}(n) = \ker(\phi_{H_n/K,n}) \subset P_{K,\mathbb{Z}}(k) \cap I_K(N) = \ker(\phi_{H_k/K,n}).$$

In particular, H_n contains the compositum $H_q \cdot H_m$ as a subfield. As $H_q \cap H_m = H$, we have an isomorphism

$$\mathrm{Gal}(H_q \cdot H_m/H) \simeq \mathrm{Gal}(H_q/H) \times \mathrm{Gal}(H_m/H). \tag{1.34}$$

Using formula (1.32), we then see that $[H_q \cdot H_m : H] = [H_n : H]$, hence $H_q \cdot H_m = H_n$. ◻

Let us draw the following diagram of Galois extensions:



(1.35)

Note that the natural restriction maps induce isomorphisms

$$\mathrm{Gal}(H_n/H_m) \simeq \mathrm{Gal}(H_q/H) \qquad\qquad \mathrm{Gal}(H_n/H_q) \simeq \mathrm{Gal}(H_m/H), \tag{1.36}$$

as can be seen by comparing cardinalities.

Proposition 1.8. *Let n be a square-free positive integer, and let q be a rational prime which is inert in K. The ideal $q\mathcal{O}_K$ has residual degree 1 in H_n/K.*

Proof. If $q \mid n$, we write $n = qm$ with $(q, m) = 1$. If $q \nmid n$, then we set $m = n$. In any case, we have $(q, m) = 1$. Since q is coprime to m, the ideal $q\mathcal{O}_K$ belongs to $P_{K,\mathbb{Z}}(m)$, hence its class in $\mathrm{Cl}(\mathcal{O}_m) = I_K(m)/P_{K,\mathbb{Z}}(m)$ is trivial. Thus, its image under the Artin reciprocity map $\phi_{H_m/K,m}$ is trival in $\mathrm{Gal}(H_m/K)$. Since q is inert, the ideal $q\mathcal{O}_K$ is prime and its image under this map is the Frobenius element at q. In particular, this Frobenius element is trivial and $q\mathcal{O}_K$ splits completely in the extension H_m/K. This completes the proof in the case $q \nmid n$.

From now on, suppose that $q \mid n$ and let $m = n/q$. Since q is inert in K, the residual degree of $q\mathcal{O}_K$ is 2. Observe then, following Section 1.3.1, that

$$\mathrm{Gal}(H_q/H) \simeq (I_K(q) \cap P_K)/P_{K,\mathbb{Z}}(q) \simeq (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times \tag{1.37}$$

is cyclic of order $q+1$. From the first part of the proof (with $n=1$), $q\mathcal{O}_K$ splits completely in H. Let $\mathfrak{q}$ denote a prime of H above q. Since $H_q \neq H$, by Definitions 1.10 and 1.11 we see that $q\mathcal{O}_K$ must ramify in H_q. In particular, $\mathfrak{q}$ must ramify in H_q/H. This fact, combined with the fact that $\mathrm{Gal}(H_q/H)$ is cyclic, implies that there is a unique prime of H_q above $\mathfrak{q}$. The fact that H is the maximal abelian unramified extension of K can then be used to show that the ramification degree of $\mathfrak{q}$ is $q+1$. In other words, $\mathfrak{q}$ is totally ramified in H_q/H. In particular, the ramification index of $q\mathcal{O}_K$ in H_n/K is greater or equal to $q+1$. Recall that $q\mathcal{O}_K$ splits completely in H_m and let $\mathfrak{q}'$ denote a prime of H_m above $q\mathcal{O}_K$. Since the degree of H_n/H_m is $q+1$, as seen from the isomorphism (1.36), the ramification index of $\mathfrak{q}'$ in H_n is forced to be $q+1$. In conclusion, each factor of $q\mathcal{O}_K$ in H_m is totally ramified in H_n and the proof is complete. □

Corollary 1.2. *Let $\mathfrak{N}$ denote a prime ideal of $\mathcal{O}_K$ and let N denote its norm. Let q be a prime satisfying $(2N,q)=1$ and such that q is inert in K. Fix a prime ideal $\mathfrak{q}$ in H above q and denote by s its residual degree in the extension $K_{\mathfrak{N}}/H$. For any square-free positive integer n coprime to N, the residual degree of $\mathfrak{q}$ in the compositum $K_{\mathfrak{N}} \cdot H_n$ is equal to s.*

Proof. We begin by noting that $K_{\mathfrak{N}} \cap H_n = H$. Indeed, if a prime ideal in K ramifies in the abelian extension $K_{\mathfrak{N}} \cap H_n$ over K, then it divides both $\mathfrak{N}$ and $n\mathcal{O}_K$. But these two ideals are coprime by assumption since the norm of $\mathfrak{N}$ is N. Thus $K_{\mathfrak{N}} \cap H_n$ is everywhere unramified above K and is therefore contained in H by Definition 1.10.

We have the following diagram of Galois extensions:

$$\begin{array}{ccccc} & & K_{\mathfrak{N}} \cdot H_n & & \\ & / & & \backslash & \\ K_{\mathfrak{N}} & & & & H_n \\ & \backslash & & / & \\ & & H = K_{\mathfrak{N}} \cap H_n & & \\ & & | & & \\ & & K & & \end{array} \tag{1.38}$$

The natural restriction map induces an isomorphism of Galois groups

$$\mathrm{Gal}(K_{\mathfrak{N}} \cdot H_n/K_{\mathfrak{N}}) \simeq \mathrm{Gal}(H_n/H). \tag{1.39}$$

Let $\mathfrak{q}_{\mathfrak{N}}$ denote a prime ideal of $K_{\mathfrak{N}}$ above $\mathfrak{q}$. Let $D_{\mathfrak{q}}$ and $I_{\mathfrak{q}}$ be respectively the decomposition group and inertia group of $\mathfrak{q}$ in $\mathrm{Gal}(H_n/H)$. Similarly, denote by $D_{\mathfrak{q}_{\mathfrak{N}}}$ and $I_{\mathfrak{q}_{\mathfrak{N}}}$ respectively the decomposition and inertia groups of $\mathfrak{q}_{\mathfrak{N}}$ in $\mathrm{Gal}(K_{\mathfrak{N}} \cdot H_n/K_{\mathfrak{N}})$. Restricting the map (1.39) to the decomposition group and inertia group yields injective maps $D_{\mathfrak{q}_{\mathfrak{N}}} \hookrightarrow D_{\mathfrak{q}}$ and $I_{\mathfrak{q}_{\mathfrak{N}}} \hookrightarrow I_{\mathfrak{q}}$, and thus induces an injection $D_{\mathfrak{q}_{\mathfrak{N}}}/I_{\mathfrak{q}_{\mathfrak{N}}} \hookrightarrow D_{\mathfrak{q}}/I_{\mathfrak{q}}$. As a result, the residual degree of $\mathfrak{q}_{\mathfrak{N}}$ in $K_{\mathfrak{N}} \cdot H_n/K_{\mathfrak{N}}$ divides the residual degree of $\mathfrak{q}$ in H_n/H. The latter is equal to 1 by Proposition 1.8. By multiplicativity of residual degrees, the residual degree of $\mathfrak{q}$ in $K_{\mathfrak{N}} \cdot H_n/H$ is s. □

1.3.2 Main theorems of complex multiplication

Let E be an elliptic curve defined over $\mathbb{C}$ and consider its ring of endomorphisms $\mathrm{End}_{\mathbb{C}}(E)$. The elliptic curve admits a complex uniformisation $E(\mathbb{C}) = \mathbb{C}/\Lambda_E$ where Λ_E is the period lattice of E. Given this uniformisation, we have

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_E \subset \Lambda_E\},$$

hence $\mathrm{End}_{\mathbb{C}}(E)$ is a discrete subring of $\mathbb{C}$, as it preserves a lattice, and thus must be either $\mathbb{Z}$ or an order in a quadratic imaginary field. In fact, this ring acts faithfully on both the one dimensional complex vector space $\Omega^1(E) = H^{1,0}(E(\mathbb{C}))$ and the 2-dimensional module $H_1(E(\mathbb{C}), \mathbb{Z})$, and therefore injects into both $\mathbb{C}$ and $M_2(\mathbb{Z})$.

Definition 1.12. If $\mathrm{End}_{\mathbb{C}}(E)$ is an order in a quadratic imaginary field, then E is said to have complex multiplication (CM).

Definition 1.13. Let $\mathcal{O}$ be an order in a quadratic imaginary field K. For any field F, let $\mathrm{CM}_F(\mathcal{O})$ denote the set of $\bar{F}$-isomorphism classes of elliptic curves E/F equipped with an isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$ satisfying, for $\alpha \in \mathcal{O}$, $[\alpha]^*\omega = \alpha\omega$. Here $\alpha \in \mathcal{O}$ is viewed as an endomorphism $[\alpha] : E \longrightarrow E$ and $[\alpha]^* : \Omega^1(E/F) \longrightarrow \Omega^1(E/F)$ is the pull-back on differentials.

When $F = \mathbb{C}$, we have $|\,\mathrm{CM}_{\mathbb{C}}(\mathcal{O})| = h(\mathcal{O})$, as elliptic curves over $\mathbb{C}$ correspond to lattices up to homothety and E has CM by $\mathcal{O}$ if and only if the corresponding lattice Λ_E is a projective $\mathcal{O}$-module. There are $h(\mathcal{O})$ distinct such homothety classes. This set can be described as follows

$$\begin{aligned}\mathrm{CM}_{\mathbb{C}}(\mathcal{O}) &= \{\tau \in \mathbf{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \mid a\tau^2 + b\tau + c = 0, \gcd(a,b,c) = 1, \mathrm{Disc}(\mathcal{O}) = b^2 - 4ac\} \\ &= \{[\tau_1], \ldots, [\tau_{h(\mathcal{O})}]\}.\end{aligned}$$

If $E/\mathbb{C}$ has CM by $\mathcal{O}$, then the j-invariant $j(E)$ of E is algebraic and generates a field of degree less than or equal to $h(\mathcal{O})$ over K. This results from the fact that $\mathrm{Aut}(\mathbb{C}/K)$ acts on $\mathrm{CM}_{\mathbb{C}}(\mathcal{O})$ and thus permutes the j-invariants $j(\tau_1), \ldots, j(\tau_{h(\mathcal{O})})$. Let $L_{\mathcal{O}}$ denote the field generated by $j(\tau_1), \ldots, j(\tau_{h(\mathcal{O})})$ over K. This is a finite extension of K and every elliptic curve with CM by $\mathcal{O}$ is defined over $L_{\mathcal{O}}$. Thus, using the fixed embedding $L_{\mathcal{O}} \hookrightarrow \mathbb{C}$ of Notation 1.1, we may identify $\mathrm{CM}_{L_{\mathcal{O}}}(\mathcal{O}) = \mathrm{CM}_{\mathbb{C}}(\mathcal{O})$.

The first main theorem of complex multiplication asserts that $L_{\mathcal{O}}$ is the ring class field $H_{\mathcal{O}}$ of K associated to the order $\mathcal{O}$, see Definition 1.11.

Theorem 1.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let $E \in \mathrm{CM}_{\mathbb{C}}(\mathcal{O})$ be an elliptic curve with complex multiplication by $\mathcal{O}$. Then the j-invariant $j(E)$ is an algebraic integer and $K(j(E)) = H_{\mathcal{O}}$ is the ring class field of K associated to the order $\mathcal{O}$.*

Proof. This is [42, Theorem 11.1]. □

The theorem gives an explicit description of the ring class fields of K, hence enables a description of all abelian extension of K which are generalised dihedral over $\mathbb{Q}$. See the comment following Definition 1.11. The second main theorem of complex multiplication completes the description of all abelian extensions of K by describing the ray class fields.

Theorem 1.3. *Let $\mathfrak{N}$ be an ideal of $\mathcal{O}_K$. The ray class field $K_{\mathfrak{N}}$ of conductor $\mathfrak{N}$ is obtained from the Hilbert class field H by adjoining the coordinates of the torsion points $E(\bar{H})[\mathfrak{N}]$ of some $E \in \mathrm{CM}_H(\mathcal{O}_K)$. As a consequence, for such a choice of elliptic curve E, we have $K_{\mathfrak{N}} = K(j(E), E(\bar{H})[\mathfrak{N}])$.*

Proof. This is [42, Theorem 11.39]. □

1.4 Algebraic cycles

We review the definition of algebraic cycles and various associated adequate equivalence relations. This will enable us to state the Beilinson–Bloch conjecture, a generalisation of the Birch and Swinnerton-Dyer conjecture to higher dimensional varieties. We introduce tools, in the form of Abel–Jacobi maps, for the study of algebraic cycles and their properties.

By an algebraic variety we shall mean an integral separated scheme of finite type over a field. A subvariety is an integral separated closed subscheme.

1.4.1 Algebraic cycles and Chow groups

Let X be a smooth projective algebraic variety of dimension d defined over a field K of characteristic zero. Fix an algebraic closure $\bar{K}$ of K, as well as an embedding $\sigma : \bar{K} \hookrightarrow \mathbb{C}$.

Definition 1.14. Let r be a non-negative integer. The group $\mathcal{Z}^r(X)$ of codimension r algebraic cycles in X is the free abelian group generated by the codimension r subvarieties of $X_{\bar{K}}$. A codimension r algebraic cycle Z is thus a $\mathbb{Z}$-linear combination $Z = \sum_V n_V \cdot V$, where the sum is over all codimension r subvarieties of $X_{\bar{K}}$ and $n_V = 0$ for all but finitely many V.

If F is a field extension of K contained in $\bar{K}$, we denote by $\mathcal{Z}^r(X)(F)$ the subgroup of algebraic cycles which are fixed by the natural action of the Galois group $\mathrm{Gal}(\bar{K}/F) =: G_F$. Note that $\mathcal{Z}^1(X) = \mathrm{Div}(X)$ is the group of Weil divisors. In particular, when X is a curve, elements of $\mathcal{Z}^1(X)$ are formal linear combinations of points in $X(\bar{K})$.

Let V be a subvariety of $X_{\bar{K}}$ of codimension $r-1$ and let W be a subvariety of V of codimension 1. The local ring $\mathcal{O}_{W,V}$, i.e., the localisation of $\mathcal{O}_V$ at the generic point of W, is a discrete valuation ring with quotient field $R(V)$, the function field of V. We denote the associated discrete valuation by ord_W. For any $f \in R(V)^\times$, we may form the codimension r cycle

$$\mathrm{div}(f) := \sum_W \mathrm{ord}_W(f) \cdot W \in \mathcal{Z}^r(X)$$

where the sum ranges over all subvarieties of V of codimension 1.

Definition 1.15. Two codimension r cycles Z_1 and Z_2 are rationally equivalent if there exists subvarieties $V_1, \ldots, V_t$ of $X_{\bar{K}}$ of codimension $r-1$ and functions $f_i \in R(V_i)^\times$ for $i = 1, \ldots, t$ such that

$$Z_1 - Z_2 = \sum_{i=1}^{t} \mathrm{div}(f_i).$$

In this case we write $Z_1 \sim_{\mathrm{rat}} Z_2$. This defines an equivalence relation on codimension r cycles and the subgroup of cycles rationally equivalent to zero will be denoted $\mathcal{Z}^r(X)_{\mathrm{rat}}$. The codimension r Chow group is the quotient $\mathrm{CH}^r(X) := \mathcal{Z}^r(X)/\mathcal{Z}^r(X)_{\mathrm{rat}}$. We shall often write $[Z]$ for the image of a cycle Z in the Chow group.

We regard the Chow group as a functor from the category of field extensions of K contained in $\mathbb{C}$ to the category of abelian groups given by the rule

$$F/K \quad \mapsto \quad \mathrm{CH}^r(X)(F) := \{[Z] \in \mathrm{CH}^r(X) \ : \ \sigma(Z) \sim_{\mathrm{rat}} Z, \quad \forall \sigma \in \mathrm{Aut}(\mathbb{C}/F)\}.$$

For any non-negative integers r and s, there is an intersection product

$$\mathrm{CH}^r(X) \times \mathrm{CH}^s(X) \longrightarrow \mathrm{CH}^{r+s}(X), \qquad ([Z], [Z']) \mapsto [Z] \cdot [Z']$$

which endows $\mathrm{CH}^*(X) := \bigoplus_{r \geq 0} \mathrm{CH}^r(X)$ with the structure of a graded ring.

Let $f : X \longrightarrow Y$ be a morphism of smooth projective varieties over K, with $\dim X = d_X$ and $\dim Y = d_Y$. If f is proper, then the push-forward map on cycles preserves rational equivalence and induces a push-forward map

$$f_* : \mathrm{CH}^r(X) \longrightarrow \mathrm{CH}^{r+d_Y-d_X}(Y),$$

defined by mapping a codimension r subvariety V of X to $[R(V) : R(f(V))] \cdot f(V)$ if $\dim f(V) = \dim V$ and to 0 if $\dim f(V) < \dim V$, and extended by linearity to arbitrary cycles.

If f is flat, then the pull-back map on cycles preserves rational equivalence and induces a pull-back map

$$f^* : \mathrm{CH}^r(Y) \longrightarrow \mathrm{CH}^r(X)$$

given by mapping a codimension r subvariety V to the cycle associated to the subscheme $X \times_Y V$, and extending by linearity to arbitrary cycles. See [72, Ch. 1 §1.5] for the cycle associated to a subscheme.

1.4.2 Correspondences and pure motives

We briefly introduce the notion of a pure motive. We will not use any deep facts related to the theory of motives, but the language and notations are convenient.

Correspondences

Let X and Y be two smooth projective varieties of respective dimensions d_X and d_Y, defined over some field K.

Definition 1.16. A correspondence between X and Y of degree r is an element of the Chow group $\mathrm{CH}^{d_X+r}(X \times Y)$. We denote the set of correspondences of degree r by $\mathrm{Corr}^r(X, Y)$.

Let $\mathrm{pr}_X : X \times Y \longrightarrow X$ and $\mathrm{pr}_Y : X \times Y \longrightarrow Y$ denote the two natural projection maps, and note that these are smooth and proper. In particular, they induce push-forward and pull-back maps on Chow groups and any correspondence $\Gamma \in \mathrm{Corr}^r(X, Y)$ induces a push-forward and a pull-back map on Chow groups defined as follows:

$$\Gamma_* : \mathrm{CH}^j(X) \longrightarrow \mathrm{CH}^{r+j}(Y) \qquad Z \mapsto (\mathrm{pr}_Y)_*(Z \cdot \mathrm{pr}_X^*(\Gamma)) \tag{1.40}$$

$$\Gamma^* : \mathrm{CH}^j(Y) \longrightarrow \mathrm{CH}^{r+j+d_x-d_y}(X) \qquad Z \mapsto (\mathrm{pr}_X)_*(Z \cdot \mathrm{pr}_Y^*(\Gamma)). \tag{1.41}$$

Suppose we are given three smooth projective varieties X_1, X_2 and X_3, and denote by $\mathrm{pr}_{i,j} : X_1 \times X_2 \times X_3 \longrightarrow X_i \times X_j$ the natural projection maps for $1 \le i < j \le 3$. For any two correspondences $T \in \mathrm{Corr}^r(X_1, X_2)$ and $S \in \mathrm{Corr}^s(X_2, X_3)$, we define their composition

$$T \circ S = (\mathrm{pr}_{13})_*(\mathrm{pr}_{12}^*(T) \cdot \mathrm{pr}_{23}^*(S)) \in \mathrm{Corr}^{r+s}(X_1, X_3), \tag{1.42}$$

where $\cdot$ denotes the intersection product on Chow groups. Note that the composition of degree zero correspondences is again a degree zero correspondence. In particular, the group $\mathrm{Corr}^0(X, X)$ for a smooth projective variety X is endowed with a ring structure.

Pure Chow motives

The category of pure Chow motives $\mathbf{Chow}(K)$ over a field K has objects defined as triples (X, p, n) where X is a smooth projective variety over K, p is an idempotent in the ring of correspondences $\mathrm{Corr}^0(X, X)$ and $n \in \mathbb{Z}$ is an integer. A morphism between two objects $f : (X, p, n) \longrightarrow (Y, q, m)$ is a correspondence $f \in \mathrm{Corr}^{m-n}(X, Y)$ such that $f \circ p = f = q \circ f$. There is a functor $h : \mathbf{SmProj}(K) \longrightarrow \mathbf{Chow}(K)$ from the category of smooth projective varieties over K to the category of pure Chow motives given by

$$h(X) := (X, \Delta_X, 0) \qquad h(f : X \longrightarrow Y) = \Gamma_f$$

where $\Delta_X \subset X \times X$ denotes the graph of the identity morphism id_X and $\Gamma_f \subset X \times Y$ denotes the graph of the morphism f. The image $h(X)$ of X under this functor is called the motive of X.

For any commutative ring A, we will also talk about the category $\mathbf{Chow}(K)_A$ of pure Chow motives over K with coefficients in A, which is defined by tensoring the morphisms of $\mathbf{Chow}(K)$ by A.

Realisations of motives

There are functors from $\mathbf{Chow}(K)$ to various categories which associate to a motive its various cohomology groups with their additional structures. The image of a motive under these functors are called its realisations.

Let $M = (X, p, n)$ denote an object in $\mathbf{Chow}(K)$. Let $\mathcal{H}^*(X)$ denote a Weil cohomology associated to the smooth projective variety X. Any idempotent correspondence $p \in \mathrm{Corr}^0(X, X)$ induces a projection map, also denoted by p, on $\mathcal{H}^r(X)$, in any degree of cohomology. We list some of the realisations of M:

- The Betti realisation $M_B := pH^*(X(\mathbb{C}), \mathbb{Q})(n)$ where $H^*(X(\mathbb{C}), \mathbb{Q})$ denotes the rational singular cohomology of the complex manifold $X(\mathbb{C})$, and we used the fixed embedding $\sigma : \bar{K} \hookrightarrow \mathbb{C}$.

- The de Rham realisation $M_{\mathrm{dR}} := pH^*_{\mathrm{dR}}(X/K)(n)$ where $H^*_{\mathrm{dR}}(X/K)$ denotes the algebraic de Rham cohomology of X over K. The finite dimensional K-vector space M_{dR} comes equipped with a Hodge filtration.

- For a prime ℓ, the ℓ-adic realisation $M_\ell := pH^*_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell)(n)$ where $H^*_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ denotes the geometric ℓ-adic étale cohomology $\varprojlim H^*_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of X. The finite dimensional $\mathbb{Q}_\ell$-vector space M_ℓ comes equipped with an action of the absolute Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$.

- The crystalline realisation M_{cris} is similarly defined when K is a discrete valuation field over $\mathbb{Q}_p$ using the crystalline cohomology of X. It is naturally equipped with the structure of a Frobenius monodromy module.

There are various natural comparison isomorphisms relating the realisations of M:

$$M_B \otimes_{\mathbb{Q}} \mathbb{C} \simeq M_{\mathrm{dR}} \otimes_K \mathbb{C}$$
$$M_B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq M_\ell.$$

Furthermore, there are theorems C_{cris} and C_{st} of p-adic Hodge theory which relate, for K a finite extension of $\mathbb{Q}_p$, M_{cris} and M_p by tensoring with Fontaine's period rings B_{cris} or B_{st}, and M_{cris} with M_{dR} by tensoring with K.

1.4.3 Cycle class maps and homological equivalence

Cycle class maps are maps from Chow groups to various Weil cohomology groups which double degrees. These maps are central in the formulation of the Hodge conjecture and the Tate conjecture. They allow us to define homological equivalence on algebraic cycles, and subsequently the null-homologous Chow group, which is the domain of various Abel–Jacobi maps that we will describe in the next section.

The Betti – de Rham cycle class maps

The exposition follows [147]. Let X be a smooth projective variety of dimension d defined over a subfield K of $\mathbb{C}$. The set of complex points of $X(\mathbb{C})$ is endowed with the structure of a compact complex manifold and the Betti cohomology of X is the singular cohomology of $X(\mathbb{C})$, i.e., $H^*_B(X,\mathbb{Z}) := H^*(X(\mathbb{C}),\mathbb{Z})$. The (topological) cycle class map is a homomorphism

$$\mathrm{cl} : \mathrm{CH}^r(X_{\mathbb{C}}) \longrightarrow H^{2r}(X(\mathbb{C}),\mathbb{Z}). \tag{1.43}$$

It is defined on codimension r subvarieties of $X_{\mathbb{C}}$ and then extended to codimension r algebraic cycles by linearity. It can then be shown to factor through rational equivalence, and hence gives a map defined on the Chow group.

A subvariety $Z \subset X_{\mathbb{C}}$ can be viewed as an analytic subset of the complex manifold $X(\mathbb{C})$. For the general definition of $\mathrm{cl}(Z)$ we refer to [147, §11.1.2] and we content ourselves with a description of $\mathrm{cl}(Z)$ in the case where Z is a complex submanifold of $X(\mathbb{C})$, i.e., when Z is smooth. Let therefore $Z \subset X(\mathbb{C})$ be a closed complex submanifold of codimension r. Let $H^j_Z(X(\mathbb{C}), \mathbb{Z})$ denote the relative singular cohomology group $H^j(X(\mathbb{C}), X(\mathbb{C}) \setminus Z, \mathbb{Z})$, or cohomology with support in Z. Associated to the pair $(X(\mathbb{C}), X(\mathbb{C}) \setminus Z)$ is a long exact sequence

$$\cdots \longrightarrow H^j_Z(X(\mathbb{C}), \mathbb{Z}) \xrightarrow{\iota^j_Z} H^j(X(\mathbb{C}), \mathbb{Z}) \longrightarrow H^j(X(\mathbb{C}) \setminus Z, \mathbb{Z}) \longrightarrow H^{j+1}_Z(X(\mathbb{C}), \mathbb{Z}) \longrightarrow \cdots$$

and we have Thom isomorphisms $T^j : H^j_Z(X(\mathbb{C}), \mathbb{Z}) \simeq H^{j-2r}(Z, \mathbb{Z})$. In particular, taking $j = 2r$, we obtain a homomorphism

$$j_Z : H^0(Z, \mathbb{Z}) \xrightarrow{(T^{2r})^{-1}} H^{2r}_Z(X(\mathbb{C}), \mathbb{Z}) \xrightarrow{\iota^{2r}_Z} H^{2r}(X(\mathbb{C}), \mathbb{Z})$$

and we define $\mathrm{cl}(Z) := j_Z(1)$.

Since $X(\mathbb{C})$ is a compact complex manifold, we have at our disposal Poincaré duality for singular cohomology, as well as the de Rham comparison theorem:

$$\mathrm{PD} : H^{2r}(X(\mathbb{C}), \mathbb{Z}) \simeq H_{2d-2r}(X(\mathbb{C}), \mathbb{Z}) \tag{1.44}$$

$$\alpha_{\mathrm{dR}} : H^{2r}(X(\mathbb{C}), \mathbb{R}) \simeq H^{2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}) \tag{1.45}$$

induced respectively by the intersection pairing on homology and the integration pairing of closed differential forms against homology classes. Tensoring with $\mathbb{R}$ and composing with α_{dR} leads to the definition of the de Rham cycle class map

$$\mathrm{cl}_{\mathrm{dR}} = \alpha_{\mathrm{dR}} \circ (\mathrm{cl} \otimes \mathbb{R}) : \mathrm{CH}^r(X_{\mathbb{C}}) \longrightarrow H^{2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}). \tag{1.46}$$

Consider the de Rham pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{dR}} : H^{2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}) \times H^{2d-2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}) \longrightarrow H^{2d}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}) \longrightarrow \mathbb{R}$$

given by cup-product followed by integration. If $Z \subset X(\mathbb{C})$ is a complex submanifold of codimension r, then $\mathrm{cl}_{\mathrm{dR}}$ is characterised by

$$\langle \mathrm{cl}_{\mathrm{dR}}(Z), [\alpha] \rangle_{\mathrm{dR}} = \int_Z \alpha, \qquad \forall\, [\alpha] \in H^{2d-2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}).$$

In particular, $\mathrm{PD}(\mathrm{cl}(Z)) \in H_{2d-2r}(X(\mathbb{C}), \mathbb{Z})$ is the canonical homology class of Z. More generally, if $Z \subset X(\mathbb{C})$ is an analytic subset of a smooth compact complex manifold, then

$$\langle \mathrm{cl}_{\mathrm{dR}}(Z), [\alpha] \rangle_{\mathrm{dR}} = \int_{Z_{\mathrm{smooth}}} \alpha, \qquad \forall\, [\alpha] \in H^{2d-2r}_{\mathrm{dR}}(X(\mathbb{C}), \mathbb{R}), \tag{1.47}$$

where Z_{smooth} denotes the smooth locus of Z. See [147, Theorem 11.21].

Finally, by precomposing these cycle class maps with the map $\mathrm{CH}^r(X) \longrightarrow \mathrm{CH}^r(X_{\mathbb{C}})$ arising from the embedding $\bar{K} \subset \mathbb{C}$, we obtain the Betti and de Rham cycle class maps

$$\mathrm{cl}_B : \mathrm{CH}^r(X) \longrightarrow H^{2r}_B(X, \mathbb{Z})$$
$$\mathrm{cl}_{\mathrm{dR}} : \mathrm{CH}^r(X) \longrightarrow H^{2r}_{\mathrm{dR}}(X/\mathbb{C}).$$

Proposition 1.9. *For $Z \in \mathcal{Z}^r(X)$, the image in $H^{2r}_B(X, \mathbb{C})$ of the class $\mathrm{cl}_B(Z) \in H^{2r}_B(X, \mathbb{Z})$ lies in $H^{r,r}(X/\mathbb{C})$, i.e., $\mathrm{cl}_B(Z)$ is a Hodge class.*

Proof. This is [147, Proposition 11.20] and follows from (1.47). □

We will write $\mathrm{Hdg}^{2r}(X) := H^{2r}_B(X, \mathbb{Z}) \cap H^{r,r}(X/\mathbb{C})$ for the set of Hodge classes of the Hodge structure $H^{2r}_B(X, \mathbb{Z})$. Consider the cycle class map tensored with $\mathbb{Q}$

$$\mathrm{cl}_B \otimes \mathbb{Q} : \mathrm{CH}^r(X) \otimes \mathbb{Q} \longrightarrow H^{2r}_B(X, \mathbb{Q}).$$

The famous Hodge conjecture, now one of the Clay Millennium Problems, is concerned with the cycle class map and says the following:

Conjecture 1.3 (Hodge)**.** *The map* $\mathrm{cl}_B \otimes \mathbb{Q}$ *surjects onto* $\mathrm{Hdg}^{2r}(X)$*, i.e., for any Hodge class* $\alpha \in \mathrm{Hdg}^{2r}(X)$*, there exist a positive integer* N *and an algebraic cycle* $Z \in \mathcal{Z}^r(X)$ *such that* $\mathrm{cl}_B(Z) = N\alpha$*.*

Definition 1.17. Define the subgroup of null-homologous codimension r algebraic cycles to be $\mathcal{Z}^r(X)_0 := \ker(\mathrm{cl}_B)$. Two cycles Z_1 and Z_2 are said to be homologically equivalent, written $Z_1 \sim_{\mathrm{hom}} Z_2$, if $Z_1 - Z_2 \in \mathcal{Z}^r(X)_0$. The r-th null-homologous Chow group is defined as $\mathrm{CH}^r(X)_0 := \mathcal{Z}^r(X)_0/\mathcal{Z}^r(X)_{\mathrm{rat}}$.

If $f : X \longrightarrow Y$ is a morphism of smooth projective varieties, $\dim X = d_X$ and $\dim Y = d_Y$, then proper push-forward and flat pull-back preserve null-homologous cycles, as do maps induces by correspondences $\Gamma \in \mathrm{Corr}^r(X, Y)$:

$$f_* : \mathrm{CH}^j(X)_0 \longrightarrow \mathrm{CH}^{j+d_Y-d_X}(Y)_0$$
$$f^* : \mathrm{CH}^j(Y)_0 \longrightarrow \mathrm{CH}^j(X)_0$$
$$\Gamma_* : \mathrm{CH}^j(X)_0 \longrightarrow \mathrm{CH}^{r+j}(Y)_0$$
$$\Gamma^* : \mathrm{CH}^j(Y)_0 \longrightarrow \mathrm{CH}^{r+j+d_x-d_y}(X)_0.$$

The étale and ℓ-adic cycle class maps

This expository section follows [117]. As per usual, X is a smooth projective variety over a field K of characteristic zero and the dimension of X is d. Let ℓ denote a fixed prime. For each n, r and ν we use the convention

$$H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) := H^n_{\mathrm{et}}(X_{\bar{K}}, \mu_{\ell^\nu}^{\otimes r})$$

where μ_{ℓ^ν} is the étale sheaf of ℓ^ν-roots of unity. There are natural multiplication-by-ℓ maps

$$H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^{\nu+1}\mathbb{Z}(r)) \longrightarrow H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^{\nu}\mathbb{Z}(r)) \tag{1.48}$$

induced by the natural quotient maps $\mathbb{Z}/\ell^{\nu+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/\ell^\nu\mathbb{Z}$, or the quotient maps $\mu_{\ell^{\nu+1}} \twoheadrightarrow \mu_{\ell^\nu}$ given by $\zeta \mapsto \zeta^\ell$. By taking the inverse limit, we obtain the ℓ-adic cohomology groups

$$H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r)) := \varprojlim H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$$
$$H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r)) := H^n_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The étale cycle class map is a homomorphism

$$\mathrm{cl}^{\ell,\nu}_{\mathrm{et}} : \mathrm{CH}^r(X) \longrightarrow H^{2r}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)).$$

It is defined for codimension r subvarieties of $X_{\bar{K}}$, and then extended by linearity to codimension r algebraic cycles. It can then be shown that the map on cycles factors through rational equivalence and hence induces a map on the Chow group. As in the previous section, we will content ourselves with describing $\mathrm{cl}^{\ell,\nu}_{\mathrm{et}}(Z)$ in the case where $Z \subset X_{\bar{K}}$ is a smooth subvariety of codimension r, referring to [117, Ch. VI §9] for the more general situation. For any sheaf $\mathcal{F}$ on X_{et}, we shall denote by $H^j_Z(X_{\bar{K}}, \mathcal{F})$ the étale cohomology of X with support on Z. Associated to the pair $(X_{\bar{K}}, X_{\bar{K}} \setminus Z)$ is a long exact cohomology sequence

$$\cdots \longrightarrow H^j_Z(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \xrightarrow{\iota^j_Z} H^j_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \longrightarrow H^j_{\mathrm{et}}(X_{\bar{K}} \setminus Z, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$$
$$\longrightarrow H^{j+1}_Z(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \longrightarrow \cdots$$

and by purity (since Z is smooth) there are canonical isomorphisms

$$P^j : H^{j-2r}_{\mathrm{et}}(Z, \mathbb{Z}/\ell^\nu\mathbb{Z}) \simeq H^j_Z(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$$

for all $j \geq 0$. In particular, taking $j = 2r$, we obtain a homomorphism

$$\iota_{Z,*} : H^0_{\text{et}}(Z, \mathbb{Z}/\ell^\nu\mathbb{Z}) \xrightarrow{P^{2r}} H^{2r}_Z(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \xrightarrow{\iota^{2r}_Z} H^{2r}_{\text{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$$

known as the Gysin map. Then we define $\text{cl}^{\ell,\nu}_{\text{et}}(Z) := \iota_{Z,*}(1)$.

The maps $\text{cl}^{\ell,\nu}_{\text{et}}$ are compatible with the maps (1.48) for ν varying and therefore give rise, by taking the inverse limit, to the ℓ-adic cycle class map

$$\text{cl}_\ell : \text{CH}^r(X) \longrightarrow H^{2r}_{\text{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r)). \tag{1.49}$$

We shall use the same name and notation for the map obtained when passing to $\mathbb{Q}_\ell$ coefficients

$$\text{cl}_\ell : \text{CH}^r(X) \longrightarrow H^{2r}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r)) = H^{2r}_{\text{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Since K has characteristic zero, we may fix an embedding $\sigma : \bar{K} \hookrightarrow \mathbb{C}$. Following [121], the following diagram commutes

$$\begin{array}{ccccc} \text{CH}^r(X) & \xrightarrow{\text{cl}_\ell} & H^{2r}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r)) & \xrightarrow[\sim]{\sigma_*} & H^{2r}_{\text{et}}(X_{\mathbb{C}}, \mathbb{Q}_\ell(r)) \\ \downarrow \sigma_* & & & & \downarrow \wr \\ \text{CH}^r(X_{\mathbb{C}}) & & \xrightarrow{\text{cl}} & & H^{2r}(X(\mathbb{C}), \mathbb{Q}(r)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \end{array}$$

where σ_* is an isomorphism on étale cohomology by [117, Ch. VI Corollary 4.3] and the vertical isomorphism is the comparison theorem [117, Ch. III Theorem 3.12] between étale cohomology and singular cohomology. In particular, this implies that $\ker(\text{cl}_\ell)$ is independent of the prime ℓ since $\ker(\text{cl}_\ell) = \ker(\text{cl}_B) = \mathcal{Z}^r(X)_0$.

1.4.4 Algebraic equivalence and Griffiths groups

We have seen in Section 1.4.1 the definition of rational equivalence on algebraic cycles in terms of divisors of functions on subvarieties. There is an alternative formulation which involves correspondences. Given $\Gamma \in \mathcal{Z}^r(\mathbb{P}^1_K \times X)$ such that the projection to $\mathbb{P}^1_K$ restricted to Γ is flat, there is an induced push-forward map on algebraic cycles

$$\Gamma_* : \mathcal{Z}^1(\mathbb{P}^1_K) \longrightarrow \mathcal{Z}^r(X)$$

defined by the same formula as (1.40). Note that $\mathcal{Z}^1(\mathbb{P}^1_K) = \mathrm{Div}(\mathbb{P}^1_K)$ consists of formal finite sums of points in $\mathbb{P}^1(\bar{K})$ with coefficients in $\mathbb{Z}$. Two codimension r cycles Z_1 and Z_2 are rationally equivalent if and only if there exists $\Gamma_1, \ldots, \Gamma_t \in \mathcal{Z}^r(\mathbb{P}^1_K \times X)$ flat over $\mathbb{P}^1_K$ such that

$$Z_1 - Z_2 = \sum_{i=1}^{t} (\Gamma_i)_*((0) - (\infty)).$$

If we replace $\mathbb{P}^1_K$ by any smooth projective connected curve C over K and $0, \infty \in \mathbb{P}^1_K$ by any two points $a, b \in C$, then we obtain the definition of algebraic equivalence. More precisely, we have the following definition.

Definition 1.18. Let $\mathcal{Z}^r(X)_{\mathrm{alg}}$ denote the subgroup of $\mathcal{Z}^r(X)$ generated by all subgroups $\Gamma_*(\mathcal{Z}^1(C)_0)$, where C is any smooth projective connected curve over K and $\Gamma \in \mathcal{Z}^r(C \times X)$ is flat over C. We write $Z_1 \sim_{\mathrm{alg}} Z_2$ and say that Z_1 and Z_2 are algebraically equivalent whenever $Z_1 - Z_2 \in \mathcal{Z}^r(X)_{\mathrm{alg}}$.

If C is a smooth projective connected curve over K, then we have $\mathcal{Z}^1(C) = \mathrm{Div}(C)$, and $\mathcal{Z}^1(C)_0 = \mathrm{Div}^0(C)$ is the subgroup of degree zero divisors. Therefore, if $Z_1, Z_2 \in \mathcal{Z}^r(X)$, then $Z_1 \sim_{\mathrm{alg}} Z_2$ if and only if there exist smooth projective connected curves $C_1, \ldots, C_t$ over K, cycles $\Gamma_i \in \mathcal{Z}^r(C_i \times X)$ flat over C_i for $i = 1, \ldots, t$, and points $a_i, b_i \in C_i(\bar{K})$, such that

$$Z_1 - Z_2 = \sum_{i=1}^{t} \Gamma_{i,*}((a_i) - (b_i)).$$

Example 1.2. If C is smooth projective connected curve over K and $a, b \in C(\bar{K})$, then $(a) \sim_{\mathrm{alg}} (b)$. Indeed, we can take $\Delta_C \in \mathcal{Z}^1(C \times C)$ to be the graph of the identity id_C, and then

$$\Delta_{C,*}((a)-(b)) = \mathrm{pr}_{2,*}(\Delta_C \cdot \mathrm{pr}_1^*((a)-(b)))$$
$$= \mathrm{pr}_{2,*}(\Delta \cdot (\{a\}\times C - \{b\}\times C)) = \mathrm{pr}_{2,*}((a,a)-(b,b)) = (a)-(b).$$

As a consequence, we have $\mathcal{Z}^1(C)_{\mathrm{alg}} = \mathcal{Z}^1(C)_0$.

By Definition 1.18 and the fact that correspondences preserve null-homologous cycles, we immediately see that cycles that are algebraically equivalent to zero are also null-homologous. We have defined three equivalence relations on algebraic cycles, which give rise to subgroups nested as follows:

$$\mathcal{Z}^r(X)_{\mathrm{rat}} \subset \mathcal{Z}^r(X)_{\mathrm{alg}} \subset \mathcal{Z}^r(X)_0 \subset \mathcal{Z}^r(X).$$

Modulo rational equivalence, this gives rise to a filtration of the Chow group

$$0 \subset \mathrm{CH}^r(X)_{\mathrm{alg}} \subset \mathrm{CH}^r(X)_0 \subset \mathrm{CH}^r(X).$$

The subgroup $\mathrm{CH}^r(X)_0$ is referred to as the r^{th} null-homologous Chow group as in Definition 1.17 and the 0-th graded piece satisfies, under Conjecture 1.3,

$$\mathrm{cl}_B \otimes \mathbb{Q} : \mathrm{CH}^r(X)_{\mathbb{Q}} / \mathrm{CH}^r(X)_{0,\mathbb{Q}} \simeq \mathrm{Hdg}^{2r}(X),$$

where the subscript $\mathbb{Q}$ denotes the tensor product with $\mathbb{Q}$.

Definition 1.19. The first graded piece of the above filtration is called the r-th Griffiths group

$$\mathrm{Gr}^r(X) := \mathrm{CH}^r(X)_0 / \mathrm{CH}^r(X)_{\mathrm{alg}} = \mathcal{Z}^r(X)_0 / \mathcal{Z}^r(X)_{\mathrm{alg}}. \tag{1.50}$$

We regard the Griffiths group as a functor from the category of field extensions of K

contained in $\mathbb{C}$ to the category of abelian groups given by the rule

$$F/K \quad \mapsto \quad \mathrm{Gr}^r(X)(F) := \{[Z] \in \mathrm{Gr}^r(X) \,:\, \sigma(Z) \sim_{\mathrm{alg}} Z, \quad \forall \sigma \in \mathrm{Aut}(\mathbb{C}/F)\}.$$

1.4.5 The Beilinson–Bloch conjecture

Let X denote a smooth projective variety of dimension d defined over a number field K. For any $0 \leq j \leq 2d$, consider the motive $h^j(X)$ attached to X, whose realisations correspond to the cohomology of X in degree j. The ℓ-adic realisations $H^j_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ of $h^j(X)$ give rise to a compatible family of ℓ-adic Galois representations. Following Section 1.1.4, one associates to this motive an L-function $L(h^j(X)/K, s)$ which converges on some right half-plane. When appropriately completed, this L-function should admit analytic continuation to the whole complex plane and satisfy a functional equation as formulated in Conjecture 1.9.

Bloch [28] has formulated what he describes as a "recurring fantasy". The same statement was formulated independently by Beilinson and is referred to as the Beilinson–Bloch conjecture.

Conjecture 1.4 (Beilinson–Bloch)**.** *The null-homologous Chow group* $\mathrm{CH}^r(X)_0(K)$ *is a finitely generated abelian group whose rank is given by*

$$\mathrm{rank}_{\mathbb{Z}}\, \mathrm{CH}^r(X)_0(K) = \mathrm{ord}_{s=r}\, L(h^{2r-1}(X)/K, s).$$

Remark 1.6. When $X = E$ is an elliptic curve over a number field, $\mathcal{Z}^1(E)_0 = \mathrm{Div}^0(E)$ and rational equivalence is linear equivalence on divisors. Hence $\mathrm{CH}^1(E) = \mathrm{Pic}(E)$ and $\mathrm{CH}^1(E)_0 = \mathrm{Pic}^0(E)$. Recall from Section 1.2 the identification $\mathrm{Pic}^0(E)(K) = E(K)$ which implies that $\mathrm{CH}^1(E)_0(K)$ is a finitely generated abelian group by the Mordell–Weil theorem. Moreover, the L-function $L(h^1(E)/K, s)$ is the Hasse–Weil L-function $L(E/K, s)$ of E over K. It follows that the statement of the Beilinson–Bloch conjecture in the case of elliptic curves reduces to the Birch and Swinnerton-Dyer conjecture 1.2. As a consequence, the

Beilinson–Bloch conjecture can be viewed as a higher dimensional generalisation of the Birch and Swinnerton-Dyer conjecture.

Suppose that $M = (X, p, 0)$ is a pure motive defined over the number field K. The idempotent correspondence p acts as a projector on cohomology groups and Chow groups. We shall write $\mathrm{CH}^j(M) := p\,\mathrm{CH}^j(X)$ and let $L(h^j(M)/K, s)$ be the L-function associated to the family of ℓ-adic realisations M_ℓ^j of M in degree j, as defined in Section 1.1.4. One is led naturally to formulate the Beilinson–Bloch conjecture for the motive M.

Conjecture 1.5.

$$\mathrm{rank}_{\mathbb{Z}}\,\mathrm{CH}^r(M)_0(K) = \mathrm{ord}_{s=r}\,L(h^{2r-1}(M)/K, s).$$

Consider the decomposition

$$H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Q}_\ell) = I \oplus M_\ell^{2r-1}.$$

Suppose that the Betti realisation M_B^{2r-1} has Hodge structure of type $(2r-1, 0) + (0, 2r-1)$ and that $h^{2r-1,0}(I) = 0$. In this case, Bloch makes a further conjecture which he calls the "son of recurring fantasy".

Conjecture 1.6.

$$\mathrm{rank}_{\mathbb{Z}}\,\mathrm{Gr}^r(X)(K) = \mathrm{ord}_{s=r}\,L(h^{2r-1}(M)/K, s).$$

The Beilinson–Bloch conjectures remain open today, but there has been gathering evidence for their truth in special cases, see for example [14, 28, 32, 130].

1.5 Abel–Jacobi maps

We define three types of Abel–Jacobi maps: the complex Abel–Jacobi map, the Bloch map, and the ℓ-adic étale Abel–Jacobi map. We review some of their key features and explain the relationships between them.

1.5.1 The complex Abel–Jacobi map

Let C be a smooth projective curve over a number field K. Recall the Abel–Jacobi isomorphism

$$\mathrm{AJ}_C : \mathrm{CH}^1(C)_0(\mathbb{C}) \xrightarrow{\sim} J^1(C/\mathbb{C}) := \frac{H^0(C(\mathbb{C}), \Omega^1_C)^\vee}{\mathrm{Im}\, H_1(C(\mathbb{C}), \mathbb{Z})}$$

given by the familiar integration formula, for D a degree zero divisor,

$$\mathrm{AJ}_C(D)(\alpha) := \int_{\partial^{-1}(D)} \alpha \qquad \text{for } \alpha \in H^0(C(\mathbb{C}), \Omega^1_C),$$

where $\partial^{-1}(D)$ denotes any continuous 1-chain in $C(\mathbb{C})$ whose image under the boundary map ∂ is D.

Remark 1.7. In the case when C is an elliptic curve E, using the identification of E with $\mathrm{Pic}^0(E)$ (after fixing as base point the origin O_E), the Abel–Jacobi isomorphism

$$\mathrm{AJ}_E : E(\mathbb{C}) \xrightarrow{\sim} J^1(E/\mathbb{C}) := \frac{H^0(E(\mathbb{C}), \Omega^1_E)^\vee}{\mathrm{Im}\, H_1(E(\mathbb{C}), \mathbb{Z})}$$

is given by

$$\mathrm{AJ}_E(P)(\alpha) := \int_{O_E}^{P} \alpha \qquad \text{for } \alpha \in H^0(E(\mathbb{C}), \Omega^1_E).$$

Since E has genus 1 by definition, the complex vector space $H^0(E(\mathbb{C}), \Omega^1_E)$ is 1-dimensional and the lattice $\mathrm{Im}\, H_1(E(\mathbb{C}), \mathbb{Z})$ is the period lattice $\Lambda_E \subset \mathbb{C}$ of E. Hence the complex Abel–Jacobi map is the familiar complex uniformisation map of E which identifies $E(\mathbb{C})$ with the complex torus $\mathbb{C}/\Lambda_E$.

The g-dimensional complex torus $J^1(C/\mathbb{C})$ is called the Jacobian of C and will often be denoted $\mathrm{Jac}(C)(\mathbb{C})$. The Abel–Jacobi isomorphism identifies $\mathrm{Jac}(C)(\mathbb{C})$ with the complex points of $\mathrm{Pic}^0_{C/K}$ and endows it with the structure of an abelian variety defined over K which we shall denote $\mathrm{Jac}(C)$.

Abel–Jacobi maps for algebraic varieties

Let X denote a smooth projective variety of dimension d defined over a number field K. The complex Abel–Jacobi map admits a higher dimensional analogue

$$\mathrm{AJ}_X^r : \mathrm{CH}^r(X)_0(\mathbb{C}) \longrightarrow J^r(X/\mathbb{C}) := \frac{\mathrm{Fil}^{d-r+1} H_{\mathrm{dR}}^{2d-2r+1}(X/\mathbb{C})^\vee}{\mathrm{Im}\, H_{2d-2r+1}(X(\mathbb{C}), \mathbb{Z})}. \tag{1.51}$$

Originally considered by Griffiths, this map is defined by the formula

$$\mathrm{AJ}_X^r(Z)(\alpha) = \int_{\partial^{-1}(Z)} \alpha \qquad \text{for } \alpha \in \mathrm{Fil}^{d-r+1} H_{\mathrm{dR}}^{2d-2r+1}(X/\mathbb{C}),$$

where $\partial^{-1}(Z)$ denotes any continuous $(2d-2r+1)$-chain in $X(\mathbb{C})$ whose image under the boundary map ∂ is Z.

The complex torus $J^r(X/\mathbb{C})$ is called the r-th intermediate Jacobian of X and Poincaré duality induces an isomorphism

$$J^r(X/\mathbb{C}) \simeq H^{2r-1}(X(\mathbb{C}), \mathbb{C})/(\mathrm{Fil}^r H_{\mathrm{dR}}^{2r-1}(X/\mathbb{C}) \oplus \mathrm{Im}\, H^{2r-1}(X(\mathbb{C}), \mathbb{Z})). \tag{1.52}$$

Remark 1.8. In general, when r is not 1 or d these complex tori do not have the structure of abelian varieties. When $r = 1$, $\mathrm{CH}^1(X)_0$ is the connected component of the identity in the Picard scheme of X, and Abel's theorem implies that the Abel–Jacobi map is an isomorphism, hence $J^1(X)$ admits the structure of an abelian variety. When $r = d$, $J^d(X/\mathbb{C})$ is an abelian variety by [147, Corollary 12.12], called the Albanese variety of X.

Transcendental Abel–Jacobi maps

Consider C a smooth projective connected curve over K and $\Gamma \in \mathrm{CH}^r(C \times X)$. Recall the map $\Gamma_* : \mathrm{CH}^1(C)_0 \longrightarrow \mathrm{CH}^r(X)_0$ and compose it with AJ^r_X in order to obtain a map

$$\psi_{C,\Gamma} : \mathrm{Jac}(C)(\mathbb{C}) \longrightarrow J^r(X/\mathbb{C}), \qquad (a) - (b) \mapsto \mathrm{AJ}^r_X(\Gamma_*((a) - (b)))$$

where we identified $\mathrm{CH}^1(C)_0 = \mathrm{Jac}(C)$ using the isomorphism AJ_C. This is equal to the map of complex tori which is induced by the morphism

$$[\Gamma] : H^1_B(C, \mathbb{Z}) \longrightarrow H^{2r-1}_B(X, \mathbb{Z}), \tag{1.53}$$

given by the Künneth component $[\Gamma]^{1,2r-1} \in H^1_B(C, \mathbb{Z}) \otimes H^{2r-1}_B(X, \mathbb{Z}) \subset H^{2r}_B(C \times X, \mathbb{Z})$ of $\mathrm{cl}_B(\Gamma)$. See [147, Theorem 12.17]. Here, using Poincaré duality, we make the identification

$$H^1_B(C, \mathbb{Z}) \otimes H^{2r-1}_B(X, \mathbb{Z}) = H^1_B(C, \mathbb{Z})^\vee \otimes H^{2r-1}_B(X, \mathbb{Z}) = \mathrm{Hom}(H^1_B(C, \mathbb{Z}), H^{2r-1}_B(X, \mathbb{Z})).$$

Since $\mathrm{cl}_B(\Gamma)$ is a Hodge class by Proposition 1.9, the corresponding morphism (1.53) is a morphism of Hodge structures of bidegree $(r-1, r-1)$ by [147, Lemma 11.41], and therefore does indeed induce a map between intermediate Jacobians as can be seen from the description (1.52).

Proposition 1.10. *The image of the map (1.53) is contained in $H^{r,r-1}(X) \oplus H^{r-1,r}(X)$. In particular, the image of $\psi_{C,\Gamma}$ is a complex subtorus of $J^r(X/\mathbb{C})$ whose tangent space at 0 is contained in $H^{r-1,r}(X)$.*

Proof. This is a special case of the more general [147, Corollary 12.19]. The Hodge structure $H^1_B(C, \mathbb{Z})$ is of type $(1,0)+(0,1)$ and $[\Gamma]$ is of bidegree $(r-1, r-1)$, hence the image of $[\Gamma]$ is contained in $H^{r,r-1}(X) \oplus H^{r-1,r}(X)$. Following the description (1.52), we identify the tangent space at 0 of $J^r(X/\mathbb{C})$ with the complex vector space $H^{2r-1}(X(\mathbb{C}), \mathbb{C}) / \mathrm{Fil}^r H^{2r-1}_{\mathrm{dR}}(X/\mathbb{C})$

which naturally contains $H^{r-1,r}(X)$, and the result follows. □

Definition 1.20. Let $J^r(X/\mathbb{C})_{\text{alg}} \subset J^r(X/\mathbb{C})$ denote the largest complex subtorus of $J^r(X/\mathbb{C})$ whose tangent space at 0 is contained in $H^{r-1,r}(X)$.

Proposition 1.11. *The image of* $\mathrm{CH}^r(X)_{\text{alg}}$ *under the complex Abel–Jacobi map* AJ^r_X *is contained in* $J^r(X)_{\text{alg}}$.

Proof. This is an immediate consequence of Definition 1.18 of algebraic equivalence and Proposition 1.10. □

As a consequence of this proposition, we can define the transcendental Abel–Jacobi map from the Griffiths group to the transcendental part of the intermediate Jacobian

$$\mathrm{AJ}^r_{X,\text{tr}} : \mathrm{Gr}^r(X) \longrightarrow J^r(X/\mathbb{C})_{\text{tr}} := J^r(X/\mathbb{C})/J^r(X/\mathbb{C})_{\text{alg}} \tag{1.54}$$

as the factorisation of AJ^r_X.

Remark 1.9. When $r = 1$, we have $J^1(X/\mathbb{C})_{\text{alg}} = J^1(X/\mathbb{C})$ by definition, so $\mathrm{AJ}^1_{X,\text{tr}} = 0$. Let D be a degree zero divisor on X, i.e., a null-homologous algebraic cycle of codimension 1, and write $D = D_1 - D_2$ as the difference of two effective divisors. The divisors D_1 and D_2 lie in the same connected component of $\mathrm{Pic}(X)$ and one can choose a curve connecting these two points. This curve can be taken to be algebraic by algebraicity of the Picard scheme. The universal divisor restricted to this curve gives an algebraic family through D_1 and D_2, showing that their difference D is algebraically trivial. Hence for divisors on a smooth projective variety, homological equivalence and algebraic equivalence coincide and $\mathrm{Gr}^1(X) = 0$. As a consequence, $\mathrm{AJ}^1_{X,\text{tr}}$ is the trivial map.

1.5.2 The Bloch map

Let X denote a smooth projective variety of dimension d defined over a number field K and let ℓ denote a prime. For each n, r and ν, there are natural maps

$$H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \longrightarrow H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^{\nu+1}\mathbb{Z}(r)) \tag{1.55}$$

induced by the natural inclusion maps $\mathbb{Z}/\ell^\nu\mathbb{Z} \hookrightarrow \mathbb{Z}/\ell^{\nu+1}\mathbb{Z}$ given by $m \mapsto \ell m$, or the natural inclusion maps $\mu_{\ell^\nu} \hookrightarrow \mu_{\ell^{\nu+1}}$. By taking the direct limit, we obtain the cohomology groups of X with ℓ-torsion coefficients:

$$H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) := \varinjlim H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)). \tag{1.56}$$

Viewing $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ as a torsion étale sheaf on X, there is a natural isomorphism

$$H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Q}_\ell/\mathbb{Z}_\ell} \mathbb{Q}_\ell/\mathbb{Z}_\ell(r) \simeq H^n_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) \tag{1.57}$$

where the right hand side cohomology group is defined by (1.56).

Let $\text{CH}^r(X)(\ell) := \text{CH}^r(X)[\ell^\infty]$ denote the ℓ-power torsion subgroup of the Chow group. Bloch [27] has defined a map

$$\lambda^r_\ell : \text{CH}^r(X)(\ell) \longrightarrow H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r))$$

which, when restricted to null-homologous cycles, can be regarded as an arithmetic avatar of the complex Abel–Jacobi map on torsion.

Sketch of construction

Let $\mathbf{H}^q(\mu_{\ell^\nu}^{\otimes r})$ denote the Zariski sheaf on $X_{\bar{K}}$ associated to the presheaf $U \mapsto H^q_{\text{et}}(U, \mu_{\ell^\nu}^{\otimes r})$. If $\pi : (X_{\bar{K}})_{\text{Zar}} \longrightarrow (X_{\bar{K}})_{\text{et}}$ denotes the natural morphism from the Zariski site to the étale site of $X_{\bar{K}}$, then $\mathbf{H}^q(\mu_{\ell^\nu}^{\otimes r}) := R^q\pi_*\mu_{\ell^\nu}^{\otimes r}$. The Leray spectral sequence of the morphisms of sites $(X_{\bar{K}})_{\mathrm{Zar}}\xrightarrow{\pi}(X_{\bar{K}})_{\mathrm{et}}\longrightarrow\mathrm{Spec}(\bar{K})$ is

$$E_2^{p,q} = H^p(X_{\bar{K}}, \mathbf{H}^q(\mu_{\ell^\nu}^{\otimes r})) \implies H_{\mathrm{et}}^{p+q}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)). \tag{1.58}$$

The main theorem of [30] gives an acyclic resolution [27, (1.3)] of $\mathbf{H}^q(\mu_{\ell^\nu}^{\otimes r})$ which computes its Zariski cohomology groups $E_2^{\bullet,q}$. From the particular shape of this resolution, one derives two important consequences, the first one being that $E_2^{p,q} = 0$ for $p > q$, which simplifies the shape of the spectral sequence (1.58). As a corollary, we obtain the following.

Proposition 1.12. *There is a map*

$$H^{r-1}(X_{\bar{K}}, \mathbf{H}^r(\mu_{\ell^\nu}^{\otimes r}))\longrightarrow H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \tag{1.59}$$

obtained as the boundary map coming from the spectral sequence (1.58).

Proof. This is [27, Corollary 1.4] and is standard given the shape of the spectral sequence. Nevertheless, we review the construction briefly. Since $E_2^{p,q} = 0$ whenever $p > q$, we have in particular that $E_2^{p,q} = 0 = E_\infty^{p,q}$ whenever $p + q = 2r - 1$ and $p \geq r$. It follows that $\mathrm{Fil}^p H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) = 0$ for all $p \geq r$ where Fil denotes the filtration of $H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$ induced by the spectral sequence. Next, since $E_2^{r+1,r-1} = 0$, the second page around $E_2^{r-1,r}$ is of the shape

$$E_2^{r-3,r+1}\xrightarrow{d_2}E_2^{r-1,r}\longrightarrow 0,$$

where d_2 denotes the second page differential. It follows that there is a natural quotient map $E_2^{r-1,r} \twoheadrightarrow E_\infty^{r-1,r} = \mathrm{gr}^{r-1} H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) = \mathrm{Fil}^{r-1} H_{\mathrm{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))$, where gr stands for the graded piece of the filtration. The boundary map (1.59) is now given by the composition

$$H^{r-1}(X_{\bar{K}}, \mathbf{H}^r(\mu_{\ell^\nu}^{\otimes r})) = E_2^{r-1,r} \twoheadrightarrow \operatorname{Fil}^{r-1} H_{\text{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) \hookrightarrow H_{\text{et}}^{2r-1}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)).$$

□

Recall from Section 1.4.1 the definition of rational equivalence and the Chow group; we have the defining exact sequence

$$\bigoplus_{V^{r-1} \subset X_{\bar{K}}} R(V)^\times \xrightarrow{\partial} \mathcal{Z}^r(X) \longrightarrow \mathrm{CH}^r(X) \longrightarrow 0, \tag{1.60}$$

where the direct sum is taken over all subvarieties of $X_{\bar{K}}$ of codimension $r-1$, and the map ∂ sends a function $f \in R(V)^\times$ to its divisor $\operatorname{div}(f) \in \mathcal{Z}^r(X)$. By Definition 1.15, the image of ∂ is $\mathcal{Z}^r(X)_{\text{rat}}$. One can consider the reduction of ∂ modulo ℓ^ν and obtain the map

$$\partial_{\ell^\nu} : \bigoplus_{V^{r-1} \subset X_{\bar{K}}} R(V)^\times/(R(V)^\times)^{\ell^\nu} \longrightarrow \mathcal{Z}^r(X) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^\nu\mathbb{Z}.$$

The second consequence of the explicit acyclic resolution [27, (1.3)] is that there is a surjection [27, Corollary 1.5]

$$\ker \partial_{\ell^\nu} \twoheadrightarrow H^{r-1}(X_{\bar{K}}, \mathbf{H}^r(\mu_{\ell^\nu}^{\otimes r})). \tag{1.61}$$

Consider the following commutative diagram of groups with exact rows [27, (2.1)]

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_{V^{r-1}} R(V)^\times/\bar{K}^\times & \xrightarrow{(\cdot)^{\ell^\nu}} & \bigoplus_{V^{r-1}} R(V)^\times/\bar{K}^\times & \longrightarrow & \bigoplus_{V^{r-1}} R(V)^\times/(R(V)^\times)^{\ell^\nu} & \longrightarrow & 0 \\ & & \downarrow \partial & & \downarrow \partial & & \downarrow \partial_{\ell^\nu} & & \\ 0 & \longrightarrow & \mathcal{Z}^r(X) & \xrightarrow{\ell^\nu} & \mathcal{Z}^r(X) & \longrightarrow & \mathcal{Z}^r(X) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^\nu\mathbb{Z} & \longrightarrow & 0. \end{array} \tag{1.62}$$

We obtain a commutative diagram of groups with exact rows [1, A.11]

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{\ker\partial}{\ell^\nu\ker\partial} & \longrightarrow & \ker\partial_{\ell^\nu} & \longrightarrow & \mathrm{CH}^r(X)[\ell^\nu] & \longrightarrow & 0 \\
 & & \downarrow & \searrow^{\rho_{\ell^\nu}} & \downarrow{\scriptstyle (1.61)} & & \downarrow & & \\
 & & & & H^{r-1}(X_{\bar{K}}, \mathbf{H}^r(\mu_{\ell^\nu}^{\otimes r})) & & & & \\
 & & & & \downarrow{\scriptstyle (1.59)} & & & & \\
0 & \longrightarrow & \delta_{\ell^\nu} & \longrightarrow & H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) & \longrightarrow & H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r))/\delta_{\ell^\nu} & \longrightarrow & 0
\end{array}
\tag{1.63}
$$

where the top row results from applying the Snake lemma to the previous diagram (1.62) and recalling the exact sequence (1.60). This diagram (1.63) is an extended version of the diagram [27, 2.2]. Following [1], δ_{ℓ^ν} denotes the image of $\ker\partial/\ell^\nu\ker\partial$ under the map ρ_{ℓ^ν} defined by commutativity of the diagram. The lower row is then just the natural short exact sequence obtained by quotienting by the subgroup δ_{ℓ^ν}.

Following Bloch, one can define the map

$$\rho : \ker\partial \longrightarrow \varprojlim(\ker\partial/\ell^\nu\ker\partial) \xrightarrow{\varprojlim \rho_{\ell^\nu}} \varprojlim H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}/\ell^\nu\mathbb{Z}(r)) = H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))$$

by compatibility of ρ_{ℓ^ν} with the maps (1.48) when ν varies.

Lemma 1.1. *The image of ρ is torsion and so is the image of the map $\varprojlim \rho_{\ell^\nu}$.*

Proof. The first assertion is Bloch's key lemma [27, Lemma 2.4] and the second assertion follows from the first as explained in [1, Lemma A.5]. In his proof, Bloch uses the Weil conjectures as proved by Deligne [57] via specialisation to finite fields. □

Since taking direct limits is an exact functor, from diagram (1.63) we obtain the following commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \varinjlim \left(\frac{\ker \partial}{\ell^\nu \ker \partial}\right) & \longrightarrow & \varinjlim \ker \partial_{\ell^\nu} & \longrightarrow & \mathrm{CH}^r(X)(\ell) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle (1.61)} & & & & \\
 & & \downarrow \quad \searrow{\scriptstyle \varinjlim \rho_{\ell^\nu}} & & \varinjlim H^{r-1}(X_{\bar{K}}, \mathbf{H}^r(\mu_{\ell^\nu}^{\otimes r})) & & \downarrow & & \\
 & & & & \downarrow{\scriptstyle (1.59)} & & & & \\
0 & \longrightarrow & \varinjlim \delta_{\ell^\nu} & \longrightarrow & H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) & \longrightarrow & \frac{H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r))}{\varinjlim \delta_{\ell^\nu}} & \longrightarrow & 0.
\end{array}
\tag{1.64}
$$

Lemma 1.2. *The map*

$$\varinjlim \rho_{\ell^\nu} : \varinjlim \left(\frac{\ker \partial}{\ell^\nu \ker \partial}\right) \longrightarrow H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r))$$

is the zero map.

Proof. This is stated in [27, p. 112] as a consequence of Lemma 1.1. The detailed proof can be found in [1, Lemma A.8]. □

Definition 1.21. The Bloch map in codimension r

$$\lambda^r_\ell : \mathrm{CH}^r(X)(\ell) \longrightarrow H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r))$$

is the negative of the map obtained from diagram (1.64) and Lemma 1.2.

As explained by Bloch, the minus sign is there for reasons of compatibility in the case $r = 1$ with the natural map arising from the Kummer sequence. See Proposition 1.16 below.

Properties

Following [27] and [1, Appendix A], we now collect some of the properties of the Bloch map. Another brief overview of some of these properties is provided in [129].

Proposition 1.13. *The Bloch map is functorial with respect to flat pull-back, proper push-forward and actions of correspondences.*

Proof. Functoriality for pull-back and push-forward is [27, Proposition 3.3]. The statement for correspondences is [27, Proposition 3.5] and follows from the compatibility of the Bloch map with products [27, Proposition 3.4]; if $Z \in \mathrm{CH}^j(X)$ and $\Gamma \in \mathrm{CH}^r(X)(\ell)$, then

$$\lambda_\ell^{r+j}(\Gamma \cdot Z) = \lambda_\ell^r(\Gamma) \cup \mathrm{cl}_\ell(Z)$$

where $\cup$ denotes the cup product on étale cohomology induced by the bilinear map

$$\mathbb{Q}_\ell/\mathbb{Z}_\ell(r) \times \mathbb{Z}_\ell(j) \longrightarrow \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+j).$$

□

Proposition 1.14. *The Bloch map is* $\mathrm{Gal}(\bar{K}/K)$*-equivariant.*

Proof. This follows from functoriality for pull-back and push-forward as explained in the proof of [1, Proposition A.22]. □

Proposition 1.15. *The Bloch map is compatible with specialisation.*

Proof. This is [27, Proposition 3.8]. □

Proposition 1.16. *The Bloch map λ_ℓ^1 in codimension* 1 *is the natural isomorphism arising from the Kummer sequence.*

Proof. This is [27, Proposition 3.6]. □

Proposition 1.17. *The Bloch map λ_ℓ^2 in codimension* 2 *is injective.*

Proof. This is [1, Proposition A.27] and is originally due to [116]. □

Proposition 1.18. *The Bloch map λ_ℓ^d in codimension $d = \dim X$ is an isomorphism.*

Proof. The proof is presented in [27] and attributed to Roitman. □

From the long exact sequence in cohomology associated to the short exact sequence

$$0 \longrightarrow \mathbb{Z}_\ell \longrightarrow \mathbb{Q}_\ell \longrightarrow \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow 0 \tag{1.65}$$

we obtain a connecting homomorphism

$$\delta : H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) \longrightarrow H^{2r}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r)).$$

The following proposition says that the Bloch map λ^r_ℓ is compatible with the ℓ-adic cycle class map (1.49).

Proposition 1.19. *Up to sign, the map $\delta \circ \lambda^r_\ell$ is equal to the cycle class map cl_ℓ.*

Proof. This is [39, Corollary 4]. □

Corollary 1.3. *When restricted to null-homologous cycles, the image of the Bloch map λ^r_ℓ lies in $D^r_\ell(X_{\bar{K}}) := H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r))/H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))$, hence we obtain a map*

$$\lambda^r_\ell : \mathrm{CH}^r(X)_0(\ell) \longrightarrow D^r_\ell(X_{\bar{K}}) \subset H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)). \tag{1.66}$$

Proof. This is a direct consequence of the previous proposition using the long exact sequence in cohomology coming from the short exact sequence (1.65). □

Remark 1.10. The notation $D^r_\ell(X_{\bar{K}})$ is borrowed from [129].

Comparison with the complex Abel–Jacobi map

We now make precise the claim that the Bloch map, when restricted to null-homologous cycles, can be viewed as an arithmetic avatar of the complex Abel–Jacobi map introduced in Section 1.5.1. This link between the complex Abel–Jacobi map and the Bloch will prove to be crucial in Chapter 2.

Observe that we have an isomorphism of $\mathbb{R}$-vector spaces

$$H^{2r-1}(X(\mathbb{C}),\mathbb{R}) \simeq H^{2r-1}(X(\mathbb{C}),\mathbb{C})/\operatorname{Fil}^r H^{2r-1}_{\mathrm{dR}}(X/\mathbb{C}), \tag{1.67}$$

hence by (1.52) we have

$$J^r(X/\mathbb{C}) \simeq H^{2r-1}(X(\mathbb{C}),\mathbb{R})/\operatorname{Im} H^{2r-1}(X(\mathbb{C}),\mathbb{Z}),$$

and we may identify

$$J^r(X/\mathbb{C})_{\mathrm{tors}} \simeq H^{2r-1}(X(\mathbb{C}),\mathbb{Q})/\operatorname{Im} H^{2r-1}(X(\mathbb{C}),\mathbb{Z}). \tag{1.68}$$

From the long exact sequence in singular cohomology associated to the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{1.69}$$

we deduce a short exact sequence

$$0 \longrightarrow J^r(X/\mathbb{C})_{\mathrm{tors}} \xrightarrow{u} H^{2r-1}(X(\mathbb{C}),\mathbb{Q}/\mathbb{Z}) \longrightarrow H^{2r}(X(\mathbb{C}),\mathbb{Z})_{\mathrm{tors}} \longrightarrow 0. \tag{1.70}$$

Note that $H^{2r}(X(\mathbb{C}),\mathbb{Z})$ is a group of finite type and thus its torsion subgroup is finite. We have thus identified $J^r(X/\mathbb{C})_{\mathrm{tors}}$ up to a finite group with $H^{2r-1}(X(\mathbb{C}),\mathbb{Q}/\mathbb{Z})$.

