Southwest Center
for Arithmetic Geometry

ARIZONA WINTER SCHOOL 2018

Department of Mathematics
The University of Arizona®

Deadline to apply for funding:
November 10, 2017

http://swc.math.arizona.edu

IWASAWA THEORY

John Coates
Classical algebraic Iwasawa theory

David Loeffler and Sarah Zerbes
Euler systems

Romyar Sharifi
Modular curves and cyclotomic fields

Christopher Skinner
Iwasawa theory, modular forms, and elliptic curves

TUCSON, MARCH 3-7, 2018

Funded by the National Science Foundation
and organized in partnership
with the Clay Mathematics Institute

University of Arizona

Arizona Winter School 2018
Iwasawa Theory

Notes By: Caleb McWhorter

March 2018

Contents

Part I

Talk Notes

1 Ralph Greenberg: Remarks on Iwasawa theory for elliptic curves

2 John Coates: Classical algebraic Iwasawa theory

2.1 Lecture 1

$[F : \mathbb{Q}] < \infty$, F_∞/F, $\Gamma = \mathrm{Gal}(F_\infty/F)$
$\Gamma \xrightarrow{\sim} \mathbb{Z}_p$, $\Gamma_n \xrightarrow{\sim} p^n\mathbb{Z}_p$,
$F_\infty^{\Gamma_n} = F_n$, $\mathrm{Gal}(F_n/F) = \mathbb{Z}/p^n\mathbb{Z}$
$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots F_\infty = \cup F_n$
Facet 1. F_∞/F
Classical Iwasawa Theory: p-adic behavior of ideal class groups and units in F_∞/F, and interpretation via global class field theory.
$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$

(a) Complex zeros of $\zeta(s) \leftrightarrow$ distribution of prime numbers.

(b) $\zeta(1 - n) \in \mathbb{Q}(n = 2, 4, 6, \ldots)$

Kummer $\leftrightarrow$ class number of $\mathbb{Q}(\mu_p)^+$
Leopoldt-Kubota: p-adic analogue of $\zeta(s)$.
Iwasawa: zeroes of p-adic analogue of $\zeta(s) \leftrightarrow$ classical Iwasawa Theory of $\mathbb{Q}(\mu_p^\infty)^+/\mathbb{Q}(\mu_p)^+$.

2.2 Lecture 2

2.3 Lecture 3

2.4 Lecture 4

3 David Loeffler and Sarah Zerbes: Euler systems

3.1 Lecture 1

3.2 Lecture 2

3.3 Lecture 3

3.4 Lecture 4

4 Romyar Sharifi: Modular curves and cyclotomic fields

4.1 Lecture 1

4.2 Lecture 2

4.3 Lecture 3

4.4 Lecture 4

5 Christopher Skinner: Iwasawa theory, modular forms, and elliptic curves

5.1 Lecture 1

5.2 Lecture 2

5.3 Lecture 3

5.4 Lecture 4

5.5 Lecture 5

Part II

Course/Project Outlines & Lecture Notes

CLASSICAL ALGEBRAIC IWASAWA THEORY.

JOHN COATES

If one wants to learn Iwasawa theory, the starting point has to be the basic material covered in §1 - §8 of Iwasawa's paper [1]. The aim of these lectures will be to give a concise account of this work, concentrating on proving one of the main results of the paper, which is the so called weak Leopoldt conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any number field, i.e. that the p-adic defect of Leopoldt is always bounded as one goes up the cyclotomic $\mathbb{Z}_p$-extension. The course will also include a brief introduction to the notion of the Iwasawa algebra of $\mathbb{Z}_p$, and the structure theory of modules for this Iwasawa algebra. The background required for the lectures will be basic algebraic number theory, including a knowledge of the main facts of abelian global class field theory.

1. Possible Project

One possible project will be to consider some analogues of the weak Leopoldt conjecture, which remain unproven. For example, if K is any imaginary quadratic field and p is a prime which splits in K into two distinct primes w and $w*$, there is a unique $\mathbb{Z}_p$-extension K_∞/K which is unramified outside the prime w. If F is any finite extension of K, one can then define the compositum of F and K_∞ to obtain a $\mathbb{Z}_p$-extension F_∞/F. There is now an obvious analogue of the Leopoldt conjecture and the Leopoldt defect if one now considers the p-adic closure of the image of the global units in the product of the local units at the primes above w, for any finite layer of F_∞/F. In particular, the analogue of the weak Leopoldt conjecture for F_∞/F should be that this defect of Leopoldt is bounded as one mounts the tower. This question is important in the study of the Iwasawa theory of elliptic curves with complex multiplication [2]. Unfortunately, Iwasawa's proof of weak Leopoldt for the cyclotomic $\mathbb{Z}_p$-extension does not seem to extend to this situation. When F is abelian over K, the p-adic analogue of Baker's theorem proves the w-adic Leopoldt defect is zero for every finite layer of F_∞/F, but only a few examples are known where even the weak w-adic Leopoldt conjecture has been proven once F is not abelian over K. One possible project would be to discuss this material, and extend some of the known non-abelian examples.

References

[1] K. Iwasawa On $\mathbb{Z}_l$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246-326.

[2] J. Coates *Infinite descent on elliptic curves with complex multiplication*, in Arithmetic and Geometry, Progress in Mathematics 35 (1983), Birkhauser, 107-137.

John Coates,
Emmanuel College, Cambridge,
United Kingdom
jhc13@dpmms.cam.ac.uk

$[F:\mathbb{Q}] < \infty$, F_∞ / F - a $\mathbb{Z}_p$-extension, $\Gamma = Gal(F_\infty/F)$

$\Gamma \xrightarrow{\sim} \mathbb{Z}_p$; $\Gamma_n \subset \Gamma$. $[\Gamma : \Gamma_n] = p^n$, $F_n = F_\infty^{\Gamma_n}$, $\Gamma/\Gamma_n = \mathbb{Z}/p^n\mathbb{Z}$

$F = F_0 \subset F_1 \ldots \subset F_n \subset \ldots F_\infty$

Every F has a unique $\mathbb{Z}_p$-extension $F_\infty^{cyc} \subset F(\mu_{p^\infty})$.

Iwasawa theory is a p-adic theory about arithmetic questions which uses $\mathbb{Z}_p$-extensions as the basic underlying tool. p-adic world.

FACET 1. F_∞ / F

Iwasawa. Study behaviour of ideal class groups and units p-adically in the tower F_∞/F, and their interpretation via global class field theory.

This is classical Iwasawa theory.

$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ and its analytic continuation

Important for arithmetic for two reasons:-

(a). Location of non-trivial zeroes $\Leftrightarrow$ asymptotic distribution of prime numbers. (Riemann)

No known analogue in Iwasawa theory.

(b). $\zeta(1-n) \in \mathbb{Q}$ $(n = 2, 4, 6, \ldots)$

Kummer: related to p-adic arithmetic of $\mathbb{Q}(\mu_p)^+$.

Leopoldt Kubota: p-adic analogue of $\zeta(s)$

22 Iwasawa made the great discovery that there appeared to be a precise relation between the zeroes of the Kubota-Leopoldt analogue of $S(s)$ and the arithmetic of the tower $\mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}(\mu_p)^+$.

Proved a beautiful general theorem in this direction in his great paper "On some modules in the theory of cyclotomic field".

Only proved his "main conjecture" when class number of $\mathbb{Q}(\mu_p)^+$ is prime to p. Mazur & Wiles found the first proof that it holds for all p.

Arithmetic application to $\mathbb{Z}$ itself:-

Quillen: $K_{2n}\mathbb{Z}$ $(n=1,2,\dots)$.

Borel-Garland: $K_{2n}\mathbb{Z}$ finite $(n=1,2,\dots)$.

Birch-Tate, Lichtenbaum:

Theorem. For $n=1,2,\dots$

$$\#\left(K_{2n}\mathbb{Z}\right) = \left|w_n(\mathbb{Q})\,S(1-n)\right|.$$

Proof hinges on Iwasawa's "main conjecture".

Open problem. Prove the analogue for the Kubota-Leopoldt p-adic zeta function of the fact

Fact. $S(s)$ has a simple zero at $s=-2,-4,-6,\dots$

FACET 2. $[F:\mathbb{Q}]<\infty$, M/F - a motive

Ex. $F=\mathbb{Q}$, M = elliptic curve $E/\mathbb{Q}$.

Complex L-function. $L(E,s)$ - entire by Deuring, Wiles,...

Birch-Swinnerton-Dyer conjecture. Precise relation between $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ and behaviour of $L(E,s)$ at $s=1$.

Only hope of proving exact formula for $\#(Ш(E/\mathbb{Q}))$ in this conjecture is via Iwasawa theory.

Conjecture. $L(E,1)\neq 0 \Leftrightarrow E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})(p)$ finite for any prime p.

$\Rightarrow$ known for all p (Kolyvagin-Gross-Zagier).

$\Leftarrow$ known for p sufficiently large for "most" E by Iwasawa theory.

Key Remark. We need Iwasawa theory for every prime p to answer this type of question.

$E: y^2 = x^3 - N^2x$, prove the above for $p=2$?

Important because of Smith's recent work.

Goal. Prove the full BSD conjecture for every $E/\mathbb{Q}$ such that $L(E,s)$ has a zero at $s=1$ of order ≤ 1.

FACET 3. Carry out the analogue of Iwasawa theory when we replace the $\mathbb{Z}_p$-extension F_∞/F by a Galois extension F_∞/F whose Galois group is a compact p-adic Lie group e.g. $GL_2(\mathbb{Z}_p)$.

FACET 4. Most mysterious and very little is known about it at present.

General question. Prove that some of the classical Iwasawa modules are smaller than one would naively expect.

Iwasawa's $\mu=0$ conjecture for F_∞^{cyc}/F.
Greenberg's conjectures.

End with an even more classical example, due to Weber ($p=2$) and Fukuda-Komatsu in general.

Conjecture. Let p be any prime number, $\mathbb{Q}_\infty/\mathbb{Q}$ the unique $\mathbb{Z}_p$-extension. Then the class number of every finite layer $\mathbb{Q}_n$ of $\mathbb{Q}_\infty/\mathbb{Q}$ is equal to 1.

Iwasawa proved class number of $\mathbb{Q}_n$ is prime to p.
How do we attak this even for $p=2$.
Overwhelming numerical evidence in support of conjecture.

Classical Iwasawa theory

Arizona Winter School 2018

§1. Foundational material

The lecture will briefly cover, without proofs, the background in algebra and number theory needed at the beginning of Iwasawa theory. Throughout, p will denote an arbitrary prime number, and Γ a topological group which is isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. Thus, for each $n \geq 0$, Γ will have a closed subgroup of index p^n, which we will denote by Γ_n, and Γ/Γ_n will then be a cyclic group of order p^n. The Iwasawa algebra $\Lambda(\Gamma)$ of Γ is defined by

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n],$$

and it is endowed with the natural topology coming from the p-adic topology on the $\mathbb{Z}_p[\Gamma/\Gamma_n]$.

1.1 Some relevant algebra

We recall without proof some of the basic algebra needed in classical Iwasawa theory. Let $R = \mathbb{Z}_p[[T]]$ be the ring of formal power series in an indeterminate T with coefficients in $\mathbb{Z}_p$. Then R is a Noetherian regular local ring of dimension 2 with maximal ideal $\mathfrak{M} = (p, T)$. We say that a monic polynomial $q(T) = \sum_{i=0}^{n} a_i T^i$ in R is <u>distinguished</u> if $a_0, \ldots, a_{n-1} \in p\mathbb{Z}_p$. The Weierstrass preparation theorem for R tells us that every non-zero $f(T)$ in R can be written uniquely in the form $f(T) = p^{\mu} q(T) u(T)$, where $\mu \geq 0$, $q(T)$ is a distinguished polynomial, and $u(T)$ is a unit in R.

<u>Proposition 1.1.</u> Let γ be a fixed topological generator of Γ. Then there is a unique isomorphism of $\mathbb{Z}_p$-algebras

$$\Lambda(\Gamma) \xrightarrow{\sim} R = \mathbb{Z}_p[[T]]$$

which maps γ to $1+T$.

In the following, we shall often identify $\Lambda(\Gamma)$ and R, bearing in mind that Γ will not usually have a canonical topological generator.

Let X be any profinite abelian p-group, on which Γ acts continuously. Then the Γ-action extends by continuity and linearity to an action of the whole Iwasawa algebra $\Lambda(\Gamma)$. Moreover, X will be finitely generated over $\Lambda(\Gamma)$ if and only if $X/\mathfrak{m}X$ is finite, where $\mathfrak{m} = (p, \gamma - 1)$, with γ a topological generator of Γ, is the maximal ideal of $\Lambda(\Gamma)$. We write $\mathcal{R}(\Gamma)$ for the category of finitely generated $\Lambda(\Gamma)$-modules. If X is in $\mathcal{R}(\Gamma)$, we define the $\Lambda(\Gamma)$-rank of X to be $Q(\Gamma)$-dimension of $X \otimes_{\Lambda(\Gamma)} Q(\Gamma)$, where $Q(\Gamma)$ denotes the field of fractions of $\Lambda(\Gamma)$. We say X is $\Lambda(\Gamma)$-torsion if it has $\Lambda(\Gamma)$-rank 0, or equivalently if $\alpha X = 0$ for some non-zero α in $\Lambda(\Gamma)$.

Although $\Lambda(\Gamma)$ is not a principal ideal domain, there is nevertheless a beautiful structure theory for modules in $\mathcal{R}(\Gamma)$ (see Bourbaki, Commutative Algebra, Chap. 7, §4), which can be summarized by the following result:-

Theorem 1.2. For each X in $\mathcal{R}(\Gamma)$, we have an exact sequence of $\Lambda(\Gamma)$-modules

$$0 \longrightarrow D_1 \longrightarrow X \longrightarrow \Lambda(\Gamma)^r \oplus \bigoplus_{i=1}^{m} \Lambda(\Gamma)/(f_i) \longrightarrow D_2 \longrightarrow 0,$$

where D_1 and D_2 have finite cardinality, and $f_i \neq 0$ for $i = 1, \ldots, m$. Moreover, the ideal $c(X) = f_1 \ldots f_m \Lambda(\Gamma)$ is uniquely determined by X when $r = 0$.

We list some of the main consequences of the structure theory used in Iwasawa theory. First, X will be $\Lambda(\Gamma)$-torsion if and only if $r = 0$. Suppose now that X is $\Lambda(\Gamma)$-torsion. The principal ideal $c(X)$ is called the characteristic ideal of X. A characteristic element of X is any generator $f_X(T)$ of $c(X)$. By the Weierstrass preparation theorem, we can write

$$f_X(T) = p^{\mu(X)} q_X(T) u(T),$$

where $\mu(X)$ is an integer ≥ 0, $q_X(T)$ is a distinguished polynomial, and $u(T)$ is a unit in $\Lambda(\Gamma)$. Clearly $\mu(X)$ and $q_X(T)$ are uniquely determined by X. We define $\mu(X)$ to be the μ-invariant of X, and we define the degree $\lambda(X)$ of $q_X(T)$ to be λ-invariant of X.

Exc 1. Assume X in $\mathcal{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion. Prove that X is finitely generated as a $\mathbb{Z}_p$-module if and only if $\mu(X) = 0$.

Recall that Γ_n denotes the unique subgroup of Γ of index p^n. Thus, if Γ has a topological generator γ, then Γ_n is topologically generated by γ^{p^n}. If X is in $\mathcal{R}(\Gamma)$, we define X^{Γ_n} and X_{Γ_n} to be the largest submodule and quotient module of X, respectively, on which Γ_n acts trivially. Thus

$$(X)_{\Gamma_n} = X/(\gamma^{p^n} - 1)X.$$

Exc 2. Assume X is in $\mathcal{R}(\Gamma)$, and that, for all $n \geq 0$, we have

28

$\mathbb{Q}_p$-dimension of $\left((X)_{\Gamma_n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right) = m\, p^n + \delta_n$,

where m is independent of n, and δ_n is bounded as $n \to \infty$. Prove that X has $\Lambda(\Gamma)$-rank equal to m, and that δ_n is constant for n sufficiently large.

Exc. 3. Assume X in $\mathcal{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion, and let $f_X(T)$ be any characteristic element. Prove that the following are equivalent :- (i) $f_X(0) \neq 0$, (ii) X_Γ is finite, and (iii) X^Γ is finite. When all three are valid, prove the Euler characteristic formula

$$\left| f_X(0) \right|_p^{-1} = \#(X_\Gamma) / \#(X^\Gamma).$$

1.2. Some basic class field theory. We recall basic facts from abelian class field theory which will be used repeatedly later. As always, p is any prime number. Let F be a finite extension of $\mathbb{Q}$, and K an extension of F. We recall that an infinite place v of F is said to ramify in K if v is real and if there is at least one complex prime of K above v. In these lectures, we will mainly be concerned with the maximal abelian p-extension L of F, which is unramified at all finite and infinite places of F (i.e. L is the p-Hilbert class field of F), and with the maximal abelian p-extension M of F, which is unramified at all infinite places of F and all finite places of F which do not lie above p. Artin's global reciprocity law gives the following explicit descriptions of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(M/F)$, in which we simply write isomorphisms for the relevant Artin maps. Firstly, we have

$$A_F \xrightarrow{\sim} \mathrm{Gal}(L/F),$$

where A_F denotes the p-primary subgroup of the ideal class group of F. Secondly, for each place v of F lying above p, write U_v for the group of local units in the completion of F at v which are $\equiv 1 \bmod v$. Put

$$U_F = \prod_{v|p} U_v.$$

If W is any $\mathbb{Z}_p$-module, we define the $\mathbb{Z}_p$-rank of W to be $\dim_{\mathbb{Q}_p}(W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Then U_F is a $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $[F:\mathbb{Q}]$. Let E_F be the group of all global units of F which are $\equiv 1 \bmod v$ for all primes v of F above p. By Dirichlet's theorem, E_F has $\mathbb{Z}$-rank equal to $r_1 + r_2 - 1$, where r_1 is the number of real and r_2 the number of complex places of F. Now we have the obvious embedding of E_F in U_F, and we define $\overline{E}_F$ to be the closure in the p-adic topology of the image of E_F (equivalently, $\overline{E}_F$ is the $\mathbb{Z}_p$-submodule of U_F which is generated by the image of E_F). Secondly, the Artin map then induces an isomorphism

$$U_F / \overline{E}_F \xrightarrow{\sim} \mathrm{Gal}(M/L),$$

where, as above, L is the p-Hilbert class field of F. Clearly, the $\mathbb{Z}_p$-module $\overline{E}_F$ must have $\mathbb{Z}_p$-rank equal to $r_1 + r_2 - 1 - \delta_{F,p}$ for some integer $\delta_{F,p} \geq 0$, and so we immediately obtain:—

Theorem 1.3. Let M be the maximal abelian p-extension of F which is unramified outside the primes of F lying above p. Then $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $r_2 + 1 + \delta_{F,p}$.

Leopoldt's Conjecture[30]. $\delta_{F,p} = 0$.

The conjecture follows from Baker's theorem on linear forms in the p-adic logarithms of algebraic numbers when F is a finite abelian extension of either $\mathbb{Q}$ or an imaginary quadratic field.

1.3. $\mathbb{Z}_p$-extensions.

Let F be a finite extension of $\mathbb{Q}$. A $\mathbb{Z}_p$-extension of F is defined to be any Galois extension F_∞ of F such that the Galois group of F_∞ over F is topologically isomorphic to $\mathbb{Z}_p$.

The most basic example of a $\mathbb{Z}_p$-extension is the cyclotomic $\mathbb{Z}_p$-extension of F. For each $m > 1$, let μ_m denote the group of m-th roots of unity, and put $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$. The action of the Galois group of $\mathbb{Q}(\mu_{p^\infty})$ over $\mathbb{Q}$ on μ_{p^∞} defines an injection of this Galois group into $\mathbb{Z}_p^\times$, and this injection is an isomorphism by the irreducibility of the p-power cyclotomic polynomials. Put $V = 1 + 2p\mathbb{Z}_p$, so that V is isomorphic to $\mathbb{Z}_p$ under the p-adic logarithm. Then $\mathbb{Z}_p^\times = \mu_2 \times V$ when $p = 2$, and $\mu_{p-1} \times V$ when $p > 2$. Hence $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$, where $\Gamma \simeq \mathbb{Z}_p$, and Δ is cyclic of order 2 or $p-1$, according as $p = 2$ or $p > 2$. Thus

$$\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$$

will be a $\mathbb{Z}_p$-extension of $\mathbb{Q}$, which we call the cyclotomic $\mathbb{Z}_p$-extension. Theorem 1.3 shows that it is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. If now F is any finite extension, the compositum $F\mathbb{Q}_\infty$ will be a $\mathbb{Z}_p$-extension of F, called the cyclotomic $\mathbb{Z}_p$-extension of F. Note that, if F is totally real, we see from Theorem 1.3 that, provided Leopoldt's conjecture is valid for F, then the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of F.

Here is another example of a $\mathbb{Z}_p$-extension. Let K be an imaginary quadratic field, and let p be a rational prime which splits in K into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$. Then global class field theory shows that there is a unique $\mathbb{Z}_p$-extension K_∞ of K in which only the prime $\mathfrak{p}$ (but not $\mathfrak{p}^*$) is ramified. If now F is any finite extension of K, the compositum $F_\infty = FK_\infty$ will be another example of a $\mathbb{Z}_p$-extension of F, which is not the cyclotomic $\mathbb{Z}_p$-extension. We shall call this $\mathbb{Z}_p$-extension the split prime $\mathbb{Z}_p$-extension of F. Interestingly, the cyclotomic and the split prime $\mathbb{Z}_p$-extensions of any number field seem to have many properties in common. 31

Exc 4. Let F be a number field. If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F, prove that there are only finitely many places of F_∞ lying above each finite prime of F. If F contains an imaginary quadratic field K, and p splits in K, prove the same assertion for the split prime $\mathbb{Z}_p$-extension of F.

Finally, we point out the following result.

Proposition 1.4. Let F be a finite extension of $\mathbb{Q}$, and J_∞/F a Galois extension such that $\mathrm{Gal}(J_\infty/F) = \mathbb{Z}_p^d$ for some $d \geq 1$. If a prime v of F is ramified in J_∞, then v must divide p.

Proof. If v is a prime of F not dividing p, then its inertia group in J_∞/F must be tamely ramified. But then, by class field theory, such a tamely ramified group must be finite, and so it must be 0 in $\mathrm{Gal}(J_\infty/F)$.

32

§2. 2.1 Henceforth, F will denote a finite extension of $\mathbb{Q}$, and r_2 will always denote the number of complex places of F. For the moment, F_∞/F will denote an arbitrary $\mathbb{Z}_p$-extension of F, where p is any prime number. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$, and let Γ_n denote the unique closed subgroup of Γ of index p^n. Let F_n denote the fixed field of Γ_n, so that $[F_n : F] = p^n$. Let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the set of places of F_∞ lying above p, and put $X(F_\infty) = \mathrm{Gal}(M_\infty/F_\infty)$. For each $n \geq 0$, let M_n be the maximal abelian p-extension of F_n unramified outside p. Since F_∞/F is unramified outside p, we see that $M_n \supset F_\infty$ and that M_n is the maximal abelian extension of F_n contained in M_∞. We next observe that there is a canonical (left) action of Γ on $X(F_\infty)$, which is defined as follows. By maximality, it is clear that M_∞ is Galois over F, so that we have the exact sequence of groups

$$0 \longrightarrow X(F_\infty) \longrightarrow \mathrm{Gal}(M_\infty/F) \longrightarrow \Gamma \longrightarrow 0.$$

If $\tau \in \Gamma$, let $\tilde{\tau}$ denote any lifting of τ to $\mathrm{Gal}(M_\infty/F)$. We then define, for x in $X(F_\infty)$, $\tau x = \tilde{\tau} x \tilde{\tau}^{-1}$. This action is well defined because $X(F_\infty)$ is abelian, and is continuous. Now let $X(F_\infty)_{\Gamma_n}$ be the largest quotient of $X(F_\infty)$ on which the subgroup Γ_n of Γ acts trivially. Since M_n is the maximal abelian extension of F_n contained in M_∞, it follows easily that

$$X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty).$$

In particular, since class field theory tells us that $\mathrm{Gal}(M_0/F_\infty)$

is a finitely generated $\mathbb{Z}_p$-module, it follows from Nakayama's lemma that $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module, where the $\Lambda(\Gamma)$-action is given by extending the Γ-action by linearity and continuity. For each $n \geq 0$, let $\delta_{F_n,p}$ denote the discrepancy of the Leopoldt conjecture for the field F_n (see §1).

Proposition 2.1. The $\Lambda(\Gamma)$-rank of $X(F_\infty)$ is always $\geq r_2$. It is equal to r_2 if and only if the $\delta_{F_n,p}$ are bounded as $n \to \infty$.

Proof. Since $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module, it follows from the structure theory (see Ex. 2) that, provided n is sufficiently large, we have

$$(2.1)\quad \mathbb{Z}_p\text{-rank } X(F_\infty)_{\Gamma_n} = m p^n + c,$$

where m is the $\Lambda(\Gamma)$-rank of $X(F_\infty)$, and c is a constant integer ≥ 0. On the other hand, since $X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty)$, we conclude from Theorem 1.3 applied to the extension M_n/F_n that

$$(2.2)\quad \mathbb{Z}_p\text{-rank of } X(F_\infty)_{\Gamma_n} = r_2 p^n + \delta_{F_n,p};$$

here we are using the fact that the number of complex places of F_n is $r_2 p^n$, because no real place can ramify in the $\mathbb{Z}_p$-extension F_∞/F. The equalities (2.1) and (2.2) immediately imply the Proposition.

Exc 2.1. If $\delta_{F,p} = 0$, prove that the $\delta_{F_n,p}$ are bounded as $n \to \infty$.

34

Our aim in these lectures is to prove the following theorem, which is one of the principal results of Iwasawa's 1973 Annals paper.

Theorem. Let p be any prime number and F_∞/F the cyclotomic $\mathbb{Z}_p$-extension. Then $X(F_\infty)$ has $\Lambda(\Gamma)$-rank r_2, or equivalently $\delta_{F_n,p}$ is bounded as $n \to \infty$.

The essential idea of Iwasawa's proof is to use multiplicative Kummer theory. We do not know how to prove this result for non-cyclotomic $\mathbb{Z}_p$-extensions.

2.2. Multiplicative Kummer theory. For each integer $m > 1$, μ_m will denote the group of m-th roots of unity in $\overline{\mathbb{Q}}$. Until further notice, we shall assume that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, and that

(2.3) $\mu_p \subset F$ if $p > 2$, $\mu_4 \subset F$ if $p = 2$.

Thus we have

(2.4) $F_\infty = F(\mu_{p^\infty})$.

Since $\mu_{p^\infty} \subset F_\infty$, classical multiplicative Kummer theory is as follows. Let $F_\infty^\times$ be the multiplicative group of F_∞, and let F_∞^{ab} be the maximal abelian p-extension of F_∞. Then we have the canonical dual pairing

(2.5) $\langle , \rangle : \mathrm{Gal}(F_\infty^{ab}/F_\infty) \times (F_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mu_{p^\infty}$

given by (here $\alpha \in F_\infty^\times$ and $a \geq 0$)

$$\langle \sigma, \alpha \otimes (p^{-a} \bmod \mathbb{Z}_p) \rangle = \sigma\beta/\beta \quad \text{where } \beta^{p^a} = \alpha.$$

Of course, there is a natural action of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on all of these groups, and the pairing gives rise to an isomorphism of Γ-modules

$$\mathrm{Gal}(F_\infty^{ab}/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}).$$

As before, let M_∞ be the maximal abelian p-extension of F_∞ which is unramified outside p. Since $M_\infty \subset F_\infty$, the Kummer pairing induces an isomorphism of Γ-modules

$$(2.6) \quad \mathrm{Gal}(M_\infty/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{M}_\infty, \mu_{p^\infty}),$$

for a subgroup $\mathcal{M}_\infty \subset F_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$, which can be described explicitly as follows. Recall that, as F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, there are only finitely many primes of F_∞ lying above each rational prime number, and that the primes which do not lie above p all have discrete valuations. Let I'_∞ be the free abelian group on the primes of F_∞ which do not lie above p. Then every $\alpha \in F_\infty^\times$ determines a unique ideal $(\alpha)' \in I'_\infty$. The following lemma is then easily proven.

Lemma. $\mathcal{M}_\infty$ is the subgroup of all elements of $F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ of the form $\alpha \otimes p^{-a} \bmod \mathbb{Z}_p$ where $\alpha \in F_\infty^\times$ is such that $(\alpha)' \in I_\infty^{p^a}$.

We can then analyse $\mathcal{M}_\infty$ by the following exact sequence. Let E'_∞ be the group of all elements α in $F_\infty^\times$ with $(\alpha)' = 1$. We have the obvious map

$$i_\infty : E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathcal{M}_\infty$$

given by $i_\infty(\varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p) = \varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p$, which is easily seen to be injective. Moreover, the map

$$j_\infty : \mathcal{M}_\infty \longrightarrow A'_\infty$$

is defined by $j_\infty(\alpha \otimes p^{-a} \bmod \mathbb{Z}_p) = cl(\mathfrak{a})$, where $(\alpha)' = \mathfrak{a}^{p^a}$. Both i_∞ and j_∞ are obviously Γ-homomorphisms.

Lemma. The sequence of Γ-modules

$$(2.6)\quad 0 \longrightarrow E'_\infty \otimes_{\mathbb{Z}} \mathcal{Q}_p/\mathbb{Z}_p \xrightarrow{i_\infty} \mathcal{M}_\infty \xrightarrow{j_\infty} A'_\infty \longrightarrow 0$$

is exact.

The proof of exactness is completely straightforward. In view of the exact sequence (2.6), we can now break up the Iwasawa module $X(F_\infty) = \mathrm{Gal}(M_\infty/F_\infty)$ into two parts. Define

$$N'_\infty = F_\infty\left(\sqrt[n]{\varepsilon} \text{ for all } \varepsilon \in E'_\infty \text{ and all } n \geq 1\right).$$

Then, thanks to (2.6), the Kummer pairing induces Γ-isomorphisms

$$\mathrm{Gal}(N'_\infty/F_\infty) \xrightarrow{\sim} \mathrm{Hom}\left(E'_\infty \otimes_{\mathbb{Z}} \mathcal{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}\right)$$

and

$$\mathrm{Gal}(M_\infty/N'_\infty) \xrightarrow{\sim} \mathrm{Hom}\left(A'_\infty, \mu_{p^\infty}\right).$$

Let $T_p(\mu) = \varprojlim \mu_{p^n}$ be the Tate module of μ_{p^∞}. Thus $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 on which Γ acts via the character giving the action of Γ on μ_{p^∞}. Thus, if we now define

$$(2.7)\quad Z'_\infty = \mathrm{Hom}\left(A'_\infty, \mathcal{Q}_p/\mathbb{Z}_p\right),$$

we see immediately that $\mathrm{Gal}(M_\infty/N'_\infty) = Z'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu)$, endowed with the diagonal action of Γ.

Theorem A (Iwasawa). Z'_∞ is always a finitely generated torsion $\Lambda(\Gamma)$-module.

In fact, Iwasawa proved Theorem A for an arbitrary $\mathbb{Z}_p$-extension F_∞/F (the definition of A'_∞ we have given must be slightly modified for an arbitrary $\mathbb{Z}_p$-extension).

Now it is easy to see that if Z'_∞ is $\Lambda(\Gamma)$-torsion, then so is $Z'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu)$. Hence, for the cyclotomic $\mathbb{Z}_p$-extension, Theorem A has the following corollary:-

Corollary. $\mathrm{Gal}(M_\infty/N'_\infty)$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

In the next lecture we will outline Iwasawa's proof of the following result:—

Theorem B (Iwasawa). Let $F_\infty = F(\mu_{p^\infty})$, where $\mu_p \subset F$ if $p > 2$ and $\mu_4 \subset F$ if $p = 2$. Then $\mathrm{Gal}(N'_\infty / F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module of rank $r_2 = [F:\mathbb{Q}]/2$.

The value of r_2 is as given because F is clearly totally imaginary. As we shall see in the next lecture, Iwasawa's proof gives very precise information about the $\Lambda(\Gamma)$-torsion submodule of $\mathrm{Gal}(N'_\infty/F_\infty)$.

Of course, Theorem A and Theorem B together imply that $\mathrm{Gal}(M_\infty/F_\infty)$ has $\Lambda(\Gamma)$-rank equal to $r_2 = [F:\mathbb{Q}]/2$, proving the weak Leopoldt conjecture in this case.

2.3 Elementary properties of p-units in F_∞/F.

As a first step towards proving Theorem B, we establish some basic properties of the units E'_∞. Let W_n be the group of all roots of unity in F_n, and W_∞ the group of all roots of unity in F_∞. Thus W_∞ is the product of μ_{p^∞} with a finite group of order prime to p. Define

$$\mathcal{E}'_n = E'_n/W_n, \quad \mathcal{E}'_\infty = E'_\infty/W_\infty \ ;$$

here E'_n denotes the group of p-units of F_n. Let σ_n denote

38 the number of primes of F_n lying above $\mathfrak{p}$. Then, by the generalization of the unit theorem to $\mathfrak{p}$-units, $\mathcal{E}'_n$ is a free abelian group of rank $r_2 p^n + s_{n-1}$, where $r_2 = [F:\mathbb{Q}]/2$. Moreover, $\mathcal{E}'_\infty$ is the union of the increasing sequence of subgroups $\mathcal{E}'_n$.

Lemma. $\mathcal{E}'_\infty$ is a free abelian group, and, for all $n \geq 0$, $\mathcal{E}'_n$ is a direct summand of $\mathcal{E}'_\infty$.