Composing the complex Abel–Jacobi map (1.51) restricted to torsion with u yields a map

$$u \circ \mathrm{AJ}^r_X : \mathrm{CH}^r(X)(\mathbb{C})_0(\ell) \longrightarrow H^{2r-1}(X(\mathbb{C}),\mathbb{Q}_\ell/\mathbb{Z}_\ell). \tag{1.71}$$

For each natural number ν, we have a sequence of isomorphisms

$$H^{2r-1}_{\mathrm{et}}(X_{\bar{K}},\mu_{\ell^\nu}^{\otimes r}) \overset{\sigma_*}{\simeq} H^{2r-1}_{\mathrm{et}}(X_{\mathbb{C}},\mu_{\ell^\nu}^{\otimes r}) \simeq H^{2r-1}(X(\mathbb{C}),\mu_{\ell^\nu}^{\otimes r}). \tag{1.72}$$

For the first isomorphism, apply [117, VI Corollary 4.3] with respect to the fixed complex embedding $\sigma : \bar{K} \hookrightarrow \mathbb{C}$. The second isomorphism is an application of [117, III Theorem 3.12]. Taking direct limits, we obtain a sequence of isomorphisms

$$H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) \overset{\sigma_*}{\simeq} H^{2r-1}_{\text{et}}(X_{\mathbb{C}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) \simeq H^{2r-1}(X(\mathbb{C}), \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)). \tag{1.73}$$

Proposition 1.20. *If we identify $\mathbb{Q}_\ell/\mathbb{Z}_\ell \simeq \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)$ by taking $e^{\frac{2\pi i}{\ell^\nu}}$ as the generator of the ℓ^ν-th roots of 1, then the diagram*

$$\begin{array}{ccc} \mathrm{CH}^r(X)_0(\ell) & \xrightarrow{\lambda^r_\ell} & H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r)) \\ \downarrow \sigma_* & & \wr \downarrow (1.73) \\ \mathrm{CH}^r(X_{\mathbb{C}})_0(\ell) & \xrightarrow{u \circ \mathrm{AJ}^r_X} & H^{2r-1}(X(\mathbb{C}), \mathbb{Q}_\ell/\mathbb{Z}_\ell) \end{array} \tag{1.74}$$

commutes.

Proof. This is [27, Proposition 3.7]. □

1.5.3 The ℓ-adic étale Abel–Jacobi map

We give an alternative description of the Bloch map restricted to null-homologous cycles (1.66) in terms of the perhaps more classic ℓ-adic étale Abel–Jacobi map first considered by Bloch in [28]:

$$\mathrm{AJ}^r_{X,\text{et}} : \mathrm{CH}^r(X)_0(K) \longrightarrow H^1(K, H^{2r-1}_{\text{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))). \tag{1.75}$$

The cohomology appearing on the right hand side is continuous Galois cohomology of the group $G_K := \mathrm{Gal}(\bar{K}/K)$.

We briefly review Bloch's construction. The variety X comes equipped with a cycle class map

$$\mathrm{cl}_{X_K,\ell} : \mathrm{CH}^r(X)(K) \longrightarrow H^{2r}_{\text{et}}(X_K, \mathbb{Z}_\ell(r)) \tag{1.76}$$

from the Chow group to the (continuous in the sense of [93]) arithmetic étale cohomology.

This map is due to Grothendieck and coincides with the usual cycle class map cl_ℓ (1.49) after passage to $\bar{K}$. The Hochschild–Serre spectral sequence

$$E_2^{p,q} = H^p(K, H^q_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r)) \implies H^{p+q}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \tag{1.77}$$

is obtained from the Leray spectral sequence of the structure morphism $X_K \longrightarrow \mathrm{Spec}(K)$ using proper base change. It degenerates at E_2, hence there are isomorphisms

$$E_\infty^{j,m-j} = \mathrm{gr}^j\, H^m_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \xrightarrow{\sim} H^j(K, H^{m-j}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r)) = E_2^{j,m-j}. \tag{1.78}$$

Using (1.78) in the case $j = 0, m = 2r$, one obtains the composite map

$$\mathrm{cl}_\ell : \mathrm{CH}^r(X)(K) \xrightarrow{(1.76)} H^{2r}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \twoheadrightarrow \mathrm{gr}^0\, H^{2r}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \xrightarrow{(1.78)} (H^{2r}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r))^{G_K} \tag{1.79}$$

which corresponds to the cycle class map (1.49).

Since $\mathrm{CH}^r(X)_0(K) = \ker \mathrm{cl}_\ell$, we see that the image of $\mathrm{CH}^r(X)_0(K)$ under (1.76) lands in $\mathrm{Fil}^1\, H^{2r}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r))$. Using (1.78) in the case $j = 1, m = 2r$, we may form the composite map

$$\mathrm{CH}^r(X)_0(K) \xrightarrow{(1.76)} \mathrm{Fil}^1\, H^{2r}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \twoheadrightarrow \mathrm{gr}^1\, H^{2r}_{\mathrm{et}}(X_K, \mathbb{Z}_\ell(r)) \xrightarrow{(1.78)} H^1(K, H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r)). \tag{1.80}$$

By definition this map is (1.75) and is called the ℓ-adic étale Abel–Jacobi map of X over K in codimension r.

Remark 1.11. There is an alternative description of $\mathrm{AJ}^r_{X,\mathrm{et}}$ in terms of extensions using the identification

$$H^1(K, H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r)) = \mathrm{Ext}^1_{\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)}(\mathbb{Q}_\ell, H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell)(r)) \tag{1.81}$$

where $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ denotes the category of finite-dimensional continuous $\mathbb{Q}_\ell$-representations of G_K. For details about this description we refer to [93, Lemma 9.4].

Recall the notation $D^r_\ell(X_{\bar{K}}) := H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r))/H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))$ of Corollary 1.3. The short exact sequence of Galois modules

$$0 \longrightarrow H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))/\operatorname{tors} \longrightarrow H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Q}_\ell(r)) \longrightarrow D^r_\ell(X_{\bar{K}}) \longrightarrow 0$$

gives rise to a long exact sequence of continuous Galois cohomology. The first connecting homomorphism yields a surjective map

$$D^r_\ell(X_{\bar{K}})^{G_K} \twoheadrightarrow H^1(K, H^{2r-1}_{\mathrm{et}}(X_{\bar{K}}, \mathbb{Z}_\ell(r))/\operatorname{tors})_{\mathrm{tors}} \tag{1.82}$$

which can be shown to be an isomorphism [38, Theorem 1.5]. Composing $\mathrm{AJ}^r_{X,\mathrm{et}}$ restricted to torsion with the inverse of (1.82) yields a map

$$\alpha^r_{X,K} : \mathrm{CH}^r(X)_0(K)(\ell) \longrightarrow D^r_\ell(X_{\bar{K}})^{G_K}.$$

Passing to the limit over finite extensions of K yields a map

$$\alpha^r : \mathrm{CH}^r(X)_0(\ell) \longrightarrow D^r_\ell(X_{\bar{K}}) \tag{1.83}$$

Proposition 1.21. *The Bloch map in codimension r restricted to null-homologous cycles* (1.66) *agrees up to a sign with the map* (1.83)*.*

Proof. This is [129, Theorem 1.2.7], see references in the proof. □

Chapter 2

Generalised Heegner cycles

This chapter is a reformatted version of the article [11] and all results presented herein are joint with Massimo Bertolini, Henri Darmon and Kartik Prasanna.

Generalised Heegner cycles were introduced in [12] as a variant of Heegner cycles on Kuga–Sato varieties. The first main result of this chapter is a formula for the image of these cycles under the complex Abel–Jacobi map of Section 1.5.1 in terms of explicit line integrals of modular forms on the complex upper half-plane. The second main theorem uses this formula to show that the Chow group and the Griffiths group, defined in Sections 1.4.1 and 1.4.4, of the product of a Kuga–Sato variety with an elliptic curve with complex multiplication are not finitely generated. See Sections 1.2.4 and 1.3.2 for details about Kuga–Sato varieties and the theory of complex multiplication. More precisely, it is shown that the subgroup generated by the image of generalised Heegner cycles has infinite rank in the group of null-homologous cycles modulo both rational and algebraic equivalence.

Introduction

In their article [12], Bertolini, Darmon and Prasanna introduced a distinguished collection of null-homologous, codimension $r+1$ cycles on the $(2r+1)$-dimensional variety

$$X_r := W_r \times A^r,$$

where W_r is the Kuga–Sato variety of Definition 1.7 obtained from the r-fold fibre power (1.27) of the universal elliptic curve over the modular curve $X_1(N)$, and A is a fixed elliptic curve with complex multiplication, see Definition 1.12. Referred to as generalised Heegner cycles in [12] because of their close affinity with the Heegner cycles on Kuga–Sato varieties studied in [128], [120] and [155], they are indexed by isogenies $\varphi : A \longrightarrow A'$. The cycle Δ_φ labeled by φ is supported on the fibre $(A')^r \times A^r$ above a point of $X_1(N)$ attached to A', and is equal, roughly speaking, to the r-fold self-product of the graph of φ.

One may consider the images of the Δ_φ under the p-adic syntomic Abel–Jacobi map

$$\mathrm{AJ}_p : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}_p) \longrightarrow J^{r+1}(X_r/\mathbb{C}_p) := \mathrm{Fil}^{r+1} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C}_p)^\vee \tag{2.1}$$

whose domain is the Chow group of null-homologous codimension $r+1$ cycles on X_r over $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}}}_p$ and whose target is the $\mathbb{C}_p$-linear dual of the middle step in the de Rham cohomology $H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C}_p)$ relative to the Hodge filtration. The main result of [12] is a formula relating $\mathrm{AJ}_p(\Delta_\varphi)$ to special values of certain p-adic Rankin L-series. An analogous formula for the p-adic heights of the same cycles was later obtained in [137]. A key ingredient in [12], made explicit in Section 3 of *loc.cit.*, is a description of the relevant p-adic Abel–Jacobi images in terms of p-adic integration of higher weight modular forms, à la Coleman.

The goal of the present chapter is to give an analogous description of the image of the cycles Δ_φ under the complex Abel–Jacobi map (1.51)

$$\mathrm{AJ}_{\mathbb{C}} := \mathrm{AJ}_{X_r}^{r+1} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow J^{r+1}(X_r/\mathbb{C}) = \frac{\mathrm{Fil}^{r+1} H_{\mathrm{dR}}^{2r+1}(X_r/\mathbb{C})^\vee}{\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})}, \tag{2.2}$$

where $J^{r+1}(X_r/\mathbb{C})$ is the $r+1$ Griffiths intermediate Jacobian. This map is defined in terms of complex integration of differential forms attached to classes in $H_{\mathrm{dR}}^{2r+1}(X_r/\mathbb{C})$. One of the main results of this work is Theorem 2.1 of Section 2.2.4, which gives a formula for $\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)$ in terms of explicit line integrals of modular forms on the complex upper half-plane. An application of this formula is given in Theorem 2.2 of Section 2.3, where it is shown that the Chow group of homologically trivial cycles (resp. the Griffiths group when $r \geq 2$) of X_r over $\bar{\mathbb{Q}}$ has infinite rank. More precisely, it is proved that the subgroup generated by the images of generalised Heegner cycles in these groups has infinite rank. A second motivation for publishing a detailed proof of Theorem 2.1 is that this result forms the basis for the numerical calculations of Chow–Heegner points carried out in [13, §3], as explained in more details in Section 0.4.1. It may also be useful in further numerical explorations of generalised Heegner cycles – for instance, in extending the calculations of [86] beyond the more "traditional" setting of Heegner cycles on Kuga–Sato varieties.

The proof of Theorem 2.2 follows closely that of Theorem 4.7 of [128] which treats the case of "usual" Heegner cycles on a Kuga–Sato threefold, and rests on an ingenious method of Bloch. The most significant difference lies in the setting that is treated: whereas Schoen's cycles are indexed by arbitrary quadratic orders of varying discriminant, generalised Heegner cycles are forced by necessity to be indexed by (not necessarily maximal) orders of a fixed imaginary quadratic field.

The present work can be compared with [14], which studies the position of generalised Heegner cycles relative to the coniveau filtration on the relevant Chow groups, constructing non-torsion elements in the Griffiths group by methods that are purely p-adic, relying crucially on p-adic Hodge theoretic invariants and their relation to p-adic L-functions. In contrast, the approach described herein rests on a blend of complex and p-adic techniques, and the results obtained are more general if somewhat more qualitative.

The preliminary Section 2.1 provides an overview of the theory of generalised Heegner cycles and modular forms over the complex numbers. Section 2.2 deals with the computation of the Abel–Jacobi map. In Sections 2.2.1 and 2.2.2, purely transcendental, or Hodge theoretic, arguments are used for the computation. Specific properties of modular forms on modular curves (period lattices, modular symbols) lead to simplifications of the previous Abel–Jacobi computations, culminating in the proof of Theorem 2.1 in Section 2.2.4. Section 2.2.5 provides a summary of the proof, which is hopefully helpful for the reader. Section 2.3, which forms the technical core of the chapter, is devoted to the study of the Chow group and Griffiths group of X_r. Section 2.3.1 singles out a distinguished subcollection of generalised Heegner cycles. The aim is to study the subgroup generated by these in the various cycle groups. Analytic estimates of the explicit line integrals appearing in the Abel–Jacobi formula are used in Section 2.3.2 in order to determine their vanishing (or not), and consequences for the order of the cycles in the relevant groups. Section 2.3.3 uses class field theory as described in Section 1.3, the Bloch map from Section 1.5.2 and fundamental properties of étale cohomology to upgrade the previous order estimates and show that infinitely many of the cycles have infinite order. Class field theory and complex multiplication theory as formulated by Shimura are key in Section 2.3.4 where it is proved that the cycles generate a subgroup of infinite rank. Section 2.3.5 goes through the necessary modifications that allow one to deduce, when $r \geq 2$, the analogous result for the Griffiths group.

2.1 Preliminaries

We give an overview of the theory of generalised Heegner cycles and modular forms over the complex numbers. Along the way, we introduce conventions and notations necessary for the later sections. We end this preliminary section with a detailed proof of the homological triviality of generalised Heegner cycles, laying the groundwork for the Abel–Jacobi computations to come.

2.1.1 Generalised Heegner cycles

We begin with the definition of generalised Heegner cycles, following the notations of [12, §2]. Fix an integer $N \geq 5$ and let $\Gamma := \Gamma_1(N)$ be the standard congruence subgroup of level N whose definition (1.17) we recall:

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}. \tag{2.3}$$

Let $Y_1(N)$ and $X_1(N)$ denote the usual (affine and projective, respectively) modular curves of level $\Gamma_1(N)$ described in Section 1.2.2 and Section 1.2.4, and write W_r for the r-th Kuga–Sato variety over $X_1(N)$ as described for instance in Section 1.2.4 and the appendix of [12].

Let K be an imaginary quadratic field of dicriminant $-d_K$, let $\mathcal{O}_K$ be its ring of integers, and let H denote the Hilbert class field of K of Definition 1.10. Choose once and for all a complex embedding $\bar{K} \hookrightarrow \mathbb{C}$, and let A be a fixed elliptic curve over $\mathbb{C}$ with complex multiplication by the maximal order $\mathcal{O}_K$. See Definition 1.12. By the theory of complex multiplication, see Theorem 1.2, the curve A is defined over H and satisfies $\mathrm{End}_H(A) \simeq \mathcal{O}_K$.

The generalised Heegner cycles of [12] are an infinite collection of codimension $r+1$ cycles on the smooth projective $(2r+1)$-dimensional variety

$$X_r := W_r \times A^r.$$

To define them precisely, assume that K satisfies the Heegner hypothesis relative to N:

Assumption 2.1. *The integer N is the norm of an ideal $\mathfrak{N}$ for which $\mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Equivalently, all primes dividing N are split in $K/\mathbb{Q}$.*

Let $t_A \in A[\mathfrak{N}]$ be a choice of $\mathfrak{N}$-torsion point on A. Following the moduli description in

Section 1.2.2 of $X_1(N)$, the pair (A, t_A) corresponds to a complex point on $X_1(N)(\mathbb{C})$. This point is defined, in fact, over the ray class field $K_{\mathfrak{N}}$ of K of conductor $\mathfrak{N}$ by Theorem 1.3. For obvious reasons, the datum of the point t_A on A of order N is sometimes referred to as a $\Gamma_1(N)$-structure on A.

Consider the set of pairs (φ, A'), where $\varphi : A \longrightarrow A'$ is an isogeny of A defined over $\bar{K}$. Two pairs (φ_1, A'_1) and (φ_2, A'_2) are said to be isomorphic if there is a $\bar{K}$-isomorphism $\iota : A'_1 \longrightarrow A'_2$ satisfying $\iota\varphi_1 = \varphi_2$. Let

$$\mathrm{Isog}(A) := \{\text{Isomorphism classes of pairs } (\varphi, A')\}.$$

There is a natural bijection between this set and the set of finite subgroups of $A(\bar{H})$. The absolute Galois group $G_H = \mathrm{Gal}(\bar{H}/H)$ acts naturally on $\mathrm{Isog}(A)$ by acting on the corresponding subgroups and a pair (φ, A') admits a representative defined over a field $F \subset \bar{H}$ if it is fixed by the subgroup $G_F \subset G_H$.

The generalised Heegner cycles are naturally indexed by the subset $\mathrm{Isog}^{\mathfrak{N}}(A)$ of $\mathrm{Isog}(A)$ consisting of pairs (φ, A'), where φ is an isogeny whose kernel intersects $A[\mathfrak{N}]$ trivially. An element $(\varphi, A') \in \mathrm{Isog}^{\mathfrak{N}}(A)$ determines a point $P_{A'} = (A', t_{A'} := \varphi(t_A))$ on $X_1(N)$, and an embedding

$$\iota_{A'} : (A')^r \longrightarrow W_r$$

of $(A')^r$ as the fibre of W_r above the point $P_{A'}$ with respect to the structural morphism $\pi_r : W_r \longrightarrow X_1(N)$. Given $(\varphi, A') \in \mathrm{Isog}^{\mathfrak{N}}(A)$, let Υ_φ be the codimension $r+1$ cycle on X_r defined by letting $\mathrm{Graph}(\varphi) \subset A \times A'$ be the graph of φ, and setting

$$\Upsilon_\varphi := \mathrm{Graph}(\varphi)^r \subset (A \times A')^r \xrightarrow{\simeq} (A')^r \times A^r \subset W_r \times A^r, \tag{2.4}$$

where the last inclusion is induced from the pair $(\iota_{A'}, \mathrm{id}_A^r)$.

Definition 2.1 ($r = 0$)**.** When $r = 0$, the cycle Υ_φ is just the CM point on the modular curve $X_1(N)$ attached to the pair $(A', t_{A'})$. The generalised Heegner cycle Δ_φ attached to φ is then obtained by setting

$$\Delta_\varphi := \Upsilon_\varphi - \infty \in \mathrm{CH}^1(X_1(N))_0(\mathbb{C}), \tag{2.5}$$

where ∞ is the standard cusp on $X_1(N)$ (although any fixed choice will do). This modification has the effect of making the cycle Δ_φ homologically trivial.

For general $r \geq 1$, we obtain a homologically trivial cycle by applying to Υ_φ a suitable correspondence $\epsilon_{X_r} \in \mathrm{Corr}^0(X_r, X_r)_{\mathbb{Q}}$, which we now define. Recall from Definition 1.8 the idempotent

$$\epsilon_{W_r} := \epsilon_{W_r}^{(1)} \circ \epsilon_{W_r}^{(2)} \in \mathbb{Q}[\mathrm{Aut}(W_r/X_1(N))],$$

where the idempotents $\epsilon_{W_r}^{(1)}$ and $\epsilon_{W_r}^{(2)}$ are defined by (1.28) and (1.29) respectively. By taking the graphs of automorphisms, we will view ϵ_{W_r} as an element of $\mathrm{Corr}^0(W_r, W_r)_{\mathbb{Q}}$, and by slight abuse keep the same notation for this element.

Replacing the generalised elliptic curve $\bar{\mathcal{E}}/X_1(N)$ in the definition of $\epsilon_{W_r}^{(2)}$ by the elliptic curve A, we obtain similarly an idempotent of $\mathbb{Q}[\mathrm{Aut}(A^r)]$. More precisely, recall that S_r denotes the symmetric group on r letters. Multiplication by -1 on A together with the natural permutation action of S_r on A^r gives rise to an action of the semi-direct product $(\mu_2)^r \rtimes S_r$ on A^r. Let $j : (\mu_2)^r \rtimes S_r \longrightarrow \mu_2$ be the homomorphism which is the identity on μ_2 and the sign character on S_r and define

$$\epsilon_{A^r} := \frac{1}{2^r r!} \sum_{\sigma \in (\mu_2)^r \rtimes S_r} j(\sigma)\sigma \in \mathbb{Q}[\mathrm{Aut}(A^r)]. \tag{2.6}$$

By taking the graphs of automorphisms, we will view ϵ_{A^r} as an element of $\mathrm{Corr}^0(A^r, A^r)_{\mathbb{Q}}$, and by slight abuse keep the same notation for this element.

Definition 2.2. Let $\pi_{W_r} : X_r \longrightarrow W_r$ and $\pi_{A^r} : X_r \longrightarrow A^r$ denote the natural projections and define the idempotent

$$\epsilon_{X_r} := \epsilon_{W_r} \otimes \epsilon_{A^r} := (\pi_{W_r} \times \pi_{W_r})^*(\epsilon_{W_r}) \cdot (\pi_{A^r} \times \pi_{A^r})^*(\epsilon_{A^r}) \in \mathrm{Corr}(X_r, X_r)_{\mathbb{Q}}.$$

We can now define generalised Heegner cycles by letting the projector ϵ_{X_r} act on Υ_φ (2.4).

Definition 2.3 ($r \geq 1$)**.** For $r \geq 1$, we define the generalised Heegner cycle associated to an isogeny $\varphi \in \mathrm{Isog}^{\mathfrak{N}}(A)$ by

$$\Delta_\varphi := \epsilon_{X_r} \Upsilon_\varphi \in \mathrm{CH}^{r+1}(X_r)(\mathbb{C}), \tag{2.7}$$

where the correspondence ϵ_{X_r} acts on the Chow group via either of the fomulas (1.40) or (1.41) (so this action is denoted ϵ_{X_r} again by slight abuse of notation).

Since the correspondence ϵ_{X_r} is compatible with the projection $\pi_r : X_r \longrightarrow X_1(N)$, the generalised Heegner cycle Δ_φ is supported on the fibre $\pi_r^{-1}(P_{A'})$ of π_r above $P_{A'}$. As in the case where $r = 0$, it is also homologically trivial. This follows from the fact that the image of Δ_φ under the cycle class map belongs to $\epsilon_{X_r} H^{2r+2}_{\mathrm{dR}}(X_r/\mathbb{C})$, which is zero by [12, Prop. 2.4]. Section 2.1.3 below gives a more explicit description of a chain of real dimension $2r+1$ in $X_r(\mathbb{C})$ having Δ_φ as boundary, which will be used in subsequent calculations.

2.1.2 Modular forms and de Rham cohomology of X_r

We retain the notations and definitions introduced in Section 1.2.4. Recall in particular the canonical line bundle of relative differentials $\underline{\omega}$ on $X_1(N)$, defined as the extension of $\pi_* \Omega^1_{\mathcal{E}/Y_1(N)}$ to a coherent sheaf on $X_1(N)$, where $\pi : \mathcal{E} \longrightarrow Y_1(N)$ is the universal elliptic curve with $\Gamma_1(N)$-level structure over $Y_1(N)$.

The sheaf $\underline{\omega}$ is a subsheaf of the relative logarithmic de Rham cohomology sheaf on $X_1(N)$ defined by taking the relative hypercohomology of the complex of sheaves

$$\mathcal{L}_1 := \mathbb{R}^1 \pi_*(0 \longrightarrow \mathcal{O}_{\mathcal{E}} \longrightarrow \Omega^1_{\mathcal{E}/Y_1(N)} \longrightarrow 0), \tag{2.8}$$

and extending to $X_1(N)$ following the prescription given in [12, §1.1]. The Hodge filtration gives rise to an exact sequence of coherent sheaves over $X_1(N)$:

$$0 \longrightarrow \underline{\omega} \longrightarrow \mathcal{L}_1 \longrightarrow \underline{\omega}^{-1} \longrightarrow 0. \tag{2.9}$$

The vector bundle $\mathcal{L}_1$ is also equipped with the canonical integrable Gauss–Manin connection

$$\nabla : \mathcal{L}_1 \longrightarrow \mathcal{L}_1 \otimes \Omega^1_{X_1(N)}(\log \mathrm{cusps}), \tag{2.10}$$

and Poincaré duality on the fibres of $\mathcal{L}_1$ gives rise to a canonical pairing

$$\langle\ ,\ \rangle : \mathcal{L}_1 \times \mathcal{L}_1 \longrightarrow \mathcal{O}_{X_1(N)}. \tag{2.11}$$

Let $\mathcal{L}_r := \mathrm{Sym}^r \mathcal{L}_1$ denote the r-th symmetric power of $\mathcal{L}_1$. Definition 1.6 and the natural inclusion $\underline{\omega}^r \longrightarrow \mathcal{L}_r$ give rise to inclusions

$$S_{r+2}(\Gamma_1(N)) := H^0(X_1(N), \underline{\omega}^r \otimes \Omega^1_{X_1(N)}) \hookrightarrow H^0(X_1(N), \mathcal{L}_r \otimes \Omega^1_{X_1(N)}). \tag{2.12}$$

The self-duality

$$\langle\ ,\ \rangle : \mathcal{L}_r \times \mathcal{L}_r \longrightarrow \mathcal{O}_{X_1(N)} \tag{2.13}$$

induced by (2.11) is given by the rule

$$\langle \alpha_1 \cdots \alpha_r, \beta_1 \cdots \beta_r \rangle = \frac{1}{r!} \sum_{\sigma \in S_r} \langle \alpha_1, \beta_{\sigma(1)} \rangle \cdots \langle \alpha_r, \beta_{\sigma(r)} \rangle. \tag{2.14}$$

We will also have use for further coherent sheaves of $\mathcal{O}_{X_1(N)}$-modules arising in the cohomology of the fibres for the natural projection $\pi_r : X_r \longrightarrow X_1(N)$,

$$\mathcal{L}_{r,r} = \mathcal{L}_r \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A). \tag{2.15}$$

Note that $\mathcal{L}_{r,r}$ is also equipped with the self-duality

$$\langle\ ,\ \rangle : \mathcal{L}_{r,r} \times \mathcal{L}_{r,r} \longrightarrow \mathcal{O}_{X_1(N)} \tag{2.16}$$

arising from (2.14), which is discussed in more details in [12, §2.2].

As explained in [12, §1.1], all the notions introduced so far in this section are purely algebraic and make sense over an arbitrary field over which the modular curve $X_1(N)$ can be defined. We will be interested solely in their complex incarnations. The set $X_1(N)(\mathbb{C})$ of complex points of $X_1(N)$ is a compact Riemann surface, and the analytic map

$$\mathrm{pr} : \mathcal{H} \longrightarrow Y_1(N)(\mathbb{C}), \qquad \mathrm{pr}(\tau) := \left(\mathbb{C}/\langle 1, \tau\rangle, \frac{1}{N}\right)$$

identifies $Y_1(N)(\mathbb{C})$ with the quotient $\Gamma_1(N)\backslash\mathcal{H}$. Let τ denote a point on $\mathcal{H}$, w the standard complex coordinate on the elliptic curve $\mathbb{C}/\langle 1, \tau\rangle$ and recall the Hodge decomposition (1.23) $H^1_{\mathrm{dR}}(\mathbb{C}/\langle 1, \tau\rangle) := \mathbb{C}dw \oplus \mathbb{C}d\bar{w}$. In terms of the coordinates τ, dw, and $d\bar{w}$, one has [12, §1.2]

$$\nabla dw = \left(\frac{dw - d\bar{w}}{\tau - \bar{\tau}}\right) d\tau. \tag{2.17}$$

The coherent sheaf $\mathcal{L}_r$ gives rise to an analytic sheaf $\mathcal{L}_r^{\mathrm{an}}$ on the surface $X_1(N)(\mathbb{C})$. Let $\tilde{\mathcal{L}}_r^{\mathrm{an}} := \mathrm{pr}^* \mathcal{L}_r^{\mathrm{an}}$ denote its pullback to $\mathcal{H}$. Recall the elliptic fibration $\pi : \mathcal{E} \longrightarrow Y_1(N)$ and let

$$\mathbb{L}_1^B := R^1\pi_*\mathbb{Z}, \qquad \mathbb{L}_r^B := \mathrm{Sym}^r\, \mathbb{L}_1^B, \tag{2.18}$$

be the locally constant sheaves of $\mathbb{Z}$-modules whose fibres at $x \in Y_1(N)(\mathbb{C})$ are identified with the Betti cohomology $H^1_B(\mathcal{E}_x, \mathbb{Z})$ and $\mathrm{Sym}^r\, H^1_B(\mathcal{E}_x, \mathbb{Z})$ respectively. The local system

$$\mathbb{L}_r := \mathbb{L}_r^B \otimes_{\mathbb{Z}} \mathbb{C} \tag{2.19}$$

is identified with the sheaf of horizontal sections of $(\mathcal{L}_r^{\mathrm{an}}, \nabla)$ over $Y_1(N)(\mathbb{C})$, see [55, thm. 2.17].

Likewise, let

$$\mathbb{L}_{r,r} := \mathbb{L}_r \otimes \operatorname{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C}) \tag{2.20}$$

denote the sheaf of locally constant sections (for the complex topology on $Y_1(N)(\mathbb{C})$) of the sheaf $\mathcal{L}_{r,r}$.

The relation between the sheaves $\mathcal{L}_{r,r}$, the cohomology of X_r and the spaces of cusp forms is described in the following result.

Proposition 2.1. *Assume that $r \geq 1$. Let F be any field extension of the Hilbert class field H. The image of the projector ϵ_{X_r} acting on the de Rham cohomology of X_r is*

$$\epsilon_{X_r} H^j_{\mathrm{dR}}(X_r/F) = \begin{cases} 0 & \text{if } j \neq 2r+1 \\ H^1_{\mathrm{par}}(X_1(N)/F, \mathcal{L}_{r,r}, \nabla) & \text{if } j = 2r+1 \end{cases}$$

where $H^1_{\mathrm{par}}(X_1(N)/F, \mathcal{L}_{r,r}, \nabla) = H^1_{\mathrm{par}}(X_1(N)/F, \mathcal{L}_r, \nabla) \otimes \operatorname{Sym}^r H^1_{\mathrm{dR}}(A/F)$ denotes parabolic cohomology [12, (2.1.3)] of $X_1(N)$ attached to $(\mathcal{L}_{r,r}, \nabla)$. Moreover, there is an identification

$$\operatorname{Fil}^{r+1} \epsilon_{X_r} H^{2r+1}_{\mathrm{dR}}(X_r/F) = H^0(X_1(N)/F, \underline{\omega}^r \otimes \Omega^1_{X_1(N)}) \otimes \operatorname{Sym}^r H^1_{\mathrm{dR}}(A/F). \tag{2.21}$$

In particular, using (1.25), the assignment $f \otimes \alpha \mapsto \omega_f \wedge \alpha$ induces an identification

$$S_{r+2}(\Gamma_1(N), F) \otimes \operatorname{Sym}^r H^1_{\mathrm{dR}}(A/F) \simeq \operatorname{Fil}^{r+1} \epsilon_{X_r} H^{2r+1}_{\mathrm{dR}}(X_r/F). \tag{2.22}$$

Proof. This is [12, Proposition 2.4 & 2.5] and follows from Proposition 1.6. □

2.1.3 Homological triviality

All Chow groups will henceforth be taken with rational coefficients, so that they consist of $\mathbb{Q}$-linear combinations of cycles modulo rational equivalence.

The goal of this section is to express the generalised Heegner cycles Δ_φ as the boundaries of explicit $(2r+1)$-dimensional topological chains in $X_r^0(\mathbb{C})$. Such a calculation will be useful in calculating the images of these cycles under the complex Abel–Jacobi map, which is the goal of the next section.

Let $W_r^0 := W_r \times_{X_1(N)} Y_1(N)$ and $X_r^0 = X_r \times_{X_1(N)} Y_1(N)$ denote the complements in W_r and X_r respectively of the fibres above the cusps of $X_1(N)$. Let $\tilde{W}_r$ be the r-fold product of the universal elliptic curve over the upper half-plane $\mathcal{H}$ (which we will denote $\mathcal{E}$ by slight abuse of notation). It is isomorphic as an analytic variety to the quotient $\mathbb{Z}^{2r}\backslash(\mathbb{C}^r \times \mathcal{H})$, where $\mathbb{Z}^{2r}$ acts on $\mathbb{C}^r \times \mathcal{H}$ by the rule

$$(m_1, n_1, \ldots, m_r, n_r)(w_1, \ldots, w_r, \tau) := (w_1 + m_1 + n_1\tau, \ldots, w_r + m_r + n_r\tau, \tau). \qquad (2.23)$$

Finally, let

$$\tilde{X}_r = \tilde{W}_r \times A^r(\mathbb{C}).$$

It follows from these definitions that

$$W_r^0(\mathbb{C}) = \Gamma_1(N)\backslash\tilde{W}_r, \qquad X_r^0(\mathbb{C}) = \Gamma_1(N)\backslash\tilde{X}_r,$$

where $\Gamma_1(N)$ acts on $\tilde{W}_r$ by the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (w_1, \ldots, w_r, \tau) = \left(\frac{w_1}{c\tau + d}, \ldots, \frac{w_r}{c\tau + d}, \frac{a\tau + b}{c\tau + d}\right), \qquad (2.24)$$

and acts trivially on $A^r(\mathbb{C})$. Write pr for the natural $\Gamma_1(N)$-covering maps $\tilde{X}_r \longrightarrow X_r^0(\mathbb{C})$ and $\mathcal{H} \longrightarrow Y_1(N)(\mathbb{C})$, and let $\tilde{\pi}_r$ be the natural fibreing $\tilde{X}_r \longrightarrow \mathcal{H}$. These maps fit into the cartesian diagram

$$\begin{array}{ccc} \tilde{X}_r & \xrightarrow{\text{pr}} & X_r^0(\mathbb{C}) \\ {\scriptstyle \tilde{\pi}_r}\downarrow & \square & \downarrow{\scriptstyle \pi_r} \\ \mathcal{H} & \xrightarrow[\text{pr}]{} & Y_1(N)(\mathbb{C}). \end{array} \qquad (2.25)$$

The fundamental group $\Gamma_1(N)$ of $Y_1(N)$ acts naturally on $H_{2r}(\tilde{X}_r, \mathbb{Q})$, and the kernel of the pushforward map

$$\mathrm{pr}_* : H_{2r}(\tilde{X}_r, \mathbb{Q}) \longrightarrow H_{2r}(X_r^0(\mathbb{C}), \mathbb{Q})$$

contains the module $I_{\Gamma_1(N)} H_{2r}(\tilde{X}_r, \mathbb{Q})$, where $I_{\Gamma_1(N)}$ is the augmentation ideal in the rational group ring $\mathbb{Q}[\Gamma_1(N)]$.

Following the recipe of Definition 2.2, one can define the idempotent correspondence

$$\epsilon_{\tilde{X}_r} = \epsilon_{\tilde{W}_r} \otimes \epsilon_{A^r} \in \mathrm{Corr}^0(\tilde{X}_r, \tilde{X}_r)_{\mathbb{Q}} \tag{2.26}$$

via the same formulas as for ϵ_{X_r}, but replacing the universal elliptic curve $\mathcal{E}/Y_1(N)$ with the universal elliptic curve $\mathcal{E}/\mathcal{H}$. This projector acts on $H_{2r}(\tilde{X}_r, \mathbb{Q})$ and we have the following description of its image.

Lemma 2.1. *Let $\tau \in \mathcal{H}$ and denote by $\mathcal{E}_\tau$ the fibre of $\mathcal{E} \longrightarrow \mathcal{H}$ above τ. For all $r \geq 1$,*

$$\epsilon_{\tilde{X}_r} H_{2r}(\tilde{X}_r, \mathbb{Q}) = \mathrm{Sym}^r H_1(\mathcal{E}_\tau, \mathbb{Q}) \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Q}) \subset I_{\Gamma_1(N)} H_{2r}(\tilde{X}_r, \mathbb{Q}).$$

Proof. Since $\mathcal{H}$ is contractible, the inclusion

$$\iota_\tau : \tilde{\pi}_r^{-1}(\tau) \longrightarrow \tilde{X}_r$$

induces an isomorphism

$$\iota_{\tau,*} : H_{2r}(\tilde{\pi}_r^{-1}(\tau), \mathbb{Q}) \xrightarrow{\sim} H_{2r}(\tilde{X}_r, \mathbb{Q}). \tag{2.27}$$

The fibre $\tilde{\pi}_r^{-1}(\tau)$ is $(\mathcal{E}_\tau)^r \times A(\mathbb{C})^r$, hence we obtain an identification

$$H_{2r}((\mathcal{E}_\tau)^r \times A(\mathbb{C})^r, \mathbb{Q}) \xrightarrow{\sim} H_{2r}(\tilde{X}_r, \mathbb{Q}). \tag{2.28}$$

Since multiplication by (-1) acts as -1 on $H^1_{\mathrm{dR}}(A/F)$ and as 1 on $H^0_{\mathrm{dR}}(A/F)$ and $H^2_{\mathrm{dR}}(A/F)$, it follows that ϵ_{A^r} annihilates all the terms except $H^1_{\mathrm{dR}}(A/F)^{\otimes r}$ in the Künneth decomposition

$$H^*_{\mathrm{dR}}(A^r/F) = \bigoplus_{(i_1,\ldots,i_r)} H^{i_1}_{\mathrm{dR}}(A/F) \otimes \cdots \otimes H^{i_r}_{\mathrm{dR}}(A/F), \tag{2.29}$$

where the direct sum is taken over all r-tuples $(i_1, \ldots, i_r)$ with $0 \le i_j \le 2$. The natural action of S_r on $H^1_{\mathrm{dR}}(A/F)^{\otimes r}$ corresponds to the geometric permutation action of S_r on A^r, twisted by the sign character. It follows that the restriction of ϵ_{A^r} to $H^1_{\mathrm{dR}}(A/F)^{\otimes r}$ induces the natural projection onto the space $\mathrm{Sym}^r H^1_{\mathrm{dR}}(A/F)$ of symmetric tensors. A similar argument applies to the projector $\epsilon_{\tilde{W}_r}$ and its action on the cohomology of $(\mathcal{E}_\tau)^r$. The first equality follows.

Following (2.18), consider the locally constant sheaf of $\mathbb{Z}$-modules

$$\mathbb{L}^B_{r,r} := \mathbb{L}_r \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Z}),$$

such that $\mathbb{L}^B_{r,r} \otimes \mathbb{C} = \mathbb{L}_{r,r}$ is the sheaf (2.20) of locally constant sections of $(\mathcal{L}^{\mathrm{an}}_{r,r}, \nabla)$. Pulling back to $\mathcal{H}$ using the Cartesian square (2.25), we obtain

$$\tilde{\mathbb{L}}^B_{r,r} := \mathrm{pr}^*(\mathbb{L}^B_{r,r}) = \mathrm{Sym}^r R^1\tilde{\pi}_*\mathbb{Z} \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Z}),$$

where $\tilde{\pi} : \mathcal{E} \longrightarrow \mathcal{H}$ is the elliptic fibration. Since $\mathcal{H}$ is contractible, this is the constant sheaf

$$(\mathrm{Sym}^r H_1(\mathcal{E}_\tau, \mathbb{Z}) \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Z})).$$

The second containment of the lemma is a consequence of the fact that

$$(\mathrm{Sym}^r H_1(\mathcal{E}_\tau, \mathbb{Q}) \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Q})) \otimes_{\mathbb{Q}} \mathbb{C} = \mathrm{pr}^*(\mathbb{L}_{r,r}) =: \tilde{\mathbb{L}}_{r,r},$$

and that the representation of $\Gamma_1(N)$ associated to this local system is isomorphic to a direct sum of $r+1$ copies of the r-th symmetric power of the standard two-dimensional representation of $\Gamma_1(N)$. Each of these copies is irreducible and, since $r > 0$, is non-trivial and hence has a trivial space of $\Gamma_1(N)$-coinvariants. $\square$

Given $(\varphi, A') \in \mathrm{Isog}^{\mathfrak{N}}(A)$, set $t' := \varphi(t_A)$, so that $\varphi : (A, t_A) \longrightarrow (A', t')$ is an isogeny of elliptic curves with $\Gamma_1(N)$-level structure, in the obvious sense. Let $P_{A'}$ be the point of $Y_1(N)(\mathbb{C})$ associated to the pair (A', t'). The main result of this section, which directly implies the homological triviality of Δ_φ, is the following.

Proposition 2.2. *Assume $r > 0$. Then there exists a topological cycle $\widetilde{\Delta}_\varphi$ on $\tilde{X}_r$ satisfying:*

1. *The pushforward $\mathrm{pr}_*(\widetilde{\Delta}_\varphi)$ satisfies $\mathrm{pr}_*(\widetilde{\Delta}_\varphi) = \Delta_\varphi + \partial\xi$, where ξ is a topological $(2r+1)$-chain supported on $\pi_r^{-1}(P_{A'})$.*
2. *The cycle $\widetilde{\Delta}_\varphi$ is homologically trivial on $\tilde{X}_r$.*

Proof. Choose a point $\tau_{A'} \in \mathcal{H}$ such that $\mathrm{pr}(\tau_{A'}) = P_{A'}$. Since pr induces an isomorphism between $\tilde{\pi}_r^{-1}(\tau_{A'})$ and $\pi_r^{-1}(P_{A'})$, the choice of $\tau_{A'}$ determines cycles $\varUpsilon_\varphi^\natural$ and $\Delta_\varphi^\natural$ on $\tilde{X}_r$ supported on $\tilde{\pi}_r^{-1}(\tau_{A'})$ and satisfying

$$\mathrm{pr}_*(\varUpsilon_\varphi^\natural) = \varUpsilon_\varphi, \qquad \mathrm{pr}_*(\Delta_\varphi^\natural) = \Delta_\varphi. \tag{2.30}$$

These cycles need not be homologically trivial on $\tilde{X}_r$. In fact, there is an isomorphism (2.27)

$$\iota_{\tau_{A'},*} : H_{2r}(\tilde{\pi}_r^{-1}(\tau_{A'}), \mathbb{Q}) \xrightarrow{\sim} H_{2r}(\tilde{X}_r, \mathbb{Q}), \tag{2.31}$$

and the classes $[\varUpsilon_\varphi^\natural] := \mathrm{PD}(\mathrm{cl}(\varUpsilon_\varphi^\natural))$ and $[\Delta_\varphi^\natural] := \mathrm{PD}(\mathrm{cl}(\Delta_\varphi^\natural))$ of $\varUpsilon_\varphi^\natural$ and $\Delta_\varphi^\natural$ in $H_{2r}(\tilde{X}_r, \mathbb{Q})$ are identified with those of $\varUpsilon_\varphi$ and Δ_φ in $H_{2r}((A' \times A)^r(\mathbb{C}), \mathbb{Q})$. (Recall the definitions (1.44) and (1.43) of PD and cl).

Note that the projector $\epsilon_{\tilde{X}_r}$ of (2.26) acts naturally on $H_{2r}(\tilde{X}_r, \mathbb{Q})$ and $[\Delta_\varphi^\natural] = \epsilon_{\tilde{X}_r}[\Upsilon_\varphi^\natural]$ belongs to $\epsilon_{\tilde{X}_r} H_{2r}(\tilde{X}_r, \mathbb{Q})$. It now follows from Lemma 2.1 that

$$\mathrm{PD}(\mathrm{cl}(\Delta_\varphi)) = \mathrm{pr}_*([\Delta_\varphi^\natural]) \in \mathrm{pr}_*(I_{\Gamma_1(N)} H_{2r}(\tilde{X}_r, \mathbb{Q})) = 0,$$

and therefore Δ_φ is homologically trivial. To produce the cycle $\widetilde{\Delta}_\varphi$ explicitly, let

$$[\Delta_\varphi^\natural] = \sum_{j=1}^{t} (\gamma_j^{-1} - 1) Z_j, \qquad \begin{array}{l} \gamma_1, \dots, \gamma_t \in \Gamma_1(N), \\ Z_1, \dots, Z_t \in H_{2r}(\tilde{X}_r, \mathbb{Q}) \end{array} \tag{2.32}$$

be an expression of $[\Delta_\varphi^\natural]$ as an element of $I_{\Gamma_1(N)} H_{2r}(\tilde{X}_r, \mathbb{Q})$. Letting $\mathcal{Z}(\tau, Z)$ denote any topological $2r$-cycle supported on $\tilde{\pi}_r^{-1}(\tau)$ and determined by the class of Z in $H_{2r}(\tilde{X}_r, \mathbb{Q})$ via (2.27), define

$$\widetilde{\Delta}_\varphi := \sum_{j=1}^{t} \big(\mathcal{Z}(\gamma_j \tau_{A'}, Z_j) - \mathcal{Z}(\tau_{A'}, Z_j) \big). \tag{2.33}$$

It is then straightforward to check that $\widetilde{\Delta}_\varphi$ has the required properties. For example, the homological triviality of $\widetilde{\Delta}_\varphi$ follows from the fact that

$$\widetilde{\Delta}_\varphi = \partial \widetilde{\Delta}_\varphi^\sharp, \qquad \text{with} \qquad \widetilde{\Delta}_\varphi^\sharp := \sum_{j=1}^{t} \mathcal{Z}(\tau_{A'} \to \gamma_j \tau_{A'}, Z_j), \tag{2.34}$$

where

$$\mathcal{Z}(\tau_{A'} \to \gamma_j \tau_{A'}, Z_j) := \mathrm{path}(\tau_{A'} \to \gamma_j \tau_{A'}) \times Z_j \tag{2.35}$$

and $\mathrm{path}(\tau_{A'} \to \gamma_j \tau_{A'})$ is any continuous path on $\mathcal{H}$ joining $\tau_{A'}$ to $\gamma_j \tau_{A'}$. Note that in (2.35) we have identified $\tilde{X}_r(\mathbb{C})$ with $\mathcal{H} \times (\mathbb{C}^{2r}/\mathbb{Z}^{4r})$. □

Remark 2.1. Yet another approach to proving the homological triviality of Δ_φ, by deforming these cycles to the fibres supported above the cusps of the modular curve, is described in [128]. The approach we have given adapts more readily to the setting of Shimura curves attached to arithmetic subgroups of $\mathbf{SL}_2(\mathbb{R})$ with compact quotient.

Remark 2.2. A decomposition as in (2.32) with $Z_1, \ldots, Z_t \in H_{2r}(\tilde{X}_r, \mathbb{Z})$ is said to be integral. Such a decomposition may not always be possible, owing to the possible presence of torsion in $H_{2r}(X_r^0(\mathbb{C}), \mathbb{Z})$. But it may be obtained after replacing $[\Delta_\varphi^\natural]$ by a suitable integer multiple. In the rest of this note, when the image of Δ_φ under the complex Abel–Jacobi map is computed, it will be tacitly assumed that the Z_i do belong to this integral lattice.

2.2 The complex Abel–Jacobi formula

The complex Abel–Jacobi map (1.51) is a function from the Chow group $\mathrm{CH}^{r+1}(X_r)_0(\mathbb{C})$ into a complex torus:

$$\mathrm{AJ}_{\mathbb{C}} := \mathrm{AJ}_{X_r}^{r+1} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow J^{r+1}(X_r/\mathbb{C}) = \frac{\mathrm{Fil}^{r+1} H_{\mathrm{dR}}^{2r+1}(X_r/\mathbb{C})^\vee}{\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})},$$

where the superscript $^\vee$ denotes the dual of complex vector spaces, and $\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})$ is viewed as a sublattice of $\mathrm{Fil}^{r+1} H_{\mathrm{dR}}^{2r+1}(X_r\mathbb{C})^\vee$ via integration of closed differential $(2r+1)$-forms against singular integral homology classes of dimension $2r+1$. Recall from Section 1.5.1 that the linear functional $\mathrm{AJ}_{\mathbb{C}}(\Delta)$ is defined by choosing a continuous integral $(2r+1)$-chain $\Delta^\sharp$ on $X_r(\mathbb{C})$ whose boundary $\partial(\Delta^\sharp)$ is equal to Δ, and setting

$$\mathrm{AJ}_{\mathbb{C}}(\Delta)(\alpha) = \int_{\Delta^\sharp} \alpha, \qquad \text{for all } \alpha \in \mathrm{Fil}^{r+1} H_{\mathrm{dR}}^{2r+1}(X_r/\mathbb{C}). \tag{2.36}$$

We will be solely interested in the piece of the Abel–Jacobi map that survives after applying the projector ϵ_{X_r} of Definition 2.2. Proposition 2.1 allows us to view $\mathrm{AJ}_{\mathbb{C}}$ as a map

$$\mathrm{AJ}_{\mathbb{C}} : \epsilon_{X_r} \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow \frac{(S_{r+2}(\Gamma_1(N)) \otimes \mathrm{Sym}^r H_{\mathrm{dR}}^1(A/\mathbb{C}))^\vee}{\Pi_{r,r}},$$

where the lattice $\Pi_{r,r}$ is defined by

$$\Pi_{r,r} := \epsilon_{X_r}(\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})). \tag{2.37}$$

The goal of the present section is to prove Theorem 2.1 of Section 2.2.4, which gives a formula for $\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)$ in terms of explicit line integrals of modular forms on the complex upper half-plane.

2.2.1 Global primitives

We will follow the notations that were introduced in Section 2.1.2 and in the proof of Lemma 2.1. Let $\tilde{\mathbb{L}}_r := \mathrm{pr}^*(\mathbb{L}_r), \tilde{\mathbb{L}}_{r,r} := \mathrm{pr}^*(\mathbb{L}_{r,r})$, and $\tilde{\mathcal{L}}_r := \mathrm{pr}^*(\mathcal{L}_r^{\mathrm{an}}), \tilde{\mathcal{L}}_{r,r} := \mathrm{pr}^*(\mathcal{L}_{r,r}^{\mathrm{an}})$ denote the pullbacks via the analytic projection pr of (2.25).

Remark 2.3. The local systems $\tilde{\mathbb{L}}_r$ and $\tilde{\mathbb{L}}_{r,r}$ are trivial, i.e., they admit a basis of global sections over $\mathcal{H}$. In other words, if θ is an element of the fibre $\tilde{\mathbb{L}}_{r,r}(\tau)$ of $\tilde{\mathbb{L}}_{r,r}$ at $\tau \in \mathcal{H}$, then there is a unique global horizontal section $\theta^\nabla \in H^0(\mathcal{H}, \tilde{\mathcal{L}}_{r,r})^{\nabla=0}$ satisfying $\theta^\nabla(\tau) = \theta$.

More generally, if $\mathcal{L}$ is any vector bundle over $Y_1(N)$ equipped with an integrable connection and $\mathbb{L}$ denotes the corresponding local system, we will write $\tilde{\mathbb{L}} := \mathrm{pr}^*(\mathbb{L})$ and $\tilde{\mathcal{L}} := \mathrm{pr}^*(\mathcal{L}^{\mathrm{an}})$, and define global primitives in the following way:

Definition 2.4. Let ω be a global section of $\mathcal{L} \otimes \Omega^1_{X_1(N)}$ over $Y_1(N)$. A primitive of ω is an element $F \in H^0(\mathcal{H}, \tilde{\mathcal{L}})$ satisfying

$$\nabla F = \mathrm{pr}^*(\omega).$$

Such a primitive always exists, and is well-defined up to elements of the space of global horizontal sections of $\tilde{\mathcal{L}}$ over $\mathcal{H}$.

Definition 2.5. An $\mathbb{L}$-*valued divisor* on $X_1(N)$ is a finite formal linear combination of the form $\sum_{j=1}^t \theta_j \cdot P_j$ with $P_j \in X_1(N)(\mathbb{C})$ and $\theta_j \in \mathbb{L}(P_j)$. The module of all such divisors is denoted $\mathrm{Div}(X_1(N), \mathbb{L})$.

One defines the notion of a $\tilde{\mathbb{L}}$-valued divisor on $\mathcal{H}$ in a similar way. The analytic projection $\mathrm{pr} : \mathcal{H} \longrightarrow Y_1(N)(\mathbb{C})$ induces the natural push-forward map

$$\mathrm{pr}_* : \mathrm{Div}(\mathcal{H}, \tilde{\mathbb{L}}) \longrightarrow \mathrm{Div}(X_1(N), \mathbb{L}).$$

Given $G \in H^0(\mathcal{H}, \tilde{\mathcal{L}}_{r,r})$ and $D = \sum_{j=1}^{t} \theta_j \cdot \tau_j \in \mathrm{Div}(\mathcal{H}, \tilde{\mathbb{L}}_{r,r})$, the "value" of G at D is defined by the rule:

$$[G, D] := \sum_{j=1}^{t} \langle G(\tau_j), \theta_j \rangle,$$

where the pairing $\langle \ , \ \rangle$ on the right is the duality on the fibres at τ_j of the local system $\tilde{\mathbb{L}}_{r,r}$ induced by the pairing of equation (2.16).

For $D = \sum_{j=1}^{t} \theta_j \cdot \tau_j$ as above, the coefficient θ_j belongs to $\tilde{\mathbb{L}}_{r,r}(\tau_j)$ by definition, i.e., to $\mathrm{Sym}^r H^1_{\mathrm{dR}}(\mathcal{E}_{\tau_j}) \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A)$, where $\mathcal{E}_{\tau_j}$ denotes the fibre at τ_j of the pull-back of $\mathcal{E}$ to $\mathcal{H}$ by pr. Calculations similar to those in the proof of Lemma 2.1 identify

$$\varepsilon_{\tilde{X}_r} H^{2r}_{\mathrm{dR}}(\tilde{\pi}_r^{-1}(\tau_j)) = \tilde{\mathbb{L}}_{r,r}(\tau_j). \tag{2.38}$$

Moreover, since $\mathcal{H}$ is contractible, the inclusion of $\tilde{\pi}_r^{-1}(\tau_j)$ in $\tilde{X}_r$ induces a canonical isomorphism of $H^{2r}_{\mathrm{dR}}(\tilde{X}_r)$ onto $H^{2r}_{\mathrm{dR}}(\tilde{\pi}_r^{-1}(\tau_j))$, and hence a canonical identification

$$\varepsilon_{\tilde{X}_r} H^{2r}_{\mathrm{dR}}(\tilde{X}_r) = \tilde{\mathbb{L}}_{r,r}(\tau_j). \tag{2.39}$$

In view of these remarks, the degree of an $\tilde{\mathbb{L}}_{r,r}$-valued divisor on $\mathcal{H}$ can be defined by the equation

$$\deg\left(\sum_{j=1}^{t} \theta_j \cdot \tau_j\right) := \sum_{j=1}^{t} \theta_j \in \epsilon_{\tilde{X}_r} H^{2r}_{\mathrm{dR}}(\tilde{X}_r).$$

Given $\tau \in \mathcal{H}$ or $P \in Y_1(N)$, let

$$\mathrm{cl}_\tau : \mathrm{CH}^r((\mathcal{E}_\tau)^r \times A^r) \longrightarrow \tilde{\mathbb{L}}_{r,r}(\tau), \quad \mathrm{cl}_P : \mathrm{CH}^r((\mathcal{E}_P)^r \times A^r) \longrightarrow \mathbb{L}_{r,r}(P)$$

denote the (ε_{X_r}-components of the) cycle class maps on the associated fibres. The first map is defined by composing the usual cycle class map (1.46) with isomorphism (2.38). The second map is defined in terms of the first by identifying $\mathcal{E}_P$ with $\mathcal{E}_\tau$ and $\mathbb{L}_{r,r}(P)$ with $\tilde{\mathbb{L}}_{r,r}(\tau)$ if $P = \mathrm{pr}(\tau)$.

The cycle $\Delta_\varphi^\natural$ that was introduced in the proof of Proposition 2.2 gives rise to the $\tilde{\mathbb{L}}_{r,r}$-valued divisor (which shall be denoted by the same symbol, by abuse of notation):

$$\Delta_\varphi^\natural = \mathrm{cl}_{\tau_{A'}}(\Delta_\varphi^\natural) \cdot \tau_{A'}.$$

Note that $\mathrm{pr}_*(\Delta_\varphi^\natural) = \mathrm{cl}_{P_{A'}}(\Delta_\varphi) \cdot P_{A'}$, but that $\Delta_\varphi^\natural$ is not of degree 0. We will identify the cycle $\tilde{\Delta}_\varphi$ defined in equation (2.33) with the corresponding degree zero divisor on $\mathcal{H}$ with values in $\tilde{\mathbb{L}}_{r,r}$ given by

$$\widetilde{\Delta}_\varphi := \sum_{j=1}^{t} \big(\mathrm{PD}_{\gamma_j \tau_{A'}}(Z_j) \cdot (\gamma_j \tau_{A'}) - \mathrm{PD}_{\tau_{A'}}(Z_j) \cdot \tau_{A'} \big), \tag{2.40}$$

where, for $\tau \in \mathcal{H}$, we define the map PD_τ as the composition

$$\begin{aligned} \mathrm{PD}_\tau : H_{2r}(\tilde{X}_r, \mathbb{Q}) &\stackrel{(2.27)}{\longrightarrow} H_{2r}(\tilde{\pi}_r^{-1}(\tau), \mathbb{Q}) \stackrel{(1.44)}{\longrightarrow} H^{2r}(\tilde{\pi}_r^{-1}(\tau), \mathbb{Q}) \stackrel{(1.45)}{\longrightarrow} H^{2r}_{\mathrm{dR}}(\tilde{\pi}_r^{-1}(\tau)) \\ &\stackrel{\epsilon_{\tilde{X}_r}}{\longrightarrow} \epsilon_{\tilde{X}_r} H^{2r}_{\mathrm{dR}}(\tilde{\pi}_r^{-1}(\tau)) \stackrel{(2.38)}{\longrightarrow} \tilde{\mathbb{L}}_{r,r}(\tau). \end{aligned} \tag{2.41}$$

Remark 2.4. Let $\omega_f \in S_{r+2}(\Gamma_1(N))$ be a cusp form, viewed in $H^0(X_1(N), \mathcal{L}_r \otimes \Omega^1_{X_1(N)})$ via (2.12). Given a class $\alpha \in \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C})$, a primitive of $\omega_f \wedge \alpha \in H^0(X_1(N), \mathcal{L}_{r,r} \otimes \Omega^1_{X_1(N)})$ is given by $F_f \wedge \alpha$, where F_f is a primitive of ω_f. This is because α is a horizontal section of the trivial bundle $\mathrm{Sym}^r H^1_{\mathrm{dR}}(A) = \mathrm{Sym}^r \mathcal{H}^1_{\mathrm{dR}}((A \times X_1(N))/X_1(N))$ over $X_1(N)$ that arises in the identification $\mathcal{L}_{r,r} = \mathcal{L}_r \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C})$.

The following proposition gives an explicit formula for $\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)$ in terms of this divisor and a primitive of ω_f.

Proposition 2.3. *For all $f \in S_{r+2}(\Gamma_1(N))$ and all $\alpha \in \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C})$,*

$$\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f \wedge \alpha) = [F_f \wedge \alpha, \widetilde{\Delta}_\varphi] \pmod{\Pi_{r,r}}, \tag{2.42}$$

where F_f is any primitive of ω_f.

Remark 2.5. Both sides in (2.42) are to be viewed as belonging to the complex vector space $(S_{r+2}(\Gamma_1(N)) \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C}))^\vee$, the equality being up to an element of the lattice $\Pi_{r,r}$ (2.37) in this vector space. Note also that the right hand side of (2.42) depends on the choice of a degree 0 divisor $\tilde{\Delta}_\varphi$ satisfying $\mathrm{pr}_*(\widetilde{\Delta}_\varphi) = \Delta_\varphi$, but only up to an element of $\Pi_{r,r}$.

Proof. Recall the $(2r+1)$-cycle $\widetilde{\Delta}^\sharp_\varphi$ arising in equation (2.34). The definition of $\mathrm{AJ}_\mathbb{C}$ and Proposition 2.2, combined with Fubini's theorem, imply the equalities

$$\begin{aligned}\mathrm{AJ}_\mathbb{C}(\Delta_\varphi)(\omega_f \wedge \alpha) &= \int_{\mathrm{pr}_*(\widetilde{\Delta}^\sharp_\varphi)} \omega_f \wedge \alpha = \int_{\widetilde{\Delta}^\sharp_\varphi} \mathrm{pr}^*\,\omega_f \wedge \alpha \pmod{\Pi_{r,r}} \\ &= \sum_{j=1}^{t} \int_{\tau_{A'}}^{\gamma_j \tau_{A'}} \langle \mathrm{pr}^*\,\omega_f \wedge \alpha, \theta^\nabla_{Z_j} \rangle \pmod{\Pi_{r,r}},\end{aligned}$$

where $\theta^\nabla_{Z_j}$ is the horizontal section of $\tilde{\mathcal{L}}_{r,r}$ whose value at $\tau_{A'}$ is equal to $\mathrm{PD}_{\tau_{A'}}(Z_j)$ as in Remark 2.3, and the integral is taken over any continuous path in $\mathcal{H}$ joining $\tau_{A'}$ to $\gamma_j\tau_{A'}$. Note the independence on the choice of paths, which follows from the fact that the expressions $\langle \mathrm{pr}^*\,\omega_f \wedge \alpha, \theta^\nabla_{Z_j} \rangle$ are holomorphic 1-forms on $\mathcal{H}$. Since $\theta^\nabla_{Z_j}$ is horizontal, it follows from the definition of the Gauss-Manin connection that

$$\langle \mathrm{pr}^*\,\omega_f \wedge \alpha, \theta^\nabla_{Z_j} \rangle = \langle \nabla F_f \wedge \alpha, \theta^\nabla_{Z_j} \rangle = d\langle F_f \wedge \alpha, \theta^\nabla_{Z_j} \rangle.$$

Hence Stokes' theorem yields the equalities modulo $\Pi_{r,r}$

$$\begin{aligned}\mathrm{AJ}_\mathbb{C}(\Delta_\varphi)(\omega_f \wedge \alpha) &= \sum_{j=1}^{t} \Big(\langle F_f(\gamma_j\tau_{A'}) \wedge \alpha, \theta^\nabla_{Z_j} \rangle - \langle F_f(\tau_{A'}) \wedge \alpha, \theta^\nabla_{Z_j} \rangle \Big) \\ &= \sum_{j=1}^{t} \Big([F_f \wedge \alpha, \mathrm{PD}_{\gamma_j\tau_{A'}}(Z_j) \cdot (\gamma_j \tau_{A'})] - [F_f \wedge \alpha, \mathrm{PD}_{\tau_{A'}}(Z_j) \cdot \tau_{A'}] \Big) \\ &= [F_f \wedge \alpha, \widetilde{\Delta}_\varphi],\end{aligned}$$

as was to be shown. ∎

Remark 2.6. The expression on the right of Proposition 2.3 is independent of the choice of primitive F_f for ω_f. This is because the primitive $F_f \wedge \alpha$ is well-defined up to addition of global horizontal sections of the sheaf $\tilde{\mathcal{L}}_{r,r}$ over $\mathcal{H}$. If θ is such a horizontal section, we have

$$[\theta, \widetilde{\Delta}_\varphi] = \langle \theta, \deg \widetilde{\Delta}_\varphi \rangle = 0.$$

Note that this independence ceases to hold if $\widetilde{\Delta}_\varphi$ is replaced by $\Delta_\varphi^\natural$, because the latter divisor is not of degree 0.

2.2.2 Calculation of the primitive

We now turn to the explicit calculation of the primitive F_f that appears in Proposition 2.3. Let p_1 and p_τ denote the elements of $H_1(\mathcal{E}_\tau, \mathbb{Q})$ corresponding to a closed path from 0 to 1 and from 0 to τ respectively along the fibre $\mathcal{E}_\tau = \mathbb{C}/\langle 1, \tau \rangle$. Write η_1 and η_τ for the associated basis of $H^1_{\mathrm{dR}}(\mathcal{E}_\tau)$, satisfying

$$\langle \omega, \eta_1 \rangle = \int_{p_1} \omega, \qquad \langle \omega, \eta_\tau \rangle = \int_{p_\tau} \omega, \qquad \text{for all } \omega \in H^1_{\mathrm{dR}}(\mathcal{E}_\tau). \tag{2.43}$$

After writing w for the natural holomorphic coordinate on $\mathcal{E}_\tau$, the values of $\langle dw, \xi \rangle$ and $\langle d\bar{w}, \xi \rangle$ for various classes ξ are summarised in the following table:

	dw	$d\bar{w}$	η_1	η_τ
dw	0	$\frac{-1}{2\pi i}(\tau - \bar{\tau})$	1	τ
$d\bar{w}$	$\frac{1}{2\pi i}(\tau - \bar{\tau})$	0	1	$\bar{\tau}$

(2.44)

It follows directly from this table that

$$2\pi i dw = \tau \eta_1 - \eta_\tau, \quad 2\pi i d\bar{w} = \bar{\tau}\eta_1 - \eta_\tau, \tag{2.45}$$

and that

$$\langle dw^r, \eta_\tau^j \eta_1^{r-j} \rangle = \tau^j. \tag{2.46}$$

It will be convenient to work with the basis for $H^1_{\mathrm{dR}}(\mathcal{E}_\tau)$ given by setting

$$\omega = 2\pi i dw, \qquad \eta = \frac{d\bar{w}}{\bar{\tau} - \tau}. \tag{2.47}$$

The class η is completely determined (relative to ω) by the conditions

$$\eta \in H^{0,1}_{\mathrm{dR}}(\mathcal{E}_\tau), \qquad \langle \omega, \eta \rangle = 1.$$

A basis for $H^0(\mathcal{H}, \tilde{\mathcal{L}}_r)$ is given by the expressions $\omega^j \eta^{r-j}$, as $0 \le j \le r$.

Proposition 2.4. *Choose a base point $\tau_0 \in \mathcal{H}$, and let ω, η be given by (2.47). The section F_f of $\tilde{\mathcal{L}}_r$ over $\mathcal{H}$ satisfying*

$$\langle F_f(\tau), \omega^j \eta^{r-j} \rangle = \frac{(-1)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{\tau_0}^{\tau} (z-\tau)^j (z - \bar{\tau})^{r-j} f(z) dz, \quad (0 \le j \le r)$$

is a primitive of ω_f.

Proof. By definition of the Gauss-Manin connection, since the sections $\eta_\tau^j \eta_1^{r-j}$ are horizontal,

$$d\langle F_f, \eta_\tau^j \eta_1^{r-j} \rangle = \langle \nabla F_f, \eta_\tau^j \eta_1^{r-j} \rangle = \langle \mathrm{pr}^* \omega_f, \eta_\tau^j \eta_1^{r-j} \rangle. \tag{2.48}$$

By formula (1.25) for $\mathrm{pr}^* \omega_f$, this last expression is equal to

$$\langle \mathrm{pr}^* \omega_f, \eta_\tau^j \eta_1^{r-j} \rangle = (2\pi i)^{r+1} \langle f(\tau) dw^r, \eta_\tau^j \eta_1^{r-j} \rangle d\tau = (2\pi i)^{r+1} f(\tau) \tau^j d\tau. \tag{2.49}$$

Combining (2.48) and (2.49) and integrating the resulting identity with respect to τ, we find (after fixing some $\tau_0 \in \mathcal{H}$) that the global section of $\tilde{\mathcal{L}}_r$ over $\mathcal{H}$ defined by the rule

$$\langle F_f, \eta_\tau^j \eta_1^{r-j} \rangle = (2\pi i)^{r+1} \int_{\tau_0}^{\tau} f(z) z^j dz, \qquad (0 \le j \le r) \tag{2.50}$$

is a global primitive of ω_f. The defining relation (2.50) implies that, for all homogenous polynomials $P(x, y)$ of degree r,

$$\langle F_f, P(\eta_\tau, \eta_1) \rangle = (2\pi i)^{r+1} \int_{\tau_0}^{\tau} f(z) P(z, 1) dz.$$

After noting from (2.44) that

$$\omega^j \eta^{r-j} = Q(\eta_\tau, \eta_1), \qquad \text{with } Q(x, y) = \frac{(-1)^j}{(2\pi i(\tau - \bar{\tau}))^{r-j}} (x - \tau y)^j (x - \bar{\tau} y)^{r-j},$$

we obtain

$$\langle F_f, \omega^j \eta^{r-j} \rangle = \frac{(-1)^j (2\pi i)^{r+1}}{(2\pi i(\tau - \bar{\tau}))^{r-j}} \int_{\tau_0}^{\tau} (z - \tau)^j (z - \bar{\tau})^{r-j} f(z) dz,$$

as was to be shown. □

Remark 2.7. Recall the Shimura–Maass differential operator δ_r defined by

$$\delta_r f(\tau) := \frac{1}{2\pi i} \left(\frac{d}{d\tau} + \frac{r}{\tau - \bar{\tau}} \right) f(\tau), \tag{2.51}$$

which maps real analytic modular forms of weight r to real analytic modular forms of weight $r + 2$. The real analytic functions G_j on $\mathcal{H}$ defined by the rule

$$G_j(\tau) := \langle F_f(\tau), \omega^j \eta^{r-j} \rangle = \frac{(-1)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{\tau_0}^{\tau} (z - \tau)^j (z - \bar{\tau})^{r-j} f(z) dz$$

satisfy

$$\delta_r G_0(\tau) = f(\tau), \qquad \delta_{r-2j} G_j(\tau) = j G_{j-1}(\tau), \qquad \text{for all } 1 \leq j \leq r. \tag{2.52}$$

For example, the integrand in the expression defining G_0 is antiholomorphic in τ, and thus

$$\begin{aligned}\delta_r G_0(\tau) &= \frac{1}{2\pi i}\left(\frac{d}{d\tau} + \frac{r}{\tau-\bar{\tau}}\right)\frac{2\pi i}{(\tau-\bar{\tau})^r}\int_{\tau_0}^{\tau}(z-\bar{\tau})^r f(z)dz \\ &= \frac{-r}{(\tau-\bar{\tau})^{r+1}}\int_{\tau_0}^{\tau}(z-\bar{\tau})^r f(z)dz + \frac{1}{(\tau-\bar{\tau})^r}(\tau-\bar{\tau})^r f(\tau) \\ &\qquad + \frac{r}{(\tau-\bar{\tau})^{r+1}}\int_{\tau_0}^{\tau}(z-\bar{\tau})^r f(z)dz \\ &= f(\tau).\end{aligned}$$

A similar direct calculation proves (2.52) for all $1 \le j \le r$.

An analogous formula in the p-adic context, with δ_r replaced by the operator $\theta = q\frac{d}{dq}$ on p-adic modular forms, is proved in [12, Prop. 3.24]. The reader may find it instructive to compare (2.52) with its p-adic analogue given in [12, (3.8.6)].

2.2.3 Integral primitives

Propositions 2.3 and 2.4 yield a formula for $\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)$, but this formula is not as explicit as one could desire, because it requires evaluating the primitives $F_f \wedge \alpha$ on the divisor $\widetilde{\Delta}_\varphi$ instead of the simpler divisors $\Delta_\varphi^\natural$ which are supported on a single point $\tau_{A'}$ (but are not of degree 0). We will now study the relation between $[F_f \wedge \alpha, \widetilde{\Delta}_\varphi]$ and $[F_f \wedge \alpha, \Delta_\varphi^\natural]$. Given $Z \in \tilde{\mathbb{L}}_r(\tau) = H^0(\mathcal{H}, \tilde{\mathcal{L}}_r)^{\nabla=0}$, let $P_Z \in \mathbb{C}[x,y]$ be the homogenous polynomial of degree r satisfying

$$Z = P_Z(\eta_\tau, \eta_1).$$

Lemma 2.2. *Let F_f be the primitive of f given in Proposition 2.4. Then for all $\gamma \in \Gamma_1(N)$,*

$$\langle F_f(\gamma\tau), Z\rangle - \langle \gamma F_f(\tau), Z\rangle = (2\pi i)^{r+1}\int_{\tau_0}^{\gamma\tau_0} P_Z(z,1)f(z)dz. \tag{2.53}$$

Proof. By (2.50),

$$\langle F_f(\gamma\tau), Z\rangle = (2\pi i)^{r+1}\int_{\tau_0}^{\gamma\tau} P_Z(z,1)f(z)dz. \tag{2.54}$$

The fact that f is a modular form of weight $r+2$ on $\Gamma_1(N)$, coupled with the fact that P_Z is homogenous of degree r, shows that

$$P_Z(\gamma w, 1)f(\gamma w)d(\gamma w) = P_{\gamma^{-1}Z}(w, 1)f(w)dw.$$

Therefore

$$\begin{aligned}\langle \gamma F_f(\tau), Z\rangle = \langle F_f(\tau), \gamma^{-1}Z\rangle &= (2\pi i)^{r+1}\int_{\tau_0}^{\tau} P_{\gamma^{-1}Z}(z,1)f(z)dz \\ &= (2\pi i)^{r+1}\int_{\gamma\tau_0}^{\gamma\tau} P_Z(z,1)f(z)dz.\end{aligned} \tag{2.55}$$

The lemma follows from (2.54) and (2.55). □

Note in particular that the global section $\tau \mapsto F_f(\gamma\tau) - \gamma F_f(\tau)$ does not depend on τ, and can be viewed as a horizontal section of $\tilde{\mathcal{L}}_r$ over $\mathcal{H}$. The function κ_{F_f} defined on $\Gamma_1(N)$ by

$$\kappa_{F_f}(\gamma) := F_f(\gamma\tau) - \gamma F_f(\tau)$$

is a one-cocycle on $\Gamma_1(N)$ with values in

$$H^0(\mathcal{H}, \tilde{\mathcal{L}}_r)^{\nabla=0} = \tilde{\mathbb{L}}_r(\tau) \simeq L_r(\mathbb{C}),$$

where $L_r(\mathbb{C})$ is the space of homogenous polynomials of degree r in two variables with complex coefficients, equipped with its natural action of $\Gamma_1(N)$. The class of κ_{F_f} in the cohomology group $H^1(\Gamma_1(N), L_r(\mathbb{C}))$ depends only on the differential ω_f and not on the choice of primitive F_f. This class will therefore be denoted by κ_f.

We briefly recall the definition of the period lattice in the space $S_{r+2}(\Gamma_1(N))^\vee$. Let $L_r(\mathbb{Q})$ and $L_r(\mathbb{Z})$ be the rational structure and lattice in $L_r(\mathbb{C})$ obtained by considering the polynomials with rational and integer coefficients respectively, and let $L_r(\mathbb{Z})^\vee$ inside $L_r(\mathbb{Q})$ be the dual lattice relative to the inner product on $L_r(\mathbb{C}) = \mathbb{L}_r(\tau)$ arising from equation

(2.14). After choosing a basis $f_1, \ldots, f_g$ for $S_{r+2}(\Gamma_1(N))$, and a $\mathbb{Z}$-module basis $\kappa_1, \ldots, \kappa_{2g}$ for $H^1_{\mathrm{par}}(\Gamma_1(N), L_r(\mathbb{Z})^\vee)$, let (λ_{ij}) be the $g \times 2g$ matrix with complex entries satisfying

$$\begin{aligned} \kappa_{f_1} &= \lambda_{1,1}\kappa_1 + \cdots + \lambda_{1,2g}\kappa_{2g}, \\ \kappa_{f_2} &= \lambda_{2,1}\kappa_1 + \cdots + \lambda_{2,2g}\kappa_{2g}, \\ \vdots \quad &\vdots \quad \vdots \\ \kappa_{f_g} &= \lambda_{g,1}\kappa_1 + \cdots + \lambda_{g,2g}\kappa_{2g}. \end{aligned} \tag{2.56}$$

For each $1 \leq j \leq 2g$, let $\phi_j \in S_{r+2}(\Gamma_1(N))^\vee$ be the element defined by the rule

$$\phi_j(f_i) = \lambda_{ij}.$$

Definition 2.6. The period lattice attached to $S_{r+2}(\Gamma_1(N))$, denoted Λ_r, is the $\mathbb{Z}$-submodule of $S_{r+2}(\Gamma_1(N))^\vee$ generated by the vectors $\phi_1, \ldots, \phi_{2g}$.

Hodge theory asserts that Λ_r is indeed a lattice (of rank $2g$) in the complex vector space $S_{r+2}(\Gamma_1(N))^\vee$, justifying this terminology. Note that the module Λ_r does not depend on the choices of complex basis for $S_{r+2}(\Gamma_1(N))$ and of integral basis for $H^1_{\mathrm{par}}(\Gamma_1(N), L_r(\mathbb{Z})^\vee)$ that were made to define it.

Let $F_1, \ldots, F_g$ be arbitrarily chosen primitives of $\omega_{f_1}, \ldots, \omega_{f_g}$, and let $\tilde{\kappa}_1, \ldots, \tilde{\kappa}_{2g}$ be a choice of one-cocycles on Γ representing $\kappa_1, \ldots, \kappa_{2g}$. The linear equations (2.56) defining the period lattice imply that there exist vectors $\xi_1, \ldots, \xi_g \in L_r(\mathbb{C})$ such that, for all $\gamma \in \Gamma_1(N)$ and all $\tau \in \mathcal{H}$:

$$\begin{aligned} \kappa_{F_1}(\gamma) &= \lambda_{1,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{1,2g}\tilde{\kappa}_{2g}(\gamma) + (\gamma\xi_1 - \xi_1), \\ \kappa_{F_2}(\gamma) &= \lambda_{2,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{2,2g}\tilde{\kappa}_{2g}(\gamma) + (\gamma\xi_2 - \xi_2), \\ \vdots \quad &\vdots \quad \vdots \\ \kappa_{F_g}(\gamma) &= \lambda_{g,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{g,2g}\tilde{\kappa}_{2g}(\gamma) + (\gamma\xi_g - \xi_g). \end{aligned} \tag{2.57}$$

After replacing F_j by $F_j + \xi_j$ (viewing the ξ_j as elements of $H^0(\mathcal{H}, \tilde{\mathcal{L}}_r)^{\nabla=0}$), we obtain a new collection of primitives satisfying the following relation, for all $\gamma \in \Gamma_1(N)$ and $\tau \in \mathcal{H}$:

$$\begin{aligned} F_1(\gamma\tau) - \gamma F_1(\tau) &= \lambda_{1,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{1,2g}\tilde{\kappa}_{2g}(\gamma), \\ F_2(\gamma\tau) - \gamma F_2(\tau) &= \lambda_{2,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{2,2g}\tilde{\kappa}_{2g}(\gamma), \\ &\vdots \\ F_g(\gamma\tau) - \gamma F_g(\tau) &= \lambda_{g,1}\tilde{\kappa}_1(\gamma) + \cdots + \lambda_{g,2g}\tilde{\kappa}_{2g}(\gamma). \end{aligned} \tag{2.58}$$

Definition 2.7. A collection of integral primitives is a choice of a primitive F_j of f_j for each $j = 1, \ldots, g$ satisfying (2.58). Such a collection determines, by linearity, a primitive F_f of f for each $f \in S_{r+2}(\Gamma_1(N))$. The primitive F_f arising from such a choice will be called an integral primitive of ω_f.

Lemma 2.3. *Let $f \mapsto F_f$ be a choice of integral primitives of f. For each $\gamma \in \Gamma_1(N)$ and $v \in L_r(\mathbb{Z})$, the assignment*

$$f \mapsto \langle F_f(\gamma\tau) - \gamma F_f(\tau), v\rangle$$

belongs to $\Lambda_r \subset S_{r+2}(\Gamma_1(N))^\vee$.

Proof. This follows directly from (2.58) in light of the fact that the scalars

$$\langle \tilde{\kappa}_1(\gamma), v\rangle, \ldots, \langle \tilde{\kappa}_{2g}(\gamma), v\rangle$$

are integers. □

By definition, the $\mathbb{Z}$-module

$$\Lambda_{r,r} := \Lambda_r \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Z})$$

is a lattice in $S_{r+2}(\Gamma)^\vee \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C})^\vee = \mathrm{Fil}^{r+1} \epsilon_{X_r} H^{2r+1}_{\mathrm{dR}}(X_r)^\vee$. It is commensurable with the lattice $\Pi_{r,r}$ appearing in (2.37). After eventually replacing $\Lambda_{r,r}$ by a larger lattice, we may therefore assume that $\Lambda_{r,r}$ contains $\Pi_{r,r}$. This assumption allows us to replace $\Pi_{r,r}$ by $\Lambda_{r,r}$ in the arguments to follow.

Lemma 2.3 implies that

$$\langle F_f(\gamma\tau)\wedge\alpha, Z\rangle = \langle F_f(\tau)\wedge\alpha, \gamma^{-1}Z\rangle \pmod{\Lambda_{r,r}}, \tag{2.59}$$

for all $Z \in L_r(\mathbb{Z}) \otimes \operatorname{Sym}^r H^1(A,\mathbb{Z})$. Here both f and α are treated as variables, and the equality is viewed as taking place in $\operatorname{Fil}^{r+1} \epsilon_{X_r} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C})^\vee$.

The Abel–Jacobi image of generalised Heegner cycles can be expressed more simply in terms of integral primitives, as follows.

Proposition 2.5. *Let $f \mapsto F_f$ be a choice of integral primitives, and let Δ_φ be a generalised Heegner cycle attached to $\varphi : A \longrightarrow A'$. Then*

$$\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f\wedge\alpha) = \langle F_f(\tau_{A'})\wedge\alpha, \mathrm{cl}_{\tau_{A'}}(\Delta_\varphi^\natural)\rangle \pmod{\Lambda_{r,r}},$$

where the pairing is the natural one on $\tilde{\mathbb{L}}_{r,r}(\tau_{A'})$.

Proof. By Proposition 2.3 combined with the formula (2.33) for $\widetilde{\Delta}_\varphi$,

$$\begin{aligned}
\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f\wedge\alpha) &= [F_f\wedge\alpha, \widetilde{\Delta}_\varphi] \pmod{\Lambda_{r,r}} \\
&= \sum_{j=1}^{t}\langle F_f(\gamma_j\tau_{A'})\wedge\alpha, Z_j\rangle - \langle F_f(\tau_{A'})\wedge\alpha, Z_j\rangle \pmod{\Lambda_{r,r}} \\
&= \sum_{j=1}^{t}\langle F_f(\tau_{A'})\wedge\alpha, \gamma_j^{-1}Z_j\rangle - \langle F_f(\tau_{A'})\wedge\alpha, Z_j\rangle \pmod{\Lambda_{r,r}} \\
&= \langle F_f(\tau_{A'})\wedge\alpha, \sum_{j=1}^{t}(\gamma_j^{-1}-1)Z_j\rangle \pmod{\Lambda_{r,r}},
\end{aligned}$$

where we have used (2.59) in deriving the penultimate equality. Proposition 2.5 now follows from equation (2.32) for the class of $\Delta_\varphi^\natural$. □

Proposition 2.6. *With the same notations as in Proposition 2.5,*

$$\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f \wedge \alpha) = \langle \varphi^* F_f(\tau_{A'}), \alpha \rangle_A \pmod{\Lambda_{r,r}},$$

where the pairing $\langle\ ,\ \rangle_A$ *on the right is the Poincaré duality on* $\mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C})$.

Proof. Let

$$\varrho := (\varphi^r, \mathrm{id}^r) : A^r \longrightarrow \Upsilon_\varphi \subset (A')^r \times A^r.$$

Note that

$$\varrho^*(F_f(\tau_{A'}) \wedge \alpha) = \varphi^*(F_f(\tau_{A'})) \wedge \alpha, \qquad \varrho([A^r]) = \mathrm{cl}_{\tau_{A'}}(\Upsilon^\natural_\varphi),$$

where $[A^r] \in H^0_{\mathrm{dR}}(A^r/\mathbb{C})$ is the fundamental class associated to the variety A^r. Let

$$\langle\ ,\ \rangle_{A,j} : H^{2r-j}_{\mathrm{dR}}(A^r/\mathbb{C}) \times H^j_{\mathrm{dR}}(A^r/\mathbb{C}) \longrightarrow H^{2r}(A^r/\mathbb{C}) = \mathbb{C}$$

denote the Poincaré pairing, so that the restriction of $\langle\ ,\ \rangle_{A,r}$ to the subspace

$$\mathrm{Sym}^r H^1_{\mathrm{dR}}(A/\mathbb{C}) \subset H^r_{\mathrm{dR}}(A/\mathbb{C})$$

agrees with $\langle\ ,\ \rangle_A$. Observe that

$$\langle F_f(\tau_{A'}) \wedge \alpha, \mathrm{cl}_{\tau_{A'}}(\Delta^\natural_\varphi)\rangle = \langle F_f(\tau_{A'}) \wedge \alpha, \mathrm{cl}_{\tau_{A'}}(\Upsilon^\natural_\varphi)\rangle = \langle F_f(\tau_{A'}) \wedge \alpha, \varrho([A^r])\rangle. \tag{2.60}$$

The functoriality properties of the Poincaré pairing imply that

$$\begin{aligned} \langle F_f(\tau_{A'}) \wedge \alpha, \varrho([A^r])\rangle &= \langle \varrho^*(F_f(\tau_{A'}) \wedge \alpha), [A^r]\rangle_{A,0} \\ &= \langle \varphi^*(F_f(\tau_{A'})) \wedge \alpha, [A^r]\rangle_{A,0} = \langle \varphi^*(F_f(\tau_{A'})), \alpha\rangle_A. \end{aligned} \tag{2.61}$$

Proposition 2.6 follows by combining Proposition 2.5 with (2.60) and (2.61). □

2.2.4 Modular symbols

Propositions 2.5 and 2.6 gain in explicitness because they involve the divisor $\Delta_\varphi^\natural$ supported on a single point, rather that the more complicated divisor (2.32) which is given in terms of a (non-canonical) expression for the class of $\Delta_\varphi^\natural$ as an element of $I_{\Gamma_1(N)}H_{2r}(\tilde{X}_r, \mathbb{Q})$. The price one pays is that it becomes necessary to work with integral primitives rather than arbitrary primitives.

In the case of a group like $\Gamma_1(N)$ containing parabolic elements, an integral primitive can be defined explicitly by invoking the theory of modular symbols. More precisely, let us define primitives F_f of ω_f by allowing the base point τ_0 appearing in Proposition 2.4 to tend to a cusp. The integrals appearing in Proposition 2.4 still converge, by the cuspidality of f. Furthermore, the right-hand term appearing in (2.53) is of the form

$$J_{s,t,P}(f) := (2\pi i)^{r+1}\int_s^t P(z)f(z)dz, \qquad \text{with } s,t\in\mathbb{P}^1(\mathbb{Q}), \quad P(x)\in\mathbb{Z}[x]^{\deg=r}.$$

Let Λ_r' denote the $\mathbb{Z}$-module generated by Λ_r and the functionals $J_{s,t,P}$ in the complex vector space $S_{r+2}(\Gamma_1(N))^\vee$. The following theorem is the basis for the theory of "modular symbols" attached to modular forms of higher weight.

Proposition 2.7. *The group Λ_r' is a sublattice of $S_{r+2}(\Gamma_1(N))^\vee$ which contains Λ_r with finite index.*

Proof. The proof of this theorem can be found, for instance, in Proposition 3.5 of [128]. The statement and proof are given there for $r = 2$, i.e., forms of weight 4, but no serious modification is required to handle the case of general r. □

After replacing the period lattice Λ_r by the possibly slightly larger lattice Λ_r', and re-defining $\Lambda_{r,r}$ accordingly, we obtain Theorem 2.1 below on the complex Abel–Jacobi images of generalised Heegner cycles, which is one of the two main results of this chapter. Because the formula is given modulo a larger lattice, it is slightly less precise, but has the virtue of being more explicit and amenable to numerical calculation.

Theorem 2.1. *Let $\varphi : A \longrightarrow \mathbb{C}/\langle 1, \tau\rangle$ be an isogeny of degree $d_\varphi = \deg(\varphi)$, satisfying*

$$\varphi(t_A) = \frac{1}{N}, \qquad \varphi^*(2\pi i dw) = \omega_A,$$

and let Δ_φ be the associated generalised Heegner cycle on X_r. Then

$$\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f \wedge \omega_A^j \eta_A^{r-j}) = \frac{(-d_\varphi)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{i\infty}^{\tau} (z-\tau)^j (z-\bar{\tau})^{r-j} f(z) dz \pmod{\Lambda_{r,r}}.$$

Proof. Let F_f be the integral primitive of ω_f obtained by setting $\tau_0 = i\infty$. By Proposition 2.6,

$$\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f \wedge \omega_A^j \eta_A^{r-j}) = \langle \varphi^* F_f(\tau), \omega_A^j \eta_A^{r-j}\rangle_A \pmod{\Lambda_{r,r}}. \tag{2.62}$$

But letting $\omega', \eta' \in H^1_{\mathrm{dR}}(\mathbb{C}/\langle 1,\tau\rangle)$ be defined by

$$\omega' = 2\pi i dw, \qquad \eta' \in H^{0,1}_{dR}(\mathbb{C}/\langle 1, \tau\rangle), \qquad \langle \omega', \eta'\rangle = 1,$$

we have

$$\varphi^*(\omega') = \omega_A, \qquad \varphi^*(\eta') = d_\varphi \eta_A. \tag{2.63}$$

Hence

$$\begin{aligned} \langle \varphi^* F_f(\tau), \omega_A^j \eta_A^{r-j}\rangle_A &= d_\varphi^{j-r} \langle \varphi^* F_f(\tau), \varphi^*((\omega')^j (\eta')^{r-j})\rangle_A \\ &= d_\varphi^j \langle F_f(\tau), (\omega')^j (\eta')^{r-j}\rangle_{A'}. \end{aligned}$$

The result now follows from Proposition 2.4 with $\tau_0 = i\infty$. □

2.2.5 Summary

For the convenience of the reader, we summarise the Abel–Jacobi computation in one big self-contained calculation. Hopefully, this will allow for a better overview of the underlying strategy, as well as for a broader appreciation of the bigger picture.

So let $f \in S_{r+2}(\Gamma_1(N))$, and let F_f be the integral primitive of ω_f obtained from Proposition 2.4 by taking $\tau_0 = i\infty$. As previously, we work modulo $\Lambda_{r,r} = \Lambda_r \otimes \mathrm{Sym}^r H_1(A(\mathbb{C}), \mathbb{Z})$, where $\Lambda_r \subset S_{r+2}(\Gamma_1(N))^\vee$ is taken large enough so that it contains the lattice Λ_r' of Proposition 2.7. Retain the notations and assumptions of Theorem 2.1. Then, working with equalities modulo $\Lambda_{r,r}$, we have:

$$\begin{aligned}
\mathrm{AJ}_{\mathbb{C}}(\Delta_\varphi)(\omega_f \wedge \omega_A^j \eta_A^{r-j}) &= \int_{\mathrm{pr}_*(\widetilde{\Delta}_\varphi^\sharp)} \omega_f \wedge \omega_A^j \eta_A^{r-j} \\
&= \int_{\widetilde{\Delta}_\varphi^\sharp} \mathrm{pr}^* \omega_f \wedge \omega_A^j \eta_A^{r-j} \\
&= \sum_{j=1}^{t} \int_\tau^{\gamma_j \tau} \langle \mathrm{pr}^* \omega_f \wedge \omega_A^j \eta_A^{r-j}, \theta_{Z_j}^\nabla \rangle \\
&= \sum_{j=1}^{t} \int_\tau^{\gamma_j \tau} d\langle F_f \wedge \omega_A^j \eta_A^{r-j}, \theta_{Z_j}^\nabla \rangle \\
&= \sum_{j=1}^{t} (\langle F_f(\gamma_j\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{PD}_{\gamma_j\tau}(Z_j)\rangle - \langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{PD}_\tau(Z_j)\rangle) \\
&= \sum_{j=1}^{t} (\langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{PD}_\tau(\gamma_j^{-1} Z_j)\rangle - \langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{PD}_\tau(Z_j)\rangle) \\
&= \left\langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \sum_{j=1}^{t} \mathrm{PD}_\tau((\gamma_j^{-1} - 1) Z_j) \right\rangle \\
&= \langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{cl}_\tau(\Delta_\varphi^\natural)\rangle \\
&= \langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \mathrm{cl}_\tau(\Upsilon_\varphi^\natural)\rangle \\
&= \langle F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}, \varrho([A^r])\rangle \\
&= \langle \varrho^*(F_f(\tau) \wedge \omega_A^j \eta_A^{r-j}), [A^r])\rangle_{A,0} \\
&= \langle \varphi^*(F_f(\tau)) \wedge \omega_A^j \eta_A^{r-j}, [A^r])\rangle_{A,0} \\
&= \langle \varphi^*(F_f(\tau)), \omega_A^j \eta_A^{r-j}\rangle_A \\
&= d_\varphi^{j-r} \langle \varphi(F_f(\tau)), \varphi^*((\omega')^j (\eta')^{r-j})\rangle_A \\
&= d_\varphi^j \langle F_f(\tau), (\omega')^j (\eta')^{r-j}\rangle_{A'} \\
&= \frac{(-d_\varphi)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{i\infty}^{\tau} (z-\tau)^j (z - \bar{\tau})^{r-j} f(z) dz.
\end{aligned}$$

2.3 The Chow group of X_r

Assume in this section that A is isomorphic over $\mathbb{C}$ to the complex torus $\mathbb{C}/\mathcal{O}_K$ and let X_r be the $(2r+1)$-dimensional variety over H defined previously. For simplicity, we assume that $d_K \neq 3, 4$, so that $\mathcal{O}_K^\times = \{\pm 1\}$. For any field F, recall from (1.50) the definition of the Griffiths group

$$\mathrm{Gr}^{r+1}(X_r)(F) := \mathrm{CH}^{r+1}(X_r)_0(F)/\,\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(F),$$

where $\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(F)$ is the subgroup of null-homologous codimension $r+1$ cycles on X_r that are defined over F and are algebraically equivalent to zero.

The goal of this section is to prove the following:

Theorem 2.2. *For all $r \geq 0$ the Chow group $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ of null-homologous cycles modulo rational equivalence has infinite rank. Furthermore, for all $r \geq 2$, the Griffiths group $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$ also has infinite rank.*

The proof follows closely that of Theorem 4.7 of Schoen's paper [128] which treats the case of "usual" Heegner cycles on a Kuga–Sato threefold, and rests on an ingenious method of Bloch. The most significant difference lies in the setting that is treated: whereas Schoen's cycles are indexed by arbitrary quadratic orders of varying discriminant, generalised Heegner cycles are forced by necessity to be indexed by (not necessarily maximal) orders of the fixed imaginary quadratic field K. The reader is referred to Chapter 1 for background material on the tools from class field theory, complex multiplication theory, and étale cohomology that are used below, as well as to the introduction of [12] for further background on generalised Heegner cycles beyond the material covered in the earlier sections.

Remark 2.8. When $r = 0$ the variety X_0 is the modular curve $X_1(N)$ which is defined over $\mathbb{Q}$. Codimension 1 cycles are divisors and rational equivalence corresponds to linear equivalence on divisors, whence $\mathrm{CH}^1(X_1(N)) = \mathrm{Pic}(X_1(N))$. Moreover, a divisor is null-homologuous if and only if it has degree zero and any degree zero divisor on a smooth connected curve is algebraically equivalent to zero, as explained in Example 1.2. It follows that the Griffiths group $\mathrm{Gr}^1(X_1(N))$ is trivial. The content of Theorem 2.2 is that the Chow group $\mathrm{CH}^1(X_1(N))_0(\bar{\mathbb{Q}})$ has infinite rank, a well-known result. The generalised Heegner cycles in this case are images of Heegner points on the Jacobian variety of $X_1(N)$, see Definition 2.1, and the method consists in showing that the subgroup generated by these Heegner points has infinite rank. In [90, Proposition 2.8], it is shown that $E(\bar{\mathbb{Q}})$ has infinite rank where E is an elliptic curve defined over $\mathbb{Q}$ by proving that the subgroup generated by Heegner points on $X_0(N)$ via a modular parametrisation $X_0(N) \longrightarrow E$ has infinite rank. In particular, this implies Theorem 2.2 in the case $r = 0$.

Notation 2.1. Throughout this section we will adopt the following notational conventions. If X is a variety defined over H and F is any field containing H, then we let X_F denote its base change to F, i.e., $X \times_{\mathrm{Spec}\, H} \mathrm{Spec}\, F$. We fix an algebraic closure $\bar{H}$ of H and we will use the shorthand notation $\bar{X} := X_{\bar{H}}$. Recall that K has discriminant $-d_K$ and $\mathcal{O}_K$ denotes its ring of integers. Let $\tau := (-d_K + \sqrt{-d_K})/2$ be the standard generator of $\mathcal{O}_K = \langle 1, \tau \rangle$, as in the beginning of Section 1.3.1. Fix an analytic isomorphism $\xi : \mathbb{C}/\mathcal{O}_K \simeq A(\mathbb{C})$ and let $\omega_A \in \Omega^1_{A/H}$ be the regular differential satisfying $\xi^*(\omega_A) = 2\pi i dw$.

2.3.1 A subcollection of cycles

We introduce a distinguished subcollection of generalised Heegner cycles. The fields of definition of these cycles will play a crucial role in Section 2.3.3 and the understanding of the Galois action on these cycles is key in Section 2.3.4.

Let p and q be distinct odd primes which are congruent to 1 modulo N, and consider the following lattices associated to $\beta \in \mathbb{P}^1(\mathbb{F}_q)$,

$$\Lambda_{p,q,\infty} := \mathbb{Z}\frac{1}{pq} \oplus \mathbb{Z}\tau, \qquad \Lambda_{p,q,\beta} := \mathbb{Z}\frac{1}{p} \oplus \mathbb{Z}\frac{\tau + \beta}{q}, \quad \text{for } 0 \leq \beta \leq q-1,$$

which each contain $\mathcal{O}_K$ with index pq, and let $A_{p,q,\beta}$ be the elliptic curve whose complex points are isomorphic to $\mathbb{C}/\Lambda_{p,q,\beta}$. The natural isogeny

$$\varphi_{p,q,\beta} : A \longrightarrow A_{p,q,\beta} \tag{2.64}$$

of degree pq gives rise to the generalised Heegner cycle

$$\Delta_{p,q,\beta} := \Delta_{\varphi_{p,q,\beta}}. \tag{2.65}$$

The theory of complex multiplication, as reviewed in Section 1.3, allows us to pin down the field of definition of the cycles $\Delta_{p,q,\beta}$. Let F_{pq} denote the field compositum of $K_{\mathfrak{N}}$ and H_{pq}, where $K_{\mathfrak{N}}$ denotes the ray class field of K of modulus $\mathfrak{N}$ defined in Assumption 2.1, and H_{pq} is the ring class field of K conductor pq. See Definition 1.9 and 1.11.

Proposition 2.8. *For all $\beta \in \mathbb{P}^1(\mathbb{F}_q)$, the cycle $\Delta_{p,q,\beta}$ is defined over F_{pq}.*

Proof. The Kuga–Sato variety W_r is defined over $\mathbb{Q}$, and the elliptic curve A along with its complex multiplication can be defined over the Hilbert class field H of K by Theorem 1.2. Following the moduli description of $X_1(N)$, the pair (A, t_A) corresponds to a complex point on $X_1(N)$ defined over the abelian extension of K corresponding to the subgroup $K^\times W \subset \mathbb{A}_K^\times$, where

$$W := \left\{ x \in \mathbb{A}_K^\times \,:\, x\mathcal{O}_K = \mathcal{O}_K,\ x\xi^{-1}(t_A) = \xi^{-1}(t_A) \right\}.$$

This field is the ray class field $K_{\mathfrak{N}}$ of K of conductor $\mathfrak{N}$ by Theorem 1.3. The elliptic curves $A_{p,q,\beta}$ have complex multiplication by the order $\mathcal{O}_{pq}$ of conductor pq and can thus be defined over the ring class field H_{pq} by Theorem 1.2. The isogenies $\varphi_{p,q,\beta}$ are also defined over H_{pq}. Note that since $(pq, N) = 1$, we have $(\varphi_{p,q,\beta}, A_{p,q,\beta}) \in \mathrm{Isog}^{\mathfrak{N}}(A)$. The point $(A_{p,q,\beta}, t_{A_{p,q,\beta}})$ on $X_1(N)$ can thus be defined over the field compositum F_{pq}. Since the correspondence ϵ_{X_r} of Definition 2.2 that was used to define the generalised Heegner cycle is defined over $\mathbb{Q}$, we can conclude that the cycle $\Delta_{p,q,\beta}$ is defined over F_{pq} as well. □

Remark 2.9. More generally, let (φ, A') be an element of $\mathrm{Isog}(A)$. Since A has complex multiplication by $\mathcal{O}_K$, the endomorphism ring of A' is an order in $\mathcal{O}_K$. Such an order is completely determined by its conductor, as explained in Section 1.3.1, and therefore there is a unique integer $c \geq 1$ such that $\mathrm{End}_{\bar{K}}(A') = \mathcal{O}_c := \mathbb{Z} + c\mathcal{O}_K$. The pair (φ, A') is then said to be of conductor c and we set

$$\mathrm{Isog}_c(A) := \{\text{Isomorphism classes of pairs } (\varphi, A') \text{ of conductor } c\}$$

and $\mathrm{Isog}_c^{\mathfrak{N}}(A) := \mathrm{Isog}_c(A) \cap \mathrm{Isog}^{\mathfrak{N}}(A)$. Note that if $(\varphi, A') \in \mathrm{Isog}_c^{\mathfrak{N}}(A)$, then by a similar reasoning as above the associated cycle Δ_φ is defined over the field compositum $F_\varphi := K_{\mathfrak{N}} \cdot H_c$, where $H_c := K(j(\mathcal{O}_c))$ denotes the ring class field of K of conductor c.

2.3.2 Cycles of large order

Using the explicit formula for the image of generalised Heegner cycles under the complex Abel–Jacobi map obtained in Theorem 2.1, we will now prove, following the approach of [128, §3], that many of the cycles $\Delta_{p,q,\beta}$ are of large (possibly infinite) order in the Chow group and even in the Griffiths group (if $r \geq 1$). This part of the argument uses only complex analytic and Hodge theoretic methods, and rests on the following theorem.

Theorem 2.3. *For all $r \geq 0$ (resp. for all $r \geq 1$) the order of $\Delta_{p,q,\beta}$ in $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ (resp. in $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$) tends to ∞ as p/q tends to ∞.*

Remark 2.10. If $f \in S_{r+2}(\Gamma_1(N))$ and $0 \leq j \leq r$, then we will identify, by a slight abuse of notation, $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j})$ with the complex number appearing in the right hand side of the displayed equation in Theorem 2.1. This amounts to choosing a fixed representative of $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})$ in $(S_{r+2}(\Gamma_1(N)) \otimes \mathrm{Sym}^r H^1_{\mathrm{dR}}(A))^\vee$, and then evaluating it at $\omega_f \wedge \omega_A^j \eta_A^{r-j}$.

The proof of Theorem 2.3 relies on the following intermediate result.

Lemma 2.4. *For any non-zero cusp form f,*

$$\lim_{p/q\to\infty} \mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) = 0$$

and $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j})$ *is non-zero for all large enough* p/q.

Proof. Fix p, q, and $\beta \in \mathbb{P}^1(\mathbb{F}_q)$. The lattice $\Lambda_{p,q,\beta}$ is homothetic to $\langle 1, \tau_{p,q,\beta}\rangle$, where

$$\tau_{p,q,\infty} := pq\tau, \qquad \tau_{p,q,\beta} := \frac{p}{q}(\tau+\beta). \tag{2.66}$$

Set $\tau_{p,q,\beta} := X_\beta + iY_\beta$, and note that

$$Y_\beta = \begin{cases} pq\cdot\sqrt{d_K}/2 & \text{if } \beta=\infty \\ p/q\cdot\sqrt{d_K}/2 & \text{if } \beta\neq\infty. \end{cases}$$

By Theorem 2.1, $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j})$ is equal to

$$\begin{aligned} \frac{(-1)^j(2\pi i)^{j+1}\cdot\kappa_\beta}{(\tau-\bar{\tau})^{r-j}} &\int_{i\infty}^{\tau_{p,q,\beta}} (z-\tau_{p,q,\beta})^j (z-\bar{\tau}_{p,q,\beta})^{r-j} f(z)dz \\ &= \gamma_\beta \int_{Y_\beta}^{\infty} (y-Y_\beta)^j (y+Y_\beta)^{r-j} f(X_\beta+iy)dy, \end{aligned} \tag{2.67}$$

where

$$\kappa_\beta := \begin{cases} (pq)^{2j-2r} & \text{if } \beta=\infty, \\ p^{2j-2r}q^r & \text{if } \beta\neq\infty, \end{cases} \qquad \gamma_\beta := (-1)^{j+1}\cdot i^{r+1}\cdot(2\pi i)^{j+1}\cdot\frac{\kappa_\beta}{(\tau-\bar{\tau})^{r-j}},$$

and the equality in (2.67) is obtained by performing the change of variables $z = X_\beta + iy$.

Assume, without loss of generality, that f is a normalised cuspidal eigenform. By examination of the Fourier expansion of f, there is an absolute real constant $C_f > 0$ (depending only on f) for which

$$|f(z) - e^{2\pi i z}| \le C_f \cdot e^{-4\pi \mathrm{Im}(z)}$$

on the domain $\{\mathrm{Im}(z) > 1\}$. Combining this with (2.67) gives

$$\begin{aligned}\left|\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) - \gamma_\beta \cdot e^{2\pi i X_\beta} \cdot A_\beta\right| \\ \leq \gamma_\beta \cdot C_f \cdot \int_{Y_\beta}^{\infty} (y - Y_\beta)^j (y + Y_\beta)^{r-j} e^{-4\pi y} dy, \quad (2.68)\end{aligned}$$

where

$$A_\beta := \int_{Y_\beta}^{\infty} (y - Y_\beta)^j (y + Y_\beta)^{r-j} e^{-2\pi y} dy \tag{2.69}$$

is clearly non-zero and positive since the function appearing in the integral is strictly positive on the domain of integration. The error term in (2.68) is majorised by

$$\left|\gamma_\beta \cdot C_f \cdot \int_{Y_\beta}^{\infty} (y - Y_\beta)^j (y + Y_\beta)^{r-j} e^{-4\pi y} dy\right| \leq C_f \cdot \gamma_\beta \cdot e^{-2\pi Y_\beta} A_\beta. \tag{2.70}$$

If we let

$$B_\beta := \gamma_\beta \cdot e^{2\pi i X_\beta} \cdot A_\beta, \tag{2.71}$$

then (2.70) implies that $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j})$ is asymptotically equivalent, as a function of p and q, to B_β as p/q tends to infinity, in the sense that the ratio of these two functions tends to 1 as p/q tends to infinity. The result now follows after observing that the quantity B_β is non-zero but tends to 0 as p/q tends to infinity. □

Proof of Theorem 2.3. As p/q tends to ∞, Lemma 2.4 shows that $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})$ tends to the origin in $J^{r+1}(X_r/\mathbb{C})$ without being equal to it. Consequently, the order of $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})$ tends to ∞ in $J^{r+1}(X_r/\mathbb{C})$. It follows that the order of $\Delta_{p,q,\beta}$ in the Chow group $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ tends to ∞ as p/q tends to ∞.

To treat the image of $\Delta_{p,q,\beta}$ in the Griffiths group, let $J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}}$ denote, following Definition 1.20, the complex subtorus of $J^{r+1}(X_r/\mathbb{C})$ which is the intermediate Jacobian of the largest sub-Hodge structure V of $H^{r+1,r}(X_r) \oplus H^{r,r+1}(X_r)$. More precisely,

$$J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}} = J^{r+1}(V) := V_{\mathbb{C}}/(\mathrm{Fil}^{r+1} V \oplus V_{\mathbb{Z}}). \tag{2.72}$$

The image of $\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\mathbb{C})$ under $\mathrm{AJ}_{\mathbb{C}}$ is a complex subtorus of $J^{r+1}(X_r/\mathbb{C})$ which is contained in $J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}}$ and has the structure of an abelian variety, as explained in Proposition 1.11. One can thus define the transcendental part of the Abel–Jacobi map (1.54)

$$\mathrm{AJ}_{\mathbb{C},\mathrm{tr}} : \mathrm{Gr}^{r+1}(X_r)(\mathbb{C}) \longrightarrow J^{r+1}(X_r/\mathbb{C})_{\mathrm{tr}} := J^{r+1}(X_r/\mathbb{C})/J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}} \tag{2.73}$$

as the factorisation of $\mathrm{AJ}_{\mathbb{C}}$. Note that for $r = 0$, $J^{r+1}(X_r/\mathbb{C}) = J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}}$ and $\mathrm{Gr}^{r+1}(X_r)(\mathbb{C}) = 0$ by Remark 2.8, so the transcendental part of the Abel–Jacobi map is trivial in this case. For $r \geq 1$, by (2.1), we observe that

$$(H^{r+1,r}(X_r) \oplus H^{r,r+1}(X_r)) \cap \epsilon_{X_r} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C}) = (S_{r+2}(\Gamma_1(N)) \otimes \mathbb{C}\eta^r_A) \oplus (\overline{S_{r+2}(\Gamma_1(N))} \otimes \mathbb{C}\omega^r_A).$$

The same reasoning as before shows that the order of $\Delta_{p,q,\beta}$ in $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$ tends to ∞ with p/q. □

2.3.3 Cycles of infinite order

Theorem 2.3 implies that for sufficiently large p/q, the cycles $\Delta_{p,q,\beta}$ have large (possibly infinite) order in the Chow group. Following [128, §4], we show that for large p/q, the cycles $\Delta_{p,q,\beta}$ are non-torsion in the Chow group. This section constitutes the algebraic part of the argument, where the fields of definition of the cycles play a crucial role.

Proposition 2.9. *For all $r \geq 0$, there exists a non-negative integer M_r with the property that if $\Delta \in \langle\{\Delta_{p,q,\beta}\}\rangle \subset \mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ is such that the order of $\mathrm{AJ}_{\mathbb{C}}(\Delta)$ in $J^{r+1}(X_r/\mathbb{C})$ does not divide M_r, then Δ has infinite order in $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$.*

Before proving this proposition, we deduce the following two corollaries.

Corollary 2.1. *For p/q sufficiently large, $\Delta_{p,q,\beta}$ has infinite order in the Chow group.*

Proof. It suffices to combine Lemma 2.4 and Proposition 2.9. □

Corollary 2.2. *Fix a rational prime q congruent to 1 modulo N. There exist infinitely many rational primes p congruent to 1 modulo N such that the cycle $\Delta_{p,q,\beta} - \Delta_{p,q,\gamma}$ has infinite order in the Chow group when $\beta \neq \gamma$.*

Proof. Let f be a normalised cuspidal eigenform and consider $B_\beta = \gamma_\beta \cdot e^{2\pi i X_\beta} \cdot A_\beta$ of (2.71) defined in the proof of Lemma 2.4 for all $\beta \in \mathbb{P}^1(\mathbb{F}_q)$. If $\beta = \infty$, then $\gamma \neq \infty$ and a comparison of integrals reveals that

$$\left|\frac{B_\infty}{B_\gamma}\right| \leq e^{-\pi\frac{p}{q}(q^2-1)\sqrt{d_K}} q^{2(j+1)-r}$$

from which we deduce that B_∞/B_γ tends to zero as p/q tends to ∞. In particular, B_∞ and B_γ are not asymptotically equivalent as $p/q \to \infty$ and it follows that for infinitely many p/q,

$$\mathrm{AJ}_\mathbb{C}(\Delta_{p,q,\infty})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) \neq \mathrm{AJ}_\mathbb{C}(\Delta_{p,q,\gamma})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) \tag{2.74}$$

since asymptotic equivalence is an equivalence relation. Moreover, we have

$$\lim_{p/q \to \infty} \mathrm{AJ}_\mathbb{C}(\Delta_{p,q,\infty} - \Delta_{p,q,\gamma}) = 0. \tag{2.75}$$

Suppose now that $\beta, \gamma \neq \infty$ and observe that $B_\beta = e^{2\pi i \frac{p}{q}(\beta-\gamma)} B_\gamma$, so the complex argument of the ratio B_β/B_γ is greater in absolute value than $2\pi/q$ for all p. In particular, B_β and B_γ are not asymptotically equivalent as p tends to ∞ and thus for infinitely many rational primes p congruent to 1 modulo N,

$$\mathrm{AJ}_\mathbb{C}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) \neq \mathrm{AJ}_\mathbb{C}(\Delta_{p,q,\gamma})(\omega_f \wedge \omega_A^j \eta_A^{r-j}). \tag{2.76}$$

Moreover, we have $\lim_{p/q\to\infty} \mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta} - \Delta_{p,q,\gamma}) = 0$.

Hence, by taking p sufficiently large, we can ensure that the order of $\mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta} - \Delta_{p,q,\gamma})$ in $J^{r+1}(X_r/\mathbb{C})$ is greater than M_r and thus, by Proposition 2.9, $\Delta_{p,q,\beta} - \Delta_{p,q,\gamma}$ is non-torsion in $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$. □

We now turn to the proof of Proposition 2.9. For any rational prime ℓ, Bloch [27] has defined a map of Galois modules

$$\lambda_\ell := \lambda_\ell^{r+1} : \mathrm{CH}^{r+1}(X_r)(\bar{H})(\ell) \longrightarrow H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1)) \tag{2.77}$$

where $\mathrm{CH}^{r+1}(X_r)(\bar{H})(\ell)$ denotes the ℓ-power torsion subgroup. The construction of this map was reviewed in Section 1.5.2 along with its salient properties. Recall in particular the short exact sequence (1.70)

$$0 \longrightarrow J^{r+1}(X_r/\mathbb{C})_{\mathrm{tors}} \xrightarrow{u} H^{2r+1}(X_r(\mathbb{C}), \mathbb{Q}/\mathbb{Z}) \longrightarrow H^{2r+2}(X_r(\mathbb{C}), \mathbb{Z})_{\mathrm{tors}} \longrightarrow 0, \tag{2.78}$$

which identifies $J^{r+1}(X_r/\mathbb{C})_{\mathrm{tors}}$ up to a finite group with $H^{2r+1}(X_r(\mathbb{C}), \mathbb{Q}/\mathbb{Z})$.

Summing over all primes ℓ yields a map of Galois modules

$$\lambda : \mathrm{CH}^{r+1}(X_r)(\bar{H})_{\mathrm{tors}} \longrightarrow H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1)) \tag{2.79}$$

which, by Proposition 1.20, fits into a commutative diagram

$$\begin{array}{ccc} \mathrm{CH}^{r+1}(X_r)_0(\bar{H})_{\mathrm{tors}} & \xrightarrow{\lambda} & H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1)) \\ \downarrow \sigma_* & & \wr\downarrow (1.73) \\ \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C})_{\mathrm{tors}} & \xrightarrow{u\circ \mathrm{AJ}_{\mathbb{C}}} & H^{2r+1}(X_r(\mathbb{C}), \mathbb{Q}/\mathbb{Z}), \end{array} \tag{2.80}$$

where $\sigma : \bar{H} \hookrightarrow \mathbb{C}$ denotes the fixed embedding.

Lemma 2.5. *For all $r \geq 0$, there exists a non-negative integer M_r that annihilates the group*

$$H^{2r+1}_{\text{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1))^{G_{F_n}}$$

for any square-free positive integer n coprime to N, where $F_n = K_{\mathfrak{N}} \cdot H_n$.

Proof. We refer to Section 1.3 for the various notations and tools from class field theory used in this proof. Let us fix two distinct rational primes q_1 and q_2 which are inert in K and satisfy $(2N, q_1q_2) = 1$ with the property that there exist two primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in H which lie above q_1 and q_2 respectively such that X_r has good reduction at $\mathfrak{q}_1$ and $\mathfrak{q}_2$. See [12, Appendix]. Let s_1 and s_2 denote the residual degrees of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in $K_{\mathfrak{N}}/H$ respectively. By Corollary 1.2, the residual degrees of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in F_n/H are again equal to s_1 and s_2 respectively. In particular, these residual degrees are independent of n. Let H_∞ denote the compositum of all ring class fields of K of square-free conductor coprime to N and define $F_\infty = K_{\mathfrak{N}} \cdot H_\infty$. It follows from the above that the residual degrees of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in F_∞/H are equal to s_1 and s_2, respectively. We fix $\mathfrak{q}_1^\infty$ and $\mathfrak{q}_2^\infty$ two primes of F_∞ above $\mathfrak{q}_1$ and $\mathfrak{q}_2$ respectively, and let D_1 and D_2 denote the decomposition groups in G_{F_∞} of a prime above $\mathfrak{q}_1^\infty$ and $\mathfrak{q}_2^\infty$, respectively.

Let ℓ be a rational prime and pick $i \in \{1, 2\}$ such that $\ell \neq q_i$. Because of the assumption of good reduction, the inertia group $I_i \subset D_i$ acts trivially on $H^{2r+1}_{\text{et}}(\bar{X}_r, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))$ and we have, by [117, VI Corollary 4.2],

$$H^{2r+1}_{\text{et}}(\bar{X}_r, \mu_{\ell^\nu}^{\otimes(r+1)})^{D_i} \simeq H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mu_{\ell^\nu}^{\otimes(r+1)})^{G_{\mathbb{F}_{q_i^{s_i}}}} \tag{2.81}$$

for all ν. Taking direct limits, we obtain an isomorphism

$$H^{2r+1}_{\text{et}}(\bar{X}_r, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))^{D_i} \simeq H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))^{G_{\mathbb{F}_{q_i^{s_i}}}}. \tag{2.82}$$

From the long exact sequence in ℓ-adic cohomology associated to the short exact sequence

$$0 \longrightarrow \mathbb{Z}_\ell(r+1) \longrightarrow \mathbb{Q}_\ell(r+1) \longrightarrow \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1) \longrightarrow 0 \tag{2.83}$$

we obtain a short exact sequence

$$\begin{aligned} 0 \longrightarrow \frac{H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Q}_\ell(r+1))}{\operatorname{Im}(H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Z}_\ell(r+1)))} &\longrightarrow H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1)) \\ &\longrightarrow H^{2r+2}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Z}_\ell(r+1))_{\text{tors}} \longrightarrow 0. \end{aligned} \tag{2.84}$$

Consequently, the order of $H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))^{G_{\mathbb{F}_{q_i^{s_i}}}}$ is bounded by the product of

$$|H^{2r+2}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Z}_\ell(r+1))_{\text{tors}}| \qquad \text{and} \qquad \left| \left(\frac{H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Q}_\ell(r+1))}{\operatorname{Im}(H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Z}_\ell(r+1)))} \right)^{G_{\mathbb{F}_{q_i^{s_i}}}} \right|.$$

We claim that both these quantities are finite, and equal to 1 for all but finitely many ℓ.

On the one hand, we have a sequence of isomorphisms

$$\begin{aligned} H^{2r+2}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}}, \mathbb{Z}_\ell(r+1)) &\simeq H^{2r+2}_{\text{et}}(X_{r,\bar{H}_{\mathfrak{q}_i}}, \mathbb{Z}_\ell(r+1)) \\ &\simeq H^{2r+2}_{\text{et}}(\bar{X}_r, \mathbb{Z}_\ell(r+1)) \simeq H^{2r+2}(X_r(\mathbb{C}), \mathbb{Z})(r+1) \otimes \mathbb{Z}_\ell \end{aligned}$$

where $H_{\mathfrak{q}_i}$ denotes the completion of H at $\mathfrak{q}_i$. The first isomorphism is obtained from [117, VI Corollary 4.2] by taking inverse limits. For the second one, we fix an embedding $\bar{H} \hookrightarrow \overline{H_{\mathfrak{q}_i}}$, apply [117, VI Corollary 4.3] and take inverse limits. The last one is a consequence of [117, III Theorem 3.12] and taking inverse limits. Since $H^{2r+2}(X_r(\mathbb{C}), \mathbb{Z})$ is finitely generated, its torsion subgroup is finite and thus the torsion subgroup of $H^{2r+2}(X_r(\mathbb{C}), \mathbb{Z})(r+1) \otimes \mathbb{Z}_\ell$ is trivial for all but finitely many ℓ.

On the other hand, we have

$$\left|\left(\frac{H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}},\mathbb{Q}_\ell(r+1))}{\operatorname{Im}(H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}},\mathbb{Z}_\ell(r+1)))}\right)^{G_{\mathbb{F}_{q_i}{}^{s_i}}}\right| \\ = \left|\ker\left(1-\operatorname{Frob}_{\mathfrak{q}_i^\infty} \mid \frac{H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}},\mathbb{Q}_\ell(r+1))}{\operatorname{Im}(H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}},\mathbb{Z}_\ell(r+1)))}\right)\right| \quad (2.85)$$

which is equal to the ℓ-part of

$$|\det(1-\operatorname{Frob}_{\mathfrak{q}_i^\infty} \mid \operatorname{Im}(H^{2r+1}_{\text{et}}(X_{r,\bar{\mathbb{F}}_{q_i}},\mathbb{Z}_\ell(r+1))))|. \quad (2.86)$$

By the Weil conjectures as proved by Deligne [57], the quantity (2.86) does not depend on ℓ. In particular, (2.85) is equal to 1 for all but finitely many ℓ.

We conclude that the order of $H^{2r+1}_{\text{et}}(\bar{X}_r,\mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))^{G_{F_\infty}}$ is finite and equal to 1 for almost all ℓ. Hence $H^{2r+1}_{\text{et}}(\bar{X}_r,\mathbb{Q}/\mathbb{Z}(r+1))^{G_{F_\infty}}$ is finite and we may define

$$M_r := |H^{2r+1}_{\text{et}}(\bar{X}_r,\mathbb{Q}/\mathbb{Z}(r+1))^{G_{F_\infty}}|. \quad (2.87)$$

Then M_r annihilates $H^{2r+1}_{\text{et}}(\bar{X}_r,\mathbb{Q}_\ell/\mathbb{Z}_\ell(r+1))^{G_{F_n}}$ for all square-free n coprime to N. □

We are now in a good position to prove Proposition 2.9. We will do so by proving the contrapositive of the statement.

Proof of Proposition 2.9. Let M_r be the non-negative integer of Lemma 2.5 defined in (2.87). The cycle Δ is defined over the field $F_n = K_{\mathfrak{N}} \cdot H_n$ for some square-free integer n coprime to N by Proposition 2.8. Suppose that Δ is a torsion element of the group $\operatorname{CH}^{r+1}(X_r)_0(\bar{H})$. Using the Galois equivariance of the Bloch map of Proposition 1.14, Lemma 2.5 implies that the order, say m, of $\lambda(\Delta)$ must divide M_r. By compatibility of the Bloch map with the complex Abel–Jacobi map (2.80), we have $\lambda(\Delta) = u \circ \operatorname{AJ}_{\mathbb{C}}(\Delta)$, where u is the map defined in (2.78). Thus $u(m\operatorname{AJ}_{\mathbb{C}}(\Delta)) = 0$ and by injectivity of u, we deduce that $m\operatorname{AJ}_{\mathbb{C}}(\Delta) = 0$.

Hence the order of $\mathrm{AJ}_{\mathbb{C}}(\Delta)$ divides m and in particular divides M_r. □

2.3.4 Infinite rank

In this section we prove the following result, which directly implies the part of Theorem 2.2 concerned with the Chow group of X_r.

Theorem 2.4. *The subgroup of $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ generated by the generalised Heegner cycles $\Delta_{p,q,\beta}$ (for p, q distinct odd primes congruent to 1 modulo N and $\beta \in \mathbb{P}^1(\mathbb{F}_q)$) has infinite rank.*

Let q be a rational odd prime q congruent to 1 modulo N which remains inert in K. There are $q+1$ distinct isogenies $\varphi_{q,\beta} : A \longrightarrow A_{q,\beta}$ of degree q with $\beta \in \mathbb{P}^1(\mathbb{F}_q)$ attached to the following lattices $\Lambda_{q,\beta}$ containing $\mathcal{O}_K$ with index q:

$$\Lambda_{q,\infty} := \mathbb{Z}\frac{1}{q} \oplus \mathbb{Z}\tau, \qquad \Lambda_{q,\beta} := \mathbb{Z} \oplus \mathbb{Z}\frac{\tau+\beta}{q}, \quad \text{for } 0 \leq \beta \leq q-1.$$

The theory of complex multiplication, see Theorem 1.2, implies that the elliptic curves $A_{q,\beta}$, as well as the isogenies $\varphi_{q,\beta}$, can be taken to be rational over H_q, the ring class field of K of conductor q. As q is assumed to be inert in K, the extension H_q/H is cyclic of degree $q+1$, as remarked in (1.37). We let σ_q denote a fixed generator of its Galois group $G_q = \mathrm{Gal}(H_q/H)$.

As we will see, the proof of Theorem 2.4 exploits the action of the Galois group G_H on generalised Heegner cycles. The understanding of this Galois action rests on the following intermediate result.

Lemma 2.6. *The Galois group $G_q = \mathrm{Gal}(H_q/H)$ acts simply transitively on the set of isogenies $\{\varphi_{q,\beta}\}_{\beta\in\mathbb{P}^1(\mathbb{F}_q)}$.*

Proof. Recall the analytic isomorphism $\xi : \mathbb{C}/\mathcal{O}_K \simeq A(\mathbb{C})$ fixed in Notation 2.1. Define, for all $\beta \in \mathbb{P}^1(\mathbb{F}_q)$, the point

$$t_{q,\beta} := \begin{cases} \xi((\tau+\beta)/q), & \text{if } \beta \neq \infty \\ \xi(1/q), & \text{if } \beta = \infty \end{cases}$$

of $A(\mathbb{C})$ and note that $\ker(\varphi_{q,\beta}) = \langle t_{q,\beta} \rangle$.

For any $\sigma \in \mathrm{Aut}(\mathbb{C}/H)$, observe that $A^\sigma = A$ and $\sigma|_{K^{\mathrm{ab}}} = (s|K)$ is the Artin symbol for an idele s of K, which is a unit at all finite places by the idelic description of the ideal class group and the idelic formulation of class field theory. In particular, for any $\sigma \in G_q$ and any idele s of K with $\sigma = (s|K)|_{H_q}$ and $s_v \in \mathcal{O}_{K,v}^\times$ for all $v \nmid \infty$, there is a unique analytic isomorphism $\xi_\sigma : \mathbb{C}/\mathcal{O}_K \simeq A(\mathbb{C})$ such that the diagram

$$\begin{array}{ccc} K/\mathcal{O}_K & \xrightarrow{\ \xi\ } & A \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/\mathcal{O}_K & \xrightarrow[\ \xi_\sigma\ ]{} & A \end{array} \tag{2.88}$$

commutes, according to Shimura's formulation of the main theorem of complex multiplication [136, Theorem 5.4]. Observe that $\xi_\sigma = \xi \circ \alpha_\sigma$ for some $\alpha_\sigma \in \mathcal{O}_K^\times = \{\pm 1\}$ (recall the assumption $d_K \neq 3, 4$), as $\sigma \in \mathrm{Aut}_H(A) = \mathcal{O}_K^\times$. Note that $\ker(\varphi_{q,\beta})$ is a subgroup of the q-torsion group of A, and we may thus restrict the focus to the q-torsion subgroup of $K/\mathcal{O}_K$, namely $q^{-1}\mathcal{O}_{K,q}/\mathcal{O}_{K,q}$.

Since $(s|K)|_{H_q}$ is an element of G_q, the fractional ideal (s^{-1}) associated to s^{-1} belongs to the group $(I_K(q) \cap P_K)/P_{K,\mathbb{Z}}(q)$ described in Section 1.3.1. This group is isomorphic to the quotient $(\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times$ and acts on $\mathbb{F}_q$-lines in $q^{-1}\mathcal{O}_{K,q}/\mathcal{O}_{K,q} \simeq \mathcal{O}_{K,q}/q\mathcal{O}_{K,q}$ by multiplication. In particular, we see that s^{-1} permutes the $\mathbb{F}_q$-lines in $q^{-1}\mathcal{O}_{K,q}/\mathcal{O}_{K,q}$ without preserving any of them. We conclude from (2.88) that σ permutes the kernels $\langle t_{q,\beta} \rangle$ without preserving any of them. In other words, the action of G_q on the set of $q+1$ isogenies $\varphi_{q,\beta}$ is simply transitive. □

Proof of Theorem 2.4. Let ℓ be an arbitrary odd rational prime which does not divide $d_K N$. Fix a rational odd prime q congruent to 1 modulo N, which remains inert in K and such that ℓ divides the degree of H_q/H, i.e., $q+1 \equiv 0 \mod \ell$.

Let p be a rational prime congruent to 1 modulo N and distinct from q. The isogeny $\varphi_{p,q,\beta}$ of (2.64) corresponds to the subgroup $\langle \xi(1/p), t_{q,\beta} \rangle$ of $A(\bar{H})$, which is defined over H_{pq}. Because p and q are distinct, we have $H_{pq} = H_p \cdot H_q$ and $H_p \cap H_q = H$ by Proposition 1.7, and the natural restriction map induces an isomorphism

$$\mathrm{Gal}(H_{pq}/H_p) \simeq \mathrm{Gal}(H_q/H). \tag{2.89}$$

Recall from Proposition 2.8 that $\Delta_{p,q,\beta}$ is defined over $F_{pq} = K_{\mathfrak{N}} \cdot H_{pq}$ and since the intersection $K_{\mathfrak{N}} \cap H_{pq}$ is H, as explained in the proof of Corollary 1.2, we have an isomorphism induced by restriction

$$\mathrm{Gal}(F_{pq}/K_{\mathfrak{N}}) \simeq \mathrm{Gal}(H_{pq}/H). \tag{2.90}$$

Consider the cyclic subgroup of $\mathrm{Gal}(H_q/H)$ of order ℓ which exists because of the assumption $q+1 \equiv 0 \mod \ell$. Let G_ℓ denote the image of this group in $\mathrm{Gal}(F_{pq}/K_{\mathfrak{N}})$ under the above isomorphisms (2.89) and (2.90), and let σ_ℓ be a generator of G_ℓ. Consider the homomorphism of $\mathbb{Q}$-vector spaces

$$\psi : \mathbb{Q}[G_\ell] \longrightarrow \mathrm{CH}^{r+1}(X_r)_0(\bar{H}) \otimes \mathbb{Q}, \tag{2.91}$$

which to $\sigma \in G_\ell$ associates $\sigma(\Delta_{p,q,\beta})$. Note that the kernel of ψ is stable under multiplication by $\mathbb{Q}[G_\ell]$, hence $\ker(\psi)$ is an ideal of $\mathbb{Q}[G_\ell]$. But $\mathbb{Q}[G_\ell]$ has a very simple structure; it is isomorphic to the product of two fields, namely $\mathbb{Q}$ and $\mathbb{Q}(\zeta_\ell)$, where ζ_ℓ is a primitive ℓ-th root of unity. Indeed, the map

$$\mathbb{Q}[G_\ell] \longrightarrow \mathbb{Q} \times \mathbb{Q}(\zeta_\ell), \qquad \sum_{i=0}^{\ell-1} \lambda_i \sigma_\ell^i \mapsto \left(\sum_{i=0}^{\ell-1} \lambda_i, \sum_{i=0}^{\ell-1} \lambda_i \zeta_\ell^i \right)$$

is an isomorphism of rings. There are exactly two proper ideals of $\mathbb{Q} \times \mathbb{Q}(\zeta_\ell)$, namely $\{0\} \times \mathbb{Q}(\zeta_\ell)$ and $\mathbb{Q} \times \{0\}$, which correspond respectively to the augmentation ideal and the ideal $\mathbb{Q} \cdot N$ of $\mathbb{Q}[G_\ell]$, where $N = \sum_{i=0}^{\ell-1} \sigma_\ell^i$.

By Corollary 2.1, we may assume, by taking p large enough, that $\Delta_{p,q,\beta}$ is non-torsion in the Chow group. In other words $\psi(1) \neq 0$ and therefore $\ker(\psi)$ is not equal to all of $\mathbb{Q}[G_\ell]$.

Because the action of $\mathrm{Gal}(H_q/H)$ on the set of q-isogenies of A is simply transitive by Lemma 2.6, we see that $(\varphi_{q,\beta}, A_{q,\beta})^{\sigma_\ell} = (\varphi_{q,\gamma}, A_{q,\gamma})$ in $\mathrm{Isog}(A)$ for some $\gamma \neq \beta$ in $\mathbb{P}^1(\mathbb{F}_q)$. Since σ_ℓ fixes H_p it must fix the subgroup $\langle \xi(1/p) \rangle$ of $A(\bar{H})$, and consequently

$$(\varphi_{p,q,\beta}, A_{p,q,\beta})^{\sigma_\ell} = (\varphi_{p,q,\gamma}, A_{p,q,\gamma}) \tag{2.92}$$

in $\mathrm{Isog}(A)$. It follows that $\sigma_\ell(\Delta_{p,q,\beta}) = \Delta_{p,q,\gamma}$ in $\mathrm{CH}^{r+1}(X_r)_0(\bar{H})$, i.e., $\psi(\sigma_\ell) = \Delta_{p,q,\gamma}$.

By Corollary 2.2, we may choose p such that $\Delta_{p,q,\beta} - \Delta_{p,q,\gamma}$ is non-torsion in the Chow group. In other words, $\psi(\sigma_\ell - 1) \neq 0$ and thus $\ker(\psi)$ is not equal to the augmentation ideal.

We conclude that the kernel of ψ is either trivial or equal to $\mathbb{Q} \cdot N$. In any case, we have

$$\dim_{\mathbb{Q}} \mathbb{Q}[G_\ell]/\ker(\psi) \geq \ell - 1 \tag{2.93}$$

and we have thus constructed a subgroup of the Chow group of rank greater or equal to $\ell - 1$. Since ℓ was chosen arbitrarily, this proves the theorem. □

2.3.5 The Griffiths group of X_r

By Theorem 2.3, we know that many of the generalised Heegner cycles have large (possibly infinite) order in the Griffiths group, at least when $r \geq 1$. In the proof of this theorem, we were able to extract information concerning the Griffiths group by studying the transcendental Abel–Jacobi map (2.73), a modified version of the complex Abel–Jacobi map which enjoys the property that it factors through $\mathrm{Gr}^{r+1}(X_r)(\mathbb{C})$. If we wish to apply the algebraic arguments of Section 2.3.3 in order to show that many of the cycles have infinite order in the

Griffiths group, we need a modified version of Bloch's map λ of Galois modules (2.79) which factors through $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$. To this end, we introduce an algebraic projector which we compose with λ.

We use the same conventions and notations for motives as in [58, §0], see also Section 1.4.2. Given two nonsingular varieties X and Y, we define the rings of correspondences

$$\mathrm{Corr}^0(X,Y) := \mathrm{CH}^{\dim(X)}(X \times Y) \quad \text{and} \quad \mathrm{Corr}^0(X,Y)_E := \mathrm{Corr}^0(X,Y) \otimes E,$$

if E is a number field, as in Section 1.4.2.

Proposition 2.10. *For all $r \geq 2$, there exists an idempotent element P_{X_r} in $\mathrm{Corr}^0(X_r, X_r)_{\mathbb{Q}}$ with the following properties:*

1. *The map*
$$\mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \xrightarrow{\mathrm{AJ}_{\mathbb{C}}} J^{r+1}(X_r/\mathbb{C}) \xrightarrow{(P_{X_r})_*} J(N)$$
factors through $\mathrm{Gr}^{r+1}(X_r)(\mathbb{C})$, where $J(N)$ denotes the intermediate Jacobian associated to the Betti realisation of the Chow motive $N := (X_r, P_{X_r}, r+1)$ over H with coefficients in $\mathbb{Q}$.

2. *The map of Galois modules*
$$\mathrm{CH}^{r+1}(X_r)_0(\bar{H})_{\mathrm{tors}} \xrightarrow{\lambda} H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1)) \xrightarrow{(P_{X_r})_*} H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1))$$
factors through $\mathrm{Gr}^{r+1}(X_r)(\bar{H})_{\mathrm{tors}}$, and thus induces a map of Galois modules
$$(P_{X_r})_* \circ \lambda : \mathrm{Gr}^{r+1}(X_r)(\bar{H})_{\mathrm{tors}} \longrightarrow H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1)).$$

We begin with the construction of the projector P_{X_r} and assume from now on that $r \geq 2$. Write $[x]$ for $x \in K$ viewed as an element of $\mathrm{End}_H(A) \otimes \mathbb{Q}$. The identification of K with $\mathrm{End}_H(A) \otimes \mathbb{Q}$ is normalised such that $[x]^*\omega_A = x\omega_A$ for all $x \in K$. We shall consider the following idempotents of $\mathrm{End}_H(A) \otimes K$:

$$e = \frac{\sqrt{-d_K} + [\sqrt{-d_K}]}{2\sqrt{-d_K}} \qquad \text{and} \qquad \bar{e} = \frac{\sqrt{-d_K} - [\sqrt{-d_K}]}{2\sqrt{-d_K}}$$

and view them as elements of $\mathrm{Corr}^0(A, A)_K$ by taking their graphs. For all $0 \leq j \leq r$, we define the idempotent

$$e^{(j)} := \sum_{\substack{I \subset \{1,\ldots,r\} \\ |I|=j}} e_{1,I} \otimes \ldots \otimes e_{r,I} \in \mathrm{Corr}^0(A^r, A^r)_K,$$

where $e_{i,I} := e$ or $\bar{e}$ depending on whether $i \in I$ or $i \notin I$.

Consider the Chow motive $M := (A^r, e_r, 0)$ over H with coefficients in $\mathbb{Q}$ where

$$e_r := \left(\sum_{0<j<r} e^{(j)} \right) \circ \left(\frac{1 - [-1]}{2} \right)^{\otimes r} \in \mathrm{Corr}^0(A^r, A^r)_{\mathbb{Q}}.$$

The Betti realisation M_B of this motive is a Hodge structure of weight r. We have $M_B(\mathbb{C}) = e_r H^r_{\mathrm{dR}}(A^r)$ and its Hodge decomposition is given by

$$H^{j,r-j}(M_B(\mathbb{C})) = \begin{cases} H^{j,r-j}(A^r) & \text{for } 0 < j < r \\ 0 & \text{for } j = 0 \text{ or } j = r. \end{cases} \tag{2.94}$$

We will use the same notation for e_r and its pull-back to $\mathrm{Corr}^0(X_r, X_r)_{\mathbb{Q}}$ and define

$$P_{X_r} := e_r \circ \epsilon_{X_r} \in \mathrm{Corr}^0(X_r, X_r)_{\mathbb{Q}}, \tag{2.95}$$

which is an idempotent in the ring of correspondences of X_r with coefficients in $\mathbb{Q}$ since e_r and ϵ_{X_r} commute.

Remark 2.11. As in Remark 2.2, we will assume throughout that the projector P_{X_r} has been multiplied by a suitable integer so that it lies in $\mathrm{Corr}^0(X_r, X_r)$.

The correspondence P_{X_r} induces morphisms $(P_{X_r})_* = (\mathrm{pr}_2)_* \circ (\cdot P_{X_r}) \circ (\mathrm{pr}_1)^*$ between Chow groups, cohomology groups and intermediate Jacobians and acts as a projector on these various objects.

The map of intermediate Jacobians

$$(P_{X_r})_* : J^{r+1}(X_r/\mathbb{C}) \longrightarrow J^{r+1}(X_r/\mathbb{C}) \tag{2.96}$$

is induced from the map on singular cohomology

$$(P_{X_r})_* : H^{2r+1}(X_r(\mathbb{C}), \mathbb{Z}) \longrightarrow H^{2r+1}(X_r(\mathbb{C}), \mathbb{Z}) \tag{2.97}$$

which makes sense since the latter is a morphism of Hodge structures of bidegree $(0, 0)$ by [147, Lemma 11.41], and thus maps $\mathrm{Fil}^{r+1} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C})$ into itself.

We will henceforth work with the Chow motive $N := (X_r, P_{X_r}, r+1)$ over H with coefficients in $\mathbb{Q}$. Its Betti realisation $N_B = (P_{X_r})_*(H^{2r+1}(X_r(\mathbb{C}), \mathbb{Z}))(r+1)$ is a Hodge structure of weight -1 and the 0-th step of its Hodge filtration is given by

$$\begin{aligned} \mathrm{Fil}^0 N_B(\mathbb{C}) &= (P_{X_r})_* \mathrm{Fil}^{r+1} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C}) \\ &= S_{r+2}(\Gamma_1(N)) \otimes \left(\bigoplus_{j=1}^{r-1} \mathbb{C}\omega_A^j \eta_A^{r-j} \right) \subset \bigoplus_{j=1}^{r-1} H^{r+1+j, r-j}(X_r). \end{aligned} \tag{2.98}$$

We note that $H^{0,-1}(N_B(\mathbb{C})) = H^{r,-(r+1)}(N_B(\mathbb{C})) = 0$ and in particular we have the crucial property

$$(P_{X_r})_*(H^{r+1,r}(X_r) \oplus H^{r,r+1}(X_r)) = 0. \tag{2.99}$$

Associated to the Hodge structure N_B is a complex torus

$$J(N) := N_B(\mathbb{C}) / (\mathrm{Fil}^0(N_B(\mathbb{C})) \oplus N_B)$$

which is the image of the projection (2.96). By (2.98) and Poincaré duality, we have an isomorphism of complex tori

$$J(N) \simeq \frac{\left(S_{r+2}(\Gamma_1(N)) \otimes \left(\bigoplus_{j=1}^{r-1} \mathbb{C}\omega_A^j \eta_A^{r-j}\right)\right)^\vee}{\Pi'_{r,r}}, \tag{2.100}$$

where the lattice $\Pi'_{r,r}$ is defined by

$$\Pi'_{r,r} := (P_{X_r})_*(\mathrm{Im}\, H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})). \tag{2.101}$$

Proof of Proposition 2.10. Recall from (2.72) that $J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}} = J^{r+1}(V)$ where V is the largest sub-Hodge structure of $H^{r+1,r}(X_r) \oplus H^{r,r+1}(X_r)$ and the image of $\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\mathbb{C})$ under $\mathrm{AJ}_{\mathbb{C}}$ is a complex subtorus of $J^{r+1}(X_r/\mathbb{C})$ which is contained in $J^{r+1}(X_r/\mathbb{C})_{\mathrm{alg}}$. The morphism of tori $(P_{X_r})_* : J^{r+1}(X_r/\mathbb{C}) \longrightarrow J(N)$ is induced from the morphism of Hodge structures (2.97). The latter restricts to a morphism of Hodge structures $(P_{X_r})_* : V_{\mathbb{Z}} \longrightarrow N_B$ which is the zero map when tensored up to $\mathbb{C}$ by (2.99) since $V_{\mathbb{C}} \subset H^{r+1,r}(X_r) \oplus H^{r,r+1}(X_r)$. Hence the induced map $(P_{X_r})_* : J^{r+1}(V) \longrightarrow J(N)$ is the zero map and the first statement of the proposition follows.