Proof. Now $(E'_\infty)^{\Gamma_n} = E'_n$ for all $n \geq 0$. As $H^1(\Gamma_n, W_\infty) = (W_\infty)_{\Gamma_n} = 0$, it follows that $(\mathcal{E}'_\infty)^{\Gamma_n} = \mathcal{E}'_n$ for all $n \geq 0$. We next observe that $\mathcal{E}'_\infty / \mathcal{E}'_n$ is torsion free. Indeed, suppose u is an element of $\mathcal{E}'_\infty$ with $u^k \in \mathcal{E}'_n$ for some integer $k \geq 1$. If γ is any element of Γ_n, we must then have $(\gamma u / u)^k = 1$, whence $\gamma u = u$ since $\mathcal{E}'_\infty$ is torsion free, and so $u \in \mathcal{E}'_n$ as required. Hence, for all $m \geq n$, $\mathcal{E}'_m / \mathcal{E}'_n$ is torsion free. As $\mathcal{E}'_m$ and $\mathcal{E}'_n$ are both finitely generated torsion free abelian groups, it follows that $\mathcal{E}'_n$ must be a direct summand of $\mathcal{E}'_m$ for all $m \geq n$, and the ~~finish~~ assertions of the lemma follow.

§3. We now give Iwasawa's proof of Theorem B of the last lecture. Let φ' be the ring of all rational numbers whose denominator is a power of p. Note that $\varphi'/\mathbb{Z} = \varphi_p/\mathbb{Z}_p$. Hence, for all $n \geq 0$, we have the exact sequence

$$0 \to \mathcal{E}_n' \to \mathcal{E}_n' \otimes_{\mathbb{Z}} \varphi' \to \mathcal{E}_n' \otimes_{\mathbb{Z}} \varphi_p/\mathbb{Z}_p \to 0$$

Also, we have the exact sequence

$$(3.1)\quad 0 \to \mathcal{E}_\infty' \to \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \varphi' \to \mathcal{E}_\infty' \otimes \varphi_p/\mathbb{Z}_p \to 0.$$

Recall that, for all $n \geq 0$, $\mathcal{E}_n'$ is a direct summand of $\mathcal{E}_\infty'$, and $(\mathcal{E}_\infty')^{\Gamma_n} = \mathcal{E}_n'$. It follows that

$$\left(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \varphi'\right)^{\Gamma_n} = \mathcal{E}_n' \otimes_{\mathbb{Z}} \varphi'.$$

Also, for all $n \geq 0$,

$$H^1\left(\Gamma_n, \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \varphi'\right) = \varinjlim_{m \geq n} H^1\left(\mathrm{Gal}(K_m/K_n), \mathcal{E}_m' \otimes_{\mathbb{Z}} \varphi'\right),$$

and this last cohomology group is 0 because $\mathcal{E}_m' \otimes_{\mathbb{Z}} \varphi'$ is p-divisible. Hence we have

$$H^1\left(\Gamma_n, \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \varphi'\right) = 0.$$

Thus, taking Γ_n-cohomology of the exact sequence (3.1), we immediately obtain:—

<u>Proposition 3.1</u> For all $n \geq 0$, we have the exact sequence

$$0 \to \mathcal{E}_n' \otimes_{\mathbb{Z}} \varphi_p/\mathbb{Z}_p \to \left(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \varphi_p/\mathbb{Z}_p\right)^{\Gamma_n} \to H^1\left(\Gamma_n, \mathcal{E}_\infty'\right) \to 0.$$

To prove Theorem B, we also need to know that $H^1(\Gamma_n, \mathcal{E}_\infty')$ is a finite group. In fact, it is a torsion group, and it must be finitely generated because the Pontrjagin dual of $\mathcal{E}_\infty \otimes \varphi_p/\mathbb{Z}_p$ is a finitely generated $\Lambda(\Gamma)$-module.

40 However, a more intrinsic proof, which in the end yields more information about the structure of $Gal(N_\infty' | F_\infty)$ as a $\Lambda(\Gamma)$-module, comes from the following result. For all $n \geq 0$, let I_n' denote the multiplicative group of all fractional ideals of F_n which are prime to p, and let $P_n' = \{(\alpha)' : \alpha \in F_n^\times\}$ be the subgroup of principal ideals. Put A_n' for the p-primary subgroup of I_n'/P_n'. For all $n \geq 0$, we have the natural injection $I_n' \longrightarrow I_\infty'$, and this induces a homomorphism $A_n' \longrightarrow A_\infty'$.

Proposition 3.2. For all $n \geq 0$, we have

$$H^1(\Gamma_n, \mathcal{E}_\infty') = \mathrm{Ker}\,(A_n' \longrightarrow A_\infty').$$

In particular, $H^1(\Gamma_n, \mathcal{E}_\infty')$ is finite.

We remark that, in his 1973 Annals paper, Iwasawa proves that Proposition 3.2 is valid for every $\mathbb{Z}_p$-extension F_∞/F in which every prime of F above p is ramified. Under the same hypotheses, he also shows that the order of $H^1(\Gamma_n, \mathcal{E}_\infty')$ is bounded as $n \to \infty$. In his Ph.D thesis at Princeton under Iwasawa, Ralph Greenberg showed the existence of many examples when $\mathrm{Ker}\,(A_n' \longrightarrow A_\infty')$ is non-zero. However, in the most classical case when $F = \mathbb{Q}(\mu_p)$ with p an odd prime, and $F_\infty = \mathbb{Q}(\mu_{p^\infty})$, it is still unknown whether there exist primes p such that $\mathrm{Ker}\,(A_n' \longrightarrow A_\infty')$ is non-zero.

Before proving Proposition 3.2, we first show that Theorem B is an easy consequence of Proposition 3.1. For each $n \geq 0$, let s_n denote the number of primes of F_n lying above p. Then the analogue of Dirichlet's

theorem for the E_n' tells us that $\mathcal{E}_n'$ is a free abelian group of rank $r_2 p^n + s_n - 1$. Moreover, since p is totally ramified in the extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, it follows that there exists $n_0 \geq 0$ such that every prime above p is totally ramified in the extension F_∞/F_{n_0}. Hence we conclude that $s_n = s$, where $s = s_{n_0}$, for all $n \geq n_0$. Thus, since $H^1(\Gamma_n, \mathcal{E}_\infty')$ is finite, it follows from Proposition 3.1 that, provided $n \geq n_0$, the maximal divisible subgroup of $(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}$ has $\mathbb{Z}_p$-corank $r_2 p^n + s - 1$. Put

$$Y_\infty' = \mathrm{Hom}\left(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Then it follows immediately from Pontrjagin duality that $(Y_\infty')_{\Gamma_n}$ has $\mathbb{Z}_p$-rank $r_2 p^n + s - 1$ for all $n \geq n_0$. Now Y_∞' is a finitely generated $\Lambda(\Gamma)$-module because $(Y_\infty')_\Gamma$ is a finitely generated $\mathbb{Z}_p$-module, and so it follows immediately from the structure theory (see Exc 2) that Y_∞' has $\Lambda(\Gamma)$-rank equal to r_2. But Kummer theory immediately shows that

$$Y_\infty' \otimes_{\mathbb{Z}_p} T_p(\mu) = \mathrm{Gal}\left(N_\infty'/F_\infty\right).$$

Thus Theorem B then follows from the following simple algebraic exercise.

<u>Exc 3.1</u>. Let W be any finitely generated $\Lambda(\Gamma)$-module. Assume $\mu_{p^\infty} \subset F_\infty$, and let $V = W \otimes_{\mathbb{Z}_p} T_p(\mu)$, where Γ acts on V by the twisted action $\sigma(w \otimes \alpha) = \sigma w \otimes \sigma\alpha$, with $w \in W$ and $\alpha \in T_p(\mu)$. Prove that the $\Lambda(\Gamma)$-module V has the same $\Lambda(\Gamma)$-rank as W.

42

We remark that, in his 1973 Annals paper, Iwasawa shows that a further analysis of the above proof of Theorem B yields more information about the $\Lambda(\Gamma)$-module $Gal(N'_\infty/F_\infty)$. Let $t(Gal(N'_\infty/F_\infty))$ denote the $\Lambda(\Gamma)$-torsion submodule of $Gal(N'_\infty/F_\infty)$. Then Iwasawa proves the following facts:- (i) $Gal(N'_\infty/F_\infty)$ contains no non-zero $\mathbb{Z}_p$-torsion, (ii) $t(Gal(N'_\infty/F_\infty))$ is a free $\mathbb{Z}_p$-module of rank $s-1$, where s = number of primes above p in the extension F_∞/F_{n_0} as above, and he determines exactly its characteristic power series (even its structure up to pseudo-isomorphism), and (iii). $Gal(N'_\infty/F_\infty)/t(Gal(N'_\infty/F_\infty))$ is a free $\Lambda(\Gamma)$-module if and only if $H^1(\Gamma_n, \mathcal{E}'_\infty) = 0$ for all $n \geq a$, where a is an explicitly determined integer $\leq s-1$.

Finally, we give the proof of Proposition 3.2. For all $m \geq n$, we will prove that there is an isomorphism

$$\tau_{n,m} : \mathrm{Ker}(A'_n \longrightarrow A'_m) \xrightarrow{\sim} H^1(Gal(F_m/F_n), E'_m).$$

Passing to the inductive limit over all $m \geq n$, and noting that $H^i(\Gamma_n, W_\infty) = 0$ for all $i \geq 1$, Proposition 3.2 will then follow. Fix a generator σ of $Gal(F_m/F_n)$, and write $\mathcal{O}'_m$ for the ring of p-integers of F_m. If c is some element of $\mathrm{Ker}(A'_n \to A'_m)$, and $\mathfrak{w} \in I_n$ is an ideal in c, then $\mathfrak{w}\mathcal{O}'_m = \alpha\mathcal{O}'_m$ for some $\alpha \in \mathcal{O}'_m$. Define $\varepsilon = \sigma\alpha/\alpha$. Thus ε is an element of E'_m with $N_{F_m/F_n}(\varepsilon) = 1$. It is easy to see that the cohomology class $\{\varepsilon\}$ of ε in $H^1(Gal(F_m/F_n), E'_m)$ depends only on c, and we define $\tau_{n,m}(c) = \{\varepsilon\}$. One checks easily that $\tau_{n,m}$ is injective. To prove surjectivity, let $\{\varepsilon\}$ be any cohomology class in $H^1(Gal(F_m/F_n), E'_m)$ which is represented by an element ε of E'_m with $N_{m,n}(\varepsilon) = 1$. By Hilbert's Theorem 90, we then have $\varepsilon = \alpha^{\sigma-1}$ for some $\alpha \in \mathcal{O}'_m$. Let $\mathfrak{w}$ in I'_m be given by $\mathfrak{w} = \alpha\mathcal{O}'_m$. Since ε is in E'_m, we see that $\mathfrak{w}^\sigma = \mathfrak{w}$. Moreover, no prime of F_n which does not divide p is ramified in F_m, and so it follows that $\mathfrak{w}$ must be the image of an ideal $\mathfrak{v}$ in I'_n under the natural inclusion $I'_n \subset I'_m$. Let c be the class of $\mathfrak{v}$ in I'_n. One sees easily that c lies in $\mathrm{Ker}(A'_n \to A'_m)$, and $\tau_{n,m}(c) = \{\varepsilon\}$, completing the proof.

§4. We now rapidly explain Iwasawa's proof of Theorem A. Let F_∞/F be an arbitrary $\mathbb{Z}_p$-extension. For each $n \geq 0$, let $\mathcal{O}_n'$ be the ring of p-integers of F_n, I_n' the group of invertible $\mathcal{O}_n'$-ideals, $P_n' \subset I_n'$ the group of principle invertible $\mathcal{O}_n'$-ideals, and A_n' the p-primary subgroup of I_n'/P_n'. If $n \leq m$, we have the two natural homomorphisms

$$i_{n,m} : A_n' \longrightarrow A_m', \quad N_{m,n} : A_m' \longrightarrow A_n'$$

which are respectively induced by the natural inclusion of I_n' into I_m' and the norm map from I_m' to I_n'. We then define the Γ-modules

$$A_\infty' = \varinjlim A_n', \quad W_\infty' = \varprojlim A_n',$$

where the inductive limit is taken with respect to the $i_{n,m}$ and the projective limit is taken with respect to the $N_{m,n}$, and both are endowed with their natural action of Γ. Thus A_∞' is a discrete $\Lambda(\Gamma)$-module, and W_∞' is a compact $\Lambda(\Gamma)$-module.

Proposition 4.1. W_∞' is canonically isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(L_\infty'/F_\infty)$, where L_∞' denotes the maximal unramified abelian p-extension of F_∞, in which every prime of F_∞ lying above p splits completely.

Proof. Let L_n' be the maximal unramified abelian p-extension of F_n in which every prime above p splits completely. By global class field theory, the Artin map induces an isomorphism $A_n' \xrightarrow{\sim} \mathrm{Gal}(L_n'/F_n)$, which preserves the natural action of Γ/Γ_n on both abelian groups.

Let $n_0 \geq 0$ be such that every prime of $F_{\infty n_0}$ which is ramified in F_∞ is totally ramified in F_∞. Thus, if $m \geq n \geq n_0$, we must have $L'_n \cap F_m = F_n$, so that $\mathrm{Gal}(L'_n F_m / F_m) \simeq \mathrm{Gal}(L'_m / F_n)$. Moreover, global class field theory then tells us that the diagram

$$\begin{array}{ccc} A'_m & \xrightarrow{\sim} & \mathrm{Gal}(L'_m/F_m) \\ {\scriptstyle N_{m,n}}\downarrow & & \downarrow \\ A'_n & \xrightarrow{\sim} & \mathrm{Gal}(L'_n F_m/F_m) = \mathrm{Gal}(L'_n/F_n) \end{array}$$

is commutative. Hence $W_\infty = \varprojlim A'_n$ is isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(R_\infty/F_\infty)$, where $R_\infty = \bigcup_{n \geq 0} L'_n$. Obviously $R_\infty \subset L'_\infty$. But every element of L'_∞ satisfies an equation with coefficients in F_n for some $n \geq n_0$, whence we see that also $L'_\infty \subset R_\infty$, and so $L'_\infty = R_\infty$, and W_∞ is isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(L'_\infty/F_\infty)$, as required.

Proposition 4.2. Let $s \geq 1$ be the number of primes of F_∞ which are ramified in the $\mathbb{Z}_p$-extension F_∞/F. Then, for all $n \geq n_0$, we have that

$$\mathbb{Z}_p\text{-rank of } (W'_\infty)_{\Gamma_n} \leq s-1.$$

In particular, W'_∞ is a torsion $\Lambda(\Gamma)$-module.

Proof. For each $n \geq 0$, let $\mathcal{L}'_n$ denote the maximal abelian extension of F_n contained in L'_∞. Obviously $\mathcal{L}'_n \supset F_\infty$, and by the definition of the Γ-action on $W'_\infty = \mathrm{Gal}(L'_\infty/F_\infty)$, we have

$$(4.1) \qquad (W'_\infty)_{\Gamma_n} = \mathrm{Gal}(\mathcal{L}'_n/F_\infty).$$

Assume now that $n \geq n_0$, so that there are precisely

s primes of F_n which are ramified in the extension $\mathcal{L}_n' / F_n$. Denote these primes by w_i $(i = 1, \dots, s)$, and let T_i be the inertia group of w_i in $\mathcal{L}_n' / F_n$. Since w_i is completely ramified in F_∞ / F_n, and then splits completely in $\mathcal{L}_n' / F_\infty$, we must have $T_i \xrightarrow{\sim} \Gamma_n \xrightarrow{\sim} \mathbb{Z}_p$ for $i = 1, \dots, s$. Now L_n' is the maximal unramified extension of F_n contained in $\mathcal{L}_n'$. Hence

$$\mathrm{Gal}\left(\mathcal{L}_n' / L_n'\right) = T_1 \dots T_s .$$

Since $\mathrm{Gal}\left(L_n' / F_n\right)$ is finite, we conclude that the module $\mathrm{Gal}\left(\mathcal{L}_n' / F_n\right)$ has $\mathbb{Z}_p$-rank at most s. As $\mathrm{Gal}\left(F_\infty / F_n\right)$ has $\mathbb{Z}_p$-rank equal to 1, it follows that

$$\mathbb{Z}_p\text{-rank of } \mathrm{Gal}\left(\mathcal{L}_n' / F_\infty\right) \leq s - 1 \quad \text{for all } n \geq n_0 .$$

In view of (4.1), it now follows from the structure theory that W_∞' is a torsion $\Lambda(\Gamma)$-module, as claimed.

We end these notes by explaining, without proofs, the precise relationship between W_∞' and $\mathrm{Hom}\left(A_\infty', \mathcal{Q}_p / \mathbb{Z}_p\right)$ as $\Lambda(\Gamma)$-modules, which shows, in particular, that $\mathrm{Hom}\left(A_\infty', \mathcal{Q}_p / \mathbb{Z}_p\right)$ is also a torsion $\Lambda(\Gamma)$-module. Let X be any finitely generated torsion $\Lambda(\Gamma)$-module. We define the $\Lambda(\Gamma)$-module $\alpha(X)$, called the adjoint of X by

$$\alpha(X) = \mathcal{E}\mathrm{xt}^1_{\Lambda(\Gamma)}\left(X, \Lambda(\Gamma)\right).$$

It turns out that $\alpha(X)$ is pseudo-isomorphic to X, and contains no non-zero finite $\Lambda(\Gamma)$-submodule.

Theorem 4.3. $\mathrm{Hom}\left(A_\infty', \mathcal{Q}_p / \mathbb{Z}_p\right) = \alpha\left(\mathrm{Gal}\left(L_\infty' / F_\infty L_{n_0}'\right)\right)$.

Hence $\mathrm{Hom}\left(A_\infty', \mathcal{Q}_p / \mathbb{Z}_p\right)$ is pseudo-isomorphic to $W_\infty' = \mathrm{Gal}\left(L_\infty / F_\infty\right)$, and so is $\Lambda(\Gamma)$-torsion.

CLASSICAL IWASAWA THEORY
ARIZONA WINTER SCHOOL 2018

JOHN COATES

(typeset by Robert JS McDonald, UConn[1])

Lecture 1. Foundational material.

The lecture will briefly cover, without proofs, the background in algebra and number theory needed at the beginning of Iwasawa theory. Throughout, p will denote an arbitrary prime number, and Γ a topological group which is isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. Thus, for each $n \geq 0$, Γ will have a closed subgroup of index p^n, which we will denote by Γ_n, and Γ/Γ_n will then be a cyclic group of order p^n. The Iwasawa algebra $\Lambda(\Gamma)$ of Γ is defined by

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$$

and it is endowed with the natural topology coming from the p-adic topology on the $\mathbb{Z}_p[\Gamma/\Gamma_n]$.

1.1. **Some relevant algebra.** We recall without proof some of the basic algebra needed in classical Iwasawa theory. Let $R = \mathbb{Z}_p[\![T]\!]$ be the ring of formal power series in an indeterminate T with coefficients in $\mathbb{Z}_p$. Then R is a Noetherian regular local ring of dimension 2 with maximal ideal $\mathfrak{m} = (p, T)$. We say that a monic polynomial $q(T) = \sum_{i=0}^{n} a_i T^i$ in R is *distinguished* if $a_0, \ldots, a_{n-1} \in p\mathbb{Z}_p$. The Weierstrass preparation theorem for R tells us that every non-zero $f(T)$ in R can be written uniquely in the form $F(T) = p^\mu q(T) u(T)$, where $\mu \geq 0$, $q(T)$ is distinguished polynomial, and $u(T)$ is a unit in R.

Proposition 1.1. *Let γ be a fixed topological generator of Γ. Then there is a unique isomorphism of $\mathbb{Z}_p$-algebras*

$$\Lambda(\Gamma) \xrightarrow{\sim} R = \mathbb{Z}_p[\![T]\!]$$

which maps γ to $1 + T$.

In the following, we shall often identify $\Lambda(\Gamma)$ and R, bearing in mind that Γ will not usually have a canonical topological generator.

Let X be any profinite abelian p-group, on which Γ acts continuously. Then the Γ-action extends by continuity and linearity to an action of the whole Iwasawa algebra $\Lambda(\Gamma)$. Moreover, X will be finitely generated over $\Lambda(\Gamma)$ if and only if $X/\mathfrak{m}X$ is finite, where $\mathfrak{m} = (p, \gamma - 1)$, with γ a topological generator of Γ, is the maximal ideal of $\Lambda(\Gamma)$. We write $\mathcal{R}(\Gamma)$ for the category of finitely generated $\Lambda(\Gamma)$-rank of X to be the $Q(\Gamma)$-dimension of $X \otimes_{\Lambda(\Gamma)} Q(\Gamma)$, where $Q(\Gamma)$ denotes the field of fractions of $\Lambda(\Gamma)$. We say X is $\Lambda(\Gamma)$-torsion if it has $\Lambda(\Gamma)$-rank 0, or equivalently if $\alpha X = 0$ for some non-zero α in $\Lambda(\Gamma)$.

Although $\Lambda(\Gamma)$ is not a principal ideal domain, there is nevertheless a beautiful structure theory for modules in $Q(\Gamma)$ (see Bourbaki, Commutative Algebra, Chap. 7, §4), which can be summarized by the following result:

[1] please feel free to contact me with corrections: robert.j.mcdonald@uconn.edu

Theorem 1.2. *For each X in $\mathcal{R}(\Gamma)$, we have an exact sequence of $\Lambda(\Gamma)$-modules*

$$0 \longrightarrow D_1 \longrightarrow X \longrightarrow \Lambda(\Gamma)^r \oplus \bigoplus_{i=1}^{m} \Lambda(\Gamma)/(f_i) \longrightarrow D_2 \longrightarrow 0,$$

where D_q and D_2 have finite cardinality, and $f_i \neq 0$ for $i = 1, \dots m$. Moreover, the ideal $c(X) = f_1 \cdots f_m \Lambda(\Gamma)$ is uniquely determined by X when $r = 0$.

We list some of the main consequences of the structure theory used in Iwasawa theory. First, X will be $\Lambda(\Gamma)$-torsion if and only if $r = 0$. Suppose now that X is $\Lambda(\Gamma)$-torsion. The principal ideal $c(X)$ is called the characteristic ideal of X. A characteristic element of X is any generator $f_X(T)$ of $c(X)$. By the Weierstrass preparation theorem, we can write

$$f_X(T) = p^{\mu(X)} q_X(T) u(T),$$

where $\mu(X)$ is an integer ≥ 0, $q_X(T)$ is a distinguished polynomial, and $u(T)$ is a unit in $\Lambda(\Gamma)$. Clearly $\mu(X)$ and $q_X(T)$ are uniquely determined by X. We define $\mu(X)$ to be the μ-invariant of X, and we define the degree $\lambda(X)$ of $q_X(T)$ to be the λ-invariant of X.

Ex 1.1. Assume X in $\mathcal{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion. Prove that X is finitely generated as a $\mathbb{Z}_p$-module if and only if $\mu(X) = 0$.

Recall that Γ_n denotes the unique subgroup of Γ of index p^n. Thus, if Γ has a topological generator γ, then Γ_n is topologically generated by γ^{p^n}. If X is in $\mathcal{R}(\Gamma)$, we define X^{Γ_n} and X_{Γ_n} to be the largest submodule and quotient submodule of X, respectively, on which Γ_n acts trivially. Thus

$$(X)_{\Gamma_n} = X/(\gamma^{p^n} - 1)X.$$

Ex 1.2. Assume X is in $\mathcal{R}(\Gamma)$, and that, for all $n \geq 0$, we have

$$\mathbb{Q}_p\text{-dimension of } \Big((X)_{\Gamma_n} \bigotimes_{\mathbb{Z}_p} \mathbb{Q}_p \Big) = mp^n + \delta_n,$$

where m is independent of n, and δ_n is bounded as $n \to \infty$. Prove that X has $\Lambda(\Gamma)$-rank equal to m, and that δ_n is constant for n sufficiently large.

Ex 1.3. Assume X in $\mathcal{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion, and let $f_X(T)$ be any characteristic element. Prove that the following are equivalent:

(i) $f_X(0) \neq 0$,
(ii) X_Γ is finite, and
(iii) X^Γ is finite.

When all three are valid, prove the Euler characteristic formula

$$|f_X(0)|_p^{-1} = \#(X_\Gamma)/\#(X^\Gamma)$$

1.2. **Some basic class field theory.** We recall basic facts from abelian class field theory which will be used repeatedly later. As always, p is any prime number. Let F be a finite extension of $\mathbb{Q}$, and K an extension of F. We recall that an infinite place v of F is said to ramify in K if v is real and if there is at least one complex prime of K above v. In these lectures, we will mainly be concerned with the maximal abelian p-extension L of F, which is unramified at all finite and infinite places of F (i.e. L is the p-Hilbert class field of F), and with the maximal abelian p-extension of F, which is unramified at all infinite places of F and all finite places of F which do not lie above p. Artin's global reciprocity law gives the following explicit descriptions of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(M/F)$, in which we simply write isomorphisms for the relevant Artin maps. Firstly, we have

$$A_F \xrightarrow{\sim} \mathrm{Gal}(L/F),$$

where A_F denotes the p-primary subgroup of the ideal class group of F. Secondly, for each place v of F lying above p, write U_v for the group of local units in the completion of F at v which are $\equiv 1 \bmod v$. Put

$$U_F = \prod_{v|p} U_v.$$

If W is any $\mathbb{Z}_p$-module, we define the $\mathbb{Z}_p$-rank of W to be $\dim_{\mathbb{Q}_p}(W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Then U_F is a $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $[F : \mathbb{Q}]$. Let E_F be the group of all global units of F which are $\equiv 1 \bmod v$ for all primes v of F lying above p. By Dirichlet's theorem, E_F has $\mathbb{Z}$-rank equal to $r_1 + r_2 - 1$, where r_1 is the number of real and r_2 the number of complex places of F. Now we have the obvious embedding of E_F into U_F and we define $\overline{E}_F$ to be the closure in the p-adic topology of the image of E_F (equivalently, $\overline{E}_F$ is the $\mathbb{Z}_p$-submodule of U_F which is generated by the image of E_F). Secondly, the Artin map then induces an isomorphism

$$U_F/\overline{E}_F \xrightarrow{\sim} \mathrm{Gal}(M/L),$$

where, as above, L is the p-Hilbert class field of F. Clearly, the $\mathbb{Z}_p$-module $\overline{E}_F$ must have $\mathbb{Z}_p$-rank equal to $r_q + r_2 - 1 - \delta_{F,p}$ for some integer $\delta_{F,p} \geq 0$, and so we immediately obtain:

Theorem 1.3. *Let M be the maximal abelian p-extension of F which is unramified outside the primes of F lying above p. Then $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $r_2 + 1 + \delta_{F,p}$.*

Leopoldt's Conjecture. $\delta_{F,p} = 0$.

The conjecture follows from Baker's thorem on linear forms in the p-adic logarithms of algebraic numbers when F is a finite abelian extension of either $\mathbb{Q}$ or an imaginary quadratic field.

1.3. **$\mathbb{Z}_p$-extensions.** Let F be a finite extension of $\mathbb{Q}$. A $\mathbb{Z}_p$-extension of F is defined to be any Galois extension F_∞ of F such that the Galois group of F_∞ over F is topologically isomorphic to $\mathbb{Z}_p$.

The most basic example of a $\mathbb{Z}_p$-extension is the cyclotomic $\mathbb{Z}_p$ extension of F. For each $m > 1$, let μ_m denote the group of m-th roots of unity, and put $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$. The action of the Galois group of $\mathbb{Q}(\mu_{p^\infty})$ over $\mathbb{Q}$ on μ_{p^∞} defines an injection of this Galois group into $\mathbb{Z}_p^\times$, and this injection is an isomorphism by the irreducibility of the p-power cyclotomic polynomials. Put $V = 1 + 2p\mathbb{Z}_p$, so that V is isomorphic to $\mathbb{Z}_p$ under the p-adic logarithm. Then $\mathbb{Z}_p^\times = \mu_2 \times V$ when $p = 2$, and

$\mu_{p-1} \times V$ when $p > 2$. Hence $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$, where $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$ and Δ is cyclic of order 2 or $p-1$, according as $p = 2$ or $p > 2$. Thus

$$\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$$

will be a $\mathbb{Z}_p$ extension of $\mathbb{Q}$, which we call the cyclotomic $\mathbb{Z}_p$-extension. Theorem 1.3 shows that it is the unique $\mathbb{Z}_p$ extension of $\mathbb{Q}$. If now F is any finite extension, the compositum $F\mathbb{Q}_\infty$ will be a $\mathbb{Z}_p$-extension of F, called the cyclotomic $\mathbb{Z}_p$-extension of F. Note that, if F is totally real, we see from Theorem 1.3 that, provided Leopoldt's conjecture is valid for F, then the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of F.

Here is another example of a $\mathbb{Z}_p$-extension. Let K be an imaginary quadratic field, and let p be a rational prime which splits in K into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$. Then global class field theory shows that there is a unique $\mathbb{Z}_p$-extension K_∞ of K in which only the prime $\mathfrak{p}$ (but not $\mathfrak{p}^*$) is ramified. If now F is any finite extension of K, the compositum $F_\infty = FK_\infty$ will be another example of a $\mathbb{Z}_p$ extension, which is not the cyclotomic $\mathbb{Z}_p$-extension. We shall call this $\mathbb{Z}_p$-extension the split prime $\mathbb{Z}_p$-extension of F. Interestingly, the cyclotomic and the split prime $\mathbb{Z}_p$-extensions of any number field seem to have many properties in common.

Ex 1.4. Let F be a number field. If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F, prove that there are only finitely many places of F_∞ lying above each finite prime of F. If F contains an imaginary quadratic field K, and p splits in K, prove the same assertion for the split prime $\mathbb{Z}_p$-extension of F.

Finally, we point out the following result.

Proposition 1.4. *Let F be a finite extension of $\mathbb{Q}$, and J_∞/F a Galois extension such that $\mathrm{Gal}(J_\infty/F) = \mathbb{Z}_p^d$ for some $d \geq 1$. If a prime v of F is ramified in J_∞, then v must divide p.*

Proof. If v is a prime of F not dividing p, then its inertia group in J_∞/F must be tamely ramified. But then, by class field theory, such a tamely ramified group must be finite, and so it must be 0 in $\mathrm{Gal}(J_\infty/F)$. □

Lecture 2.

2.1. Henceforth, F will denote a finite extension of $\mathbb{Q}$, and r_2 will always denote the number of complex places of F. For the moment, F_∞/F will denote an arbitrary $\mathbb{Z}_p$-extension of F, where p is any prime number. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$, and let Γ_n denote the unique closed subgroup of Γ of index p^n. Let F_n denote the fixed field of Γ_n, so that $[F_n : F] = p^n$. Let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the set of places of F_∞ lying above p, and put $X(F_\infty) = \mathrm{Gal}(M_\infty/F_\infty)$. For each $n \geq 0$, let M_n be the maximal abelian p-extension of $F)n$ unramified outside p. Since F_∞/F is unramified outside p, we see that $M_n \supset F_\infty$ and that M_n is the maximal abelian extension of F_n contained in M_∞. We next observe that there is a canonical (left) action of Γ on $X(F_\infty)$, which is defined as follows. By maximality, it is clear that M_∞ is Galois over F, so that we have the exact sequence of groups

$$0 \longrightarrow X(F_\infty) \longrightarrow \mathrm{Gal}(M_\infty/F) \longrightarrow \Gamma \longrightarrow 0.$$

If $\tau \in \Gamma$, let $\tilde{\tau}$ denote any lifting of τ to $\mathrm{Gal}(M_\infty/F)$. We then define, for $x \in X(F_\infty)$, $\tau x = \tilde{\tau} x \tilde{\tau}^{-1}$. This action is well defined because $X(F_\infty)$ is abelian, and is continuous. Now let $X(F_\infty)_{\Gamma_n}$ be the

largest quotient of $X(F_\infty)$ on which the subgroup Γ_n of Γ acts trivially. Since M_n is the maximal abelian extension of F_n contained in M_∞, it follows easily that

$$X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty).$$

In particular, since class field theory tells us that $\mathrm{Gal}(M_0/F_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, it follows from Nakayama's lemma that $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module where the $\Lambda(\Gamma)$-action is given by extending the Γ-action by linearity and continuity. For each $n \geq 0$, let $\delta_{F_n,p}$ denote the discrepancy of the Leopoldt conjecture for the field F_n (see §1).

Proposition 2.1. *The $\Lambda(\Gamma)$-rank of $X(F_\infty)$ is always $\geq r_2$. It is equal to r_2 if and only if the $\delta_{F_n,p}$ are bounded as $n \to \infty$.*

Proof. Since $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module, it follows from the structure theory (see Ex 1.2) that, provided n is suffiiciently large, we have

$$\mathbb{Z}_p\text{-rank } X(F_\infty)_{\Gamma_n} = mp^n + c \tag{1}$$

where m is the $\Lambda(\Gamma)$-rank of $X(F_\infty)$, and c is a constant integer ≥ 0. On the other hand, since $X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty)$, we conclude from Theorem 1.3 applied to the extension M_n/F_n that

$$\mathbb{Z}_p\text{-rank of } X(F_\infty)_{\Gamma_n} = r_2 p^n + \delta F_n, p; \tag{2}$$

here we are using the fact that the number of complex places of F_n is $r_2 p^n$, because no real place can ramify in the $\mathbb{Z}_p$-extension F_∞/F. The equalities (1) and (2) immediately imply the proposition. □

Ex 2.1. If $\delta_{F,p} = 0$, prove that the $\delta_{F_n,p}$ are bounded as $n \to \infty$.

Our aim in these lectures is to prove the following theorem which is one of the principal results of Iwasawa's 1973 Annals paper.