The group $\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\bar{H})$ is divisible since it is generated by images under correspondences of $\bar{H}$-valued points on Jacobians of curves, by Definition 1.18 of algebraic equivalence. Therefore we have an exact sequence

$$0 \longrightarrow \mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\bar{H})_{\mathrm{tors}} \longrightarrow \mathrm{CH}^{r+1}(X_r)_0(\bar{H})_{\mathrm{tors}} \longrightarrow \mathrm{Gr}^{r+1}(X_r)(\bar{H})_{\mathrm{tors}} \longrightarrow 0 \tag{2.102}$$

and in order to prove the second statement of the proposition it suffices to show that the subgroup $\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\bar{H})_{\mathrm{tors}}$ lies in the kernel of $(P_{X_r})_* \circ \lambda$. Observe from (2.80) that

$$(P_{X_r})_* \circ \lambda = (P_{X_r})_* \circ u \circ \mathrm{AJ}_{\mathbb{C}} \tag{2.103}$$

where we use the compatibility of the comparison isomorphism (1.73) with correspondences, which follows from the compatibility of the cycle class maps with respect to the comparison isomorphism. See [94, §5.3]. Note that the maps (2.97) and (2.96) commute with u since the latter is induced from the former and we therefore have

$$(P_{X_r})_* \circ \lambda = u \circ (P_{X_r})_* \circ \mathrm{AJ}_{\mathbb{C}}\,. \tag{2.104}$$

It follows from statement (1.) that $(P_{X_r})_* \circ \lambda(\mathrm{CH}^{r+1}(X_r)_{\mathrm{alg}}(\bar{H})_{\mathrm{tors}}) = 0$. □

When $r \geq 2$, applying the map $(P_{X_r})_*$ on Chow groups yields the cycles

$$\Xi_{p,q,\beta} := (P_{X_r})_* \Delta_{p,q,\beta}, \tag{2.105}$$

whose classes in the Griffiths group will be denoted $[\Xi_{p,q,\beta}]$. Since the projector P_{X_r} is defined over $\mathbb{Q}$, these cycles and their classes are defined over F_{pq} by Proposition 2.8.

Proposition 2.11. *For all $r \geq 2$, the order of $[\Xi_{p,q,\beta}]$ in $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$ tends to ∞ as p/q tends to infinity.*

Proof. By functoriality of the complex Abel–Jacobi map [65], we may view $\mathrm{AJ}_{\mathbb{C}}(\Xi_{p,q,\beta})$ as an element of $J(N)$. If $f \in S_{r+2}(\Gamma_1(N))$ is non-zero and $0 < j < r$, then

$$\mathrm{AJ}_{\mathbb{C}}(\Xi_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) = \mathrm{AJ}_{\mathbb{C}}(\Delta_{p,q,\beta})(\omega_f \wedge \omega_A^j \eta_A^{r-j}). \tag{2.106}$$

As p/q tends to ∞, by Lemma 2.4, $\mathrm{AJ}_{\mathbb{C}}(\Xi_{p,q,\beta})$ becomes arbitrarily close but not equal to the origin in $J(N)$. It follows, by Proposition 2.10 (1.), that the order of $[\Xi_{p,q,\beta}]$ tends to ∞ with p/q. □

Proposition 2.12. *For all $r \geq 2$, if $\Xi \in \langle\{\Xi_{p,q,\beta}\}\rangle \subset \mathrm{CH}^{r+1}(X_r)_0(\bar{H})$ is such that the order of $\mathrm{AJ}_{\mathbb{C}}(\Xi)$ in $J^{r+1}(X_r/\mathbb{C})$ does not divide M_r, then Ξ has infinite order in $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$.*

Proof. Suppose that $[\Xi]$ is a torsion element. The cycle Ξ and its class in the Griffiths group are both defined over the field $F_n = K_{\mathfrak{N}} \cdot H_n$ for some square-free integer n coprime to N by

Proposition 2.8 and we have the identity $(P_{X_r})_*\Xi = \Xi$. By Proposition 2.10 (2.),

$$(P_{X_r})_* \circ \lambda([\Xi]) \in H^{2r+1}_{\mathrm{et}}(\bar{X}_r, \mathbb{Q}/\mathbb{Z}(r+1))^{G_{F_n}}$$

and thus by Lemma 2.5, the order, say m, of $(P_{X_r})_* \circ \lambda([\Xi])$ must divide M_r. By (2.104), we have

$$(P_{X_r})_* \circ \lambda([\Xi]) = u \circ (P_{X_r})_* \circ \mathrm{AJ}_{\mathbb{C}}([\Xi]) = u \circ (P_{X_r})_* \circ \mathrm{AJ}_{\mathbb{C}}(\Xi).$$

By functoriality of the complex Abel–Jacobi map with respect to correspondences, see [65], we obtain

$$(P_{X_r})_* \circ \lambda([\Xi]) = u(\mathrm{AJ}_{\mathbb{C}}((P_{X_r})_*\Xi)) = u(\mathrm{AJ}_{\mathbb{C}}(\Xi)).$$

By injectivity of u, the order of $\mathrm{AJ}_{\mathbb{C}}(\Xi)$ must divide m and thus divides M_r. □

Proof of Theorem 2.2. Proceeding as in Section 2.3.3, one uses Propositions 2.11 and 2.12 to deduce the analogue statements of Corollaries 2.1 and 2.2 for the Griffiths group and the classes $[\Xi_{p,q,\beta}]$. Using these two statements, the same arguments as in Section 2.3.4 apply, proving that $\mathrm{Gr}^{r+1}(X_r)(\bar{H})$ has infinite rank. □

Remark 2.12. Applying the construction of the projector P_{X_r} in the case $r = 1$ yields nothing interesting. In fact, there is no algebraic splitting of the motive X_1 into its algebraic and transcendental components and for this reason we cannot apply the arguments to show that the Griffiths group is infinitely generated in this case. More precisely, we cannot obtain Proposition 2.10 (2.) and therefore we fail to obtain Proposition 2.12. As a consequence, even though we can show that many of the cycles have large order in the Griffiths group, we are unable to prove that they generate a group of infinite rank.

Remark 2.13. Section 2.4 in [12] exhibits a correspondence from X_{2r} to W_{2r} under which generalised Heegner cycles are mapped to (rational multiples of) “traditional” Heegner cycles on Kuga–Sato varieties. While this does not imply directly the analogue of Theorem 2.2 in the setting of Kuga–Sato varieties, the methods of this paper can be expected to carry over to proving the analogues of Theorem 2.1 and Theorem 2.2 in this setting.

Remark 2.14. In [90], Bo-Hae Im exploits Heegner points in an ingenious way to prove that Mordell–Weil groups over large fields are of infinite rank, where a field is said to be large if it is of the form $\bar{\mathbb{Q}}^\sigma$, with σ an element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We believe that the techniques used in the proof [90, Prop. 2.9] can be combined with Theorem 2.2 to show that

$$\dim \mathrm{CH}^{r+1}(X_r)_0(\bar{\mathbb{Q}}^\sigma) \otimes \mathbb{Q} = \infty,$$

as well as similar statements for the Griffiths group when $r \geq 2$.

Chapter 3

Geometric quadratic Chabauty over number fields

This chapter is a reformatted version of the preprint article [41] and all results presented herein are joint with Pavel Čoupek, Luciena Xiao Xiao and Zijian Yao.

It is known by Faltings' famous proof of Mordell's conjecture that any smooth, projective, geometrically irreducible curve of genus greater than one over a number field has only finitely many rational points. However, this does not allow for the explicit determination of this finite set, given that Faltings' proof is not effective. In this chapter we generalise the geometric quadratic Chabauty method, initiated over $\mathbb{Q}$ by Edixhoven and Lido, to higher genus curves defined over arbitrary number fields. This results in a conditional bound on the number of rational points on curves that satisfy an additional Chabauty type condition on the rank of the Jacobian of the curve. The method gives a more direct approach to the generalisation by Dogra of the quadratic Chabauty method to arbitrary number fields using restriction of scalars. As such, this work can naturally be viewed as part of the non-abelian Chabauty program initiated by Kim.

Introduction

It has been known since Faltings' proof [68] in 1983 of Mordell's conjecture [118] that there are only finitely many rational points on (smooth, proper, geometrically connected) curves C_K of genus $g \geq 2$ defined over a number field K. However, Faltings' proof cannot be made effective, hence the problem of explicitly determining this set remains open.

The first partial result towards Mordell's conjecture came in the form of the pioneering work of Chabauty [35] in 1941. He proved finiteness of the set of rational points under an additional constraint, known as the Chabauty condition – namely, the rank r of the Mordell–Weil group of the Jacobian J_K of C_K is less than g. Let us, for the purpose of exposition, restrict ourselves to the case $K = \mathbb{Q}$. Upon choosing a prime p of good reduction, Chabauty considered the following commutative diagram

$$\begin{array}{ccccc} C_{\mathbb{Q}}(\mathbb{Q}) & \longrightarrow & & \longrightarrow & C_{\mathbb{Q}}(\mathbb{Q}_p) \\ \downarrow & & & & \downarrow \\ J_{\mathbb{Q}}(\mathbb{Q}) & \longrightarrow & Z & \longrightarrow & J_{\mathbb{Q}}(\mathbb{Q}_p) \end{array} \tag{3.1}$$

where the vertical maps are Abel–Jacobi embeddings based at a fixed point $b \in C_{\mathbb{Q}}(\mathbb{Q})$, and $Z := \overline{J_{\mathbb{Q}}(\mathbb{Q})} \subset J_{\mathbb{Q}}(\mathbb{Q}_p)$ is the closure of the Mordell–Weil group in the p-adic Lie group $J_{\mathbb{Q}}(\mathbb{Q}_p)$. Chabauty proved that $\dim Z \leq r$ and thus, under the Chabauty condition $r < g$, the dimensions suggest that the intersection $C_{\mathbb{Q}}(\mathbb{Q}_p) \cap Z$ should be at most 0-dimensional, thus should be finite. Chabauty proved finiteness of this intersection, and hence also of its subset $C_{\mathbb{Q}}(\mathbb{Q})$. In 1985, Coleman [36] succeeded in making Chabauty's method effective, resulting in explicit upper bounds on the number of rational points on curves satisfying the Chabauty condition. This led to the explicit determination of the set of rational points on many examples of such curves. The so-called Chabauty–Coleman method is described in more detail in Sections 0.3.1 and 0.4.2.

In the mid 2000's, Kim [101, 102] initiated a fascinating program, known as the non-abelian Chabauty program (or Chabauty–Kim method), which aims to relax the restrictive

Chabauty condition $r < g$. The first non-abelian instance of the program is called the quadratic Chabauty method. It has recently been made effective over $\mathbb{Q}$ by Balakrishnan, Dogra, Müller, Tuitman and Vonk [8], and spectacularly applied to determine the rational points of the "cursed" curve $X_s(13)$. More details about these developments can be found in Section 0.3.2.

Recently, Edixhoven and Lido [62] have found a different approach to quadratic Chabauty over $\mathbb{Q}$. Their method is expected to work under the condition $r < g + \rho - 1$, known as the quadratic Chabauty condition, where ρ is the rank of the Néron–Severi group of $J_{\mathbb{Q}}$. It lies close in spirit to the original method of Chabauty and presents the advantage that it avoids the (complicated) language of non-abelian p-adic Hodge theory used by Kim. An overview of their method is described in Section 0.3.3.

A natural question is the generalisation of these methods to arbitrary number fields. In order to apply the ideas of Chabauty–Coleman, Siksek [138] considered the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}}(J_K)$ and studied Coleman integration in this context; this gives rise to the Restriction of Scalars (RoS) Chabauty method. The work of Balakrishnan, Besser, Bianchi and Müller [4] builds on this idea and studies rational points on hyperelliptic or bielliptic curves satisfying a more relaxed Chabauty condition compared to [138], see Section 3.3.3; this is the RoS quadratic Chabauty method. The work of Dogra [60] combines restriction of scalars with the ideas of Kim, leading to an RoS generalisation of the Chabauty–Kim program. For a more detailed account of these methods, we refer to Section 0.4.2.

In this chapter, we generalise the Edixhoven–Lido method, also known as the geometric quadratic Chabauty method, to general number fields. The main theorem is, in rough form, the following.

Theorem 3.1. *Let K be a number field of degree d. Let C_K be a smooth, proper, geometrically connected curve of genus $g \geq 2$ defined over K with Mordell–Weil rank $r = \operatorname{rank}_{\mathbb{Z}} J(K)$ satisfying the condition*

$$r + \delta(\rho - 1) \leq (g + \rho - 2)d, \tag{3.2}$$

where $\delta := \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K^\times$ *and* $\rho = \operatorname{rank}_{\mathbb{Z}} \operatorname{NS}(J_K)$*. Let* $R := \mathbb{Z}_p\langle z_1, ..., z_{r+\delta(\rho-1)}\rangle$ *be the p-adically completed polynomial algebra over* $\mathbb{Z}_p$*. There exists an ideal* I *of* R*, which is explicitly computable modulo* p*, such that if* $\overline{A} := (R/I) \otimes \mathbb{F}_p$ *is a finite dimensional* $\mathbb{F}_p$*-vector space, then the set of rational points* $C_K(K)$ *is finite and*

$$|C_K(K)| \leq \dim_{\mathbb{F}_p} \overline{A}.$$

Remark 3.1. The precise form of this theorem is slightly more involved than what is stated above. We need to work integrally with a regular proper model $\mathbf{C}$ of C over $\mathcal{O}_K$, and in order for the method to work, we need to cover the smooth locus $\mathbf{C}^{\text{sm}}$ by certain open subschemes $\mathbf{U}_i$ and work with one $\mathbf{U}_i$ at a time. Moreover, we work separately on each residue disk at p of $\mathbf{U}_i$ and produce a bound on the size of $\mathbf{U}_i(\mathcal{O}_K)_u$ by constructing an ideal $I_{i,u} \subset R$ for each i and each $u \in \mathbf{U}_i(\mathcal{O}_K \otimes \mathbb{F}_p)$. The bound on the size of $C(K)$ is then obtained by summing the bounds for each i and u. This is made precise in Corollary 3.2.

Remark 3.2. The condition (3.2), which we refer to as the geometric quadratic Chabauty condition in Definition 3.8, is the "best bound" for explicit quadratic Chabauty methods over number fields in the literature. See for instance Section 0.4.2 or Section 3.3.3 for comparisons with other Chabauty bounds that arise in the aforementioned works [4, 60, 138].

The strategy, following [62], is to replace the Jacobian in Chabauty's original approach (3.1) by something higher dimensional in order to play the Chabauty game. More precisely, we will construct a certain $\mathbb{G}_m^{\rho-1}$-torsor T_K over J_K (where ρ is defined in Theorem 3.1) which will replace J_K. This, however, introduces "too many rational points" as the fibre of T_K over J_K is $\mathbb{G}_m^{\rho-1}$ and $\mathbb{G}_m(K) = K^\times$ is not finitely generated, thus it becomes necessary to consider a regular proper model $\mathbf{C}$ of C_K over the ring of integers $\mathcal{O}_K$ and spread out the geometry. Consequently, we construct a certain $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$, the latter being the Néron model of J_K. The idea is then to carefully lift the Abel–Jacobi map $j_b : \mathbf{C} \to \mathbf{J}$ to the torsor $\mathbf{T}$

$$\begin{array}{ccc} & & \mathbf{T} \\ & \overset{\tilde{j}_b}{\nearrow} & \downarrow \\ \mathbf{C} & \overset{j_b}{\hookrightarrow} & \mathbf{J}. \end{array}$$

(The exposition here is too crude, as this steps requires the introduction of the subschemes $\mathbf{U}_i$ of Remark 3.1). We then let $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and consider the following quadratic Chabauty diagram (compare with (3.1))

$$\begin{array}{ccccc} \mathbf{C}(\mathcal{O}_K) & \longrightarrow & & & \mathbf{C}(\mathcal{O}_{K,p}) \\ \downarrow \tilde{j}_b & & & & \downarrow \tilde{j}_b \\ \mathbf{T}(\mathcal{O}_K) & \longrightarrow & \mathbf{Y} & \longrightarrow & \mathbf{T}(\mathcal{O}_{K,p}). \end{array} \tag{3.3}$$

Here $\mathbf{Y} := \overline{\mathbf{T}(\mathcal{O}_K)}^p$ is the closure of $\mathbf{T}(\mathcal{O}_K)$ in $\mathbf{T}(\mathcal{O}_{K,p})$ for the p-adic topology. The rational points $C_K(K) = \mathbf{C}(\mathcal{O}_K)$ are contained in $\tilde{j}_b(\mathbf{C}(\mathcal{O}_{K,p})) \cap \mathbf{Y}$, which is often finite and computable.

The key of the approach is thus to analyse the p-adic closure $\mathbf{Y}$ of the $\mathcal{O}_K$-points of the torsor $\mathbf{T}$. If $K = \mathbb{Q}$, then this can be done by parametrising the p-adic closure of $\mathbf{J}(\mathbb{Z}) = J(\mathbb{Q})$, as $\mathbb{G}_m(\mathbb{Z}) = \pm 1$. This is a major simplification and essentially why [62] decides to work over $\mathbb{Q}$. In fact, it was suggested to us by the authors of [62] that a restriction of scalars approach might reduce the case of general number fields K back to the case of $\mathbb{Q}$. In this work, however, we decide to take a more direct approach which departs from the RoS arguments of [4, 60, 138]. One of the main observations is that one can in fact fully utilise the $\mathbb{G}_m$-action on the fibres of the torsor $\mathbf{T} \longrightarrow \mathbf{J}$ to parametrise $\mathbf{Y}$, which is sufficient for the purposes of this work. Roughly, we pick a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^r \to \mathbf{T}(\mathcal{O}_K)$ essentially by choosing a basis for the Mordell–Weil group $J(K)$. We then use the $\mathbb{G}_m$-action to propagate these coordinates to get a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^{\delta(\rho-1)+r} \to \mathbf{T}(\mathcal{O}_K)$, where δ is as defined in Theorem 3.1. Finally, interpolating these coordinates p-adically allows us to parametrise $\mathbf{Y}$ via a surjective map

$$\kappa : \mathbb{Z}_p^{\delta(\rho-1)+r} \longrightarrow \mathbf{Y},$$

which turns out to be given by convergent p-adic power series. In fact, the ideal I in Theorem 3.1 is built such that the cardinality of $\operatorname{Spec}(R/I)(\mathbb{Z}_p)$ is the size of $\kappa^{-1}(\mathbf{Y} \cap \tilde{j}_b(\mathbf{C}(\mathcal{O}_{K,p})))$. In particular, in order for the method to be able to explicitly determine the rational points on C_K, we need to choose a prime p such that

$$\begin{cases} \mathbf{Y} \cap \tilde{j}_b(\mathbf{C}(\mathcal{O}_{K,p})) \text{ is finite} \\ \kappa \text{ is ``finite-to-one'' on } \kappa^{-1}(\mathbf{Y} \cap \tilde{j}_b(\mathbf{C}(\mathcal{O}_{K,p}))). \end{cases}$$

This observation prompts the following question:

Question 3.1. *Let p be a prime of good reduction for C_K. What conditions are necessary to guarantee that the intersection $\mathbf{Y} \cap \mathbf{C}(\mathcal{O}_{K,p})$ as in the commutative diagram (3.3) is finite ?*

In Section 3.1 we recall some basic background on the Poincaré torsor, from which we build the torsor T_K over J_K mentioned in the overview above. We then spread out the entire picture from $\operatorname{Spec} K$ to $\operatorname{Spec} \mathcal{O}_K$ to obtain a precise version of diagram (3.3). In Section 3.2 we construct the torsor $\mathbf{T}$. Section 3.3 makes the strategy of geometric quadratic Chabauty precise and the main technical results of this work are stated. We also explain how the geometric quadratic Chabauty condition arises and discuss how it specialises to the condition that appear in the RoS quadratic Chabauty method that is part of Dogra's generalisation of Kim's program. In Section 3.4, which is the technical core of this chapter, we parametrise the p-adic closure $\mathbf{Y}$ of the rational points $\mathbf{T}(\mathcal{O}_K)$ by performing a p-adic interpolation. Finally, we complete the proof of the main theoretical results in Section 3.5 and discuss Question 3.1 raised above.

3.1 Preliminaries

In this section we recall some background on algebraic geometry necessary for the method of geometric quadratic Chabauty. In particular, we review the key geometric object studied in this chapter, namely the Poincaré torsor along with its biextension structure. We also explain how to extend this picture to obtain a biextension over $\operatorname{Spec} \mathcal{O}_K$.

3.1.1 The Poincaré biextension

We recall the definition of the Poincaré bundle and the associated torsor. We then recall that the Poincaré torsor can be endowed with the structure of a $\mathbb{G}_m$-biextension.

The Poincaré bundle

For details about this section, we refer to [63, Chapter VI]. As in the introduction, we let C_K be a smooth proper geometrically connected curve of genus $g \geq 2$ defined over K with $C_K(K) \neq \emptyset$. Let J_K be its Jacobian, i.e., $J_K := \operatorname{Pic}^0_{C_K/K}$ is the connected component of the identity of the Picard scheme $\operatorname{Pic}_{C_K/K}$; this is an abelian variety of dimension g defined over K. We denote its zero section by $0 \in J_K(K)$ or $e : \operatorname{Spec} K \longrightarrow J_K$.

Consider the Picard scheme $\operatorname{Pic}_{J_K/K}$ over K defined as the contravariant functor from K-schemes to the category of abelian groups given by

$$T \mapsto \operatorname{Pic}(J_K \times T)/\operatorname{pr}_T^* \operatorname{Pic}(T), \tag{3.4}$$

where $\operatorname{pr}_T : J_K \times T \longrightarrow T$ is the base-change of the structural morphism $J_K \longrightarrow \operatorname{Spec} K$. The scheme $\operatorname{Pic}_{J_K/K}$ is a group scheme over K with projective connected components. The connected component $\operatorname{Pic}^0_{J_K/K}$ of the identity is reduced, hence an abelian variety. This is the dual abelian variety of J_K, and we shall denote it by $J_K^\vee := \operatorname{Pic}^0_{J_K/K}$. It comes equipped with a canonical principal polarisation $\lambda : J_K \xrightarrow{\sim} J_K^\vee$ by translating the theta divisor.

The functor described by (3.4) is isomorphic to the functor given by

$$T \mapsto \{ \text{ isomorphism classes of rigidified line bundles } (L, \alpha) \text{ on } J_K \times T \},$$

where a rigidification of the line bundle L is an isomorphism $\alpha : \mathcal{O}_T \xrightarrow{\sim} e_T^* L$, where the section $e_T : T \longrightarrow J_K \times T$ is the one induced by e. Since this moduli problem is representable by $\mathrm{Pic}_{J_K/K}$, there is a universal rigidified line bundle (P_K, ν) on $J_K \times \mathrm{Pic}_{J_K/K}$ which satisfies the following universal property: if (L, α) is a rigidified line bundle on $J_K \times T$ along the zero section e, then there is a unique morphism $g : T \longrightarrow \mathrm{Pic}_{J_K/K}$ such that $(L, \alpha) \simeq (\mathrm{id}_{J_K} \times g)^*(P_K, \nu)$.

Definition 3.1. The restriction of the universal line bundle P_K to $J_K \times J_K^\vee$ along with its canonical rigidification ν along e is called the Poincaré bundle of J_K, and is denoted P_K by slight abuse of notation.

The canonical rigidification of the Poincaré bundle yields an isomorphism

$$\nu : \mathcal{O}_{J_K^\vee} \xrightarrow{\sim} P_K|_{\{0\} \times J_K^\vee}.$$

Let $0 \in J_K^\vee(K)$ denote the identity element of the abelian variety $J_K^\vee$. There is a unique rigidification

$$\nu' : \mathcal{O}_{J_K} \xrightarrow{\sim} P_K|_{J_K \times \{0\}},$$

such that ν and ν' agree at the origin $(0, 0) \in (J_K \times J_K^\vee)(K)$. As a consequence, (P_K, ν, ν') is a birigidified line bundle on $J_K \times J_K^\vee$ with respect to the identity elements.

The Poincaré torsor

First we recall that, given a line bundle L on an arbitrary scheme X, its associated $\mathbb{G}_m$-torsor is $L^\times = \mathbf{Isom}_X(\mathcal{O}_X, L)$, which is equipped with a natural free and transitive action of $\mathbb{G}_m$. Note that $L^\times$ is Zariski locally trivial. In particular, it is represented by a scheme over X which we again denote by $L^\times$ by slight abuse of notation. Concretely, $L^\times$ is (locally) obtained by deleting the zero section of L. As $\mathbb{G}_m$-torsors on X are classified by the Čech cohomology group $\check{H}^1(X, \mathbb{G}_m)$, the operation $L \mapsto L^\times$ describes a morphism $\mathrm{Pic}(X) \longrightarrow \check{H}^1(X, \mathbb{G}_m)$, which is an isomorphism inverse to the canonical isomorphism $\check{H}^1(X, \mathbb{G}_m) \longrightarrow H^1(X, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$;

in particular, every $\mathbb{G}_m$-torsor on X arises in the way described above, and $\mathrm{Pic}(X)$ classifies isomorphism classes of $\mathbb{G}_m$-torsors on X.

Definition 3.2. The Poincaré torsor $P_K^\times$ is the $\mathbb{G}_m$-torsor on $J_K \times J_K^\vee$ associated to the Poincaré bundle P_K.

As above, we again denote by $P_K^\times$ the scheme represented by the Poincaré torsor and denote by $j_K : P_K^\times \longrightarrow J_K \times J_K^\vee$ the structural morphism. The torsor $P_K^\times$ inherits the compatible birigidification over $J_K \times \{0\}$ and $\{0\} \times J_K^\vee$ coming from P_K.

The Poincaré biextension

In this subsection we explain the biextension structure of the Poincaré torsor that plays a central role in the rest of this chapter. The assertion is that $P_K^\times$ admits a unique structure of $\mathbb{G}_m$-biextension of the couple $(J_K, J_K^\vee)$, which is compatible with its canonical birigidified $\mathbb{G}_m$-torsor structure inherited from P_K. For the proof of this, we refer to [79, VII.Definition 2.1, Exemple 2.9.5]. Instead of repeating the definition from SGA 7, let us briefly explain what this means.

- **Partial composition $+_1$:** First, we may view $P_K^\times$ as a scheme over $J_K^\vee$ via the structure morphism $\mathrm{pr}_2 \circ j_K$. As such, $P_K^\times$ becomes a commutative $J_K^\vee$-group scheme which is an extension of $J_{K,J_K^\vee} := J_K \times J_K^\vee$ by $\mathbb{G}_{m,J_K^\vee} = \mathbb{G}_m \times J_K^\vee$. In other words, $P_K^\times$ fits into the following short exact sequence of $J_K^\vee$-group schemes

$$1 \longrightarrow \mathbb{G}_{m,J_K^\vee} \longrightarrow P_K^\times \longrightarrow J_{K,J_K^\vee} \longrightarrow 0. \tag{3.5}$$

  To wit, let S be a K-scheme, $y \in J_K^\vee(S)$ be an S-point of $J_K^\vee$, and $x_1, x_2 \in J_K(S)$ be two S-points of J_K. Let $z_1, z_2 \in P_K^\vee(S)$ be two S-points lying above (x_1, y) and (x_2, y) respectively via the structure map j_K. This group structure can be described as follows. The data of the point z_1 (resp. z_2) is equivalent to a nowhere vanishing section $\alpha_1 \in (x_1, y)^* P_K(S)$ (resp. α_2) of the pullback of the Poincaré bundle. Now, as part of the requirement of being a $\mathbb{G}_m$-biextension, we have an isomorphism of line bundles over $\mathcal{O}_S$

$$(x_1, y)^* P_K \otimes (x_2, y)^* P_K \simeq (x_1 + x_2, y)^* P_K, \tag{3.6}$$

(supplied in this case by the theorem of the cube). Under this (canonical) isomorphism, the tensor product $\alpha_1 \otimes \alpha_2$ corresponds to a nowhere zero section α_3 of $(x_1+x_2, y)^* P_K$, thus producing a point $z_3 \in P_K^\times(S)$ that lies above the point (x_1+x_2, y) of $J_K \times J_K^\vee$. The commutativity of $P_K^\times$ as a $J_K^\vee$-group is clear, as well as the exact sequence displayed above. We denote by $+_1$ the resulting partial composition law on $P_K^\times$, which provides the group structure of $P_K^\times$ over $J_K^\vee$ (but not over K), in other words, it is defined on couples of points $z_1, z_2 \in P_K^\times(S)$ such that

$$\mathrm{pr}_2(j_K(z_1)) = \mathrm{pr}_2(j_K(z_2)).$$

Let us also denote the group structure on the $J_K^\vee$-group scheme $J_{K,J_K^\vee}$ by $+_1$ (again slightly abusing notations), then the partial composition law $+_1$ on $P_K^\times$ satisfies

$$z_1 +_1 z_2 \in P_K^\times(S) \ \longmapsto\ (x_1, y) +_1 (x_2, y) = (x_1 + x_2, y) \in J_{K,J_K^\vee}(S).$$

- **Partial composition $+_2$:** On the other hand, we may view $P_K^\times$ as a J_K-scheme via the structure morphism $\mathrm{pr}_1 \circ j_K$. As above, this makes $P_K^\times$ into an extension of $J_{K,J_K}^\vee$ by $\mathbb{G}_{m,J_K}$, which fits into a short exact sequence of commutative J_K-group schemes

$$1 \longrightarrow \mathbb{G}_{m,J_K} \longrightarrow P_K^\times \longrightarrow J_{K,J_K}^\vee \longrightarrow 0. \tag{3.7}$$

We denote by $+_2$ the resulting partial composition law on $P_K^\times$, this time defined on couples of points $z_1, z_2 \in P_K^\times(S)$ that satisfy

$$\mathrm{pr}_1(j_K(z_1)) = \mathrm{pr}_1(j_K(z_2)).$$

- **Compatibility:**

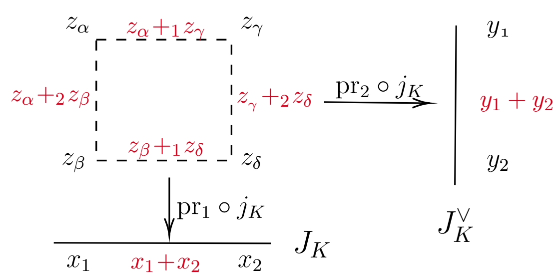
  The commutative group scheme extensions (3.5) and (3.7) are compatible in the following sense. Let S be any K-scheme. Let $z_\alpha, z_\beta, z_\gamma, z_\delta \in P_K^\times(S)$ be arbitrary S-points such that

$$j_K(z_\alpha) = (x_1, y_1), \quad j_K(z_\beta) = (x_1, y_2), \quad j_K(z_\gamma) = (x_2, y_1), \quad j_K(z_\delta) = (x_2, y_2)$$

  for some S-points $x_1, x_2 \in J_K(S)$ and $y_1, y_2 \in J_K^\vee(S)$. Then

$$(z_\alpha +_2 z_\beta) +_1 (z_\gamma +_2 z_\delta) = (z_\alpha +_1 z_\gamma) +_2 (z_\beta +_1 z_\delta). \tag{3.8}$$

  We summarise this compatibility in the following picture for the convenience of the reader.



Action of $\mathbb{G}_m$

Next, we briefly describe the action of $\mathbb{G}_m$ on the Poincaré torsor (or more general biextensions). To this end, we let $e_{J_K} \in \mathrm{Hom}_{J_K}(J_K, P_K^\vee)$ (resp. $e_{J_K^\vee} \in \mathrm{Hom}_{J_K^\vee}(J_K^\vee, P_K^\times)$) denote the identity section of $P_K^\times$ as a J_K (resp. $J_K^\vee$)-group scheme. Restricting the short exact sequence (3.5) of commutative $J_K^\vee$-group schemes via the identity section $\operatorname{Spec} K \to J_K^\vee$, we get a short exact sequence of commutative K-group schemes

$$1 \longrightarrow \mathbb{G}_{m,K} \longrightarrow P_K^\times|_{J_K \times \{0\}} \underset{\longrightarrow}{\overset{e_{J_K}}{\longleftarrow}} J_K \longrightarrow 0$$

which is split by the section e_{J_K}. In particular, we have $P_K^\times|_{J_K\times\{0\}} = \mathbb{G}_{m,J_K} = \mathbb{G}_{m,K}\times J_K$, and by a similar reasoning using the identity section $e_{J_K^\vee}$, $P_K^\times|_{\{0\}\times J_K^\vee} = \mathbb{G}_{m,J_K^\vee}$. These canonical splittings allow for a useful description of the $\mathbb{G}_m$-action on $P_K^\times$ in terms of the partial group laws $+_2$ and $+_1$. For a $(J_K \times J_K^\vee)$-scheme S, consider $t \in P_K^\times(S)$ and $u \in \mathbb{G}_m(S)$ and let (x, y) be the image of t in $(J_K \times J_K^\vee)(S)$. Consider a point $v = v_{x,u} \in P_K^\times(S)$ lying over $(x, 0)$, corresponding to $(u, 0)$ under the identification $P_K^\times|_{J_K\times\{0\}}(S) \simeq \mathbb{G}_m(S) \times J_K(S)$. The action of u on the point t is given by

$$u \cdot t = v +_2 t. \tag{3.9}$$

The point $v_{x,u}$ does not depend on t, only on x and u. The change of $v_{x,u}$ in the parameter x is described by the relative group law $+_1$, namely $v_{x_1+x_2,u} = v_{x_1,u} +_1 v_{x_2,u}$. Similarly, we have $v_{x,u_1u_2} = v_{x,u_1} +_2 v_{x,u_2}$.

Clearly, instead of using the point $(x, 0)$, one could work with $(0, y)$ and the operation $+_1$. These two points of view are equivalent by the compatibility between $+_1$ and $+_2$. As a consequence, the $\mathbb{G}_m$-action commutes with the operations $+_1$ and $+_2$: given two points $a, b \in P_K^\times(S)$ lying over points of the form $(x, *)$ in $J_K \times J_K^\vee(S)$ and $u, u' \in \mathbb{G}_m(S)$, we have

$$\begin{aligned}(u \cdot a) +_2 (u' \cdot b) &= (v_{x,u} +_2 a) +_2 (v_{x,u'} +_2 b)\\ &= (v_{x,u} +_2 v_{x,u'}) +_2 (a +_2 b)\\ &= (uu') \cdot (a +_2 b),\end{aligned} \tag{3.10}$$

and similarly for $+_1$.

3.1.2 Spreading out the geometry

As will become apparent, in the method of geometric quadratic Chabauty it is crucial to spread out the geometry over $\mathcal{O}_K$. Roughly speaking, one wants to work with finitely generated $\mathbb{Z}$-modules, and $\mathbb{G}_m(\mathcal{O}_K) = \mathcal{O}_K^\times$ is such a module whereas $\mathbb{G}_m(K) = K^\times$ is not.

Indeed, if r_1 and r_2 denote respectively the number of real embeddings and pairs of complex embeddings of K, then

$$\delta := \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K^\times = r_1 + r_2 - 1.$$

Models over $\mathcal{O}_K$

Let $\mathbf{C}$ denote a regular proper model of C_K over $\mathcal{O}_K$. Let $\mathbf{C}^{\mathrm{sm}}$ denote the smooth locus of $\mathbf{C}$. By properness and regularity, respectively, we have the identifications

$$C_K(K) = \mathbf{C}(\mathcal{O}_K) = \mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K).$$

Let $\mathbf{J}$ and $\mathbf{J}^\vee$ denote respectively the Néron models of J_K and $J_K^\vee$ over $\mathcal{O}_K$. Denote by $\mathbf{J}^\circ$ and $\mathbf{J}^{\vee,\circ}$ the fibrewise connected components of 0 in $\mathbf{J}$ and $\mathbf{J}^\vee$ respectively. The quotient $\mathbf{J}^\vee/\mathbf{J}^{\vee,\circ}$ is an étale group scheme over $\mathcal{O}_K$ with finite fibres.

Suppose that $C_K(K)$ is non-empty and let $b \in C_K(K)$ be a fixed rational point. Such a choice leads to the Abel–Jacobi map $j_b : C_K \hookrightarrow J_K$ which sends a point x to the linear equivalence class of the divisor $(x) - (b)$. The map j_b extends uniquely to a morphism

$$j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$$

over $\mathcal{O}_K$ by the Néron Mapping Property, which we shall again denote by j_b. Next, we wish to extend the Poincaré bundle to $\operatorname{Spec} \mathcal{O}_K$. This is supplied by Grothendieck's theory of biextensions.

Proposition 3.1. *The Poincaré torsor $P_K^\times$ extends uniquely to a biextension $\mathbf{P}^\times$ of $(\mathbf{J}, \mathbf{J}^{\vee,\circ})$ by $\mathbb{G}_m$. In particular, given an $\mathcal{O}_K$-scheme S and two points $(x,y), (x,y') \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(S)$, we have an isomorphism*

$$(x,y)^*\mathbf{P} \otimes (x,y')^*\mathbf{P} \simeq (x, y+y')^*\mathbf{P}, \tag{3.11}$$

where $\mathbf{P}$ is the line bundle over $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ corresponding to $\mathbf{P}^\times$.

Proof. This is [79, VIII. Theorem 7.1(b) and Remark 7.2]. Note that we have restricted to the connected subscheme $\mathbf{J}^{\vee,\circ}$ in order to apply the theorem cited above. □

We denote the structural morphism of this $\mathbb{G}_m$-torsor by

$$j : \mathbf{P}^{\times} \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}.$$

The uniqueness of the extension follows from the connectedness of $\mathbf{J}^{\vee,\circ}$. Let us remark that the commutative group scheme extension structures and their compatibilities from the discussion in Section 3.1.1 extend to the integral version $\mathbf{P}^{\times}$.

Integral points on the Poincaré torsor

The goal of this subsection is to lift certain integral points on $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ across the structure map $j : \mathbf{P}^{\times} \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}$. Let (x, y) be an $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$, and $(x, y)^*\mathbf{P}^{\times}$ be the pull-back of $\mathbf{P}^{\times}$ to $\mathcal{O}_K$ – which is a $\mathbb{G}_{m,\mathcal{O}_K}$-torsor over $\operatorname{Spec} \mathcal{O}_K$ – as shown in the diagram

$$\begin{array}{ccc} (x,y)^*\mathbf{P}^{\times} & \longrightarrow & \mathbf{P}^{\times} \\ \downarrow & \square & \downarrow \\ \operatorname{Spec} \mathcal{O}_K & \xrightarrow{(x,y)} & \mathbf{J} \times \mathbf{J}^{\vee,\circ}. \end{array} \tag{3.12}$$

Lifting the point (x, y) to $\mathbf{P}^{\times}$ amounts to finding a section of the torsor $(x, y)^*\mathbf{P}^{\times} \to \operatorname{Spec} \mathcal{O}_K$.

Note that, in the case $K = \mathbb{Q}$, all $\mathbb{G}_m$-torsors are trivial over $\operatorname{Spec} \mathbb{Z}$ and admit a section over $\mathbb{Z}$, unique up to $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. Thus a lift of the integral point (x, y) to $\mathbf{P}^{\times}$ always exists. In the case of a general number field K, it is not always possible to lift an $\mathcal{O}_K$-point (x, y) of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ to $\mathbf{P}^{\times}$ when the class number h of K is non-trivial. However, the previous argument carries over to $\mathcal{O}_K$-points of the form $(x, h \cdot y)$.

Lemma 3.1. *Any $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ of the form $(x, h \cdot y)$ with $(x, y) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$ admits a lift to an $\mathcal{O}_K$-point of the Poincaré torsor $\mathbf{P}^{\times}$. This lift is unique up to multiplication by an element of $\mathcal{O}_K^{\times}$.*

Proof. We repeatedly apply the isomorphisms (3.11) and obtain an isomorphism

$$((x,y)^*\mathbf{P})^{\otimes h} \simeq (x, h\cdot y)^*\mathbf{P}$$

of line bundles over $\operatorname{Spec}\mathcal{O}_K$. In particular, we know that $(x, h\cdot y)^*\mathbf{P}^\times$ is trivial as a $\mathbb{G}_m$-torsor over $\mathcal{O}_K$, since $\operatorname{Pic}(\mathcal{O}_K)$ has size h. □

3.2 Construction of the torsor T

The goal of this section is to construct a certain $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$ along with a lift of the Abel–Jacobi map $j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$ to it. This is the torsor alluded to in the introduction, and we recall that ρ denotes the rank of the Néron-Severi group of J_K. We begin by constructing the corresponding torsor T_K over J_K at the level of generic fibres, and then proceed to spread out the geometry. Once the torsor $\mathbf{T}$ has been defined, we construct the lift of the Abel–Jacobi map.

3.2.1 Trivialisation of the Poincaré torsor

Let $\lambda : J_K \xrightarrow{\sim} J_K^\vee$ be the canonical principal polarisation of Section 3.1.1. By functoriality of Pic we have the following commutative diagram of commutative K-group schemes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_K^\vee & \longrightarrow & \mathrm{Pic}_{J_K/K} & \xrightarrow{\pi} & \mathrm{NS}_{J_K/K} & \longrightarrow & 0 \\ & & \wr\downarrow -\lambda^{-1} & & \downarrow j_b^* & & \downarrow j_{b,\mathrm{NS}}^* & & \\ 0 & \longrightarrow & J_K & \longrightarrow & \mathrm{Pic}_{C_K/K} & \xrightarrow{\deg} & \mathbb{Z}_K & \longrightarrow & 0. \end{array} \tag{3.13}$$

Here $\mathrm{NS}_{J_K/K}$ denotes the Néron–Severi group scheme of J_K, i.e., the étale K-group scheme of components of the Picard scheme associated to J_K. Moreover, we have used the fact that the map induced by j_b on Pic^0 agrees with $-\lambda^{-1}$, which is in particular an isomorphism.

Next, let $\mathbf{Hom}(J_K, J_K^\vee)^+ \subset \mathbf{Hom}(J_K, J_K^\vee)$ denote the closed subgroup scheme of self-dual homomorphisms. See [63, Proposition 7.14 & §7.18] for representability. There is a map

$$\varphi : \mathrm{Pic}_{J_K/K} \longrightarrow \mathbf{Hom}(J_K, J_K^\vee)^+$$

defined by sending the class of a line bundle L to the map φ_L, which maps a closed point $x \in J_K$ to $[\mathrm{t}_x^* L \otimes L^{-1}]$ where $\mathrm{t}_x : J_K \longrightarrow J_K$ denotes the translation by x. The kernel of φ is equal to $\mathrm{Pic}^0_{J_K/K} = J_K^\vee$ and the map φ induces an isomorphism of K-group schemes [63, Corollary 11.3]

$$\tilde{\varphi} : \mathrm{NS}_{J_K/K} \xrightarrow{\sim} \mathbf{Hom}(J_K, J_K^\vee)^+. \tag{3.14}$$

Definition 3.3. At the level of K-points, we define the group $\mathrm{Hom}(J_K, J_K^\vee)_0^+$ to be the kernel

$$\mathrm{Hom}(J_K, J_K^\vee)_0^+ := \ker\left(j_{b,\mathrm{NS}}^* \circ \tilde{\varphi}^{-1} : \mathrm{Hom}(J_K, J_K^\vee)^+ \to \mathbb{Z}\right)$$

Proposition 3.2. *For all $f \in \mathrm{Hom}(J_K, J_K^\vee)_0^+$, there exists a unique element $c_f \in J_K^\vee(K)$ with the property that the following $\mathbb{G}_m$-torsor*

$$j_b^*(\mathrm{id}, \mathrm{t}_{c_f} \circ f)^* P_K^\times$$

over C_K is trivial. Here $(\mathrm{id}, \mathrm{t}_{c_f} \circ f)$ denotes the map $J_K \xrightarrow{(\mathrm{id}, \mathrm{t}_{c_f} \circ f)} J_K \times J_K^\vee$. In particular, for all $n \in \mathbb{Z}_{\geq 1}$, its n^{th} power $j_b^*(\mathrm{id}, n \cdot \circ \mathrm{t}_{c_f} \circ f)^* P_K^\times$ is also trivial.

Proof. At the level of $\overline{K}$-points, the diagram (3.13) can be written as follows:

$$\begin{array}{ccccccccc}
 & & & & & & \mathrm{Hom}(J_K, J_K^\vee)_0^+ & & \\
 & & & & & \swarrow s_2, \ s_1 & \downarrow & & \\
 & & & & \ker(j_{b,\overline{K}}^*) & \xrightarrow{\sim} & \ker(j_{b,\overline{K},\mathrm{NS}}^*) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J_K^\vee(\overline{K}) & \longrightarrow & \mathrm{Pic}(J_{\overline{K}}) & \xrightarrow{\pi} & \mathrm{NS}_{J_K/K}(\overline{K}) & \longrightarrow & 0 \\
 & & \wr\downarrow -\lambda^{-1} & & \downarrow j_{b,\overline{K}}^* & & \downarrow j_{b,\overline{K},\mathrm{NS}}^* & & \\
0 & \longrightarrow & J_K(\overline{K}) & \longrightarrow & \mathrm{Pic}(C_{\overline{K}}) & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0.
\end{array} \tag{3.15}$$

The map π in the first short exact sequence in this diagram admits two splittings when restricted to $\mathrm{Hom}(J_K, J_K^\vee)_0^+$, which is viewed as a subgroup of $\ker(j^*_{b,\overline{K},\mathrm{NS}})$ via $\tilde{\varphi}^{-1}$. The first section

$$s_1 : \mathrm{Hom}(J_K, J_K^\vee)^+ \longrightarrow \mathrm{Pic}(J_{\overline{K}})$$

is defined by mapping a self-dual homomorphism f defined over K to the isomorphism class of the $\mathbb{G}_m$-torsor $L_f^\times := (\mathrm{id}, f)^* P_K^\times$ on J_K, which is an element of $\mathrm{Pic}(J_K) \subset \mathrm{Pic}(J_{\overline{K}})$. We observe, by [63, Proposition 11.1], that

$$\tilde{\varphi} \circ \pi \circ s_1(f) = \varphi_{L_f} = f + f^\vee = 2f.$$

The second splitting is given by inverting π on $\ker(j^*_{b,\overline{K}})$, in other words, by

$$s_2 : \mathrm{Hom}(J_K, J_K^\vee)_0^+ \hookrightarrow \ker(j^*_{b,\overline{K},\mathrm{NS}}) \xrightarrow{\pi^{-1}} \ker(j^*_{b,\overline{K}}) \subset \mathrm{Pic}(J_{\overline{K}}).$$

Again the image of s_2 lies in $\mathrm{Pic}(J_K)$. Now, given $f \in \mathrm{Hom}(J_K, J_K^\vee)_0^+$ we define

$$c_f := 2s_2(f) - s_1(f) \in \mathrm{Pic}(J_K).$$

As $c_f \in \ker(\pi)$ we thus have $c_f \in J_K^\vee(K)$. Now we observe that, for a line bundle L on J_K corresponding to a closed point $x \in J_K^\vee$, we have

$$(\mathrm{id}, f)^*\Big((\mathrm{id} \times \mathrm{t}_x)^* P_K\Big) \simeq (\mathrm{id}, f)^*\big(P_K \otimes \mathrm{pr}_1^* L\big) \simeq (\mathrm{id}, f)^* P_K \otimes L,$$

where pr_1 is the projection $J_K \times J_K^\vee \longrightarrow J_K$. Therefore, by construction, c_f is the unique element in $J_K^\vee(K)$ such that

$$s_1(f) + c_f = [(\mathrm{id}, \mathrm{t}_{c_f} \circ f)^* P_K^\times] \in \ker j_b^*.$$

This proves the proposition. $\square$

The group $\mathrm{NS}_{J_K/K}(K)$ is a finitely generated free $\mathbb{Z}$-module whose rank is denoted by ρ; this is the Picard number of J_K. The kernel

$$\ker(j_{b,\mathrm{NS}}^* : \mathrm{NS}_{J_K/K}(K) \to \mathbb{Z})$$

is a free $\mathbb{Z}$-module of rank $\rho - 1$, and so is the group $\mathrm{Hom}(J_K, J_K^\vee)_0^+$.

Notation 3.1. We fix the following notations from now on.

- Let $f_1, \ldots, f_{\rho-1}$ be a basis of $\mathrm{Hom}(J_K, J_K^\vee)_0^+$.
- For each $i = 1, \ldots, \rho - 1$, let $c_i := c_{f_i} \in J_K^\vee(K)$ be the element corresponding to f_i in Proposition 3.2.
- For each integer $n \in \mathbb{Z}_{\geq 1}$, denote by $\alpha_{n,i,K}$ the map

$$\alpha_{n,i,K} : J_K \xrightarrow{(\mathrm{id}, n \cdot \circ\, \mathrm{t}_{c_i} \circ f_i)} J_K \times J_K^\vee.$$

Definition 3.4. By Proposition 3.2, the pull-back $j_b^*\big(\alpha_{n,i,K}^* P_K^\times\big)$ is a trivial $\mathbb{G}_m$-torsor over C_K. In particular, it admits a section over C_K. This gives rise to a lift of j_b, unique up to $K^\times$, which we shall fix and denote by $\tilde{j}_b^{(n,i)}$ as in the diagram below:

$$\begin{array}{ccccc} & & \alpha_{n,i,K}^* P_K^\times & \longrightarrow & P_K^\times \\ & \overset{\tilde{j}_b^{(n,i)}}{\nearrow} & \downarrow & \square & \downarrow \\ C_K & \xrightarrow{j_b} & J_K & \xrightarrow{\alpha_{n,i,K}} & J_K \times J_K^\vee. \end{array} \tag{3.16}$$

3.2.2 Definition of $\mathbf{T}$

Let us introduce and recall some notations and refer the rest to Section 3.1.2. Let $\mathfrak{n}$ be the product of prime ideals in $\mathcal{O}_K$ such that $\mathbf{C}$ is smooth away from $\mathrm{Spec}(\mathcal{O}_K/\mathfrak{n})$. Let $\Phi^\vee = \mathbf{J}^\vee/\mathbf{J}^{\vee,\circ}$ be the group scheme of connected components of $\mathbf{J}^\vee$. It is trivial outside

$\mathcal{O}_K/\mathfrak{n}$ with finite étale fibres over $\mathcal{O}_K/\mathfrak{n}$. Let m denote the least common multiple of the exponents of $\Phi^\vee(\bar{\mathbb{F}}_\mathfrak{q})$ over all prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$. Finally, recall that h denotes the class number of K.

By the Néron Mapping Property, for each $i \in \{1, \ldots, \rho - 1\}$, the maps

$$\begin{cases} f_i : J_K \longrightarrow J_K^\vee \\ \mathrm{t}_{c_i} : J_K^\vee \longrightarrow J_K^\vee \\ hm\cdot : J_K^\vee \longrightarrow J_K^\vee \end{cases} \qquad \text{extend uniquely to} \qquad \begin{cases} f_i : \mathbf{J} \longrightarrow \mathbf{J}^\vee \\ \mathrm{t}_{c_i} : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee \\ hm\cdot : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee. \end{cases}$$

Therefore, the morphism $\alpha_{hm,i,K} : J_K \longrightarrow J_K \times J_K^\vee$ extends uniquely to a morphism of $\mathcal{O}_K$-schemes

$$\alpha_{hm,i} = (\mathrm{id}, hm \cdot \circ \mathrm{t}_{c_i} \circ f_i) : \mathbf{J} \longrightarrow \mathbf{J} \times \mathbf{J}^\vee.$$

The integer m is chosen so that the image of this map lies in $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$.

Definition 3.5. Taking the product over $i \in \{1, \ldots, \rho - 1\}$, we obtain the $\mathcal{O}_K$-morphism

$$\alpha = (\mathrm{id}, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})) := (\mathrm{id}, (hm\cdot \circ \mathrm{t}_{c_i} \circ f_i)_{i=1}^{\rho-1}) : \mathbf{J} \longrightarrow \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$$

Consider the map $\mathbf{P}^\times \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ} \longrightarrow \mathbf{J}$ defined as the composition of the structure map j with the first projection. Using this morphism, we form the $(\rho - 1)$-fold self-product

$$\mathbf{P}^{\times,\rho-1} := \mathbf{P}^\times \times_\mathbf{J} \ldots \times_\mathbf{J} \mathbf{P}^\times.$$

We naturally have a morphism $\mathbf{P}^{\times,\rho-1} \longrightarrow \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$, which endows $\mathbf{P}^{\times,\rho-1}$ with the structure of a $\mathbb{G}_m^{\rho-1}$-torsor over $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$. This leads to the following key construction in the article.

Definition 3.6. Retain notations from Definition 3.5. We define the $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$

to be the pull-back of the $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{P}^{\times,\rho-1}$ over $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$ by the map α:

$$\mathbf{T} := \mathbf{P}^{\times,\rho-1} \times_\alpha \mathbf{J} = \alpha^* \mathbf{P}^{\times,\rho-1} = (\mathrm{id}, hm \cdot \circ \, \mathrm{t}_{c_1} \circ f_1)^* \mathbf{P}^\times \times_{\mathbf{J}} \ldots \times_{\mathbf{J}} (\mathrm{id}, hm \cdot \circ \, \mathrm{t}_{c_{\rho-1}} \circ f_{\rho-1})^* \mathbf{P}^\times.$$

3.2.3 Lifting the Abel–Jacobi map

Now we return to the lifts $\tilde{j}_b^{(hm,i)}$ obtained in Definition 3.4. By taking the product over i of these lifts $\tilde{j}_b^{(hm,i)}$, we obtain a lift $\tilde{j}_b$ of j_b to $T_K := \mathbf{T} \times_J J_K$ as pictured in the following commutative diagram:

$$\begin{array}{ccccc} & & T_K & \longrightarrow & P_K^{\times,\rho-1} \\ & \overset{\tilde{j}_b}{\nearrow} & \downarrow & \square & \downarrow \\ C_K & \xrightarrow{j_b} & J_K & \xrightarrow{\alpha_K} & J_K \times (J_K^{\vee,0})^{\rho-1} \end{array} \tag{3.17}$$

where α_K denotes the base change of the map α to K.

The goal is to extend this diagram over $\mathcal{O}_K$. However, lifting the map $j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$ to the torsor $\mathbf{T}$ is not generally possible: the problem is that, for primes $\mathfrak{q}|\mathfrak{n}$, the fibre $C_{\mathbb{F}_\mathfrak{q}}^{\mathrm{sm}} := \mathbf{C}^{\mathrm{sm}} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} \mathbb{F}_\mathfrak{q}$ may contain too many components. To remedy this, we consider one geometrically irreducible component in each such fibre at a time.

Definition 3.7. Let $\mathbf{U} \subset \mathbf{C}^{\mathrm{sm}}$ be an open subscheme obtained by removing, for every $\mathfrak{q}|\mathfrak{n}$, all but one irreducible component of $C_{\mathbb{F}_\mathfrak{q}}^{\mathrm{sm}}$ that is further geometrically irreducible. We will later lift the map j_b to a map $\tilde{j}_b^U : \mathbf{U} \longrightarrow \mathbf{T}$ for each such open subscheme $\mathbf{U}$.

Remark 3.3. We first remark that such a subscheme $\mathbf{U}$ exists under the assumption that C_K admits a K-rational point. Moreover, for the purposes of determining the set of rational points $C_K(K) = \mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$, it suffices to consider subschemes of the form $\mathbf{U}$ as there are finitely many of them and each point in $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$ lies in exactly one such $\mathbf{U}$. Both remarks follow from the following simple lemma.

Lemma 3.2. *Let X be an irreducible variety over a field k that admits a smooth k-rational* *point. Then X is geometrically irreducible.*

Proof. Let $A = \Gamma(U, \mathcal{O}_X)$ be the ring of functions on a normal affine open neighborhood U of the smooth rational point. Then A admits a map $A \longrightarrow k$ of k-algebras. Letting k' be the separable algebraic closure of k in the function field $k(X) = \mathrm{Frac}(A)$, as U is normal we have $k' \subset A$ which forces $k' = k$. This is equivalent to X being geometrically irreducible by [80, Corollaire 4.5.10]. $\square$

We are finally able to construct the desired lift of j_b. The construction is analogous to that in [62, §2] except that we pull back $\mathbf{P}^{\times}$ via morphisms of the form

$$(\mathrm{id}, hm\cdot \circ \mathrm{t}_c \circ f) : \mathbf{J} \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ},$$

where in the second factor we incorporate an additional multiplication by h, the class number of $\mathcal{O}_K$, to ensure the existence of such a lift.

Proposition 3.3. *Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as in Definition 3.7. There exists a lift $\tilde{j}_b^U$ of $j_b|_{\mathbf{U}}$ to $\mathbf{T}$, unique up to $\mathcal{O}_K^{\times,\rho-1}$, which makes the following diagram commute:*

$$\begin{array}{ccccccc} & & & & \mathbf{T} & \longrightarrow & \mathbf{P}^{\times,\rho-1} \\ & & \overset{\tilde{j}_b^U}{\nearrow} & & \downarrow & \square & \downarrow \\ \mathbf{U} & \hookrightarrow & \mathbf{C}^{\mathrm{sm}} & \xrightarrow{j_b} & \mathbf{J} & \xrightarrow{\alpha} & \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}. \end{array} \tag{3.18}$$

Proof. The restriction of the torsor $(\mathrm{id}, m\cdot \circ \mathrm{t}_{c_i} \circ f_i)^*\mathbf{P}^{\times}$ to $\mathbf{U}$ gives an element of $\mathrm{Pic}(\mathbf{U})$, whose pull-back to C_K equals $j_b^*\alpha_{m,i,K}^* P_K^{\times}$ and is trivial by Proposition 3.2. In other words, the torsor $(\mathrm{id}, m\cdot \circ \mathrm{t}_{c_i} \circ f_i)^*\mathbf{P}^{\times}$, when restricted to $\mathbf{U}$, gives rise to an element in the kernel

$$\ker(\mathrm{Pic}(\mathbf{U}) \longrightarrow \mathrm{Pic}(C_K)).$$

Now note that we have an isomorphism of line bundles (corresponding to $\mathbb{G}_{m,\mathbf{J}}$-torsors)

$$(\mathrm{id}, hm\cdot \circ \mathrm{t}_{c_i} \circ f_i)^*\mathbf{P} \simeq ((\mathrm{id}, m\cdot \circ \mathrm{t}_{c_i} \circ f_i)^*\mathbf{P})^{\otimes h} \tag{3.19}$$

using the isomorphism (3.11). By Lemma 3.3 below, we conclude that $(\mathrm{id}, hm\cdot\circ \mathrm{t}_{c_i}\circ f_i)^*\mathbf{P}^\times$ becomes a trivial $\mathbb{G}_{m,\mathbf{U}}$-torsor when restricted to $\mathbf{U}$. Therefore, $\mathbf{T}$ pulls back to the trivial $\mathbb{G}_{m,\mathbf{U}}^{\rho-1}$-torsor over $\mathbf{U}$. In particular, the map $j_b|_{\mathbf{U}}$ admits a lift to $\mathbf{T}$, which is unique up to

$$\mathbb{G}_m^{\rho-1}(\mathbf{U}) = (\mathcal{O}_{\mathbf{U}}(\mathbf{U})^\times)^{\rho-1} = (\mathcal{O}_K^\times)^{\rho-1}$$

again by Lemma 3.3. □

The following lemma is used in the proof above.

Lemma 3.3. *Let* $\mathbf{U}$ *be an open subscheme of* $\mathbf{C}^{\mathrm{sm}}$ *as in Definition 3.7. Then* $\mathcal{O}_{\mathbf{U}}(\mathbf{U}) = \mathcal{O}_K$ *and the kernel of the restriction* $\ker(\mathrm{Pic}(\mathbf{U})\longrightarrow \mathrm{Pic}(C_K))$ *is entirely* h*-torsion. In other words, for a line bundle* L *over* $\mathbf{U}$ *that becomes trivial over the generic fibre* C_K*,* $L^{\otimes h}$ *is trivial over* $\mathbf{U}$*.*

Proof. By construction, $\mathbf{U}$ is regular and thus locally factorial, so we do not distinguish between the class of line bundles and Weil divisors. First let D be a vertical divisor on $\mathbf{U}$; namely, it does not intersect the generic fibre C_K. We claim that $hD = 0$ in $\mathrm{Pic}(\mathbf{U})$. As every irreducible vertical divisor on $\mathbf{U}$ is of the form $\mathbf{U}_{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$, we may write hD as $\sum_{\mathfrak{p}} hn_{\mathfrak{p}}U_{\mathbb{F}_{\mathfrak{p}}}$, where $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. Clearly D is the image of the divisor $\sum_{\mathfrak{p}} hn_{\mathfrak{p}}\mathfrak{p}$ along the natural map $\mathrm{Pic}(\mathcal{O}_K) \to \mathrm{Pic}(\mathbf{U})$, which is 0 since $\mathrm{Pic}(\mathcal{O}_K)$ has size h. Now let D be a general element of $\mathrm{Pic}(\mathbf{U})$ (which we view as a Weil divisor on $\mathbf{U}$) that lies in the kernel $\ker(\mathrm{Pic}(\mathbf{U})\longrightarrow \mathrm{Pic}(C_K))$. In other words, the restriction of D to C_K is a principal divisor $D_K = \mathrm{div}(f)$ for some f in the function field of C_K. Then $\mathrm{div}(f)$ extends to a principal divisor on $\mathbf{U}$, which differs from D only by a vertical divisor. The lemma thus follows. □

Remark 3.4. When $h = 1$, the lemma simply says that the restriction $\mathrm{Pic}(\mathbf{U})\longrightarrow \mathrm{Pic}(C_K)$ is injective. This map is of course not in general injective when $h \neq 1$. Indeed, in this case it suffices to take $D = U_{\mathfrak{p}} \in \mathrm{Div}(\mathbf{U})$ where $\mathfrak{p}$ is a non-principal prime ideal of $\mathcal{O}_K$.

3.3 The main theorem

In this section we state a precise version of the main theoretical results of the chapter. We also describe the strategy of the geometric method in slightly more detail.

Assumption 3.1. *Throughout, we make the following assumption on the prime p.*

- *The curve C_K has good reduction at each prime $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of K that lies above p.*
- *Each $\mathfrak{p}_i$ satisfies $e(\mathfrak{p}_i/p) < p-1$.*
- *Finally, p does not divide $|\mathcal{O}_{K,\mathrm{tors}}^{\times}|$.*

Note that the first condition is equivalent to requiring that $\mathfrak{p}_i \nmid \mathfrak{n}$ for each $i \in \{1, \ldots, s\}$ and that Assumption 3.1 excludes only finitely many primes.

Notation 3.2. We further adopt the following notation:

- Let $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes \mathbb{Z}_p$ be the p-adic completion of $\mathcal{O}_K$. This is isomorphic to the product of the $\mathfrak{p}_i$-adic completions $\mathcal{O}_{K,\mathfrak{p}_1} \times \ldots \times \mathcal{O}_{K,\mathfrak{p}_s}$.
- Let $\overline{\mathcal{O}_{K,p}}$ denote $(\mathcal{O}_K \otimes \mathbb{F}_p)_{\mathrm{red}}$, which is isomorphic to the product of the residue fields $\mathbb{F}_{\mathfrak{p}_1} \times \ldots \times \mathbb{F}_{\mathfrak{p}_s}$.
- For any $\mathcal{O}_K$-scheme X, we have natural identifications

$$\begin{cases} X(\mathcal{O}_{K,p}) = X_{\mathcal{O}_{K,\mathfrak{p}_1}}(\mathcal{O}_{K,\mathfrak{p}_1}) \times \ldots \times X_{\mathcal{O}_{K,\mathfrak{p}_s}}(\mathcal{O}_{K,\mathfrak{p}_s}), \\ X(\overline{\mathcal{O}_{K,p}}) = X_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_{\mathfrak{p}_1}) \times \ldots \times X_{\mathbb{F}_{\mathfrak{p}_s}}(\mathbb{F}_{\mathfrak{p}_s}). \end{cases}$$

  We denote the natural reduction map by

$$\mathrm{red} : X(\mathcal{O}_{K,p}) \longrightarrow X(\overline{\mathcal{O}_{K,p}}).$$

- Given a point $x \in X(\overline{\mathcal{O}_{K,p}})$, we denote by $X(\mathcal{O}_{K,p})_x$ the set $\mathrm{red}^{-1}(x)$, namely the residue disk in $X(\mathcal{O}_{K,p})$ that reduces to the point x. Likewise, we denote by $X(\mathcal{O}_K)_x$ the pre-image of $X(\mathcal{O}_{K,p})_x$ under the natural inclusion

$$X(\mathcal{O}_K) \longleftrightarrow X(\mathcal{O}_{K,p}),$$

which consists of rational points in the residue disk $X(\mathcal{O}_{K,p})_x$.

Remark 3.5. The reason for working with all primes above p simultaneously (instead of fixing a single prime) is explained in Section 0.4.2 (after the statement of Theorem C).

3.3.1 Revisiting the strategy

Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as in Definition 3.7. Let u be an element in the finite set $\mathbf{U}(\overline{\mathcal{O}_{K,p}})$, and let

$$t := \tilde{j}_b^U(u) \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$$

be its image in $\mathbf{T}$ under the lift $\tilde{j}_b^U : \mathbf{U} \longrightarrow \mathbf{T}$ of Proposition 3.3. Note that $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$ is the disjoint union of $\mathbf{U}(\mathcal{O}_K)$ for the finitely many choices of $\mathbf{U}$'s (Remark 3.3), and each $\mathbf{U}(\mathcal{O}_K)$ is the disjoint union of finitely many residue disks $\mathbf{U}(\mathcal{O}_K)_u$. Thus, it suffices to bound the size of $\mathbf{U}(\mathcal{O}_K)_u$ for each $\mathbf{U}$ and each point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$.

The key idea of the approach can be represented using the following commutative diagram:

$$\begin{array}{ccccc} \mathbf{U}(\mathcal{O}_K)_u & & \hookrightarrow & & \mathbf{U}(\mathcal{O}_{K,p})_u \\ \big\downarrow \tilde{j}_b^U & & & & \big\downarrow \tilde{j}_b^U \\ \mathbf{T}(\mathcal{O}_K)_t & \hookrightarrow & \mathbf{Y}_t & \hookrightarrow & \mathbf{T}(\mathcal{O}_{K,p})_t \end{array} \tag{3.20}$$

where the top horizontal arrow is induced by the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,p}$, while

$$\mathbf{Y}_t := \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$$

denotes the p-adic completion of $\mathbf{T}(\mathcal{O}_K)_t$ in $\mathbf{T}(\mathcal{O}_{K,p})_t$. We view $\mathbf{U}(\mathcal{O}_K)_u$ (resp. $\mathbf{U}(\mathcal{O}_{K,p})_u$) as a subset of $\mathbf{T}(\mathcal{O}_K)_t$ (resp. $\mathbf{T}(\mathcal{O}_{K,p})_t$) via the map $\tilde{j}_b^U$ in the diagram above. In particular, we have inclusions $\mathbf{U}(\mathcal{O}_K)_u \hookrightarrow \mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$. As explained in the introduction, the goal is to bound the intersection

$$\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t \tag{3.21}$$

which takes place in the p-adic manifold $\mathbf{T}(\mathcal{O}_{K,p})_t$.

Remark 3.6. For this intersection to have a chance to be finite, some conditions must be imposed in the style of the original Chabauty condition $r < g$. We will come back to this point in Section 3.3.3 after stating the main technical result of the paper.

3.3.2 The key technical result

In this subsection we give a description of $\mathbf{Y}_t$, which is a crucial step in bounding the intersection (3.21).

Notation 3.3. We fix the following notations.

- Recall that $r := \operatorname{rank}_{\mathbb{Z}} J_K(K)$ be the Mordell–Weil rank of J_K over K.
- We let $\mathbf{J}(\mathcal{O}_K)_0$ denote the subgroup of $J_K(K) = \mathbf{J}(\mathcal{O}_K)$ given by the kernel

  $$\mathbf{J}(\mathcal{O}_K)_0 := \ker\left(\mathrm{red} : \mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\overline{\mathcal{O}_{K,p}})\right).$$

- Let q^* denote the exponent of $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, that is, the least common multiple of

  $$q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$$

  for $i \in \{1, \ldots, s\}$.
- For each $i \in \{1, \ldots, s\}$, let $k_i = k_{\mathfrak{p}_i} = e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}$ be the $\mathbb{Z}_p$ rank of $\mathcal{O}_{K,\mathfrak{p}_i}$. Note that the rank of $\mathcal{O}_{K,p}$ as a $\mathbb{Z}_p$-module is $\sum_{\mathfrak{p}_i | p} k_i = d$, where d is the degree of K over $\mathbb{Q}$.

By Assumption 3.1 on p, we know that for each $i \in \{1, \dots, s\}$, the reduction map $\mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\mathbb{F}_{\mathfrak{p}_i})$ is injective on the torsion points of $\mathbf{J}(\mathcal{O}_K)$ by [99, Appendix]. Hence $\mathbf{J}(\mathcal{O}_K)_0$ is a free $\mathbb{Z}$-module of rank r. The scheme $\mathbf{T} \times_{\mathcal{O}_K} \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ is smooth over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension $g + \rho - 1$. By choosing a regular system of parameters for the residue disk above the point $t \in \mathbf{T}(\mathbb{F}_{\mathfrak{p}})$, as well as an isomorphism of $\mathbb{Z}_p$-modules $\mathcal{O}_{K,\mathfrak{p}} \simeq \mathbb{Z}_p^{k_{\mathfrak{p}}}$, we obtain a homeomorphism

$$\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_t \simeq \mathbb{Z}_p^{(g+\rho-1)k_{\mathfrak{p}}}.$$

In particular, the dimension of $\mathbf{T}(\mathcal{O}_{K,p})$ as a locally analytic p-adic manifold is

$$(g + \rho - 1) \sum_{\mathfrak{p} | p} k_{\mathfrak{p}} = (g + \rho - 1)d.$$

The idea is to parametrise the p-adic closure $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ using the free $\mathbb{Z}_p$-module

$$(\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p.$$

Here the subscript "tf" stands for the torsion free quotient, i.e., the quotient by the torsion subgroup. In Section 3.4.1, we will prove the following proposition (for the precise form, see Proposition 3.7).

Proposition 3.4. *Upon fixing a basis for the free $\mathbb{Z}$-module $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0$, there exists a map*

$$E' : \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t, \tag{3.22}$$

which can be described using the partial composition laws of Section 3.1.1, and satisfies the property

$$E'(q^* \mathbb{Z}^{\delta(\rho-1)+r}) \subset \mathbf{T}(\mathcal{O}_K)_t \subset E'(\mathbb{Z}^{\delta(\rho-1)+r}). \tag{3.23}$$

Here q^* is the integer defined in Notation 3.3.

We then p-adically interpolate the map E' to get the following result in Section 3.4.2.

Theorem 3.2. *There is a unique map*

$$\kappa : (\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$$

which makes the diagram

$$\begin{array}{ccccccc}
\mathbb{Z}^{\delta(\rho-1)+r} & \xrightarrow{\sim} & \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0 & \xrightarrow{E'} & \mathbf{T}(\mathcal{O}_{K,p})_t & \xrightarrow{\sim} & \mathbb{Z}_p^{(g+\rho-1)d} \\
\big\downarrow & & \big\downarrow & & \big\| & & \big\| \\
\mathbb{Z}_p^{\delta(\rho-1)+r} & \xrightarrow{\sim} & (\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p & \xrightarrow{\exists! \kappa} & \mathbf{T}(\mathcal{O}_{K,p})_t & \xrightarrow{\sim} & \mathbb{Z}_p^{(g+\rho-1)d}
\end{array}$$

commute, such that the composed map in the bottom row is given by a $(g+\rho-1)d$-tuple of convergent power series $(\kappa_1, \ldots, \kappa_{(g+\rho-1)d})$ with $\kappa_i \in \mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$.

Corollary 3.1. *The image of the map κ is the p-adic closure $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$.*

Proof. Since $\mathbb{Z}_p^{\delta(\rho-1)+r}$ is compact and κ is continuous, the image of κ is closed in $\mathbf{T}(\mathcal{O}_{K,p})_t$. Since κ extends E', the second containment of (3.23) implies that $\operatorname{Im}\kappa$ contains $\mathbf{T}(\mathcal{O}_K)_t$, thus also contains $\mathbf{Y}_t$. On the other hand $q^*\mathbb{Z}^{\delta(\rho-1)+r}$ is dense in $\mathbb{Z}_p^{\delta(\rho-1)+r}$ since q^* is coprime to p. By continuity of κ, we have

$$\operatorname{Im}\kappa = E'\left(\overline{q^*\mathbb{Z}^{\delta(\rho-1)+r}}\right) \subset \overline{E'(q^*\mathbb{Z}^{\delta(\rho-1)+r})} \subset \mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$$

where the last containment uses the first inclusion of (3.23). This concludes the proof. □

Finally, to finish the theoretical component of the geometric quadratic Chabauty method, we prove the following result in Section 3.5.1. To state this result, we first remark that the course of the proof of Theorem 3.2 provides us with a certain ideal

$$I_{\mathbf{U},u} \subset \mathbb{Z}_p\langle z_1, ..., z_{\delta(\rho-1)+r}\rangle =: R,$$

which depends on $\mathbf{U}$ and the point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$. See Section 3.5.1 for its construction. The more precise form of Theorem 3.1, modulo the construction of the ideal I, is the following:

Theorem 3.3. *If $\overline{A}_{\mathbf{U},u} := \big(R/I_{\mathbf{U},u}\big) \otimes \mathbb{F}_p$ is finite dimensional over $\mathbb{F}_p$, then the number of rational points in $\mathbf{U}(\mathcal{O}_K)_u$ is finite and bounded by*

$$|\mathbf{U}(\mathcal{O}_K)_u| \leq \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}.$$

As discussed in the introduction, we expect this to provide an explicit algorithm to compute rational points on C_K.

3.3.3 Chabauty conditions

We finish this section with the promised discussion on the Chabauty condition.

We retain all notations and assumptions from the previous sections, in particular Assumption 3.1 on the prime p. From Section 3.3.2, we know that, for each prime $\mathfrak{p}$ above p, the set $\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})$ is equipped with the structure of a p-adic manifold of dimension $(g+\rho-1)k_{\mathfrak{p}}$. Therefore, $\mathbf{T}(\mathcal{O}_{K,p})$ is a (locally analytic) p-adic manifold of dimension

$$(g+\rho-1)\sum_{\mathfrak{p}|p} k_{\mathfrak{p}} = (g+\rho-1)d.$$

Now, by Theorem 3.2 and Corollary 3.1, the p-adic manifold $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^{p}$ is parametrised by $\mathbb{Z}_p^{\delta(\rho-1)+r}$ via the map

$$\mathbb{Z}_p^{\delta(\rho-1)+r} \xrightarrow{\kappa} \mathbf{Y}_t \hookrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t \xrightarrow{\sim} \mathbb{Z}_p^{(g+\rho-1)d},$$

which is is given by a $(g+\rho-1)d$-tuple of elements in $R = \mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$. Therefore, the dimension of the p-adic manifold $\mathbf{Y}_t$ is at most

$$\dim \mathbf{Y}_t \leq \delta(\rho-1) + r.$$

Finally, we observe that $\mathbf{U}(\mathcal{O}_{K,p})$ has dimension d as a p-adic manifold.

Now back to the original goal. A necessary condition for the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$ in (3.21) to be finite is the following inequality on dimensions of p-adic manifolds:

$$\operatorname{codim} \mathbf{U}(\mathcal{O}_{K,p}) + \operatorname{codim} \mathbf{Y}_t \geq \dim \mathbf{T}(\mathcal{O}_{K,p})$$

where the codimensions are taken with respect to the ambient manifold $\mathbf{T}(\mathcal{O}_{K,p})$. By the discussion above, this is equivalent to requiring

$$\delta(\rho - 1) + r \leq (g + \rho - 2)d,$$

which in turn is equivalent to the condition

$$r \leq (g-1)d + (\rho - 1)(r_2 + 1). \tag{3.24}$$

Definition 3.8. We say that a smooth, projective and geometrically connected curve C_K of genus $g \geq 2$ over a number field K satisfies the geometric quadratic Chabauty condition if the inequality (3.24) holds.

Remark 3.7. The term "geometric" distinguishes condition (3.24) from the other Chabauty type conditions associated to the various methods discussed in Sections 0.3 and 0.4.2. We briefly compare these conditions:

- When $K = \mathbb{Q}$, the condition (3.24) becomes

  $$r \leq g + \rho - 2,$$

  which is the same condition as in the geometric quadratic Chabauty method over $\mathbb{Q}$ of Edixhoven and Lido [62].

- In [138], Siksek extended the classic Chabauty–Coleman method to arbitrary number fields using Weil restrictions; this is the Restriction of Scalars (RoS) Chabauty method. The method is expected to be successful when

$$r \leq (g-1)d. \tag{3.25}$$

Hence the geometric quadratic Chabauty method is expected to go beyond the RoS Chabauty method.

- In their recent work [4], Balakrishnan, Besser, Bianchi and Müller extended the method of quadratic Chabauty to number fields in the case of hyperelliptic or bielliptic curves. In Section 0.4.2, we referred to this method as the RoS quadratic Chabauty method. It performs under the relaxed condition (compared to (3.25))

  $$r \leq (g-1)d + r_2 + 1.$$

  The geometric Chabauty condition (3.24) agrees with this when ρ is equal to 2, and in fact generalises this bound for $\rho \geq 2$.

- In his recent work [60], Dogra proved that, under an extra condition on J_K and K, a certain "arithmetic quadratic Chabauty condition" implies that the quadratic set $C_K(K \otimes \mathbb{Q}_p)_2$ appearing in the method of Chabauty–Kim of Section 0.4.2 is finite. If one assumes the finiteness of the p-primary part of the Shafarevich–Tate group for J_K, then the aforementioned Chabauty condition of Dogra agrees with the geometric condition (3.24). See [60, Proposition 1.1 & Remark 1.3] for more details.

3.4 The parametrisation of $\mathbf{Y}_t$

We maintain the notations of Section 3.3. The goal of this section is to prove Theorem 3.2, in other words, to describe the p-adic closure $\mathbf{Y}_t$ of $\mathbf{T}(\mathcal{O}_K)_t$ inside $\mathbf{T}(\mathcal{O}_{K,p})_t$.

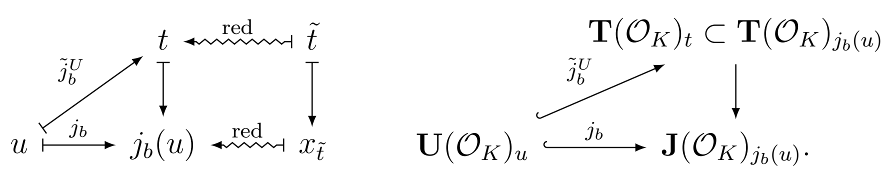
3.4.1 Construction of the map E'

In this subsection we construct the map E' of Proposition 3.4.

Notation 3.4. We begin by introducing some notation.

- Fix a basis $x_1, \ldots, x_r$ of $\mathbf{J}(\mathcal{O}_K)_0 = \ker\big(\mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\overline{\mathcal{O}_{K,p}})\big)$. Recall that u is a fixed $\overline{\mathcal{O}_{K,p}}$-point of $\mathbf{U}$ and $t = \tilde{j}_b^U(u)$.
- Denote by $\tilde{t}$ any lift of t to an $\mathcal{O}_K$-point of the torsor $\mathbf{T}$ (assumed to exist, otherwise $\mathbf{U}(\mathcal{O}_K)_u = \emptyset$ and we are done) and by $x_{\tilde{t}}$ its image in $\mathbf{J}(\mathcal{O}_K)$.
- Let $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ be the set of points of $\mathbf{T}(\mathcal{O}_K)$ whose image in $\mathbf{J}(\overline{\mathcal{O}_{K,p}})$ is $j_b(u)$.

For the reader's convenience, we remark that the points defined above and the set $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ fit in the following diagrams



Construction of the map D

The first step is the construction of a map

$$D : \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^r \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$$

in terms of the biextension laws. This is similar to the construction in [62, §4]. We carry out this step in detail and point out differences compared to [62] along the way. As a starting point, let us choose points $P_{i,j}, R_i, S_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_K)$ lifting the following points of

$\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}(\mathcal{O}_K)$:

$$\begin{aligned} P_{i,j} &\longmapsto \Big(x_i,\, \underline{f}(hmx_j)\Big) = \Big(x_i,\, hm\underline{f}(x_j)\Big), \\ R_i &\longmapsto \Big(x_i,\, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})\Big), \\ S_j &\longmapsto \Big(x_{\tilde{t}},\, \underline{f}(hmx_j)\Big) = \Big(x_{\tilde{t}},\, hm\underline{f}(x_j)\Big). \end{aligned}$$

Here $\underline{f}$ is given by the functions f_i from Notation 3.1. Note that the points to be lifted are of the form $(*, h\cdot *)$, thus the existence of such lifts is guaranteed by Lemma 3.1. Also note that unlike the situation of [62], these lifts are no longer defined up to a finite choice as they are now parametrised by $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$.

Given $\underline{n} \in \mathbb{Z}^r$, set

$$A(\underline{n}) = \sum\nolimits_{2,j} n_j \cdot_2 S_j, \quad B(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 R_i, \quad C(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 \Big(\sum\nolimits_{2,j} n_j \cdot_2 P_{i,j}\Big)$$

(here $\cdot_1$ and $\cdot_2$ denote the iteration of the operation $+_1$ and $+_2$, respectively, and similarly for $\sum_1$ and $\sum_2$), so that

$$\begin{aligned} A(\underline{n}) &\longmapsto \Big(x_{\tilde{t}},\, \sum_i n_i \underline{f}(hmx_i)\Big) = \Big(x_{\tilde{t}},\, hm\underline{f}\big(\sum_i n_i x_i\big)\Big), \\ B(\underline{n}) &\longmapsto \Big(\sum_i n_i x_i,\, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})\Big), \\ C(\underline{n}) &\longmapsto \Big(\sum_i n_i x_i,\, \sum_i n_i \underline{f}(hmx_i)\Big) = \Big(\sum_i n_i x_i,\, hm\underline{f}\big(\sum_i n_i x_i\big)\Big). \end{aligned}$$

Next, set

$$D(\underline{n}) = \big(C(\underline{n}) +_2 B(\underline{n})\big) +_1 \big(A(\underline{n}) +_2 \tilde{t}\big).$$

Thus $D(\underline{n})$ is a point lying over the point

$$(x_{\underline{n}}, \alpha(x_{\underline{n}})) := \left(x_{\tilde{t}} + \sum_i n_i x_i,\, \big(hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f}\big)\left(x_{\tilde{t}} + \sum_i n_i x_i\right)\right)$$

in $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}(\mathcal{O}_K)$. To see this, note that the point $\tilde{t} \in \mathbf{T}(\mathcal{O}_K)$, when viewed as an point in $\mathbf{P}^{\times,\rho-1}$, lies over the point

$$(x_{\tilde{t}}, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})).$$

Construction of the map E

The next step is inspired by a similar construction in [62, §4], though we have to use the $\mathbb{G}_m$ action on the Poincaré torsor in a more crucial way. This is one of the main technical innovations of this work (compared to [62]). The aim is to extend the map

$$D : \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^r \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$$

to a map

$$E : \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)$$

by including the $\mathbb{G}_m^{\rho-1}$-action on fibres, that is, by the formula

$$E(\zeta, \underline{n}) = \zeta \cdot D(\underline{n}), \quad \forall \zeta \in \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1}$$

. Here the subscript tf stands for "torsion-free quotient" as before. It will be, however, important later on that this expression admits a description in terms of $+_1$, $+_2$ and their iterates $\cdot_1, \cdot_2$. To make this explicit, we describe this construction as follows.

Notation 3.5. We define the following notation.

- We fix a free basis $u_1, \ldots, u_\delta$ of $\mathcal{O}_{K,\mathrm{tf}}^\times = \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}$, viewed as a subgroup of $\mathcal{O}_K^\times$ via an (arbitrary) splitting.

- For each $(\rho-1)$-tuple $u_{k,l} = (1, \ldots, 1, u_k, 1, \ldots, 1) \in \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$ where u_k sits at the l-th spot, we denote the corresponding elements in $\mathbf{P}^\times_{|\mathbf{J}\times 0}(\mathcal{O}_K)$ above the point $(x_{\tilde{t}}, 0)$ by $V_{k,l}$ (in the sense of Formula (3.9) but with $\mathbf{P}^\times$ in place of $P_K^\times$), and likewise denote the corresponding element above $(x_i, 0)$ by $W_{k,l,i}$.

Definition 3.9. For $\underline{n} \in \mathbb{Z}^r$, $k \in \{1, \ldots, \delta\}$ and $l \in \{1, \ldots, \rho - 1\}$, we define

$$U_{k,l}(\underline{n}) := V_{k,l} +_1 \sum_{1,i} n_i \cdot_1 W_{k,l,i},$$

so that $U_{k,l}(\underline{n})$ is the element representing multiplication by $u_{k,l}$ and lying above the point

$$(x_{\tilde{t}} + \sum_i n_i x_i, 0).$$

Finally, for a $(\rho - 1)$-tuple of δ-tuples of integers $\underline{m} = (m_{k,l})_{\substack{1 \le k \le \delta \\ 1 \le l \le \rho - 1}} \in \mathbb{Z}^{\delta(\rho-1)}$, the map E is defined by the formula

$$E(\underline{m}, \underline{n}) = \left(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U_{k,l}(\underline{n}) \right) +_2 D(\underline{n}).$$

In particular, $E(\underline{m}, \underline{n})$ defines a point in $\mathbf{T}(\mathcal{O}_K)$.

One easily checks that $E(\underline{m}, \underline{n})$ lies over the same point

$$\big(x_{\underline{n}}, \alpha(x_{\underline{n}})\big) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$$

as $D(\underline{n})$ does. After all, the parameters $\underline{m}$ just encode part of the $\mathbb{G}_m^{\rho-1}$-action on the fibres as was previously indicated. Passing from $\mathcal{O}_K$ to $\overline{\mathcal{O}_{K,p}}$, the contribution of the x_i's vanishes and the point becomes

$$(j_b(u), (hm \cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(j_b(u))).$$

In other words, we have

$$E(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_K)_{j_b(u)}.$$

Proposition 3.5. *The map*

$$\mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1} \times \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$$
$$(\varepsilon, \underline{m}, \underline{n}) \longmapsto \varepsilon \cdot E(\underline{m}, \underline{n})$$

(where the subscript tors *stands for "torsion part") is bijective.*

Proof. This is immediate after tracking the definitions. As $\underline{n} \in \mathbb{Z}^r$ varies, $x_{\underline{n}} = x_{\tilde{t}} + \sum_i n_i x_i$ runs over all the points of $\mathbf{J}(\mathcal{O}_K)$ that reduce to $j_b(u)$, and $D(\underline{n})$ provides a single point in $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ lying above $x_{\underline{n}}$ (in particular, $\underline{n} \mapsto D(\underline{n})$ is injective). To get all the points of $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$, one needs to move these around by the (simply transitive) $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$-action. Since $E(\underline{m}, \underline{n}) = \zeta(\underline{m}) \cdot D(\underline{n})$ accounts for the torsion-free part of the action by the discussion above, what is left is the torsion part, hence the factor $\mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1}$. □

Construction of the map E'

For the purpose of computing rational points, we wish to parametrise $\mathbf{T}(\mathcal{O}_K)_t$ instead of all of $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$. In this subsection, we modify the map E to obtain a map E' that additionally lands in the correct residue disk, i.e., so that $E'(\underline{m}, \underline{n})$ reduces to t in $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$ for all $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$. The starting point is the following observation, which asserts that this is already satisfied by E on a certain finite-index subgroup of $\mathbb{Z}^{\delta(\rho-1)+r}$.

Proposition 3.6. *Let q^* be the exponent of $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, that is, the least common multiple of $q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$ for $i = 1, 2, \ldots, s$. Then*

$$E(q^*\underline{m}, q^*\underline{n}) \in \mathbf{T}(\mathcal{O}_K)_t, \qquad \forall (\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}.$$

Proof. We need to show that $E(q^*\underline{m}, q^*\underline{n})$ reduces to the point t in $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$. To that end, we consider the elements

$$A(q^*\underline{n}), \qquad B(q^*\underline{n}), \qquad C(q^*\underline{n}), \qquad U_{k,l}(q^*\underline{n})$$

lying in the fibres of the $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$-torsor $\mathbf{P}^{\times,\rho-1}(\overline{\mathcal{O}_{K,p}})$ above the points

$$(j_b(u),0), \qquad (0,(hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(j_b(u))), \qquad (0,0), \qquad (j_b(u),0),$$

respectively. The $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$-torsors obtained from $\mathbf{P}^{\times,\rho-1}$ by taking the fibres over each of these points in $\mathbf{J}\times\mathbf{J}^{\vee,\circ}(\overline{\mathcal{O}_{K,p}})$ are all trivial since at least one coordinate is zero in each case. See Section 3.1.1. That is, they are groups isomorphic to $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$ whose group operation is given by $+_2$ in the cases of A and the $U_{k,l}$'s, by $+_1$ in the case of B, and by either of the two operations in the case of C (since $+_1$ and $+_2$ agree above the point $(0,0)$). By linearity of their definitions, we obtain

$$A(q^*\underline{n}) = q^* \cdot_2 A(\underline{n}) = 1, \qquad B(q^*\underline{n}) = q^* \cdot_1 B(\underline{n}) = 1, \qquad U_{k,l}(q^*\underline{n}) = q^* \cdot_2 U_{k,l}(\underline{n}) = 1$$

as elements of $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$. Finally, for C we have

$$C(q^*\underline{n}) = q^* \cdot_1 \left(\sum\nolimits_{1,i} n_i \cdot_1 \left(\sum\nolimits_{2,j} q^* n_j \cdot_2 P_{i,j}\right)\right) = 1.$$

Putting these together, we obtain

$$D(q^*\underline{n}) = (1 +_2 1) +_1 (1 +_2 t) = t$$

(note the clash of additive and multiplicative notations). Therefore, we have

$$E(q^*\underline{m}, q^*\underline{n}) = q^* \cdot_2 \left(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U_{k,l}(q^*\underline{n})\right) +_2 D(q^*\underline{n}) = 1 +_2 t = t\ .$$

This verifies the claim. □

In fact, to get the desired map $\mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)_t$, which agrees with E on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, is strictly speaking not possible. However, we can still obtain a map E' on the entire group $\mathbb{Z}^{\delta(\rho-1)+r}$ that agrees with E on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$ at the cost of allowing

p-adic coefficient. We prove the following more precise version of Proposition 3.4.

Proposition 3.7. *There exists a map*

$$E' = E'(\underline{m}, \underline{n}) : \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$$

with the following properties:

1. *$E'(\underline{m}, \underline{n})$ can be described using the partial group laws $+_1$, $+_2$ of $P^{\times,\rho-1}(\mathcal{O}_{K,p})$, and its iterates $\cdot_1, \cdot_2$, after a choice of finitely many points; more precisely, it is built from analogous terms $A'(\underline{n}), B'(\underline{n}), C'(\underline{n})$ and $U'_{k,l}(\underline{n})$ as in the description of $E(\underline{m}, \underline{n})$.*

2. *For each $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$, there is a unique $(\rho-1)$-tuple of roots of unity of prime-to-p orders $\xi(\underline{m}, \underline{n}) \in \mathcal{O}_{K,p}^{\times,\rho-1}$ such that $\xi(\underline{m}, \underline{n}) \cdot E(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_{K,p})_t$, and we additionally have*

$$E'(\underline{m}, \underline{n}) = \xi(\underline{m}, \underline{n}) \cdot E(\underline{m}, \underline{n}).$$

Proof. Note that there is a unique multiplicative lift of units

$$\iota : \overline{\mathcal{O}_{K,p}}^{\times} = \mathbb{F}_{\mathfrak{p}_1}^{\times} \times \cdots \times \mathbb{F}_{\mathfrak{p}_s}^{\times} \hookrightarrow \mathcal{O}_{K,\mathfrak{p}_1}^{\times} \times \cdots \times \mathcal{O}_{K,\mathfrak{p}_s}^{\times} = \mathcal{O}_{K,p}^{\times}$$

right inverse to the reduction map, mapping precisely onto the prime-to-p part of the roots of unity in $\mathcal{O}_{K,p}$. Denote also by ι the induced map $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}) \longrightarrow \mathbb{G}_m^{\rho-1}(\mathcal{O}_{K,p})$.

Since the action of $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ on $\mathbf{T}(\overline{\mathcal{O}_{K,p}})_{j_b(u)}$(= fibre of $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$ containing t) is simply transitive, it follows that each $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-orbit of $\mathbf{T}(\mathcal{O}_{K,p})_{j_b(u)}$ contains a unique point from $\mathbf{T}(\mathcal{O}_{K,p})_t$. This shows the existence and uniqueness of $\xi(\underline{m}, \underline{n})$ in (2) by considering the point $E(\underline{m}, \underline{n})$ viewed inside $\mathbf{T}(\mathcal{O}_{K,p})_{j_b(u)}$ via the canonical map $\mathbf{T}(\mathcal{O}_K) \hookrightarrow \mathbf{T}(\mathcal{O}_{K,p})$.

The strategy for defining E' is to modify the choices of the initial points in the construction of E. Note that the images $\overline{P_{i,j}}, \overline{R_i}, \overline{S_j}$ in $\mathbf{P}^{\times,\rho-1}(\overline{\mathcal{O}_{K,p}})$ lie over points of the form $(0,*), (0,*)$ and $(*,0)$ respectively. The fibres over these points are canonically isomorphic to $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}) = \overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$ by the discussion in Section 3.1.1. Thus, the neutral element 1 in these fibres makes sense, and, for example, there is a unique $\xi_{i,j} \in \mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ such that $\xi_{i,j}\overline{P_{i,j}} = 1$; then we set $P'_{i,j} = \iota(\xi_{i,j})P_{i,j}$. One obtains the points $R'_i, S'_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$ in a similar fashion. Likewise, we modify the points $V_{k,l}$ and $W_{k,l,i}$ in the same fashion. (Alternatively, one can multiply the chosen basis of the torsion-free part of $\mathcal{O}_K$-units $u_1, \ldots, u_\delta$ by suitable roots of unity (of prime-to-p order) in $\mathcal{O}_{K,p}$ so that the resulting units are congruent to 1 mod $p\mathcal{O}_{K,p}$).

Using these points, one can define the terms $A'(\underline{n}), B'(\underline{n}), C'(\underline{n})$, etc. as in the definition of $E(\underline{m}, \underline{n})$. Denote by $E'(\underline{m}, \underline{n})$ the result of this process. A formal computation similar to the proof of Proposition 3.6 then shows that $E'(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_{K,p})_t$ for all $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$. This proves (1).

Finally, since $E'(\underline{m}, \underline{n})$ was obtained by the same operations in terms of $+_1, +_2, \cdot_1$, and $\cdot_2$ as $E(\underline{m}, \underline{n})$ apart from the $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification of the initial points, it follows from (an analogue of) (3.10) that $E'(\underline{m}, \underline{n})$ also differs from $E(\underline{m}, \underline{n})$ only by $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification, that is, $E'(\underline{m}, \underline{n}) = \xi(\underline{m}, \underline{n})E(\underline{m}, \underline{n})$ for some $\xi(\underline{m}, \underline{n}) \in \iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$. Using the uniqueness part of (2), this proves the indicated equality in (2). □

It remains to prove the following result.

Proposition 3.8. *We have:*

1. *The following inclusions*

$$\mathbf{T}(\mathcal{O}_K)_t \subseteq E'(\mathbb{Z}^{\delta(\rho-1)+r}) \subseteq \mathbf{T}(\mathcal{O}_{K,p})_t$$

   where $\mathbf{T}(\mathcal{O}_K)$ is viewed as a subset of $\mathbf{T}(\mathcal{O}_{K,p})$ via the canonical map.

2. *The equality $\xi(q^*\mathbb{Z}^{\delta(\rho-1)+r}) = 1$; that is, E and E' agree on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$.*

Proof. Part (2) follows directly from Propositions 3.6 and 3.7 (2). Let us prove (1). Given $Q \in \mathbf{T}(\mathcal{O}_K)_t \subseteq \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$, by Proposition 3.5, there is a unique $\varepsilon \in \mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1}$ and a unique

$(\underline{m},\underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$ such that $\varepsilon E(\underline{m},\underline{n}) = Q$. Using the fact that $\mathcal{O}_{K,\mathrm{tors}}^{\times}$ embeds, into the prime-to-p part of $\mathcal{O}_{K,p,\mathrm{tors}}^{\times}$, since by Assumption 3.1 the prime p does not divide $|\mathcal{O}_{K,\mathrm{tors}}^{\times}|$, it follows that ε may be treated as a uniquely determined element of $\mathcal{O}_{K,p}^{\times,\rho-1}$ whose order is finite and coprime to p. By the uniqueness part of Proposition 3.7, we have $\varepsilon = \xi(\underline{m},\underline{n})$, so that

$$Q = \varepsilon E(\underline{m},\underline{n}) = \xi(\underline{m},\underline{n})E(\underline{m},\underline{n}) = E'(\underline{m},\underline{n}).$$

□

To summarise, we have constructed the promised map

$$E' : \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t.$$

It is described in terms of the operations $+_1, +_2$ and its iterates $\cdot_1, \cdot_2$ on $\mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$, and agrees with E on $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, with the property (anticipated in (3.23)):

$$E'(q^*\mathbb{Z}^{\delta(\rho-1)+r}) \subseteq \mathbf{T}(\mathcal{O}_K)_t \subseteq E'(\mathbb{Z}^{\delta(\rho-1)+r}).$$

3.4.2 The p-adic interpolation

The remaining part of this section aims to prove Theorem 3.2. This is done along the same lines as [62, §3, §5.1], in a slightly more general context. We will use the following result (whose proof will be given shortly) to deduce Theorem 3.2.

Proposition 3.9. *The following statements hold:*

1. *Let X, Y be smooth schemes over $\mathcal{O}_K$ of relative dimensions m and n respectively. Let $f : X \longrightarrow Y$ be a morphism of $\mathcal{O}_K$-schemes and let $x \in X(\overline{\mathcal{O}_{K,p}})$ be a point. Then there are bijections $X(\mathcal{O}_{K,p})_x \simeq \mathbb{Z}_p^{dm}, Y(\mathcal{O}_{K,p})_{f(x)} \simeq \mathbb{Z}_p^{dn}$ (given by local parameters followed by restriction of scalars) such that the induced map $f : X(\mathcal{O}_{K,p})_x \longrightarrow Y(\mathcal{O}_{K,p})_{f(x)}$ is given by convergent power series with $\mathbb{Z}_p$-coefficients.*

2. *Let $G \longrightarrow Y$ be a smooth group scheme with identity section e, where Y is smooth over $\mathcal{O}_K$. Let $y \in Y(\overline{\mathcal{O}_{K,p}})$ be a point. Then the map*

$$\mathbb{Z} \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow G(\mathcal{O}_{K,p})_{e(y)}, \qquad (z, g) \mapsto z \cdot g,$$

extends to a map $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow G(\mathcal{O}_{K,p})_{e(y)}$, describing the $\mathbb{Z}_p$-module action on fibres over $Y(\mathcal{O}_{K,p})_y$, and this map is given by convergent power series with $\mathbb{Z}_p$-coefficients.

Remark 3.8. We postpone the proof of this result to the end of this section. The proof of (1) relies on the description of local parameters at a point x using blow-ups. The proof of (2) uses the formal logarithm and exponential maps to interpret the action $z \cdot g$ as $\exp(z \cdot \log(g))$. Since exp and log are given by convergent power series by Proposition 3.11, one can extend $z \cdot g$ to allow $\mathbb{Z}_p$-coefficients. The proofs are technical and quite general. For the sake of clarity and readability, we have chosen to defer them to after the proof of Theorem 3.2.

Proof of Theorem 3.2. By Proposition 3.7 and Definition 3.9, for all $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)} \times \mathbb{Z}^r$,

$$E'(\underline{m}, \underline{n}) = \left(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U'_{k,l}(\underline{n})\right) +_2 \left(\left(C'(\underline{n}) +_2 B'(\underline{n})\right) +_1 \left(A'(\underline{n}) +_2 \tilde{t}\right)\right), \tag{3.26}$$

where

$$A'(\underline{n}) = \sum\nolimits_{2,j} n_j \cdot_2 S'_j, \quad B'(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 R'_i, \quad C'(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 \left(\sum\nolimits_{2,j} n_j \cdot_2 P'_{i,j}\right),$$

and

$$U'_{k,l}(\underline{n}) := V'_{k,l} +_1 \sum_{1,i} n_i \cdot_1 W'_{k,l,i}.$$

The points $S'_j, R'_i, P'_{i,j} \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$, as well as $V'_{k,l}, W'_{k,l,i} \in \mathbf{P}^{\times}(\mathcal{O}_{K,p})$, are defined in the course of the proof of Proposition 3.7.

The point is that the map E' is built (after the choice of finitely many points) from the operations $+_1$ and $+_2$, and their iterates $\cdot_1$ and $\cdot_2$.

Proposition 3.9 (2) applied respectively to the group schemes $\mathbf{P}^\times \longrightarrow \mathbf{J}^{\vee,\circ}$ and $\mathbf{P}^\times \longrightarrow \mathbf{J}$, implies that the operations $(n, g) \mapsto n \cdot_1 g$ and $(n, g) \mapsto n \cdot_2 g$ for $n \in \mathbb{Z}$ extend to $n \in \mathbb{Z}_p$, and the resulting operations are given by convergent power series with $\mathbb{Z}_p$-coefficients. Hence, formula (3.26) makes sense with $(\underline{m}, \underline{n}) \in \mathbb{Z}_p^{\delta(\rho-1)} \times \mathbb{Z}_p^r$; allowing for $\mathbb{Z}_p$ coefficients using the extended actions $\cdot_1$ and $\cdot_2$ thus gives rise via formula (3.26) to the desired map

$$\kappa : \mathbb{Z}_p^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t,$$

which by definition agrees with E' when restricted to $\mathbb{Z}^{\delta(\rho-1)+r} \subset \mathbb{Z}_p^{\delta(\rho-1)+r}$.

By Proposition 3.9 (1), both the operations

$$+_1 : \mathbf{P}^{\times,\rho-1} \times_{(\mathbf{J}^{\vee,\circ})^{\rho-1}} \mathbf{P}^{\times,\rho-1} \longrightarrow \mathbf{P}^{\times,\rho-1},$$
$$+_2 : \mathbf{P}^{\times,\rho-1} \times_{\mathbf{J}} \mathbf{P}^{\times,\rho-1} \longrightarrow \mathbf{P}^{\times,\rho-1}$$

induce maps given by convergent power series over $\mathbb{Z}_p$ on the appropriate residue disks (after choosing a regular system of parameters inducing $\mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})_x \simeq \mathbb{Z}_p^{d(g+g(\rho-1)+\rho-1)}$ upon restricting scalars from $\mathcal{O}_{K,p}$ to $\mathbb{Z}_p$).

Since the composition of convergent power series with $\mathbb{Z}_p$-coefficients produces again convergent power series with $\mathbb{Z}_p$-coefficients, the map κ is indeed given by a tuple of convergent p-adic power series. $\square$

Local parameters and blow-ups

Notation 3.6. We fix a prime $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ above p. Denote by π a uniformizer of $\mathcal{O}_{K,\mathfrak{p}}$. Let X be a smooth scheme over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension m. Similarly as before, for a point $x \in X(\mathbb{F}_\mathfrak{p})$, denote by $X(\mathcal{O}_{K,\mathfrak{p}})_x$ the set of all $\mathcal{O}_{K,\mathfrak{p}}$-points reducing to x modulo $\mathfrak{p}$. By smoothness, the maximal ideal $\mathfrak{m}_x$ admits a regular system of parameters $(\pi, t_1, t_2, \ldots, t_m)$.

The point x factors through the natural map $\operatorname{Spec} \widehat{\mathcal{O}_{X,x}} \longrightarrow X$, and $X(\mathcal{O}_{K,\mathfrak{p}})_x$ bijectively corresponds to Spec $\widehat{\mathcal{O}_{X,x}}(\mathcal{O}_{K,\mathfrak{p}})_x$. The isomorphism $\mathcal{O}_K[[t_1,\ldots,t_m]] \simeq \widehat{\mathcal{O}_{X,x}}$ then shows that there is a bijection of sets

$$\begin{aligned} t = (t_1, t_2, \ldots, t_m) : X(\mathcal{O}_{K,\mathfrak{p}})_x &\xrightarrow{\sim} (\mathfrak{m}_{K,\mathfrak{p}})^m \\ \tilde{x} &\longmapsto (t_1(\tilde{x}), \ldots, t_m(\tilde{x})) \end{aligned}$$

and after dividing by π, one gets

$$\tilde{t} = \left(\frac{t_1}{\pi}, \frac{t_2}{\pi}, \ldots, \frac{t_m}{\pi}\right) : X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{\sim} (\mathcal{O}_{K,\mathfrak{p}})^m\ . \tag{3.27}$$

Now let $f : X \longrightarrow Y$ be a morphism of schemes that are smooth over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimensions m and n, respectively. Denote the analogous choice of a regular system of parameters at Y by $s_1, s_2, \ldots, s_n$ and the corresponding bijection by

$$\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)} \longrightarrow (\mathcal{O}_{K,\mathfrak{p}})^n.$$

The immediate goal is the following.

Proposition 3.10. *In the above setting, the composition*

$$f' : (\mathcal{O}_{K,\mathfrak{p}})^m \xrightarrow{\tilde{t}^{-1}} X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{f} Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)} \xrightarrow{\tilde{s}} (\mathcal{O}_{K,\mathfrak{p}})^n$$

is given by a n-tuple of convergent power series with coefficients in $\mathcal{O}_{K,\mathfrak{p}}$.

(Here by convergent power series we mean elements of $\mathcal{O}_{K,\mathfrak{p}}\langle X_1, X_2, \ldots, X_m\rangle$, the p-adic, or equivalently π-adic, completion of $\mathcal{O}_{K,\mathfrak{p}}[X_1, X_2, \ldots, X_m]$). To show this, we follow closely [62, §3] and investigate the geometry of the situation.

Proof. By shrinking X to a sufficiently small affine open neighbourhood of x, we may assume that $t_1, t_2, \ldots, t_m$ are regular global functions, defining an étale map

$$t = (t_1, t_2, \ldots, t_m) : X \longrightarrow \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} = \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}[X_1, \ldots, X_m],$$

mapping x to the origin (over $\mathbb{F}_\mathfrak{p}$, i.e., the point corresponding to $(\pi, X_1, \ldots, X_d)$). By possibly shrinking X further we may assume that x is in fact the only preimage of the origin.

Note that a point $\tilde{x} : \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}} \longrightarrow X$ reduces to x if and only if the pullback of x along $\tilde{x}$ is the (effective Cartier) divisor cut out by π. Consequently, the universal property of the blowup $\mathrm{Bl}_x X$ of X at x implies that every $\tilde{x} \in X(\mathcal{O}_{K,\mathfrak{p}})_x$ factors uniquely through $\mathrm{Bl}_x X$, more precisely through the open subscheme $\mathrm{Bl}_x^{(\pi)} X$ of $\mathrm{Bl}_x X$ where π is the generator of the exceptional divisor. Thus, we have a natural identification between $X(\mathcal{O}_{K,\mathfrak{p}})_x$ and $\mathrm{Bl}_x^{(\pi)} X(\mathcal{O}_{K,\mathfrak{p}})$.

Up to this identification, the map $\tilde{t}$ can be described as follows. We consider the analogous construction for the $\mathbb{F}_\mathfrak{p}$-origin $o : \operatorname{Spec} \mathbb{F}_\mathfrak{p} \longrightarrow \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ to get $\mathrm{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ and

$$\mathrm{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} = \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}[\tilde{X}_1, \ldots, \tilde{X}_m],$$

where $\tilde{X}_i = X_i/\pi$ in the expression above. Since blowing up commutes with flat base change, we obtain a cartesian diagram of schemes

$$\begin{array}{ccccc}
\mathrm{Bl}_x^{(\pi)} X & \hookrightarrow & \mathrm{Bl}_x X & \longrightarrow & X \\
\downarrow \tilde{t} & \square & \downarrow & \square & \downarrow t \\
\mathrm{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \hookrightarrow & \mathrm{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \longrightarrow & \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} .
\end{array} \tag{3.28}$$

The map $\tilde{t}$ from (3.27) is just the morphism $\tilde{t}$ in the above diagram evaluated at $\mathcal{O}_{K,\mathfrak{p}}$-points (thus, in particular, the notations are compatible).

The map $\tilde{t}_{\mathbb{F}_\mathfrak{p}}$, obtained from base-changing the diagram (3.28) to $\mathbb{F}_\mathfrak{p}$, can be (non-canonically) interpreted as the tangent map at x between the respective tangent spaces.

In particular, it is an isomorphism. Since $\tilde{t}$ is étale, $\tilde{t}$ is an isomorphism when base-changed to $\mathcal{O}_{K,\mathfrak{p}}/(\pi^j)$ for every j. Denoting the rings of global functions of the (affine) schemes in question by $\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$ and $\mathcal{O}(\mathrm{Bl}_o^{(\pi)}\mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}})$ respectively, we infer that their π-adic (equivalently, p-adic) completions are the same, that is,

$$\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)} \simeq \widehat{\mathcal{O}(\mathrm{Bl}_o^{(\pi)}\mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}})} = \mathcal{O}_{K,\mathfrak{p}}\widehat{[\tilde{X}_1,\dots,\tilde{X}_m]} = \mathcal{O}_{K,\mathfrak{p}}\langle\tilde{X}_1,\dots,\tilde{X}_m\rangle, \tag{3.29}$$

namely the algebra of integral formal power series converging on the unit disk.

Finally, we perform the same analysis for Y, $f(x)$ and its fixed system of parameters s_i. Using again the universal property of the blowup of Y at $f(x)$, we obtain that f also induces a morphism

$$\tilde{f} : \mathrm{Bl}_x^{(\pi)}X \longrightarrow \mathrm{Bl}_{f(x)}^{(\pi)}Y$$

which on the level of $\mathcal{O}_{K,\mathfrak{p}}$-points may be identified with $f : X(\mathcal{O}_{K,\mathfrak{p}})_x \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)}$. Taking the p-adic completion of the associated ring map $\mathcal{O}(\mathrm{Bl}_{f(x)}^{(\pi)}Y) \longrightarrow \mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$ and conjugating by the isomorphisms (3.29) for X and Y then yields a map

$$\mathcal{O}_{K,\mathfrak{p}}\langle\tilde{Y}_1,\dots,\tilde{Y}_n\rangle \longrightarrow \mathcal{O}_{K,\mathfrak{p}}\langle\tilde{X}_1,\dots,\tilde{X}_m\rangle.$$

This is described by specifying n-tuple of elements of $\mathcal{O}_{K,\mathfrak{p}}\langle\tilde{X}_1,\dots,\tilde{X}_m\rangle$ as images of the variables $\tilde{Y}_i$. Since the map f' is obtained from the above map of rings by applying the functor $\mathrm{Hom}_{\mathrm{Alg}_{\mathcal{O}_{K,\mathfrak{p}}}}(-,\mathcal{O}_{K,\mathfrak{p}})$, it follows that f' is described by these power series. This proves the claim. □

Remark 3.9. It will be useful later to note that $\mathcal{O}_{X,x}$ naturally embeds into $\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}$. The maximal ideal of $\mathcal{O}_X(X)$ corresponding to x becomes (π) in $\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$, hence is mapped to the radical in $\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}$. There is thus an induced map

$$\mathcal{O}_{X,x} \longrightarrow \widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}.$$

For injectivity: after taking completions at the maximal ideal, the map becomes

$$\mathcal{O}[[X_1, \ldots, X_m]] \hookrightarrow \mathcal{O}[[\tilde{X}_1, \ldots, \tilde{X}_m]]$$

given by $X_i \mapsto p\tilde{X}_i$, which is injective.

Remark 3.10 (Restriction of scalars)**.** It will be beneficial to replace the power series expressions with $\mathcal{O}_{K,\mathfrak{p}}$-coefficients by convergent power series with $\mathbb{Z}_p$-coefficients. To that end, we let

$$k = ef = \operatorname{rank}_{\mathbb{Z}_p} \mathcal{O}_{K,\mathfrak{p}}$$

following earlier conventions, and fix a free basis $e_1, e_2, \ldots, e_k$ of $\mathcal{O}_{K,\mathfrak{p}}$ as a $\mathbb{Z}_p$-module. Expressing everything with respect to this basis, the description of maps $\mathcal{O}_{K,\mathfrak{p}}^m \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^n$ in terms of power series gives rise to a power series description of maps $\mathbb{Z}_p^{km} \longrightarrow \mathbb{Z}_p^{kn}$. More precisely, upon the introduction of formal variables $X_{i,j}$ by the rule

$$X_i = X_{i,1}e_1 + X_{i,2}e_2 + \cdots + X_{i,k}e_k, \tag{3.30}$$

any convergent power series $f \in \mathcal{O}_{K,\mathfrak{p}}\langle X_1, X_2, \ldots X_m\rangle$ can be written as

$$f = f_1 e_1 + f_2 e_2 + \cdots + f_k e_k$$

for a unique k-tuple of power series $f_1, f_2, \ldots, f_k \in \mathbb{Z}_p\langle X_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq k\rangle$.

Remark 3.11. Keeping the notation from the proof of Proposition 3.10, the map

$$\tilde{f}_{\mathbb{F}_\mathfrak{p}} : (\mathrm{Bl}_x^{(\pi)} X)_{\mathbb{F}_\mathfrak{p}} \longrightarrow (\mathrm{Bl}_{f(x)}^{(\pi)} Y)_{\mathbb{F}_\mathfrak{p}}$$

can be, again, identified with the tangent map of $f_{\mathbb{F}_\mathfrak{p}} : X_{\mathbb{F}_\mathfrak{p}} \longrightarrow Y_{\mathbb{F}_\mathfrak{p}}$ at x. Assume that this map is injective. By a lift of a suitable $\mathbb{F}_\mathfrak{p}$-affine change of coordinates on $(\mathrm{Bl}_{f(x)}^{(\pi)} Y)_{\mathbb{F}_\mathfrak{p}}$, one can make sure that the map $(f')^\# : \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_n\rangle \longrightarrow \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \ldots, \tilde{X}_m\rangle$ is given by $\tilde{Y}_i \mapsto \tilde{X}_i$ for

$i \leq m$ and by $\tilde{Y}_i \mapsto 0$ for $i > m$. In other words, the parameters s_i, t_i may be chosen so that $f^{\#}(s_i) = t_i$ for $i \leq m$ and $s_{m+1}, \dots s_n$ generate the kernel of the map $f^{\#} : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$. In that case, $X(\mathcal{O}_{K,\mathfrak{p}})_x$ is embedded in $Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)}$ and in the chosen coordinates, equal to the vanishing locus of $\tilde{Y}_{m+1}, \dots, \tilde{Y}_n$. As in Remark 3.10, we can identify the embedding with the affine embedding $\mathbb{Z}_p^{km} \longrightarrow \mathbb{Z}_p^{kn}$, whose image is cut out by the $k(n-m)$ variables $\tilde{Y}_{i,j}$, $m < i \leq n, 1 \leq j \leq k$.

The exp-log argument

Let us now focus on a special case where $Y \longrightarrow \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ is a smooth scheme of relative dimension n and $X = G$ is a smooth commutative group scheme over Y of relative dimension m. (Thus, m from the previous discussion corresponds to $m+n$ in the situation at hand. We hope this does not cause too much confusion). Let $e : Y \longrightarrow G$ denote the identity section. We now consider a point $y \in Y(\mathbb{F}_{\mathfrak{p}})$ and the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_y$.

As in the beginning of this subsection, we may replace Y by $\operatorname{Spec} \mathcal{O}_{Y,y}$ and G by $G_{\mathcal{O}_{Y,y}}$. Let us fix a system of parameters $\pi, s_1, s_2, \dots, s_n$, inducing a bijection $\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_y \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^n$.

By [142, 05D9], there is an affine open neighborhood $\operatorname{Spec} B = U \subseteq G_{\mathcal{O}_{Y,y}}$ of $e(y)$ such that e factors through U and such that, denoting by I the kernel of the associated map $e^{\#} : B \longrightarrow \mathcal{O}_{Y,y}$, I/I^2 is a free $\mathcal{O}_{Y,y}$-module of rank m. Upon fixing a sequence $t_1, t_2, \dots, t_m \in I$ that becomes the free basis of I/I^2, the sequence $\pi, s_1, s_2, \dots, s_n, t_1, t_2, \dots, t_m$ forms a system of parameters of $G_{\mathcal{O}_{Y,y}}$ at $e(y)$, establishing a bijection $(\tilde{s}, \tilde{t}) : G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^{n+m}$.

We further consider the formal $\mathcal{O}_{Y,y}$-group $\widehat{G_{\mathcal{O}_{Y,y}}}$, the completion of $G_{\mathcal{O}_{Y,y}}$ with respect to the ideal of the identity section. In terms of the chosen coordinates, it is the formal spectrum of the I-adic completion of B, which in turn is the formal power series ring $\mathcal{O}_{Y,y}[[t_1, t_2, \dots, t_m]]$. The group operation then induces a m-dimensional commutative formal group law $F_G(\underline{U}, \underline{V}) = (F_1, \dots, F_m)(U_1, \dots, U_m, V_1, \dots, V_m)$ over $\mathcal{O}_{Y,y}$, that is, formal group in the sense of [85]. By [85, Theorem 1], over $\mathcal{O}_{Y,y} \otimes \mathbb{Q}$, there are mutually inverse isomorphisms of formal group laws

$$F_{G,\mathbb{Q}} \underset{\exp}{\overset{\log}{\rightleftarrows}} (\widehat{\mathbb{G}}_a)^m_{\mathbb{Q}}$$

(here $(\widehat{\mathbb{G}}_a)^m$ denotes the m-dimensional addition law, given by the polynomials $U_i + V_i$ treated as power series over $\mathcal{O}_{Y,y}$, and the subscript $\mathbb{Q}$ denotes the "formal base change" to $\mathbb{Q}$). Explicitly, fixing a basis of invariant differentials of F_G (in the sense of [85, Proposition 1.1]) $\omega_1, \ldots, \omega_m \in \bigoplus_{i=1}^m \mathcal{O}_{Y,y}[[t_1, \ldots, t_m]]\mathrm{d}t_i$, log is given by an m-tuple of formal power series $L_1, L_2, \ldots, L_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \ldots, t_m]]$ characterized by the property

$$L_i(0, \ldots, 0) = 0, \;\; \mathrm{d}L_i = \omega_i, \;\; i = 1, 2, \ldots, m \tag{3.31}$$

(and additionally, each L_i equals t_i in degree 1). The exponential is then given as a formal inverse to log, i.e., by a m-tuple of power series $E_1, E_2, \ldots, E_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \ldots, t_m]]$ characterized by the identities

$$E_i(L_1, L_2, \ldots, L_m) = t_i, \;\; i = 1, 2, \ldots, m \tag{3.32}$$

(and it again follows that each E_i equals t_i in degrees ≤ 1).

The fibres of the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_y$ are naturally not only abelian groups but, moreover, $\mathbb{Z}_p$-modules: given a point $\tilde{y} \in Y(\mathcal{O}_{K,\mathfrak{p}})_y$, the fibre over $\tilde{y}$ is the kernel of the reduction map $G_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}) \longrightarrow G_{\tilde{y}}(\mathbb{F}_{\mathfrak{p}})$ (where $G_{\tilde{y}}$ denotes the $\mathcal{O}_{K,\mathfrak{p}}$-group scheme obtained from G by base change along $\tilde{y}$). This kernel is the set of $\mathcal{O}_{K,\mathfrak{p}}$-points of the associated formal group, $\widehat{G_{\tilde{y}}}(\mathcal{O}_{K,\mathfrak{p}}) = \varprojlim_j \widehat{G_{\tilde{y}}}(\mathcal{O}_{K,\mathfrak{p}}/p^j\mathcal{O}_{K,\mathfrak{p}})$ (and the group law of $\widehat{G_{\tilde{y}}}$ may be viewed as the "formal base change" of the formal group law for $\widehat{G_{\mathcal{O}_{Y,y}}}$ above). The fact that any formal group law is of the form $\underline{U} + \underline{V} +$ (higher order terms) shows that $\widehat{G_{\tilde{y}}}(\mathcal{O}_{K,\mathfrak{p}}/p^j\mathcal{O}_{K,\mathfrak{p}})$ is an abelian group annihilated by p^j, verifying the claim.

The goal is to p-adically interpolate the function $z \mapsto z \cdot g$ for $g \in G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$, or more precisely, describe the action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ coming from the $\mathbb{Z}_p$-action on fibres, in terms of convergent power series.

Proposition 3.11. *The formal logarithm and exponential induce the mutually inverse maps* log *and* exp

$$G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \xrightarrow[\simeq]{(\tilde{s},\tilde{t})} (\mathcal{O}_{K,\mathfrak{p}})^{n+m} \underset{\exp}{\overset{\log}{\rightleftarrows}} (\mathcal{O}_{K,\mathfrak{p}})^{n+m}$$

given by convergent power series (elements of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_n, \tilde{X}_1, \ldots, \tilde{X}_m\rangle$). For $z \in \mathbb{Z}_p$, and $g \in G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ (viewed as an element of $(\mathcal{O}_{K,\mathfrak{p}})^{n+m}$ via $(\tilde{s},\tilde{t})$) we have $z \cdot g = \exp(z \cdot \log(g))$. Consequently, the action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ is described by convergent power series with coefficients in $\mathbb{Z}_p$.

Proof. Write $L_i = \sum_{J \neq 0} a_{i,J} \underline{t}^J$ and $E_i = \sum_{J \neq 0} b_{i,J} \underline{t}^J$ for the formal power series that are components of the formal logarithm and formal exponential, respectively. It can be deduced from the identity (3.31) that

$$|J| a_{i,J} \in \mathcal{O}_{Y,y} \text{ for all } J, \tag{3.33}$$

and a formal computation of the exponential based on the identities (3.32) as in [83, A.4.6] together with (3.33) shows that

$$(|J|!) b_{i,J} \in \mathcal{O}_{Y,y} \text{ for all } J. \tag{3.34}$$

The induced map $\log : \mathcal{O}_{K,\mathfrak{p}}^{n+m} \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^{n+m}$ is then given by the identity on the first n components (which correspond to the base $Y(\mathcal{O}_{K,\mathfrak{p}})_y$) and by the power series

$$\tilde{L}_i(\underline{\tilde{X}}) = \pi^{-1} \sum_{J \neq 0} a_{i,J} (\pi \underline{\tilde{X}})^J = \sum_{J \neq 0} \frac{\pi^{|J|-1}}{|J|} (|J| a_{i,J}) (\underline{\tilde{X}})^J, \quad i = 1, \ldots, m \tag{3.35}$$

on the remaining components. Here $|J| a_{i,J}$ is considered as an element of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_m\rangle$ in the sense of Remark 3.9.

Its formal inverse is then given by the analogous modification of the formal exponential, namely, $\exp : \mathcal{O}_{K,\mathfrak{p}}^{n+d} \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^{n+d}$ is given by the identity on the first n components and on the remaining m components by the formal power series

$$\tilde{E}_i(\underline{\tilde{X}}) = \pi^{-1}\sum_{J\neq 0} b_{i,J}(\pi\underline{\tilde{X}})^J = \sum_{J\neq 0}\frac{\pi^{|J|-1}}{|J|!}((|J|!)b_{i,J})(\underline{\tilde{X}})^J, \;\; i = 1,\dots,m \tag{3.36}$$

where $(|J|!)b_{i,J}$ is again considered as an element of $\mathcal{O}_{K,\mathfrak{p}}\langle\tilde{Y}_1.\dots,\tilde{Y}_m\rangle$.

To conclude that the power series (3.35), (3.36) define elements of the ring $\mathcal{O}_{K,\mathfrak{p}}\langle\underline{\tilde{Y}},\underline{\tilde{X}}\rangle$, it is enough to observe that the coefficients $\pi^{|J|-1}/(|J|!)$ (hence also $\pi^{|J|-1}/|J|$) are integral and converge to zero p-adically as $|J|\to\infty$. This is satisfied by the imposed condition $e < p-1$ on the ramification index in Assumption 3.1, since then the p-adic valuations are

$$v_p\left(\frac{\pi^{k-1}}{k!}\right) \geq \frac{k-1}{e} - \frac{k-1}{p-1} = \frac{(k-1)(p-1-e)}{e(p-1)},$$

which is non-negative for all $k\geq 1$ and tends to ∞ as $k\to\infty$.

Finally, we may interpret log and exp as given by $ef(n+m)$ power series with coefficients in $\mathbb{Z}_p$ as in Remark 3.10. The action map $\mathbb{Z}_p\times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}\longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ then becomes a p-adically continuous map $\mathbb{Z}_p\times\mathbb{Z}_p^{ef(n+m)}\longrightarrow\mathbb{Z}_p^{ef(n+m)}$ extending the map

$$(z,g)\mapsto z\cdot g = \exp(z\cdot\log(g))$$

from $\mathbb{Z}\times\mathbb{Z}_p^{ef(n+m)}$ to $\mathbb{Z}_p\times\mathbb{Z}_p^{ef(n+m)}$. The same is true about the map on $\mathbb{Z}_p\times\mathbb{Z}_p^{ef(n+m)}$ given by $(z,g)\mapsto\exp(z\cdot\log(g))$, so these two maps agree. In particular, the $\mathbb{Z}_p$-action map is described by convergent power series with $\mathbb{Z}_p$-coefficients as claimed. □

Proof of Proposition 3.9

Proof. As in (3.2), a point $x\in X(\overline{\mathcal{O}_{K,p}})$ is given by an s-tuple $x_1\in X(\mathbb{F}_{\mathfrak{p}_1}),\dots,x_s\in X(\mathbb{F}_{\mathfrak{p}_s})$, and we have $X(\mathcal{O}_{K,p})_x = \prod_{i=1}^s X(\mathcal{O}_{K,\mathfrak{p}_i})_{x_i}$. Similarly, for any map $f: X\longrightarrow Y$ of $\mathcal{O}_K$-schemes, the induced map $f: X(\mathcal{O}_{K,p})_x\longrightarrow Y(\mathcal{O}_{K,p})_{f(x)}$ decomposes into the product of the maps $f: X(\mathcal{O}_{K,\mathfrak{p}})_{x_i}\longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x_i)}$. Part (1) thus follows from Proposition 3.10 and

Remark 3.10.

Similarly, we have $G(\mathcal{O}_{K,p})_{e(y)} = \prod_{i=1}^{s} G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)}$, and thus, $G(\mathcal{O}_{K,p})_{e(y)}$ has $\mathbb{Z}_p$-module structure on fibres over $Y(\mathcal{O}_{K,p})_y = \prod_{i=1}^{s} Y(\mathcal{O}_{K,\mathfrak{p}_i})_{y_i}$. By Proposition 3.11, each of the action maps $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)}$ is given by convergent power series with $\mathbb{Z}_p$-coefficients. The action map for $G(\mathcal{O}_{K,p})_{e(y)}$ is then obtained by taking the product of the above action maps and precomposing with $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow \prod_i (\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)})$, where $\mathbb{Z}_p$ is embedded into the s copies of $\mathbb{Z}_p$ diagonally. It follows that the map has a description in terms of convergent power series over $\mathbb{Z}_p$ as well, proving (2). □

3.5 End of proof and questions

In this section we conclude the proof of Theorem 3.1 (or rather its more precise formulation Theorem 3.3). We formulate a precise version of Questions 3.1, and discuss expected answers.

3.5.1 Bounding the number of rational points

In this section we prove Theorem 3.3 of Section 3.3, which gives a conditional upper bound on the size of the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$. Let $\mathfrak{p}$ be a prime above p as usual. As in Notation 3.6, we choose parameters $x_1^{\mathfrak{p}}, \ldots, x_g^{\mathfrak{p}}$ for $\mathbf{J}$ at the point $x_{\mathfrak{p}} := j_b^U(u_{\mathfrak{p}})$ as well as parameters $t_1^{\mathfrak{p}}, \ldots, t_{\rho-1}^{\mathfrak{p}} \in \mathcal{O}_{\mathbf{T},t_{\mathfrak{p}}}$ such that

$$\pi_{\mathfrak{p}}, x_1^{\mathfrak{p}}, \ldots, x_g^{\mathfrak{p}}, t_1^{\mathfrak{p}}, \ldots, t_{\rho-1}^{\mathfrak{p}}$$

is a system of local parameters at $t_{\mathfrak{p}}$ for the smooth scheme $\mathbf{T}$ over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension $g+\rho-1$. We obtain the following identifications, as in (3.27):

$$\tilde{x} : \mathbf{J}(\mathcal{O}_{K,\mathfrak{p}})_{x_{\mathfrak{p}}} \simeq (\mathcal{O}_{K,\mathfrak{p}})^g$$
$$(\tilde{x}, \tilde{t}) : \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}} \simeq (\mathcal{O}_{K,\mathfrak{p}})^{g+\rho-1}.$$

Now, the tangent map of the lifted Abel–Jacobi map $\tilde{j}_b^U : \mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_\mathfrak{p}} \hookrightarrow \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_\mathfrak{p}}$ of Proposition 3.3 is injective at $\mathfrak{p}$ by smoothness. It follows, by Remark 3.11, that $\mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_\mathfrak{p}}$ is a complete intersection in $\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_\mathfrak{p}}$, i.e., it is cut out by $g + \rho - 2$ equations

$$f_1^\mathfrak{p}, \dots, f_{g+\rho-2}^\mathfrak{p} \;\in\; \mathcal{O}(\widehat{\mathrm{Bl}_{t_\mathfrak{p}}^{(\pi_\mathfrak{p})}(\mathbf{T})}) = \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{x}_1^\mathfrak{p}, \dots, \tilde{x}_g^\mathfrak{p}, \tilde{t}_1^\mathfrak{p}, \dots, \tilde{t}_{\rho-1}^\mathfrak{p} \rangle,$$

which generate the kernel of the surjection

$$(\tilde{j}_b^U)_\mathfrak{p}^\# : \mathcal{O}(\widehat{\mathrm{Bl}_{t_\mathfrak{p}}^{(\pi_\mathfrak{p})}(\mathbf{T})}) \longrightarrow \mathcal{O}(\widehat{\mathrm{Bl}_{u_\mathfrak{p}}^{(\pi_\mathfrak{p})}(\mathbf{U})}).$$

As before let $k_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$ be the $\mathbb{Z}_p$-rank of $\mathcal{O}_{K,\mathfrak{p}}$. Following Remark 3.10, upon choosing a $\mathbb{Z}_p$-basis of $\mathcal{O}_{K,\mathfrak{p}}$ and introducing new variables $\tilde{x}_{i,j}^\mathfrak{p}$ for $i = 1, \dots, g$ and $j = 1, \dots, k_\mathfrak{p}$ as well as $\tilde{t}_{l,k}^\mathfrak{p}$ for $l = 1, \dots, \rho - 1$ and $k = 1, \dots, k_\mathfrak{p}$, each $f_i^\mathfrak{p}$ corresponds uniquely to a $k_\mathfrak{p}$-tuple of power series

$$f_{i,1}^\mathfrak{p}, \dots, f_{i,k_\mathfrak{p}}^\mathfrak{p} \in \mathbb{Z}_p \left\langle \tilde{x}_{i,j}^\mathfrak{p}, \tilde{t}_{l,j}^\mathfrak{p} \right\rangle_{\substack{1 \le i \le g,\ 1 \le j \le k_\mathfrak{p} \\ 1 \le l \le \rho - 1}}.$$

In conclusion, the analytic p-adic manifold $\mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_\mathfrak{p}} \subset \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_\mathfrak{p}}$ is cut out by $(g+\rho-2)k_\mathfrak{p}$ convergent power series in $(g + \rho - 1)k_\mathfrak{p}$ variables with coefficients in $\mathbb{Z}_p$.

Finally, note that $\mathbf{U}(\mathcal{O}_{K,p})_u$ inside $\mathbf{T}(\mathcal{O}_{K,p})_t$ is cut out by $(g+\rho-2)\sum_{\mathfrak{p}|p} k_\mathfrak{p} = (g+\rho-2)d$ convergent power series with coefficients in $\mathbb{Z}_p$. By Theorem 3.2, we have

$$\begin{array}{ccccc}
 & & \mathbb{Z}_p^{\delta(\rho-1)+r} & & \\
 & & \downarrow \kappa & \searrow (\kappa_i)_{i=1}^{(g+\rho-1)d} & \\
\mathbf{U}(\mathcal{O}_K)_u & \xhookrightarrow{\tilde{j}_b^U} & \mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p & & \\
\downarrow & & \downarrow & & \\
\mathbf{U}(\mathcal{O}_{K,p})_u & \xhookrightarrow{\tilde{j}_b^U} & \mathbf{T}(\mathcal{O}_{K,p})_t & = & \mathbb{Z}_p^{(g+\rho-1)d}.
\end{array}$$

The computation of the desired intersection is accomplished via pulling all equations back via κ.

Definition 3.10. The elements $\kappa^* f_{i,j}^{\mathfrak{p}}$ (with $1 \leq i \leq g+\rho-2$, $1 \leq j \leq k_{\mathfrak{p}}$ and $\mathfrak{p}|p$) all lie in $R = \mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$. Let $I_{\mathbf{U},u}$ denote the ideal in R generated by these elements and let $A_{\mathbf{U},u} := R/I_{\mathbf{U},u}$ denote the resulting quotient ring.

The intersection is algebraically expressed as the tensor product of rings, i.e., by taking the quotient by $I_{\mathbf{U},u}$. It follows that there is a bijection

$$\operatorname{Hom}(A_{\mathbf{U},u}, \mathbb{Z}_p) \longleftrightarrow \kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t). \tag{3.37}$$

Let $\bar{f}_{i,j}^{\mathfrak{p}} \in \mathbb{F}_p[\tilde{x}_{i,j}^{\mathfrak{p}}, \tilde{t}_{l,j}^{\mathfrak{p}}]$ denote the reduction modulo p and $\kappa^* \bar{f}_{i,j}^{\mathfrak{p}} \in \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]$. The ideal $\bar{I}_{\mathbf{U},u} = I_{\mathbf{U},u}\mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]$ is generated by the elements $\kappa^* \bar{f}_{i,j}^{\mathfrak{p}}$ and we let

$$\overline{A}_{\mathbf{U},u} := A_{\mathbf{U},u} \otimes \mathbb{F}_p = \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]/\bar{I}_{\mathbf{U},u}.$$

We are now ready to prove Theorem 3.3, which we conveniently restate for the reader.

Theorem 3.3. If $\overline{A}_{\mathbf{U},u}$ is finite, then $|\mathbf{U}(\mathcal{O}_K)_u| \leq \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}$.

Proof. For the sake of notation, we drop the subscripts $(\mathbf{U}, u)$ in this proof. The ring A is p-adically complete by the same proof of [62, Theorem 4.12]. Moreover, since $\overline{A}$ is finite, A is finitely generated as a $\mathbb{Z}_p$-module. Hence it follows that

$$\operatorname{Hom}(A, \mathbb{Z}_p) = \coprod_{\mathfrak{m}} \operatorname{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p) = \coprod_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \operatorname{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p),$$

where the union is over the maximal ideals of A. This gives the bound

$$|\operatorname{Hom}(A, \mathbb{Z}_p)| \leq \sum_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \operatorname{rank}_{\mathbb{Z}_p} A_{\mathfrak{m}} = \sum_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \dim_{\mathbb{F}_p} \overline{A}_{\mathfrak{m}} \leq \dim_{\mathbb{F}_p} \overline{A}.$$

This establishes, by (3.37), that the number of points in $\kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t)$ is bounded by

$\dim_{\mathbb{F}_p} \overline{A}$, thus we have

$$|\mathbf{U}(\mathcal{O}_K)_u| \leq |\kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t) \cap \overline{T(\mathcal{O}_K)_t}^p)| \leq \dim_{\mathbb{F}_p} \overline{A}.$$

□

Remark 3.12. The geometric quadratic Chabauty condition is implicit in the assumption of Theorem 3.3. Indeed, in order for the ring $\overline{A} = \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]/\langle \kappa^* \overline{f}_{i,j}^{\mathfrak{p}} \rangle_{i,j,\mathfrak{p}}$ to have a chance to be finite, the number of relations we quotient by must be at least the number of variables. Thus, we need $\delta(\rho-1)+r \leq (g+\rho-2)d$ which is equivalent to condition (3.24).

Corollary 3.2. *Suppose that $\overline{A}_{\mathbf{U},u}$ is finite for all $\mathbf{U}$ as in Definition 3.7 and all $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$. Then the set of rational points $C_K(K)$ is finite and satisfies*

$$|C_K(K)| \leq \sum_{\mathbf{U}} \sum_{u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})} \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}.$$

Proof. There are finitely many $\mathbf{U} \subset \mathbf{C}^{\mathrm{sm}}$ satisfying the conditions of Definition 3.7 and the union of $\mathbf{U}(\mathcal{O}_K)$ covers $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$ which is equal to $C(K)$ by properness and regularity of the model $\mathbf{C}$. Moreover, each $\mathbf{U}(\mathcal{O}_K)$ is the disjoint union of its residue disks $\mathbf{U}(\mathcal{O}_K)_u$, and the result follows. □

3.5.2 Refined questions

A more precise form of Questions 3.1 from the introduction is the following:

Question 3.2. *Given a subscheme $\mathbf{U}$ as in Definition 3.7 and $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$ mapping to $\tilde{j}_b^U(u) = t \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$, what conditions are necessary to guarantee the finiteness of the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathcal{O}_{K,p})_u$?*

In [62, §9], Edixhoven and Lido have given a new proof of Faltings' theorem, using their method, in the case of higher genus curves defined over $\mathbb{Q}$ satisfying $r < g+\rho-1$. Their argument is quite elegant: it uses complex analytic methods to prove a Zariski density statement, which can then be bridged with their p-adic geometric situation using formal geometry. This proves the finiteness of the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathbb{Z}_p)_u$ and in particular the finiteness of $C_{\mathbb{Q}}(\mathbb{Q})$.

The setting over arbitrary number fields is more complicated. Reminiscent of the failures of Siksek's method described in Section 0.4.2, there are examples of curves satisfying (3.24) for which the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathcal{O}_{K,p})_u$ is not finite. Examples include curves base changed from $\mathbb{Q}$ which do not satisfy the quadratic Chabauty condition over $\mathbb{Q}$. Based on Dogra's results in [60], presented in Section 0.4.2, we expect the intersection to be finite whenever the conditions (3.24) and

$$\mathrm{Hom}(J_{\bar{\mathbb{Q}},\sigma_1}, J_{\bar{\mathbb{Q}},\sigma_2}) = 0 \text{ for any two distinct embeddings } \sigma_1, \sigma_2 : K \hookrightarrow \bar{\mathbb{Q}} \tag{3.38}$$

are both satisfied. Unfortunately, the proof of this still eludes us.

The following question also demands attention:

Question 3.3. *Assuming conditions* (3.24) *and* (3.38)*, does there always exist a prime p such that for each open subscheme $\mathbf{U}$ of Definition 3.7 and each point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$, the ring $\overline{A}_{\mathbf{U},u}$ constructed in Definition 3.10 is finite-dimensional over $\mathbb{F}_p$?*

In order to extract an explicit bound for $|C_{\mathbb{Q}}(\mathbb{Q})|$, Edixhoven and Lido similarly rely on an analogous $\mathbb{F}_p$-vector space being of finite dimension. They conjecture [62, Section 4] that it is always possible in practice to choose p such that their condition is satisfied. We expect, following Edixhoven and Lido, that for curves satisfying conditions (3.24) and (3.38), there always exists a prime p such that the conditions of Question 3.3 are satisfied. We plan to address this in the near future by applying the method to explicit examples of curves.

Chapter 4

Diagonal cycles on $X_0(p)^3$

We explore the setting of diagonal type cycles on the triple product of the modular curve $X_0(p)$ of prime level p. See Section 1.2.2 for the definition of the latter. The main motivation stems from the Beilinson–Bloch conjecture 1.4 in this particular setting. This conjecture predicts the equality between the central order of vanishing of the triple product L-function associated to three normalised newforms in $S_2(\Gamma_0(p))$ on the one hand, and the rank of the (f_1, f_2, f_3)-isotypic component of the null-homologous Chow group of $X_0(p)^3$ of codimension two on the other hand. We refer to Sections 1.2.3 and 1.4 respectively for the definitions of newforms and Chow groups. One of the main results asserts that the global root number of the triple product L-function of (f_1, f_2, f_3) twisted by the Legendre symbol χ at p is always -1. The theory of root numbers was recalled in Section 1.1. In parallel, we construct a canonical null-homologous cycle on $X_0(p)^3$ of codimension 2 which lies in the (-1)-eigenspace of the Chow group for the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{\chi(-1)p})/\mathbb{Q})$. This leads us to formulate refinements of the Beilinson–Bloch conjecture in a setting which has not been considered before. Specialising to the case where f_3 has rational coefficients and $f_1 = f_2$, we formulate further refined conjectures concerned with the associated Chow–Heegner points on the elliptic curve associated with f_3. See Section 0.2.2 for the theory of Chow–Heegner points. When the global root number of the triple product (f_1, f_2, f_3) is $+1$, we prove that the image of the Gross–Kudla–Schoen cycle under the complex Abel–Jacobi map is torsion in the (f_1, f_2, f_3)-isotypic component of the second intermediate Jacobian of $X_0(p)^3$, and deduce torsion properties of the related Chow–Heegner points, which had originally been studied by Darmon, Rotger and Sols in the case where the root number is -1. Moreover, we prove that the Chow–Heegner points associated to the special cycle defined over $\mathbb{Q}(\sqrt{-p})$ are torsion whenever $p \equiv 3 \pmod 4$. Such torsion properties fit nicely with the proposed conjectures, and are in line with the Beilinson–Bloch and Birch and Swinnerton-Dyer conjectures.

Introduction

We study the setting of the triple product of the modular curve $X_0(p)$ of prime level p. Given three normalised newforms $f_1, f_2, f_3 \in S_2(\Gamma_0(p))$, we denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple tensor product. Associated to F is a motive

$$M(F) := (X_0(p)^3, t_F, 0) \in \mathbf{Chow}(\mathbb{Q})_{K_F}$$

over $\mathbb{Q}$ with coefficients in the finite extension K_F of $\mathbb{Q}$ obtained by adjoining the Fourier coefficients of f_1, f_2 and f_3. We refer to Section 1.4.2 for the definition of motives. Here $t_F \in \mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)_{K_F}$ is an idempotent correspondence – the F-isotypic projector – built from the projectors that cut out the motives of the three forms f_1, f_2 and f_3. The associated L-function $L(F, s) := L(M(F)/\mathbb{Q}, s)$, defined in Section 1.1.4, is the Garrett–Rankin triple product L-function attached to F. The analytic properties and functional equation of this L-function have been established by Gross and Kudla [76]. The Beilinson–Bloch conjecture 1.4 in this context predicts the equality

$$\operatorname{ord}_{s=2} L(F, s) = \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes K_F). \tag{4.1}$$

In [76], Gross and Kudla introduced a particular cycle $\Delta_{\mathrm{GKS}} \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$, the study of which was taken up by Gross and Schoen in [77]. We will therefore refer to it as the Gross–Kudla–Schoen cycle. It arises from the diagonal embedding of $X_0(p)$ in $X_0(p)^3$ after applying a certain projector whose effect is to make the resulting cycle null-homologous. Guided by the Beilinson–Bloch conjecture (4.1), Gross and Kudla conjectured, in the case when the global root number is $W(F) = -1$, that $L'(F, 2)$ is equal (up to a non-zero constant) to the Beilinson–Bloch height of the cycle $(t_F)_*(\Delta_{\mathrm{GKS}})$. A proof of this conjecture is expected to appear in [154].