Theorem 2.2. *Let p be any prime number and F_∞/F the cyclotomic $\mathbb{Z}_p$-extension. Then $X(F_\infty)$ has $\Lambda(\Gamma)$-rank r_2, or equivalently $\delta_{F_n,p}$ is bounded as $n \to \infty$.*

The essential idea of Iwasawa's proof is to use multiplicative Kummer theory. We do not know how to prove this result for non-cyclotomic $\mathbb{Z}_p$-extensions.

2.2. **Multiplicative Kummer theory.** For each integer $m > 1$, μ_m will denote the group of m-th roots of unity in $\overline{\mathbb{Q}}$. Until further notice, we shall assume that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, and that

$$\mu_p \subset F \text{ if } p > 2, \ \mu_4 \subset F \text{ if } p = 2.$$

Thus, we have

$$F_\infty = F(\mu_{p^\infty}).$$

Since $\mu_{p^\infty} \subset F_\infty$, classical multiplicative Kummer theory is as follows. Let $F_\infty^\times$ be the multiplicative group of F_∞, and let F_∞^{ab} be the maximal abelian extension of F_∞. Then we have the canonical dual pairing

$$\langle\ ,\ \rangle : \mathrm{Gal}(F_\infty^{\mathrm{ab}}/F_\infty) \times (F_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p) \to \mu_{p^\infty}$$

given by (here $\alpha \in F_\infty^\times$ and $a \geq 0$)

$$\langle \sigma, \alpha \otimes (p^{-a} \bmod \mathbb{Z}_p)\rangle = \sigma\beta/\beta \text{ where } \beta^{p^a} = \alpha.$$

Of course, there is a natural action of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on all of these groups, and the pairing gives rise to an isomorphism of Γ-modules

$$\mathrm{Gal}(F_\infty^{\mathrm{ab}}/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}).$$

AS before, let M_∞ be the maximal abelian p-extension of F_∞ which is unramified outside of p. Since $M_\infty \subset F_\infty$, the Kummer pairing induces an isomorphism of Γ-modules

$$\mathrm{Gal}(M_\infty/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{M}_\infty, \mu_{p^\infty}),$$

for a subgroup $\mathcal{M}_\infty \subset F_\infty^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$, which can be described explicitly as follows. Recall that, as F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, there are only finitely many primes of F_∞ lying above each rational prime number, and that the primes which do not lie above p all have discrete valuations. Let I'_∞ be the free abelian group on the primes of F_∞ which do not lie above p. Then every $\alpha \in F_\infty^\times$ determines a unique ideal $(\alpha)' \in I'_\infty$. The following lemma is then proven.

Lemma. *$\mathcal{M}_\infty$ is the subgroup of all elements of $F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ of the form $\alpha \otimes p^{-a} \bmod \mathbb{Z}_p$ where $\alpha \in F_\infty^\times$ is such that $(\alpha)' \in I_\infty^{p^a}$.*

We can then analyze $\mathcal{M}_\infty$ by the following exact sequence. Let E'_∞ be the graph of all elements α in $F_\infty^\times$ with $(\alpha)' = 1$. We have the obvious map

$$i_\infty : E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{M}_\infty$$

given by $i_\infty(\varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p) = \varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p$, which is easily seen to be injective. Moreover, the map

$$j_\infty : \mathcal{M}_\infty \to A'_\infty$$

is defined by $j_\infty(\alpha \otimes p^{-a} \bmod \mathbb{Z}_p) = d(\mathfrak{a})$ where $(\alpha)' = \mathfrak{a}^{p^a}$. Both i_∞ and j_∞ are obviously Γ-homomorphisms.

Lemma. *The sequence of Γ-modules*

$$0 \longrightarrow E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{i_\infty} \mathcal{M}_\infty \xrightarrow{j_\infty} A'_\infty \longrightarrow 0 \tag{3}$$

is exact.

The proof of exactness is completely straightforward. In view of the exact sequence (3), we can now break up the Iwasawa module $X(F_\infty) = \mathrm{Gal}(M_\infty/F_\infty)$ into two parts. Define

$$N'_\infty = F_\infty(\sqrt[p^n]{\varepsilon} \text{ for all } \varepsilon \in E'_\infty \text{ and all } n \geq 1).$$

Then, thanks to (3), the Kummer pairing induces Γ-isomorphisms

$$\mathrm{Gal}(N'_\infty/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$$

and

$$\mathrm{Gal}(M_\infty/N'_\infty) \xrightarrow{\sim} \mathrm{Hom}(A'_\infty, \mu_{p^\infty}).$$

Let $T_p(\mu) = \varprojlim \mu_{p^n}$ be the Tate module of μ_{p^∞}. Thus, $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 on which Γ acts via the character giving the action of Γ on μ_{p^∞}l Thus, if we now define

$$Z'_\infty = \mathrm{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p),$$

we see immediately that $\mathrm{Gal}(M_\infty/N'_\infty) = Z'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu)$, endowed with the diagonal action of Γ.

Theorem A (Iwasawa)**.** *Z'_∞ is always a finitely generated torsion $\Lambda(\Gamma)$-module.*

In fact, Iwasawa proves Theorem A for an *arbitrary* $\mathbb{Z}_p$-extension F_∞/F (the definition of A'_∞ we have given must be slightly modified for an arbitrary $\mathbb{Z}_p$-extension).

Now it is easy to see that if Z'_∞ is $\Lambda(\Gamma)$-torsion, then so is $Z'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu)$. Hence, for the cyclotomic $\mathbb{Z}_p$-extension, Theorem A has the following corollary:

Corollary. $\mathrm{Gal}(M_\infty/N'_\infty)$ *is a finitely generated* $\Lambda(\Gamma)$*-module.*

In the next lecture, we will outline Iwasawa's proof of the following result:

Theorem B (Iwasawa)**.** *Let* $F_\infty = F(\mu_{p^\infty})$*, where* $\mu_p \subset F$ *if* $p > 2$ *and* $\mu_4 \subset F$ *if* $p = 2$*. Then* $\mathrm{Gal}(N'_\infty/F_\infty)$ *is a finitely generated* $\Lambda(\Gamma)$*-module of rank* $r_2 = [F : \mathbb{Q}]/2$*.*

The value of r_2 is as given because F is clearly totally imaginary. As we shall see in the next lecture, Iwasawa's proof gives very precise information about the $\Lambda(\Gamma)$-torsion submodule of $\mathrm{Gal}(N'_\infty/F_\infty)$.

Of course, Theorem A and Theorem B together imply that $\mathrm{Gal}(M_\infty/F_\infty)$ has $\Lambda(\Gamma)$-rank equal to $r_2 = [F : \mathbb{Q}]/2$, proving the weak Leopoldt conjecture in this case.

2.3. **Elementary properties of p-units in F_∞/F.** As a first step towards proving Theorem B, we establish some basic properties of the units E'_∞. Let W_n be the group of all roots of unity in F_n, and W_∞ to group of all roots of unity in F_∞. Thus, W_∞ is the product of μ_{p^∞} with a finite group of order prime to p. Define

$$\mathcal{E}'_n = E'_n/W_n, \qquad\qquad \mathcal{E}'_\infty = E'_\infty/W_\infty;$$

here E'_n denotes the group of p-units of F_n. Let s_n denote the number of primes of F_n lying above p. Then, by the generalization of the unit theorem to p-units, $\mathcal{E}'_n$ is a free abelian group of rank $r_2 p^n + s_n - 1$, where $r_2 = [F : \mathbb{Q}]/2$. Moreover, $\mathcal{E}'_\infty$ is the union of the increasing sequence of subgroups $\mathcal{E}'_n$.

Lemma. $\mathcal{E}'_\infty$ *is a free abelian group, and, for all* $n \geq 0$*,* $\mathcal{E}'_n$ *is a direct summand of* $\mathcal{E}'_\infty$*.*

Proof. Now $(E'_\infty)^{\Gamma_n} = E'_n$ for all $n \geq 0$. As $H^1(\Gamma_n, W_\infty) = (W_\infty)_{\Gamma_n} = 0$, it follows that $(\mathcal{E}'_\infty)^{\Gamma_n} = \mathcal{E}'_n$ for all $n \geq 0$. We next observe that $\mathcal{E}'_\infty/\mathcal{E}'_n$ is torsion free. Indeed, suppose u is an element of $\mathcal{E}'_\infty$ with $u^k \in E'_n$ for some integer $k \geq 1$. If γ is any element of Γ_n, we must then have $(\gamma u/u)^k = 1$, where $\gamma u = u$ since $\mathcal{E}'_\infty$ is torsion free, and so $u \in \mathcal{E}'_n$ as required. Hence, for all $m \geq n$, $\mathcal{E}'_m/\mathcal{E}'_n$ is torsion free. As $\mathcal{E}'_m$ and $\mathcal{E}'_n$ are both finitely generated torsion free abelian groups, it follows that $\mathcal{E}'_n$ must be a direct summand of $\mathcal{E}'_m$ for all $m \geq n$, and the assertions of the lemma follow. □

Lecture 3.

We now give Iwasawa's proof of Theorem B of the last lecture. Let $\mathbb{Q}'$ be the ring of all rational numbers whose denominator is a power of p. Note that $\mathbb{Q}'/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$. Hence, for all $n \geq 0$, we have the exact sequence

$$0 \longrightarrow \mathcal{E}'_n \longrightarrow \mathcal{E}'_n \otimes_{\mathbb{Z}} \mathbb{Q}' \longrightarrow \mathcal{E}'_n \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0.$$

Also, we have the exact sequence

$$0 \longrightarrow \mathcal{E}'_\infty \longrightarrow \mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}' \longrightarrow \mathcal{E}'_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0. \tag{4}$$

Recall that, for all $n \geq 0$, $\mathcal{E}'_n$ is a direct summand of $\mathcal{E}'_\infty$, and $(\mathcal{E}_\infty)^{\Gamma_n} = \mathcal{E}'_n$. It follows that

$$(\mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}')^{\Gamma_n} = \mathcal{E}'_n \otimes_{\mathbb{Z}} \mathbb{Q}'.$$

Also, for all $n \geq 0$,

$$H^1(\Gamma_n, \mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}') = \varinjlim_{m \geq n} H^1(\mathrm{Gal}(K_m/K_n), \mathcal{E}'_m \otimes_{\mathbb{Z}} \mathbb{Q}'),$$

and this last cohomology group is 0 because $\mathcal{E}'_m \otimes \mathbb{Z}\mathbb{Q}'$ is p-divisible. Hence we have

$$H^1(\Gamma)n, \mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}') = 0.$$

Thus, taking Γ_n-cohomology of the exact sequence (4), we immediately obtain:

Proposition 3.1. *For all $n \geq 0$, we have the exact sequence*

$$0 \longrightarrow \mathcal{E}'_n \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow (\mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n} \longrightarrow H^1(\Gamma_n, \mathcal{E}'_\infty) \longrightarrow 0.$$

To prove Theorem B, we also need to know that $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is a finite group. In fact, it is a torsion group, and it must be finitely generated because the Pontrjagin dual of $\mathcal{E}_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a finitely generated $\Lambda(\Gamma)$-module. However, a more intrinsic proof, which in the end yields more information about hte strucutre of $\mathrm{Gal}(N'_\infty/F_\infty)$ as a $\Lambda(\Gamma)$-module, comes from the following result. For all $n \geq 0$, let I'_n denote the multiplicative group of all fractional ideals of F_n which are prime to p, and let $P'_n = \{(\alpha)' : \alpha \in F_n^\times\}$ be the subgroup of principal ideals. Put A'_n for the p-primary subgroup of I'_n/P'_n. For all $n \geq 0$, we have the natural injection $I'_n \to I'_\infty$, and this induces a homomorphism $A'_n \to A'_\infty$.

Proposition 3.2. *For all $n \geq 0$, we have*

$$H^1(\Gamma_n, \mathcal{E}'_\infty) = \ker(A'_n \to A'_\infty).$$

In particular, $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is finite.

We remark that, in his 1973 Annals paper, Iwasawa proves that Proposition 3.2 is valid for every $\mathbb{Z}_p$-extension F_∞/F in which every prime of F aove p is ramified. Under the same hypotheses, he also shows that the order of $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is bounded as $n \to \infty$. In his Ph.D thesis at Princeton under Iwasawa, Ralph Greenberg showed the existence of many examples when $\ker(A'_n \to A'_\infty)$ is non-zero. However, in the most classical case when $F = \mathbb{Q}(\mu_p)$ with p an odd prime, and $F_\infty = \mathbb{Q}(\mu_{p^\infty})$, it is still unknown whether there exist primes p such that $\ker(A'_n \to A'_\infty)$ is non-zero.

Before proving Proposition 3.2, we first show that Theorem B is an easy consequence of Proposition 3.1. For each $n \geq 0$, let s_n denote the number of primes of F_n lying above p. Then the analogue of Dirichlet's theorem for the E'_n tells us that $\mathcal{E}'_n$ is a free abelian group of rank $r_2 p^n + s_n - 1$. Moreover, since p is totally ramified in the extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, it follows that there exists $n_0 \geq 0$ such that every prime above p is totally ramified in the extension F_∞/F_{n_0}. Hence, we conclude that $s_n = s$, where $s = s_{n_0}$ for all $n \geq n_0$. Thus, since $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is finite, it follows from Proposition 3.1 that, provided $n \geq n_0$, the maximal divisible subgroup of $(\mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}$ has $\mathbb{Z}_p$-corank $r_2 p^n + s - 1$.

Put

$$Y'_\infty = \mathrm{Hom}(\mathcal{E}'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

Then it follows immediately from Pontrjagin duality that $(Y'_\infty)_{\Gamma_n}$ has $\mathbb{Z}_p$-rank $r_2 p^n + s - 1$ for all $n \geq n_0$. Now Y'_∞ is a finitely generated $\Lambda(\Gamma)$-module because $(Y'_\infty)_\Gamma$ is a finitely generated $\mathbb{Z}_p$-module, and so it follows immediately from the structure theory (see Ex 1.2) that Y'_∞ has $\Lambda(\Gamma)$-rank equal to r_2. But Kummer theory immediately shows that

$$Y'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu) = \mathrm{Gal}(N'_\infty/F_\infty).$$

Thus Theorem B follows from the following simple algebraic exercise.

Ex 3.1. Let W be any finitely generated $\Lambda(\Gamma)$-module. Assume $\mu_{p^\infty} \subset F_\infty$ and let $V = W \otimes_{\mathbb{Z}_p} T_p(\mu)$, where Γ acts on V by the twisted action $\sigma(w \otimes \alpha) = \sigma w \otimes \sigma\alpha$, with $w \in W$ and $\alpha \in T_p(\mu)$. Prove that the $\Lambda(\Gamma)$-module V has the same $\Lambda(\Gamma)$-rank as W.

We remark that, in his 1073 Annals paper, Iwasawa shows that a further analysis of the above proof of Theorem B yields more information about the $\Lambda(\Gamma)$-module $\mathrm{Gal}(N'_\infty/F_\infty)$. Let $t(\mathrm{Gal}(N_\infty/F_\infty))$ denote the $\Lambda(\Gamma)$-torsion submodule of $\mathrm{Gal}(N'_\infty/F_\infty)$. Then Iwasawa proves the following facts:

(i) $\mathrm{Gal}(N'_\infty/F_\infty)$ contains non non-zero $\mathbb{Z}_p$-torsion,
(ii) $t(\mathrm{Gal}(N'_\infty/F_\infty))$ is a free $\mathbb{Z}_p$-module of rank $s-1$ where s = number of primes above p in the extension F_∞/F_{n_0} as above, and he determines exactly its characteristic power series (even its structure up to pseudo-isomorphism), and
(iii) $\mathrm{Gal}(N'_\infty/F_\infty)/t(\mathrm{Gal}(N'_\infty/F_\infty))$ is a free $\Lambda(\Gamma)$-module if and only if $H^1(\Gamma_n, \mathcal{E}'_\infty) = 0$ for all $n \geq a$, where a is an explicitly determined integer $\leq s-1$.

Finally, we give the proof of Proposition 3.2. For all $m \geq n$, we will prove that there is an isomorphism

$$\tau_{n,m} : \ker(A'_n \to A'_m) \xrightarrow{\sim} H^1(\mathrm{Gal}(F_m/F_n), E'_m).$$

Passing to the inductive limit over all $m \geq n$, and noting that $H^i(\Gamma_n, W_\infty) = 0$ for all $i \geq 1$, Proposition 3.2 will then follow. Fix a generator σ of $\mathrm{Gal}(F_m/F_n)$, and write $\mathcal{O}'_m$ for the ring of p-integers of F_m. If c is some element of $\ker(A'_n \to A'_m)$, and $\mathfrak{a} \in I_n$ is an ideal in c, then $\mathfrak{a}\mathcal{O}'_m = \alpha\mathcal{O}'_m$ for some $\alpha \in \mathcal{O}'_m$. Define $\varepsilon = \sigma\alpha/\alpha$. Thus ε is an element of E'_m with $\mathrm{N}_{F_m/F_n}(\varepsilon) = 1$. It is easy to see that the cohomology class $\{\varepsilon\}$ of ε in $H^1(\mathrm{Gal}(F_m/F_n), E'_m)$ depends only on c, and we define $\tau_{n,m}(c) = \{\varepsilon\}$. One checks easily that $\tau_{n,m}$ is injective. To prove surjectivity, let $\{\varepsilon\}$ be any cohomology class in $H^1(\mathrm{Gal}(F_m/F_n), E'_m)$ which is represented by an element ε of E'_m with $\mathrm{N}_{m,n}(\varepsilon) = 1$. By Hilbert's Theorem 90, we then have $\varepsilon = \alpha^{\sigma-1}$ for some $\alpha \in \mathcal{O}'_m$. Let $\mathfrak{a}$ in I'_m be given by $\mathfrak{a} = \alpha\mathcal{O}'_m$. Since ε is in E'_m, we see that $\mathfrak{a}^\sigma = \mathfrak{a}$. Moreover, no prime of F_n which does not divide p is ramified in F_m, and so it follows that $\mathfrak{a}$ must be the image of an ideal $\mathfrak{b}$ in I'_n under the natural inclusion $I'_n \hookrightarrow I'_m$. Let c be the class of $\mathfrak{b}$ in I'_n. One sees easily that c lies in $\ker(A'_n \to A'_m)$, and $\tau_{n,m} = \{\varepsilon\}$, completing the proof.

Lecture 4.

We now rapidly explain Iwasawa's proof of Theorem A. Let F_∞/F be an arbitrary $\mathbb{Z}_p$-extension. For each $n \geq 0$, let $\mathcal{O}'_n$ be the ring of p integers of F_n, I'_n the group of invertible $\mathcal{O}'_n$-ideals, $P'_n \subset I'_n$ the group of principle invertible $\mathcal{O}'_n$-ideals, and A'_n the p-primary subgroup of I'_n/P'_n. If $n \leq m$, we have the two natural homomorphisms

$$i_{n,m} : A'_n \longrightarrow A'_m, \qquad \mathrm{N}_{m,n} : A'_m \longrightarrow A'_n$$

which are respectively induced by the natural inclusion of I'_n into I'_m and the norm map from I'_m to I'_n. We then define the Γ-modules

$$A'_\infty = \varinjlim A'_n, \qquad W'_\infty = \varprojlim A'_n,$$

where the inductive limit is taken with respect to the $i_{n,m}$ and the projective limit is taken with respect to the $\mathrm{N}_{m,n}$, and both are endowed with their natural action of Γ. Thus A'_∞ is a discrete $\Lambda(\Gamma)$-module, and W'_∞ is a compact $\Lambda(\Gamma)$-module.

Proposition 4.1. *W'_∞ is canonically isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(L'_\infty/F_\infty)$ where L'_∞ denotes the maximal unramified abelian p-extension of F_∞, in which every prime F_∞ lying above p splits completely.*

Proof. Let L'_n be the maximal unramified abelian p-extension of F_n in which every prime above p splits completely. By global class field theory, the Artin map induces an isomorphism $A'_n \xrightarrow{\sim} \mathrm{Gal}(L'_n/F_n)$, which preserves the natural action of Γ/Γ_n on both abelian groups. Let $n_0 \geq 0$ be such that every prime of F_{n_0} which is ramified in F_∞ is totally ramified in F_∞. Thus, if $m \geq n \geq n_0$, we must have $L_n \cap F_m = F_n$, so that $\mathrm{Gal}(L'_n F_m/F_m) \xrightarrow{\sim} \mathrm{Gal}(L'_n/F_n)$. Moreover, global class field theory then tells us that the diagram

$$\begin{array}{ccccc} A'_m & \xrightarrow{\sim} & \mathrm{Gal}(L'_m/F_m) & & \\ {\scriptstyle \mathrm{N}_{m,n}}\downarrow & & \downarrow & & \\ A'_n & \xrightarrow{\sim} & \mathrm{Gal}(L'_n F_m/F_m) & = & \mathrm{Gal}(L'_n/F_n) \end{array}$$

is commutative. Hence, $W_\infty = \varprojlim A'_n$ is isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(R_\infty/F_\infty)$, where $R_\infty = \bigcup_{n\geq 0} L'_n$. Obviously, $R_\infty \subset L'_\infty$. But every element of L'_∞ satisfies an equation with coefficients in F_n for some $n \geq n_0$, whence we see that also $L'_\infty \subset R_\infty$, and so $L'_\infty = R_\infty$, and W_∞ is isomorphic as a $\Lambda(\Gamma)$-module to $\mathrm{Gal}(L'_\infty/F_\infty)$, as required. □

Proposition 4.2. *Let $s \geq 1$ be the number of primes of F_∞ which are ramified in the $\mathbb{Z}_p$-extension F_∞/F. Then, for all $n \geq n_0$, we have that*

$$\mathbb{Z}_p\text{-rank of } (W'_\infty)_{\Gamma_n} \leq s - 1.$$

In particular, W'_∞ is a torsion $\Lambda(\Gamma)$-module.

Proof. For each $n \geq 0$, let $\mathcal{L}'_n$ denote the maximal abelian extension of F_n contained in L'_∞. Obviously, $\mathcal{L}'_n \supset F_\infty$, and by the definition of the Γ-action on $W'_\infty = \mathrm{Gal}(L'_\infty/F_\infty)$, we have

$$(W'_\infty)_{\Gamma_n} = \mathrm{Gal}(\mathcal{L}'_n/F_\infty). \tag{5}$$

Assume now that $n \geq n_0$, so that there are precisely s primes of F_n which are ramified in the extension $\mathcal{L}'_n/F_n$. Denote these primes by w_i $(i = 1, \ldots, s)$, and let T_i be the inertia group of w_i in $\mathcal{L}'_n/F_n$. Since w_i is completely ramified in F_∞/F_n, and then splits completely in $\mathcal{L}'_n/F_\infty$, we must have $T_i \xrightarrow{\sim} \Gamma_n \xrightarrow{\sim} \mathbb{Z}_p$ for $i = 1, \ldots, s$. Now, L'_n is the maximal unramified extension of F_n contained in $\mathcal{L}'_n$. Hence

$$\mathrm{Gal}(\mathcal{L}'_n/L'_n) = T_1 \cdots T_s.$$

Since $\mathrm{Gal}(L'_n/F_n)$ is finite, we conclude that the module $\mathrm{Gal}(\mathcal{L}'_n/F_n)$ has $\mathbb{Z}_p$-rank at most s. As $\mathrm{Gal}(F_\infty/F_n)$ has $\mathbb{Z}_p$-rank equal to 1, it follows that

$$\mathbb{Z}_p\text{-rank of } \mathrm{Gal}(\mathcal{L}'_n/F_\infty) \leq s - 1 \text{ for all } n \geq n_0.$$

In view of (5), it now follows from the structure theory that W'_∞ is a torsion $\Lambda(\Gamma)$-module, as claimed. □

We end these notes by explaining, without proofs, the precise relationship between W'_∞ and $\mathrm{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ as $\Lambda(\Gamma)$-modules, which shows, in particular, that $\mathrm{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is also a

torsion $\Lambda(\Gamma)$-module. Let X be any finitely generated torsion $\Lambda(\Gamma)$-module. We define the $\Lambda(\Gamma)$-module $\alpha(X)$, called the adjoint of X by

$$\alpha(X) = \mathrm{Ext}^1_{\Lambda(\Gamma)}\big(X, \Lambda(\Gamma)\big).$$

It turns out that $\alpha(X)$ is pseudo-isomorphic to X, and contains no non-zero finite $\Lambda(\Gamma)$-submodule.

Theorem 4.3. $\mathrm{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = \alpha(\mathrm{Gal}(L'_\infty/F_\infty L'_{n_0}))$. *Hence* $\mathrm{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ *is pseudo-isomorphic to* $W'_\infty = \mathrm{Gal}(L'_\infty/F_\infty)$*, and so is* $\Lambda(\Gamma)$*-torsion.*

Project.

Let K be an imaginary quadratic field, and p a rational prime which splits in K into two distinct primes $\mathfrak{p}, \mathfrak{p}^*$. By class field theory, there is a unique $\mathbb{Z}_p$-extension K_∞/K which is unramified outside of $\mathfrak{p}$. Assume now that F is an arbitrary finite extension of K. We call

$$F_\infty = FK_\infty$$

the "split prime" $\mathbb{Z}_p$-extension of F. It seems probable that this split prime $\mathbb{Z}_p$-extension F_∞/F has many properties in close analogy with those of the cyclotomic $\mathbb{Z}_p$-extension of F. The aim of the project is to discuss several of these analogies, and establish a few rather limited theoretical and numerical examples in support of them.

Part I

Analogues of the Leopoldt and weak Leopoldt conjectures.

We assume from now on that K is an imaginary quadratic in which p splits into $\mathfrak{p}, \mathfrak{p}^*$, and that F is an arbitrary finite extension of K. For each prime v of F lying above $\mathfrak{p}$, write U_v for the group of local units in the completion of F at v which are $\equiv 1 \bmod v$. Put $U_F = \prod U_v$. Thus U_F is a $\mathbb{Z}_p$-module of rank equal to $r_2^{v|\mathfrak{p}}$, where r_2 denotes the number of complex primes of F $\left(= [F:K]\right)$. Let E_F be the group of all global units of F which are $\equiv 1 \bmod v$ for all $v|\mathfrak{p}$. By Dirichlet's theorem, E_F has $\mathbb{Z}$-rank equal to $r_2 - 1$. Now we have the obvious embedding of E_F into U_F, and we define $\overline{E}_F$ to be the closure of the image in U_F under the $\mathfrak{p}$-adic topology (equivalently, $\overline{E}_F$ is the $\mathbb{Z}_p$-submodule of U_F

58

which is generated by the image of E_F). Thus $\overline{E}_F$ must have $\mathbb{Z}_p$-rank equal to $r_2 - 1 - \delta_{F,p}$ for some integer $\delta_{F,p} \geq 0$.

<u>p-adic Leopoldt conjecture</u>. $\delta_{F,p} = 0$.

Again global class field theory gives a Galois-theoretic interpretation of this conjecture. Let L be the p-Hilbert class field of F, and let M be the maximal abelian p-extension of F, which is unramified outside the set of primes of F lying above p. Then the Artin map induces an isomorphism

$$U_F / \overline{E}_F \xrightarrow{\sim} \mathrm{Gal}(M/L),$$

whence we obtain:—

<u>Theorem</u> 1.1. Let M be the maximal abelian p-extension of F which is unramified outside the primes of F lying above p. Then $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $1 + \delta_{F,p}$.

<u>Corollary 1.2</u>. $\delta_{F,p} = 0$ if and only if $\mathrm{Gal}(M/F_\infty)$ is finite.

Let $\sigma_1, \dots, \sigma_{r_2}$ be the embeddings of F into $\overline{\mathbb{Q}}_p$ extending the embedding of K into $\mathbb{Q}_p$ given by p. Let $\varepsilon_1, \dots, \varepsilon_{r_2-1}$ be a $\mathbb{Z}$-basis of E_F modulo torsion. Note that the series $\log x$ converges on all principal units of $\overline{\mathbb{Q}}_p$. Define

$$R_p(F) = \det\left(\log \sigma_i(\varepsilon_j)\right)_{i,j=1,\dots,r_2-1}.$$

<u>Exc</u> 1.1. Prove that $\delta_{F,p} \neq 0$ if and only if $R_p(F) \neq 0$. If F is an abelian extension of K, use Baker's theorem that $\log \varepsilon_1, \dots, \log \varepsilon_{r_2-1}$ are linearly independent over the field of algebraic numbers to show that $R_p(F) \neq 0$.

Exa 1.2. With the help of SAGE or MAGMA, one can often check numerically that $R_{\mathfrak{p}}(F) \neq 0$ even when F is not an abelian extension of K. Here is one example. Take $K = \mathbb{Q}(i)$, $p = 5$, and $\mathfrak{p} = (1-2i)\mathbb{Z}[i]$. Let $w = \frac{1-\sqrt{5}}{2}$, and take

$$F = K\left(w, \beta^{1/4}\right), \text{ where } \beta = w(1-2i)^3.$$

Show that $F = \mathbb{Q}(\delta)$, where δ is a root of $x^8+4x^6+9x^4+10x^2+5=0$. Using one of the above programmes, find the group of global units of F, and check that $\mathrm{ord}_{\mathfrak{p}}\left(R_{\mathfrak{p}}(F)\right) = 3/2$.

We now turn to the weak $\mathfrak{p}$-adic Leopoldt conjecture for F_∞/F. For each $n \geq 0$, let F_n be the unique extension of F contained in F_∞ with $[F_n : F] = p^n$. Let $\delta_{F_n,\mathfrak{p}}$ denote the $\mathfrak{p}$-adic default of Leopoldt for F_n.

Weak $\mathfrak{p}$-adic Leopoldt conjecture for F_∞/F.

$\delta_{F_n,\mathfrak{p}}$ is bounded as $n \to \infty$.

Of course, the analogue of this statement for the cyclotomic $\mathbb{Z}_p$-extension of F was proven by Iwasawa, but unfortunately his proof does not seem to extend to F_∞/F.

There is an equivalent formulation of this conjecture purely in terms of an Iwasawa module. Let $M(F_\infty)$ be the maximal abelian p-extension of F_∞, which is unramified outside the set of primes of F_∞ lying above $\mathfrak{p}$, and put

$$X(F_\infty) = \mathrm{Gal}\left(M(F_\infty)/F_\infty\right).$$

Clearly $M(F_\infty)$ is Galois over F, and so $\Gamma = \mathrm{Gal}(F_\infty/F)$ acts on $X(F_\infty)$ in the usual fashion. It follows that $X(F_\infty)$ is a module over the Iwasawa algebra $\Lambda(\Gamma)$ of Γ, and it is easily seen to be finitely generated over $\Lambda(\Gamma)$. Moreover, we have

$$\left(X(F_\infty)\right)_{\Gamma_n} = \mathrm{Gal}\left(M_n/F_\infty\right),$$

where M_n is the maximal abelian p-extension of F_n, which is unramified outside the primes of F_n lying above p.

Theorem 1.3. $X(F_\infty)$ is $\Lambda(\Gamma)$-torsion if and only if $\delta_{F_n,p}$ is bounded as $n \to \infty$.

Corollary 1.4 If $\delta_{F,p} = 0$, then $\delta_{F_n,p}$ is bounded as $n \to \infty$.

Of course, one can use Corollary 1.4 to prove the weak p-adic Leopoldt conjecture in numerical examples (e.g. in the example of Exc 1.2).

There are two other important aspects of the weak p-adic Leopoldt conjecture for F_∞/F which we mention briefly. Firstly, there is an exact formula for $\#(\mathrm{Gal}(M/F_\infty))$ when $R_p(F) \neq 0$, which is a first hint that there may be a "main conjecture" for $X(F_\infty)$. Let $h(F)$ be the class number of F, $w(F)$ the number of roots of unity in F, and $\Delta(F/K)$ any generator of the discriminant ideal of F/K. If v is a finite place of F, Nv will denote the cardinality of the residue field of v.

Exc 1.3 (see [CW1]). Assume that $R_p(F) \neq 0$. Then

$$[M : F_\infty] = \left| \frac{p^{e(F)+1} h(F) R_p(F)}{w(F) \sqrt{\Delta(F/K)}} \prod_{v \mid p} \left(1 - \frac{1}{Nv}\right) \right|_p^{-1},$$

where the integer $e(F)$ is defined by $F \cap K_\infty = K_{e(F)}$. Here the p-adic valuation on $\overline{\mathbb{Q}}_p$ is normalized by $\left|\frac{1}{p}\right|_p = p$.

Secondly, the weak Leopoldt conjecture for F_∞/F is closely related to the Iwasawa theory for F_∞/F of elliptic curves with complex multiplication by the full ring of integers of K (see [C2]).

Exc 1.4. In the specific numerical example discussed in Example 1.2, use the formula of Example 1.3 to prove that $X(F_\infty) = 0$.

Part II

Analogue of Iwasawa's $\mu = 0$ conjecture.

We first recall Iwasawa's $\mu = 0$ conjecture. Let F be any finite extension of $\mathbb{Q}$, p any prime number, and F_∞^{cyc}/F the cyclotomic $\mathbb{Z}_p$-extension of F.

Iwasawa's $\mu = 0$ conjecture. Let L_∞ be the maximal abelian p-extension of F_∞^{cyc}, which is unramified everywhere. Then $Gal(L_\infty/F_\infty^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module. Iwasawa (see [IW2]) has given examples of fields F and primes p for which the analogue of this conjecture is false for certain non-cyclotomic $\mathbb{Z}_p$-extensions of F. The best result to date in support of Iwasawa's conjecture is the following:—

Theorem (Ferrero-Washington, Sinnott). Iwasawa's $\mu = 0$ conjecture is valid for all finite abelian extensions F of $\mathbb{Q}$, and all primes p.

Now assume F is a finite extension of an imaginary quadratic field K, and F_∞/F is the split prime $\mathbb{Z}_p$-extension of K. Let $\mathfrak{p}_0$ be the degree 1 prime of K giving rise to F_∞/F.

Split prime analogue of Iwasawa's $\mu = 0$ conjecture.

Let F_∞/F be the split prime $\mathbb{Z}_p$-extension, and let $M(F_\infty)$ be the maximal abelian p-extension of F_∞ which is unramified outside the primes of F_∞ lying above $\mathfrak{p}_0$. Then $X(F_\infty) = Gal(M(F_\infty)/F_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.

Exc 1.5. Let J/F be a finite Galois extension, whose Galois group is cyclic of order p. Let J_∞/J and F_∞/F be the split prime $\mathbb{Z}_p$-extensions, so that $J_\infty = F_\infty J$. If $X(F_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, prove that $X(J_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.

There is a considerable body of literature showing how Sinnott's beautiful proof, by analytic means, of the Iwasawa $\mu = 0$ for conjecture for the cyclotomic $\mathbb{Z}_p$-extension of a finite abelian extension F of $\mathbb{Q}$ can be generalized to the split prime $\mathbb{Z}_p$-extension $\mu = 0$ conjecture given above for F a finite abelian extension of K. However, it must be said that the analytic arguments needed in the split prime case are not fully worked out in the existing literature, especially for the primes $p = 2, 3$. There would be real interest in writing a fully detailed and comprehensible proof showing that Sinnott's method proves in complete generality the above $\mu = 0$ conjecture for the split prime $\mathbb{Z}_p$-extension of any finite abelian extension F of K.

CONSTRUCTION OF EULER SYSTEMS

DAVID LOEFFLER AND SARAH LIVIA ZERBES

1. COURSE OUTLINE

There are a number of conjectures – some proved, some wide open – relating the special values of L-functions to the properties of arithmetic objects; for instance, the main conjecture of Iwasawa theory (which concerns class groups of number fields) and the Birch–Swinnerton-Dyer conjecture (describing points on elliptic curves). One attempt at a unified formulation is the Bloch–Kato conjecture, which relates values of L-functions to the cohomology of global Galois representations.

One of the most important tools that has been used to make progress on these conjectures is the idea of an *Euler system*. These are certain families of Galois cohomology classes, satisfying precise compatibilities ("norm relations"), which can be used to control the sizes of Galois cohomology groups. Unsurprisingly, these objects are rather difficult to construct, and the list of known examples is still relatively short. All of the known constructions rely, in some way, on exploiting the properties of modular and automorphic forms.

The goal of this lecture course will be to explain how some of the known Euler systems are constructed, focussing on three main examples: the Euler system of Kato, associated to a modular form; the Euler system of Beilinson–Flach elements, associated to a pair of modular forms (and its generalisation to Hilbert modular forms); and the Euler system of Lemma–Flach elements, associated to a genus 2 Siegel modular form. All of these are ultimately built up from certain special rational functions on modular curves called *Siegel units*.

Another topic which we will also aim to cover (although in rather less detail) is the relation between Euler systems and the values of L-functions, via p-adic regulator formulae. This is a much more advanced topic, and one where the known results are quite fragmentary; the principal tools involved come from p-adic Hodge theory and arithmetic geometry, notably Besser's rigid syntomic cohomology.

2. POSSIBLE PROJECTS

2.1. **An Euler system for $GSp(4) \times GL(2)$.** The goal of this project would be to construct an Euler system for the Galois representations appearing in the cohomology of a certain 4-dimensional Shimura variety: namely, the product of a Siegel modular threefold and a modular curve. Recent work of Francesco Lemma [Lem17] shows that there is a supply of interesting cohomology classes available for this variety, so the aim is to show that these can be assembled into an Euler system. This would be closely analogous to the construction of an Euler system for $GSp(4)$ alone, carried out recently by us together with Chris Skinner.

This project has several sub-projects, which are to some extent orthogonal (so it would be suitable for a fairly large team):

- determining which weights (i.e. coefficient systems for cohomology) are accessible;
- writing down the relevant cohomology classes, following Lemma;
- proving norm-compatibility statements in the "vertical" aspect (i.e. for classes over cyclotomic fields $\mathbf{Q}(\mu_m)$ where m is a power of p)
- proving the "horizontal" norm relation (in which we take m to be a prime not dividing the level) – this is a rather more difficult problem, since extra Euler factors make an appearance.

2.2. **Euler systems and Selmer groups in Coleman families.** Modular forms can often be deformed in p-adic families (Hida families of ordinary forms, or the more general finite-slope families constructed by Coleman [Col97]). One knows that the Euler system of Kato, and the Euler system of Beilinson–Flach elements, can be interpolated in Coleman families (see [Wan12, Han15] for the former, and [LZ16] for the latter). This raises (at least) two natural questions.

- In the Beilinson–Flach setting, can one define a Selmer group attached to the family, and use the Euler system to give upper bounds on its size? There is a general approach to defining Selmer groups in families, due to Pottharst [Pot13], and it would be interesting to try to formulate and prove a bound for Pottharst's Selmer groups in this setting.
- Are there analogous interpolation results for other Euler systems, e.g. in the Hilbert or Siegel settings? The existence of p-adic families of finite-slope automorphic forms in these cases is known, by recent works of Andreatta et al; but whether the Euler systems interpolate in these families is an open question.

3. Suggested reading

Bellaïche's notes [Bel09] are an excellent introduction to Galois representations, their cohomology, and the statement of the Bloch–Kato conjecture. For the algebraic side of the theory of Euler systems, Rubin's book [Rub00] is the canonical reference, while some may prefer the alternative account found in [MR04]; however, both of these works concentrate heavily on the algebraic side of the theory – how Euler systems can be used to bound Selmer groups – rather than saying much about how Euler systems are actually constructed, which is the emphasis of this course.

Kato's Euler system is described in detail in [Kat04]. In particular, §2 of this book is an excellent source for the definition and properties of Siegel units. There is also an alternative viewpoint on Kato's construction to be found in Colmez's Bourbaki seminar [Col04]. For the newer constructions – Beilinson–Flach elements for $GL(2) \times GL(2)$, and Lemma–Flach elements for $GSp(4)$ – see [LLZ14] and [LSZ] respectively.

The relations between Euler systems and special values of (complex and p-adic) L-functions are surveyed in [BCD$^+$14][1].

[1]Note that this survey takes a different, and much broader, interpretation of the term "Euler system", so many of the examples considered are not Euler systems in the sense we consider here.

REFERENCES

[Bel09] Joël Bellaïche, *An introduction to Bloch and Kato's conjecture*, lectures at the Clay Mathematical Institute Summer School, Honolulu, Hawaii, 2009.

[BCD+14] Massimo Bertolini, Francesc Castella, Henri Darmon, Samit Dasgupta, Kartik Prasanna, and Victor Rotger, *p-adic L-functions and Euler systems: a tale in two trilogies*, Automorphic forms and Galois representations. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 414, Cambridge Univ. Press, 2014, pp. 52–101. MR 3444223.

[Col97] Robert Coleman, *p-adic Banach spaces and families of modular forms*, Invent. Math. **127** (1997), no. 3, 417–479. MR 1431135.

[Col04] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294** (2004), 251–319, Séminaire Bourbaki, Vol. 2002/03, Exp. No. 919. MR 2111647.

[Han15] David Hansen, *Iwasawa theory of overconvergent modular forms*, preprint, 2015.

[Kat04] Kazuya Kato, *P-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III. MR 2104361.

[LLZ14] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for Rankin–Selberg convolutions of modular forms*, Ann. of Math. (2) **180** (2014), no. 2, 653–771. MR 3224721.

[Lem17] Francesco Lemma, *Algebraic cycles and residues of degree eight L-functions of* $\mathrm{GSp}(4) \times \mathrm{GL}(2)$, preprint, 2017.

[LSZ] David Loeffler, Christopher Skinner, and Sarah Livia Zerbes, *Euler systems for* $\mathrm{GSp}(4)$, preprint, `arXiv:1706.00201`.

[LZ16] David Loeffler and Sarah Livia Zerbes, *Rankin–Eisenstein classes in Coleman families*, Res. Math. Sci. **3** (2016), no. 29, special collection in honour of Robert F. Coleman.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR 2031496.

[Pot13] Jonathan Pottharst, *Analytic families of finite-slope Selmer groups*, Algebra & Number Theory **7** (2013), no. 7, 1571–1612. MR 3117501.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton Univ. Press, 2000. MR 1749177.

[Wan12] Shanwen Wang, *Le systéme d'Euler de Kato en famille (I)*, preprint, 2012, `arXiv:1211.4256`.

Euler systems (Arizona Winter School 2018 notes)

David Loeffler and Sarah Livia Zerbes

Introduction

The theory of Euler systems is one of the most powerful tools available for studying the arithmetic of global Galois representations. However, constructing Euler systems is a difficult problem, and the list of known constructions was until recently accordingly rather short. In these lecture notes, we outline a general strategy for constructing new Euler systems in the cohomology of Shimura varieties: these Euler systems arise via pushforward of certain units on subvarieties.

We study in detail two special cases of this construction: the Euler system of Beilinson–Flach elements, where the underlying Shimura variety is the fibre product of two modular curves; and the Euler system of Lemma–Flach elements, arising in the cohomology of Siegel modular threefolds.

The lecture notes are structured as follows.

- In Chapter 1, we will review the definition of Euler systems for Galois representations, and their arithmetic application to the Bloch–Kato conjecture.
- In Chapter 2, we introduce some general tools for constructing global cohomology classes for Galois representations arising in geometry, assuming the existence of a supply of subvarieties of appropriate codimension and units on them. We also introduce Siegel units, which are the key for all the Euler system constructions to follow.
- Chapter 3 is largely motivational (and can be skipped at a first reading): it explains how one can use Rankin–Selberg-type integral formulas for L-functions as a guide to where to look for Euler systems.
- Chapter 4 is devoted to the construction of the Beilinson–Flach Euler system for pairs of modular forms of weight 2; and in Chapter 5, we discuss how to adapt this construction to pairs of modular forms of higher weight, using cohomology with coefficients.
- In Chapter 6 we explain the construction of the Lemma–Flach Euler system for genus 2 Siegel modular forms of parallel weight 3.
- In the concluding Chapter 7 we outline some projects.

Updated 13/2/2018, incorporating corrections from Chi-Yun Hsu.

Contents

CHAPTER 1

Galois representations and Galois cohomology

References: for §§1.1—1.3, an excellent source is Bellaiche's CMI notes on the Bloch–Kato conjecture.

1.1. Galois representations

1.1a. Definitions. Let K be a number field, $\overline{K}$ its algebraic closure, $G_K = \mathrm{Gal}(\overline{K}/K)$; and let p be a prime, and E a finite extension of $\mathbf{Q}_p$. We're interested in representations of G_K on finite-dimensional E-vector spaces V.

We always assume that

(1) $\rho : G_K \to \mathrm{Aut}(V) \cong \mathrm{GL}_d(E)$ is continuous (where $d = \dim(V)$), with respect to profinite topology of G_K and the p-adic topology on $\mathrm{GL}_d(E)$.
(2) V is "unramified almost everywhere": for all but finitely many prime ideals v of K, we have $\rho(I_v) = \{1\}$, where I_v is an[1] inertia group at v.

1.1b. Examples.

The representation $\mathbf{Z}_p(1)$. Let $\mu_{p^n} = \{x \in \overline{K}^\times : x^{p^n} = 1\}$. Then μ_{p^n} is finite cyclic of order p^n and G_K acts on it.

The p-power map sends $\mu_{p^{n+1}} \to \mu_{p^n}$ and we define

$$\mathbf{Z}_p(1) \coloneqq \varprojlim_n \mu_{p^n}, \quad \mathbf{Q}_p(1) \coloneqq \mathbf{Z}_p(1) \otimes \mathbf{Q}_p.$$

This is a 1-dimensional continuous $\mathbf{Q}_p$-linear representation, unramified outside the primes dividing p; G_K acts by "cyclotomic character" $\chi_{\mathrm{cyc}} : G_K \to \mathbf{Z}_p^\times$.

(Notation: for any V, $n \in \mathbf{Z}$, we set $V(n) = V \otimes \mathbf{Q}_p(1)^{\otimes n}$.)

Tate modules of elliptic curves. A/K elliptic curve $\Rightarrow$ $A(\overline{K})$ abelian group with G_K-action. Let $A(\overline{K})[p^n]$ subgroup of p^n-torsion points.

Define

$$T_p(A) \coloneqq \varprojlim_n A(\overline{K})[p^n] \text{ (w.r.t. multiplication-by-}p\text{ maps)}, \qquad V_p(A) \coloneqq T_p(A) \otimes \mathbf{Q}_p.$$

This is a 2-dimensional continuous G_K-representation, unramified outside the set $\{v : v \mid p\} \cup \{v : A \text{ has bad reduction at } v\}$. (The same works for abelian varieties of any dimension g, giving $2g$-dimensional representations of G_K.)

[1] I_v depends on a choice of prime of $\overline{K}$ above v, but only up to conjugation in G_K, so whether or not V is unramified at v is well-defined.

Etale cohomology. Let X/K be a smooth algebraic variety. We can define vector spaces

$$H^i_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p) \quad \text{for } 0 \le i \le 2\dim X,$$

which are finite-dimensional p-adic Galois representations, unramified outside p and primes of bad reduction[2] of X.

1.1c. Representations coming from geometry. Our second example is a special case of the third: for an elliptic curve A, it turns out that we have $V_p(A) \cong H^1_{\text{ét}}(A_{\overline{K}}, \mathbf{Q}_p)(1)$.

DEFINITION. *We say an E-linear Galois rep V* comes from geometry *if it is a subquotient of $H^i_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)(j) \otimes_{\mathbf{Q}_p} E$, for some variety X/K and some integers i, j.*

So all my examples come from geometry. In these lectures we're only ever going to be interested in representations coming from geometry.

REMARK. Conjecturally the representations coming from geometry should be exactly those which are continuous, unramified almost everywhere, and *potentially semistable* at the primes above p (a technical condition from p-adic Hodge theory). This is called the **Fontaine–Mazur conjecture**. ◇

1.2. L-functions of Galois representations

1.2a. Local Euler factors. Let V as above, v unramified prime. Then $\rho(\text{Frob}_v)$ is well-defined up to conjugacy, where Frob_v is the arithmetic Frobenius.

DEFINITION. *The* local Euler factor *of V at v is the polynomial*

$$P_v(V,t) \coloneqq \det(1 - t \cdot \rho(\text{Frob}_v^{-1})) \in E[t].$$

Examples:

V	$P_v(V,t)$	
$\mathbf{Q}_p$	$1-t$	
$\mathbf{Q}_p(n)$	$1 - \frac{t}{q_v^n}$,	$q_v = \#\mathbf{F}_v$
$H^1(A_{\overline{K}}, \mathbf{Q}_p)$	$1 - a_v(A)t + q_v t^2$,	$a_v(A) \coloneqq 1 + q_v - \#A(\mathbf{F}_v)$

1.2b. Global L-functions (sketch). Assume V comes from geometry, and V is semisimple (direct sum of irreducibles). Then $P_v(V,t)$ has coefficients in $\overline{\mathbf{Q}}$ (Deligne); and there is a way of defining $P_v(V,t)$ for bad primes v (case $v \mid p$ is hardest).

Fix an embedding $\iota : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. Then we consider the product

$$L(V,s) \coloneqq \prod_{v \text{ prime}} P_v(V, q_v^{-s})^{-1}.$$

Miraculously, this converges for $\Re(s) \gg 0$.

[2]This is a little delicate to define properly if we don't assume X to be proper over K. Formally, we say X has "good reduction" at v if it's isomorphic to the complement of a relative normal crossing divisor in a smooth proper $O_{K,v}$-scheme.

E.g. for $V = \mathbf{Q}_p(n)$ this is $\zeta_K(s+n)$, where ζ_K is the Dedekind zeta function of K (which is just the Riemann zeta for $K = \mathbf{Q}$). For $V = H^1(A_{\overline{K}}, \mathbf{Q}_p)$, A an elliptic curve, it is the Hasse–Weil L-function $L(A/K, s)$.

CONJECTURE 1. *For V semisimple and coming from geometry, $L(V, s)$ has meromorphic continuation to $s \in \mathbf{C}$ with finitely many poles, and satisfies a functional equation relating $L(V, s)$ and $L(V^*, 1-s)$.*

Note that if V is semisimple and comes from geometry, the same is true[3] of V^*, so the conjecture is well-posed. This conjecture is of course super-super-hard – the only cases where it is known is where we can relate V to something *automorphic*, e.g. a modular form.

There are lots of conjectures (and a rather smaller set of theorems) relating properties of arithmetic objects to values of their L-functions; the Birch–Swinnerton-Dyer conjecture is perhaps the best-known of these. As we've just seen, all the information about an elliptic curve you need to define its L-function is encoded in the Galois action on its Tate module; so can we express the BSD conjecture purely in terms of Galois representations? This will be the topic of the next section.[4]

1.3. Galois cohomology

1.3a. Setup. There is a cohomology theory for Galois representations[5]: for V an E-linear G_K-rep, we get E-vector spaces $H^i(K, V)$, zero unless $i = 0, 1, 2$. Mostly we care about H^0 and H^1, which are given as follows

$$H^0(K, V) = V^{G_K}$$

$$H^1(K, V) = \frac{\{\text{cts fcns } s : G_K \to V \text{ such that } s(gh) = s(g) + gs(h)\}}{\{\text{fcns of the form } s(g) = gv - v \text{ for some } v \in V\}}.$$

These are well-behaved: short exact sequences of V's give long exact sequences of cohomology, for instance. Unfortunately they're *not* finite-dimensional in general.

1.3b. The Kummer map. For $V = \mathbf{Q}_p(1)$ the Galois cohomology is related to the multiplicative group K^*. To see this, we have to first think a bit about cohomology with *finite* coefficients.

For any n, we have a short exact sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow \overline{K}^\times \xrightarrow{[p^n]} \overline{K}^\times \longrightarrow 0$$

which leads to a long exact sequence

$$0 \longrightarrow \mu_{p^n}^{G_K} \longrightarrow K^\times \xrightarrow{[p^n]} K^\times \longrightarrow H^1(K, \mu_{p^n})$$

[3] It is not obvious if this holds without the semisimplicity assumption.

[4] Actually the answer is "no, we can't" – as far as I'm aware, there is no purely Galois-representation-theoretic statement that is precisely equivalent to BSD. But we can get pretty close, as we'll shortly see.

[5] Technical point: our representations are all continuous, so we shall work with cohomology defined by continuous cochains, which is slightly different from the cohomology of G_K as an abstract group.

and thus an injection[6]

$$K^\times \otimes \mathbf{Z}/p^n\mathbf{Z} \hookrightarrow H^1(K, \mu_{p^n}).$$

Passing to the inverse limit we get a map (**Kummer map**)

$$\kappa_p : K^\times \otimes \mathbf{Z}_p \hookrightarrow H^1(K, \mathbf{Z}_p(1)) \quad \text{or} \quad K^\times \otimes \mathbf{Q}_p \hookrightarrow H^1(K, \mathbf{Q}_p(1)).$$

REMARK. This already shows that $H^1(K, \mathbf{Q}_p(1))$ can't be finite-dimensional, because $K^\times$ has countably infinite rank. ◇

The same argument works for elliptic curves: we get an embedding

$$E(K) \otimes \mathbf{Q}_p \hookrightarrow H^1(K, V_p(E)).$$

1.3c. Selmer groups. Since the groups $H^1(K, V)$ can be infinite-dimensional, it's useful to "cut down to size" by imposing extra conditions on our H^1 elements. We'll do this by localising at primes of K. Note that we have maps

$$H^i(K, V) \to H^i(K_v, V) \text{ for all primes } v,$$

and the local groups $H^i(K_v, V)$ are finite-dimensional.

DEFINITION. *A* local condition *on V at prime v is an E-linear subspace $\mathcal{F}_v \subseteq H^1(K_v, V)$.*

Examples:

- *strict* local condition $\mathcal{F}_{v,\text{strict}} = \{0\}$
- *relaxed* local condition $\mathcal{F}_{v,\text{relaxed}} =$ everything
- *unramified* local condition
$$\mathcal{F}_{v,\text{ur}} = \text{image}\left(H^1(G_{K_v}/I_v, V^{I_v}) \to H^1(K_v, V)\right)$$
- *Bloch–Kato "finite"* local condition $\mathcal{F}_{v,\text{BK}}$ (for $v \mid p$) – defined using p-adic Hodge theory.

DEFINITION. *A* Selmer structure *is a collection $\mathcal{F} = (\mathcal{F}_v)_{v \text{ prime of } K}$, satisfying the following condition: for almost all v we have $\mathcal{F}_v = \mathcal{F}_{v,\text{ur}}$. If $\mathcal{F}$ is a Selmer structure we define the corresponding Selmer group by*

$$\text{Sel}_{\mathcal{F}}(K, V) = \{x \in H^1(K, V) : \text{loc}_v(x) \in \mathcal{F}_v \ \forall v\}.$$

THEOREM 1 (Tate). *For any Selmer structure $\mathcal{F}$, the space $\text{Sel}_{\mathcal{F}}(K, V)$ is finite-dimensional over $\mathbf{Q}_p$.*

SKETCH OF PROOF. It's easy to see that if this statement is true for one $\mathcal{F}$, it's true for any $\mathcal{F}$, since the *local* Galois cohomology groups $H^1(K_v, V)$ are all finite-dimensional. We now choose a particular Selmer structure $\mathcal{F}$ (exercise: which?) such that $\text{Sel}_{\mathcal{F}}(K, V)$ is the image of the map

$$H^1\left(\text{Gal}(K^\Sigma/K), V\right) \hookrightarrow H^1(K, V),$$

where K^Σ is the maximal extension of K unramified outside some finite set of places Σ containing all infinite places, all places above p, and all places where V is ramified. This reduces us to what Tate actually proved, which is that the cohomology groups of $\text{Gal}\left(K^\Sigma/K\right)$ are finite-dimensional. □

[6] In fact this is an isomorphism, because $H^1(K, \overline{K}^\times)$ is zero ("Hilbert's theorem 90")

We're mostly interested in three specific choices of Selmer structure, differing only in the choices of the $\mathcal{F}_v$ at primes $v \mid p$: we define the *strict Selmer group* $\mathrm{Sel}_{\mathrm{strict}}(K,V)$ by taking $\mathcal{F}_v = \mathcal{F}_{v,\mathrm{ur}}$ for $v \nmid p$, and $\mathcal{F}_v = \mathcal{F}_{v,\mathrm{strict}}$ for $v \mid p$; and similarly the *relaxed Selmer group* and *Bloch–Kato Selmer group*.

Hence the strict, relaxed, and Bloch–Kato Selmer groups satisfy

$$\mathrm{Sel}_{\mathrm{strict}}(K,V) \subseteq \mathrm{Sel}_{\mathrm{BK}}(K,V) \subseteq \mathrm{Sel}_{\mathrm{relaxed}}(K,V).$$

REMARK. As will soon become clear, it is $\mathrm{Sel}_{\mathrm{BK}}(K,V)$ which is the most important of all. We care about $\mathrm{Sel}_{\mathrm{strict}}(K,V)$ and $\mathrm{Sel}_{\mathrm{relaxed}}(K,V)$ because they are easier to study, and will give us a stepping-stone towards $\mathrm{Sel}_{\mathrm{BK}}(K,V)$. ◇

EXAMPLE. Recall that for $V = \mathbf{Q}_p(1)$ we had the Kummer map

$$K^\times \otimes \mathbf{Q}_p \hookrightarrow H^1(K, \mathbf{Q}_p(1)).$$

One can check that this induces isomorphisms

$$\mathcal{O}_K[1/p]^\times \otimes \mathbf{Q}_p \xrightarrow{\cong} \mathrm{Sel}_{\mathrm{relaxed}}(K, \mathbf{Q}_p(1)),$$
$$\mathcal{O}_K^\times \otimes \mathbf{Q}_p \xrightarrow{\cong} \mathrm{Sel}_{\mathrm{BK}}(K, \mathbf{Q}_p(1)).$$

The strict Selmer group, on the other hand, should be zero; this is exactly Leopoldt's conjecture for K. ◇

1.3d. The Bloch–Kato conjecture. Let V be a representation coming from geometry.

CONJECTURE 2 (Bloch–Kato). *We have*

$$\dim \mathrm{Sel}_{\mathrm{BK}}(K,V) - \dim H^0(K,V) = \mathrm{ord}_{s=0} L(V^*(1), s).$$

There are refined versions using $\mathbf{Z}_p$-modules in place of $\mathbf{Q}_p$-vector spaces, which predict the leading term of the L-function up to a unit; but we won't go into these here.

Let's look at what the conjecture says in some example cases.

Example 1: $V = \mathbf{Q}_p$. Here $L(V^*(1), s) = L(\mathbf{Q}_p, s+1) = \zeta_K(s+1)$, so the right-hand side is the order of vanishing of $\zeta_K(s)$ at $s = 1$, which is -1 for every K (there's a simple pole). The left-hand side is $\dim \mathrm{Sel}_{\mathrm{BK}}(K, \mathbf{Q}_p) - 1$, so the conjecture predicts that $\mathrm{Sel}_{\mathrm{BK}}(K, \mathbf{Q}_p) = 0$.

Exercise: Prove this. You'll need to use the finiteness of the ideal class group of K, together with the fact that for this representation the local condition $\mathcal{F}_{v,\mathrm{BK}}$ agrees with $\mathcal{F}_{v,\mathrm{ur}}$ for primes $v \mid p$.

Example 2: $V = \mathbf{Q}_p(1)$. Here $L(V^*(1), s) = \zeta_K(s)$. Inspecting the functional equation for Dedekind zeta functions, we see that $\mathrm{ord}_{s=0} \zeta_K(s) = r_1 + r_2 - 1$, where r_1, r_2 are the numbers of real and complex places respectively. (In particular, if $K = \mathbf{Q}$, then $\zeta(0) = -\frac{1}{2}$ is finite and non-zero.) On the algebraic side, we have $H^0(K, \mathbf{Q}_p(1)) = 0$ and

$$\dim \mathrm{Sel}_{\mathrm{BK}}(K,V) = \dim_{\mathbf{Q}_p} \left(\mathcal{O}_K^\times \otimes \mathbf{Q}_p\right) = \mathrm{rank}\, \mathcal{O}_K^\times.$$

So the Bloch–Kato conjecture here is exactly Dirichlet's unit theorem.

Example 3: Elliptic curves. If V is $V_p(E)$ for an elliptic curve E, then:

- the H^0 term is zero;
- the Kummer map lands inside the BK Selmer group, and gives an embedding
$$E(K) \otimes \mathbf{Q}_p \hookrightarrow \mathrm{Sel}_{\mathrm{BK}}(K, V),$$
so that $\dim \mathrm{Sel}_{\mathrm{BK}} \geq \mathrm{rank}(E/K)$, with equality iff the p-part of Sha is finite;
- $\mathrm{ord}_{s=0} L(V^*(1), s) = \mathrm{ord}_{s=1} L(E/K, s)$.

So this instance of Bloch–Kato is closely related to (but not quite the same as) the Birch–Swinnerton-Dyer conjecture.

Remark. Notice that $L(V^*(1), s)$ is expected to be related to $L(V, -s)$ via a functional equation; but this functional equation will involve various Γ functions as factors, which can have poles, so the orders of vanishing of the two functions at 0 are not the same in general, as we saw for $\mathbf{Q}_p$ and $\mathbf{Q}_p(1)$. On the Selmer-group side there's a corresponding relation between $\mathrm{Sel}_{\mathrm{BK}}(K, V)$ and $\mathrm{Sel}_{\mathrm{BK}}(K, V^*(1))$ coming from the Poitou–Tate global duality theorem in Galois cohomology. One can check that these factors precisely cancel out: if $L(V, s)$ has a functional equation of the expected form, then the Bloch–Kato conjecture holds for $V^*(1)$ if and only if it holds for V. This is a wonderful (but rather involved) exercise. ◇

1.4. Euler systems

We'll now introduce the key subject of these lectures: Euler systems, which are tools for studying and controlling Selmer groups. In this section we'll give the abstract definition of an Euler system, and explain (without proofs) why the existence of an Euler system for some Galois representation has powerful consequences for Selmer groups.

References: The standard work on this topic is Karl Rubin's orange book *Euler Systems* [**Rub00**]. There are also two alternative accounts in Rubin's 2004 Park City lecture notes, and in the book *Kolyvagin Systems* [**MR04**] by Mazur and Rubin.

1.4a. The definition.

Let:

- V a $G_{\mathbf{Q}}$-representation (for simplicity)
- $T \subset V$ a $G_{\mathbf{Q}}$-stable $\mathbf{Z}_p$-lattice
- Σ a finite set of primes containing p and all ramified primes for V

Since V is a $G_{\mathbf{Q}}$-rep, we can consider it as a G_K-rep for any number field K and form $H^i(K, V)$, and there are **corestriction** or **norm** maps

$$\mathrm{norm}_K^L : H^i(L, V) \to H^i(K, V) \quad \text{if } L \supset K.$$

If K is Galois, $H^i(K, V)$ is a module over $\mathbf{Q}_p[\mathrm{Gal}(K/\mathbf{Q})]$. Similarly for cohomology of lattices $H^i(K, T)$.

DEFINITION. *An* Euler system for (T, Σ) *is a collection* $\mathbf{c} = (c_m)_{m \geq 1}$*, where* $c_m \in H^1(\mathbf{Q}(\mu_m), T)$*, satisfying the following compatibility for any* $m \geq 1$ *and* ℓ *prime:*

$$\operatorname{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})}(c_{m\ell}) = \begin{cases} c_m & \text{if } \ell \in \Sigma \text{ or } \ell \mid m \\ P_\ell(V^*(1), \sigma_\ell^{-1}) \cdot c_m & \text{otherwise} \end{cases}$$

where σ_ℓ *is the image of* Frob_ℓ *in* $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$*. An* Euler system for V *is an Euler system for* (T, Σ)*, for some* $T \subset V$ *and some* Σ*.*

This definition is not very transparent, I admit! Fear not: we'll see an example before too long. Intuitively, each class c_m has "something to do with" the L-function $L(V^*(1), s)$ with its Euler factors at primes dividing $m\Sigma$ missing[7]; so when we compare elements for different m, the Euler factors appear.

The main reason to care about these objects is the following theorem, which is due to Rubin [**Rub00**], building on earlier work of Kato [**Kat04**], Kolyvagin [**Kol91**], and Thaine [**Tha88**]:

THEOREM 2. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, Σ) *with* c_1 *non-zero, and suppose* V *satisfies various technical conditions. Then* $\mathrm{Sel}_{\mathrm{strict}}(\mathbf{Q}, V^*(1))$ *is zero.*

For the purposes of these lectures we don't need to know how this theorem is proved – our goal is to understand how to *build* Euler systems, which is a separate problem. If you do want to know about the proof, then see the references listed above.

REMARK.

- The technical conditions are to do with the image of $G_{\mathbf{Q}}$ in $\mathrm{GL}(V)$. This needs to be "large enough" in a certain precise sense, which in particular implies that V is irreducible.
- For the proof of the theorem, we don't actually need c_m to be defined for all m; it's enough to have c_m for all integers m of the form $p^k m_0$, where $k \geq 0$ and m_0 is a square-free product of primes not in Σ.
- More generally, one can also define Euler systems for G_K-representations, for K a number field. In place of cyclotomic fields, one has to have classes over different ray class fields of K. However, we'll only work with $K = \mathbf{Q}$ here.
- There is also a notion of "anticyclotomic Euler system", which applies when you have a representation V of G_K, a quadratic extension L/K, and cohomology classes for V over the *anticyclotomic extensions* of L, which are the abelian extensions of L such that conjugation by $\mathrm{Gal}(L/K)$ acts on their Galois groups by -1. The most important example of an anticyclotomic Euler system is Kolyvagin's **Euler system of Heegner points** [**Kol91**], where $K = \mathbf{Q}$, $V = V_p(E)$ for E an elliptic curve, and L is an imaginary quadratic field. Other examples of anticyclotomic Euler systems have recently been found by Cornut, and by Jetchev and his collaborators.

$\diamond$

[7] This becomes more precise if you work with the *equivariant* L-function $L(V^*(1), \mathbf{Q}(\mu_m)/\mathbf{Q}, s)$ which is a Dirichlet series taking values in the group ring $\mathbf{C}[(\mathbf{Z}/m\mathbf{Z})^\times]$ rather than just in $\mathbf{C}$, encoding the L-values of V twisted by Dirichlet characters modulo m. The definition of this function only makes sense if you drop the Euler factors at primes dividing m.

1.4b. Cyclotomic units. We're going to build an Euler system for $V = \mathbf{Q}_p(1)$. Recall that we have Kummer maps $K^\times \hookrightarrow H^1(K, \mathbf{Z}_p(1))$. Also, for L/K finite, we have a commutative square

$$\begin{array}{ccc} L^\times & \xrightarrow{\kappa_p} & H^1(L, \mathbf{Z}_p(1)) \\ \Big\downarrow{\scriptstyle \mathrm{norm}_K^L} & & \Big\downarrow{\scriptstyle \mathrm{norm}_K^L} \\ K^\times & \xrightarrow{\kappa_p} & H^1(K, \mathbf{Z}_p(1)) \end{array}$$

where the left-hand norm map is the usual field norm, and the right-hand one is the Galois corestriction. So we have to find good elements of the multiplicative groups of cyclotomic fields, satisfying compatibilities under the norm maps.

Fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}^\times$ and let $\zeta_m = \iota^{-1}(e^{2\pi i/m}) \in \mu_m$.