We are interested in a different and yet unexplored setting of the Beilinson–Bloch conjecture. Namely, if χ denotes the Legendre symbol at p, and $M(F) \otimes \chi$ is the twisted motive, then the Beilinson–Bloch conjecture also predicts the equality

$$\mathrm{ord}_{s=2}\, L(F \otimes \chi, s) = \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1} \otimes K_F), \tag{4.2}$$

where $K = \mathbb{Q}(\sqrt{\chi(-1)p})$ is the quadratic field corresponding to χ, and $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ is the non-trivial automorphism. One of the main results is Theorem 4.7 which asserts that the global root number $W(F \otimes \chi)$ is always equal to -1. In particular, we have $\mathrm{ord}_{s=2}\, L(F \otimes \chi, s) \geq 1$ and we thus expect by (4.2) the existence of a non-zero cycle in $(t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1} \otimes K_F)$. In parallel, we construct a canonical cycle

$$\Xi := \varphi_+(X(p)) - \varphi_-(X(p))$$

of codimension 2 on $X_0(p)^3$, where $\varphi_+, \varphi_- : X(p) \longrightarrow X_0(p)^3$ are two algebraic maps whose common domain is the modular curve $X(p)$ of full level p. The definition of this latter curve can be found in Section 1.2.2. In Theorem 4.3, we prove that Ξ belongs to $\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}$.

Putting the above results together, it is tempting to conjecture that the torsion properties of $(t_F)_*(\Xi)$ should be determined by the order of vanishing of $L(F \otimes \chi, s)$ at its centre. This is formulated precisely in Conjecture 4.1 as a refinement of the Beilinson–Bloch conjecture.

Conjecture 4.1 would follow, assuming the non-degeneracy of the Beilinson–Bloch height, from an analogue of the Gross–Zagier formula relating $L'(F \otimes \chi, 2)$ to the Beilinson–Bloch height of $(t_F)_*(\Xi)$. Further refinements are proposed in Conjectures 4.2 and 4.3, which take into account the root number of $W(F)$ and the predicted behaviour of $(t_F)_*(\Delta_{\mathrm{GKS}})$. When $W(F) = +1$, we prove in Theorem 4.4 that the image of $(t_F)_*(\Delta_{\mathrm{GKS}})$ under the complex Abel–Jacobi map $\mathrm{AJ}_{X_0(p)^3}$ of Section 1.5.1 is torsion in the intermediate Jacobian $J^2(X_0(p)^3/\mathbb{C})$. When $W(F) = -1$, the conjectural formula of Gross and Kudla serves to guide us.

In [51], Darmon, Rotger and Sols studied certain Chow–Heegner points associated to Δ_{GKS}. These are intimately related to so-called Zhang points on abelian varieties due to S. Zhang [157]. This connection is made explicit in Daub's thesis [53]. At the level of modular forms, the Chow–Heegner points arise from the triple product setting by specialising to the case where $f_3 = f$ has rational coefficients and $f_1 = f_2 = g$ is not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f, and are denoted by

$$P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}) \in E_f(\mathbb{Q}).$$

Here E_f is the elliptic curve over $\mathbb{Q}$ associated to f by the Eichler–Shimura construction of Section 1.2.3, and $\Pi_{[g],f} \in \mathrm{Corr}^{-1}(X_0(p)^3, E_f)$ is some correspondence which depends on the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugacy class $[g]$ of g, as well as on f. Note that we have the following decomposition of the L-function

$$L(g, g, f, s) = L(\mathrm{Sym}^2\, g \otimes f, s) L(f, s-1).$$

When the root numbers satisfy $W(f) = -1$ and $W(\mathrm{Sym}^2\, g \otimes f) = +1$ (and thus in particular $W(g, g, f) = -1$), Darmon, Rotger and Sols have proved, building on the work of Yuan, Zhang and Zhang [154], that $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}})$ has infinite order if and only if $\mathrm{ord}_{s=1} L(f, s) = 1$ and $\mathrm{ord}_{s=2} L(\mathrm{Sym}^2(g^\sigma) \otimes f, s) = 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$. This provides insight into the Birch and Swinnerton-Dyer conjecture for $E_f/\mathbb{Q}$.

Meanwhile, the Birch and Swinnerton-Dyer conjecture also predicts the equality

$$\mathrm{ord}_{s=1} L(E_f^{\chi}/\mathbb{Q}, s) = \mathrm{rank}_{\mathbb{Z}} E_f(K)^{\tau=-1}, \tag{4.3}$$

where E_f^{χ} denotes the quadratic twist of E_f by the Legendre symbol χ at p. Using the cycle Ξ, we may consider the Chow–Heegner point

$$P(X_0(p)^3, \Pi_{[g],f}, \Xi) \in E_f(K)^{\tau=-1}.$$

If $p \equiv 3 \pmod 4$, then $W(E_f^{\chi}) = +1$, and we prove in Theorem 4.6 that the above point is torsion by exploiting the action of the symmetric group S_3 on Ξ. This is consistent with (4.50). If $p \equiv 1 \pmod 4$, then $W(E_f^{\chi}) = -1$ and we thus expect there to exist a point in $E_f(K)^{\tau=-1}$ of infinite order. Guided by (4.50), we formulate a refined conjecture (Conjecture 4.4) which predicts exactly when $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ has infinite order. We make further refinements in Conjectures 4.5 and 4.6 by taking into account the root number of E_f and interactions with $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}) \in E_f(\mathbb{Q})$. When $W(f) = +1$, we prove in Theorem 4.5 that the point $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}})$ is torsion, obtaining a special case of a result of Daub [53]. When $W(f) = -1$, the results of Darmon, Rotger and Sols are available to us. This fits nicely with the proposed conjectures.

We refer to Section 5.1 for a discussion of future work involving possible strategies for addressing the conjectures proposed in this chapter.

We finish with an outline of the chapter. Section 4.1 introduces the motives attached to a normalised newform in $S_2(\Gamma_0(p))$ and to the triple product of such forms. We give a brief overview of the work of Gross and Kudla [76] concerning the Garrett–Rankin triple product L-function. We also recall the construction of Chow–Heegner points in the setting of the triple product of modular curves. Section 4.2 contains a systematic construction of diagonal type cycles on $X_0(p)^3$. In particular, the cycle Ξ is defined and Theorem 4.3 is proved. Section 4.3 addresses the torsion properties of both cycles and Chow–Heegner points in various cases; it contains the proofs of Theorem 4.4, Theorem 4.5 and Theorem 4.6. Section 4.4 uses the explicit description of the Weil–Deligne representations of modular forms described in Secton 4.1 to compute global root numbers in various setting, culminating in the proof of Theorem 4.7. Section 4.5 formulates conjectures concerning the special cycle Ξ (Conjectures 4.1, 4.2, 4.3) and its associated Chow–Heegner points (Conjectures 4.4, 4.5, 4.6, 4.7) based on the results of this chapter.

4.1 Preliminaries

We begin by recalling the definition of the motive of a normalised cuspform of weight 2 and level $\Gamma_0(p)$. We then review the definition and properties of L-functions associated to triples of weight 2 normalised cuspforms of level $\Gamma_0(p)$. In particular, we will recall the main results of the work of Gross and Kudla [76] in this context. Finally, we give an overview of the Chow–Heegner construction in the context of triple products.

4.1.1 Modular forms of weight 2

For an overview of the theory of modular forms of weight 2 and level $\Gamma_0(p)$, we refer to Section 1.2.3.

Decomposition of the Hecke algebra

Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_2(\Gamma_0(p))$ be a normalised newform of level $\Gamma_0(p)$. Because the level is prime, there are no oldforms. The form f is a normalised eigenform for the $\mathbb{Q}$-algebra $\mathbb{T}_0 := \mathbb{T}_0(p)$ generated by the Hecke operators T_n for $p \nmid n$ acting on $S_2(\Gamma_0(p))$. Let $\mathbb{T} := \mathbb{T}(p)$ denote the full commutative Hecke algebra generated by the T_n for $p \nmid n$ and the operator U_p. Following the discussion of newforms in Section 1.2.3 and references therein, we have $U_p(f) = a_p(f)f$ and $w_p(f) = -a_p(f)f$. Here w_p denotes the Atkin–Lehner operator, which in the case of prime level arises from the Fricke involution on $X_0(p)$ via its pullback action on cohomology and the identification (1.19) of $S_2(\Gamma_0(p))$ with the space of regular differential 1-forms $H^0(X_0(p), \Omega^1_{X_0(p)})$. In particular, we have $a_p(f) \in \{\pm 1\}$. Note that because there are no oldforms at prime level, we have $U_p = -w_p$ in $\mathbb{T}$.

The normalised eigenform f determines a surjective algebra homomorphism $\lambda_f : \mathbb{T}_0 \longrightarrow K_f$ by sending T_n to $a_n(f)$. Here K_f is the finite extension of $\mathbb{Q}$ generated by the Fourier coefficients $a_n(f)$ of f. Note that the coefficients $a_n(f)$ are the eigenvalues of the operators T_n acting on f. In particular, K_f is a totally real number field as the operators T_n are Hermitian with respect to the Petersson inner product on $S_2(\Gamma_0(p))$.

Let $S_2(\Gamma_0(p))_f$ denote the f-isotypic component of $S_2(\Gamma_0(p))$ consisting of cusp forms $g \in S_2(\Gamma_0(p))$ such that $T(g) = \lambda_f(T)g$ for all $T \in \mathbb{T}_0$. By the multiplicity one result [3, Lemmas 20 and 21] of Atkin and Lehner for newforms, the space $S_2(\Gamma_0(p))_f$ is 1-dimensional over $\mathbb{C}$. By the results described in Section 1.2.3, we have the decomposition

$$S_2(\Gamma_0(p)) = \bigoplus_h S_2(\Gamma_0(p))_h,$$

where the sum is taken over all normalised eigenforms $h \in S_2(\Gamma_0(p))$. Since the dual space $S_2(\Gamma_0(p))^\vee$ is a free $\mathbb{T}_{0,\mathbb{C}}$-module of rank one by multiplicity one, we similarly obtain a decomposition

$$\mathbb{T}_{0,\mathbb{C}} = \bigoplus_h \mathbb{T}_{0,\mathbb{C},h},$$

where $\mathbb{T}_{0,\mathbb{C},h}$ denotes the algebra of Hecke operators T_n with $(n,p) = 1$ acting on $S_2(\Gamma_0(p))_h$, which is again a $\mathbb{C}$-vector space of dimension one.

Let $[f]$ denote the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ orbit of f. Form the $\mathbb{C}$-vector space $\bigoplus_{g \in [f]} S_2(\Gamma_0(p))_g$ of dimension $d_f := [K_f : \mathbb{Q}]$, and consider the $\mathbb{Q}$-subspace $S_2(\Gamma_0(p))_{[f]}$ of forms with rational coefficients. This $\mathbb{Q}$-vector space is stable under the action of $\mathbb{T}_{0,\mathbb{Q}}$, and we let $\mathbb{T}_{0,\mathbb{Q},[f]}$ denote the $\mathbb{Q}$-algebra generated by the Hecke operators acting on $S_2(\Gamma_0(p))_{[f]}$. We then have the decomposition

$$\mathbb{T}_0 = \bigoplus_{[h]} \mathbb{T}_{0,\mathbb{Q},[h]} \simeq \bigoplus_{[h]} K_h,$$

where the sum is taken over all $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugacy classes of normalised eigenforms in $S_2(\Gamma_0(p))$.

Remark 4.1. The exposition in this section is simplified by the fact that there are no oldforms for prime level. For the more general case where the level is composite we refer to [45, §1.6].

Let $\mathrm{End}_{\mathbb{Q}}(J_0(p))$ denote the ring of endomorphisms of the Jacobian $J_0(p)$ which are defined over $\mathbb{Q}$ and let $\mathrm{End}^0_{\mathbb{Q}}(J_0(p)) := \mathrm{End}_{\mathbb{Q}}(J_0(p)) \otimes \mathbb{Q}$. Because p is prime, we have $\mathrm{End}^0_{\mathbb{Q}}(J_0(p)) = \mathbb{T}_0$ by [125, Corollary 3.3]. In particular, we have $\mathbb{T}_0 = \mathbb{T}$. In summary, we have the decomposition

$$\mathrm{End}^0_{\mathbb{Q}}(J_0(p)) = \mathbb{T}_0 \simeq \bigoplus_{[h]} K_h. \tag{4.4}$$

Remark 4.2. Once again, the exposition is simplified by the assumption that the level is prime. For composite level N, the algebra $\mathrm{End}^0_{\mathbb{Q}}(J_0(N))$ is a product of matrix algebras. It contains $\mathbb{T}_0$ as its center and the full Hecke algebra $\mathbb{T}$ as a maximal commutative subalgebra. Moreover, $\mathrm{End}^0_{\mathbb{Q}}(J_0(N))$ is generated as a $\mathbb{Q}$-algebra by $\mathbb{T}_0$ together with certain degeneracy operators. See [95, Theorem 1].

We remark also that there is a natural isomorphism

$$\mathrm{End}^0_{\mathbb{Q}}(J_0(p)) \simeq (\mathrm{CH}^1(X_0(p)^2) \otimes \mathbb{Q})/(\mathrm{pr}_1^* \mathrm{CH}^1(X_0(p)) \otimes \mathbb{Q} + \mathrm{pr}_2^* \mathrm{CH}^1(X_0(p)) \otimes \mathbb{Q}). \tag{4.5}$$

See for instance [105, Theorem 11.5.1].

Galois representations

Let $f = \sum_{n \geq 1} a_n(f) q^n \in S_2(\Gamma_0(p))$ be a normalised eigenform. Recall that the Eichler–Shimura construction of Section 1.2.3 associates to the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugacy class of f a simple abelian variety $A_{[f]}$ defined over $\mathbb{Q}$ as a quotient of $J_0(p)$. For a given prime ℓ, the ℓ-adic Tate module of $A_{[f]}$ carries an action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, as well as an action of $K_f = \mathrm{End}_{\mathbb{Q}}(A_{[f]}) \otimes \mathbb{Q}$, and these actions commute. Since the Tate module of $A_{[f]}$ is a free module of rank two over $K_f \otimes \mathbb{Q}_\ell$, it gives rise (after a choice of basis) to a Galois representation

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(K_f \otimes \mathbb{Q}_\ell). \tag{4.6}$$

Throughout this chapter, we will use the same conventions as established in Notation 1.1. We let $\mathfrak{l}$ denote the prime of K_f above ℓ determined by the corresponding fixed field embeddings. We obtain the ℓ-adic Galois representation associated to f

$$\rho_{f,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(K_{f,\mathfrak{l}}), \tag{4.7}$$

by composing the above representation (4.6) with the projection $K_f \otimes \mathbb{Q}_\ell \longrightarrow K_{f,\mathfrak{l}}$.

Remark 4.3. The representation $\rho_{f,\ell}$ depends on the embedding of K_f in $\mathbb{C}$, as well as the embedding of K_f in $\bar{\mathbb{Q}}_\ell$, but we suppress these dependencies from the notation, as we have fixed all embeddings from the beginning.

Proposition 4.1. *Suppose that $\ell \neq p$. The representation (4.7) satisfies the following:*

- *If $q \nmid p\ell$ is a prime, then $\rho_{f,\ell}$ is unramified at q and the Frobenius element of $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ has characteristic polynomial $X^2 - a_q(f)X + q$.*
- *The determinant of $\rho_{f,\ell}$ is the ℓ-adic cyclotomic character $\omega_{\mathrm{cyc},\ell}$ of Example 1.1.*
- *Let $\lambda : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow K_{f,\mathfrak{l}}^\times$ denote the unramified quadratic character determined by $\lambda(\Phi) = a_p(f)$, where Φ is an inverse Frobenius element at p. Then*

$$\rho_{f,\ell}\big|_{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)} \simeq \begin{pmatrix} \lambda\omega_{\mathrm{cyc},\ell} & * \\ 0 & \lambda \end{pmatrix}.$$

Proof. See for instance [45, Theorem 3.1] and references therein. □

Definition 4.1. We denote by $V_\ell(f)$ the contragredient of the representation $\rho_{f,\ell}$ of (4.7). The collection $\{V_\ell(f)\}_\ell$ is a compatible family of 2-dimensional ℓ-adic (or rather $\mathfrak{l}$-adic) representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Motives

We refer to Section 1.4.2 for conventions on motives. The language of motives is not strictly speaking necessary in this section, but it will be useful starting with Section 4.1.2 below.

Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_2(\Gamma_0(p))$ be a normalised eigenform and retain the notations introduced in the previous sections. Let $V := S_2(\Gamma_0(p))^\vee$ be the $\mathbb{C}$-vector space dual to $S_2(\Gamma_0(p))$. Recall from Section 1.2.3 the identification $S_2(\Gamma_0(p)) \simeq H^0(X_0(p), \Omega^1_{X_0(p)})$, and from Section 1.5.1 the description of the complex points of $J_0(p)$ as

$$J_0(p)(\mathbb{C}) = \frac{H^0(X_0(p), \Omega^1_{X_0(p)})^\vee}{\operatorname{Im} H_1(X_0(p)(\mathbb{C}), \mathbb{Z})},$$

where $\Lambda := \operatorname{Im} H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ is viewed as a lattice via integration of differential forms. We thus have an identification $J_0(p)(\mathbb{C}) = V/\Lambda$ as a g-dimensional complex torus, where g is the genus of $X_0(p)$. Let V_f be the subspace of V on which $\mathbb{T}$ acts by λ_f and let $\pi_f : V \longrightarrow V_f$ be the orthogonal projection with respect to the Petersson scalar product. The projector π_f naturally belongs to $\mathbb{T}_{K_f} = \mathbb{T} \otimes_{\mathbb{Q}} K_f$, and by (4.4) and (4.5) we may view π_f as an idempotent correspondence $t_f \in \mathrm{Corr}^0(X_0(p), X_0(p))_{K_f}$.

Definition 4.2. The motive $M(f) := (X_0(p), t_f, 0) \in \mathbf{Chow}(\mathbb{Q})_{K_f}$ over $\mathbb{Q}$ with coefficients in K_f is the motive of f.

Remark 4.4. The Hecke operators T_ℓ for $\ell \neq p$ act on $H^2(X_0(p), \mathbb{C})$ as multiplication by $\ell+1$, the degree of the correspondence T_ℓ. By duality, T_ℓ also acts as multiplication by $\ell+1$ on $H^0(X_0(p), \mathbb{C})$. The eigenvalues of the action of the Hecke algebra on $H^1(X_0(p), \mathbb{C})$ are encoded by the algebra homomorphisms $\lambda_f : \mathbb{T}_{0,\mathbb{C}} \longrightarrow K_f$ indexed by the conjugacy classes of newforms in $S_2(\Gamma_0(p))$, where $\lambda_f(T_\ell) = a_\ell(f)$. As a consequence of Deligne's proof of the Weil conjectures [57], we have the bound $|a_\ell(f)| \leq 2\sqrt{\ell}$ generalising the Hasse bound for elliptic curves. Since $2\sqrt{\ell} < \ell + 1$, the eigenvalues of T_ℓ acting on $H^i(X_0(p), \mathbb{C})$ do not overlap between the cases $i = 1$ and $i \in \{0, 2\}$. Since t_f is the f-isotypic Hecke projector, it follows that t_f annihilates the cohomology groups of $X_0(p)$ in degree 0 and 2.

The ℓ-adic representations of $M(f)$ are equal to

$$M(f)_\ell = (t_f)_* H^*_{\mathrm{et}}(X_0(p)_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) = H^1_{\mathrm{et}}(X_0(p)_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)_f = V_\ell(f),$$

where $V_\ell(f)$ is the representation of Definition 4.1 (taking into account the fixed field embeddings of Notation 1.1). The de Rham realisation is

$$M(f)_{\mathrm{dR}} = (t_f)_* H^*_{\mathrm{dR}}(X_0(p)/\mathbb{C}) = H^1(X_0(p)(\mathbb{C}), \mathbb{C})_f \simeq S_2(\Gamma_0(p))_f \oplus \overline{S_2(\Gamma_0(p))_f}.$$

It follows that the Hodge structure $M(f)_B = (t_f)_* H^1(X_0(p)(\mathbb{C}), \mathbb{Q})$ is of type $(1,0) + (0,1)$. By multiplicity one, we have $H^{1,0}(M(f)) = \mathbb{C}\omega_f$, and the Hodge numbers are given by

$$h^{1,0}(M(f)) = h^{0,1}(M(f)) = 1. \tag{4.8}$$

If we let $V_{[f]} := \bigoplus_{g \in [f]} V_g$ and $\pi_{[f]} := \sum_{g \in [f]} \pi_f$, then $\pi_{[f]}$ is the orthogonal projection $V \longrightarrow V_{[f]}$ with respect to the Petersson scalar product. By [45, Lemma 1.46], the abelian variety $A_{[f]}$ is isomorphic over $\mathbb{C}$ to the complex torus $V_{[f]}/\pi_{[f]}(\Lambda)$, with the projection map $\pi_{[f]} : V/\Lambda \longrightarrow V_{[f]}/\pi_{[f]}(\Lambda)$ corresponding to the natural projection $J_0(p) \longrightarrow A_{[f]}$. In particular, $\pi_{[f]}$ naturally belongs to $\mathbb{T} = \mathrm{End}^0_{\mathbb{Q}}(J_0(p))$, and corresponds under (4.4) to the idempotent element $e_{[f]} \in \bigoplus_{[h]} K_h$ which has 1 as $[f]$-coordinate and 0 as $[h]$-coordinate for $[h] \neq [f]$. By (4.5), we may view $\pi_{[f]}$ as an idempotent correspondence $t_{[f]} \in \mathrm{Corr}^0(X_0(p), X_0(p))_{\mathbb{Q}}$. It follows that the motive $M([f]) := (X_0(p), t_{[f]}, 0) \in \mathbf{Chow}(\mathbb{Q})_{\mathbb{Q}}$ is equal to $A_{[f]}$.

Remark 4.5. The motive $M([f])$ is very convenient to work with as it is realised by the abelian variety $A_{[f]}$. On the other hand, the motive $M(f)$ associated to f has coefficients in K_f and is merely a piece of the cohomology of $A_{[f]}$; it is not physically realised by some abelian variety quotient of $A_{[f]}$, hence it is a little more delicate to work with.

Weil–Deligne representations

We drop the notation $\mathfrak{l}$ as this prime ideal is determined completely by the fixed choices of field embeddings made in Notation 1.1. Let q be a prime, let ℓ be a prime different from q and fix an embedding $\iota_\ell : K_{f,\mathfrak{l}} \hookrightarrow \mathbb{C}$. Following [126, §4 Generalization], one may associate to $V_\ell(f)$ a 2-dimensional complex representation $\sigma'_{f,\ell,\iota_\ell,q} = (\sigma_{f,\ell,\iota_\ell,q}, N_{f,\ell,\iota_\ell,q})$ of the Weil–Deligne group $W'(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$. See Section 1.1. It turns out, as we will see shortly, that the isomorphism class of the Weil–Deligne representation $\sigma'_{f,\ell,\iota_\ell,q}$ is independent of ℓ and ι_ℓ and we shall simply write $\sigma'_{f,q} = (\sigma_{f,q}, N_{f,q})$. This is the Weil–Deligne representation of f at q.

Proposition 4.2. *The Weil–Deligne representations of f satisfy the following:*

- *At the infinite place, we have $\sigma'_{f,\infty} = \mathrm{ind}_{\mathbb{C}/\mathbb{R}}\, \varphi_{0,1} \otimes H^{0,1}(M(f))$.*
- *If $q \neq p$, then $N_{f,q} = 0$ and $\sigma_{f,q} \simeq \xi_q \oplus \xi_q^{-1}\omega_q^{-1}$ for some unramified character ξ_q. Here ω_q is the Weil–Deligne representation of the ℓ-adic cyclotomic character of Definition 1.2 and Example 1.1.*
- *Let λ be the unramified quadratic character of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ defined by $\lambda(\Phi) = a_p(f)$, where Φ denotes an inverse Frobenius element. Then $\sigma'_{f,p} \simeq \lambda\omega_q^{-1} \otimes \mathrm{sp}(2)$, so that, in particular, $N_{f,q} \neq 0$ and $\sigma'_{f,q}$ is ramified. Here $\mathrm{sp}(2)$ is the special representation of Definition 1.5.*

Proof. Using Proposition 4.1, the proofs in [126, §14, §15] adapt to this setting and give the above descriptions of the Weil–Deligne representations of f. In particular, these are independent of the choices of a prime ℓ and an embedding $\iota_\ell : K_{f,\mathfrak{l}} \hookrightarrow \mathbb{C}$. □

L-functions

Following Section 1.1.4, we can associate an L-function

$$\Lambda(M(f)/\mathbb{Q}, s) = L(\sigma'_{f,\infty}, s) \prod_q L(\sigma'_{f,q}, s)$$

to the motive $M(f) \in \mathbf{Chow}(\mathbb{Q})_{K_f}$ of Definition 4.2, and use Proposition 4.2 to give an explicit description of the local factors. Since $h^{1,0}(M(f)) = 1$, the above Weil–Deligne representations have already been encountered in Section 1.2, and we see that

$$\Lambda(M(f)/\mathbb{Q}, s) = 2(2\pi)^{-s}\Gamma(s)(1 - a_p(f)p^{-s})^{-1} \prod_{q \neq p} (1 - a_q(f)q^{-s} + q^{1-2s})^{-1},$$

which is the completed L-function of f, namely

$$\Lambda(f, s) = 2(2\pi)^{-s}\Gamma(s) \sum_{n \geq 1} \frac{a_n(f)}{n^s}.$$

The conductor of $M(f)$ is p and the global root number is $W(M(f)/\mathbb{Q}) = a_p(f)$, as follows from the proof of Proposition 1.5 suitably adapted to the present situation. Conjecture 1.9 predicts that the L-function $\Lambda^*(M(f)/\mathbb{Q}, s) = p^{\frac{s}{2}}\Lambda(M(f)/\mathbb{Q}, s)$ satisfies the functional equation

$$\Lambda^*(M(f)/\mathbb{Q}, s) = a_p(f)\Lambda^*(M(f)/\mathbb{Q}, 2 - s).$$

This is true and can be checked using the integral representation of $\Lambda(f, s)$ and the weight 2 transformation property of the modular form f.

Following Section 1.1.4, we can associate an L-function $\Lambda(M([f])/\mathbb{Q}, s)$ to the motive $M([f]) \in \mathbf{Chow}(\mathbb{Q})_{\mathbb{Q}}$, and by previous observations, we have

$$\Lambda(M([f])/\mathbb{Q}, s) = \Lambda(A_{[f]}/\mathbb{Q}, s) = \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} \Lambda(f^\sigma, s).$$

4.1.2 Triple products of modular forms of weight 2

Let

$$f_1 = \sum_{n\geq 1} a_n(f_1)q^n, \qquad f_2 = \sum_{n\geq 1} a_n(f_2)q^n, \qquad f_3 = \sum_{n\geq 1} a_n(f_3)q^n$$

be three normalised newforms of level $\Gamma_0(p)$, and let $F := f_1 \otimes f_2 \otimes f_3$ be the newform of weight $(2,2,2)$ for $\Gamma_0(p)^3$ obtained from f_1, f_2 and f_3. Let $K_F = K_{f_1} \cdot K_{f_2} \cdot K_{f_3}$ denote the compositum of the Fourier coefficient fields of the forms f_1, f_2 and f_3. Using the notations of the previous section, define the idempotent correspondence

$$t_F := t_{f_1} \otimes t_{f_2} \otimes t_{f_3} = \mathrm{pr}_{14}^*(t_{f_1}) \cdot \mathrm{pr}_{25}^*(t_{f_2}) \cdot \mathrm{pr}_{36}^*(t_{f_3}) \in \mathrm{Corr}^0(X_0(p)^3, X_0(p)^3) \otimes K_F. \quad (4.9)$$

Definition 4.3. The motive of the triple product F is defined to be the motive

$$M(F) := M(f_1) \otimes M(f_2) \otimes M(f_3) = (X_0(p)^3, t_F, 0) \in \mathbf{Chow}(\mathbb{Q})_{K_F}$$

over $\mathbb{Q}$ with coefficients in K_F.

Remark 4.6. By Remark 4.4, when acting on the cohomology $H^*(X_0(p)^3)$ of $X_0(p)^3$, the correspondence t_F annihilates all cohomology except in degree 3, in which all components except the Künneth $(1,1,1)$-component are annihilated. As a consequence, we have

$$(t_F)_* H^*(X_0(p)^3) = (t_{f_1})_* H^1(X_0(p)) \otimes (t_{f_2})_* H^1(X_0(p)^1) \otimes (t_{f_3})_* H^1(X_0(p)^1).$$

The ℓ-adic realisations of $M(F)$ give rise to a compatible family of 8-dimensional ℓ-adic Galois representations

$$\{V_\ell(F) := M(F)_\ell = V_\ell(f_1) \otimes V_\ell(f_2) \otimes V_\ell(f_3)\}_\ell,$$

where the representations $V_\ell(f_i)$ for $i \in \{1,2,3\}$ are the ones of Definition 4.1. The Weil–

Deligne representation of F at a prime q is the 8-dimensional representation given by

$$\sigma'_{F,q} = \sigma'_{f_1,q} \otimes \sigma'_{f_2,q} \otimes \sigma'_{f_3,q}.$$

Concretely, we have

$$(\sigma_{F,q}, N_{F,q}) = (\sigma_{f_1,q} \otimes \sigma_{f_2,q} \otimes \sigma_{f_3,q}, N_{f_1,q} \otimes 1 \otimes 1 + 1 \otimes N_{f_2,q} \otimes 1 + 1 \otimes 1 \otimes N_{f_3,q}).$$

The de Rham realisation is given by

$$M(F)_{\mathrm{dR}} = H^1(X_0(p)(\mathbb{C}), \mathbb{C})_{f_1} \otimes H^1(X_0(p)(\mathbb{C}), \mathbb{C})_{f_2} \otimes H^1(X_0(p)(\mathbb{C}), \mathbb{C})_{f_3},$$

hence, using (4.8), the Hodge numbers of $M(F)$ are given by

$$h^{3,0}(M(F)) = h^{0,3}(M(F)) = 1 \qquad \text{and} \qquad h^{2,1}(M(F)) = h^{1,2}(M(F)) = 3. \tag{4.10}$$

In particular, the Weil–Deligne representation of F at infinity is

$$\sigma'_{F,\infty} = (\mathrm{ind}_{\mathbb{C}/\mathbb{R}}(\varphi_{1,2})) \otimes H^{1,2}(M(F)) \oplus (\mathrm{ind}_{\mathbb{C}/\mathbb{R}}(\varphi_{0,3})) \otimes H^{0,3}(M(F)). \tag{4.11}$$

Triple product L-functions

Following Section 1.1.4, one attaches to the motive of F the L-function

$$\Lambda(M(F)/\mathbb{Q}, s) := L(\sigma'_{F,\infty}, s) \prod_q L(\sigma'_{F,q}, s).$$

This is the Garrett–Rankin triple product L-function associated to f_1, f_2 and f_3.

Remark 4.7. We will alternatively write $\Lambda(F, s)$ or $\Lambda(f_1, f_2, f_3, s)$ for this L-function. Similarly, we write $L(F, s)$ or $L(f_1, f_2, f_3, s)$ for the finite part $\prod_q L(\sigma'_{F,q}, s)$ and also refer to this as the triple product L-function.

We obtain the local L-factor at the finite prime q by the formula

$$L(\sigma'_{F,q}, s) := \det(1 - q^{-s}\Phi \mid \mathbf{V}_{q,N_{\mathbf{E},q}}^{I_q})^{-1},$$

where $\mathbf{V}_q$ is the underlying complex vector space of $\sigma'_{F,q}$ and $\mathbf{V}_{q,N_{F,q}}^{I_q} := \mathbf{V}_q^{I_q} \cap \ker N_{F,q}$. Using the description of the Weil–Deligne representations of F, one can work out the explicit expressions for these local factors, as in [76, (1.7), (1.8)]: at primes $q \neq p$ they are of degree 8 and at p it is of degree 3. Following Section 1.1.4 and using (4.10), the local L-factor at infinity is given by

$$L(\sigma'_{F,\infty}, s) = L_{\mathbb{C}}(\varphi_{1,2}, s)^3 L_{\mathbb{C}}(\varphi_{0,3}, s) = \Gamma_{\mathbb{C}}(s-1)^3\Gamma_{\mathbb{C}}(s) = 2^4(2\pi)^{3-4s}\Gamma(s-1)^3\Gamma(s).$$

If we let

$$\Lambda^*(F, s) := \mathrm{cond}(M(F)/\mathbb{Q})^{\frac{s}{2}}\Lambda(F, s), \tag{4.12}$$

then Conjecture 1.9 predicts that this L-function admits analytic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda^*(F, s) = W(F) \cdot \Lambda^*(F, 4-s), \tag{4.13}$$

where $W(F) = W(f_1, f_2, f_3) = W(M(F)/\mathbb{Q})$ is the global root number of the motive $M(F)$.

Remark 4.8. Using the explicit description of the Weil–Deligne representations of $M(F)$, it is possible to prove that

$$W(F) = a_p(f_1)a_p(f_2)a_p(f_3) \qquad \text{and} \qquad \mathrm{cond}(M(F)/\mathbb{Q}) = p^5.$$

These results are stated for instance in [76, §1]. In Proposition 4.5 and Remark 4.26 later in this chapter, we give a full proof of these facts.

The analytic continuation of $\Lambda^*(F, s)$ and the functional equation (4.13) have been proved by Gross and Kudla [76, Proposition 1.1]. The centre of symmetry of the functional equation is the point $s = 2$ at which $L(F, s)$ has no pole. Moreover, $L(\sigma'_{\infty,F}, s)$ has neither zero nor pole at $s = 2$, so the centre is a critical point and

$$W(F) = (-1)^{\mathrm{ord}_{s=2} L(F,s)}.$$

Note that the Bloch–Beilinson conjecture 1.4 predicts in this setting that

$$\mathrm{ord}_{s=2} L(F, 2) = \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)(\mathbb{Q})_0 \otimes K_F). \tag{4.14}$$

The case $W(F) = +1$

Define the complex period associated to F by

$$\Omega_F := \frac{\|\omega_{f_1}\|^2 \cdot \|\omega_{f_2}\|^2 \cdot \|\omega_{f_3}\|^2}{4\pi p}, \tag{4.15}$$

where $\omega_{f_j} := 2\pi i f_j(z)dz$ is the normalised eigendifferential on $X_0(p)$ associated to f_j for $j \in \{1, 2, 3\}$, see Section 1.2.3, and where $\| \cdot \|$ denotes the Petersson norm. In this section we work under the assumption $W(F) = +1$, which implies that $L(F, s)$ vanishes to even order at the central critical point $s = 2$. The Gross–Kudla formula is then an expression for the central critical value of the form

$$L(F, 2) = \Omega_F \cdot A_F$$

where A_F is a real algebraic number in the subfield of $\mathbb{C}$ generated by the coefficients of the Dirichlet series of the triple product L-function. Gross and Kudla [76, Proposition 10.8] give a description of the algebraic quantity A_F in terms of the height of a "cycle" on the triple product of the definite Shimura curve $X_{1,p}$ in the notation of [10], which we will now describe. The curve $X_{1,p}$ is not the one obtained from the canonical construction of Shimura curves. The construction we give below is originally due to Gross [74, p. 131].

Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Let $\hat{\mathbb{Z}} = \prod_{l \neq \infty} \mathbb{Z}_l$ denote the profinite completion of $\mathbb{Z}$ and let $\hat{\mathbb{Q}} := \hat{\mathbb{Z}} \otimes \mathbb{Q}$. We set $\hat{B} := B \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}$ and for each place l of $\mathbb{Q}$ we let $B_l := B \otimes \mathbb{Q}_l$. For any prime $\ell \neq p$ we identify B_ℓ with $M_2(\mathbb{Q}_\ell)$ and for $l = p, \infty$ we let R_l denote the unique maximal order of B_l. Then

$$R := B \cap \left(\prod_{\ell \neq p, \infty} M_2(\mathbb{Z}_\ell) \times R_p \times R_\infty \right)$$

is a maximal order of B. One associates to the datum (B, R) a Shimura curve $X_{1,p}$ which is a complete algebraic curve over $\mathbb{Q}$ and may be described as the double coset space

$$X_{1,p} = \hat{R} \setminus (\hat{B}^\times \times Y) \,/\, B^\times$$

where Y is the genus zero curve defined over $\mathbb{Q}$ with the property that

$$Y(K) = \{x \in B \otimes K \mid \mathrm{norm}(x) = \mathrm{trace}(x) = 0\}$$

for every $\mathbb{Q}$-algebra K.

The cardinality of the double coset space $\hat{R} \setminus \hat{B}^\times \,/\, B^\times$ is called the class number of B (it is independent of the choice of R) and is given by

$$h(B) := |\hat{R} \setminus \hat{B}^\times \,/\, B^\times| = g + 1,$$

where g denotes the genus of the modular curve $X_0(p)$ given by (1.18).

Let $\{x_0, \ldots, x_g\}$ be a set of representatives of this double coset space and define, for each $i \in \{0, 1, \ldots, g\}$, the maximal order $R_i := B \cap x_i^{-1} \hat{R} x_i$ of B, along with the finite subgroup $\Gamma_i := R_i^\times / \langle \pm 1 \rangle$ of $B^\times / \langle \pm 1 \rangle$ and the associated curve $Y_i := Y / \Gamma_i$ over $\mathbb{Q}$ of genus zero. Each conjugacy class of maximal orders in B is represented once or twice in $\{R_0, \ldots, R_g\}$. The number of distinct conjugacy classes of maximal orders in B is called the type number of B. We have the identification

$$X_{1,p} = \bigsqcup_{i=0}^{g} Y_i,$$

and the group $\mathrm{Pic}(X_{1,p})$ of divisor classes is a free abelian group of rank $g+1$ isomorphic to

$$\mathrm{Pic}(X_{1,p}) = \mathbb{Z}\epsilon_0 \oplus \ldots \oplus \mathbb{Z}\epsilon_g, \tag{4.16}$$

where ϵ_i corresponds to the class generated by a single point supported on Y_i.

Let S denote the set of isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$. It has cardinality $g+1$ and we may order it as $S = \{E_0, \ldots, E_g\}$ where $\mathrm{End}(E_i) = R_i$ for each $i \in \{0, 1, \ldots, g\}$. We can then define, for $i \in \{0, 1, \ldots, g\}$, the integer

$$w_i := |\Gamma_i| = \frac{\#\,\mathrm{Aut}(E_i)}{2}. \tag{4.17}$$

Note that two maximal orders R_i and R_j are conjugate if and only if E_i and E_j are conjugate by an automorphism of $\bar{\mathbb{F}}_p$, which is the case if and only if $i = j$ or $E_i^{(p)} \cong E_j$.

Remark 4.9. Let $i \in \{0, 1, \ldots, g\}$. If $j(E_i) = 0$, then $w_i = 3$. This happens if and only if $p \equiv 5, 11 \pmod{12}$. If $j(E_i) = 1728$, then $w_i = 2$. This happens if and only if $p \equiv 7, 11 \pmod{12}$. Otherwise $w_i = 1$. This is explained for instance in [54, §0.1].

By the Jacquet–Langlands correspondence [92], as formulated in [10, Theorem 1.2], the newform f_j, for $j \in \{1, 2, 3\}$, gives rise to an algebra homomorphism $\phi_{f_j} : \mathbb{T}_{1,p} \longrightarrow \mathcal{O}_{f_j}$ satisfying

$$\phi_{f_j}(w_p^-) = a_p(f_j) \qquad \text{and} \qquad \phi_{f_j}(T_\ell) = a_\ell(f_j) \text{ for all } \ell \neq p.$$

Here $\mathbb{T}_{1,p}$ is the Hecke algebra generated by the Hecke operators T_ℓ ($\ell \neq p$) and the Atkin–Lehner involution w_p^- acting on $X_{1,p}$. See [10, §1.5]. By multiplicity one, there corresponds to f_j a unique line $\mathbb{R}a_{f_j}$ in $\mathrm{Pic}(X_{1,p}) \otimes_{\mathbb{Z}} \mathbb{R}$ such that

$$w_p^-(a_{f_j}) = a_p(f_j)a_{f_j} \qquad \text{and} \qquad T_\ell(a_{f_j}) = a_\ell(f_j)a_{f_j} \text{ for all } \ell \neq p.$$

(This is the formulation of the Jacquet–Langlands correspondence employed in [76, Proposition 10.2]). We express the eigenvector a_{f_j} in the basis (4.16)

$$a_{f_j} = \sum_{i=0}^{g} \lambda_i(f_j)\epsilon_i,$$

with coefficients $\lambda_i(f_j)$ lying in the totally real field K_{f_j} and uniquely determined up to a scalar. As noted in [76, p. 202], we have $\sum_{i=0}^{g} \lambda_i(f_j) = 0$ since f_j is a cusp form; indeed, cusp forms are orthogonal to the Eisenstein class $a_E := \sum_{i=0}^{g} \frac{1}{w_i}\epsilon_i$ with respect to the paring $\langle \epsilon_i, \epsilon_j \rangle = \delta_{ij}w_i$ on $\mathrm{Pic}(X_{1,p})$. The following result is proved in [76, Proposition 10.8] and will be referred to as the Gross–Kudla formula.

Theorem 4.1 (Gross–Kudla)**.**

$$\frac{L(F,2)}{\Omega_F} = \frac{\left(\sum_i w_i^2 \lambda_i(f_1)\lambda_i(f_2)\lambda_i(f_3)\right)^2}{\prod_{j=1}^{3}\left(\sum_i w_i \lambda_i(f_j)^2\right)}.$$

The case $W(F) = -1$

Suppose in this section that $W(F) = -1$, i.e., that $L(F,s)$ vanishes to odd order at its centre $s = 2$. Recall the projector t_F of (4.9) and the Beilinson–Bloch conjecture (4.14). In particular, under the assumption $W(F) = -1$, we expect the F-isotypic component of $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes K_F$ to have dimension greater or equal to 1.

A natural element of $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ to consider is the modified diagonal cycle, also referred to as the Gross–Kudla–Schoen cycle. Let Δ denote the image of $X_0(p)$ under the diagonal embedding $X_0(p) \longrightarrow X_0(p)^3$, i.e.,

$$\Delta = \{(x,x,x) \mid x \in X_0(p)\} \subset X_0(p)^3. \tag{4.18}$$

In order to get a null-homologous cycle, we apply a certain projector to Δ, originally defined in [77].

Definition 4.4. Let X be a smooth projective geometrically connected curve over a number field k and let e be a k-rational point of X. For any non-empty subset T of $\{1,2,3\}$, let T' denote the complementary set. Write $p_T : X^3 \longrightarrow X^{|T|}$ for the natural projection map and let $q_T(e) : X^{|T|} \longrightarrow X^3$ denote the inclusion obtained by filling in the missing coordinates using the point e. Let $P_T(e)$ denote the graph of the morphism $q_T(e) \circ p_T : X^3 \longrightarrow X^3$ viewed as a codimension 3 cycle on the product $X^3 \times X^3$. Define the Gross–Kudla–Schoen projector

$$P_{\mathrm{GKS}}(e) := \sum_T (-1)^{|T'|} P_T(e) \in \mathrm{CH}^3(X^3 \times X^3),$$

where the sum is taken over all subsets of $\{1,2,3\}$. This is an idempotent in the ring of correspondences of X^3 by [77, Proposition 2.3] with the property that it annihilates the cohomology groups $H^i(X^3(\mathbb{C}),\mathbb{Z})$ for $i \in \{4,5,6\}$ and maps $H^3(X^3(\mathbb{C}),\mathbb{Z})$ onto the Künneth summand $H^1(X(\mathbb{C}),\mathbb{Z})^{\otimes 3}$ by [77, Corollary 2.6].

Definition 4.5. Let $e \in X_0(p)(\mathbb{Q})$ be a rational point. The Gross–Kudla–Schoen cycle with base point e is defined as

$$\Delta_{\mathrm{GKS}}(e) := P_{\mathrm{GKS}}(e)_*(\Delta) \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}).$$

Note that $\Delta_{\mathrm{GKS}}(e)$ is null-homologous as $P_{\mathrm{GKS}}(e)$ annihilates $H^4_B(X_0(p)^3,\mathbb{Z})$, i.e., the target of the cycle class map cl^2_B of (1.43). When e is the cusp ξ_∞ of $X_0(p)$ at infinity, we shall simply write $\Delta_{\mathrm{GKS}} := \Delta_{\mathrm{GKS}}(\xi_\infty)$.

Gross and Kudla [76, Conjecture 13.2] conjectured the following formula:

$$\frac{L'(F,2)}{\Omega_F} = \langle (t_F)_*(\Delta_{\mathrm{GKS}}), (t_F)_*(\Delta_{\mathrm{GKS}}) \rangle^{BB}, \tag{4.19}$$

where $\langle\ ,\ \rangle^{BB} : \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes \mathbb{R} \times \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes \mathbb{R} \longrightarrow \mathbb{R}$ is the Beilinson–Bloch height pairing [76, (13.9)]. A proof due to Yuan, Zhang and Zhang has been announced in [154] but has not yet appeared in print.

4.1.3 Triple product Chow–Heegner points

Let f be a normalised newform in $S_2(\Gamma_0(p))$ with rational coefficients, and let E_f be the elliptic curve associated to f by the Eichler–Shimura construction. In particular, there is a quotient map

$$\pi_f : J_0(p) \longrightarrow E_f,$$

induced by the idempotent correspondence t_f in $\mathrm{Corr}^0(X_0(p), X_0(p))_{\mathbb{Q}}$ of Section 4.1.1. In this special case of rational coefficients, note that $E_f = M(f) = M([f]) = (X_0(p), t_f, 0)$.

Remark 4.10. To the best of the authors knowledge, it is unknown whether there are finitely or infinitely many elliptic curves over $\mathbb{Q}$ with a prime conductor. It is a result of Setzer [134, Theorem 2] that given a prime p distinct from $2, 3$ and 17, there is an elliptic curve of conductor p over $\mathbb{Q}$ with a rational 2-torsion point if and only if $p = u^2 + 64$ for some rational integer u. A conjecture of Hardy and Littlewood [81, Conjecture F] implies that there are infinitely many values of u such that $u^2 + 64$ is prime. Thus, conditionally on this conjecture of Hardy and Littlewood, there are infinitely many primes p which occur as the conductor of an elliptic curve over $\mathbb{Q}$. This is explained in detail in the preprint [87].

Let g be a choice of auxiliary normalised newform in $S_2(\Gamma_0(p))$ such that g is not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f. Recall the idempotent correspondence $t_{[g]} \in \mathrm{Corr}^0(X_0(p), X_0(p))_{\mathbb{Q}}$ which cuts out the motive $M([g]) = (X_0(p), t_{[g]}, 0) = A_{[g]}$. Consider the correspondence

$$\Pi_{[g]} := \mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(\Delta) \in \mathrm{CH}^2(X_0(p)^4)(\mathbb{Q}) \otimes \mathbb{Q},$$

where $\Delta \in \mathrm{CH}^1(X_0(p)^2)(\mathbb{Q})$ is the diagonal cycle. After clearing denominators, we may and will consider $\Pi_{[g]}$ as an element of $\mathrm{Corr}^{-1}(X_0(p)^3, X_0(p))$, which thus induces, by (1.40), a map of Chow groups

$$\Pi_{[g],*} : \mathrm{CH}^2(X_0(p)^3)_0(L) \longrightarrow \mathrm{CH}^1(X_0(p))_0(L) = J_0(p)(L)$$

for any field extension L of $\mathbb{Q}$. By composing correspondences, using (1.42), we can define

$$\Pi_{[g],f} := \Pi_{[g]} \circ t_f = \mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_f) \in \mathrm{Corr}^{-1}(X_0(p)^3, E_f). \tag{4.20}$$

This induces, in the terminology of Section 0.2.2, a generalised modular parametrisation

$$\Pi_{[g],f,*} = \pi_f \circ \Pi_{[g],*} : \mathrm{CH}^2(X_0(p)^3)_0(L) \longrightarrow E_f(L)$$

for any field extension L of $\mathbb{Q}$.

Remark 4.11. Instead of defining the correspondence $\Pi_{[g]}$ as $\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(\Delta)$, one could alternatively propose to use $\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_{[g]})$. One checks that

$$\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_{[g]}) = (\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(\Delta)) \circ t_{[g]},$$

hence $(\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_{[g]})) \circ t_f = (\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(\Delta)) \circ (t_{[g]} \circ t_f)$. But f and g are not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugates, hence $\pi_f \circ \pi_{[g]} = 0$ in $\mathrm{End}_{\mathbb{Q}}^0(J_0(p))$. In particular, the generalised modular parametrisation $((\mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_{[g]})) \circ t_f)_* : \mathrm{CH}^2(X_0(p)^3)_0 \longrightarrow E_f$ is the zero map in this case.

Using the three ingredients (or three pillars of the BSD strategy as they are referred to in Section 0.2.2) – the modular parametrisation $\Pi_{[g],f,*}$, the cycle $\Delta_{\mathrm{GKS}} \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$, and the conjectural formula (4.19) of Gross and Kudla (see [51, Theorem 3.5] for a precise formulation in the present setup) – Darmon, Rotger and Sols [51, Theorem 3.7] have proved the following concerning the Chow–Heegner point

$$P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}) := \Pi_{[g],f,*}(\Delta_{\mathrm{GKS}}) = \pi_f(\Pi_{[g],*}(\Delta_{\mathrm{GKS}})) \in E_f(\mathbb{Q}), \tag{4.21}$$

by building on the work of Yuan, Zhang and Zhang:

Theorem 4.2 (Darmon–Rotger–Sols)**.** *Assume that* $W(f) = -1$ *and* $W(\mathrm{Sym}^2 g \otimes f) = +1$. *Then* $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}})$ *has infinite order in* $E_f(\mathbb{Q})$ *if and only if*

$$\mathrm{ord}_{s=1} L(f,s) = 1 \qquad \textit{and} \qquad \mathrm{ord}_{s=2} L(\mathrm{Sym}^2(g^\sigma) \otimes f, s) = 0, \ \forall \sigma : K_g \hookrightarrow \mathbb{C}.$$

Remark 4.12. Note that the triple product L-function attached to (g, g, f) decomposes as

$$L(g, g, f, s) = L(f, s-1)L(\mathrm{Sym}^2 g \otimes f, s),$$

and therefore the assumptions of the theorem imply in particular that $W(g, g, f) = -1$.

4.2 Cycle constructions

Let $\Delta(p)$ be the curve that fits into the Cartesian diagram

$$\begin{array}{ccc} \Delta(p) & \hookrightarrow & X_0(p)^3 \\ \downarrow & \square & \downarrow \\ \Delta & \hookrightarrow & X(1)^3. \end{array}$$

We will systematically study the cycles in $\mathrm{CH}^2(X_0(p)^3)$ arising as components of $\Delta(p)$. We will describe all such cycles as images under maps $X(p) \longrightarrow X_0(p)^3$, where $X(p)$ denotes the (component of) the modular curve $\bar{M}_p$ described in Section 1.2.2. We then focus on making null-homologous variants of these cycles.

4.2.1 Diagonal type cycles on $X_1(p)^3$

Throughout this section we will assume that $p > 3$. Recall from Section 1.2.2 that $\bar{M}_p$ denotes the fine moduli scheme representing pairs (E, α_p) consisting of a generalised elliptic curve E together with a full level p structure $\alpha_p : E[p] \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^2$. It is a smooth proper curve over $\mathbb{Q}$, whose base change to $\mathbb{Q}(\zeta_p)$ is the disjoint union of $p-1$ geometrically connected smooth proper curves $X^j(p)$ with $j \in \{1, \dots, p-1\}$. The curve $X^j(p)$ classifies pairs $(E, (P, Q))$, where (P, Q) is a basis of $E[p]$ satisfying $e_p(P, Q) = \zeta_p^j$.

Let $x_i = (a_i, b_i) \in \mathbb{F}_p^2 \setminus \{(0,0)\}$ for $i \in \{1, 2, 3\}$ and consider the map

$$\widetilde{\varphi}_{(x_1,x_2,x_3)} : \bar{M}_p \longrightarrow X_1(p)^3, \qquad (E, (P, Q)) \mapsto ((E, a_1P+b_1Q), (E, a_2P+b_2Q), (E, a_3P+b_3Q)),$$

defined over $\mathbb{Q}$. After base changing to $\mathbb{Q}(\zeta_p)$, one may restrict this map to each of the $p-1$ connected components of $\bar{M}_p$, yielding morphisms, for each $j \in \mathbb{F}_p^\times$, of geometrically connected smooth proper curves over $\mathbb{Q}(\zeta_p)$

$$\widetilde{\varphi}^j_{(x_1,x_2,x_3)} : X^j(p) \longrightarrow X_1(p)^3.$$

Denote by $\widetilde{\Delta}^j_{(x_1,x_2,x_3)} := \widetilde{\varphi}^j_{(x_1,x_2,x_3)}(X^j(p))$ the image of $X^j(p)$ under this map. This is a cycle of codimension 2 on $X_1(p)^3$ defined over $\mathbb{Q}(\zeta_p)$ and we shall consider its image in $\mathrm{CH}^2(X_1(p)^3)(\mathbb{Q}(\zeta_p))$, which we will denote again by $\widetilde{\Delta}^j_{(x_1,x_2,x_3)}$ by slight abuse of notation. So far we have produced a collection

$$\widetilde{\mathcal{C}} := \left\{ \widetilde{\Delta}^j_{(x_1,x_2,x_3)} : (x_1, x_2, x_3) \in (\mathbb{F}_p^2 \setminus \{(0,0)\})^3, j \in \mathbb{F}_p^\times \right\} \subset \mathrm{CH}^2(X_1(p)^3)(\mathbb{Q}(\zeta_p))$$

which inherits from $\bar{M}_p$ and $X_1(p)^3$ various actions of groups, which we will now define and study.

Action of the group $\mathbf{SL}_2(\mathbb{F}_p)$

There is a natural left action of the group $\mathbf{SL}_2(\mathbb{F}_p)$ on $\bar{M}_p$, as can be seen, using the moduli interpretation, as follows: if $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{F}_p)$, then

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \cdot (E,(P,Q)) := (E,(\alpha P + \beta Q, \gamma P + \delta Q)).$$

Because the determinant is one, the Weil pairing on the basis is preserved, and thus the connected components of $\bar{M}_p \otimes \mathbb{Q}(\zeta_p)$ are stable under this action. The above action naturally induces a right action of $\mathbf{SL}_2(\mathbb{F}_p)$ on the set $\widetilde{\mathcal{C}}$ via

$$\widetilde{\Delta}^j_{x_1,x_2,x_3} \cdot \kappa := \widetilde{\varphi}^j_{(x_1,x_2,x_3)} \circ \kappa(X^j(p)),$$

but since $\mathbf{SL}_2(\mathbb{F}_p)$ acts by automorphisms this action is the trivial one. An easy calculation reveals that

$$\widetilde{\Delta}^j_{(x_1,x_2,x_3)} \cdot \kappa = \widetilde{\Delta}^j_{(x_1,x_2,x_3)\cdot\kappa}$$

where the right action of $\mathbf{SL}_2(\mathbb{F}_p)$ on the set $(\mathbb{F}_p^2 \setminus \{(0,0)\})^3$ is defined as follows. Let $\kappa = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{F}_p)$ and $(x_1,x_2,x_3) \in (\mathbb{F}_p^2 \setminus \{(0,0)\})^3$ with $x_i = (a_i,b_i)$, $i = 1,2,3$, then write the vector (x_1,x_2,x_3) as a 3×2 matrix and multiply on the right by κ:

$$\begin{aligned}(x_1,x_2,x_3)\cdot\kappa :&= \begin{pmatrix}a_1 & b_1\\ a_2 & b_2\\ a_3 & b_3\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\\ &= ((a_1\alpha + b_1\gamma, a_1\beta + b_1\delta),(a_2\alpha + b_2\gamma, a_2\beta + b_2\delta),(a_3\alpha + b_3\gamma, a_3\beta + b_3\delta)).\end{aligned}$$

It follows that the indexing set of the cycles can be taken to be

$$\widetilde{I} := (\mathbb{F}_p^2 \setminus \{(0,0)\})^3 / \mathbf{SL}_2(\mathbb{F}_p).$$

We shall write $[x_1, x_2, x_3]$ for the image of (x_1, x_2, x_3) in $\widetilde{I}$. Thus we have

$$\widetilde{\mathcal{C}} = \left\{ \widetilde{\Delta}^j_{(x_1,x_2,x_3)} : [x_1, x_2, x_3] \in \widetilde{I}, j \in \mathbb{F}_p^\times \right\}.$$

To understand the set $\widetilde{I}$ we introduce a determinant map

$$\mathrm{Det} : \widetilde{I} \longrightarrow (\mathbb{F}_p)^3$$

defined as follows. If (x_1, x_2, x_3) is a representative of a class in $\widetilde{I}$ with $x_i = (a_i, b_i)$ for $i \in \{1, 2, 3\}$, then

$$\mathrm{Det}([x_1, x_2, x_3]) := \left(\begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix}, \begin{vmatrix} a_3 & b_3 \\ a_1 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \right).$$

This map is well-defined as follows from the definition of the action of $\mathbf{SL}_2(\mathbb{F}_p)$.

Lemma 4.1. *The map* Det *is surjective.*

Proof. Start by observing that $\mathrm{Det}([(1,0),(1,0),(1,0)]) = (0,0,0)$. Now, let $(a,b,c) \in (\mathbb{F}_p)^3$ be non-zero, and suppose that $a \neq 0$ so that $a \in \mathbb{F}_p^\times$. Then

$$\mathrm{Det}([(-b, -(c+b)a^{-1}), (a,1), (0,1)]) = (a,b,c).$$

The cases when $b \neq 0$ or $c \neq 0$ are treated similarly. □

The map Det is however not injective as we will see shortly. Consider the following three subsets of $\widetilde{I}$:

$$\widetilde{I}_0 := \mathrm{Det}^{-1}((0,0,0)), \qquad \widetilde{I}_1 := \widetilde{I} \setminus \widetilde{I}_0, \qquad \widetilde{I}^\times := \mathrm{Det}^{-1}((\mathbb{F}_p^\times)^3) \subset \widetilde{I}_1.$$

Remark 4.13. Let $[x_1, x_2, x_3] \in \widetilde{I}$ and suppose that $\mathrm{Det}([x_1, x_2, x_3])$ has two coordinates equal to zero, say the first two. Since the first entry is zero, the vectors x_2 and x_3 are linearly dependent and since the second entry is zero, x_1 and x_3 are linearly dependent. Thus x_1 and x_2 are linearly dependent which implies that the last entry is also zero. The same reasoning applies whenever two coordinates are zero and shows that in that case we necessarily have $[x_1, x_2, x_3] \in \widetilde{I}_0$. In other words, $\widetilde{I}_1 \setminus \widetilde{I}^\times$ consists of those classes $[x_1, x_2, x_3]$ for which one and only one coordinate of $\mathrm{Det}([x_1, x_2, x_3])$ is zero.

Lemma 4.2. *The set $\widetilde{I}_0$ has cardinality equal to $(p-1)^2$. In particular, the map* Det *is not injective.*

Proof. Let $[x_1, x_2, x_3] \in \widetilde{I}_0$ and let $x_i = (a_i, b_i)$ for $i = 1, 2, 3$. Up to multiplying on the right by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ we may assume without loss of generality that $a_1 \neq 0$. Multiplying on the right by $\begin{pmatrix} a_1^{-1} & 0 \\ 0 & a_1 \end{pmatrix}$ we obtain the vector $((1, a_1b_1), (a_1^{-1}a_2, a_1b_2), (a_1^{-1}a_3, a_1b_3))$. Multiplying on the right by the matrix $\left(\begin{smallmatrix} 1 & -a_1b_1 \\ 0 & 1 \end{smallmatrix}\right)$ we obtain the vector

$$((1,0), (a_1^{-1}a_2, -a_2b_1 + a_1b_2), (a_1^{-1}a_3, -a_3b_1 + a_1b_3)) = ((1,0), (a_1^{-1}a_2, 0), (a_1^{-1}a_3, 0))$$

where we used the fact that $[x_1, x_2, x_3] \in I_0$. We conclude that

$$[x_1, x_2, x_3] = [(1,0), (a_1^{-1}a_2, 0), (a_1^{-1}a_3, 0)].$$

This proves that any $[x_1, x_2, x_3] \in \widetilde{I}_0$ admits a representative of the form $((1,0), (n,0), (m,0))$ where $n, m \in \mathbb{F}_p^\times$. Moreover, if $[(1,0), (n,0), (m,0)] = [(1,0), (n',0), (m',0)]$, then there exists $\kappa = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{F}_p)$ such that

$$((1,0), (n,0), (m,0)) \cdot \kappa = ((\alpha, \beta), (n\alpha, n\beta), (m\alpha, m\beta)) = ((1,0), (n',0), (m',0))$$

which implies that $\alpha = 1, \beta = 0$ and thus $n = n'$ and $m = m'$. We conclude that any $[x_1, x_2, x_3] \in \widetilde{I}_0$ admits a unique representative of the form $((1,0), (n,0), (m,0))$ where n and m belong to $\mathbb{F}_p^\times$. Thus $\widetilde{I}_0$ is in bijection with $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ and the lemma is proved. ◻

Lemma 4.3. *When restricted to $\widetilde{I}_1$, the map* Det *is injective. In particular, the set $\widetilde{I}_1$ has* *cardinality* $(p+2)(p-1)^2$*, and the set* $\widetilde{I}^\times$ *is in bijection with* $(\mathbb{F}_p^\times)^3$ *of cardinality* $(p-1)^3$*.*

Proof. Let $[x_1, x_2, x_3] \in \widetilde{I}_1$ with $x_i = (a_i, b_i)$, for $i = 1, 2, 3$. Then at least one entry of $\mathrm{Det}([x_1, x_2, x_3])$ is non-zero. Let us assume that $\left|\begin{smallmatrix} a_1 & b_1 \\ a_2 & b_2 \end{smallmatrix}\right| = n \neq 0$ in $\mathbb{F}_p$. The other cases are treated similarly. Then $\kappa := \left(\begin{smallmatrix} a_1 & b_1 \\ a_2 & b_2 \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{F}_p)$ and by multiplying on the right by κ, we obtain $[x_1, x_2, x_3] = [(n, 0), (0, 1), (a_3', b_3')]$ where $a_3' = -\left|\begin{smallmatrix} a_2 & b_2 \\ a_3 & b_3 \end{smallmatrix}\right|$ and $b_3' = -n^{-1}\left|\begin{smallmatrix} a_3 & b_3 \\ a_1 & b_1 \end{smallmatrix}\right|$. Hence $[x_1, x_2, x_3] \in \widetilde{I}_1$ is completely determined by $\mathrm{Det}([x_1, x_2, x_3])$. □

It is natural to express the collection $\widetilde{\mathcal{C}}$ of cycles as the disjoint union of the two sets $\widetilde{\mathcal{C}}_0$ and $\widetilde{\mathcal{C}}_1$ consisting of cycles indexed by $\widetilde{I}_0$ and $\widetilde{I}_1$, respectively. We will also use the notation $\widetilde{\mathcal{C}}^\times$ to denote the collection of cycles indexed by $\widetilde{I}^\times$. In view of the preceding two lemmas, we will adopt the following simplified notations. If $[x_1, x_2, x_3] \in \widetilde{I}_0$ corresponds to the class $[(1, 0), (n, 0), (m, 0)]$ then we write $\widetilde{\Delta}^j_{(n,m)} := \widetilde{\Delta}^j_{(x_1,x_2,x_3)}$ where $j \in \mathbb{F}_p^\times$. If $[x_1, x_2, x_3] \in \widetilde{I}_1$ with $\mathrm{Det}([x_1, x_2, x_3]) = (a, b, c)$, then we write $\widetilde{\Delta}^j_{a,b,c} := \widetilde{\Delta}^j_{(x_1,x_2,x_3)}$ where $j \in \mathbb{F}_p^\times$. We then have the descriptions

$$\begin{cases} \widetilde{\mathcal{C}}_0 = \left\{ \widetilde{\Delta}^j_{(n,m)} : n, m, j \in \mathbb{F}_p^\times \right\} \\ \widetilde{\mathcal{C}}_1 = \left\{ \widetilde{\Delta}^j_{a,b,c} : a, b, c \in \mathbb{F}_p, j \in \mathbb{F}_p^\times, (a, b, c) \neq (0, 0, 0) \right\}. \end{cases}$$

Lemma 4.4. *For all* $j \in \mathbb{F}_p^\times$*, the following holds:*

i) $\widetilde{\Delta}^j_{(n,m)} = \widetilde{\Delta}^1_{(n,m)}$ *for all* $n, m \in \mathbb{F}_p^\times$*.*

ii) $\widetilde{\Delta}^j_{a,b,c} = \widetilde{\Delta}^1_{ja,jb,jc}$ *for all* $a, b, c \in \mathbb{F}_p$ *with* $(a, b, c) \neq (0, 0, 0)$*.*

Proof. Observe that if $[x_1, x_2, x_3] \in \widetilde{I}$ with $x_i = (a_i, b_i)$ for $i = 1, 2, 3$, then

$$\begin{aligned} \widetilde{\Delta}^j_{(x_1,x_2,x_3)} &= \{(E, a_iP + b_iQ)_{i=1,2,3} : e_p(P, Q) = \zeta_p^j\} \\ &= \{(E, ja_i(j^{-1}P) + b_iQ)_{i=1,2,3} : e_p(P, Q) = \zeta_p^j\} \\ &= \{(E, ja_iP' + b_iQ)_{i=1,2,3} : e_p(P', Q) = \zeta_p\} \\ &= \widetilde{\Delta}^1_{((ja_1,b_1),(ja_2,b_2),(ja_3,b_3))}, \end{aligned}$$

by bilinearity of the Weil pairing.

If $[x_1, x_2, x_3] \in \widetilde{I}_0$ is represented by $((1,0),(n,0),(m,0))$ then

$$[(ja_1, b_1), (ja_2, b_2), (ja_3, b_3)] = [(j, 0), (jn, 0), (jm, 0)] = [(1, 0), (n, 0), (m, 0)] = [x_1, x_2, x_3].$$

If $[x_1, x_2, x_3] \in \widetilde{I}_1$ has determinant (a, b, c) then $(ja_1, b_1), (ja_2, b_2), (ja_3, b_3)$ has determinant (ja, jb, jc). □

We conclude that it suffices to consider cycles coming only from the component $X^1(p)$. From now on we shall write $X(p)$ for $X^1(p)$ and $\widetilde{\Delta}_{(x_1,x_2,x_3)}$ for $\widetilde{\Delta}^1_{(x_1,x_2,x_3)}$. To summarise, we have $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}_0 \sqcup \widetilde{\mathcal{C}}_1$ with

$$\begin{cases} \widetilde{\mathcal{C}}_0 = \left\{ \widetilde{\Delta}_{(n,m)} : n, m \in \mathbb{F}_p^\times \right\} \\ \widetilde{\mathcal{C}}_1 = \left\{ \widetilde{\Delta}_{a,b,c} : a, b, c \in \mathbb{F}_p, (a, b, c) \neq (0, 0, 0) \right\}. \end{cases}$$

Action of the diamond operators

The modular curve $X_1(p)$ carries a natural left action of the group $\mathbb{F}_p^\times$ via the so-called diamond operators. If $d \in \mathbb{F}_p^\times$, then in terms of the modular description one defines

$$\langle d \rangle \cdot (E, P) = (E, dP).$$

This action naturally extends to the closed curve and is defined over $\mathbb{Q}$. We get an induced action of $(\mathbb{F}_p^\times)^3$ on the triple product $X_1(p)^3$ described by

$$\langle d_1, d_2, d_3 \rangle \cdot ((E_1, P_1), (E_2, P_2), (E_3, P_3)) = ((E_1, d_1P_1), (E_2, d_2P_2), (E_3, d_3P3)).$$

This in turn induces a left action of $(\mathbb{F}_p^\times)^3$ on the collection of cycles $\widetilde{\mathcal{C}}$ via

$$\langle d_1, d_2, d_3 \rangle \cdot \widetilde{\Delta}_{(x_1,x_2,x_3)} := \langle d_1, d_2, d_3 \rangle \circ \widetilde{\varphi}_{(x_1,x_2,x_3)}(X(p)),$$

and this action preserves the subsets $\widetilde{\mathcal{C}}_0$ and $\widetilde{\mathcal{C}}_1$. Let $[x_1, x_2, x_3] \in \widetilde{I}$ with $x_i = (a_i, b_i)$ for $i = 1, 2, 3$. If $d_1, d_2, d_3 \in \mathbb{F}_p^\times$, then

$$\langle d_1, d_2, d_3 \rangle \circ \widetilde{\varphi}_{(x_1,x_2,x_3)} = \widetilde{\varphi}_{((d_1a_1,d_1b_1),(d_2a_2,d_2b_2),(d_3a_3,d_3b_3))} = \widetilde{\varphi}_{(d_1x_1,d_2x_2,d_3x_3)}. \tag{4.22}$$

Lemma 4.5. *Let $d_1, d_2, d_3 \in \mathbb{F}_p^\times$.*

i) $\langle d_1, d_2, d_3 \rangle \cdot \widetilde{\Delta}_{(n,m)} = \widetilde{\Delta}_{(d_1^{-1}d_2n, d_1^{-1}d_3m)}$ *for all $n, m \in \mathbb{F}_p^\times$.*

ii) $\langle d_1, d_2, d_3 \rangle \cdot \widetilde{\Delta}_{a,b,c} = \widetilde{\Delta}_{d_2d_3a, d_1d_3b, d_1d_2c}$ *for all $a, b, c \in \mathbb{F}_p$ with $(a, b, c) \neq (0, 0, 0)$.*

Proof. From (4.22) we see that $\langle d_1, d_2, d_3 \rangle \cdot \widetilde{\Delta}_{(n,m)} = \widetilde{\Delta}_{((d_1,0),(d_2n,0),(d_3m,0))}$ and $i)$ follows after observing that $[(d_1, 0), (d_2n, 0), (d_3m, 0)] = [(1, 0), (d_1^{-1}d_2n, 0), (d_1^{-1}d_3m, 0)]$.

Let $[x_1, x_2, x_3] \in \widetilde{I}_1$ with determinant (a, b, c). Then $ii)$ follows from the fact that the determinant of $[d_1x_1, d_2x_2, d_3x_3]$ is $(d_2d_3a, d_1d_3b, d_1d_2c)$. □

The following three corollaries describe the action of the diamond operators on the sets $\widetilde{\mathcal{C}}_0$, $\widetilde{\mathcal{C}}_1 \setminus \widetilde{\mathcal{C}}^\times$ and $\widetilde{\mathcal{C}}^\times$ respectively and are easy consequences of the above lemma.