DEFINITION. *For $m > 1$, set $u_m = 1 - \zeta_m \in \mathbf{Q}(\mu_m)^\times$.*

A pleasant computation (exercise!) shows that[8]

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{m\ell})} u_m = \begin{cases} u_m & \text{if } \ell \mid m \\ (1 - \sigma_\ell^{-1}) \cdot u_m & \text{if } \ell \nmid m \text{ and } m > 1 \\ \ell & \text{if } m = 1 \end{cases}$$

This is almost what we need for an Euler system, but there are two problems: firstly, there is no sensible way to define u_1; secondly, we are seeing Euler factors at *all* primes, whereas we only want to see them for primes outside Σ (and Σ can't be empty because it has to contain p). We can get around both of these problems by setting

$$v_m = \begin{cases} u_m & \text{if } p \mid m, \\ \mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{pm})}(u_{pm}) & \text{if } p \nmid m \text{ (including } m = 1). \end{cases}$$

THEOREM 3. *The classes $c_m = \kappa_p(v_m)$ are an Euler system for $(\mathbf{Z}_p(1), \{p\})$.* □

1.4c. Soulé twists. Rubin's theorem applied directly to the cyclotomic unit Euler system isn't actually very interesting (it follows easily from class field theory that $\mathrm{Sel}_{\mathrm{strict}}(\mathbf{Q}, \mathbf{Q}_p) = 0$). However, there is a notion of *twisting* for Euler systems.

THEOREM 4. *Let $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ be a continuous character unramified outside Σ (e.g. any power of the cyclotomic character). Then there is a canonical bijection $\mathbf{c} \mapsto \mathbf{c}^\chi$ between Euler systems for T and for the twist $T(\chi)$.*

Note that the "bottom class" c_1^χ in the twisted Euler system depends on whole system $\mathbf{c} = \{c_m\}_{m \geq 1}$, not just on c_1. So even if $c_1 \neq 0$ we might have $c_1^\chi = 0$, and we have to check carefully that the twisted Euler system satisfies the conditions for Rubin's theorem.

The twists of the cyclotomic unit Euler system have many applications in number theory; see e.g. §3.2 of [**Rub00**]. For instance, they play a major role in Huber

[8] This is stated in Rubin's book "Euler Systems", §3.2, but with a sign error: he sets $u_m = \zeta_m - 1$, which doesn't quite work, since $\mathrm{norm}_{\mathbf{Q}(\mu_4)}^{\mathbf{Q}(\mu_8)}(\zeta_8 - 1) \neq \zeta_4 - 1$.

and Kings' proof of the Bloch–Kato conjecture for $\mathbf{Q}_p(n)$ for all $n \in \mathbf{Z}$, an account of which can be found in [**CRSS15**].

CHAPTER 2

A toolkit for building Euler systems

2.1. Etale cohomology and the Hochschild–Serre spectral sequence

(*References*: not as many as there should be. Jannsen's article "Continuous étale cohomology" [**Jan88**] has the details, but it is not an easy read.)

We saw before that, for a variety X/K, the étale cohomology groups $H^i_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)$ were an interesting source of Galois representations.

But this isn't the only thing we can do with étale cohomology. Rather than base-extending to $\overline{K}$, we can also take étale cohomology of X/K directly[1]; there are groups $H^i_{\text{ét}}(X, \mathbf{Q}_p(m))$ for all i and m. These "absolute" étale cohomology groups are *not* themselves Galois representations, but it turns out that these are related to the Galois cohomology of the étale cohomology over $\overline{K}$:

THEOREM 5 (Jannsen). *For any variety X/K, and any n, there is a convergent "Hochschild–Serre" spectral sequence*

$$E_2^{ij} = H^i\left(K, H^j_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)(n)\right) \Rightarrow H^{i+j}_{\text{ét}}(X, \mathbf{Q}_p(n)).$$

In particular, we get edge maps $H^i(X, \mathbf{Q}_p(n)) \to H^i(X_{\overline{K}}, \mathbf{Q}_p(n))^{G_K}$, and if F^1H^i denotes the kernel of this map (the "homologically trivial" classes), there is a map

$$F^1H^i(X, \mathbf{Q}_p(n)) \to H^1\Big(K, H^{i-1}(X_{\overline{K}}, \mathbf{Q}_p)(n)\Big).$$

So, if X is defined over $\mathbf{Q}$ and V is the Galois representation $H^{i-1}(X_{\overline{\mathbf{Q}}})$ (or a direct summand of it), we can try to construct an Euler system for V by building classes in $F^1H^i(X_{\mathbf{Q}(\mu_m)})$ for varying m.

How will we do this? We'll use geometry! To be precise, we'll rely on the following rather simple bag of tricks:

- **Cup products**: étale cohomology has cup-product maps
$$H^i(X, \mathbf{Q}_p(m)) \times H^j(X, \mathbf{Q}_p(n)) \to H^{i+j}(X, \mathbf{Q}_p(m+n)).$$
- **Kummer maps**: if $f \in \mathcal{O}(X)^\times$ is a unit in the ring of rational functions on X, then there is a class $\kappa_p(f) \in H^1(X, \mathbf{Q}_p(1))$.
- **Pushforward maps**: if $Z \subset X$ is a closed subvariety of codimension d (and X and Z are both smooth), then there are pushforward maps
$$H^i(Z, \mathbf{Q}_p(n)) \to H^{i+2d}(X, \mathbf{Q}_p(n+d)).$$

[1] Technical point: what we actually want here is "continuous étale cohomology" in the sense of Jannsen. This is consistent with our use of continuous cochains to define cohomology of Galois representations.

In particular, the pushforward of the identity class $1_Z \in H^0(Z, \mathbf{Q}_p(0))$ is a class in $H^{2d}(X, \mathbf{Q}_p(d))$, the *cycle class* of Z.

So if we have a good supply of units on X, or of subvarieties of X (or of subvarieties of X with units on them, etc) then we have some objects to play with; and we can try to write down classes landing in the "right" cohomological degree to map into H^1 of our target Galois representation.

If you have a random variety, it's not clear how to find lots of subvarieties, or lots of units, on it; but we're going to home in on the case where X is a *Shimura variety* – a variety coming from automorphic theory, such as a modular curve. Then we can try and write down units and subvarieties using automorphic ideas.

2.2. Modular curves and modular forms

(*References*: Diamond–Shurman [**DS05**], Darmon–Diamond–Taylor [**DDT97**].)

We're particularly interested in the Galois representations associated to modular forms, which come from geometry via modular curves. We'll consider weight 2 modular forms first, as these are the simplest to handle.

2.2a. Modular curves. For $N \geq 1$ let

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c = 0, d = 1 \bmod N \right\}.$$

This acts on the upper half-plane $\mathcal{H}$ via $\tau \mapsto \frac{a\tau+b}{c\tau+d}$. It turns out that the quotient is naturally an algebraic variety:

THEOREM 6. *For $N \geq 4$ there is an algebraic variety $Y_1(N)$ over $\mathbf{Q}$ with the following properties:*

- *$Y_1(N)$ is a smooth geometrically connected affine curve.*
- *For any field extension[2] $F/\mathbf{Q}$, the F-points of $Y_1(N)$ biject with isomorphism classes of pairs (E, P), where E/F is an elliptic curve and $P \in E(F)$ is a point of order N on E.*
- *$Y_1(N)(\mathbf{C}) \cong \Gamma_1(N)\backslash\mathcal{H}$, via the map sending $\tau \in \mathcal{H}$ to (E_τ, P_τ) where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and $P_\tau = 1/N \bmod \mathbf{Z} + \mathbf{Z}\tau$.*

(Much stronger theorems are known – for instance, $Y_1(N)$ has a canonical smooth model over $\mathbf{Z}[1/N]$ – but we won't need this just now.)

REMARK. There are two different choices of conventions for $\mathbf{Q}$-models for $Y_1(N)$; everyone agrees what $Y_1(N)$ means over $\mathbf{C}$, but there are two different ways to descend it to $\mathbf{Q}$, classifying elliptic curves with either a point of order N (our convention) or an embedding of the group scheme μ_N (the alternative convention). ◇

[2]Any $\mathbf{Q}$-algebra, in fact; this is important if you want to make precise the idea that $Y_1(N)$ represents a functor.

2.2b. Galois representations. We can use these rational models of modular curves to attach Galois representations to modular forms. Let $f = \sum a_n q^n$ be a cuspidal modular eigenform of weight 2 and level $\Gamma_1(N)$, normalised so that $a_1 = 1$. By a theorem of Shimura, there is a number field L such that all $a_n \in L$. We shall fix an embedding $\iota : L \hookrightarrow \overline{\mathbf{Q}}_p$, and assume that our p-adic coefficient field $E/\mathbf{Q}_p$ contains the image of ι.

DEFINITION. *We let $V_p(f)$ be the largest subspace of $H^1_{\text{ét}}(Y_1(N)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p) \otimes E$ on which the Hecke operators $T(\ell)$, for $\ell \nmid N$, act as multiplication by $a_\ell(f)$.*

By construction, $V_p(f)$ is an E-linear Galois representation coming from geometry. However, one can also show that

(1) $V_p(f)$ is 2-dimensional and irreducible.
(2) $V_p(f)$ is a direct summand of $H^1_{\text{ét}}$ (not just a subspace).
(3) For $\ell \nmid pN$, $V_p(f)$ is unramified at ℓ and the trace of Frob_ℓ^{-1} on $V_p(f)$ is $a_\ell(f)$. More precisely, the local Euler factor is given by
$$P_\ell(V_p(f), t) = 1 - a_\ell(f)t + \ell\chi(\ell)t^2,$$
where χ is the character of f.
(4) $V_p(f)^* = V_p(f \otimes \chi^{-1})(1)$.

It follows from (3) that (up to finitely many bad Euler factors at primes $\ell \mid pN$)[3] the global L-series $L(V_p(f), s)$ is just the L-series of f,
$$L(f, s) = \sum a_n(f) n^{-s}.$$
In particular if $L = \mathbf{Q}$, so that f corresponds to an elliptic curve A, then we have $V_p(f) \cong H^1_{\text{ét}}\left(A_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right) \cong V_p(A)(-1)$.

REMARK. Warning: in Diamond–Shurman chapter 9, the representation they denote by $\rho_{f,p}$ is the *dual* of our $V_p(f)$, which is compensated for by the fact that they use arithmetic Frobenius Frob_p rather than geometric Frobenius Frob_p^{-1} to define the Euler factor. The same applies to Romyar Sharifi's notes at this Arizona Winter School: the representation (ρ_f, V_f) defined in §3.5 of his notes is the dual of our $V_p(f)$. ◇

2.2c. Tensor products. Later on, we'll be interested in *tensor products* of Galois representations associated to modular forms. If you take two newforms f, g (both with coefficients in E) and let V be the four-dimensional Galois representation $V = V_p(f) \otimes V_p(g)$, then using the Kunneth formula for étale cohomology you can show that V is a direct summand of $H^2_{\text{ét}}\left(Y_1(N)^2_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right) \otimes E$, for any N divisible by N_f and N_g.

The L-function attached to this tensor product representation is a rather classical object: it's the so-called *Rankin–Selberg convolution L-function* of f and g, denoted

[3] In fact, if f is a newform, then $L(f, s)$ and $L(V_p(f), s)$ have the same Euler factors at the bad primes too, although this is much harder to check. This doesn't work for the Rankin–Selberg L-function; the "naive" Rankin–Selberg L-series (‡) frequently has the wrong local factors at the bad primes, even if f and g are newforms.

by $L(f \otimes g, s)$. Up to finitely many bad Euler factors, this agrees with the Dirichlet series

$$(\ddagger) \qquad L(\chi_f \chi_g, 2s-2) \sum_{n \geq 1} a_n(f) a_n(g) n^{-s}.$$

2.3. Numerology

For instance, let's suppose we want to build an Euler system for $V_p(f)$, where f is a modular form of weight 2. Since we can twist Euler systems, we can choose to work with $V_p(f)(n)$ for any integer n.

Because $Y = Y_1(N)_{\mathbf{Q}}$ is affine, we have $H^2_{\text{ét}}(Y_{\overline{\mathbf{Q}}}, \mathbf{Q}_p) = 0$, and $H^1_{\text{ét}}(Y_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)(n)$ contains $V_p(f)(n)$ as a direct summand. So the Hochschild–Serre spectral sequence gives us a map

$$H^2_{\text{ét}}(Y, \mathbf{Q}_p(n)) \to H^1\left(\mathbf{Q}, H^1_{\text{ét}}(Y_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)(n)\right) \to H^1(\mathbf{Q}, V_p(f)(n)).$$

How can we get at the groups $H^2_{\text{ét}}(Y, \mathbf{Q}_p(n))$ using our geometric toolkit?

- For $n \leq 0$ this is hopeless, because our toolkit will only ever give classes in $H^i(-, \mathbf{Q}_p(n))$ for $n \geq \frac{i}{2}$ (check this!)
- For $n = 1$, you can use cycle classes of codimension 1 subvarieties of Y – i.e., points. This is Kolyvagin's original approach [**Kol91**]: to build an Euler system using cycle classes of Heegner points. However, this gives an anticyclotomic Euler system (relative to some choice of imaginary quadratic field), not a full Euler system in the sense of §1.4a.[4].
- For $n = 2$, you can use cup-products of units: the Kummer map gives you classes in $H^1_{\text{ét}}(Y, \mathbf{Q}_p(1))$, and the cup-product of two such classes lands in $H^2_{\text{ét}}(Y, \mathbf{Q}_p(2))$. This is Kato's approach [**Kat04**].
- $n \geq 3$ can also be made to work similarly (but gives no more information than for $n = 2$).

We can also ask the same question for $V_p(f) \otimes V_p(g)$, using the geometry of $Y \times Y$. Again, different twists n give very different geometric setups; and taking n too small is hopeless – you want $n \geq 2$ at least. The sensible choices are:

- $n = 3$: we can get classes here as cup-products $\kappa_p(f_1) \cup \kappa_p(f_2) \cup \kappa_p(f_3)$, where f_1, f_2, f_3 are units on $Y \times Y$.
- $n = 2$: we can get classes by taking a curve $Z \subset Y \times Y$ and a unit $f \in \mathcal{O}(Z)^\times$, and pushing forward $\kappa_p(f) \in H^1_{\text{ét}}(Z, \mathbf{Q}_p(1))$ along the embedding $Z \hookrightarrow Y \times Y$.

The $n = 3$ approach has, I believe, never been carried out (and people have tried very hard to make it work without success). The $n = 2$ approach leads to the Euler system of Beilinson–Flach elements, which we'll discuss later in these lectures.

[4]This is an instance of a general phenomenon. We have seen that one needs $i \leq 2n$ for geometric techniques to work. It turns out that in the boundary case $i = 2n$, one can only work with cycle classes of subvarieties (not with units); and these cannot give a full Euler system, only an anticyclotomic one.

2.4. Changing the field and changing the level

To build an Euler system using the Hochschild–Serre spectral sequence, we need to build classes in $H^i(X_K, \mathbf{Q}_p(n))$ as K varies over cyclotomic fields. It turns out that, for modular curves, we can "sneak up" on this field extension by varying the level of our modular curves instead.

DEFINITION. *We write μ_m° for the $\mathbf{Q}$-variety of primitive m-th roots of unity.*

Concretely, this is the 0-dimensional subvariety of the affine line cut out by $\Phi_m(X) = 0$, where Φ_m is the m-th cyclotomic polynomial. This variety is connected (since the cyclotomic polynomials are irreducible over $\mathbf{Q}$) but not, of course, geometrically connected once $m > 2$.

Hence, for any variety $X/\mathbf{Q}$, we can consider the product variety $X \times \mu_m^\circ$, which is also a variety over $\mathbf{Q}$.

PROPOSITION 1. *For any i, m, n, we have isomorphisms of $G_{\mathbf{Q}}$-representations*

$$H^i_{\text{ét}}\left((X \times \mu_m^\circ)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right) \cong \operatorname{Ind}_{G_{\mathbf{Q}(\mu_m)}}^{G_{\mathbf{Q}}} H^i_{\text{ét}}\left(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p\right)$$

and isomorphisms of $\mathbf{Q}_p$-vector spaces

$$H^i_{\text{ét}}\left(X_{\mathbf{Q}(\mu_m)}, \mathbf{Q}_p(n)\right) \cong H^i_{\text{ét}}\left(X \times \mu_m^\circ, \mathbf{Q}_p(n)\right).$$

(This is a form of Shapiro's lemma; it corresponds to the fact that $\mu_m^\circ = \operatorname{Spec} \mathbf{Q}(\mu_m)$, and hence $X_{\mathbf{Q}} \times \mu_m^\circ$ is the image of $X_{\mathbf{Q}(\mu_m)}$ under the forgetful functor from $\mathbf{Q}(\mu_m)$-varieties to $\mathbf{Q}$-varieties.)

This is useful to us because, if $X = Y_1(N)$, the base-extension $Y_1(N) \times \mu_m^\circ$ is *also* a modular curve. More precisely, for any open compact subgroup $U \subset \mathrm{GL}_2(\mathbf{A}_{\mathrm{f}})$, there is an algebraic curve $Y(U)$ defined over $\mathbf{Q}$, whose $\mathbf{C}$-points are the quotient

$$Y(U)(\mathbf{C}) = \mathrm{GL}_2^+(\mathbf{Q}) \backslash \left[\mathcal{H} \times \mathrm{GL}_2(\mathbf{A}_{\mathrm{f}})/K\right]. \tag{1}$$

If U is the subgroup

$$U_1(N) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbf{Z}}) : c = 0, d = 1 \bmod N\widehat{\mathbf{Z}} \right\}$$

then $Y(U)$ is just $Y_1(N)$. However, if we set $U' = \{u \in U_1(N) : \det(u) = 1 \bmod m\}$, then $Y(U')$ is canonically isomorphic to $Y_1(N) \times \mu_m^\circ$, and the action of the quotient U/U' on $Y(U')$ matches up with the Galois action via the usual isomorphism $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^*$.

This transports our problem – constructing cohomology classes for $Y_1(N)$ over varying cyclotomic fields – into a more "automorphic" problem: constructing cohomology classes for modular curves over $\mathbf{Q}$ of varying levels.

REMARK. To some extent this is just a superficial change of language. However, it seems to be a helpful one, as will be clear from our proofs of norm relations later in these lectures. ◇

2.5. Siegel units

As we saw above, we can get potentially useful cohomology classes if we have a source of units in the coordinate rings of our varieties. Fortunately, for modular curves, we have lots of nice units at our disposal. (References: §§1–2 of [**Kat04**] are the definitive source; [**Lan87**] is also useful.)

2.5a. The construction. Let U be an open compact subgroup of $\mathrm{GL}_2(\mathbf{A}_\mathrm{f})$ (such as the group $U_1(N)$ from the previous section).

Definition. *A **modular unit** of level U is a unit in the coordinate ring of the algebraic variety $Y(U)$.*

This definition is very clean, but hard to work with concretely. So we'll unwrap it a bit. Recall that $Y(U)(\mathbf{C})$ is defined as a quotient of $\mathcal{H} \times \mathrm{GL}_2(\mathbf{A}_\mathrm{f})$, so the image of $\mathcal{H} \times \{1\}$ in this quotient is a connected component of $Y(U)(\mathbf{C})$. It turns out that this image is exactly $\Gamma\backslash\mathcal{H}$, where Γ is the discrete group $U \cap \mathrm{GL}_2^+(\mathbf{Q})$ (which is commensurable with $\mathrm{SL}_2(\mathbf{Z})$). So we get a map

$$\left(\begin{array}{c}\text{modular units}\\ \text{of level } U\end{array}\right) \longrightarrow \left(\begin{array}{c}\text{nowhere-zero holomorphic fcns}\\ \text{on } \Gamma\backslash\mathcal{H} \text{ with finite-order poles at cusps}\end{array}\right).$$

Fact: This map is *injective*, because the Galois group acts transitively on the components of $Y(U)$. □

For a general subgroup U the image is a little fiddly to describe. However, for some nice subgroups we can make it very concrete:

Proposition 2. *Let $U(N) \subset \mathrm{GL}_2(\widehat{\mathbf{Z}})$ be the kernel of the reduction map $\mathrm{GL}_2(\hat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, and $\Gamma(N) = U(N) \cap \mathrm{SL}_2(\mathbf{Z})$. Then the modular units of level $U(N)$ are precisely the functions on $\Gamma(N)\backslash\mathcal{H}$ which are holomorphic and nonzero away from the cusps, are meromorphic at the cusps, and have q-expansion coefficients in $\mathbf{Q}(\mu_N)$.* □

We're going to construct some "special" modular units of level $U(N)$, using nothing but classical 19th-century elliptic function theory. These functions are called **Siegel units** and they are really amazingly powerful gadgets. In fact, you can recover virtually every known example of an Euler system by starting from Siegel units!

Definition. *Let $\alpha, \beta \in \mathbf{Q}/\mathbf{Z}$, not both zero. Define the function $g_{\alpha,\beta} : \mathcal{H} \to \mathbf{C}$ as follows: write $(\alpha, \beta) = (a/N, b/N)$ for some $N \geq 1$ and $a, b \in \mathbf{Z}$, with $0 \leq a < N$ without loss of generality. Then*

$$g_{\alpha,\beta}(\tau) = q^w \prod_{n\geq 0}\left(1 - q^{n+a/N}\zeta_N^b\right)\prod_{n\geq 1}\left(1 - q^{n-a/N}\zeta_N^{-b}\right),$$

where $q = e^{2\pi i\tau}$ and $w = \frac{1}{12} - \frac{a}{N} + \frac{a^2}{2N^2}$.

This is well-defined (independent of the choice of common denominator N). We'd like to say it's modular of level N, but this doesn't quite work: acting on it by an element of $\Gamma(N)$ multiplies it by a root of unity. These error terms can be killed by a very simple modification:

DEFINITION (Siegel units). *For $c > 1$ coprime to 6 and to the order of α, β in $\mathbf{Q}/\mathbf{Z}$, let*

$$ {}_cg_{\alpha,\beta} = \frac{(g_{\alpha,\beta})^{c^2}}{g_{c\alpha,c\beta}}. $$

PROPOSITION 3. *The functions ${}_cg_{\alpha,\beta}$, for $(\alpha,\beta) \in (\frac{1}{N}\mathbf{Z}/\mathbf{Z})^{\oplus 2} - \{(0,0)\}$, are modular units of level $U(N)$. The left action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on $Y(U(N))$ transforms these units via the rule*

$$ {}_cg_{\alpha,\beta} \mid \sigma = {}_cg_{\alpha',\beta'}, \quad \text{where} \quad (\alpha',\beta') = (\alpha,\beta)\sigma. \quad \square $$

In particular, because $(0, \frac{1}{N})$ is preserved by right-multiplication by matrices of the form $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$, which give the action of the quotient $U_1(N)/U(N)$, we see that:

PROPOSITION 4. *The function ${}_cg_{0,1/N}$ is a modular unit of level $U_1(N)$.* $\square$

2.5b. Changing the level: the basic norm relation.

THEOREM 7. *Let $\alpha, \beta \in \mathbf{Q}/\mathbf{Z}$, not both zero, and let $A \geq 1$. Then we have the three relations*

$$ \prod_{\alpha' : A\alpha' = \alpha} {}_cg_{\alpha',\beta}(\tau) = {}_cg_{\alpha,\beta}(A^{-1}\tau), \tag{2} $$

$$ \prod_{\beta' : A\beta' = \beta} {}_cg_{\alpha,\beta'}(\tau) = {}_cg_{\alpha,\beta}(A\tau), \tag{3} $$

$$ \prod_{\substack{\alpha',\beta' \\ A(\alpha',\beta') = (\alpha,\beta)}} {}_cg_{\alpha',\beta'}(\tau) = {}_cg_{\alpha,\beta}(\tau). \tag{4} $$

SKETCH OF PROOF. Note that (1) and (2) imply (3), and (2) follows from (1) via the action of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; so it suffices to prove (1). This can be bashed out directly from the infinite product formula, but there is a much slicker argument in[**Kat04**], involving a 2-variable theta function ${}_c\theta(\tau, z)$ such that ${}_c\theta(\tau, \alpha\tau + \beta) = {}_cg_{\alpha\beta}$. $\square$

The most important relation is (3), which can be written in a more conceptual way using push-forward maps between modular curves. Suppose ℓ is a prime; then there's a quotient map $\pi : Y_1(N\ell) \to Y_1(N)$, and associated to this is a norm map $\pi_* : \mathcal{O}(Y_1(N\ell))^\times \to \mathcal{O}(Y_1(N))^\times$, characterised by

$$ (\pi_* f)(x) = \prod_{y \in \pi^{-1}(x)} f(y) \quad \text{for } x \in \Gamma_1(N)\backslash\mathcal{H}. $$

COROLLARY 1. *The Siegel units satisfy*

$$ \pi_*({}_cg_{0,1/N\ell}) = \begin{cases} {}_cg_{0,1/N} & \text{if } \ell \mid N, \\ {}_cg_{0,1/N} \cdot \left({}_cg_{0,u/N}\right)^{-1} & \text{if } \ell \nmid N. \end{cases} $$

where u is the inverse of ℓ modulo N. $\square$

PROOF. Exercise. $\square$

This is hugely important, because it's the underlying input for all of the Euler systems we will build out of Siegel units.

CHAPTER 3

Interlude: motivic cohomology and period integrals

Note: This chapter is provided only for motivation, and involves some very deep and advanced concepts; these will not be needed in the following sections, so you may wish to skip this part at a first reading.

We've seen in the last section that:

- Interesting Galois representations often appear in the étale cohomology (over $\overline{\mathbf{Q}}$) of Shimura varieties.
- One can build classes in H^1 of these Galois representations via Hochschild–Serre, using cup-products, pushforwards from subvarieties, and the Kummer map.
- We have a supply of interesting units on modular curves to use as input to the Kummer map.

For example, if we want to build Euler systems for tensor products $V_f \otimes V_g$, we want classes in $H^3_{\text{ét}}(Y_1(N) \times Y_1(N), \mathbf{Z}_p(2))$; and we can get these by choosing curves $Z \subset Y_1(N)^2$, and pushing forward $\kappa_p(u)$ for some $u \in \mathcal{O}(Z)^\times$. A natural thing to try, of course, is to take Z to be the diagonal copy of $Y_1(N)$, and $u = {}_c g_{0,1/N}$ the Siegel unit.

However, why should this construction give *interesting* classes? How are we going to relate them to the special values of L-functions?

3.1. The Rankin–Selberg integral formula

Here's a very classical result, discovered independently by Rankin and by Selberg in the 1930s.

THEOREM 8. *Let $N \geq 1$, and for $s \in \mathbf{C}$ with $\Re(s) \gg 0$, let E_s be the (non-holomorphic) function on the upper half-plane $\mathcal{H}$ defined by*

$$E_s(\tau) = \pi^{-s}\Gamma(s) \sum_{(c,d)\in\mathbf{Z}^2} \frac{\Im(\tau)^s}{|c\tau + d + 1/N|^{2s}}.$$

Then, for any two newforms f, g of level N and weight 2, we have

$$\langle \bar{f}, gE_s \rangle = \int_{\Gamma_1(N)\backslash\mathcal{H}} f(-\bar{\tau})g(\tau)E_s(\tau)\,\mathrm{d}\tau \wedge \mathrm{d}\bar{\tau} = (*) \cdot L(V_f \otimes V_g, s+1),$$

where $(*)$ is an explicit factor.

This is surprisingly simple to prove: after interchanging summation and integration, you get the integral of $f(-\bar{\tau})g(\tau)\Im(\tau)^{-s}$ over the region $\{x+iy : 0 \le x \le 1, 0 \le y \le \infty\}$, and substituting in the q-expansions of f and g and integrating term-by-term gives the result. However, it has a lot of important consequences; for instance, it follows easily from this formula and the properties of E_s that $L(V_f \otimes V_g, s)$ has meromorphic continuation to all $s \in \mathbf{C}$ (with well-understood poles) and satisfies a functional equation relating s and $3 - s$.

However, the reason I want to consider it here is the following classical result ("Kronecker's second limit formula")[1]

THEOREM 9 (Kronecker). *We have* $E_0(\tau) = -\log|g_{0,1/N}|$.

So there's some connection between $E_0(\tau)$ and Siegel units, and on the other hand between $E_s(\tau)$ and Rankin–Selberg convolutions. In order to state this properly, we need to introduce another cohomology theory.

3.2. Motivic cohomology

References: Mazza–Voevodsky–Weibel, *Lecture notes on motivic cohomology* [**MVW06**]; Beilinson, *Higher regulators and values of L-functions* [**Beĭ84**].

There is a cohomology theory for algebraic varieties called *motivic cohomology*, introduced by Beilinson and greatly refined by the late Vladimir Voevodsky. It gives groups $H^i_{\text{mot}}(X, \mathbf{Z}(n))$, and for each prime p, there are maps (étale regulators)

$$r_{\text{ét}} : H^i_{\text{mot}}(X, \mathbf{Z}(n)) \otimes \mathbf{Z}_p \to H^i_{\text{ét}}(X, \mathbf{Z}_p(n)).$$

For small i and n the motivic cohomology groups have explicit descriptions. $H^1_{\text{mot}}(X, \mathbf{Z}(1))$ is literally equal to $\mathcal{O}(X)^\times$, and the étale regulator on this group is the Kummer map κ_p.

REMARK. The étale regulator is compatible with pushforward and cup-products, so in fact our entire toolkit for building elements of étale cohomology factors through motivic cohomology. This also explains why our tools can't get at $H^i_{\text{ét}}(X, \mathbf{Z}_p(n))$ when $i > 2n$: in this range the group $H^i_{\text{mot}}(X, \mathbf{Z}(n))$ is zero. ◇

THEOREM 10 (Landsburg [**Lan91**]). *If S is an algebraic surface over a field k, $H^3_{\text{mot}}(S, \mathbf{Z}(2))$ is isomorphic to the quotient*

$$\left\{ \begin{array}{c} \text{formal sums} \displaystyle\sum_i (Z_i, u_i),\ Z_i \subset S \text{ irreducible curve}, \\ u_i \in k(Z_i)^\times, \text{ with} \displaystyle\sum_i \operatorname{div} u_i = 0 \end{array} \right\} / \sim$$

where $\sim$ is some equivalence relation.

In particular, if we have a curve $Z \subset S$ and an element $u \in \mathcal{O}(Z)^\times$, then $\operatorname{div} u$ is trivial, so (Z, u) defines a class in $H^3_{\text{mot}}(S, \mathbf{Z}(2))$; and (unsurprisingly) the image of this class in $H^3_{\text{ét}}(X, \mathbf{Z}_p(2))$ is just $\iota_*(\kappa_p(u))$, where $\iota : Z \hookrightarrow S$ is the inclusion morphism.

[1] I did say this was 19th-century stuff; Kronecker died in 1891.

However, as well as the étale regulator $r_{\text{ét}}$, there's a second regulator map defined on $H^3_{\text{mot}}(S, \mathbf{Z}(2)) \otimes \mathbf{R}$, the *Beilinson regulator* $r_{\mathbf{C}}$: if ω is a (sufficiently nice) differential 2-form on $S(\mathbf{C})$, we can map an element $\mathfrak{z} = \sum_i (Z_i, u_i)$ to

$$(\dagger) \qquad \sum_i \int_{Z_i} \omega \log |u_i|.$$

This is clearly linear in ω, so we get a map from $H^3_{\text{mot}}(S, \mathbf{Z}(2))$ to the dual space of a space of differential forms – more precisely, to $\left(\text{Fil}^1 H^2_{\text{dR}}(S_{\mathbf{C}})\right)^*$.

Combining this with what we know about logs of Siegel units, something magical happens: if $S = Y_1(N) \times Y_1(N)$ and $\mathfrak{z}$ is the class of $(\text{diagonal}, {}_c g_{0,1/N})$, and we take $\omega = (f(-\bar{\tau})\, \mathrm{d}\bar{\tau}) \wedge (g(\tau)\, \mathrm{d}\tau)$, then *the integral* $(\dagger)$ *is exactly the Rankin–Selberg integral at* $s = 1$! So, to sum up,

- the class we've built in $H^3_{\text{ét}}(Y_1(N)^2, \mathbf{Z}_p(2))$ is naturally the image of something in $H^3_{\text{mot}}(Y_1(N)^2, \mathbf{Z}(2))$,
- the Beilinson regulator of this class, paired with a differential coming from f and g, computes a value of the L-function $L(f \otimes g, s)$.

This is pretty strong evidence that the Galois cohomology class we're building (the *Beilinson–Flach class*) is the right class to consider: it's the image under the étale regulator of a motivic class which is a "motivic incarnation" of the Rankin–Selberg integral.

Remark. It follows from the Beilinson regulator formula that the motivic class $\mathfrak{z} = (\text{diagonal}, {}_c g_{0,1/N}) \in H^3_{\text{mot}}(S, \mathbf{Z}(2))$ is non-zero. If the étale regulator from here to $H^3_{\text{ét}}(S, \mathbf{Z}_p(2))$ were injective, then we could actually deduce that our class in $H^3_{\text{ét}}(S, \mathbf{Z}_p(2))$ was non-zero, and we'd be in a good position to apply Rubin's theorem.

Sadly, we don't know this. We can replace S with an integral model $\mathcal{S}$ defined over $\mathbf{Z}[1/pN]$. It's known that $H^3_{\text{mot}}(\mathcal{S}, \mathbf{Z}(2))/p^k$ maps injectively to $H^3_{\text{ét}}(\mathcal{S}, \mathbf{Z}_p(2))/p^k$ for every k; but unfortunately we don't know any finite generation properties for $H^3_{\text{mot}}(\mathcal{S}, \mathbf{Z}(2))$, so $\mathfrak{z}$ might potentially be infinitely p-divisible, and hence zero in $H^3_{\text{mot}}(\mathcal{S}, \mathbf{Z}(2))/p^k$ for every k. It's conjectured that the motivic cohomology groups of a scheme of finite type over $\mathbf{Z}$ should always be finitely generated, which would rule out this pathology, but unfortunately this conjecture is wide open. ◇

3.3. Other Rankin–Selberg formulae

The Rankin–Selberg integral is only the first of a very wide class of formulae, which express the L-values of an automorphic form for some reductive group G in terms of its integral against an Eisenstein series on some subgroup H (a "period integral"). There is a survey article by Bump [**Bum05**]) which catalogues dozens of constructions of this kind.

So we can play the following game: if we want to build an Euler system for some class of automorphic Galois representations, then we can look for known formulae expressing the L-function of our representation in terms of periods of automorphic forms. Then we can stare at the resulting integrals and try to recognise them as Beilinson regulators of motivic cohomology classes. If we can do this, then the étale

versions of these classes should be non-zero (although we can't prove this), and they are clearly the right building blocks for an Euler system for our representation.

REMARK. This won't always work, sadly. Firstly, in many of the known Rankin–Selberg formulae the groups G and H do not have Shimura varieties, so they lie outside the world of algebraic geometry; there is a perfectly good Rankin–Selberg integral for $\mathrm{GL}_m \times \mathrm{GL}_n$ for any integers (m, n), but it doesn't correspond to anything motivic unless $m = n = 2$.

Even if G corresponds to a Shimura variety (and H to a Shimura subvariety), then there can be more subtle obstacles. One major stumbling block is the Eisenstein series appearing in the formulae; these are often not just Eisenstein series for GL_2 but for more general reductive groups, and we need a way to relate these to motivic cohomology, generalising the way that GL_2 Eisenstein series are related to units via Kronecker's limit formula. This seems to be a difficult problem in general.

Despite these apparently gloomy remarks, all is not lost: there are surprisingly many Rankin–Selberg formulae in which only GL_2 Eisenstein series appear! There's now an ongoing project, being pursued by several research groups, to build Euler systems for each such integral formula. Some examples are

- an Euler system for the Asai representation attached to quadratic Hilbert modular forms, with $H = \mathrm{GL}_2$ and $G = \mathrm{Res}^F_{\mathbf{Q}} \mathrm{GL}_2$, where F is a real quadratic field [**LLZ16**];
- an Euler system for the spin representations attached to genus 2 Siegel modular forms, with $H = \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2$ and $G = \mathrm{GSp}_4$ ([**LSZ17**]; we will discuss this example in Chapter 6);
- an Euler system for the spin representation of genus 3 Siegel modular forms, with $H = \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2$ and $G = \mathrm{GSp}_6$, which is studied by Antonio Cauchi and Joaquin Rodrigues [**CR18**];
- an Euler system for Picard modular forms (work in progress with Chris Skinner), with $H = \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{Res}^K_{\mathbf{Q}} \mathrm{GL}_1$ and $G = \mathrm{GU}(2, 1)$, where K is an imaginary quadratic field and $\mathrm{GU}(2, 1)$ a unitary group split over K. In this case, we get an *Euler system over* K: in other words, we construct cohomology classes over all the finite abelian extensions of K.

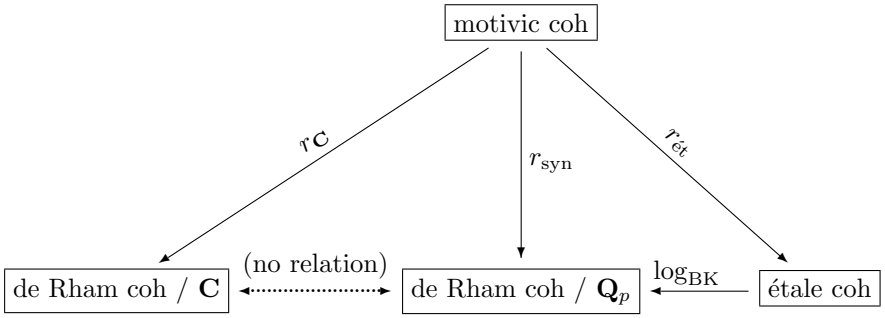
A further example of this is the $\mathrm{GSp}_4 \times \mathrm{GL}_2$ project that we are proposing for this Winter School (see Section 7.1). ◇

3.4. P-adic regulators

So we have a strategy for building Galois cohomology classes which "really ought to be" non-zero, in the sense that they are the étale images of non-zero motivic cohomology classes. However, since we can't prove that the map from motivic to étale cohomology is injective, how can we be sure these Galois cohomology classes aren't all zero?

To do this, we introduce yet another regulator map defined[2] on $H^3(S, \mathbf{Z}(2))$, besides the étale and Beilinson regulators: the *p-adic syntomic regulator* [**Bes00**], which is defined using p-adic rigid geometry, assuming $p \nmid N$. The two key properties of this regulator are that

- like Beilinson's, it can be made explicit enough to compute with: there is a formula for the p-adic regulator map for a surface, due to Besser [**Bes12**], which is very closely analogous to (†), with the integral understood via Coleman's p-adic integration theory.
- unlike Beilinson's, it can be compared to the étale regulator: a very deep theorem in p-adic Hodge theory, due (independently[3]) to Nizioł and Nekovář [**Niz97, Nek98**], shows that there is a commutative diagram relating the étale and syntomic regulators via the Bloch–Kato logarithm map of p-adic Hodge theory.



Putting these pieces together, if we can build a class $\mathfrak{z} \in H^3(S, \mathbf{Z}(2))$ and show that the syntomic regulator of $\mathfrak{z}$ is non-zero, then its etale regulator must also be non-zero. This programme was carried out in the Rankin–Selberg setting by Bertolini, Darmon and Rotger [**BDR15**], using Besser's formula [**Bes12**] to prove that the syntomic regulators of the Beilinson–Flach classes were p-adic L-values.

[2]This is not quite true: it is defined on the part of $H^3(S, \mathbf{Z}(2))$ coming from a smooth model $\mathcal{S}$ over $\mathbf{Z}_p$. This is a non-trivial restriction; the work of Flach on adjoint Selmer groups of modular forms relies strongly on the existence of motivic cohomology classes for S which don't extend to $\mathcal{S}$.

[3]Stronger results have subsequently been proved by these two authors jointly, in [**NN16**], which treats the case of varieties with bad reduction at p.

CHAPTER 4

The Beilinson–Flach Euler system

In this section we're going to write down the classes, and prove the "p-direction" norm relations, for one important example of an Euler system: the Euler system of Beilinson–Flach elements. That is, we'll define classes over the fields $\mathbf{Q}(\mu_m)$ for all integers m, and we'll show that if m is of the form p^r, then these classes are compatible under the norm maps for varying r.

References for this lecture: here there is really no alternative to the original papers [**LLZ14**], [**KLZ15**] and [**KLZ17**].

4.1. Beilinson–Flach elements

As we've seen in Sections 2.2 and 5.1, we can find this Galois representations attached to Rankin–Selberg convolutions of pairs of weight 2 modular forms in the geometry of $Y_1(N)^2$, for a suitable integer N. Suppose now that both modular forms have weight 2. Then we want to construct classes in the cohomology groups

$$H^3_{\text{ét}}\left(Y_1(N) \times Y_1(N) \times \mu_m^\circ, \mathbf{Z}_p(2)\right)$$

for $m \geq 1$. Notice that we have only one copy of μ_m° here, not two; so this is best interpreted not as a Shimura variety for $\mathrm{GL}_2 \times \mathrm{GL}_2$, but for the fibre product

$$\mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2 = \{(g_1, g_2) \in \mathrm{GL}_2 \times \mathrm{GL}_2 : \det(g_1) = \det(g_2)\}.$$

4.1a. Strategy. In the "Numerology" section above, we saw that one natural line of attack is to find curves $C \subset Y \times Y$, where $Y = Y_1(N)$, and units on C. This approach goes back to Beilinson in 1984 (and was further refined by Flach in 1992, hence the name).

An obvious first guess is to take C to be the diagonally-embedded copy of Y in $Y \times Y$, and then put modular units on C. This is exactly what we'll do for $m = 1$: we define

$${}_c\,\mathrm{BF}_{1,N} = \iota_* \left({}_c g_{0,1/N}\right),$$

where ι is the diagonal embedding, and $c > 1$ is some integer coprime to everything in sight.

However, how will we get classes over $\mathbf{Q}(\mu_m)$ for $m > 1$? If we had modular units on the curves $Y_1(N) \times \mu_m^\circ$ which were norm-compatible in m, then we could just push these forward in the same way. However, units with this kind of norm-compatibility seem to be hard to find; the Siegel units have very good compatibility properties in the "N-direction", but no interesting compatibility in the "m-direction".

So we have to make the curve C vary too, and get some contribution to our norm-compatibility this way instead. This is the first hint at a rather powerful general

machine that can turn easy norm relations on a small group into "hard" norm relations on a larger group.

We'll have a lot of use for the following basic lemma relating pushforward and pullback maps in étale cohomology:

PROPOSITION 5 (Push-pull lemma). *Suppose we have a commutative diagram of morphisms of smooth varieties*

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ Z & \xrightarrow[\delta]{} & W, \end{array}$$

in which the horizontal maps α and δ are closed embeddings of codimension c, and the vertical maps β and γ are unramified coverings of equal degrees. Then the morphisms $H^i_{\text{ét}}(Z, \mathbf{Z}_p(n)) \to H^{i+2c}_{\text{ét}}(Y, \mathbf{Z}_p(n+c))$ given by $\alpha_* \circ \beta^*$ and $\gamma^* \circ \delta_*$ coincide. □

This is a simple instance of a much more general result: the hypotheses imply that the diagram is *Cartesian*, identifying X with the fibre product $Y \times_W Z$. The identity of push-pull and pull-push maps holds for any Cartesian diagram, although we'll only use diagrams of this simple kind.

4.1b. Mixed-level modular curves.

DEFINITION. *For integers $M \mid N$, let*

$$U(M,N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbf{Z}}) : \begin{array}{c} a = 1, b = 0 \bmod M, \\ c = 0, d = 1 \bmod N \end{array} \right\}.$$

A more compact notation for the same thing, which I'll use henceforth, is that $U(M,N)$ is the subgroup of level $\begin{pmatrix} M & M \\ N & N \end{pmatrix}$. The definition makes perfect sense without assuming $M \mid N$, of course, but we will only use it in this case. We write $Y(M,N)$ for the corresponding modular curve. Notice that we've already seen two special cases: we have $U(1,N) = U_1(N)$, and $U(N,N) = U(N)$.

DEFINITION. *For ℓ prime, we'll write π_ℓ for the natural quotient map*

$$Y(M, N\ell) \to Y(M,N).$$

There is also a natural quotient map $Y(M\ell, N) \to Y(M,N)$, but we won't use this map. Instead, we'll be more interested in a "twisted" degeneracy map, which we'll now define. Let $U(M(\ell), N)$ be the group of level $\begin{pmatrix} M & M\ell \\ N & N \end{pmatrix}$. Then there is a natural quotient map $Y(M\ell, N) \to Y(M(\ell), N)$; and there are two maps

$$\hat{\pi}_{1,\ell}, \hat{\pi}_{2,\ell} : Y(M(\ell), N) \to Y(M,N),$$

where $\hat{\pi}_{1,\ell}$ is the natural quotient map, and $\hat{\pi}_{2,\ell}$ corresponds to $\tau \mapsto \tau/\ell$ on $\mathcal{H}$.

DEFINITION. *We write τ_ℓ for the composite*

$$Y(M\ell, N) \to Y(M(\ell), N) \xrightarrow{\hat{\pi}_{2,\ell}} Y(M,N).$$

The curve $Y(M,N)$ maps canonically to μ_M° (and in fact the the fibres of this map are geometrically connected). We'll abuse notation slightly by writing $Y(M,N)^2$ for the fibre product of two copies of $Y(M,N)$ over their common map to μ_M°. Again, this is most naturally seen as a Shimura variety for $\mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2$.

4.1c. Rankin–Eisenstein classes. The following is an easy check:

PROPOSITION 6. *If $M \mid N$, the group $U(M,N)$ is normalised by the element* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\hat{\mathbf{Z}})$. □

So we can make the following definition:

DEFINITION. *Let $\iota_{M,N}$ be the embedding $Y(M,N) \hookrightarrow Y(M,N)^2$ given by*

$$P \mapsto \left(P, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot P \right).$$

Notice that this corresponds to $\tau \mapsto (\tau, \tau+1)$ on the upper half-plane.

DEFINITION. *The* Rankin–Eisenstein *class ${}_c\mathrm{REis}_{M,N}$ is the image of ${}_cg_{0,1/N}$ under $(\iota_{M,N})_*$.*

4.1d. Beilinson–Flach elements. The final piece of the puzzle is to descend from the higher-level modular curves where the Rankin–Eisenstein classes live to $Y_1(N) \times \mu_M^\circ$. As above, we're identifying $Y_1(N) \times \mu_M^\circ$ with the Shimura variety of level $U' = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : c = 0, d = 1 \bmod N, ad - bc = 0 \bmod M \}$.

One checks easily that

$$\begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} U(M,MN) \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix}^{-1} \subseteq U',$$

so there is a map $s_M : Y(M,MN) \to Y_1(N) \times \mu_M^\circ$ corresponding to $\tau \mapsto \tau/M$ on $\mathcal{H}$. This gives us a pushforward map in cohomology, $(s_M \times s_M)_*$.

DEFINITION. *We define the* Beilinson–Flach class *as the class*

$${}_c\mathrm{BF}_{M,N} = (s_M \times s_M)_* \left({}_c\mathrm{REis}_{M,MN} \right) \in H^3_{\text{ét}} \left(Y_1(N)^2 \times \mu_M^\circ, \mathbf{Q}_p(2) \right).$$

These are the classes we really want to study. However, it turns out that proving the norm-compatibility relations for the Beilinson–Flach elements directly is difficult; it's easiest to investigate the norm-compatibility of the auxiliary classes ${}_c\mathrm{REis}_{M,N}$ first, and deduce norm-compatibility relations for the classes ${}_c\mathrm{BF}_{M,N}$ as a consequence. This is what we'll do in the next section.

4.2. Norm-compatibility

It's easy to see that Rankin–Eisenstein classes "inherit" from the Siegel units good norm-compatibility properties in the N-aspect. If ℓ is prime, and π denotes the natural quotient map $Y(M,N\ell) \to Y(M,N)$ as above. then we have

$$(\pi_\ell \times \pi_\ell)_* \left({}_c\mathrm{REis}_{M,\ell N} \right) = {}_c\mathrm{REis}_{M,N}$$

when $\ell \mid N$ (and there is a slightly modified formula for $\ell \nmid N$).

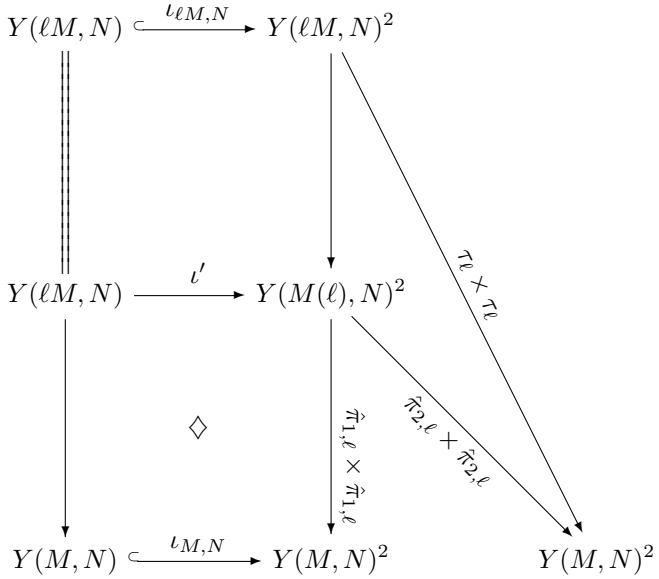
REMARK. This is a good exercise – you need to use the fact that pushforward maps in étale cohomology are functorial, so that the pushforward map for a composite is the composite of the pushforwards. ◇

However, they have also, miraculously, acquired an extra norm-compatibility in the M-aspect, which the Siegel units do not have. Recall that $\tau_\ell : Y(M\ell, N) \to Y(M, N)$ was the "twisted" degeneracy map.

THEOREM 11. *If M, N, ℓ are integers with ℓ prime, $\ell \mid M$ and $M\ell \mid N$, then the Rankin–Eisenstein classes satisfy*

$$(\tau_\ell \times \tau_\ell)_* \left({}_c\mathrm{REis}_{\ell M,N}\right) = (U'(\ell) \times U'(\ell)) \cdot {}_c\mathrm{REis}_{M,N}.$$

Here $U'(\ell)$ is the transpose of the usual Hecke operator $U(\ell)$. The proof of this involves a very important commutative diagram of maps of algebraic varieties over $\mathbf{Q}$:



Here the two diagonal maps are the ones introduced in the previous section, and the vertical maps are the natural quotient maps. The commutativity of the diagram is obvious by construction; the two really important and nonobvious properties are the following:

PROPOSITION 7. *Under the hypotheses of the theorem, the map ι' is a closed embedding, and the lower left square marked $\diamondsuit$ is a Cartesian diagram of the kind described in Proposition 5.*

PROOF. It's easy to see that the image of ι' is precisely the modular curve associated to the group

$$U(M(\ell), N) \cap \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} U(M(\ell), N) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

However, a straightforward matrix computation shows that this intersection is nothing but $U(\ell M, N)$ itself. So ι' is a closed embedding.

Since both horizontal maps in the square $\diamondsuit$ are closed embeddings, and the vertical maps are automatically finite coverings, it suffices to check that the degrees of the vertical maps agree. These degrees are equal to the indices of corresponding inclusions of level groups: on the left-hand side we have $[U(M,N) : U(\ell M, N)] = \ell^2$, and on the right-hand side $[U(M,N)^2 : U(M(\ell), N)^2] = \ell^2$. □

Exercise. Show that if M, N, ℓ are integers with ℓ prime, $\ell \nmid M$ and $M\ell \mid N$, then the Rankin–Eisenstein classes satisfy

$$(\tau_\ell \times \tau_\ell)_* \left({}_c\mathrm{REis}_{\ell M,N}\right) = \left(U'(\ell) \times U'(\ell) - \Delta_\ell^*\right) \cdot {}_c\mathrm{REis}_{M,N}, \tag{5}$$

where Δ_ℓ denotesany element of $\mathrm{GL}_2(\mathbf{Z}/MN\mathbf{Z})^2$ of the form $\left(\begin{pmatrix} x & \\ & 1 \end{pmatrix}, \begin{pmatrix} x & \\ & 1 \end{pmatrix}\right)$ with $x \equiv \ell \pmod{m}$.

Corollary 2. *The following two classes in $H^3_{\text{ét}}(Y(M(\ell), N)^2, \mathbf{Z}_p(2))$ coincide:*

- *the pushforward of ${}_c\mathrm{REis}_{\ell M,N}$ along the upper vertical arrow $Y(\ell M, N)^2 \to Y(M(\ell), N)^2$;*
- *the pullback of ${}_c\mathrm{REis}_{M,N}$ along the lower vertical arrow $Y(M(\ell), N)^2 \to Y(M, N)^2$.*

Proof. This is exactly the "push-pull" lemma applied to the square $\diamond$ (since the unit ${}_cg_{0,1/N}$ on $Y(\ell M, N)$ is, by definition, the pullback of the unit with the same name on $Y(M, N)$.) □

Since these two classes are equal on $Y(M(\ell), N)^2$, they certainly must have the same pushforward along the diagonal map to $Y(M, N)^2$. So we obtain an equality between $(\tau_\ell \times \tau_\ell)_* \left({}_c\mathrm{REis}_{\ell M,N}\right)$ and the image of ${}_c\mathrm{REis}_{\ell M,N}$ under pullback and pushforward around the triangle. This composite of pushforward and pullback maps is exactly the Hecke operator $U'(\ell) \times U'(\ell)$, so we have proved the theorem. □

Remark. The proof works with a minor modification if we drop the hypothesis that $\ell \mid M$. If $\ell \nmid M$, then ι' is still a closed embedding, but the degrees of the vertical maps in the square are $\ell(\ell-1)$ on one side and ℓ^2 on the other. In order to obtain a Cartesian square, we have to modify $\diamondsuit$ by replacing $Y(\ell M, N)$ with the disjoint union $Y(\ell M, N) \sqcup Y(M(\ell), N)$ which does have degree ℓ^2 over $Y(M, N)$. Some simple bookkeeping later we conclude that

$$(\tau_\ell \times \tau_\ell)_* \left({}_c\mathrm{REis}_{\ell M,N}\right) = \left[\left(U'(\ell) \times U'(\ell)\right) - \sigma_\ell\right] \cdot {}_c\mathrm{REis}_{M,N}.$$

On the other hand, the assumption $\ell M \mid N$ is essential, since otherwise the definition of the Rankin–Eisenstein element doesn't even make sense. ◇

We can now state and prove the main theorem:

Theorem 12. *If ℓ is prime with $\ell \mid M$ and $\ell \mid N$, and $j \in (\mathbf{Z}/\ell M\mathbf{Z})^\times$, we have*

$$\mathrm{norm}_{\mathbf{Q}(\mu_M)}^{\mathbf{Q}(\mu_{\ell M})} \left({}_c\mathrm{BF}_{\ell M,N}\right) = \left[U'(\ell) \times U'(\ell)\right] \cdot {}_c\mathrm{BF}_{M,N}.$$

PROOF. This follows from the commutativity of the diagram

$$\begin{array}{ccccc} Y(\ell M, \ell MN) & \xrightarrow{\tau_\ell} & Y(M, \ell MN) & \xrightarrow{\pi_\ell} & Y(M, MN) \\ \downarrow{\scriptstyle s_{\ell M}} & & & & \downarrow{\scriptstyle s_M} \\ Y_1(N) \times \mu_{\ell M}^\circ & & \longrightarrow & & Y_1(N) \times \mu_M^\circ, \end{array}$$

and the following compatibilities:

- the main theorem of the previous section, which we use to compare $\mathrm{REis}_{\ell M, \ell MN}$ with $\mathrm{REis}_{M, M\ell N}$;
- the norm-compatibility in N, which allows us to compare $\mathrm{REis}_{M,M\ell N}$ with $\mathrm{REis}_{M,MN}$;
- the fact that $U'(\ell)$ commutes with the pushforward along the maps π_ℓ and s_M. □

Exercise. Using (5), formulate and prove the analogous statement in the case when $\ell \nmid M$ and $\ell \mid N$.

REMARKS.

(i) It is also possible to describe the class ${}_c\mathrm{BF}_{M,N}$ directly at level N (rather than going via the higher-level curves $Y(M, MN)$ as we have done). The curve $\mathrm{image}(\iota_{M,MN}) \subset Y(M, MN)^2$ maps down via $s_M \times s_M$ to a curve $C_{M,N} \subset Y_1(N)^2 \times \mu_M^\circ$, and our class can be characterised as the pushforward of a unit on $C_{M,N}$. However, the curve $C_{M,N}$ is rather messy (it can have many self-intersections, for instance), which makes it more difficult to prove the norm relation by this approach.

(ii) The compatibility of $U'(\ell)$ with pushforwards may seem like a minor point, but I want to emphasise it here, because this is the point where the proof breaks down in the case $\ell \nmid MN$. In this case, there is an operator $U'(\ell)$ on $Y(M, \ell MN)$, and an operator $T'(\ell)$ on $Y(M, MN)$, but these aren't compatible under π_*. So to complete the argument we would need to relate

$$(\pi \times \pi)_* \Big[(U'(\ell) \times U'(\ell)) \cdot {}_c\mathrm{REis}_{M, N\ell} \Big]$$

to the objects we know about on $Y(M, MN)$. This can be done – in fact there are at least three separate approaches – but it isn't easy. The eventual outcome is that for $\ell \nmid MN$ we have a formula

$$\mathrm{norm}_{\mathbf{Q}(\mu_M)}^{\mathbf{Q}(\mu_{\ell M})} ({}_c\mathrm{BF}_{\ell M, N}) = Q_\ell(\sigma_\ell^{-1}) \cdot {}_c\mathrm{BF}_{M,N},$$

where $Q_\ell(X)$ is a degree 4 polynomial with coefficients in the Hecke algebra. ◇

4.3. Projection to the (f, g) component

We now bring the eigenforms f and g into the picture. It's important to impose some local conditions at p. We take f and g to be eigenforms of some level N, with $p \mid N$, whose $U(p)$-eigenvalues α_f, α_g are p-adic units (we say f and g are *ordinary* at p).

REMARK. If we start with some form f of level N_0 with $p \nmid N_0$, then we replace f with one of the two $U(p)$-eigenforms of level $N = pN_0$ which have the same Hecke eigenvalues away from p. This process is called **p-stabilisation**. This doesn't change the Galois representations: the Galois representations attached to the p-stabilisations of f are isomorphic to that of the original form f, although they live on a different modular curve. ◇

The quotient

$$H^1_{\text{ét}}\left(Y_1(N)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p(1)\right) / \left\langle \begin{array}{c} T'(\ell) - a_\ell(f) \ \forall \ell \nmid N, \\ U'(\ell) - a_\ell(f) \ \forall \ell \mid N \end{array} \right\rangle$$

turns out to be isomorphic to the dual[1] V_f^* of V_f. The image of the cohomology with $\mathbf{Z}_p$-coefficients gives a lattice T_f^* in V_f^*. Doing this for both f and g, and combining this with the Hochschild–Serre spectral sequence, we get a projection map

$$\Pr_{f,g} : H^3_{\text{ét}}(Y_1(N) \times \mu_M^\circ, \mathbf{Z}_p(2)) \to H^1(\mathbf{Q}(\mu_M), T_f^* \otimes T_g^*).$$

By construction, the Hecke operator $U'(\ell) \times U'(\ell)$ on the source corresponds to multiplication by $\alpha_f \alpha_g$ on the target. This gives us the following theorem:

PROPOSITION 8. *The classes*

$$(\alpha_f \alpha_g)^{-r} \Pr_{f,g}({}_c\mathrm{BF}_{p^r,N,1}) \in H^1\left(\mathbf{Q}(\mu_{p^r}), T_f^* \otimes T_g^*\right)$$

are norm-compatible for $r \geq 1$. □

Notice that it's crucial that α_f, α_g are p-adic units, since otherwise these renormalised classes wouldn't land in $T_f^* \otimes T_g^*$ any more.

Exercise. Show that if $p \mid N$, then

$$\mathrm{cores}_{\mathbf{Q}}^{\mathbf{Q}(\mu_p)} \Pr_{f,g}({}_c\mathrm{BF}_{p,N}) = (\alpha_f \alpha_g - 1) \Pr_{f,g}({}_c\mathrm{BF}_{1,N}).$$

The exercise shows that the case $r = 0$ doesn't quite work; there is an unwanted Euler factor appearing, just as in the case of cyclotomic units. Exactly as in that case, we can get rid of this error term by re-defining the $r = 0$ class to be the norm of the $r = 1$ class. This gives an element of the module

$$H^1_{\text{Iw}}\left(\mathbf{Q}(\mu_{p^\infty}), T_f^* \otimes T_g^*\right) := \varprojlim_{r \geq 0} H^1\left(\mathbf{Q}(\mu_{p^r}), T_f^* \otimes T_g^*\right),$$

which is the *Iwasawa cohomology* of $T_f^* \otimes T_g^*$.

[1]The dual appears here because the $T'(\ell)$ are the adjoints of the $T(\ell)$ under Poincaré duality.

CHAPTER 5

Modular forms of higher weight

5.1. Galois representations

When we defined Galois representations attached to modular forms, we assumed that the modular forms has weight 2. Let's now see how this extends to other weights.

Assume now that f is a cuspidal modular eigenform of level $\Gamma_1(N)$ and weight $k+2$ for some $k \geq 0$. (We say that f has *cohomological weight*.) It turns out that we can still attach a Galois representation to f, but if $k > 0$, then we have to consider *étale cohomology with coefficients*.

It follows from Theorem 6 that there is a universal elliptic curve over $Y_1(N)$, say $\pi : \mathcal{E} \to Y_1(N)$. Denote by $\mathscr{H}$ the étale sheaf $V_p(\mathcal{E})$ on $Y_1(N)$; this is a locally constant sheaf of $\mathbf{Q}_p$-vector spaces of dimension 2, whose fibre at any geometric point x is canonically identified with the Tate module $V_p(\mathcal{E}_x)$ of the elliptic curve $\mathcal{E}_x/\overline{K}$.

Remark. We have a functor

$(\star)$ $\quad$ {algebraic representations of $\mathrm{GL}_2/\mathbf{Q}_p$} $\to$ {étale $\mathbf{Q}_p$-sheaves on $Y_1(N)$}.

The sheaf $\mathscr{H}$ is the image under this functor of the defining 2-dimensional representation of GL_2. $\diamond$

Definition. *We let $V_p(f)$ be the largest subspace of $H^1_{\text{ét}}(Y_1(N)_{\overline{\mathbf{Q}}}, \mathrm{Sym}^k \mathscr{H}(-k))$ on which the Hecke operators $T(\ell)$, for $\ell \nmid N$, act as multiplication by $a_\ell(f)$.*

Then $V_p(f)$ has the expected properties (generalising those we had above for $k = 0$):

(1) $V_p(f)$ is 2-dimensional and irreducible.
(2) $V_p(f)$ is a direct summand of $H^1_{\text{ét}}$ (not just a subspace).
(3) For $\ell \nmid pN$, $V_p(f)$ is unramified at ℓ and the the local Euler factor is
$$P_\ell(V_p(f), t) = 1 - a_\ell(f)t + \ell^{k+1}\chi(\ell)t^2.$$
(4) $V_p(f)^* = V_p(f \otimes \chi^{-1})(k+1)$.

Remark. There are also Galois representations attached to weight 1 modular forms, but these are harder to construct – they don't show up in étale cohomology with coefficients in any reasonable sheaf. $\diamond$

In much the same way, if we have a pair of integers $(k, k') \geq 0$ we can form a sheaf $\mathrm{Sym}^k \mathscr{H} \boxtimes \mathrm{Sym}^{k'} \mathscr{H}$ on $Y_1(N)^2$, and the tensor product $V(f) \otimes V(g)$, for f and g eigenforms of weight $k+2$ and $k'+2$, appears as a direct summand of the space
$$H^2_{\text{ét}}\left(Y_1(N)^2_{\overline{\mathbf{Q}}}, (\mathrm{Sym}^k \mathscr{H} \boxtimes \mathrm{Sym}^{k'} \mathscr{H})(-k-k')\right).$$

5.2. Eisenstein classes

The Kummer images of Siegel units give us classes in $H^1_{\text{ét}}(Y_1(N), \mathbf{Q}_p(1))$. What should our higher-weight analogues of this be?

It turns out that for any $k \geq 0$ and $N \geq 4$, and $c > 1$ coprime to $6pN$, there exists an *étale Eisenstein class*

$$ {}_c\operatorname{Eis}^k_{0,1/N} \in H^1_{\text{ét}}\left(Y_1(N), \operatorname{Sym}^k \mathscr{H}(1)\right),$$

which in the case $k = 0$ agrees with the Kummer-map image of the Siegel unit. These étale Eisenstein symbols satisfy similar basic relations (Theorem 7) to those of the Siegel units.

Remark. One can make sense of "motivic cohomology with coefficients in $\mathscr{H}$", and then one finds that these Eisenstein classes are the étale images of motivic Eisenstein classes, whose images under the Beilinson regulator are non-holomorphic Eisenstein series of weight $-k$. This is a higher-weight generalisation of the Kronecker limit formula, since for $k = 0$ the Beilinson regulator map on $H^1_{\text{mot}}(Y_1(N), \mathbf{Z}(1)) \cong \mathcal{O}(Y_1(N))^\times$ maps a unit u to the function $\log|u| : Y_1(N)(\mathbf{C}) \to \mathbf{R}$. ⋄

5.3. The Euler system for higher weight modular forms

We can adapt the above construction for pairs of modular forms of higher weight. Suppose that f and g have weights $k+2$ and $k'+2$ with $k, k' \geq 2$. Then it follows from Section 5.1, we need to construct classes in the cohomology groups

$$H^3_{\text{ét}}\left(Y_1(N) \times Y_1(N) \times \mu_m^\circ, \operatorname{Sym}^k \mathscr{H} \boxtimes \operatorname{Sym}^{k'} \mathscr{H}(n)\right),$$

for some appropriate $n \in \mathbf{Z}$, and these classes should arise via pushforward from the cohomology of $Y_1(N)$. Assume that $m = 1$, so we want to pushforward along the diagonal embedding $\iota : Y_1(N) \to Y_1(N)^2$. (Once we have understood this case, we can construct classes for $m > 1$ using the methods from the previous sections.)

5.3a. Pushforward with coefficients. It turns out that pushforward maps "work" with coefficients: there's a natural map

$$\iota_* : H^1_{\text{ét}}\left(Y_1(N), \iota^*(\mathscr{L})(1)\right) \to H^3_{\text{ét}}\left(Y_1(N)^2, \mathscr{L}(2)\right)$$

for any étale sheaf $\mathscr{L}$, with the case above being $\mathscr{L}$ the constant sheaf $\mathbf{Q}_p$. Here $\iota^*\mathscr{L}$ is just the pullback of $\mathscr{L}$ to $Y_1(N)$. So what does the sheaf $\iota^*\left(\operatorname{Sym}^k \mathscr{H} \boxtimes \operatorname{Sym}^{k'} \mathscr{H}\right)$ look like?

Since $\mathscr{H}$ and its symmetric powers arise from irreducible algebraic representations of GL_2, we can use group theory to answer this question. Let V denote the standard 2-dimensional $\mathbf{Q}_p$-representation of GL_2. Then the sheaf $\operatorname{Sym}^k \mathscr{H} \boxtimes \operatorname{Sym}^{k'} \mathscr{H}$ on $Y_1(N)^2$ arises from the irreducible representation $\operatorname{Sym}^k V \boxtimes \operatorname{Sym}^{k'} V$ of $G := \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2$. If $H \subset G$ denotes the diagonally-embedded copy of GL_2, then the restriction of this G-representation to H breaks up as a sum of irreducible H-representations; and we have a corresponding decomposition of the pullback $\iota^*\left(\operatorname{Sym}^k \mathscr{H} \boxtimes \operatorname{Sym}^{k'} \mathscr{H}\right)$ in the category of sheaves on $Y_1(N)$.