Corollary 4.1. *The action of $(\mathbb{F}_p^\times)^3$ on $\widetilde{\mathcal{C}}_0$ via diamond operators is transitive and the stabiliser of any element is given by the set of triples (d, d, d) for $d \in \mathbb{F}_p^\times$.*

Corollary 4.2. *Concerning the action of the diamond operators on $\widetilde{\mathcal{C}}_1 \setminus \widetilde{\mathcal{C}}^\times$, the following holds:*

i) $\mathrm{orb}_\diamond(\widetilde{\Delta}_{0,1,1}) = \mathrm{Det}^{-1}(0 \times \mathbb{F}_p^\times \times \mathbb{F}_p^\times)$ *and* $\mathrm{stab}_\diamond(0, 1, 1) = \{(d^{-1}, d, d) : d \in \mathbb{F}_p^\times\}$.

ii) $\mathrm{orb}_\diamond(\widetilde{\Delta}_{1,0,1}) = \mathrm{Det}^{-1}(\mathbb{F}_p^\times \times 0 \times \mathbb{F}_p^\times)$ *and* $\mathrm{stab}_\diamond(1, 0, 1) = \{(d, d^{-1}, d) : d \in \mathbb{F}_p^\times\}$.

iii) $\mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,0}) = \mathrm{Det}^{-1}(\mathbb{F}_p^\times \times \mathbb{F}_p^\times \times 0)$ *and* $\mathrm{stab}_\diamond(1, 1, 0) = \{(d, d, d^{-1}) : d \in \mathbb{F}_p^\times\}$.

Corollary 4.3. *We have*

$$\mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,1}) = \left\{ \widetilde{\Delta}_{a,b,c} \mid a, b, c \in \mathbb{F}_p^\times,\ abc \in (\mathbb{F}_p^\times)^{(2)} \right\}.$$

Here $(\mathbb{F}_p^\times)^{(2)}$ *denotes the set of quadratic residues modulo* p *and thus the orbit of* $\widetilde{\Delta}_{1,1,1}$ *has size* $\frac{(p-1)^3}{2}$. *The stabiliser of* $\widetilde{\Delta}_{1,1,1}$ *for this action is given by* $\{\langle 1,1,1\rangle, \langle -1,-1,-1\rangle\}$. *As a consequence, there are* 2 *orbits for the action of the diamond operators on* $\widetilde{\mathcal{C}}^\times$*:*

$$\widetilde{\mathcal{C}}^\times = \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,1}) \sqcup \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,a}),$$

where $a \in \mathbb{F}_p^\times$ *is a choice of a non-quadratic residue modulo* p*.*

Action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$

As already mentioned, the cycles in the collection $\widetilde{\mathcal{C}}$ are defined over the cyclotomic field $\mathbb{Q}(\zeta_p)$. We identify $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\mathbb{F}_p^\times$ so that the element of the Galois group σ_i indexed by $i \in \mathbb{F}_p^\times$ raises ζ_p to the i-th power. We now investigate the action of this Galois group on the cycles in $\widetilde{\mathcal{C}}$.

Recall that the curve $\bar{M}_p$ is defined over $\mathbb{Q}$. When base changed to $\mathbb{Q}(\zeta_p)$, the Galois group of $\mathbb{Q}(\zeta_p)$ permutes the $p-1$ connected components $X^j(p)$ of this curve transitively. This can be seen from the moduli description of these components and the Galois equivariance of the Weil pairing. Using this, we can define a right action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ on $\widetilde{\mathcal{C}}$ by

$$\widetilde{\Delta}^{\sigma_i}_{(x_1,x_2,x_3)} := \widetilde{\varphi}_{(x_1,x_2,x_3)}(\sigma_i(X(p))).$$

The element σ_i maps the component $X(p)$ to $X^i(p)$, and thus we have

$$\widetilde{\Delta}^{\sigma_i}_{(x_1,x_2,x_3)} = \widetilde{\varphi}_{(x_1,x_2,x_3)}(X^i(p)) = \widetilde{\Delta}^{i}_{(x_1,x_2,x_3)}.$$

The following result describes the action of the Galois group on the cycles and is a direct consequence of Lemma 4.4.

Lemma 4.6. *For all* $i \in \mathbb{F}_p^\times$*, the following holds:*

i) $\widetilde{\Delta}^{\sigma_i}_{(n,m)} = \widetilde{\Delta}_{(n,m)}$ *for all* $n, m \in \mathbb{F}_p^\times$*. In particular, the cycles in* $\widetilde{\mathcal{C}}_0$ *are defined over* $\mathbb{Q}$*.*

ii) $\widetilde{\Delta}^{\sigma_i}_{a,b,c} = \widetilde{\Delta}_{ia,ib,ic}$ *for all* $a, b, c \in \mathbb{F}_p$ *with* $(a, b, c) \neq (0, 0, 0)$*. In particular, the cycles in* $\widetilde{\mathcal{C}}_1$ *are defined over* $\mathbb{Q}(\zeta_p)$ *and over no smaller field.*

4.2.2 Diagonal type cycles on $X_0(p)^3$

Recall from Section 1.2.2 that there is a natural degree $(p-1)/2$ covering of curves

$$\pi : X_1(p) \longrightarrow X_0(p)$$

defined over $\mathbb{Q}$. In terms of the (open) moduli description, this map is given by sending (E, P) to $(E, \langle P \rangle)$. It gives rise to a map on triple products $\pi^3 : X_1(p)^3 \longrightarrow X_0(p)^3$ of degree $(p-1)^3/8$ which in turn induces a push-forward map on Chow groups

$$(\pi^3)_* : \mathrm{CH}^2(X_1(p)^3) \longrightarrow \mathrm{CH}^2(X_0(p)^3).$$

Let us define, for $(x_1, x_2, x_3) \in ((\mathbb{F}_p \times \mathbb{F}_p) \setminus \{(0,0)\})^3$, the map

$$\varphi_{(x_1,x_2,x_3)} := \pi^3 \circ \widetilde{\varphi}_{(x_1,x_2,x_3)} : X(p) \longrightarrow X_0(p)^3,$$

as well as the cycle

$$\Delta_{(x_1,x_2,x_3)} := \varphi_{(x_1,x_2,x_3)}(X(p)) \in \mathrm{CH}^2(X_0(p)^3).$$

We then have $(\pi^3)_*(\widetilde{\Delta}_{(x_1,x_2,x_3)}) = \frac{(p-1)^3}{8} \Delta_{(x_1,x_2,x_3)}$.

The cycles $\Delta_{(x_1,x_2,x_3)}$ are invariant under the action of the diamond operators on the triples (x_1, x_2, x_3). Thus we obtain a collection $\mathcal{C}$ of cycles indexed by the double coset space

$$I := (\mathbb{F}_p^\times)^3 \setminus ((\mathbb{F}_p \times \mathbb{F}_p) \setminus \{(0,0)\})^3 / \mathbf{SL}_2(\mathbb{F}_p) = (\mathbb{F}_p^\times)^3 \setminus I.$$

This new index set has cardinality equal to 6 as follows from Corollaries 4.1, 4.2 and 4.3. As a consequence, the construction produces 6 codimension 2 cycles on $X_0(p)^3$ described as the schematic closures of:

1) $\Delta := \Delta_{(1,1)} = \{((E, \langle P\rangle), (E, \langle P\rangle), (E, \langle P\rangle))\}$

2) $\Delta_1 := \Delta_{0,1,1} = \{((E, \langle Q\rangle), (E, \langle P\rangle), (E, \langle P\rangle))\}$

3) $\Delta_2 := \Delta_{1,0,1} = \{((E, \langle P\rangle), (E, \langle Q\rangle), (E, \langle P\rangle))\}$

4) $\Delta_3 := \Delta_{1,1,0} = \{((E, \langle P\rangle), (E, \langle P\rangle), (E, \langle Q\rangle))\}$

5) $\Delta_+ := \Delta_{1,1,1} = \{((E, \langle P\rangle), (E, \langle Q\rangle), (E, \langle P + Q\rangle))\}$

6) $\Delta_- := \Delta_{1,1,a} = \{((E, \langle P\rangle), (E, \langle Q\rangle), (E, \langle aP + Q\rangle))\}$ (a is a non-quadratic residue).

Remark 4.14. The cycle Δ is the image of $X_0(p)$ under the diagonal embedding of $X_0(p)$ into $X_0(p)^3$ as described in (4.18). It is the diagonal cycle which underlies the definition of the Gross–Kudla–Schoen cycle of Definition 4.5.

Fields of definition

Lemma 4.7. *The cycles $\Delta, \Delta_1, \Delta_2$ and Δ_3 on $X_0(p)^3$ are defined over $\mathbb{Q}$.*

Proof. The statement for Δ follows directly from Lemma 4.6 (i) and the fact that the map π is defined over $\mathbb{Q}$, or alternatively from Remark 4.14.

Consider the cycle Δ_1. A similar reasoning applies to the cycles Δ_2 and Δ_3. By Lemma 4.6 (ii) combined with Corollary 4.2, we see that $\widetilde{\Delta}^{\sigma}_{0,1,1}$ belongs to the diamond orbit of $\widetilde{\Delta}_{0,1,1}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. As a consequence, after applying π^3 we obtain $\Delta_1^{\sigma} = \Delta_1$ and this cycle on $X_0(p)^3$ is thus defined over $\mathbb{Q}$. □

Denote by $\mathcal{C}^{\times}$ the collection of codimension 2 cycles on $X_0(p)^3$ indexed by $I^{\times} = (\mathbb{F}_p^{\times})^3 \backslash \widetilde{I}^{\times}$; it consists of two cycles, namely $\Delta_+ = \Delta_{1,1,1}$ and $\Delta_- = \Delta_{1,1,a}$, by Corollary 4.3. Note that in the case where $p \equiv 3 \pmod 4$, one may take $a = -1$.

Lemma 4.8. *The two cycles in* $\mathcal{C}^\times$ *are defined over the quadratic field*

$$K := \mathbb{Q}\left(\sqrt{p^\star}\right) \subset \mathbb{Q}(\zeta_p),$$

where $p^\star := \chi(-1)p$ *and* $\chi = \left(\frac{\cdot}{p}\right)$ *denotes the Legendre symbol modulo* p*. The non-trivial element of* $\mathrm{Gal}(K/\mathbb{Q})$ *interchanges* Δ_+ *and* Δ_-*.*

Proof. Let $G(\chi)$ denote the Gauss sum associated to χ given by the expression

$$G(\chi) := \sum_{n=0}^{p-1} \zeta_p^{n^2}.$$

The equality $G(\chi)^2 = p^\star$ goes back to Gauss and implies that K is the quadratic subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. Let τ denote the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and let σ_i denote the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ that corresponds to $i \in \mathbb{F}_p^\times$ as in Section 4.2.1. We then have

$$\sigma_i(G(\chi)) = \sum_{n=0}^{p-1} \zeta_p^{in^2} = G(\chi) \iff i \in (\mathbb{F}_p^\times)^{(2)},$$

and as a consequence $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K) \simeq (\mathbb{F}_p^\times)^{(2)}$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^{(2)}$. Thus τ acts as σ_a where $a \in \mathbb{F}_p^\times$ is not a square. It follows from Lemma 4.6 and Corollary 4.3 that both cycles in $\mathcal{C}^\times$ are fixed by $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ and moreover that

$$\Delta_+^\tau = \Delta_{1,1,1}^\tau = \Delta_{a,a,a} = \Delta_{1,1,a} = \Delta_-.$$

□

Remark 4.15. Note that $p^\star = p$ or $-p$ depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. If D_K denotes the discriminant of K, then $D_K = p^\star$. In fact, K is the unique quadratic extension of $\mathbb{Q}$ ramified only at p. Let χ_K denote the primitive quadratic Dirichlet character modulo p associated to K, namely χ_K is the Kronecker symbol $\left(\frac{p^\star}{\cdot}\right)$. This character enjoys the property that for any odd prime q we have

$$\chi_K(q) = \begin{cases} 0 & \text{if } q \text{ is ramified in } K \\ 1 & \text{if } q \text{ splits in } K \\ -1 & \text{if } q \text{ is inert in } K. \end{cases} \tag{4.23}$$

In particular, $\chi_K = \chi$ is the Legendre symbol at p.

The action of the symmetric group S_3

Consider the action of the symmetric group S_3 on $X_0(p)^3$ and $X_1(p)^3$ by permutation of the coordinates. This induces a left action of S_3 on the set of cycles $\widetilde{\mathcal{C}}$ and $\mathcal{C}$ respectively; given $\sigma \in S_3$,

$$\sigma \cdot \Delta_{(x_1,x_2,x_3)} := \sigma \circ \varphi_{x_1,x_2,x_3}(X(p)) = \Delta_{(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)})},$$

and a similar definition applies to the cycles in $\widetilde{\mathcal{C}}$.

Note that the action of S_3 on $\widetilde{\mathcal{C}}$ preserves the subset $\widetilde{\mathcal{C}}_0$, as well as the subsets

$$\widetilde{C}_1 \setminus \widetilde{\mathcal{C}}^\times = \mathrm{orb}_\diamond(\widetilde{\Delta}_{0,1,1}) \sqcup \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,0,1}) \sqcup \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,0})$$

and

$$\widetilde{\mathcal{C}}^\times = \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,1}) \sqcup \mathrm{orb}_\diamond(\widetilde{\Delta}_{1,1,a}).$$

As a consequence, the action of S_3 on $\mathcal{C}$ fixes the cycle Δ and permutes the cycles $\Delta_1, \Delta_2, \Delta_3$ transitively, as is obvious from their descriptions above. Let $[x_1, x_2, x_3] \in \widetilde{I}^\times$ with determinant $(a, b, c) \in (\mathbb{F}_p^\times)^3$. For all $\sigma \in S_3$,

$$\alpha_\sigma := \prod_{i=1}^{3} \mathrm{Det}([x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}])_i = \mathrm{sign}(\sigma)abc,$$

where $\mathrm{sign}(\sigma)$ is the sign of the permutation σ. The following lemma now follows directly from Corollary 4.3.

Lemma 4.9. *If $p \equiv 1 \pmod 4$, then the action of S_3 fixes Δ_+ and Δ_-. If $p \equiv 3 \pmod 4$, then any transposition in S_3 permutes Δ_+ and Δ_-.*

Intrinsic description

We have described 6 diagonal type cycles on $X_0(p)^3$ arising as images of certain maps $X(p) \longrightarrow X_0(p)^3$. We now give a more intrinsic description of the cycles Δ_+ and Δ_-.

Consider the curve $\Delta(p)$ defined in the beginning of Section 4.2 by the Cartesian diagram

$$\begin{array}{ccc} \Delta(p) & \hookrightarrow & X_0(p)^3 \\ \downarrow & \square & \downarrow \\ \Delta & \hookrightarrow & X(1)^3. \end{array}$$

Here $X(1)$ is the modular curve of level 1 (i.e., the j-line) and Δ is the image of $X(1)$ under the diagonal embedding $X(1) \longrightarrow X(1)^3$. By the interpretation of $X_0(p)$ as a coarse moduli space given in Section 1.2.2, $\Delta(p)$ is the schematic closure of the set

$$\{((E', C_1), (E', C_2), (E', C_3)) \ : \ E' \in X(1), C_i \text{ is a subgroup of } E' \text{ of order } p\}$$

taken modulo isomorphisms of elliptic curves with $\Gamma_0(p)$-structure.

Remark 4.16. In what follows, by slight abuse of notation, we shall write $C = C'$ for two order p subgroups of an elliptic curve E' if and only if there is an automorphism α of E' such that $\alpha(C) = C'$, i.e., the points (E', C) and (E', C') are equal in $X_0(p)$. Similarly, we write $C \neq C'$ if and only if there is no such automorphism, i.e., the points (E', C) and (E', C') are not equal in $X_0(p)$.

Using the conventions of Remark 4.16, the irreducible components of the scheme $\Delta(p)$ over $\mathbb{Q}$ can be naturally organised into S_3-orbits as follows:

- One component described by the condition $C_1 = C_2 = C_3$. This component is of course the diagonal Δ.
- Three components described by the conditions $C_1 = C_2 \neq C_3$, $C_1 = C_3 \neq C_2$ and $C_2 = C_3 \neq C_1$, respectively. These correspond respectively to the cycles Δ_1, Δ_2 and Δ_3 described above.
- One component described by the condition that C_1, C_2 and C_3 are pairwise distinct. We shall denote this component by $\Delta^{\perp}$. Note that

$$\Delta^{\perp} = \Delta_+ + \Delta_- \in \mathrm{CH}^2(X_0(p)^3)(\bar{\mathbb{Q}}).$$

Given an elliptic curve E', a triple (C_1, C_2, C_3) of distinct cyclic subgroups of order p in E' admits an invariant

$$o(E'; C_1, C_2, C_3) \in (\mu_p^{\otimes 3} - \{1\})/(\mathbb{F}_p^{\times})^{(2)},$$

described for instance in [48, p. 39]. It is defined, using the Weil pairing e_p, by choosing generators P_1, P_2, P_3 of C_1, C_2, C_3 and setting

$$o(E'; C_1, C_2, C_3) = e_p(P_2, P_3) \otimes e_p(P_3, P_1) \otimes e_p(P_1, P_2) \in \mu_p^{\otimes 3} - \{1\}.$$

This only depends on the choice of generators up to multiplication by a non-zero quadratic residue. If $[x_1, x_2, x_3] \in \widetilde{I}^{\times}$ with $\mathrm{Det}([x_1, x_2, x_3]) = (a, b, c)$, then for $(E', (P, Q)) \in X(p)$,

$$o(\widetilde{\varphi}_{x_1, x_2, x_3}(E', (P, Q))) = \zeta_p^a \otimes \zeta_p^b \otimes \zeta_p^c.$$

In terms of this invariant, we then have the more intrinsic definitions

$$\Delta_+ = \{(E', C_1), (E', C_2), (E', C_3) \,:\, o(E'; C_1, C_2, C_3) = \zeta_p^a \otimes \zeta_p^b \otimes \zeta_p^c,\ abc \in (\mathbb{F}_p^{\times})^{(2)}\},$$

$$\Delta_- = \{(E',C_1),(E',C_2),(E',C_3)\ :\ o(E';C_1,C_2,C_3) = \zeta_p^a \otimes \zeta_p^b \otimes \zeta_p^c,\ abc \notin (\mathbb{F}_p^\times)^{(2)}\}.$$

It is clear from this description that Δ_+ and Δ_- are indeed defined over the quadratic extension $K = \mathbb{Q}(\sqrt{p^\star})$.

4.2.3 Homological triviality

Recall from Definition 4.4 the definition of the Gross–Schoen projector, with base point a rational point $e \in X_0(p)(\mathbb{Q})$, given by

$$P_{\mathrm{GKS}}(e) := \sum_{T \subset \{1,2,3\}} (-1)^{|T'|} P_T(e) \in \mathrm{CH}^3(X_0(p)^3 \times X_0(p)^3).$$

This idempotent correspondence acts on cohomology and annihilates $H^4_B(X_0(p)^3, \mathbb{Z})$, the target of the Betti cycle class map cl^2_B of (1.43). Hence, for any cycle $Z \in \mathrm{CH}^2(X_0(p)^3)$, the cycle $P_{\mathrm{GKS}}(e)_*(Z)$ is null-homologous and belongs to $\mathrm{CH}^2(X_0(p)^3)_0$. In particular, applying this projector to the diagonal Δ gives the Gross–Kudla–Schoen cycle of Definition 4.5

$$\Delta_{\mathrm{GKS}}(e) = P_{\mathrm{GKS}}(e)_*(\Delta) \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}).$$

Theorem 4.3. *The cycles Δ_+ and Δ_- have the same image in cohomology. In particular, their difference $\Xi := \Delta_+ - \Delta_-$ belongs to $\mathrm{CH}^2(X_0(p)^3)_0(K)$.*

We record the following key lemma from which Theorem 4.3 follows as a corollary.

Lemma 4.10. *Let $i < j \in \{1,2,3\}$ and denote by $\mathrm{pr}_{ij} : X_0(p)^3 \longrightarrow X_0(p)^2$ the natural projection to the product of the i-th and j-th components. There exist elements $[x_1,x_2,x_3]$ and $[y_1,y_2,y_3]$ of $\widetilde{I}^\times$ satisfying*

$$\prod_{k=1}^{3} \mathrm{Det}([x_1,x_2,x_3])_k \in (\mathbb{F}_p^\times)^{(2)} \qquad \text{and} \qquad \prod_{k=1}^{3} \mathrm{Det}([y_1,y_2,y_3])_k \notin (\mathbb{F}_p^\times)^{(2)},$$

and such that we have an equality $\mathrm{pr}_{ij} \circ \varphi_{(x_1,x_2,x_3)} = \mathrm{pr}_{ij} \circ \varphi_{(y_1,y_2,y_3)}$ of maps $X(p) \longrightarrow X_0(p)^2$.

Proof. Fix some $a \notin (\mathbb{F}_p^\times)^{(2)}$.

If $i = 1$ and $j = 2$, then we may take

$$(x_1, x_2, x_3) = ((1,0),(0,1),(-1,-1)) \qquad \text{and} \qquad (y_1, y_2, y_3) = ((1,0),(0,1),(-a,-1)).$$

If $i = 1$ and $j = 3$, then we may take

$$(x_1, x_2, x_3) = ((-1,0),(1,-1),(0,1)) \qquad \text{and} \qquad (y_1, y_2, y_3) = ((-1,0),(a,-1),(0,1)).$$

If $i = 2$ and $j = 3$, then we may take

$$(x_1, x_2, x_3) = ((-1,-1),(1,0),(0,1)) \qquad \text{and} \qquad (y_1, y_2, y_3) = ((-1,-a),(1,0),(0,1)).$$

□

Remark 4.17. The maps $\varphi_{(x_1,x_2,x_3)}$ and $\varphi_{(y_1,y_2,y_3)}$ associated with the specific choices made in the above proof will be denoted $\varphi_+(ij)$ and $\varphi_-(ij) = \varphi_-(ij; a)$, respectively.

Proof of Proposition 4.3. Observe that

$$P_{\mathrm{GKS}}(e)_*(\Xi) = \Xi - P_{12}(e)_*(\Xi) - P_{13}(e)_*(\Xi) - P_{23}(e)_*(\Xi) + P_1(e)_*(\Xi) + P_2(e)_*(\Xi) + P_3(e)_*(\Xi).$$

Let $i < j \in \{1,2,3\}$ and consider $P_{ij}(e)_*(\Xi)$. Let $k \in \{1,2,3\}$ be the remaining element distinct from i and j. The correspondence $P_{ij}(e)$ is the graph of the function

$$q_{ij}(e) \circ \mathrm{pr}_{ij} : X_0(p)^3 \longrightarrow X_0(p)^3,$$

which replaces the k-th coordinate by the element e, and $P_{ij}(e)_*(\Xi)$ is the image of Ξ under $q_{ij}(e) \circ \mathrm{pr}_{ij}$. Choose $[x_1, x_2, x_3]$ and $[y_1, y_2, y_3]$ of $\widetilde{I}^\times$ satisfying the properties of Lemma 4.10

for the fixed i and j. The first condition ensures that

$$\varphi_{(x_1,x_2,x_3)}(X(p)) = \Delta_+ \quad \text{and} \quad \varphi_{(y_1,y_2,y_3)}(X(p)) = \Delta_-,$$

while the second condition implies that

$$P_{ij}(e)_*(\Delta_+) = q_{ij}(e) \circ \mathrm{pr}_{ij} \circ \varphi_{(x_1,x_2,x_3)}(X(p)) = q_{ij}(e) \circ \mathrm{pr}_{ij} \circ \varphi_{(y_1,y_2,y_3)}(X(p)) = P_{ij}(e)_*(\Delta_-).$$

As a consequence, we have $P_{ij}(e)_*(\Xi) = 0$.

Let $i \in \{1, 2, 3\}$ and consider $P_i(e)_*(\Xi)$. Let $j, k \in \{1, 2, 3\}$ such that $\{i, j, k\} = \{1, 2, 3\}$. The correspondence $P_i(e)$ is the graph of the map $q_i(e) \circ \mathrm{pr}_i : X_0(p)^3 \longrightarrow X_0(p)^3$, which replaces the j-th and k-th coordinates by the element e, and $P_i(e)_*(\Xi)$ is the image of Ξ under $q_i(e) \circ \mathrm{pr}_i$. This map can be written as the composition

$$q_i(e) \circ \mathrm{pr}_i = (q_{ik}(e) \circ \mathrm{pr}_{ik}) \circ (q_{ij}(e) \circ \mathrm{pr}_{ij}),$$

hence in terms of correspondences we have $P_i(e) = P_{ik}(e) \circ P_{ij}(e)$. It follows from the previous paragraph that $P_i(e)_*(\Xi) = 0$.

We conclude that $\Xi = P_{\mathrm{GKS}}(e)_*(\Xi)$ is null-homologous. □

Remark 4.18. A perhaps more direct way to see that the cycle Ξ is null-homologous is to consider its image under the de Rham cycle class map (1.46), namely

$$\mathrm{cl}_{\mathrm{dR}}(\Xi) = \mathrm{cl}_{\mathrm{dR}}(\Delta_+) - \mathrm{cl}_{\mathrm{dR}}(\Delta_-) \in H^4_{\mathrm{dR}}(X_0(p)^3/\mathbb{C}),$$

where we recall (1.47) that

$$\int_{X_0(p)(\mathbb{C})^3} \mathrm{cl}_{\mathrm{dR}}(\Delta_\pm) \wedge \alpha = \int_{\Delta_\pm} \alpha, \qquad \text{for all } \alpha \in H^2_{\mathrm{dR}}(X_0(p)^3/\mathbb{C}).$$

By the Künneth decomposition of $H^2_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})$, any component of α can at most involve de Rham classes coming from 2 of the three components of $X_0(p)^3$; indeed, the components are either of the form $\mathrm{pr}_i^*(\beta)$ for some $\beta \in H^2_{\mathrm{dR}}(X_0(p)/\mathbb{C})$ and $i \in \{1,2,3\}$, or of the form $\mathrm{pr}_j^*(\gamma) \wedge \mathrm{pr}_k^*(\delta)$ for some $\gamma, \delta \in H^1_{\mathrm{dR}}(X_0(p)/\mathbb{C})$ and $j < k \in \{1,2,3\}$. Using the notations of Remark 4.17, observe that

$$\int_{\Delta_\pm} \mathrm{pr}_i^*(\beta) = \int_{X(p)} (\mathrm{pr}_i \circ \varphi_\pm(ij))^*(\beta)$$
$$\int_{\Delta_\pm} \mathrm{pr}_j^*(\gamma) \wedge \mathrm{pr}_k^*(\delta) = \int_{X(p)} (\mathrm{pr}_{jk} \circ \varphi_\pm(jk))^*(\gamma \wedge \delta).$$

Since

$$\mathrm{pr}_i \circ \varphi_+(ij) = \mathrm{pr}_i \circ \varphi_-(ij) : X(p) \longrightarrow X_0(p)$$
$$\mathrm{pr}_{jk} \circ \varphi_+(jk) = \mathrm{pr}_{jk} \circ \varphi_-(jk) : X(p) \longrightarrow X_0(p)^2,$$

this implies that $\mathrm{cl}_{\mathrm{dR}}(\Delta_+) = \mathrm{cl}_{\mathrm{dR}}(\Delta_-)$ in $H^4_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})$.

Remark 4.19. We have constructed a canonical null-homologous codimension 2 cycle Ξ on $X_0(p)^3$ which does not depend on any choice of rational base point as opposed to the Gross–Kudla–Schoen cycle $\Delta_{\mathrm{GKS}}(e)$. If τ denotes the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, then

$$\Xi := \Delta_+ - \Delta_- \in \mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}.$$

4.3 Torsion properties

In this section, we prove three torsion results concerning respectively the Gross–Kudla–Schoen cycle (more precisely its Abel–Jacobi image), its associated Chow–Heegner points, and finally the Chow–Heegner points associated to the cycle Ξ.

4.3.1 The Abel–Jacobi image of the Gross–Kudla–Schoen cycle

Let f_1, f_2 and f_3 be three newforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$. In this section, we work under the following assumption on the sign of the functional equation (4.13):

Assumption 4.1. $W(F) = +1$.

The L-function $L(F, s)$ then vanishes to even order at the central critical point $s = 2$, and we have at our disposal the Gross–Kudla formula of Theorem 4.1, which gives an expression for $L(F, 2)$. Under Assumption 4.1, the Beilinson–Bloch conjecture (4.14) predicts that the algebraic rank of the F-isotypic component of $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ is even. Comparing with the situation of Heegner points on modular curves described in Section 0.2.1, it seems reasonable to expect that the F-isotypic component of $\Delta_{\mathrm{GKS}}(e)$ is torsion. While this seems difficult to prove directly in the Chow group, we can prove the corresponding statement for the image of the cycle under the complex Abel–Jacobi map

$$\mathrm{AJ}_{X_0(p)^3} : \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{C}) \longrightarrow J^2(X_0(p)^3/\mathbb{C}) := \frac{\mathrm{Fil}^2 H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})^\vee}{\mathrm{Im}\, H_3(X_0(p)^3(\mathbb{C}), \mathbb{Z})}, \tag{4.24}$$

whose definition is given in Sections 0.2.3 and 1.5.1.

We will be solely interested in the piece of the Abel–Jacobi map that survives after applying the idempotent correspondence t_F of (4.9): functoriality of Abel–Jacobi maps allows us to view $\mathrm{AJ}_{X_0(p)^3}$ as a map

$$(t_F)_* \,\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{C}) \longrightarrow (t_F^*)^\vee (J^2(X_0(p)^3/\mathbb{C})) = \frac{\mathrm{Fil}^2 (t_F)^* H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})^\vee}{\mathrm{Im} (t_F)_* H_3(X_0(p)^3(\mathbb{C}), \mathbb{Z})}. \tag{4.25}$$

The aim of this section is to prove the following statement.

Theorem 4.4. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(p))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. Then $\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e)))$ is torsion in $J^2(X_0(p)^3/\mathbb{C})$ for any base point $e \in X_0(p)(\mathbb{Q})$.*

Remark 4.20. The complex Abel–Jacobi map $\mathrm{AJ}_{X_0(p)^3}$ in codimension 2 is injective when restricted to torsion, as follows from the comparison in Proposition 1.20 with Bloch's map together with Proposition 1.17. Beilinson and Bloch have independently conjectured that in general the complex Abel–Jacobi maps for smooth proper varieties over number fields are injective up to torsion. See [94, Conjecture 9.12]. However, this remains an open problem, as kernels of Abel–Jacobi maps are in general poorly understood. In particular, Theorem 4.4 above does not imply that $(t_F)_*(\Delta_{\mathrm{GKS}}(e))$ is torsion in the Chow group, although we believe this should be the case. The author is grateful to Benedict Gross for pointing out a mistake in the original version of Theorem 4.4.

Remark 4.21. Similar arguments to the ones presented in the proof of Theorem 4.4 below can be used to prove that the image of $(t_F)_*(\Delta_{\mathrm{GKS}}(e))$ under the ℓ-adic étale Abel–Jacobi map (1.75)

$$\mathrm{AJ}_{\mathrm{et}} : \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, H^3_{\mathrm{et}}(X_0(p)^3_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(2))) \tag{4.26}$$

is torsion when the global root number is $W(F) = +1$. When restricted to torsion, the map (4.26) is injective as follows from the comparison in Proposition 1.21 with the Bloch map and Proposition 1.17. It is conjectured by Beilinson and Bloch that for any smooth proper variety over a number field and for any prime ℓ, the ℓ-adic Abel–Jacobi maps (1.75) are injective up to torsion. See for instance [94, Conjecture 9.15] or [121, Conjecture (2.1)]. Again, this is not known, and we cannot say anything about the torsion properties of the cycle $(t_F)_*(\Delta_{\mathrm{GKS}}(e))$ in the Chow group.

The rest of this section constitutes the proof of Theorem 4.4. We distinguish different situations depending on the genus g of $X_0(p)$, which we recall is given by formula (1.18).

The genus zero case

The curve $X_0(p)$ has genus zero exactly when $p \in \{2, 3, 5, 7, 13\}$. In this case the space of cusp forms $S_2(\Gamma_0(p))$ is trivial so there is no triple product L-function to consider in the first place. By [77, Proposition 4.1], we have $\Delta_{\mathrm{GKS}}(e) = 0$ in $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ since the cycle class map is injective in this case.

The genus one case

Suppose that $g = 1$, i.e., $p \in \{11, 17, 19\}$. In this case, $X_0(p)$ is an elliptic curve over $\mathbb{Q}$ of Mordell–Weil rank 0 corresponding to a unique normalised eigenform f in $S_2(\Gamma_0(p))$. Given $e \in X_0(p)(\mathbb{Q})$, consider

$$W_e = \{(x_1, x_2, x_3) \in X_0(p)^3 \mid x_i = e \text{ for some } i\}$$

and denote by $i : W_e \longrightarrow X_0(p)^3$ the natural inclusion. Following [77, Proposition 4.5, Corollary 4.7], we have $6Z = 0$ for any $Z \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ satisfying $i^*(Z) = 0$. Since we indeed have $i^*(\Delta_{\mathrm{GKS}}(e)) = 0$, we obtain $6\Delta_{\mathrm{GKS}}(e) = 0$.

Let us analyse the order of vanishing of the triple product L-function in this setting. We have $f_1 = f_2 = f_3 = f$ and by [76, (11.8)] the L-function decomposes as

$$L(F, s) = L(\mathrm{Sym}^3 f, s)L(f, s-1)^2.$$

By Theorem 4.1, we have

$$L(F, 2) = 0 \iff \sum_{i=0}^{1} w_i^2 \lambda_i(f)^3 = 0.$$

Notice that $W(F) = a_p(f)^3 = +1$ by Assumption 4.1 and thus $a_p(f) = +1$ so that the sign of the functional equation of $L(f, s)$ centred at $s = 1$ is equal to $+1$. Since $\sum_{i=0}^{1} \lambda_i(f) = 0$ by [76, p. 202], we observe that $\lambda_0(f)^3 = -\lambda_1(f)^3$, hence we deduce the equality

$$\sum_{i=0}^{1} w_i^2 \lambda_i(f)^3 = (w_0^2 - w_1^2)\lambda_0(f)^3.$$

Using Remark 4.9, we see that:

- If $p = 11$, then $w_0 = 3$ and $w_1 = 4$, so that $\sum_{i=0}^{1} w_i^2 \lambda_i(f)^3 = 5\lambda_0(f)^3$.
- If $p = 17$, then $w_0 = 3$ and $w_1 = 1$, so that $\sum_{i=0}^{1} w_i^2 \lambda_i(f)^3 = 8\lambda_0(f)^3$.
- If $p = 19$, then $w_0 = 2$ and $w_1 = 1$, so that $\sum_{i=0}^{1} w_i^2 \lambda_i(f)^3 = 3\lambda_0(f)^3$.

In each case we obtain $L(F, 2) \neq 0$ since $\lambda_0(f) \neq 0$ (cf. [76, Table 12.5]), that is, $\mathrm{ord}_{s=2}(L(F, s)) = 0$. Thus, the fact that $\Delta_{\mathrm{GKS}}(e)$ is torsion in the Chow group is consistent with conjecture (4.14).

The higher genus case

Suppose that $g \geq 2$. The Atkin–Lehner involution w_p of $X_0(p)$ is defined, following the moduli description, by mapping a p-isogeny $\phi : E \longrightarrow E'$ of elliptic curves to its dual isogeny $\phi' : E' \longrightarrow E$. On covering spaces, it is given by $\tau \mapsto -\frac{1}{p\tau}$, where τ belongs to the complex upper half-plane. This involution is defined over $\mathbb{Q}$ and therefore maps $\mathbb{Q}$-rational points of $X_0(p)$ to $\mathbb{Q}$-rational points. It will be convenient to sometimes view w_p as a correspondence by taking its graph; by slight abuse of notation we will write $w_p \in \mathrm{Corr}^0(X_0(p), X_0(p))$. In light of the discussion in Section 4.1.1, the operator w_p naturally belongs to the Hecke algebra $\mathbb{T} = \mathbb{T}_0$, and commutes with the Hecke operators. We recall that any Hecke eigenform is also an eigenform for w_p, with corresponding eigenvalue given by the negative of the p-th Fourier coefficient.

The modular forms f_j for $j = 1, 2, 3$ are thus eigenforms for the operator w_p with eigenvalues given by $-a_p(f_j)$ respectively. In particular, $\lambda_{f_j}(w_p) = -a_p(f_j)$, where $\lambda_{f_j} : \mathbb{T} \longrightarrow K_{f_j}$ is the algebra homomorphism corresponding to f_j. The local root number at p is

$$W_p(F) := -a_p(f_1)a_p(f_2)a_p(f_3) = -W(F).$$

See for instance Proposition 4.5 later in this chapter. We have an involution $u_p := w_p \times w_p \times w_p$

of $X_0(p)^3$. By taking its graph, it may be viewed as a correspondence, and we write again $u_p \in \mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)$ by slight abuse of notation. Note that, as correspondences,

$$u_p = w_p \otimes w_p \otimes w_p := \mathrm{pr}_{14}^*(w_p) \cdot \mathrm{pr}_{25}^*(w_p) \cdot \mathrm{pr}_{36}^*(w_p) \in \mathrm{Corr}^0(X_0(p)^3, X_0(p)^3).$$

The map u_p induces an involution on cohomology via pull-back, hence an involution on the space of cuspidal forms of weight $(2, 2, 2)$, and we see that

$$F|_{u_p} = W_p(F) \cdot F = -W(F) \cdot F. \tag{4.27}$$

Lemma 4.11. *We have $(u_p)_*(\Delta_{\mathrm{GKS}}(e)) = \Delta_{\mathrm{GKS}}(w_p(e))$, for all points e on $X_0(p)$.*

Proof. Remark that the induced map $(u_p)_* : \mathrm{CH}^2(X_0(p)^3) \longrightarrow \mathrm{CH}^2(X_0(p)^3)$ on Chow groups simply maps a cycle to its image under u_p. Since u_p is an automorphisms of $X_0(p)^3$, we note that $u_p(\Delta) = \Delta$. However, for any proper subset $T \subset \{1, 2, 3\}$ we have the equality $u_p(P_T(e)_*(\Delta)) = P_T(w_p(e))_*(\Delta)$ and the result follows. □

Proposition 4.3. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(p))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. We have $\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e))) = -\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(w_p(e))))$, for all points e on $X_0(p)$.*

Proof. By functoriality of Abel–Jacobi maps with respect to correspondences, we have

$$\mathrm{AJ}_{X_0(p)^3}((u_p)_*(t_F)_*(\Delta_{\mathrm{GKS}}(e))) = (u_p^*)^\vee \mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e))). \tag{4.28}$$

Since w_p commutes with t_{f_j} as correspondences for each $j \in \{1, 2, 3\}$ by (4.5) and (4.4), we see that

$$t_F \circ u_p = (t_{f_1} \circ w_p) \otimes (t_{f_2} \circ w_p) \otimes (t_{f_3} \circ w_p) = (w_p \circ t_{f_1}) \otimes (w_p \circ t_{f_2}) \otimes (w_p \circ t_{f_3}) = u_p \circ t_F,$$

as elements in $\mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)$. In particular, using Lemma 4.11, we obtain

$$(u_p)_*(t_F)_*(\Delta_{\mathrm{GKS}}(e)) = (t_F)_*(u_p)_*(\Delta_{\mathrm{GKS}}(e)) = (t_F)_*(\Delta_{\mathrm{GKS}}(w_p(e))).$$

Thus the left hand side of (4.28) is equal to $\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(w_p(e))))$.

On the other hand, $\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e)))$ lies in $(t_F^*)^\vee(J^2(X_0(p)^3/\mathbb{C}))$ by (4.25), that is, in the F-isotypic Hecke component of the intermediate Jacobian. The Hecke algebra $\mathbb{T}^{\otimes 3}$ acts via correspondences on the latter by multiplication by the Hecke eigenvalues of F. More precisely, for any $\alpha \in \mathrm{Fil}^2 H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})$, we have the following equality

$$(u_p^*)^\vee \mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e)))(\alpha) = \mathrm{AJ}_{X_0(p)^3}(\Delta_{\mathrm{GKS}}(e))(u_p^*(t_F^*(\alpha))).$$

The operator $u_p \in \mathbb{T}^{\otimes 3}$ acts via pull-back on the F-isotypic component $(t_F)^* H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})$ as multiplication by $-W(F)$ by (4.27). In particular, we have $u_p^*(t_F^*(\alpha)) = -W(F)t_F^*(\alpha)$. By Assumption 4.1, the right hand side of (4.28) is therefore given by

$$(u_p^*)^\vee \mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e))) = -\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e))),$$

and the result follows. □

Mazur has proved in [113, Theorem 1] that if $g \geq 2$ and $p \notin \{37, 43, 67, 163\}$, then $X_0(p)(\mathbb{Q}) = \{\xi_\infty, \xi_0\}$, where ξ_∞ and ξ_0 denote the two cusps of $X_0(p)$. Moreover, $X_0(37)$ has two non-cuspidal $\mathbb{Q}$-rational points, while for p belonging to $\{43, 67, 163\}$, $X_0(p)$ has a unique non-cuspidal $\mathbb{Q}$-rational point.

Corollary 4.4. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(p))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. If p belongs to $\{43, 67, 163\}$ and e is the unique non-cuspidal $\mathbb{Q}$-rational point of $X_0(p)$, then $2\,\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(e))) = 0$.*

Proof. The involution w_p maps $\mathbb{Q}$-rational points to $\mathbb{Q}$-rational points and permutes the two cusps ξ_∞ to ξ_0. It therefore fixes the non-cuspidal point e and the result follows from Proposition 4.3. □

Corollary 4.5. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(p))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. If $g \geq 2$, then $2n\,\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\xi_\infty))) = 0$, where n is the numerator of $(p-1)/12$. The same is true for the base point ξ_0.*

Proof. By [77, Proposition 3.6], the cycle $\Delta_{\mathrm{GKS}}(\xi_\infty) - \Delta_{\mathrm{GKS}}(\xi_0)$ in $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ depends only on the class of the divisor $(\xi_\infty) - (\xi_0)$ in $\mathrm{CH}^1(X_0(p))_0(\mathbb{Q}) = J_0(p)(\mathbb{Q})$. However, by [112, Theorem 1], the degree zero divisor $(\xi_\infty) - (\xi_0)$ is torsion of order n in the Jacobian $J_0(p)$. As a consequence, $n(\Delta_{\mathrm{GKS}}(\xi_\infty) - \Delta_{\mathrm{GKS}}(\xi_0)) = 0$ in $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$, and in particular

$$n(\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\xi_\infty))) - \mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\xi_0)))) = 0 \in J^2(X_0(p)^3/\mathbb{C}).$$

Recall that w_p permutes the two cusps ξ_∞ and ξ_0. By Proposition 4.3, we therefore have

$$\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\xi_\infty))) = -\,\mathrm{AJ}_{X_0(p)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\xi_0))),$$

and the result follows. □

To complete the proof of Theorem 4.4, the only remaining case is when $p = 37$ and the chosen base point is a non-cuspidal $\mathbb{Q}$-rational point. The curve $X_0(37)$ has been extensively studied by Mazur and Swinnerton-Dyer in [114, §5]. It has genus 2 and is thus hyperelliptic, with hyperelliptic involution S. In particular, for all points e on $X_0(37)$, we have $6\Delta_{\mathrm{GKS}}(e) = 0$ in the Griffiths group $\mathrm{Gr}^2(X_0(37)^3)$ by [77, Corollary 4.9]. See Section 1.4.4 for the definition of algebraic equivalence and the Griffiths group. The involution S is distinct from the Atkin–Lehner involution w_{37}, as the quotient $X_0^+(37) = X_0(37)/w_{37}$ has genus 1. Since S commutes with every automorphism of $X_0(37)$ by [114, p. 27], it commutes in particular with w_{37}, and we can define another involution $T = S \circ w_{37} = w_{37} \circ S$. Let $\gamma_0 = T(\xi_0)$ and $\gamma_\infty = T(\xi_\infty)$ be the images of the two cusps by T. By [114, Proposition 2], we have

$$X_0(37)(\mathbb{Q}) = \{\xi_0, \xi_\infty, \gamma_0, \gamma_\infty\} \qquad \text{and} \qquad w_{37}(\gamma_0) = \gamma_\infty. \tag{4.29}$$

The involution S has 6 fixed points, none of which are rational over $\mathbb{Q}$. By [77, Proposition 4.8], $6\Delta_{\mathrm{GKS}}(e) = 0$ in $\mathrm{CH}^2(X_0(37)^3)$ if e is a fixed point of S. By [114, p. 29], the two fixed points α_1 and α_2 of w_{37} are Galois conjugates defined over $\mathbb{Q}(\sqrt{37})$. We have the following result:

Corollary 4.6. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(37))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. The images under the complex Abel–Jacobi map $\mathrm{AJ}_{X_0(37)^3}$ of the cycles $(t_F)_*\Delta_{\mathrm{GKS}}(\alpha_1)$ and $(t_F)_*\Delta_{\mathrm{GKS}}(\alpha_2)$ in $\mathrm{CH}^2(X_0(37)^3)_0(\mathbb{Q}(\sqrt{37}))$ are 2-torsion in the intermediate Jacobian $J^2(X_0(37)^3/\mathbb{C})$.*

Proof. This is an immediate consequence of Proposition 4.3, given that α_1 and α_2 are the fixed points of w_{37}. □

We complete the proof of Theorem 4.4.

Corollary 4.7. *Let f_1, f_2 and $f_3 \in S_2(\Gamma_0(37))$ be three normalised cuspforms, denote by $F = f_1 \otimes f_2 \otimes f_3$ their triple product and suppose that F satisfies Assumption 4.1. Then $6\,\mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_0))) = 6\,\mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_\infty))) = 0$.*

Proof. By (4.29), the Atkin–Lehner involution w_{37} interchanges γ_0 and γ_∞. By Proposition 4.3, we have $\mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_0))) = -\,\mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_\infty)))$. The element

$$2\,\mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_0))) = \mathrm{AJ}_{X_0(37)^3}((t_F)_*(\Delta_{\mathrm{GKS}}(\gamma_0) - \Delta_{\mathrm{GKS}}(\gamma_\infty))) \in J^2(X_0(37)^3/\mathbb{C})$$

depends only on the class of $(\gamma_0) - (\gamma_\infty)$ in $J_0(37)(\mathbb{Q})$. But this class is the image of the class of $(\xi_0) - (\xi_\infty)$ by the involution of $J_0(37)$ obtained from T by push-forward. The latter class has order equal to the numerator of $(37-1)/2 = 3$ by [112, Theorem 1]. The result follows. □

4.3.2 Chow–Heegner points attached to Δ_{GKS}

Let $f \in S_2(\Gamma_0(p))$ be a normalised newform with rational Fourier coefficients and let g be an auxiliary normalised newform in $S_2(\Gamma_0(p))$ which is not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f. Recall the Chow–Heegner point defined in (4.21), namely

$$P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}(e)) := (\Pi_{[g]} \circ t_f)_*(\Delta_{\mathrm{GKS}}(e)) \in E_f(\mathbb{Q}),$$

where $\Pi_{[g]} = \mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(\Delta) \in \mathrm{CH}^2(X_0(p)^4)(\mathbb{Q})$, and $\Delta \in \mathrm{CH}^1(X_0(p)^2)$ is the diagonal cycle. Note by [53, Example 3.1.7] that the definition of this point is independent of the choice of $t_{[g]} \in \mathrm{CH}^1(X_0(p)^2)(\mathbb{Q}) \otimes \mathbb{Q}$ mapping to the idempotent $e_{[g]}$ via the map (4.5). See Section 4.1.1.

Theorem 4.5. *If E_f admits split multiplicative reduction at p, then the Chow–Heegner point $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}(e))$ is torsion in $E_f(\mathbb{Q})$ for all $e \in X_0(p)(\mathbb{Q})$.*

Proof. Recall from 4.1.1 that $t_{[g]} = \sum_{h \in [g]} t_h$, and thus

$$t_{[g]} \otimes t_{[g]} \otimes t_f = \sum_{h_1, h_2 \in [g]} t_{h_1} \otimes t_{h_2} \otimes t_f.$$

By Remark 4.8, for any $h_1, h_2 \in [g]$, the global root number of the triple product L-function $L(h_1, h_2, f, s)$ is given by $W(h_1, h_2, f) = a_p(h_1)a_p(h_2)a_p(f)$. The p-th Fourier coefficient of a normalised newform is the negative of the eigenvalue of the form with respect to the Atkin–Lehner involution w_p, hence it belongs to $\{\pm 1\}$. In particular, since this coefficient belongs to $\mathbb{Q}$, it is fixed by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and thus $a_p(g) = a_p(h_1) = a_p(h_2) \in \{\pm 1\}$. It follows that $W(h_1, h_2, f) = a_p(f) = a_p(E_f)$. By (1.13), $a_p(E_f) = 1$ since E_f admits split multiplicative reduction at p, and thus the triple (h_1, h_2, f) satisfies Assumption 4.1. By

Theorem 4.4, for any $e \in X_0(p)(\mathbb{Q})$, $\mathrm{AJ}_{X_0(p)^3}((t_{h_1} \otimes t_{h_2} \otimes t_f)_*(\Delta_{\mathrm{GKS}}(e)))$ is torsion in the intermediate Jacobian $J^2(X_0(p)^3/\mathbb{C})$. It follows that $\mathrm{AJ}_{X_0(p)^3}((t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Delta_{\mathrm{GKS}}(e)))$ is torsion in $J^2(X_0(p)^3/\mathbb{C})$. Define

$$\Pi := \mathrm{pr}_{12}^*(\Delta) \cdot \mathrm{pr}_{34}^*(\Delta) \in \mathrm{CH}^2(X_0(p)^4).$$

Viewing $t_{[g]} \otimes t_{[g]} \otimes t_f$ as an element of $\mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)_{\mathbb{Q}}$ and Π as an element of $\mathrm{Corr}^{-1}(X_0(p)^3, X_0(p))$, we may compute their composition using (1.42) to obtain

$$(t_{[g]} \otimes t_{[g]} \otimes t_f) \circ \Pi = \mathrm{pr}_{12}^*(t_{[g]} \circ t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_f) = \mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_f) = \Pi_{[g],f}, \tag{4.30}$$

as elements of $\mathrm{Corr}^{-1}(X_0(p)^3, X_0(p))_{\mathbb{Q}}$. Note that we used here the fact that $t_{[g]}$ is an idempotent correspondence, i.e., $t_{[g]} \circ t_{[g]} = t_{[g]}$. A similar calculation is carried out in [51, §3]. We deduce the equality of points in $E_f(\mathbb{Q})$

$$\Pi_*(t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Delta_{\mathrm{GKS}}(e)) = P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}(e)). \tag{4.31}$$

By functoriality of Abel–Jacobi maps with respect to correspondences, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{C}) & \xrightarrow{\mathrm{AJ}_{X_0(p)^3}} & J^2(X_0(p)^3/\mathbb{C}) \\ \downarrow{\scriptstyle \Pi_{[g],f,*}} & & \downarrow{\scriptstyle (\Pi_{[g],f}^*)^\vee} \\ E_f(\mathbb{C}) & \underset{\mathrm{AJ}_{E_f}}{\xrightarrow{\sim}} & J^1(E_f/\mathbb{C}), \end{array}$$

where AJ_{E_f} is the Abel–Jacobi isomorphism of the elliptic curve E_f described in Section 1.5.1. In particular, we have the equalities

$$\begin{aligned} \mathrm{AJ}_{E_f}(P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}(e))) &= (\Pi_{[g],f}^*)^\vee(\mathrm{AJ}_{X_0(p)^3}(\Delta_{\mathrm{GKS}}(e))) \\ &= (\Pi^*)^\vee((t_{[g]} \otimes t_{[g]} \otimes t_f)^*)^\vee \, \mathrm{AJ}_{X_0(p)^3}(\Delta_{\mathrm{GKS}}(e)) \\ &= (\Pi^*)^\vee \, \mathrm{AJ}_{X_0(p)^3}((t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Delta_{\mathrm{GKS}}(e))). \end{aligned}$$

In the second equality we used (4.30) and in the third equality we used the functoriality of $\mathrm{AJ}_{X_0(p)^3}$ with respect to the correspondence $t_{[g]} \otimes t_{[g]} \otimes t_f$.

Since $\mathrm{AJ}_{X_0(p)^3}((t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Delta_{\mathrm{GKS}}(e)))$ is torsion, the result follows from the fact that AJ_{E_f} is an isomorphism. $\square$

Remark 4.22. This is a special case of [53, Theorem 3.3.8]. In his thesis, Daub proves more generally for composite level N that if the local root number $W_p(g, g, f) = -1$ for some $p \mid N$, then the resulting Chow–Heegner points are torsion. His proof identifies these points with certain rational points known as Zhang points.

4.3.3 Chow–Heegner points attached to Ξ

Recall from Theorem 4.3 the special cycle $\Xi \in \mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}$, where $K = \mathbb{Q}(\sqrt{p^\star})$. Let $f \in S_2(\Gamma_0(p))$ be a normalised newform with rational coefficients and with associated elliptic curve E_f. Let g be an auxiliary normalised newform in $S_2(\Gamma_0(p))$ which is not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f. Using the correspondence $\Pi_{[g],f} = \Pi_{[g]} \circ t_f \in \mathrm{Corr}^{-1}(X_0(p)^3, X_0(p))$, we may form the Chow–Heegner point

$$P(X_0(p)^3, \Pi_{[g],f}, \Xi) = (\Pi_{[g],f})_*(\Xi) \in E_f(\mathbb{Q}(\sqrt{p^\star}))^{\tau=-1}.$$

Note that when $p \equiv 3 \pmod 4$, which is the situation we are concerned with in this section, the extension $K = \mathbb{Q}(\sqrt{-p})$ is imaginary quadratic.

Theorem 4.6. *Let f and g be two normalised newforms in $S_2(\Gamma_0(p))$ as above. If we assume $p \equiv 3 \pmod 4$, then the Chow–Heegner point $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ is torsion in $E_f(\mathbb{Q}(\sqrt{-p}))$.*

Proof. Consider the permutation $(12) \in S_3$ and its induced map

$$s_{12} : X_0(p)^3 \longrightarrow X_0(p)^3, \qquad (x_1, x_2, x_3) \mapsto (x_2, x_1, x_3).$$

By taking its graph we will view it as a correspondence, which will, by slight abuse of notation, be denoted $s_{12} \in \mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)$. It induces an involution $(s_{12})_* = (s_{12})^*$ of $\mathrm{CH}^2(X_0(p)^3)$ by mapping a cycle to its image under s_{12}.

Given $Z_1, Z_2, Z_3 \in \mathrm{Corr}^0(X_0(p), X_0(p))$, one verifies the following equalities of correspondences

$$\begin{aligned} Z_1 \otimes Z_2 \otimes Z_3 \circ s_{12} &= \mathrm{pr}_{15}^*(Z_1) \cdot \mathrm{pr}_{24}^*(Z_2) \cdot \mathrm{pr}_{36}^*(Z_3) \\ s_{12} \circ Z_1 \otimes Z_2 \otimes Z_3 &= \mathrm{pr}_{15}^*(Z_2) \cdot \mathrm{pr}_{24}^*(Z_1) \cdot \mathrm{pr}_{36}^*(Z_3). \end{aligned} \tag{4.32}$$

Thus, $Z_1 \otimes Z_2 \otimes Z_3$ commutes with s_{12} in the ring of correspondences $\mathrm{Corr}^0(X_0(p)^3, X_0(p)^3)$ whenever $Z_1 = Z_2$. In particular, we have

$$t_{[g]} \otimes t_{[g]} \otimes t_f \circ s_{12} = s_{12} \circ t_{[g]} \otimes t_{[g]} \otimes t_f. \tag{4.33}$$

As in the proof of Theorem 4.5, we consider

$$\Pi := \mathrm{pr}_{12}^*(\Delta) \cdot \mathrm{pr}_{34}^*(\Delta) \in \mathrm{Corr}^{-1}(X_0(p)^3, X_0(p)).$$

We compute that

$$(t_{[g]} \otimes t_{[g]} \otimes t_f \circ s_{12}) \circ \Pi = \mathrm{pr}_{12}^*(t_{[g]}) \cdot \mathrm{pr}_{34}^*(t_f) = t_{[g]} \otimes t_{[g]} \otimes t_f \circ \Pi. \tag{4.34}$$

By Lemma 4.9, because we assume $p \equiv 3 \pmod 4$, we have $(s_{12})_*(\Xi) = -\Xi$. By (4.33), we have

$$(s_{12})_*(t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Xi) = (t_{[g]} \otimes t_{[g]} \otimes t_f)_*((s_{12})_*(\Xi)) = -(t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Xi).$$

Applying Π_* to both sides yields

$$\Pi_*(s_{12})_*(t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Xi) = -\Pi_*(t_{[g]} \otimes t_{[g]} \otimes t_f)_*(\Xi) = -P(X_0(p)^3, \Pi_{[g],f}, \Xi).$$

On the other hand, using (4.34), we see that

$$\Pi_*(s_{12})_*(t_{[g]}\otimes t_{[g]}\otimes t_f)_*(\Xi) = \Pi_*(t_{[g]}\otimes t_{[g]}\otimes t_f)_*(\Xi) = P(X_0(p)^3, \Pi_{[g],f}, \Xi).$$

Taken together, we obtain $2P(X_0(p)^3, \Pi_{[g],f}, \Xi) = 0$ in $E_f(\mathbb{Q}(\sqrt{-p}))$. $\square$

4.4 Global root number calculations

Consider the unique quadratic extension $K = \mathbb{Q}(\sqrt{p^\star})$ of $\mathbb{Q}$ ramified only at p introduced in Lemma 4.8. Its associated quadratic Dirichlet character $\chi = \chi_K$ is the Kronecker symbol $\left(\frac{p^\star}{\cdot}\right)$, which is equal to the Legendre symbol at p by Quadratic Reciprocity, as noted previously in Remark 4.15. Following the recipe in Tate's thesis [144], one may lift χ to a unitary Hecke character $\chi_{\mathbb{A}} : \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \longrightarrow \mathbb{C}^\times$ by setting $\chi_{\mathbb{A}}(g) = \prod_v \chi_v(g_v)$ where v runs over all places of $\mathbb{Q}$ and

$$\chi_\infty(g_\infty) = \begin{cases} 1 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1, g_\infty > 0 \\ -1 & \text{if } \chi(-1) = -1, g_\infty < 0 \end{cases} \qquad \chi_\ell(g_\ell) = \begin{cases} \chi(\ell)^{\mathrm{ord}_\ell(g_\ell)} & \text{if } \ell \neq p \\ \chi(j)^{-1} & \text{if } g_p \in p^k(j + p\mathbb{Z}_p). \end{cases}$$

The collection of ℓ-adic characters $\{\chi_\ell : \mathbb{Q}_\ell^\times \longrightarrow \mathbb{C}^\times\}_\ell$ is characterised by the following:

- For $\ell \neq p$, χ_ℓ is unramified with $\chi_\ell(\ell) = \left(\frac{\ell}{p}\right)$.
- χ_p is tamely ramified, $\chi_p(p) = 1$ and $\chi_p|_{\mathbb{Z}_p^\times} = \left(\frac{\cdot}{p}\right)$.

In this section, we set out to compute global root numbers in the following two situations:

1) The twist by the character χ of an elliptic curve over $\mathbb{Q}$ with conductor p.

2) The twist by the character χ of the triple product of normalised newforms in $S_2(\Gamma_0(p))$.

In view of the functional equations of the associated completed L-functions, this gives information about the parity of their orders of vanishing at the centre, which in turn can be used to predict, guided by the Beilinson–Bloch and Birch and Swinnerton-Dyer conjectures, the behaviour of certain cycles and points.

4.4.1 The ramified twist of an elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$ with conductor p. We compute the global root numbers associated to the twist $E^{(p)}$ of E by the quadratic character χ.

Over $K = \mathbb{Q}(\sqrt{p^\star})$, the two elliptic curve E and $E^{(p)}$ are isomorphic. The compatible family of 2-dimensional ℓ-adic representations associated to $E^{(p)}$ is given by $\{\rho_{E,\ell} \otimes \chi\}_\ell$. It follows that the Weil–Deligne representation of $E^{(p)}$ at a prime ℓ is given by

$$\sigma'_{E^{(p)},\ell} = \sigma'_{E,\ell} \otimes \chi_\ell = (\sigma_{E,\ell} \otimes \chi_\ell, N_{E,\ell}). \tag{4.35}$$

Exactly as in Section 1.2.1, we can associate to $E^{(p)}$ a completed L-function

$$\Lambda(E^{(p)}/\mathbb{Q}, s) := \prod_v L(\sigma'_{E^{(p)},v}, s) = 2(2\pi)^{-s}\Gamma(s)L(E^{(p)}/\mathbb{Q}, s).$$

From (4.35) we see that $\Lambda(E^{(p)}/\mathbb{Q}, s) = \Lambda(E/\mathbb{Q}, \chi, s)$ and $L(E^{(p)}/\mathbb{Q}, s) = L(E/\mathbb{Q}, \chi, s)$ are the usual twists of L-functions by characters.

Remark 4.23. Notice that twisting by the finite order character χ does not affect the Hodge structure of E and thus both the local L-factors, ϵ-factors and root numbers at infinity remain unchanged under the action of twisting.

If we set $\Lambda^*(E^{(p)}/\mathbb{Q}, s) := \mathrm{cond}(E^{(p)}/\mathbb{Q})^{\frac{s}{2}}\Lambda(E^{(p)}/\mathbb{Q}, s)$, then this function is conjectured (Conjecture 1.9) to admit analytic continuation to the entire complex plane and satisfy the functional equation

$$\Lambda^*(E^{(p)}/\mathbb{Q},s) = W(E^{(p)}/\mathbb{Q})\Lambda^*(E^{(p)}/\mathbb{Q},2-s) \tag{4.36}$$

where $W(E^{(p)}/\mathbb{Q}) = \prod_v W(\sigma'_{E^{(p)},v}) \in \{\pm 1\}$ is the global root number. In the case at hand, this conjecture is known due to the extension of the modularity theorem of Taylor and Wiles by Breuil, Conrad, Diamond and Taylor [31].

Proposition 4.4. *The local root numbers are given by the following:*

$$\begin{cases} W(\sigma'_{E^{(p)},\ell}) = 1 & \text{for } \ell \neq p \\ W(\sigma'_{E^{(p)},p}) = \left(\frac{-1}{p}\right) & \\ W(\sigma'_{E^{(p)},\infty}) = -1. & \end{cases}$$

In particular, the global root number is

$$W(E^{(p)}/\mathbb{Q}) = -\left(\frac{-1}{p}\right).$$

Remark 4.24. The result in this proposition is not new; it is for instance proved by Pacetti [123, Theorem 3.2]. The proof given here follows the same method. Note also that the elliptic curve $E^{(p)}$ has additive but potentially multiplicative reduction. Indeed, by twisting this curve by χ we recover the elliptic curve E which has multiplicative reduction at p. By [126, §19 Proposition (ii)], the local root number of $E^{(p)}$ at p is $\chi(-1) = \left(\frac{-1}{p}\right)$, which is consistent with Proposition 4.4.

Proof. By Remark 4.23 and Proposition 1.5, the root number at infinity of $E^{(p)}$ is -1 and we may focus on the finite primes. For any prime ℓ, we choose an additive character ψ_ℓ with $n(\psi_\ell) = 0$ as well as the Haar measure $\mathbf{d}x_\ell$ normalised such that $\int_{\mathbb{Z}_\ell} \mathbf{d}x_\ell = 1$.

Consider first the case of a prime ℓ distinct from p. In this case, both the Weil–Deligne representation at ℓ of E and the character χ_ℓ are unramified. By Proposition 1.3, we see that the Weil–Deligne representation of $E^{(p)}$ at ℓ is given by

$$\sigma'_{E^{(p)},\ell} = \sigma_{E,\ell} \otimes \chi_\ell \simeq \chi_\ell \xi_\ell \oplus \chi_\ell \xi_\ell^{-1} \omega_\ell^{-1}$$

for some unramified character ξ_ℓ. Since all the characters involved are unramified, by Theorem 1.1 *i*) and (1.7), we find that

$$\epsilon'(\sigma'_{E^{(p)},\ell}, \psi_\ell, \mathbf{d}x_\ell) = \epsilon(\sigma_{E,\ell} \otimes \chi_\ell, \psi_\ell, \mathbf{d}x_\ell) = 1$$

given the choice of character ψ_ℓ and Haar measure, and thus $W(\sigma'_{E^{(p)},\ell}) = 1$.

We now focus on the situation at p. In this case both $\sigma'_{E,p}$ and χ_p are ramified. Let λ_p be an unramified character of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\lambda_p^2 = 1$ and the twist E^{λ_p} of E by λ_p has split multiplicative reduction at p. By Proposition 1.4 we have

$$\sigma'_{E^{(p)},p} = \chi_p \lambda_p \omega_p^{-1} \otimes \mathrm{sp}(2).$$

If V denotes the complex vector space associated to $\sigma'_{E^{(p)},p}$, then $V = \mathbb{C}(\chi_p \lambda_p \omega_p^{-1}) \otimes \mathbb{C}^2$ and $V^{I_p} = \mathbb{C}(\chi_p \lambda_p \omega_p^{-1})^{I_p} \otimes \mathbb{C}^2$. But $\mathbb{C}(\chi_p \lambda_p \omega_p^{-1})^{I_p} = 0$ since χ_p is ramified, and consequently $V^{I_p} = 0$. It follows that $\delta(\sigma'_{E^{(p)},p}) = 1$ and $\epsilon'(\sigma'_{E^{(p)},p}, \psi_p, \mathbf{d}x_p) = \epsilon(\sigma_{E^{(p)},p}, \psi_p, \mathbf{d}x_p)$. By Definition 1.5, $\sigma_{E^{(p)},p} = \chi_p \lambda_p \omega_p^{-1} \oplus \chi_p \lambda_p$, and thus, by successively applying Theorem 1.1 *i*), Proposition 1.1 and Corollary 1.1, we obtain

$$\begin{aligned}
\epsilon(\sigma_{E^{(p)},p}, \psi_p, \mathbf{d}x_p) &= \epsilon(\chi_p \lambda_p \omega_p^{-1}, \psi_p, \mathbf{d}x_p)\epsilon(\chi_p \lambda_p, \psi_p, \mathbf{d}x_p) \\
&= \epsilon(\chi_p, \psi_p, \mathbf{d}x_p)^2 \lambda_p^2 \omega_p^{-1}(p^{a(\chi_p)}) \\
&= \chi_p(-1)p^2 \\
&= \left(\frac{-1}{p}\right) p^2,
\end{aligned}$$

since $a(\chi_p) = 1$. We conclude that $W(\sigma'_{E^{(p)},p}) = \left(\frac{-1}{p}\right)$. □

Remark 4.25. Going through the proof, we see that if $\ell \neq p$, then $\sigma'_{E^{(p)},\ell}$ is unramified and thus $a(\sigma'_{E^{(p)},\ell}) = 0$. At p we saw that $\dim V^{I_p}/V_{N,p}^{I_p} = 0$ and the Weil representation $\sigma_{E,p} \otimes \chi_p$ is ramified because χ_p is tamely ramified, i.e., $a(\chi_p) = 1$. Thus

$$a(\sigma'_{E^{(p)},p}) = a(\sigma_{E,p} \otimes \chi_p) = a(\chi_p \lambda_p \omega_p^{-1}) + a(\chi_p \lambda_p) = 2a(\chi_p) = 2.$$

In conclusion, we find that

$$\mathrm{cond}(E^{(p)}/\mathbb{Q}) = \prod_{\ell} \ell^{a(\sigma'_{E^{(p)},\ell})} = p^2.$$

In particular, the completed L-function takes the shape

$$\Lambda^*(E^{(p)}/\mathbb{Q}, s) = p^s 2(2\pi)^{-s}\Gamma(s) L(E/\mathbb{Q}, \chi, s).$$

4.4.2 The triple product root number

Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$. We are interested in computing the global root number of the triple product L-function $\Lambda(F, s)$ of Section 4.1.2, as announced in Remark 4.8. A formula for this root number is stated in [76]. The proof serves as a stepping stone to calculate the twisted root number in the next section.

Proposition 4.5. *The local root numbers are given by the following:*

$$\begin{cases} W(\sigma'_{F,q}) = 1 & \text{for } q \neq p \\ W(\sigma'_{F,p}) = -a_p(f_1)a_p(f_2)a_p(f_3) & \\ W(\sigma'_{\mathbf{E},\infty}) = -1. & \end{cases}$$

In particular, the global root number is

$$W(F) = a_p(f_1)a_p(f_2)a_p(f_3).$$

Proof. For any prime ℓ, we choose an additive character ψ_ℓ with $n(\psi_\ell) = 0$ as well as the Haar measure $\mathbf{d}x_\ell$ normalised such that $\int_{\mathbb{Z}_\ell} \mathbf{d}x_\ell = 1$.

Let q be a prime distinct from p. By Proposition 4.2 we have, for $i \in \{1, 2, 3\}$,

$$\sigma'_{f_i,q} = \sigma_{f_i,q} = \xi_{i,q} \oplus \xi_{i,q}^{-1}\omega_q^{-1}$$

for some unramified characters $\xi_{i,q}$. We therefore obtain

$$\sigma'_{F,q} = \sigma_{F,q} = \xi_{1,q}\xi_{2,q}\xi_{3,q} \oplus \xi_{1,q}\xi_{2,q}^{-1}\xi_{3,q}\omega_q^{-1} \oplus \xi_{1,q}^{-1}\xi_{2,q}\xi_{3,q}\omega_q^{-1} \oplus \xi_{1,q}^{-1}\xi_{2,q}^{-1}\xi_{3,q}\omega_q^{-2}$$
$$\oplus\, \xi_{1,q}\xi_{2,q}\xi_{3,q}^{-1}\omega_q^{-1} \oplus \xi_{1,q}\xi_{2,q}^{-1}\xi_{3,q}^{-1}\omega_q^{-2} \oplus \xi_{1,q}^{-1}\xi_{2,q}\xi_{3,q}^{-1}\omega_q^{-2} \oplus \xi_{1,q}^{-1}\xi_{2,q}^{-1}\xi_{3,q}^{-1}\omega_q^{-3}.$$

Since all characters involved are unramified, Theorem 1.1 *i*) and (1.7) imply, given the choice of ψ_q and $\mathbf{d}x_q$, that

$$\epsilon'(\sigma'_{F,q}, \psi_q, \mathbf{d}x_q) = 1,$$

and in particular $W(\sigma'_{F,q}) = 1$.

We turn to the Weil–Deligne representation at p. For each $i \in \{1, 2, 3\}$, let λ_i be the unramified quadratic character of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ defined by $\lambda_i(\Phi) = a_p(f_i)$, where Φ denotes an inverse Frobenius element. We will sometimes view it as a character of $\mathbb{Q}_p^\times$ via the identification (1.1). Let $\lambda = \lambda_1\lambda_2\lambda_3$ denote the product of these characters. By Proposition 4.2, the Weil–Deligne representation of F at p is given by

$$\sigma'_{F,p} = \lambda\omega_p^{-3} \otimes \mathrm{sp}(2)^{\otimes 3}.$$

For simplicity in this proof, we shall drop the subscript p and write $\omega = \omega_p, \psi_p = \psi$ and $\mathbf{d}x_p = \mathbf{d}x$. If (e_0, e_1) denotes the standard basis of $\mathbb{C}^2$, then $\mathrm{sp}(2)$ is the representation (σ, N)

defined in Definition 1.5 by the matrices

$$\sigma := \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \qquad \text{and} \qquad N := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Let us denote by $V_i = \mathbb{C}^2$ the complex vector space associated to $\sigma'_{f_i,p}$ and by $\{e_0^{(i)}, e_1^{(i)}\}$ its standard basis for each $i \in \{1,2,3\}$. Then $V = V_1 \otimes_{\mathbb{C}} V_2 \otimes_{\mathbb{C}} V_3 = \mathbb{C}^8$ is the space of $\sigma'_{F,p}$ and an ordered basis for it is given by

$$\begin{aligned} B := (&e_0^{(1)} \otimes e_0^{(2)} \otimes e_0^{(3)}, e_0^{(1)} \otimes e_0^{(2)} \otimes e_1^{(3)}, e_0^{(1)} \otimes e_1^{(2)} \otimes e_0^{(3)}, e_0^{(1)} \otimes e_1^{(2)} \otimes e_1^{(3)}, \\ &e_1^{(1)} \otimes e_0^{(2)} \otimes e_0^{(3)}, e_1^{(1)} \otimes e_0^{(2)} \otimes e_1^{(3)}, e_1^{(1)} \otimes e_1^{(2)} \otimes e_0^{(3)}, e_1^{(1)} \otimes e_1^{(2)} \otimes e_1^{(3)}). \end{aligned} \tag{4.37}$$

With respect to the basis B, the representation

$$\mathrm{sp}(2)^{\otimes 3} = (\sigma^{\otimes 3}, N^{\otimes 3} := N \otimes 1 \otimes 1 + 1 \otimes N \otimes 1 + 1 \otimes 1 \otimes N)$$

is given by the matrices

$$\sigma^{\otimes 3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^3 \end{pmatrix} \qquad \text{and} \qquad N^{\otimes 3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

We conclude that

$$\sigma_{F,p} \simeq \lambda\omega^{-3} \oplus \lambda\omega^{-2} \oplus \lambda\omega^{-2} \oplus \lambda\omega^{-1} \oplus \lambda\omega^{-2} \oplus \lambda\omega^{-1} \oplus \lambda\omega^{-1} \oplus \lambda. \tag{4.38}$$

In particular, the Weil representation $\sigma_{F,p}$ is unramified but the Weil–Deligne representation $\sigma'_{F,p}$ is not, as $N_{F,p} = N^{\otimes 3} \neq 0$.

We start by computing the factor $\delta(\sigma'_{F,p})$ defined in (1.4). Since $\sigma_{F,p}$ is unramified, we have $V^{I_p} = V$ and $V^{I_p} \cap \ker(N_{F,p}) = \ker(N_{F,p})$. The reduced row echelon form of $N_{F,p}$ is given by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and thus

$$\ker(N_{F,p}) = \{(0,0,0,x_4,0,x_6,-x_4-x_6,x_8) \in \mathbb{C}^8 \mid x_4,x_6,x_8 \in \mathbb{C}\}$$

is of dimension 3. As a subspace of V, a basis for $V/\ker(N_{F,p})$ can be taken to be

$$(e_0^{(1)} \otimes e_0^{(2)} \otimes e_0^{(3)}, e_0^{(1)} \otimes e_0^{(2)} \otimes e_1^{(3)}, e_0^{(1)} \otimes e_1^{(2)} \otimes e_0^{(3)}, e_0^{(1)} \otimes e_1^{(2)} \otimes e_1^{(3)}, e_1^{(1)} \otimes e_0^{(2)} \otimes e_0^{(3)}),$$

that is, the 5 first basis elements in B. With respect to this basis, the action of $\sigma_{F,p}$ on $V^{I_p}/(V^{I_p} \cap \ker(N_{F,p}))$ is given by the matrix

$$\begin{pmatrix} \lambda\omega^{-3} & 0 & 0 & 0 & 0 \\ 0 & \lambda\omega^{-2} & 0 & 0 & 0 \\ 0 & 0 & \lambda\omega^{-2} & 0 & 0 \\ 0 & 0 & 0 & \lambda\omega^{-1} & 0 \\ 0 & 0 & 0 & 0 & \lambda\omega^{-2} \end{pmatrix}.$$

Recall from Definition 1.2 that $\omega(\Phi) = p^{-1}$. We deduce that

$$\delta(\sigma'_{F,p}) = -p^{10}\lambda^5(\Phi). \tag{4.39}$$

Since $\lambda(\Phi) \in \{\pm 1\}$, we see that $\lambda^5(\Phi) = \lambda(\Phi)$, and we obtain

$$\delta(\sigma'_{F,p}) = -p^{10}a_p(f_1)a_p(f_2)a_p(f_3).$$

We now compute the epsilon factor of the Weil representation $\sigma_{F,p}$. By Theorem 1.1 i) and the isomorphism (4.38), we see that

$$\epsilon(\sigma_{F,p}, \psi, \mathbf{d}x) = \epsilon(\lambda\omega^{-3}, \psi, \mathbf{d}x)\epsilon(\lambda\omega^{-2}, \psi, \mathbf{d}x)^3\epsilon(\lambda\omega^{-1}, \psi, \mathbf{d}x)^3\epsilon(\lambda, \psi, \mathbf{d}x).$$

Since all characters involved are unramified, (1.7) implies, given the choice of ψ_q and $\mathbf{d}x_q$, that $\epsilon(\sigma_{F,p}, \psi, \mathbf{d}x) = 1$. We conclude that

$$\epsilon'(\sigma'_{F,p}, \psi, \mathbf{d}x) = -p^{10}a_p(f_1)a_p(f_2)a_p(f_3),$$

and in particular

$$W(\sigma'_{F,p}) = -a_p(f_1)a_p(f_2)a_p(f_3).$$

Finally, we take care of the infinite place. Recall from (4.11) that

$$\sigma'_{F,\infty} = (\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\,\varphi_{1,2} \otimes H^{1,2}(\mathbf{E})) \oplus (\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\,\varphi_{0,3} \otimes H^{0,3}(\mathbf{E})) : W(\mathbb{C}/\mathbb{R}) \longrightarrow \mathbf{GL}_8(\mathbb{C}),$$

where the relevant Hodge numbers are given by (4.10). By Theorem 1.1 i), we have

$$\epsilon(\sigma'_{F,\infty}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = \epsilon(\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\,\varphi_{1,2}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}})^3\epsilon(\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\,\varphi_{0,3}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}).$$

By Theorem 1.1 *ii*) we have, for $p, q \in \mathbb{Z}$,

$$\epsilon(\operatorname{ind}_{\mathbb{C}/\mathbb{R}} \varphi_{p,q}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = \epsilon(\varphi_{p,q}, \psi_{\mathbb{C}}, \mathbf{d}x_{\mathbb{C}}) \frac{\epsilon(\operatorname{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}})}{\epsilon(1_{\mathbb{C}}, \psi_{\mathbb{C}}, \mathbf{d}x_{\mathbb{C}})}.$$

Recall from the proof of Proposition 1.5 that

$$\frac{\epsilon(\operatorname{ind}_{\mathbb{C}/\mathbb{R}} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}})}{\epsilon(1_{\mathbb{C}}, \psi_{\mathbb{C}}, \mathbf{d}x_{\mathbb{C}})} = i.$$

We deduce from (1.5) that

$$\epsilon(\sigma'_{F,\infty}, \psi_{\mathbb{R}}, \mathbf{d}x_{\mathbb{R}}) = (i^{2-1} \cdot i)^3 (i^{3-0} \cdot i) = (-1) \cdot 1 = -1.$$

□

Remark 4.26. We extract the conductor $\operatorname{cond}(W(F)/\mathbb{Q})$ from the proof, as promised in Remark 4.8. When q is distinct from p, we saw that $\sigma'_{F,q}$ is unramified, hence $a(\sigma'_{F,q}) = 0$. At the prime p we established that $\dim V^{I_p}/V^{I_p}_{N_{F,p}} = 5$. Moreover, the Weil representation $\sigma_{F,p}$ is unramified, so $a(\sigma_{F,p}) = 0$. We deduce that $a(\sigma'_{F,p}) = 5$ and

$$\operatorname{cond}(W(F)/\mathbb{Q}) = \prod_{\ell} \ell^{a(\sigma'_{F,p})} = p^5.$$

In particular, the completed L-function takes the shape

$$\Lambda^*(F, s) = 2^4 p^{\frac{5}{2}s} (2\pi)^{-s} \Gamma(s) L(F, s).$$

4.4.3 The ramified quadratic twist of triple products

Let χ denote the quadratic character of conductor p associated to the quadratic extension $K = \mathbb{Q}(\sqrt{p^\star})$ of $\mathbb{Q}$. Recall from the beginning of Section 4.4 that associated to it is the collection of ℓ-adic characters $\{\chi_\ell : \mathbb{Q}_\ell^\times \longrightarrow \mathbb{C}^\times\}_\ell$ characterised by the following:

- For $\ell \neq p$, χ_ℓ is unramified with $\chi_\ell(\ell) = \left(\frac{\ell}{p}\right)$.
- χ_p is tamely ramified, $\chi_p(p) = 1$ and $\chi_p|_{\mathbb{Z}_p^\times} = \left(\frac{\cdot}{p}\right)$.

Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$, and let $F = f_1 \otimes f_2 \otimes f_3$. Let $M(F)^{(p)}$ denote the motive $M(F) \otimes \chi \in \mathbf{Chow}(\mathbb{Q})_{K_F}$ obtained from $M(F)$ by twisting by χ. We will write $F^{(p)} = f_1 \otimes f_2 \otimes f_3 \otimes \chi$. The compatible family of 8-dimensional ℓ-adic representations associated to $M(F)^{(p)}$ is given by

$$\{V_\ell(f_1) \otimes V_\ell(f_2) \otimes V_\ell(f_3) \otimes \chi\}_\ell. \tag{4.40}$$

It follows that the Weil–Deligne representation of $M(F)^{(p)}$ at q is given by

$$\sigma'_{F^{(p)},q} = \sigma'_{F,q} \otimes \chi_q = (\sigma_{F,q} \otimes \chi_q, N_{F,q}).$$

Exactly as in Section 4.1.2, we can associate to $M(F)^{(p)}$ a completed L-function

$$\Lambda(M(F)^{(p)}/\mathbb{Q}, s) := \prod_v L(\sigma'_{F^{(p)},v}, s) = 2^4(2\pi)^{3-4s}\Gamma(s-1)^3\Gamma(s)L(M(F)^{(p)}/\mathbb{Q}, s).$$

We will often write $\Lambda(F^{(p)}, s) = \Lambda(M(F)^{(p)}/\mathbb{Q}, s)$ and $L(F^{(p)}, s) = L(M(F)^{(p)}/\mathbb{Q}, s)$. From (4.40), we see that $\Lambda(F^{(p)}, s) = \Lambda(F, \chi, s)$ and $L(F^{(p)}, s) = L(F, \chi, s)$ are the usual twists of L-functions by characters.

Remark 4.27. Twisting by the finite order character χ does not affect the Hodge structure of $M(F)$ and thus both the local L-factors, ϵ-factors and root numbers at infinity remain unchanged under the action of twisting by χ.

If we set $\Lambda^*(F^{(p)}, s) := \mathrm{cond}(M(F)^{(p)}/\mathbb{Q})^{\frac{s}{2}}\Lambda(F^{(p)}, s)$, then this function is conjectured (Conjecture 1.9) to admit analytic continuation to the entire complex plane and satisfy the functional equation

$$\Lambda^*(F^{(p)}, s) = W(F^{(p)})\Lambda^*(F^{(p)}, 4-s), \tag{4.41}$$

where $W(F^{(p)}) = \prod_v W(\sigma'_{F^{(p)},v}) \in \{\pm 1\}$ is the global root number of $M(F)^{(p)}$.

Remark 4.28. Notice that $F^{(p)}$ is equal to the tensor product of the three normalised newforms f_1, f_2 and $f_3^{(p)}$, where $f_3^{(p)} = f_3 \otimes \chi$. The L-function $\Lambda^*(F^{(p)}/\mathbb{Q}, s)$ is the triple product L-function associated to the triple $(f_1, f_2, f_3^{(p)})$. The first two forms have level $\Gamma_0(p)$ while the form $f_3^{(p)}$ has level $\Gamma_0(p^2)$ by Remark 4.25 adapted to the case of modular forms. Hence the analytic properties and functional equation of $\Lambda^*(F^{(p)}/\mathbb{Q}, s)$ fall outside the scope of [76] where the case of three forms of the same square-free level is treated. However, as explained in [82], the analytic properties and functional equation in this case follow from [124].

Theorem 4.7. *The local root numbers are given by the following:*

$$\begin{cases} W(\sigma'_{F^{(p)},q}) = 1 & \text{for } q \neq p \\ W(\sigma'_{F^{(p)},p}) = 1 \\ W(\sigma'_{F^{(p)},\infty}) = -1. \end{cases}$$

In particular, the global root number is

$$W(F^{(p)}) = -1.$$

Proof. By Remark 4.27 and Proposition 4.5, the root number at infinity of $F^{(p)}$ is -1 and we therefore focus on the finite places. For any prime ℓ, we choose an additive character ψ_ℓ with $n(\psi_\ell) = 0$ as well as the Haar measure $\mathbf{d}x_\ell$ normalised such that $\int_{\mathbb{Z}_\ell} \mathbf{d}x_\ell = 1$.

At a prime q distinct from p, the representation $\sigma'_{F^{(p)},q}$ is unramified, hence equal to the underlying Weil representation which decomposes as a sum of unramified characters. Just as in the proof of Proposition 4.5 we obtain $\epsilon'(\sigma'_{F^{(p)},q}, \psi_q, \mathbf{d}x_q) = 1$ and $W(\sigma'_{F^{(p)},q}) = 1$.

For each $i \in \{1, 2, 3\}$, let λ_i be the unramified quadratic character of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ defined by $\lambda_i(\Phi) = a_p(f_i)$, where Φ denotes an inverse Frobenius element. We will sometimes view it as a character of $\mathbb{Q}_p^\times$ via the identification (1.1). Let $\lambda = \lambda_1\lambda_2\lambda_3$ denote the product of these characters. By Proposition 4.2, the Weil–Deligne representation of $M(F)^{(p)}$ at p is given by

$$\sigma'_{F,p} \otimes \chi_p = \chi_p \lambda \omega_p^{-3} \otimes \mathrm{sp}(2)^{\otimes 3}.$$

Let V denote the complex vector space associated to it. The character χ_p is tamely ramified, i.e., $a(\chi_p) = 1$. Suppose, by contradiction, that $V^{I_p} \neq 0$. Then there is a non-zero vector $v \in V$ which is fixed by the action of the inertia I_p. But $\sigma_{F^{(p)},p}(g)(v) = \chi_p(g)v$ for all $g \in I_p$ since $\sigma_{F,p}$ is unramified. As $v \in V^{I_p}$, we must have $\chi_p(g)v = v$ which implies that $\chi_p(g) = 1$ since $v \neq 0$. Since this holds for all $g \in I_p$, it contradicts the fact that χ_p is ramified. Hence $V^{I_p} = 0$ and as a consequence $\delta(\sigma'_{F,p} \otimes \chi_p) = 1$.

With respect to the basis B of $\mathbb{C}^8$ from (4.37) in the proof of Proposition 4.5, we know that the Weil representation $\sigma_{F,p}$ decomposes as a sum of unramified characters (4.38) so that

$$\sigma_{F,p} \otimes \chi_p \simeq \chi_p\lambda\omega_p^{-3} \oplus \chi_p\lambda\omega_p^{-2} \oplus \chi_p\lambda\omega_p^{-2} \oplus \chi_p\lambda\omega_p^{-1} \oplus \chi_p\lambda\omega_p^{-2} \oplus \chi_p\lambda\omega_p^{-1} \oplus \chi_p\lambda\omega_p^{-1} \oplus \chi_p\lambda \quad (4.42)$$

and by Theorem 1.1 *i*) and Proposition 1.1, we obtain

$$\epsilon(\sigma_{F,p} \otimes \chi_p, \psi_p, \mathbf{d}x_p) = \lambda^8 \omega_p^{-12} (p^{(n(\psi)\dim(\chi_p) + a(\chi_p))}) \epsilon(\chi_p, \psi, \mathbf{d}x)^8 = p^{12} \epsilon(\chi_p, \psi_p, \mathbf{d}x_p)^8,$$

since $a(\chi_p) = 1$ and λ is a quadratic character. By Corollary 1.1, we see that

$$\epsilon(\sigma_{F,p} \otimes \chi_p, \psi_p, \mathbf{d}x_p) = p^{12}(p\chi_p(-1))^4 = p^{16}.$$

In conclusion, we have proved that $W(\sigma'_{F^{(p)},p}) = 1$. □

Remark 4.29. We proceed to extract the conductor $\mathrm{cond}(M(F)^{(p)}/\mathbb{Q})$ from the proof. When q is distinct from p, we saw that $\sigma'_{F^{(p)},q}$ is unramified, hence $a(\sigma'_{F^{(p)},q}) = 0$. At the prime p we established that $\dim V^{I_p}/V_{N_{F,p}}^{I_p} = 0$. We therefore have

$$a(\sigma'_{F^{(p)},p}) = a(\chi_p\lambda\omega_p^{-3}) + 3a(\chi_p\lambda\omega_p^{-2}) + 3a(\chi_p\lambda\omega_p^{-1}) + a(\chi_p\lambda) = 8a(\chi_p) = 8.$$

We conclude that

$$\mathrm{cond}(M(F)^{(p)}/\mathbb{Q}) = \prod_{\ell} \ell^{a(\sigma'_{F^{(p)},p})} = p^8.$$

In particular, the completed L-function takes the shape

$$\Lambda^*(F^{(p)}/\mathbb{Q}, s) = p^{4s}(2\pi)^{-s}\Gamma(s)L(F,\chi,s).$$

4.5 Questions and conjectures

In Section 4.2, we constructed 6 cycles of codimension 2 on $X_0(p)^3$. Understanding the torsion or non-torsion properties of these cycles is a key motivation for us, as this could lead to new instances of the Beilinson–Bloch conjecture (4.14), with applications towards the Birch and Swinnerton-Dyer conjecture 1.2 via the theory of Chow–Heegner points. Based on the results so far, we formulate in this section refinements of these conjectures in a setting that has not been considered before.

4.5.1 Conjectures about cycles

Let f_1, f_2, f_3 be three normalised eigenforms in $S_2(\Gamma_0(p))$ and let $F = f_1 \otimes f_2 \otimes f_3$ denote their triple product. Recall that χ denotes the Legendre symbol at p, which is the character attached to the quadratic extension $K = \mathbb{Q}(\sqrt{p^\star})$, where $p^\star = \chi(-1)p$. If we denote by $L(F/K, s) := L(M(F)/K, s)$ the L-function attached to the motive $M(F)$ base changed to K, then we have the equality of L-functions

$$L(F/K, s) = L(F, s)L(F^{(p)}, s), \tag{4.43}$$

where, in the notations of Section 4.4.3, $F^{(p)} = f_1 \otimes f_2 \otimes f_3 \otimes \chi$ is the twisted triple product. The Beilinson–Bloch conjecture in the triple product situation base-changed to K predicts that

$$\mathrm{ord}_{s=2} L(F/K, s) = \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(K) \otimes K_F). \tag{4.44}$$

Let τ denote the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and note that we have a decomposition

$$\mathrm{CH}^2(X_0(p)^3)_0(K) = \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \oplus \mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1} \tag{4.45}$$

into eigenspaces for τ, after identifying $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q})$ with $\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=1}$. In light of the decompositions (4.43) and (4.45), and conjectures (4.14) and (4.44), we are lead to expect the following equality

$$\mathrm{ord}_{s=2} L(F^{(p)}, s) = \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1} \otimes K_F). \tag{4.46}$$

Theorem 4.7 asserts that $W(F^{(p)}) = -1$, i.e., the L-function $L(F^{(p)}, s)$ vanishes to odd order at its centre $s = 2$. In particular, we always have $\mathrm{ord}_{s=2} L(F^{(p)}, s) \geq 1$, and thus we expect the dimension of $(t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1} \otimes K_F)$ to be at least one. The construction of cycles in Section 4.2.2 provides a special cycle Ξ of codimension 2 on $X_0(p)^3$. It is null-homologous by Theorem 4.3, and by Lemma 4.8 we have

$$\Xi \in \mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}.$$

Strikingly, this is precisely the piece of the Chow group that the global root number calculations suggest should contain a non-torsion element. Moreover, the construction of Ξ is canonical and depends on no choice of base-point as opposed to the Gross–Kudla–Schoen cycle. It exhibits no apparent geometric reason to be torsion. Finally, the construction of Ξ relies on the properties of the curves $X_0(p)$ as a solution to a moduli problem; the construction is arithmetic by nature and is not available for generic curves, as opposed to the diagonal construction of Δ_{GKS}. All in all, the cycle Ξ seems to be an interesting object, which promises to contain rich arithmetic information about triple products of modular forms. Guided by conjecture (4.46), we are thus confident in formulating the following conjecture.

Conjecture 4.1. *Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and denote by $F = f_1 \otimes f_2 \otimes f_3$ the associated triple product. The cycle*

$$(t_F)_*(\Xi) \in \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star}))^{\tau=-1} \otimes K_F$$

is non-zero if and only if $\mathrm{ord}_{s=2} L(F^{(p)}, s) = 1$.

Remark 4.30. Note that Conjecture 4.1 implies that

$$\mathrm{ord}_{s=2} L(F^{(p)}, s) = 1 \implies \dim_{K_F} (t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star}))^{\tau=-1} \otimes K_F) \geq 1,$$

and thus offers insight into a particular case of the Beilinson–Bloch conjecture that has never been considered before.

We specialise further by distinguishing between two situations depending on the root number of F.

Conjecture 4.2. *Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and denote by $F = f_1 \otimes f_2 \otimes f_3$ the associated triple product. If we assume that $W(F) = +1$, then* $\mathrm{ord}_{s=2} L(F/\mathbb{Q}(\sqrt{p^\star}), s) = 1$ *if and only if*

$$(t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star})) \otimes K_F) = K_F \cdot (t_F)_*(\Xi).$$

Remark 4.31. Since we assume $W(F) = +1$, we have $\mathrm{ord}_{s=2} L(F/K, s) = 1$ if and only if $\mathrm{ord}_{s=2} L(F, s) = 0$ and $\mathrm{ord}_{s=2} L(F^{(p)}, s) = 1$. Hence Conjecture 4.2 is implied by Conjectures 4.1 and (4.14). Note that Theorem 4.4 implies in this setting that the Abel–Jacobi image of $(t_F)_*(\Delta_{\mathrm{GKS}}(e))$ is torsion. This suggests, but does not prove, that $(t_F)_*(\Delta_{\mathrm{GKS}}(e))$ is zero in

$(t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes K_F)$. See Remark 4.20. In particular, Theorem 4.4 and Remark 4.21 can be seen as lending support to conjecture (4.14) and thus also to Conjecture 4.2.

Conjecture 4.3. *Let f_1, f_2, f_3 be three normalised newforms in $S_2(\Gamma_0(p))$ and denote by $F = f_1 \otimes f_2 \otimes f_3$ the associated triple product. If we assume that $W(F) = -1$, then* $\mathrm{ord}_{s=2} L(F/\mathbb{Q}(\sqrt{p^\star}), s) = 2$ *if and only if*

$$(t_F)_*(\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star})) \otimes K_F) = K_F \cdot (t_F)_*(\Delta_{\mathrm{GKS}}) \oplus K_F \cdot (t_F)_*(\Xi).$$

Remark 4.32. Since we assume $W(F) = -1$, we have

$$W(F/K) = W(F) \cdot W(F^{(p)}) = (-1) \cdot (-1) = +1,$$

so that $\mathrm{ord}_{s=2} L(F/K, s)$ is even. But $L(F/K, 2) = 0$ and thus $\mathrm{ord}_{s=2} L(F/K, s) \geq 2$. Note that $\mathrm{ord}_{s=2} L(F/K, s) = 2$ if and only if $\mathrm{ord}_{s=2} L(F, s) = \mathrm{ord}_{s=2} L(F^{(p)}, s) = 1$. The conjectural formula (4.19) implies that $(t_F)_*(\Delta_{\mathrm{GKS}})$ is non-zero in $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}) \otimes K_F$ if $\mathrm{ord}_{s=2} L(F, s) = 1$. The converse holds if the Beilinson–Bloch pairing is non-degenerate (as conjectured in [29]). Hence Conjecture 4.3 is implied by Conjectures 4.1, (4.14) and (4.19).

4.5.2 Conjectures about points

Let us specialise to the setting where two of the newforms are the same, and the third one has rational coefficients. Let f be a normalised newform in $S_2(\Gamma_0(p))$ with rational coefficients and let g be another normalised newform in $S_2(\Gamma_0(p))$ which is not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to f. We let E_f and $A_{[g]}$ denote the elliptic curve and abelian variety over $\mathbb{Q}$ which are respectively associated to f and $[g]$ by the Eichler–Shimura construction of Section 1.2.3.

As in Section 4.4.1, we denote by $E_f^{(p)}$ the quadratic twist of E_f by the Legendre symbol χ. We have the following equality of L-functions

$$L(E_f/K, s) = L(E_f/\mathbb{Q}, s) L(E_f^{(p)}/\mathbb{Q}, s),$$

where as usual $K = \mathbb{Q}(\sqrt{p^\star})$. The elliptic curve E_f admits multiplicative reduction at p, and thus, by Proposition 4.5 and Proposition 1.5, we have

$$W(g, g, f) = a_p(g)^2 a_p(f) = a_p(f) = a_p(E_f) = W(E_f/\mathbb{Q}). \tag{4.47}$$

By Proposition 4.4, we have $W(E_f^{(p)}/\mathbb{Q}) = -\chi(-1)$. In particular, we obtain

$$W(E_f/K) = W(E_f/\mathbb{Q})W(E_f^{(p)}/\mathbb{Q}) = -a_p(E_f)\chi(-1) = \begin{cases} -a_p(E_f) & \text{if } p \equiv 1 \pmod 4 \\ a_p(E_f) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Let $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ denote the non-trivial element and observe that we have a decomposition

$$E_f(K) = E_f(\mathbb{Q}) \oplus E_f(K)^{\tau=-1},$$

after identifying $E_f(\mathbb{Q}) = E_f(K)^{\tau=1}$. The Birch and Swinnerton-Dyer conjecture 1.2 predicts the equalities

$$\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}, s) = \mathrm{rank}_{\mathbb{Z}} E_f(\mathbb{Q}) \tag{4.48}$$

$$\mathrm{ord}_{s=1} L(E_f/K, s) = \mathrm{rank}_{\mathbb{Z}} E_f(K). \tag{4.49}$$

In particular, it predicts that

$$\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = \mathrm{rank}_{\mathbb{Z}} E_f(K)^{\tau=-1}. \tag{4.50}$$

Recall the Chow–Heegner construction in the context of the triple product of the modular curve $X_0(p)$ outlined in Section 4.1.3. In particular, we introduced a generalised modular parametrisation

$$\Pi_{[g],f,*} = \pi_f \circ \Pi_{[g],*} : \mathrm{CH}^2(X_0(p)^3)_0 \longrightarrow E_f.$$

By applying it to the special cycle $\Xi \in \mathrm{CH}^2(X_0(p)^3)_0(K)^{\tau=-1}$, we obtain a Chow–Heegner point

$$P(X_0(p)^3, \Pi_{[g],f}, \Xi) = \pi_f(\Pi_{[g],*}(\Xi)) \in E_f(K)^{\tau=-1}.$$

Given Conjecture 4.1 and the equality of correspondences (4.30), it is natural to conjecture that $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ has infinite order in $E_f(K)^{\tau=-1}$ whenever the order of vanishing of the L-function $L(E_f^{(p)}/\mathbb{Q}, s)$ respects the Birch and Swinnerton-Dyer conjecture and the conditions of Conjecture 4.1 are satisfied. Recall that

$$W(E_f^{(p)}/\mathbb{Q}) = -\chi(-1) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4 \\ +1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

If $F = g \otimes g \otimes f$, then note that we have the following decompositions of triple product L-functions

$$L(F, s) = L(\mathrm{Sym}^2(g) \otimes f, s) L(f, s-1) \tag{4.51}$$

$$L(F^{(p)}, s) = L(\mathrm{Sym}^2(g) \otimes f^{(p)}, s) L(f^{(p)}, s-1). \tag{4.52}$$

Conjecture 4.4. *Let f and g be newforms in $S_2(\Gamma_0(p))$ as above. If $p \equiv 1 \pmod 4$, then $P(X_0(p)^3, \Pi_{[g],f}, \Xi) \in E_f(\mathbb{Q}(\sqrt{p}))^{\tau=-1}$ has infinite order if and only if $\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$.*

Remark 4.33. If $p \equiv 3 \pmod 4$, then $W(E_f^{(p)}/\mathbb{Q}) = +1$ and by the work of Bhargava and Shankar [19], we generically expect $\mathrm{ord}_{s=1} L(E_f^{(p)}, s) = 0$, hence (4.50) predicts that the point $P(X_0(p)^3, \Pi_{[g],f}, \Xi) \in E_f(\mathbb{Q}(\sqrt{-p}))^{\tau=-1}$ is torsion in this case. This was proved in Theorem 4.6 by exploiting Lemma 4.9.

As in the previous section, we now specialise further to two situations depending on the global root number of E_f.

Conjecture 4.5. *Let $f, g \in S_2(\Gamma_0(p))$ be newforms as above and assume $p \equiv 1 \pmod 4$. If E_f admits split multiplicative reduction at p, then we have $\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}(\sqrt{p}), s) = 1$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$ if and only if*

$$E_f(\mathbb{Q}(\sqrt{p})) \otimes \mathbb{Q} = \mathbb{Q} \cdot P(X_0(p)^3, \Pi_{[g],f}, \Xi).$$

Remark 4.34. Since E_f admits split multiplicative reduction at p, we have $a_p(E_f) = 1$ and $W(E_f(\mathbb{Q})) = 1$. Since $p \equiv 1 \pmod 4$, we have $W(E_f^{(p)}/\mathbb{Q}) = -1$. In particular, we have $\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}(\sqrt{p}), s) = 1$ if and only if

$$\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}, s) = 0 \qquad \text{and} \qquad \mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1.$$

By Theorem 4.5, the points $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}(e)) \in E_f(\mathbb{Q})$ are all torsion. More generally, by the work of Gross, Zagier and Kolyvagin [75, 78, 103], we know (6) that all points in $E(\mathbb{Q})$ are torsion. Hence Conjecture 4.5 is implied by Conjectures 4.4 and (4.50). Note that if h is another normalised newform in $S_2(\Gamma_0(p))$, not $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ conjugate to g or f, but satisfying the condition $L(\mathrm{Sym}^2(h^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_h \hookrightarrow \mathbb{C}$, then Conjecture 4.5 implies that $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ and $P(X_0(p)^3, \Pi_{[h],f}, \Xi)$ are linearly dependent, i.e., one is a multiple of the other.

Conjecture 4.6. *Let $f, g \in S_2(\Gamma_0(p))$ be newforms as above and assume $p \equiv 1 \pmod 4$. If E_f admits non-split multiplicative reduction at p, then $\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}(\sqrt{p}), s) = 2$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0 \neq L(\mathrm{Sym}^2(g^\sigma) \otimes f, 2)$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$ if and only if*

$$E_f(\mathbb{Q}(\sqrt{p})) \otimes \mathbb{Q} = \mathbb{Q} \cdot P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}) \oplus \mathbb{Q} \cdot P(X_0(p)^3, \Pi_{[g],f}, \Xi).$$

Remark 4.35. Since E_f admits non-split multiplicative reduction at p, $a_p(E_f) = -1$, hence $W(E_f/\mathbb{Q}) = -1$. Since $p \equiv 1 \pmod 4$, we have $W(E_f^{(p)}/\mathbb{Q}) = -1$, and thus $W(E_f/\mathbb{Q}(\sqrt{p})) = +1$ with $L(E_f/\mathbb{Q}(\sqrt{p}), 1) = 0$. Hence $\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}(\sqrt{p}), s) = 2$ if and only if $\mathrm{ord}_{s=1} L(E_f/\mathbb{Q}, s) = \mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1$. Moreover, we have

$$W(g, g, f) = a_p(E_f) = -1 = W(g, g, f^{(p)}),$$

hence by (4.51) and (4.52), $W(\mathrm{Sym}^2(g^\sigma) \otimes f) = W(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}) = 1$. As explained in Section 4.1.3, Theorem 4.2 of Darmon, Rotger and Sols implies, under the conditions of Conjecture 4.6, that the point $P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}}) \in E_f(\mathbb{Q})$ has infinite order. It follows from the work of Gross, Zagier and Kolyvagin (6), that $E_f(\mathbb{Q}) \otimes \mathbb{Q} = \mathbb{Q} \cdot P(X_0(p)^3, \Pi_{[g],f}, \Delta_{\mathrm{GKS}})$. As a consequence, Conjecture 4.6 follows from Conjectures 4.4 and (4.50).

A reformulation of Conjecture 4.4

Let us assume that $p \equiv 1 \pmod 4$. Let E_f be given in short Weierstrass form by the equation

$$E_f \quad : \quad y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q}.$$

An equation for the quadratic twist is then given by

$$E_f^{(p)} \quad : \quad py^2 = x^3 + ax + b \quad \simeq \quad y^2 = x^3 + ap^2x + bp^3,$$

the isomorphism being afforded by the change of variables $(x' = px, y' = p^2y)$. The curve E_f and its twist are isomorphic over $\mathbb{Q}(\sqrt{p})$ (but not over $\mathbb{Q}$); an isomorphism is provided by

$$\varphi : E_f \xrightarrow{\sim} E_f^{(p)}; \qquad (x, y) \mapsto (px, p\sqrt{p}y)\,.$$

Observe that for any $(x, y) \in E(\bar{\mathbb{Q}})$ and any $\tilde{\tau} \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ lifting τ, we have

$$\varphi((x, y))^{\tilde{\tau}} = (px^{\tilde{\tau}}, -p\sqrt{p}y^{\tilde{\tau}}) = -\varphi((x, y)^{\tilde{\tau}}).$$

Hence φ maps $E(\mathbb{Q}(\sqrt{p}))^{\tau=-1}$ to $E^{(p)}(\mathbb{Q}(\sqrt{p}))^{\tau=1} = E^{(p)}(\mathbb{Q})$. Define the point

$$P^{(p)}(X_0(p)^3, \Pi_{[g],f}, \Xi) := \varphi(P(X_0(p)^3, \Pi_{[g],f}, \Xi)) \in E^{(p)}(\mathbb{Q}).$$

We can then reformulate Conjecture 4.4 equivalently as follows.

Conjecture 4.7. *Let f and g be newforms in $S_2(\Gamma_0(p))$ as above. If $p \equiv 1 \pmod 4$, then $P^{(p)}(X_0(p)^3, \Pi_{[g],f}, \Xi) \in E_f^{(p)}(\mathbb{Q})$ has infinite order if and only if $\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$.*

Following the notation of Section 1.2.3, let $\mathbb{T}(p^2)$ denote the full $\mathbb{Q}$-algebra generated by the Hecke operators T_n with $p \nmid n$ and U_p acting on $S_2(\Gamma_0(p^2))$, and let $\mathbb{T}_0(p^2)$ denote the subalgebra generated by the operators T_n with $p \nmid n$. Generalising Section 4.1.1 by following [44, §3.1], we have the following decompositions of the Hecke algebras

$$\mathbb{T}_0(p^2) \simeq \prod_h K_h \subset \mathbb{T}(p^2) \simeq \prod_h L_h,$$

where h runs over all conjugacy classes of newforms in $S_2(\Gamma_0(p))$ and $S_2(\Gamma_0(p^2))$, K_h is the Hecke coefficient field of h, and L_h is K_h if h has level p^2, and otherwise L_h is a commutative Artinian K_h-algebra of dimension 2.

By Remark 4.2, we have

$$\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2)) := \mathrm{End}_{\mathbb{Q}}(J_0(p^2)) \otimes \mathbb{Q} = \langle \mathbb{T}_0(p^2), \delta_1, \delta_p \rangle \simeq \prod_{h \text{ level } p^2} K_h \times \prod_{h \text{ level } p} M_2(K_h), \quad (4.53)$$

where δ_1 and δ_p are degeneracy operators defined in [95]. Note that the natural isomorphism (4.5) holds with the curve $X_0(p)$ replaced by $X_0(p^2)$. See [105, Theorem 11.5.1].

Let $t_{[g]} \in \mathbb{T}_0(p^2) \simeq \prod_h K_h$ denote the idempotent with 1 in the K_g component and 0 elsewhere. We view it also as an idempotent of $\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))$ via (4.53), so that

$$\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))[g] := t_{[g]} \cdot \mathrm{End}^0_{\mathbb{Q}}(J_0(p^2)) = M_2(K_g).$$

Given a self-correspondence T of $X_0(p^2)$, we may view it as an element of $\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))$ and let $T_{[g]} := t_{[g]} \cdot T \in \mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))[g]$. We view $T_{[g]}$ as a self-correspondence of $X_0(p^2)$ via (4.5), and define $\Pi_{T_{[g]}} := \mathrm{pr}^*_{12}(T_{[g]}) \cdot \mathrm{pr}^*_{34}(\Delta)$ in $\mathrm{CH}^2(X_0(p^2)^4)(\mathbb{Q}) \otimes \mathbb{Q}$.

The elliptic curve $E_f^{(p)}$ has conductor p^2 by Remark 4.25, and $f^{(p)}$ is a newform in $S_2(\Gamma_0(p^2))$. We let $t_{f^{(p)}} \in \mathbb{T}_0(p^2)$ denote the idempotent with 1 in the $K_{f^{(p)}}$ component and 0 elsewhere, and define $\Pi_{T_{[g]},f^{(p)}} := \Pi_{T_{[g]}} \circ t_{f^{(p)}}$. After clearing denominators, this correspondence induces by push-forward a generalised modular parametrisation

$$\Pi_{T_{[g]},f^{(p)},*} : \mathrm{CH}^2(X_0(p^2)^3)_0(\mathbb{Q}) \longrightarrow E_f^{(p)}(\mathbb{Q}).$$

Letting $\Delta^{p^2}_{\mathrm{GKS}}(\xi_0) \in \mathrm{CH}^2(X_0(p^2)^3)_0(\mathbb{Q})$ denote the Gross–Kudla–Schoen cycle in the triple product $X_0(p^2)^3$ based at the rational cusp $\xi_0 \in X_0(p^2)(\mathbb{Q})$, we may form the Chow–Heegner point $P(X_0(p^2)^3, \Pi_{T_{[g]},f^{(p)}}, \Delta^{p^2}_{\mathrm{GKS}}(\xi_0)) := \Pi_{T_{[g]},f^{(p)},*}(\Delta^{p^2}_{\mathrm{GKS}}(\xi_0)) \in E_f^{(p)}(\mathbb{Q})$. Define

$$\mathcal{S}_{[g],f} := \langle P(X_0(p^2)^3, \Pi_{T_{[g]},f^{(p)}}, \Delta^{p^2}_{\mathrm{GKS}}(\xi_0)) \ : \ T_{[g]} \in \mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))[g] \rangle \subset E_f^{(p)}(\mathbb{Q}).$$

We have the decomposition of the triple product L-function

$$L(g, g, f^{(p)}, s) = L(\mathrm{Sym}^2 g \otimes f^{(p)}, s) L(f^{(p)}, s-1),$$

hence a corresponding decomposition of global root numbers

$$W(g, g, f^{(p)}) = W(\mathrm{Sym}^2 g \otimes f^{(p)}) W(f^{(p)}).$$

Since $p \equiv 1 \pmod 4$, we have $W(f^{(p)}) = -1$ by Proposition 4.4. We have $W(g, g, f^{(p)}) = -1$ by Theorem 4.7, and thus $W(\mathrm{Sym}^2 g \otimes f^{(p)}) = +1$. By [51, Theorem 3.7], the subgroup $\mathcal{S}_{[g],f} \subset E_f^{(p)}(\mathbb{Q})$ has positive rank if and only if $\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1$ and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$. Given the Birch and Swinnerton-Dyer conjecture and

Conjecture 4.7, it appears natural to conjecture the following.

Conjecture 4.8. *If* $p \equiv 1 \pmod 4$*, then* $P^{(p)}(X_0(p)^3, \Pi_{[g],f}, \Xi) \in \mathcal{S}_{[g],f} \subset E_f^{(p)}(\mathbb{Q})$ *if and only if* $\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s) = 1$ *and* $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ *for all* $\sigma : K_g \hookrightarrow \mathbb{C}$*.*

The above conjecture predicts a relation between Chow–Heegner points arising from the cycle Ξ in the triple product $X_0(p)^3$ and Chow–Heegner points arising from the Gross–Kudla–Schoen cycle in the triple product $X_0(p^2)^3$. Proving such a relation would yield a proof of Conjecture 4.7, and thus of Conjecture 4.4, contingent on the validity of the proof of Yuan–Zhang–Zhang [154] of the Gross–Kudla formula. We do not currently see how to carry out such an explicit comparison between the two sorts of Chow–Heegner points.

Remark 4.36. Taking avantage of the fact that the character χ is quadratic, we have the equality of L-functions $L(g, g, f^{(p)}, s) = L(g^{(p)}, g^{(p)}, f^{(p)}, s)$, where $g^{(p)}$ denotes the quadratic twist of g by χ, which is a newform of level p^2. Let $t_{[g^{(p)}]} \in \mathbb{T}_0(p^2)$ denote the corresponding idempotent in the Hecke algebra. Note that $L_{g^{(p)}} = K_g$ and $\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2))[g^{(p)}] = K_g$. Analogues of the above constructions give correspondences $\Pi_{t_{[g^{(p)}]}\cdot T, f^{(p)}} \in \mathrm{CH}^2(X_0(p^2)^3)(\mathbb{Q})$ for any self-correspondence T of $X_0(p^2)$, and points $P(X_0(p^3), \Pi_{t_{[g^{(p)}]}\cdot T, f^{(p)}}, \Delta^{p^2}_{\mathrm{GKS}}(\xi_0))$ in $E_f^{(p)}(\mathbb{Q})$. Defining $\mathcal{S}_{[g^{(p)}], f^{(p)}} \subset E_f^{(p)}(\mathbb{Q})$ similarly to above, the results of Darmon, Rotger and Sols apply, and $\mathcal{S}_{[g^{(p)}], f^{(p)}}$ has positive rank if and only if $\mathrm{ord}_{s=1} L(E_f^{(p)}/\mathbb{Q}, s)$ is 1 and $L(\mathrm{Sym}^2(g^\sigma) \otimes f^{(p)}, 2) \neq 0$ for all $\sigma : K_g \hookrightarrow \mathbb{C}$. These Chow–Heegner points should therefore be related to the Chow–Heegner points $P(X_0(p^2)^3, \Pi_{t_{[g]}\cdot T, f^{(p)}}, \Delta^{p^2}_{\mathrm{GKS}}(\xi_0))$ and $P^{(p)}(X_0(p)^3, \Pi_{[g],f}, \Xi)$.

Remark 4.37. One can inquire about the relationship between the Gross–Kudla–Schoen cycle $\Delta^{p^2}_{\mathrm{GKS}}$ in $X_0(p^2)^3$ and the cycle Ξ in $X_0(p)^3$. The curve $X_0(p^2)$ comes equipped with two degeneracy maps $X_0(p^2) \longrightarrow X_0(p)$ defined over $\mathbb{Q}$, which we denote π_1 and π_2. In terms of the moduli description, π_1 maps the pair (E, C), where E is an elliptic curve and C a subgroup of E of order p^2, to (E, pC), while π_2 maps (E, C) to $(E/(pC), C/(pC))$. On complex points, the projection π_1 corresponds to the natural inclusion of $\Gamma_0(p^2)$ in $\Gamma_0(p)$. These maps induce push-forward maps $\pi_{i,j,k,*} : \mathrm{CH}^2(X_0(p^2)^3)_0 \longrightarrow \mathrm{CH}^2(X_0(p)^3)_0$, where $\pi_{i,j,k}$ is the map $\pi_i \times \pi_j \times \pi_k : X_0(p^2)^3 \longrightarrow X_0(p)^3$ with $i, j, k \in \{1, 2\}$. Note that, for any $e \in X_0(p^2)(\mathbb{Q})$, $(\pi_{1,1,1})_*(\Delta^{p^2}_{\mathrm{GKS}}(e)) = \Delta_{\mathrm{GKS}}(\pi_1(e))$ and $(\pi_{2,2,2})_*(\Delta^{p^2}_{\mathrm{GKS}}(e)) = \Delta_{\mathrm{GKS}}(\pi_2(e))$. However, if $i \neq j$ or $i \neq k$, then $(\pi_{i,j,k})_*(\Delta^{p^2}_{\mathrm{GKS}}(e))$ is not in $\Delta(p) = \Delta \times_{X(1)^3} X_0(p)^3$, so does not relate to the diagonal type cycles constructed in Section 4.2. Nevertheless, these cycles could be of independent interest. We currently do not see how to directly relate the cycles $\Delta^{p^2}_{\mathrm{GKS}}$ and Ξ.

Chapter 5

Future directions

We conclude this thesis by outlining a few projects that will be addressed in future work of the author.

5.1 Diagonal cycles

Recall that Chapter 4 ended in Section 4.5 by raising questions and conjectures about the cycles and points constructed. Recall from Theorem 4.3 the cycle $\Xi := \Delta_+ - \Delta_-$ in $\mathrm{CH}^2(X_0(p)^3)_0(\mathbb{Q}(\sqrt{p^\star}))$, where $p^\star = \left(\frac{-1}{p}\right) p$. The associated Chow–Heegner point is

$$P(X_0(p)^3, \Pi_{[g],f}, \Xi) \in E(\mathbb{Q}(\sqrt{p^\star})),$$

where $E = E_f$ is the elliptic curve defined over $\mathbb{Q}$ of conductor p associated with a normalised newform $f \in S_2(\Gamma_0(p))$, and g is an auxiliary normalised newform not conjugate to f.

5.1.1 The complex Abel–Jacobi map

Recall from Section 0.2.3 the Abel–Jacobi isomorphism

$$\mathrm{AJ}_E : E(\mathbb{C}) \xrightarrow{\sim} J^1(E)(\mathbb{C}) := \frac{H^0(E(\mathbb{C}), \Omega^1_E)^\vee}{\mathrm{Im}\, H_1(E(\mathbb{C}), \mathbb{Z})}$$

defined, using as base point the origin $O_E \in E(\mathbb{C})$, by the integration formula

$$\mathrm{AJ}_E(P)(\omega) = \int_{O_E}^{P} \omega, \qquad \text{for all } \omega \in H^0(E(\mathbb{C}), \Omega^1).$$

There is a higher dimensional analogue

$$\mathrm{AJ}_{X_0(p)^3} : \mathrm{CH}^2(X_0(p)^3)_0(\mathbb{C}) \longrightarrow J^2(X_0(p)^3/\mathbb{C}) := \frac{\mathrm{Fil}^2 H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C})^\vee}{\mathrm{Im}\, H_3(X_0(p)^3(\mathbb{C}), \mathbb{Z})}, \tag{5.1}$$

defined by the integration formula

$$\mathrm{AJ}_{X_0(p)^3}(Z)(\alpha) = \int_{\partial^{-1}(Z)} \alpha, \qquad \text{for all } \alpha \in \mathrm{Fil}^2 H^3_{\mathrm{dR}}(X_0(p)^3/\mathbb{C}).$$

The functoriality properties of these complex Abel–Jacobi maps with respect to correspondences imply, for all $\omega \in H^0(E(\mathbb{C}), \Omega^1)$, the formula

$$\mathrm{AJ}_E(P(X_0(p)^3, \Pi_{[g],f}, \Xi))(\omega) = \mathrm{AJ}_{X_0(p)^3}(\Xi)(\Pi^*_{[g],f,\mathrm{dR}}(\omega)).$$

A possible strategy for proving Conjecture 4.4 could involve computing the image of the point $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ under the Abel–Jacobi isomorphism AJ_E. By the above formula, this requires computing the higher dimensional Abel–Jacobi image $\mathrm{AJ}_{X_0(p)^3}(\Xi)$. Darmon, Rotger and Sols [51, Theorem 2.5] have successfully computed $\mathrm{AJ}_{X_0(p)^3}(\Delta_{\mathrm{GKS}})$. We hope to compute $\mathrm{AJ}_{X_0(p)^3}(\Xi)$ using the description of Δ_+ and Δ_- as images of maps $X(p) \longrightarrow X_0(p)^3$ and thereby address Conjectures 4.1 and 4.4.

5.1.2 The p-adic Abel–Jacobi map

It would be interesting to compute the image of the cycle Ξ under the p-adic (syntomic) Abel–Jacobi map

$$\mathrm{AJ}_p : \mathrm{CH}^2(X_0(p)^3)_0(F) \longrightarrow (\mathrm{Fil}^2(H^3_{\mathrm{dR}}(X_0(p)^3/F)))^\vee,$$

where F is a finite extension of $\mathbb{Q}_p$. The definition of this map relies on the p-adic étale Abel–Jacobi map of Section 1.5.3

$$\mathrm{AJ}_{\mathrm{et}} : \mathrm{CH}^2(X_0(p))_0(F) \longrightarrow H^1_{\mathrm{st}}(F, H^3_{\mathrm{et}}(X_0(p)^3_{/\bar{F}}, \mathbb{Z}_p(2))) = \mathrm{Ext}^1_{\mathbf{Rep}_{\mathrm{st}}}(\mathbb{Q}_p, H^3_{\mathrm{et}}(X_0(p)^3_{/\bar{F}}, \mathbb{Q}_p)(2)),$$

and the theory of filtered Frobenius monodromy modules.

Remark 5.1. By [120, Theorem 3.1] the image of (1.75) lands in the semistable subgroup, and since $X_0(p)^3$ admits a semistable model described in [77], we can identify the latter by [119, Proposition 1.26] with the above group of extension classes.

More precisely, using the Dieudonné functor $D_{st,F}$, we obtain an identification

$$\mathrm{Ext}^1_{\mathbf{Rep}_{\mathrm{st}}(G_F)}(\mathbb{Q}_p, H^3_{\mathrm{et}}(X_0(p)^3_{/\bar{F}}, \mathbb{Q}_p)(2)) \xrightarrow{\sim} \mathrm{Ext}^1_{\mathbf{MF}^{\mathrm{ad}}_F(\varphi,N)}(F_0, H^3_{\mathrm{dR}}(X_0(p)^3/F)[-2]),$$

where $\mathbf{MF}^{\mathrm{ad}}_F(\varphi, N)$ denotes the category of admissible filtered Frobenius monodromy modules over F. The latter extension group can be shown to be isomorphic to $(\mathrm{Fil}^2(H^3_{\mathrm{dR}}(X_0(p)^3/F)))^\vee$. The p-adic syntomic Abel–Jacobi map is defined as the composition of $\mathrm{AJ}_{\mathrm{et}}$ with the above identifications.

This is the type of map that was used by Darmon and Rotger [48–50] to relate diagonal cycles to special values of p-adic L-functions. The difference in the present setting is that $X_0(p)^3$ admits semistable reduction at p and there are no crystalline classes in $\mathrm{Fil}^2(H^3_{\mathrm{dR}}(X_0(p)^3))$. Consequently, this computation falls outside the scope of the methods developed by Besser, Loeffler and Zerbes [18] which are utilised in the work of Darmon and Rotger. However, we believe that one can use the p-adic geometry of $X_0(p)$ as a Mumford curve combined with techniques from Iovita and Spiess [91] and Masdeu [111] to compute $\mathrm{AJ}_p(\Xi)$.

One hope is to relate this to the Gross–Kudla formula (4.1) for triples f_1, f_2, f_3 of modular forms with $W(f_1, f_2, f_3) = +1$, thus shedding light on Conjecture 4.2. If f_1, f_2, f_3 correspond to elliptic curves E_1, E_2, E_3 with split multiplicative reduction at p, then such a relation would also provide a link to the central value of the third derivative of the cyclotomic p-adic triple product L-function of Hsieh and Yamana [88] at $s = 2$:

$$L_p^{(3)}(F, 2) = \frac{3}{4p} \cdot \mathcal{L}_p(F) \cdot \frac{L(F, 2)}{\Omega_F},$$

where $F = f_1 \otimes f_2 \otimes f_3$, Ω_F is the period (4.15), and $\mathcal{L}_p(F) = \mathcal{L}_p(f_1) \cdot \mathcal{L}_p(f_2) \cdot \mathcal{L}_p(f_3)$ is the product of $\mathcal{L}$-invariants.

5.1.3 Connections with Stark–Heegner points

Suppose that $p \equiv 1 \pmod 4$. In this case, the Chow–Heegner point $P(X_0(p)^3, \Pi_{[g],f}, \Xi)$ in $E(\mathbb{Q}(\sqrt{p}))$ is defined over the totally real quadratic field $\mathbb{Q}(\sqrt{p})$. If it turns out that this point is non-trivial in certain cases (as predicted by Conjectures 4.4, 4.5, 4.6, 4.7), then it would be interesting to compare this rational point with other constructions, namely Heegner points, Zhang points or Stark–Heegner points. The latter are p-adic points constructed originally by Darmon [43] using Tate's p-adic uniformisation of elliptic curves, which is available when the reduction type of the curve at p is multiplicative. These points are conjectured to be global points defined over ring class fields of real quadratic fields and to play a role in the theory of real multiplication of Darmon and Vonk [52] similar to the role played by Heegner points in the theory of complex multiplication.

5.2 Non-hyperelliptic curves with torsion Ceresa class

Let X be a smooth projective curve over $\mathbb{Q}$ and consider its Jacobian J, which is an abelian variety of dimension the genus g of X. Fix an embedding $j : X \hookrightarrow J$ via an Abel–Jacobi map and consider the Ceresa cycle

$$C := j(X) - [-1] \circ j(X) \in \mathrm{CH}^{g-1}(J)_0(\mathbb{Q}).$$

If X is hyperellliptic, then C is trivial. Recently, the first example of a non-hyperelliptic curve with torsion Ceresa class was found by Bisogno, Li, Litt and Srinivasan [25]. The Ceresa class is a term for the image of C under the ℓ-adic étale Abel–Jacobi map (1.75)

$$\mathrm{AJ}_{\mathrm{et}} : \mathrm{CH}^{g-1}(J)_0(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, H^{2g-3}_{\mathrm{et}}(J_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell(g-1)).$$

We believe other examples of such curves are available in the setting of modular abelian varieties. More precisely, the idea would be to look for a non-hyperelliptic genus 3 curve X whose Jacobian splits into the product of three elliptic curves over $\mathbb{Q}$ such that the global root number of the associated L-function is $+1$. This would put us in a setting close to the one of Section 4.3. The modularity of the elliptic curves would imply that there is a non-constant map to J from a triple product of modular curves. We hope to exploit Theorem 4.4 and Remark 4.21 together with the close connection between the Gross–Kudla–Schoen cycle and the Ceresa cycle established by Colombo and van Geemen [40] to show that the latter's cohomology class is torsion.

5.3 Geometric quadratic Chabauty

Together with my collaborators Čoupek, Xiao and Yao, we plan to continue our work on the geometric quadratic Chabauty method.

5.3.1 Finiteness criteria

We would like to investigate Question 3.2. We refer to the discussion in Section 3.5.2 for the details; this involves understanding certain unlikely intersections in higher dimensional varieties as in the work of Dogra [60], and combining this with the finiteness arguments of Edixhoven and Lido [62, §9].

5.3.2 Applications

We would like to understand the sharpness of the bound provided by Corollary 3.2 by applying the method to specific examples of curves. The goal would be to come up with examples of nice curves and hopefully be able to determine their set of rational points using geometric quadratic Chabauty. We further expect such examples to shed light on Question 3.3 raised in Section 3.5.2.

Bibliography

[1] J. Achter, S. Casalaina-Martin, and C. Vial. On the image of the second ℓ-adic Bloch map. Preprint, arXiv:2007.07180, 2020.

[2] L. Alpoge. Points on curves. Thesis (Ph.D.)–Princeton University, 2020.

[3] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[4] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller. Explicit quadratic Chabauty over number fields. *Israel J. Math.* to appear.

[5] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. S. Müller.

[6] J. S. Balakrishnan and N. Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6):1057–1075, 2019.

[7] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: generalised height functions on Selmer varieties. *Int. Math. Res. Not. IMRN*, 2020.

[8] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[9] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. Preprint, arXiv:2101.01862, 2021.

[10] M. Bertolini and H. Darmon. Heegner points on Mumford-Tate curves. *Invent. Math.*, 126(3):413–456, 1996.

[11] M. Bertolini, H. Darmon, D. Lilienfeldt, and K. Prasanna. Generalised Heegner cycles and the complex Abel-Jacobi map. *Math. Z.*, 298(1-2):385–418, 2021.

[12] M. Bertolini, H. Darmon, and K. Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad.

[13] M. Bertolini, H. Darmon, and K. Prasanna. Chow-Heegner points on CM elliptic curves and values of p-adic L-functions. *Int. Math. Res. Not. IMRN*, (3):745–793, 2014.

[14] M. Bertolini, H. Darmon, and K. Prasanna. p-adic L-functions and the coniveau filtration on Chow groups. *J. Reine Angew. Math.*, 731:21–86, 2017. With an appendix by Brian Conrad.

[15] M. Bertolini, M. A. Seveso, and R. Venerucci. Balanced diagonal classes and rational points on elliptic curves. Preprint, 2020. https://www.uni-due.de/~ade847f/BSV.M02.pdf.

[16] M. Bertolini, M. A. Seveso, and R. Venerucci. Reciprocity laws for balanced diagonal classes. Preprint, 2020. https://www.uni-due.de/~ade847f/BSV.M01.pdf.

[17] M. Bertolini, M. A. Seveso, and R. Venerucci. Diagonal classes and the Bloch-Kato conjecture. *Münster J. of Math.*, 13:317–352, 2020.

[18] A. Besser, D. Loeffler, and S. L. Zerbes. Finite polynomial cohomology for general varieties. *Ann. Math. Qué.*, 40(1):203–220, 2016.

[19] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[20] F. Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture. *Algebra Number Theory*, 14(9):2369–2416, 2020.

[21] Y. Bilu and P. Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011.

[22] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[23] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[24] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[25] D. Bisogno, W. Li, D. Litt, and P. Srinivasan. Group-theoretic Johnson classes and a non-hyperelliptic curve with torsion Ceresa class. Preprint, arXiv:2004.06146, 2020.

[26] I. Blanco-Chacón and M. Fornea. Twisted triple product p-adic L-functions and Hirzebruch-Zagier cycles. *J. Inst. Math. Jussieu*, 19(6):1947–1992, 2020.

[27] S. Bloch. Torsion algebraic cycles and a theorem of Roitman. *Compositio Math.*, 39(1):107–127, 1979.

[28] S. Bloch. Algebraic cycles and values of L-functions. *J. Reine Angew. Math.*, 350:94–108, 1984.

[29] S. Bloch. Height pairings for algebraic cycles. In *Proceedings of the Luminy conference on algebraic K-theory (Luminy, 1983)*, volume 34, pages 119–145, 1984.

[30] S. Bloch and A. Ogus. Gersten's conjecture and the homology of schemes. *Ann. Sci. École Norm. Sup. (4)*, 7:181–201 (1975), 1974.

[31] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[32] J. Buhler, C. Schoen, and J. Top. Cycles, L-functions and triple products of elliptic curves. *J. Reine Angew. Math.*, 492:93–133, 1997.

[33] A. A. Burungale. On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, II: Shimura curves. *J. Inst. Math. Jussieu*, 16(1):189–222, 2017.

[34] A. A. Burungale. On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, I: Modular curves. *J. Algebraic Geom.*, 29(2):329–371, 2020.

[35] C. Chabauty. Sur les points rationels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941.

[36] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[37] R. F. Coleman. A p-adic Shimura isomorphism and p-adic periods of modular forms. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 21–51. Amer. Math. Soc., Providence, RI, 1994.

[38] J.-L. Colliot-Thélène and W. Raskind. K_2-cohomology and the second Chow group. *Math. Ann.*, 270(2):165–199, 1985.

[39] J.-L. Colliot-Thélène, J.-J. Sansuc, and C. Soulé. Torsion dans le groupe de Chow de codimension deux. *Duke Math. J.*, 50(3):763–801, 1983.

[40] E. Colombo and B. van Geemen. Note on curves in a Jacobian. *Compositio Math.*, 88(3):333–353, 1993.

[41] P. Coupek, D. Lilienfeldt, L. X. Xiao, and Z. Yao. Geometric quadratic Chabauty over number fields. Preprint, 2020. https://www.math.mcgill.ca/lilien/Chabauty-Part1.pdf.

[42] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[43] H. Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Ann. of Math. (2)*, 154(3):589–639, 2001.

[44] H. Darmon, M. Daub, S. Lichtenstein, and V. Rotger. Algorithms for Chow-Heegner points via iterated integrals. *Math. Comp.*, 84(295):2505–2547, 2015.

[45] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Int. Press, Cambridge, MA, 1994.

[46] H. Darmon, A. Lauder, and V. Rotger. Stark points and p-adic iterated integrals attached to modular forms of weight one. *Forum Math. Pi*, 3:e8, 95, 2015.

[47] H. Darmon, A. Lauder, and V. Rotger. Gross-Stark units and p-adic iterated integrals attached to modular forms of weight one. *Ann. Math. Qué.*, 40(2):325–354, 2016.

[48] H. Darmon and V. Rotger. Stark-Heegner points and generalised Kato classes. Preprint, https://www.math.mcgill.ca/darmon/pub/Articles/Research/70.DR3/DR3.pdf.

[49] H. Darmon and V. Rotger. Diagonal cycles and Euler systems I: A p-adic Gross-Zagier formula. *Ann. Sci. Éc. Norm. Supér. (4)*, 47(4):779–832, 2014.

[50] H. Darmon and V. Rotger. Diagonal cycles and Euler systems II: The Birch and Swinnerton-Dyer conjecture for Hasse-Weil-Artin L-functions. *J. Amer. Math. Soc.*, 30(3):601–672, 2017.

[51] H. Darmon, V. Rotger, and I. Sols. Iterated integrals, diagonal cycles and rational points on elliptic curves. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2012/2*, volume 2012/ of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 19–46. Presses Univ. Franche-Comté, Besançon, 2012.

[52] H. Darmon and J. Vonk. Singular moduli for real quadratic fields: a rigid analytic approach. *Duke Math. J.*, 170(1):23–93, 2021.

[53] M. W. Daub. *Complex and p-adic Computations of Chow-Heegner Points*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–University of California, Berkeley.

[54] E. de Shalit. On the p-adic periods of $X_0(p)$. *Math. Ann.*, 303(3):457–472, 1995.

[55] P. Deligne. *Équations différentielles à points singuliers réguliers*. Lecture Notes in Mathematics, Vol. 163. Springer-Verlag, Berlin-New York, 1970.

[56] P. Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349, 1973.

[57] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[58] P. Deligne. Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[59] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[60] N. Dogra. Unlikely intersections and the Chabauty-Kim method over number fields. Preprint, arXiv:1903.05032, 2019.

[61] N. Dogra and S. Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one. *Math. Ann.*, 2020. https://doi.org/10.1007/s00208-020-02112-3.

[62] B. Edixhoven and G. Lido. Geometric quadratic Chabauty. Arxiv Preprint, arXiv:1910.10752, 2019.

[63] B. Edixhoven, G. van der Geer, and B. Moonen. *Abelian Varieties*. Book Project. https://www.math.ru.nl/~bmoonen/research.html#bookabvar.

[64] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[65] F. El Zein and S. Zucker. Extendability of normal functions associated to algebraic cycles. In *Topics in transcendental algebraic geometry (Princeton, N.J., 1981/1982)*, volume 106 of *Ann. of Math. Stud.*, pages 269–288. Princeton Univ. Press, Princeton, NJ, 1984.

[66] Y. Elias. Kolyvagin's method for Chow groups of Kuga-Sato varieties over ring class fields. *Ann. Math. Qué.*, 39(2):147–167, 2015.

[67] Y. Elias. On the Selmer group attached to a modular form and an algebraic Hecke character. *Ramanujan J.*, 45(1):141–169, 2018.

[68] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[69] M. Fornea. Growth of the analytic rank of modular elliptic curves over quintic extensions. *Math. Res. Lett.*, 26(6):1571–1586, 2019.

[70] M. Fornea. On twisted triple products and the arithmetic of elliptic curves. Thesis (Ph.D.)–McGill University, 2019.

[71] M. Fornea and Z. Jin. Hirzebruch-Zagier classes and rational elliptic curves over quintic fields. Preprint, arXiv:2005.02520, 2020.

[72] W. Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1984.

[73] F. Gatti, X. Guitart, M. Masdeu, and V. Rotger. Special values of triple product p-adic L-functions and non-crystalline diagonal classes. Preprint, 2020. https://web.mat.upc.edu/victor.rotger/docs/GGMR.pdf.

[74] B. H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[75] B. H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[76] B. H. Gross and S. S. Kudla. Heights and the central critical values of triple product L-functions. *Compositio Math.*, 81(2):143–209, 1992.

[77] B. H. Gross and C. Schoen. The modified diagonal cycle on the triple product of a pointed curve. *Ann. Inst. Fourier (Grenoble)*, 45(3):649–679, 1995.

[78] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[79] A. Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie (SGA7)*, volume 1. 1972.

[80] A. Grothendieck and J. Dieudonné. Éléments de géométrie algébrique IV. *Publ. Math. IHES*, 24:5–231, 1965.

[81] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.

[82] M. Harris and S. S. Kudla. The central critical value of a triple product L-function. *Ann. of Math. (2)*, 133(3):605–672, 1991.

[83] M. Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1978.

[84] D. Hilbert and A. Hurwitz. Über die diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, 14(1):217–224, 1890.

[85] T. Honda. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22(2):213–246, 1970.

[86] K. Hopkins. Higher-weight Heegner points. *Experiment. Math.*, 19(3):257–266, 2010.

[87] S. Howe and K. Joshi. Asymptotics of conductors of elliptic curves over $\mathbb{Q}$. Preprint, arXiv:1201.4566, 2015.

[88] M.-L. Hsieh and S. Yamana. Four-variable p-adic triple product L-functions and the trivial zero conjecture. Preprint, arXiv:1906.10474, 2019.

[89] E. Hunter Brooks. Shimura curves and special values of p-adic L-functions. *Int. Math. Res. Not. IMRN*, (12):4177–4241, 2015.

[90] B.-H. Im. Heegner points and Mordell-Weil groups of elliptic curves over large fields. *Trans. Amer. Math. Soc.*, 359(12):6143–6154, 2007.

[91] A. Iovita and M. Spieß. Derivatives of p-adic L-functions, Heegner cycles and monodromy modules attached to modular forms. *Invent. Math.*, 154(2):333–384, 2003.

[92] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970.

[93] U. Jannsen. Continuous étale cohomology. *Math. Ann.*, 280(2):207–245, 1988.

[94] U. Jannsen. *Mixed motives and algebraic K-theory*, volume 1400 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1990. With appendices by S. Bloch and C. Schoen.

[95] E. Kani. Endomorphisms of Jacobians of modular curves. *Arch. Math. (Basel)*, 91(3):226–237, 2008.

[96] E. Katz, J. Rabinoff, and D. Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell-Weil rank. *Duke Math. J.*, 165(16):3189–3240, 2016.

[97] E. Katz and D. Zureick-Brown. The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compos. Math.*, 149(11):1818–1838, 2013.

[98] N. M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350, 1973.

[99] N. M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1980.

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

[101] M. Kim. The motivic fundamental group of $\mathbb{P}_1$ - $\{0, 1, \infty\}$. *Invent. Math.*, 2005.

[102] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 2009.

[103] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and cH$(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[104] D. Kriz. Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-function. *Algebra Number Theory*, 10(2):309–374, 2016.

[105] H. Lange and C. Birkenhake. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1992.

[106] B. Lawrence and A. Venkatesh. Diophantine problems and p-adic period mappings. *Invent. Math.*, 221(3):893–999, 2020.

[107] Y. Liu. Hirzebruch-Zagier cycles and twisted triple product Selmer groups. *Invent. Math.*, 205(3):693–780, 2016.

[108] Y. Liu. Bounding cubic-triple product Selmer groups of elliptic curves. *J. Eur. Math. Soc. (JEMS)*, 21(5):1411–1508, 2019.

[109] M. Longo and M. R. Pati. Generalized Heegner cycles on Mumford curves. *Math. Z.*, 297:483–515, 2021.

[110] M. Longo and S. Vigni. Kolyvagin systems and Iwasawa theory of generalized Heegner cycles. *Kyoto J. Math.*, 59(3):717–746, 2019.

[111] M. Masdeu. CM cycles on Shimura curves, and p-adic L-functions. *Compos. Math.*, 148(4):1003–1032, 2012.

[112] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[113] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[114] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[115] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[116] A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(5):1011–1046, 1135–1136, 1982.

[117] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[118] L. J. Mordell. On the rational solutions of the indeterminate equation of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922.

[119] J. Nekovář. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progr. Math.*, pages 127–202. Birkhäuser Boston, Boston, MA, 1993.

[120] J. Nekovář. On the p-adic height of Heegner cycles. *Math. Ann.*, 302(4):609–686, 1995.

[121] J. Nekovář. p-adic Abel-Jacobi maps and p-adic heights. In *The arithmetic and geometry of algebraic cycles (Banff, AB, 1998)*, volume 24 of *CRM Proc. Lecture Notes*, pages 367–379. Amer. Math. Soc., Providence, RI, 2000.

[122] K. Ota. Big Heegner points and generalized Heegner cycles. *J. Number Theory*, 208:305–334, 2020.

[123] A. Pacetti. On the change of root numbers under twisting and applications. *Proc. Amer. Math. Soc.*, 141(8):2615–2628, 2013.

[124] I. Piatetski-Shapiro and S. Rallis. Rankin triple L functions. *Compositio Math.*, 64(1):31–115, 1987.

[125] K. A. Ribet. Endomorphisms of semi-stable abelian varieties over number fields. *Ann. of Math. (2)*, 101:555–562, 1975.

[126] D. E. Rohrlich. Elliptic curves and the Weil-Deligne group. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 125–157. Amer. Math. Soc., Providence, RI, 1994.

[127] N. Schappacher. *Periods of Hecke characters*, volume 1301 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1988.

[128] C. Schoen. Complex multiplication cycles on elliptic modular threefolds. *Duke Math. J.*, 53(3):771–794, 1986.

[129] C. Schoen. Some examples of torsion in the Griffiths group. *Math. Ann.*, 293(4):651–679, 1992.

[130] C. Schoen. Complex multiplication cycles and a conjecture of Beilinson and Bloch. *Trans. Amer. Math. Soc.*, 339(1):87–115, 1993.

[131] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 292–296. Thompson, Washington, D.C., 1967.

[132] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[133] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[134] B. Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[135] G. Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan*, 10:1–28, 1958.

[136] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.

[137] A. Shnidman. p-adic heights of generalized heegner cycles. *Ann. Inst. Fourier (Grenoble)*, 66(3):1117–1174, 2016.

[138] S. Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013.

[139] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[140] C. Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. *Ann. of Math. (2)*, 191(2):329–354, 2020.

[141] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[142] The Stacks Project Authors. Stacks project. Available online at http://stacks.math.columbia.edu, 2020.

[143] M. Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006.

[144] J. T. Tate, Jr. *FOURIER ANALYSIS IN NUMBER FIELDS AND HECKE'S ZETA-FUNCTIONS*. ProQuest LLC, Ann Arbor, MI, 1950. Thesis (Ph.D.)–Princeton University.

[145] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[146] N. Triantafillou. Restriction of Scalars Chabauty and the S-unit equation. Preprint, arXiv:2006.10590, 2020.

[147] C. Voisin. *Hodge theory and complex algebraic geometry. I*, volume 76 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2002. Translated from the French original by Leila Schneps.

[148] P. Vojta. Siegel's theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548, 1991.

[149] H. Wang. Arithmetic level raising on triple product of Shimura curves and Gross-Schoen diagonal cycles I: Ramified case. Preprint, arXiv:2004.00555, 2020.

[150] H. Wang. Arithmetic level raising on triple product of Shimura curves and Gross-Schoen diagonal cycles II: Bipartite euler system. Preprint, arXiv:2004.14916, 2020.

[151] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.

[152] J. L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley.

[153] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[154] X. Yuan, S. Zhang, and W. Zhang. Triple product L-series and Gross-Kudla-Schoen cycles. Preprint, 2012. http://math.mit.edu/~wz2113/math/online/triple.pdf.

[155] S. Zhang. Heights of Heegner cycles and derivatives of L-series. *Invent. Math.*, 130(1):99–152, 1997.

[156] S. Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001.

[157] S. Zhang. Arithmetic of Shimura curves. *Sci. China Math.*, 53(3):573–592, 2010.