REMARK. A posh way of stating this compatibility is that we have a commutative diagram of functors

$$\begin{array}{ccc} \mathrm{Rep}_G & \longrightarrow & \text{sheaves}/Y_1(N)^2 \\ \Big\downarrow{\scriptstyle \mathrm{res}^G_H} & & \Big\downarrow{\scriptstyle \iota^*} \\ \mathrm{Rep}_H & \longrightarrow & \text{sheaves}/Y_1(N) \end{array}$$

where Rep_G and Rep_H are the categories of representations of G and its subgroup H, res^G_H is restriction of representations, and the horizontal arrows are the functors $(\star)$ for G and H. An analogue of this naturality property has been established for motivic cohomology in recent works of Ancona and Torzewski. ◇

The decomposition of $\mathrm{res}^G_H\left(\mathrm{Sym}^k V \boxtimes \mathrm{Sym}^{k'} V\right) = \mathrm{Sym}^k V \otimes \mathrm{Sym}^{k'} V$ into irreducible representations of H is described by the *Clebsch–Gordan formula*:

$$\mathrm{Sym}^k V \otimes \mathrm{Sym}^{k'} V = \bigoplus_{j=0}^{\min\{k,k'\}} \mathrm{Sym}^{k+k'-2j} V \otimes \det{}^j,$$

so for every $0 \le j \le \min\{k,k'\}$, we have a GL_2-equivariant map

$$\mathrm{Sym}^{k+k'-2j} V \otimes \det{}^j \longrightarrow \iota^*\left(\mathrm{Sym}^k V \boxtimes \mathrm{Sym}^{k'} V\right).$$

The representation $\det^j$ of GL_2 corresponds to the sheaf $\mathbf{Q}_p(j)$, so this means that for every $0 \le j \le \min\{k,k'\}$ we get a map of sheaves on $Y_1(N)$,

$$\mathrm{Sym}^{k+k'-2j} \mathscr{H} \longrightarrow \iota^*\left(\mathrm{Sym}^k \mathscr{H} \boxtimes \mathrm{Sym}^{k'} \mathscr{H}(-j)\right),$$

which induces a map in étale cohomology

$$\iota_* : H^1_{\text{ét}}\left(Y_1(N), \mathrm{Sym}^{k+k'-2j} \mathscr{H}(1)\right) \longrightarrow H^3_{\text{ét}}\left(Y_1(N)^2, \mathrm{Sym}^k \mathscr{H} \boxtimes \mathrm{Sym}^{k'} \mathscr{H}(2-j)\right).$$

5.3b. Definition of the classes. As we saw above, there is a special element in $H^1_{\text{ét}}\left(Y_1(N), \mathrm{Sym}^{k+k'-2j} \mathscr{H}(1)\right)$, the étale Eisenstein class ${}_c\,\mathrm{Eis}^{(k+k'-2j)}_{0,1/N} \in H^1_{\text{ét}}\left(Y_1(N), \mathrm{Sym}^{k+k'-2j} \mathscr{H}(1)\right)$.

DEFINITION. *Let $0 \le j \le \min\{k,k'\}$. We define the Rankin–Eisenstein class*

$${}_c\,\mathrm{REis}^{(k,k',j)}_{1,N} = \iota_*\left({}_c\,\mathrm{Eis}^{(k+k'-2j)}_{0,1/N}\right),$$

which is an element of $H^3_{\text{ét}}\left(Y_1(N)^2, \mathrm{Sym}^k \mathscr{H} \boxtimes \mathrm{Sym}^{k'} \mathscr{H}(2-j)\right)$.

Using the same methods as in Sections 4.1c and 4.1d, we more generally define Rankin–Eisenstein classes ${}_c\,\mathrm{REis}^{(k,k',j)}_{M,N}$ for $M|N$; and (finally) Beilinson–Flach classes

$${}_c\,\mathrm{BF}^{(k,k',j)}_{m,N} \in H^3_{\text{ét}}\left(Y_1(N)^2 \times \mu_m^\circ, \mathrm{Sym}^k \mathscr{H} \otimes \mathrm{Sym}^{k'} \mathscr{H}(2-j)\right)$$

as the image of ${}_c\,\mathrm{REis}^{(k,k',j)}_{m,mN}$ under the map[1] $(s_m \times s_m)_*$.

[1]One needs to be a bit careful here with extending s_m to a map on cohomology with coefficients, but we don't discuss this issue here. For reference, see [**KLZ17**, §6.1].

Now let f and g be eigenforms of weights $k+2, k'+2 \geq 2$ with $k, k' \geq 0$ and level N, where $p \mid N$, both of which are ordinary at p. It then follows from Section 5.1 and the arguments in Section 4.3 that we have a projection map

$$\Pr{}_{f,g} : H^3_{\text{ét}}\left(Y_1(N)^2 \times \mu_m^\circ, \operatorname{Sym}^k \mathscr{H} \otimes \operatorname{Sym}^{k'} \mathscr{H}(2-j)\right) \longrightarrow H^1(\mathbf{Q}(\mu_m), (V_f \otimes V_g)^*(-j)),$$

and as in the parallel weight 2 case one can show that the images of the Beilinson–Flach classes $\left({}_c\,\mathrm{BF}^{(k,k',j)}_{m,N}\right)_{m \geq 1}$ under this projection map have the same properties under corestriction maps as in Proposition 8.

Remark. We also have to check that these objects land in a $\mathbf{Z}_p$-lattice independent of m. To do this, we need to find good integral lattices in $\operatorname{Sym}^k \mathscr{H}$. There is a natural $\mathbf{Z}_p$-lattice subsheaf $\mathscr{H}_{\mathbf{Z}_p} \subset \mathscr{H}$, but a small complication arises because with $\mathbf{Z}_p$-coefficients the Sym^k functor is not compatible with duality unless $p > k$. To repair this one has to introduce a slightly different sheaf, the sheaf $\operatorname{TSym}^k \mathscr{H}_{\mathbf{Z}_p}$ of symmetric tensors, which is only isomorphic to $\operatorname{Sym}^k \mathscr{H}_{\mathbf{Z}_p}$ if $p > k$. ◇

5.4. Twist-compatibility

The upshot of this construction is that for a fixed pair of forms f and g, we have not one but $1 + \min\{k, k'\}$ *different* Euler systems, which live in different cyclotomic twists of the representation $V_f^* \otimes V_g^*$. However, as we've seen above, Soulé's twisting construction gives an isomorphism between the space of Euler systems for V and for $V(m)$ for any $m \in \mathbf{Z}$, so it makes sense to compare these Euler systems to each other.

Theorem 13. *The Beilinson–Flach Euler systems associated to different values of j in the range $0 \leq j \leq \min\{k, k'\}$ are all compatible under the Soulé twist.*

This simple-looking statement turns out to be deceptively hard. See [**KLZ17**, §6].

Remark. A similar issue arises for Kato's Euler system associated to a single modular form, and in this case one even has *infinitely many* potentially different Euler systems! More precisely, for a weight 2 form f, one can use cup-products of two weight n Eisenstein classes, for any $n \geq 0$, to construct an Euler system with values in $V_p(f)^*(1+n)$.

Naturally, one expects that the Euler system thus constructed for any $n \geq 1$ should coincide with the n-th Soulé twist of the $n = 0$ Euler system. This was checked in the PhD thesis of Matthew Gealy [**Gea06**]. ◇

5.5. An adelic modification

Just in order to motivate some of the constructions we'll use in later chapters, it's worth pointing out that one can make a slight modification to the construction. Since we have defined our modular curves $Y(U)$ as quotients of $\mathrm{GL}_2(\mathbf{A}_f) \times \mathcal{H}$ (c.f. (1)), where $\mathbf{A}_f$ are the finite adéles, we have a (right) action of the normaliser of $\mathrm{GL}_2(\mathbf{A}_f)$ on the tower of curves $Y(U)$ for varying U. This is compatible with the

action of $\mathrm{GL}_2^+(\mathbf{Q}) \subset \mathrm{GL}_2(\mathbf{A}_f)$ via Möbius transformations on $\mathcal{H}$, after modifying by an inverse to interchange left and right actions.

With these conventions, we can define our Hecke operators, and our degeneracy maps τ_ℓ, s_M etc, using elements of $\mathrm{GL}_2(\mathbf{A}_f)$ which are the identity outside the place ℓ. This does not change anything major (the difference between the "old" and "new" elements is given by the action of an element of $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$) but the adelic presentation makes it a little easier to leverage results from representation theory.

CHAPTER 6

An Euler system for Siegel modular forms

We will describe the construction of the Euler system using the adelic approach, as described in Section 5.5. This is consistent with the approach taken in the main reference for this chapter [**LSZ17**].

6.1. Siegel modular 3-folds

DEFINITION. *Let J be the skew-symmetric 4×4-matrix $\begin{pmatrix} & & 1 & \\ & & & 1 \\ -1 & & & \\ & -1 & & \end{pmatrix}$. Define* GSp_4 *to be the group scheme over* $\mathbf{Z}$ *such that for any* $\mathbf{Z}$*-algebra* R*, we have*

$$\mathrm{GSp}_4(R) = \{(g,\nu) \in \mathrm{GL}_4(R) \times R^\times : gJg^t = \nu J\}.$$

We let Sp_4 *be the subgroup of elements with* $\nu = 1$*.*

The group $\mathrm{GSp}_4^+(\mathbf{R})$ (the elements of $\mathrm{GSp}_4(\mathbf{R})$ with $\nu > 0$) acts on the genus 2 Siegel upper half space

$$\mathcal{H}_2 = \{Z \in M_2(\mathbf{C}) : Z = \left(\begin{smallmatrix} y & z \\ x & y \end{smallmatrix}\right), \quad \Im(\left(\begin{smallmatrix} x & y \\ y & z \end{smallmatrix}\right)) \text{ is positive definite}\}$$

via $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \cdot Z = (AZ+B)(CZ+D)^{-1}$.

REMARK. If we use a slightly different model of GSp_4, as matrices satisfying $gJ'g^t = \nu J'$ where $J' = \left(\begin{smallmatrix} & I_2 \\ -I_2 & \end{smallmatrix}\right)$, then we can define $\mathcal{H}_2$ more tidily, as the space of symmetric complex matrices with positive-definite imaginary part. However, defining GSp_4 using the anti-diagonal matrix J, as we have done, is more convenient for representation theory (as the intersection of GSp_4 with the upper-triangular matrices in GL_4 is a Borel subgroup). ◇

If U is an open compact subgroup of $\mathrm{GSp}_4(\mathbf{A}_f)$, then we can define the double quotient

$$\tilde{Y}(U) = \mathrm{GSp}_4^+(\mathbf{Q}) \backslash \left(G(\mathbf{A}_f) \times \mathcal{H}_2\right) / U.$$

This is a 3-dimensional complex manifold, with finitely many components, each of which looks like $\Gamma\backslash\mathcal{H}_2$ for some discrete subgroup $\Gamma \subset \mathrm{Sp}_4(\mathbf{Q})$.

THEOREM 14. *If U is sufficiently small, then $\tilde{Y}(U)$ is the $\mathbf{C}$-points of a smooth algebraic variety $\tilde{Y}(N)$ defined over $\mathbf{Q}$ (a* Siegel 3-fold*), which is a moduli space for principally polarised abelian surfaces with some level structure.*

Of course, the kind of level structure that emerges depends on the group U we choose. A particularly important case is when

$$U = U_1(N) \coloneqq \{(g,\nu) \in \mathrm{GSp}_4(\hat{\mathbf{Z}}) : g = \left(\begin{smallmatrix} * & * \\ 0_2 & I_2 \end{smallmatrix}\right) \bmod N\}$$

(where 0_2 and I_2 are the 2×2 zero and identity matrices respectively). The corresponding threefold $\tilde{Y}_1(N)$ parametrises triples (A, λ, P, Q) where A is an abelian surface, λ is a principal polarisation on A, and $P, Q \in A[N]$ are two points of exact order N satisfying $\langle P, Q\rangle = 0$ (where $\langle , \rangle$ is the Weil pairing induced by the polarisation λ).

As in the case of modular curves, we can identify the basechange $\tilde{Y}_1(N) \times \mu_m^\circ$ with a Shimura variety $\tilde{Y}(U)$ for some modified level m. More precisely, if we let

$$\mathcal{U} = \{(g, \nu) \in U_1(N) : \nu = 1 \bmod m\}$$

then $\tilde{Y}(\mathcal{U})$ is canonically isomorphic to $\tilde{Y}_1(N) \times \mu_m^\circ$ as a $\mathbf{Q}$-variety.

REMARK. In terms of moduli spaces, the projection to μ_m° is given by the Weil pairing. ◇

6.2. Genus 2 Siegel modular forms

References: van der Geer's article [**vdG08**] is an excellent introduction; more details (particularly on Hecke operators) can be found in Andrianov's book [**And87**].

6.2a. Definitions.

DEFINITION. *Let $\tilde{\Gamma}_1(N) = \mathrm{Sp}_4(\mathbf{Z}) \cap \tilde{U}_1(N)$. A Siegel modular form of genus 2, level N and weight (k, k) is a holomorphic function $\mathcal{F} : \mathcal{H}_2 \to \mathbf{C}$ such that $\mathcal{F}(g \cdot Z) = \det(CZ + D)^k \mathcal{F}(Z)$ for all $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \tilde{\Gamma}_1(N)$ and $Z \in \mathcal{H}_2$. We write $M^{(2)}_{k,k}(\tilde{\Gamma}_1(N))$ for the space of such functions.*

Note the similarity to the familiar definition of modular forms (which are automorphic forms for $\mathrm{GSp}_2 \cong \mathrm{GL}_2$).

REMARK. There is a more general notion of Siegel modular forms of weight (k_1, k_2) for integers $k_1 \geq k_2$; these are holomorphic functions on $\mathcal{H}_2$, taking values the space $\mathbf{C}^{k_1 - k_2 + 1}$, and the transformation law involves the action of $CZ + D$ via the representation $\mathrm{Sym}^{k_1 - k_2} \otimes \det^{k_2}$ of $\mathrm{GL}_2(\mathbf{C})$. When $k_1 > k_2$ these are sometimes called *vector-valued Siegel modular forms*, and the forms for $k_1 = k_2$ are called *scalar-valued*. ◇

As for usual modular forms, the space $M^{(2)}_{k_1,k_2}(\tilde{\Gamma}_1(N))$ is finite-dimensional over $\mathbf{C}$, and has a subspace $S^{(2)}_{k_1,k_2}(\tilde{\Gamma}_1(N))$ of *cuspidal* forms.

6.2b. Hecke operators.

We can also describe $M^{(2)}_{k_1,k_2}(\tilde{\Gamma}_1(N))$ and $S^{(2)}_{k_1,k_2}(\tilde{\Gamma}_1(N))$ adelically, using the isomorphism

$$\tilde{\Gamma}_1(N) \backslash \mathcal{H}_2 \cong \mathrm{GSp}_4^+(\mathbf{Q}) \backslash \left(\mathrm{GSp}_4(\mathbf{A}_f) \times \mathcal{H}_2\right) / U_1(N).$$

From this interpretation, we get an action on these spaces of the *Hecke algebra* of double cosets $U_1(N) g U_1(N)$, $g \in \mathrm{GSp}_4(\mathbf{A}_f)$. This decomposes as a product of local Hecke algebras for each prime ℓ.

For $\ell \nmid N$, the local Hecke algebra is generated by three operators $T(\ell)$, $T_1(\ell^2)$, and $R(\ell)$, corresponding to the double cosets of $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ell & \\ & & & \ell \end{pmatrix}$, $\begin{pmatrix} 1 & & & \\ & \ell & & \\ & & \ell & \\ & & & \ell^2 \end{pmatrix}$, and $\begin{pmatrix} \ell & & & \\ & \ell & & \\ & & \ell & \\ & & & \ell \end{pmatrix}$

(considered as elements of $\mathrm{GSp}_4(\mathbf{Q}_\ell) \subset \mathrm{GSp}_4(\mathbf{A}_f)$, with components at all places other than ℓ being the identity).

DEFINITION. *If $\mathcal{F} \in S^{(2)}_{k_1,k_2}(\tilde{\Gamma}_1(N))$ is an eigenform for the above three operators, with eigenvalues $t(\ell), t_1(\ell^2), r(\ell)$ respectively, then the* spin L-factor *of $\mathcal{F}$ at ℓ is the degree 4 polynomial*

$$P_{\mathrm{spin},\ell}(\mathcal{F}, X) = 1 - t(\ell)X + \ell\Big(t_1(\ell^2) + (\ell^2+1)r(\ell)\Big)X^2 - \ell^3 t(\ell) r(\ell) X^3 + \ell^6 r(\ell)^2 X^4.$$

(Often we work with the renormalised polynomial $P_{\mathrm{spin},\ell}(\mathcal{F}, \ell^{-3/2}X)$, which has the advantage that its roots all have absolute value 1.)

This is, of course, crying out to be made into an Euler product

$$L_{\mathrm{spin}}(\mathcal{F}, s) = \prod_{\ell \text{ prime}} P_{\mathrm{spin},\ell}\left(\mathcal{F}, \ell^{-s-\frac{3}{2}}\right)^{-1},$$

the *spin L-function* of $\mathcal{F}$, although this only makes sense if we have a good definition of the local factors at primes $\ell \mid N$. Under some mild hypotheses on $\mathcal{F}$, a suitable recipe for these factors was found by Piatetski-Shapiro and Novodvorsky in the 1970s (although not published until 1997 [**PS97**]), and they showed that the resulting function has meromorphic continuation with a functional equation of the form $s \mapsto 1 - s$.

REMARK. As well as the spin L-function, there is another L-function associated to $\mathcal{F}$, confusingly called the *standard L-function*, given by a different Euler product in which the local factors at the good primes are reciprocals of polynomials in ℓ^{-s} of degree 5. The terminology "standard" is unfortunate for GSp_4, since the spin L-function is a much more fundamental object than the standard one, but it reflects the fact that the standard L-function generalises more easily to GSp_{2n} for general n. ◇

6.3. Galois representations

Let $\mathcal{F}$ be a genus 2 cuspidal Siegel modular form of weight $(3,3)$ and level N which is an eigenform for the Hecke operators away from N. The following result shows that one can associate to $\mathcal{F}$ a Galois representation.

THEOREM 15 (Weissauer, [**Wei05**]). *There exists a finite extension E of $\mathbf{Q}_p$ and a 4-dimensional Galois representation $V_{\mathcal{F}}$ over E, such that for all primes ℓ coprime to pN we have*

$$\det\left(1 - X\,\mathrm{Frob}_\ell^{-1} \;\middle|\; V_{\mathcal{F}}\right) = P_{\mathrm{spin},\ell}\left(\mathcal{F}, X\right).$$

Perhaps surprisingly, these representations aren't always irreducible, even if $\mathcal{F}$ is cuspidal. This is because there are certain special types of cuspidal Siegel eigenforms that are "lifts" of automorphic forms on smaller groups; these are said to be *endoscopic*. There are several types of these, but only two which can occur in weight $(3,3)$, namely *Yoshida lifts* and *Saito–Kurokawa lifts*.

If $\mathcal{F}$ is non-endoscopic, and p is large enough[1] then the representation $V_{\mathcal{F}}$ is irreducible.

[1]It's expected to be irreducible for all p, but this is only known if we assume that $p \geq 5$ and $p \nmid N$.

THEOREM 16. *If $\mathcal{F}$ is non-endoscopic, then $V_{\mathcal{F}}$ appears in the etale cohomology of the level N Siegel 3-fold. More precisely, we have a projection map*

$$\mathrm{Pr}_{\mathcal{F}} : H^3_{\text{ét}}\left(\tilde{Y}_1(N)_{\overline{\mathbf{Q}}}, \mathbf{Q}_p(3)\right) \otimes E \longrightarrow\!\!\!\!\!\rightarrow V_{\mathcal{F}}^*.$$

We can similarly construct Galois representations for Siegel modular forms of weight (k_1, k_2) whenever $k_1 \geq k_2 \geq 3$, using étale cohomology with coefficients in sheaves coming from algebraic representations of the group GSp_4.

REMARK. Note that weight $(2, 2)$ forms are not cohomological – they still have spin Galois representations, but these can't be seen in the cohomology of the Siegel threefold. This is unfortunate, since there is a conjecture due to Brumer and Kramer, the *Paramodular Conjecture*, predicting that (certain) abelian surfaces over $\mathbf{Q}$ correspond to Siegel eigenforms of weight $(2, 2)$. It would be very interesting to try to build Euler systems for these non-cohomological eigenforms, by deforming the constructions of this chapter in a p-adic family. ◇

6.4. Lemma-Flach elements

References: [**Lem15, Lem17, LSZ17**].

6.4a. Strategy. As we have seen above, the spin Galois representation of a genus 2 Siegel modular form can be found in the étale cohomology of the Siegel 3-fold $\tilde{Y}_1(N)$, for a suitable N. We therefore want to construct cohomology classes in $H^4_{\text{ét}}(\tilde{Y}_1(N) \times \mu_m^\circ, \mathbf{Z}_p(3))$ for $m \geq 1$, satisfying norm-compatibility relations as m changes (for a fixed N).

To do this, we note that we have a natural embedding

$$\iota : \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2 \longrightarrow \mathrm{GSp}_4,$$

which is given explicitly by

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] \mapsto \begin{pmatrix} a & & & b \\ & a' & b' & \\ & c' & d' & \\ c & & & d \end{pmatrix}.$$

This embedding induces a map from the product of two modular curves into a Siegel 3-fold with compatible level structures; for instance, we get maps

$$Y_1(N) \times Y_1(N) \to \tilde{Y}_1(N),$$

which are injective if N is large enough. This in turn induces a pushforward map on the étale cohomology groups

$$\iota_* : H^i_{\text{ét}}(Y_1(N)^2, \mathbf{Z}_p(j)) \longrightarrow H^{i+2}(\tilde{Y}_1(N), \mathbf{Z}_p(j+1)).$$

Consider the case when $i = j = 2$: Then the exterior cup product of two Siegel units ${}_c g_{0,1/N} \sqcup {}_d g_{0,1/N}$ defines an element of $H^2_{\text{ét}}(Y_1(N)^2, \mathbf{Z}_p(2))$, and we define the *Lemma–Flach element* for $m = 1$ to be

$${}_{c,d}\,\mathrm{LF}_{1,N} = \iota_*({}_c g_{0,1/N} \sqcup {}_d g_{0,1/N}).$$

6.4b. Motivation: integral formulae. As in Chapter 3 above, there is a good motivation for why this class ${}_{c,d}\,\mathrm{LF}_{1,N}$ should be interesting.

There is an integral formula for the spin L-function of GSp_4, which is due to Piatetskii-Shapiro. If $\mathcal{F}$ is a non-endoscopic, holomorphic eigenform of weight $(3,3)$ (or of any cohomological weight), then we can consider the integral

$$\int_{(\Gamma_1(N)\backslash\mathcal{H})^2} E(\tau_1,s)E(\tau_2,s)\mathcal{F}(\tau_1,\tau_2)\mathrm{d}A$$

where $E(\tau,s)$ is a suitably-chosen family of Eisenstein series, and $\mathrm{d}A = \frac{\mathrm{d}\tau_1\wedge\mathrm{d}\bar{\tau}_1\wedge\mathrm{d}\tau_2\wedge\mathrm{d}\bar{\tau}_2}{\Im(\tau_1)\Im(\tau_2)}$ is the invariant measure on $(\Gamma_1(N)\backslash\mathcal{H})^2$. The general theory tells us that this unfolds into a product of local integrals, and the local integral at a finite place computes the spin L-factor.

The problem is that the local integral at ∞ is always zero! This can be fixed by replacing the holomorphic eigenform $\mathcal{F}$ with an "evil twin" $\mathcal{F}^g$, which is a real-analytic but non-holomorphic function on $\tilde{Y}_1(N)(\mathbf{C})$ with the same Hecke eigenvalues as $\mathcal{F}$; this doesn't change the local integrals at the finite places, but gives us a non-vanishing archimedean integral.

As in the Rankin–Selberg setting, the Lemma–Flach class we've defined is naturally the image under the étale regulator of a motivic cohomology class. The main result of [**Lem17**] shows that the Beilinson regulator of this motivic class, paired with an appropriate differential on $\tilde{Y}_1(N)(\mathbf{C})$ coming from $\mathcal{F}^g$, gives Piatetskii-Shapiro's integral for $L_{\mathrm{spin}}(\mathcal{F},s)$ at $s=-\frac{1}{2}$.

Remark. The g stands for "generic". Representation-theoretically, the problem is that the discrete-series representations of $\mathrm{GSp}_4(\mathbf{R})$ come in pairs ("local L-packets"), consisting of a holomorphic representation and a non-holomorphic one, and it is the non-holomorphic one which is generic (admits a Whittaker model) and thus can contribute to the integral formula.

One can also replace $Y_1(N)\times Y_1(N)$ with a symmetric space associated to GL_2/K, where K is an imaginary quadratic field; this gives an alternative integral representation which does involve the holomorphic eigenform $\mathcal{F}$. However, it seems to be impossible to interpret this integral as the regulator of a motivic cohomology class, since the symmetric space for GL_2/K is not an algebraic variety. ◇

6.4c. Lemma–Eisenstein classes. Our task is now to extend this to an Euler system: that is, to define classes ${}_{c,d}\,\mathrm{LF}_{m,N}$ for $m>1$ satisfying good norm-compatibility properties. As before, we'll start by defining classes on higher-level modular varities, which are easier to work with, and proving norm-compatibility relations for these auxiliary classes.

Let us define $\mathcal{U}(M,N) = \left\{\gamma\in\mathrm{GSp}_4(\hat{\mathbf{Z}}) : \gamma = \left(\begin{smallmatrix} I_2 & 0_2 \\ 0_2 & I_2\end{smallmatrix}\right) \bmod \left(\begin{smallmatrix} M & M \\ N & N\end{smallmatrix}\right)\right\}$, and $\tilde{Y}(M,N)$ the corresponding Siegel threefold.

Lemma 1. *If $M|N$, the group $\mathcal{U}(M,N)$ is normalised by the element $u = \begin{pmatrix} 1 & & 1 & \\ & 1 & & 1 \\ & & 1 & \\ & & & 1\end{pmatrix}$.*

Define $\iota_{M,N} : Y(M,N)^2 \to \tilde{Y}(M,N)$ to be the composite

$$Y(M,N)^2 \xhookrightarrow{\iota} \tilde{Y}(M,N) \xrightarrow{u} \tilde{Y}(M,N).$$

Here, $Y(M,N)^2$ denotes as above the fibre product of two copies of $Y(M,N)$ over μ°_M.

DEFINITION. *The Lemma-Eisenstein class* ${}_{c,d}\,\mathrm{LEis}_{M,N}$ *is the image of* ${}_cg_{0,1/N} \sqcup {}_dg_{0,1/N}$ *under* $(\iota_{M,N})_*$. *Here, we regard* ${}_cg_{0,1/N} \sqcup {}_dg_{0,1/N}$ *as an element of* $H^2_{\text{ét}}(Y(M,N)^2, \mathbf{Z}_p(2))$ *via pullback.*

6.4d. Norm relations. Exactly as before, one sees straightforwardly that the Lemma–Eisenstein classes satisfy norm relations as N changes.

PROPOSITION 9. *Suppose that* $M|N$ *and* ℓ *is a prime with* $\ell \mid N$. *Then*

$$(\mathrm{pr}_1)_*({}_{c,d}\,\mathrm{LEis}_{M,\ell N}) = {}_{c,d}\,\mathrm{LEis}_{M,N},$$

where pr_1 *is the natural quotient map* $\tilde{Y}(M,N\ell) \to \tilde{Y}(M,N)$. □

(*Exercise*: formulate and prove a similar formula for $\ell \nmid N$.)

The second norm relation: changing M. Let us write τ_ℓ for the "non-standard" degeneracy map $\tilde{Y}(\ell M, N)$ to $\tilde{Y}(M,N)$, given by the right-translation action of $\begin{pmatrix} \ell & & & \\ & \ell & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \in \mathrm{GSp}_4(\mathbf{Q}_\ell) \subset \mathrm{GSp}_4(\mathbf{A}_f)$. Note that τ_ℓ factors as

$$\tilde{Y}(\ell M, N) \longrightarrow \tilde{Y}(M(\ell), N) \xrightarrow{\tilde{\pi}_{2,\ell}} \tilde{Y}(M,N),$$

where the first map is the natural degeneracy map.

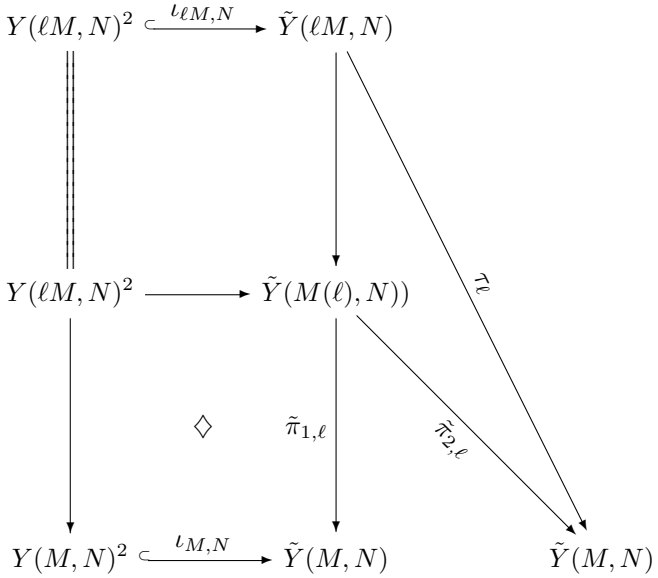
THEOREM 17. *Suppose* $\ell|M$ *and* $\ell M \mid N$. *Then we have*

$$(\tau_\ell)_* \left({}_{c,d}\,\mathrm{LEis}_{\ell M,N}\right) = \mathcal{U}'_\ell \cdot {}_{c,d}\,\mathrm{LEis}_{M,N}\,.$$

Here, $\mathcal{U}'_\ell$ *is the Hecke correspondence on* $\tilde{Y}(M,N)$ *given by the element of* $\mathrm{GSp}_4(\mathbf{A}_f)$ *which is* $\begin{pmatrix} \ell & & & \\ & \ell & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$ *at* ℓ, *and the identity elsewhere.*

REMARK. Again, there is a similar but slightly more complicated formula in the case when $\ell \nmid M$ (but still $\ell M \mid N$). ◇

PROOF. We erect the following commutative diagram, in which all vertical arrows are the natural degeneracy maps:



We claim that the middle arrow is actually injective. This is equivalent to the claim that

$$H(\mathbf{A}_f) \cap u\tilde{U}(M(\ell), N)u^{-1} = U(M\ell, N)^2,$$

which is an easy matrix computation.

When $\ell \mid M$, we see that the square marked $\diamondsuit$ has both horizontal arrows closed immersions, and both vertical arrows of degree ℓ^3. So it is Cartesian, and we may conclude that the image of ${}_{c,d}\,\mathrm{LEis}_{\ell M,N}$ under pushforward to $\tilde{Y}(M(\ell), N)$ coincides with the pullback of ${}_{c,d}\,\mathrm{LEis}_{M,N}$. The result now follows by pushing both of these elements forward along the diagonal arrow and observing that $\mathcal{U}'_\ell = (\tilde{\pi}_{2,\ell})_* \circ (\tilde{\pi}_{1,\ell})^*$. □

6.4e. Lemma-Flach classes and their norm relations. Let $m \geq 1$. We let ϖ_m denote the element of $\mathbf{A}_f^\times$ whose ℓ-th component is $\ell^{v_\ell(m)}$. Then right translation by the element $\begin{pmatrix} \varpi_m & & & \\ & \varpi_m & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \in \mathrm{GSp}_4(\mathbf{A}_f)$ induces a map

$$s_m : \tilde{Y}(m, mN) \to \tilde{Y}_1(N) \times \mu_m^\circ.$$

DEFINITION. *We define the Lemma-Flach element* ${}_{c,d}\,\mathrm{LF}_{m,N}$ *to be the image of* ${}_{c,d}\,\mathrm{LEis}_{m,mN}$ *under* $(s_m)_*$.

THEOREM 18. *Let* ℓ *be prime such that* $\ell | M$ *and* $\ell | N$. *Then we have*

$$\mathrm{norm}_{\mathbf{Q}(\mu_m)}^{\mathbf{Q}(\mu_{\ell m})} ({}_{c,d}\,\mathrm{LF}_{\ell m,N}) = \mathcal{U}'_\ell \cdot {}_{c,d}\,\mathrm{LF}_{m,N}\,.$$

PROOF. Analogous to the proof of the corresponding statement for Beilinson–Flach elements. □

CHAPTER 7

Projects

7.1. An Euler system for $\mathrm{GSp}_4 \times \mathrm{GL}_2$

The goal of this project is to construct an Euler system for the Galois representations appearing in the cohomology of a certain 4-dimensional Shimura variety: namely, the product of a Siegel modular threefold and a modular curve.

The underlying Rankin–Selberg formula (in the sense of Section 3.3) was proven by Novodvorsky [**Nov79**]: it uses the embedding $\iota : \mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2 \hookrightarrow \mathrm{GSp}_4 \times_{\mathrm{GL}_1} \mathrm{GL}_2$ given by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \mapsto \left[\begin{pmatrix} a & & & b \\ & a' & b' & \\ & c' & d' & \\ c & & & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right].$$

Novodvorsky's formula expresses values of the degree 8 L-function of an automorphic form $\mathcal{F}$ for $\mathrm{GSp}_4 \times_{\mathrm{GL}_1} \mathrm{GL}_2$ in terms of an integal over $\mathrm{GL}_2 \times_{\mathrm{GL}_1} \mathrm{GL}_2$; roughly, one integrates $\iota^*(\varpi_{\mathcal{F}})$, where $\varpi_{\mathcal{F}}$ is a certain differential associated to $\mathcal{F}$, against an Eisenstein series on the first GL_2 factor of $\mathrm{GL}_2 \times \mathrm{GL}_2$.

The corresponding Euler system should roughly be constructed as follows: let Y be a modular curve, and let g_Y be a Siegel unit on Y. Its image under the Kummer map $\kappa_p(g_Y)$ is an element of $H^1_{\text{ét}}(Y, \mathbf{Q}_p(1))$. We can regard it as an element of $H^1_{\text{ét}}(Y \times Y, \mathbf{Q}_p(1))$ via pullback along the natural projection map $Y \times Y \to Y$ onto the first factor. Then the bottom class of the Euler system (with trivial coefficients) should be given by

$$\iota_*(\kappa_p(g_Y)) \in H^5_{\text{ét}}(S \times Y, \mathbf{Q}_p(3)),$$

where S denotes a Siegel 3-fold of a suitable level.

Remark. As in Section 3.3, this is visibly the étale regulator of a motivic class, whose Beilinson regulator is a special value of Novodvorsky's integral. ◇

The aim of the project is to show that the methods of Chapters 4 and 6 can be adapted to give an Euler system of $\mathrm{GSp}_4 \times \mathrm{GL}_2$.

This project has several sub-projects, which are to some extent orthogonal (so it would be suitable for a fairly large team):

- Writing down the relevant cohomology classes over the cyclotomic extensions of $\mathbf{Q}$, using suitable level structures on Y and S.
- Proving norm-compatibility statements in the "vertical" aspect (i.e. proving a relation under the Galois corestriction map for the the classes over $\mathbf{Q}(\mu_{p^{n+1}})$ and $\mathbf{Q}(\mu_{p^n})$ where p is a prime and $n \geq 1$). This ought to be

possible using a "Cartesian square" diagram analogous to those we had above for the Beilinson–Flach and Lemma–Flach elements.

- Proving the "horizontal" (or *tame*) norm relation (i.e. proving a relation under the Galois corestriction map for the classes over $\mathbf{Q}(\mu_{m\ell})$ and $\mathbf{Q}(\mu_m)$, where ℓ is a prime *not dividing* m. This is a rather more difficult problem, since extra Euler factors make an appearance, and we did not discuss it in these lecture notes. In [**LLZ14**] and [**KLZ17**], we proved these norm relations by explicit computations, but this method does not generalize easily. A different and much more flexible approach for proving the tame norm relations (using local zeta integrals) was developed in the GSp_4-case in [**LSZ17**, §§3, 10], and this strategy should generalize[1] to $\mathrm{GSp}_4 \times \mathrm{GL}_2$.
- studying the case of higher weights (i.e. determining for which coefficient systems $\mathscr{F}$ on $S \times Y$ one can construct elements in $H^5_{\text{ét}}(S \times Y, \mathscr{F}(3))$). The corresponding calculation for the GSp_4-case can be found in [**LSZ17**, §§4, 8].

7.2. Euler systems and Selmer groups in Coleman families

Modular forms can often be deformed in p-adic families (Hida families of ordinary forms, or the more general finite-slope families constructed by Coleman [**Col97**]). One knows that the Euler system of Kato, and the Euler system of Beilinson–Flach elements, can be interpolated in Coleman families (see [**Wan14**], [**Han15**] for the former, and [**LZ16**] for the latter). This raises (at least) two natural questions.

- In the Beilinson–Flach setting, can one define a Selmer group attached to the family, and use the Euler system to give upper bounds on its size? There is a general approach to defining Selmer groups in families, due to Pottharst [**Pot13**], and it would be interesting to try to formulate and prove a bound for Pottharst's Selmer groups in this setting.
- Are there analogous interpolation results for other Euler systems, e.g. in the Hilbert or Siegel settings? The existence of Hida families in these settings is well-known ([**Hid89, TU99**]), so as a first step one could show that the Euler systems vary in these families.

  Andreatta, Iovita and Pilloni have recently shown the existence of p-adic families of finite-slope automorphic forms in both the Hilbert [**AIP16**] and the Siegel case [**AIP15**]; but whether the Euler systems interpolate in these families is an open question.

[1] It is possible to give a new proof of the tame norm relations for Beilinson–Flach elements using local zeta integrals. This is currently being worked out by Giada Grossi.

Bibliography

[AIP15] Fabrizio Andreatta, Adrian Iovita, and Vincent Pilloni, *p-adic families of Siegel modular cuspforms*, Ann. of Math. (2) **181** (2015), no. 2, 623–697. MR 3275848 ↑ 54

[AIP16] ———, *On overconvergent Hilbert modular cusp forms*, Astérisque (2016), no. 382, 163–193. MR 3581177 ↑ 54

[And87] Anatolij N. Andrianov, *Quadratic forms and Hecke operators*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 286, Springer-Verlag, Berlin, 1987. MR 884891 ↑ 46

[Beĭ84] A. A. Beĭlinson, *Higher regulators and values of L-functions*, Current problems in mathematics, Vol. 24, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984, pp. 181–238. MR 760999 ↑ 26

[BDR15] Massimo Bertolini, Henri Darmon, and Victor Rotger, *Beilinson–Flach elements and Euler systems I: syntomic regulators and p-adic Rankin L-series*, J. Algebraic Geom. **24** (2015), no. 2, 355–378. MR 3311587 ↑ 29

[Bes00] Amnon Besser, *Syntomic regulators and p-adic integration. I. Rigid syntomic regulators*, Israel J. Math. **120** (2000), no. 1, 291–334. MR 1809626 ↑ 29

[Bes12] ———, *On the syntomic regulator for K_1 of a surface*, Israel J. Math. **190** (2012), no. 1, 29–66. MR 2956231 ↑ 29

[Bum05] Daniel Bump, *The Rankin-Selberg method: an introduction and survey*, Automorphic representations, L-functions and applications: progress and prospects, Ohio State Univ. Math. Res. Inst. Publ., vol. 11, de Gruyter, Berlin, 2005, pp. 41–73. MR 2192819 ↑ 27

[CR18] Antonio Cauchi and Joaquin Rodrigues, *Euler systems for GSp(6)*, in preparation, 2018. ↑ 28

[CRSS15] John Coates, A. Raghuram, Anupam Saikia, and R. Sujatha (eds.), *The Bloch-Kato conjecture for the Riemann zeta function*, London Mathematical Society Lecture Note Series, vol. 418, Cambridge University Press, Cambridge, 2015. MR 3410209 ↑ 15

[Col97] Robert F. Coleman, *p-adic Banach spaces and families of modular forms*, Invent. Math. **127** (1997), no. 3, 417–479. MR 1431135 ↑ 54

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140. MR 1605752 ↑ 18

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196 ↑ 18

[Gea06] Matthew Thomas Gealy, *On the Tamagawa Number Conjecture for motives attached to modular forms*, Caltech PhD thesis, 2006. ↑ 42

[Han15] David Hansen, *Iwasawa theory of overconvergent modular forms*, preprint, 2015. ↑ 54

[Hid89] Haruzo Hida, *On nearly ordinary Hecke algebras for* GL(2) *over totally real fields*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 139–169. MR 1097614 ↑ 54

[Jan88] Uwe Jannsen, *Continuous étale cohomology*, Math. Ann. **280** (1988), no. 2, 207–245. MR 929536 ↑ 17

[Kat04] Kazuya Kato, *P-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290, Cohomologies *p*-adiques et applications arithmétiques. III. MR 2104361 ↑ 13, 20, 22, 23

[KLZ15] Guido Kings, David Loeffler, and Sarah Livia Zerbes, *Rankin–Eisenstein classes for modular forms*, to appear, 2015, `arXiv:1501.03289`. ↑ 31

[KLZ17] ———, *Rankin–Eisenstein classes and explicit reciprocity laws*, Cambridge J Math **5** (2017), no. 1, 1–122. ↑ 31, 41, 42, 54

[Kol91] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Lecture Notes in Math., vol. 1479, Springer, Berlin, 1991, pp. 94–121. MR 1181210 ↑ 13, 20

[Lan91] Steven E. Landsburg, *Relative Chow groups*, Illinois J. Math. **35** (1991), no. 4, 618–641. MR 1115990 ↑ 26

[Lan87] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate. MR 890960 ↑ 22

[LLZ14] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for Rankin–Selberg convolutions of modular forms*, Ann. of Math. (2) **180** (2014), no. 2, 653–771. MR 3224721 ↑ 31, 54

[LLZ16] ———, *Euler systems for Hilbert modular surfaces*, preprint, 2016, `arXiv:1607.07813`. ↑ 28

[Lem15] Francesco Lemma, *On higher regulators of Siegel threefolds I: The vanishing on the boundary*, Asian J. Math. **19** (2015), no. 1, 83–120. MR 3318014 ↑ 48

[Lem17] ———, *On higher regulators of Siegel threefolds II: the connection to the special value*, Compos. Math. **153** (2017), no. 5, 889–946. MR 3705247 ↑ 48, 49

[LSZ17] David Loeffler, Christopher Skinner, and Sarah Livia Zerbes, *Euler systems for GSp(4)*, preprint, 2017, `arXiv:1706.00201`. ↑ 28, 45, 48, 54

[LZ16] David Loeffler and Sarah Livia Zerbes, *Rankin–Eisenstein classes in Coleman families*, Res. Math. Sci. **3** (2016), no. 29, special collection in honour of Robert F. Coleman. ↑ 54

[MR04] Barry Mazur and Karl Rubin, *Introduction to Kolyvagin systems*, Stark's conjectures: recent work and new directions, Contemp. Math., vol. 358, Amer. Math. Soc., Providence, RI, 2004, pp. 207–221. MR 2088718 ↑ 12

[MVW06] Carlo Mazza, Vladimir Voevodsky, and Charles Weibel, *Lecture notes on motivic cohomology*, Clay Mathematics Monographs, vol. 2, American Mathematical Society, Providence, RI; Clay Mathematics Institute, Cambridge, MA, 2006. MR 2242284 ↑ 26

[Nek98] Jan Nekovář, *Syntomic cohomology and p-adic regulators*, preprint, 1998. ↑ 29

[NN16] Jan Nekovář and Wiesława Nizioł, *Syntomic cohomology and p-adic regulators for varieties over p-adic fields*, Algebra Number Theory **10** (2016), no. 8, 1695–1790, With appendices by Laurent Berger and Frédéric Déglise. MR 3556797 ↑ 29

[Niz97] Wiesława Nizioł, *On the image of p-adic regulators*, Invent. Math. **127** (1997), no. 2, 375–400. MR 1427624 ↑ 29

[Nov79] Mark Novodvorsky, *Automorphic L-functions for the symplectic group* GSp(4), Automorphic forms, representations and L-functions (Corvallis, 1977) (Armand Borel and William Casselman, eds.), Proc. Sympos. Pure Math, vol. 33 Part 2, Amer. Math. Soc., 1979, pp. 87–95. ↑ 53

[PS97] I. I. Piatetski-Shapiro, *L-functions for* GSp_4, Pacific J. Math. (1997), no. Special Issue, 259–275, Olga Taussky-Todd: in memoriam. MR 1610879 ↑ 47

[Pot13] Jonathan Pottharst, *Analytic families of finite-slope Selmer groups*, Algebra Number Theory **7** (2013), no. 7, 1571–1612. MR 3117501 ↑ 54

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton Univ. Press, 2000. MR 1749177 ↑ 12, 13, 14

[Tha88] Francisco Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. (2) **128** (1988), no. 1, 1–18. MR 951505 ↑ 13

[TU99] J. Tilouine and E. Urban, *Several-variable p-adic families of Siegel–Hilbert cusp eigensystems and their Galois representations*, Ann. Sci. École Norm. Sup. (4) **32** (1999), no. 4, 499–574. MR 1693583 ↑ 54

[vdG08] Gerard van der Geer, *Siegel modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 181–245. MR 2409679 ↑ 46

[Wan14] Shanwen Wang, *Le système d'Euler de Kato en famille (I)*, Comment. Math. Helv. **89** (2014), no. 4, 819–865. MR 3284296 ↑ 54

[Wei05] Rainer Weissauer, *Four dimensional Galois representations*, Astérisque **302** (2005), 67–150, Formes automorphes. II. Le cas du groupe GSp(4). MR 2234860 ↑ 47

COURSE AND PROJECT OUTLINE
MODULAR CURVES AND CYCLOTOMIC FIELDS
ARIZONA WINTER SCHOOL 2018

ROMYAR SHARIFI

COURSE OUTLINE

The prototypical example of an Iwasawa module is the inverse limit X of p-parts of class groups under norm maps up the tower of cyclotomic fields of p-power roots of unity. This group X is a finitely generated torsion module over the completed $\mathbb{Z}_p$-group ring of the tower of fields, known as an Iwasawa algebra. In this course, we study the structure of X.

Attached to the part of X on which complex conjugation acts by -1 is a characteristic ideal that provides a measure of the size of the module. Iwasawa conjectured that this ideal is generated by an element of the Iwasawa algebra determined the p-adic L-functions of even characters of the Galois group of the pth cyclotomic field over $\mathbb{Q}$. This statement, known as the Iwasawa main conjecture, provides a fundamental example of the links between algebraic and analytic objects in number theory. It was proven by Mazur and Wiles in 1984, building on ideas of Ribet in his 1976 proof of the converse to Herbrand's theorem.

Ribet and Mazur-Wiles look to the two-dimensional Galois representations attached to modular forms to construct unramified p-extensions of p-power cyclotomic fields. That is, the desired finite extensions are fixed by the kernel of a Galois representation ρ attached to a newform congruent to an Eisenstein series modulo a prime over p. The key idea is that ρ is residually reducible, and this enables one to find a 1-cocycle that gives rise to the unramified extension. More precisely, such cocycles can be used to construct a canonical homomorphism from X to the quotient of a space of cuspidal modular symbols of p-power levels by the action of an Eisenstein ideal of Hida's p-adic Hecke algebra.

There is a much more explicit map in the other direction, which is conjecturally inverse to the above map. At finite level, it takes modular symbols to cup products of cyclotomic p-units in Galois cohomology. All indications are that this is just one incarnation of a much more general phenomenon. The idea is that the geometry of locally symmetric spaces near their boundary strata describes the arithmetic of lower-dimensional objects.

Tentatively speaking, the structure of this course will be roughly as follows:

- background on Iwasawa modules and p-adic L-functions,
- the main conjecture and its proof,
- modular symbols and cup products,
- a refined conjecture, its consequences, and known results.

PROJECT OUTLINE

The projects will be of two sorts: purely Iwasawa theoretic and largely algebraic, and less Iwasawa theoretic but closely related to the above conjecture and its possible extensions. We give some ideas here of the sort of questions that could potentially form the bases of projects.

0.1. **Cohomology and Iwasawa modules.** Cup products of p-units provide information on the second stage of a certain augmentation filtration of an Iwasawa module over a Kummer extension of the field of p-power roots of unity. Are there instances where such cup products vanish where one can obtain deeper information on the structure of this Iwasawa module using higher operations (see [Sh1])? Can this be computed for a small irregular prime like 37, for instance, perhaps using a refinement of a method applied in [MS] to show the nonvanishing of a cup product? What other Galois groups and Iwasawa modules can one use these to describe the structure of more precisely (see for instance [Sh2])?

0.2. **The original conjecture.**

(1) For the conjecture of [Sh3], what is the arithmetic significance of a relation given by the choice of congruence subgroup, the cusps in the relative homology group, or a generator of the Eisenstein ideal for a Hecke operator dividing the level?
(2) What can be said about the relationship between other standard Iwasawa modules and modular symbols?
(3) Phrase a form of the conjecture relating K-groups of cyclotomic integer rings and higher weight modular symbols.
(4) Can one obtain a halfway decent bound on the p-rank of the class group of the pth cyclotomic field using modular symbols?

0.3. **Analogues over imaginary quadratic fields.** For an imaginary quadratic field F, one expects a similar relationship between modular symbols on a Bianchi space for a congurence subgroup of $\mathrm{GL}_2(\mathscr{O}_F)$ modulo Eisenstein and a second cohomology group of an ray class field of F (see [FKS]). Here, Manin symbols are replaced by symbols of Cremona (if F is Euclidean) and cyclotomic units are replaced by elliptic units.

(1) In what instances can one prove that there is a well-defined, canonical map in either direction?
(2) What if F is not Euclidean, but for instance has class number one?

REFERENCES

[FK] T. Fukaya, K. Kato, On conjectures of Sharifi, preprint, 2012, http://math.ucla.edu/∼sharifi/sharificonj.pdf.
[FKS] T. Fukaya, K. Kato, R. Sharifi, Modular symbols in Iwasawa theory, *Iwasawa Theory 2012 - State of the Art and Recent Advances*, Contrib. Math. Comput. Sci. **7**, Springer, 2014, 177–219.
[Gr] R. Greenberg, Iwasawa theory – Past and Present, *Class field theory – its centenary and prospect (Tokyo, 1998)*, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001, 335–385.
[MS] W. McCallum, R. Sharifi, A cup product in the Galois cohomology of number fields, *Duke Math. J.* **120** (2003), 269–310.

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

[Oh] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves II, *Math. Ann.* **318** (2000), 557–583.

[Ri] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[Sh1] R. Sharifi, Massey products and ideal class groups, *J. reine angew. Math.* **603** (2007), 1–33.

[Sh2] R. Sharifi, On Galois groups of unramified pro-p extensions, *Math. Ann.* **342** (2008), 297–308.

[Sh3] R. Sharifi, A reciprocity map and the two variable p-adic L-function, *Annals of Math.* **173** (2011), 251–300.

[Sh4] R. Sharifi, Iwasawa theory (lecture notes), http://math.ucla.edu/∼iwasawa.pdf.

[Wa] P. Wake, Eisenstein Hecke algebras and conjectures in Iwasawa theory, *Algebra Number Theory* **9** (2015), 53–75.

[WW] P. Wake, C. Wang Erickson, Pseudo-modularity and Iwasawa theory, to appear in *Amer J. Math.*, arXiv:1505.05128v3.

The above is a sampling of relevant references. The lecture notes on Iwasawa theory [Sh4] may be useful for getting a head start. The ideas of the paper of Ribet [Ri] are central to the course as well. The article [Gr] gives a fascinating survey of Iwasawa theory at the turn of the millenium. For the material later in the course, and an introduction to the papers [Sh3] and [FK], one might try reading the first part of the survey article [FKS].

Modular curves and cyclotomic fields

Romyar T. Sharifi

Contents

CHAPTER 1

Introduction

These notes concern the arithmetic of the p^nth cyclotomic fields $F_n = \mathbb{Q}(\mu_{p^n})$ for an odd prime p and a positive integer n. Here, μ_{p^n} denotes the group of p^nth roots of unity inside the complex numbers. When we speak of arithmetic, we speak not just of field elements but of algebraic integers in this field, which is to say elements of the ring $\mathcal{O}_n = \mathbb{Z}[\mu_{p^n}]$ generated by the p^nth roots of unity. This ring is of course also generated by the single primitive p^nth root of unity $\zeta_{p^n} = e^{2\pi i/p^n}$.

The failure of the rings $\mathcal{O}_n$ to always be principal ideal domains is measured by the class group Cl_n of F_n. Of particular interest is its Sylow p-subgroup A_n, which consists of the elements of p-power order. The prime p is said to be regular if $A_n = 0$ and irregular otherwise. In 1850, Kummer showed that Fermat's last theorem holds for regular prime exponents, employing the factorization

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$$

in $\mathbb{Z}[\mu_p]$ for integers x and y.

Iwasawa studied the growth of the groups A_n as n increases. In particular, he showed that their orders have a surprising regularity. That is, there exist nonnegative integers μ and λ and an integer ν such that

$$|A_n| = p^{p^n\mu+n\lambda+\nu}$$

for all sufficiently large n [**Iwa1**]. Each of these groups A_n has an action of the Galois group $\mathrm{Gal}(F_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$, and in particular of the group $\Gamma_n = \mathrm{Gal}(F_n/F_1)$, which is noncanonically isomorphic to $\mathbb{Z}/p^{n-1}\mathbb{Z}$. The inverse limit $X_\infty = \varprojlim_n A_n$ of the groups A_n under norm maps is a profinite group with the corresponding profinite topology. By definition, it has a continuous action of the group $\Gamma = \mathrm{Gal}(F_\infty/F_1)$, where $F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_n F_n$. The group Γ is then noncanonically isomorphic to $\mathbb{Z}_p$, and by continuity, the action extends to an action of the completed group ring $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \cong \varprojlim_n \mathbb{Z}_p[\Gamma_n]$ on X_∞. This group ring is in turn continuously isomorphic to the one variable power-series ring $\mathbb{Z}_p[\![T]\!]$, with the isomorphism determined by a choice of topological generator γ of Γ. That is, $\gamma - 1$ is sent to T, and this allows us to identify the two compact $\mathbb{Z}_p$-algebras.

As a module over this group ring, X_∞ can be seen to be finitely generated and torsion over Λ. Moreover, its coinvariant group $(X_\infty)_{\mathrm{Gal}(F_\infty/F_n)}$, which is the maximal quotient of X_∞ on which the action of Γ factors through Γ_n, is isomorphic to A_n via the canonical map given by definition of the inverse limit. The statement on the order of A_n then reduces to a statement about finitely generated, torsion modules over Λ, as was observed by Serre [**Ser**]. That is, any

finitely generated torsion Λ-module M is "pseudo-isomorphic" to a direct sum of quotients of Λ by principal ideals, in the sense that there exists a Λ-module homomorphism to such a direct sum with finite kernel and cokernel. The product of the latter principal ideals is an invariant of M called the characteristic ideal of M.

Now, the group ring $\mathbb{Z}_p[\Delta]$ of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ also acts on X_∞, and X_∞ breaks into a direct sum of components

$$X_\infty^{(i)} = \{x \in X_\infty \mid \delta(x) = a^i x\},$$

where δ is a generator of Δ and $a \in \mathbb{Z}_p^\times$ is the unique $(p-1)$th root of unity such that $\delta(\zeta_p) = \zeta_p^a$. The main conjecture of Iwasawa theory (cf. [**Iwa4, Iwa5**]) states that the characteristic ideal of $X_\infty^{(i)}$ for an odd integer i has characteristic ideal generated by a power series g_i attached to a Kubota-Leopoldt p-adic L-function $L_p(\omega^{1-i}, s)$ in the sense that $g_i(\upsilon^s - 1) = L_p(\omega^{1-i}, s)$ for all $s \in \mathbb{Z}_p$ for the topological generator υ of $1 + p\mathbb{Z}_p$ that is the evaluation of the p-adic cyclotomic character on γ.

The main conjecture was proven by Mazur and Wiles in 1984 using the geometry of modular curves [**MaWi1**]. In fact, what they proved is that for each odd i, the characteristic ideal of $X_\infty^{(i)}$ is divisible by (g_i). This is sufficient as the analytic class number formula tells us that the product of the (g_i) is the product of the characteristic ideals of $X_\infty^{(i)}$. Mazur and Wiles construct a large enough unramified abelian pro-p extension of F_∞ with the desired action of Δ, significantly extending a method introduced by Ribet [**Rib**]. They do so by studying the irreducible two-dimensional Galois representations attached to cuspidal eigenforms that satisfy congruences with Eisenstein series modulo primes over p. By virtue of these congruences, these representations are residually reducible: in fact, there exists a Galois-stable lattice in the representation such that its reduction modulo the prime is unramified upon restriction to the absolute Galois group of F_∞. To find a large enough unramified extension to produce $X_\infty^{(i)}$ via the isomorphism of class field theory, they must consider cusp forms of increasing p-power level.

The cusp forms used in the main conjecture can be placed in a family of cusp forms of varying level and weight, and if one likes, may be viewed as a single modular form with coefficients in a finite flat algebra over Λ, with the variable coming from certain diamond operators. The Galois representations may be similarly encapsulated in a single two-dimensional representation over the Hecke algebra acting on such Λ-adic modular forms. This is made possible by the fact that the modular forms under consideration are ordinary: their pth Fourier coefficients are units, and the good control one has over the growth of spaces of such forms is the subject of Hida theory, which has much of the flavor of Iwasawa theory.

The Mazur-Wiles proof of the main conjecture indicates that the geometry of modular curves "near the cusps" has much to say about the arithmetic of cyclotomic fields. That is, the "Eisenstein ideal" determining the congruences between our Λ-adic cusp forms and Eisenstein series is essentially the annihilator of the cusp at ∞. So, when we look at residual representations attached to our cusp forms, we are essentially exploring the geometry of a modular curve near ∞.

The characteristic ideal of an Iwasawa module being a rather rough invariant of its structure, one might ask how far one can push this connection between geometry and arithmetic. The construction of the unramified extension in the Mazur-Wiles proof is rather far from canonical,

but this can be improved. Out of the residual Galois representation attached to the Λ-adic cusp forms one uses in the proof, one can construct a canonical map Υ from the Tate twist $X_\infty^{(i)}(1)$ to a space of Λ-adic cusp forms $\mathfrak{S}$ reduced modulo an Eisentein ideal I_i. This map is not obviously an isomorphism, but that it is has recently been shown by M. Ohta [**Oht4**].

There is also a map $\varpi\colon \mathfrak{S}/I_i\mathfrak{S} \to X_\infty^{(i)}(1)$ in the opposite direction that is explicitly defined to take certain compatible sequences of classes in the real parts of homology groups of modular curves to compatible sequences of cup products of cyclotomic units in Galois cohomology. As we shall explain, the two maps Υ and ϖ are conjecturally inverse to each other. A major result in this direction, in which the derivative $L_p(\omega^{1-i}, s)$ intervenes (and which, though weaker, may be the most natural statement), has been proven by Fukaya and Kato [**FuKa**].

ACKNOWLEDGMENTS. The author thanks Preston Wake and Ashay Burungale for detailed comments on these notes that have improved them significantly.

CHAPTER 2

Arithmetic of cyclotomic fields

We shall not attempt to describe results in their most general form in these notes. For a more complete accounting, we suggest the book of Washington [**Was**] or our lecture notes [**Sha5**] (still in draft form at this writing). We will frequently restrict our discussion to the p-power cyclotomic fields.

2.1. Class numbers and L-functions

We recall the definition of the Dedekind zeta function of a number field.

DEFINITION 2.1.1. The Dedekind zeta function of a number field F is the meromorphic continuation to $\mathbb{C}$ of the series

$$\zeta_F(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_F} (N\mathfrak{a})^{-s},$$

which converges on $s \in \mathbb{C}$ satisfying $\mathrm{Re}(s) > 1$. Here, the sum is taken over ideals $\mathfrak{a}$ of the ring of integers $\mathcal{O}_F$ of F, and $N\mathfrak{a} = [\mathcal{O}_F : \mathfrak{a}]$ is the absolute norm of $\mathfrak{a}$.

Also associated to F is a positive real number known as its regulator R_F, formed out of the determinant of a matrix with entries given by the logarithms of all but one of the real and complex absolute values on F applied to a set of generators of the units group $\mathcal{O}_F^\times$, modulo torsion. This regulator appears in proofs of Dirichlet's unit theorem.

THEOREM 2.1.2 (ANALYTIC CLASS NUMBER FORMULA). *Let F be a number field. Then*

$$\lim_{s \to 1} (s-1)\zeta_F(s) = \frac{2^{r_1(F)}(2\pi)^{r_2(F)} h_F R_F}{w_F |d_F|^{1/2}},$$

where for F, the quantities $r_1(F)$ and $r_2(F)$ are respectively the number of its real and complex places, h_F is its class number, R_F is its regulator, w_F is the number of roots of unity it contains, and d_F is its discriminant.

DEFINITION 2.1.3. For a commutative ring R (with 1), an R-valued Dirichlet character is a multiplicative function $\chi \colon \mathbb{Z}/N\mathbb{Z} \to R$ for some positive integer N known as its modulus, that is defined as 0 on all non-units in $\mathbb{Z}/N\mathbb{Z}$. By composition with reduction modulo N, we typically view χ as a function on $\mathbb{Z}$.

REMARK 2.1.4. When R is not specified, we take it either to be $\mathbb{C}$ or an arbitrary ring, as needed in the context.

DEFINITION 2.1.5. The minimal positive integer such that the restriction of a Dirichlet character χ to $(\mathbb{Z}/N\mathbb{Z})^\times$ of modulus N factors through $(\mathbb{Z}/f\mathbb{Z})^\times$ is known as its conductor. We say that χ is primitive if its modulus and conductor agree.

DEFINITION 2.1.6. We say that a Dirichlet character χ is odd if $\chi(-1) = -1$, and even if $\chi(-1) = 1$.

DEFINITION 2.1.7. Let χ be a Dirichlet character of modulus N. The Dirichlet L-function associated to a Dirichlet character χ is the meromorphic continuation to $\mathbb{C}$ of the series

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

which converges on $s \in \mathbb{C}$ satisfying $\mathrm{Re}(s) > 1$.

REMARK 2.1.8. The L-function $L(\chi, s)$ is entire unless χ is the trivial character of its modulus.

REMARK 2.1.9. The L-series $L(\chi, s)$ has an Euler product expansion

$$L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}.$$

By the Kronecker-Weber theorem, any abelian number field F (i.e., number field that is an abelian extension of $\mathbb{Q}$) is contained in $\mathbb{Q}(\mu_N)$ for some $N \geq 1$, in which case $\mathrm{Gal}(F/\mathbb{Q})$ is identified with a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times$ via the Nth cyclotomic character. Let $X(F)$ denote the set of primitive Dirichlet characters of conductor dividing N that, viewed as characters on $(\mathbb{Z}/N\mathbb{Z})^\times$, factor through $\mathrm{Gal}(F/\mathbb{Q})$ under this identification.

PROPOSITION 2.1.10. *For an abelian number field F, we have*

$$\zeta_F(s) = \prod_{\chi \in X(F)} L(\chi, s).$$

EXERCISE 2.1.11. Prove Proposition 2.1.10 by examining the Euler product expansions of the two sides.

We next turn to the special values of our Dirichlet L-functions and the Riemann zeta function. For these, we introduce the Bernoulli numbers and their generalized counterparts.

DEFINITION 2.1.12. The nth Bernoulli number B_n is the value of the nth derivative of $\frac{x}{e^x - 1}$ at 0.

The Bernoulli numbers B_n for odd n are 0 except for $B_1 = -\frac{1}{2}$, and the Bernoulli numbers for even n starting with B_0 are

$$1, \frac{1}{6}, -\frac{1}{30}, \frac{1}{42}, -\frac{1}{30}, \frac{5}{66}, -\frac{691}{2730}, \frac{7}{6}, \frac{3617}{510} \ldots.$$

These numbers are nearly the special values of the Riemann zeta function at nonpositive integers. That is, we have the following.

REMARK 2.1.13. The Bernoulli numbers satisfy

$$\zeta(1 - n) = (-1)^{n-1} \frac{B_n}{n}$$

for $n \geq 1$.

Let us list the prime factorizations of the absolute values of the numerators of the $\frac{B_k}{k}$ for even $k \geq 2$:

$$1, 1, 1, 1, 1, 691, 1, 3617, 43867, 283 \cdot 617, 131 \cdot 593, ...$$

The prime numbers which occur in this list are known as irregular primes. They play a central role in our study.

We also have a generalized notion of Bernoulli numbers for Dirichlet characters.

DEFINITION 2.1.14. The nth generalized Bernoulli number $B_{n,\chi}$ for a Dirichlet character χ of modulus N is the nth derivative at 0 of the polynomial

$$\sum_{a=1}^{N} \chi(a) \frac{xe^{ax}}{e^{Nx} - 1}.$$

EXAMPLE 2.1.15. For any Dirichlet character χ of modulus dividing N, we have

$$B_{1,\chi} = \frac{1}{N} \sum_{a=1}^{N} \chi(a) a.$$

REMARK 2.1.16. Similarly to the values of Riemann zeta function, we have

$$L(\chi, 1 - n) = -\frac{B_{n,\chi}}{n}$$

for all $n \geq 1$.

DEFINITION 2.1.17. A number field is totally real if its archimedean places are all real, and it is CM if it is a purely imaginary (i.e., having only complex archimedean places) quadratic extension of a totally real field.

Any abelian number field F is either totally real or CM. Let F^+ denote the maximal totally real subfield of F, which is of index at most 2 in F.

DEFINITION 2.1.18. The plus and minus parts of the class number of a CM number field F are the integers

$$h_F^+ = h_{F^+} \quad \text{and} \quad h_F^- = \frac{h_F}{h_F^+}.$$

EXERCISE 2.1.19. Show that h_F^- is an integer.

The analytic class number formula yields individual formulas for the plus and minus parts of the class number. We write $a \sim b$ for integers a and b if they agree up to a power of 2. Let $X^-(F)$ denote the set of primitive odd Dirichlet characters in $X(F)$.

THEOREM 2.1.20. *For any positive integer N, we have*

$$h_{\mathbb{Q}(\mu_N)}^- \sim N \prod_{\chi \in X^-(\mathbb{Q}(\mu_N))} B_{1,\chi}.$$

The ring of integers of $\mathbb{Q}(\mu_N)$ is $\mathbb{Z}[\mu_N]$, and we let $E_N = \mathbb{Z}[\mu_N]^\times$ denote its unit group for brevity. By Dirichlet's unit theorem, the rank of E_N is $\frac{\varphi(N)}{2} - 1$. Let us fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, which singles out the primitive Nth root of unity $\zeta_N = e^{2\pi i/N}$.

REMARK 2.1.21. The element $1-\zeta_N \in \mathbb{Q}(\mu_N)^\times$ is a unit if N is composite, but it is merely a p-unit (i.e., a unit in $\mathbb{Z}[\frac{1}{p}, \mu_N]$) if N is a power of p.

DEFINITION 2.1.22. For $N \geq 1$, the group of cyclotomic units C_N in $\mathbb{Q}(\mu_N)$ is the intersection with E_N of the subgroup of $\mathbb{Q}(\mu_N)^\times$ generated by its roots of unity and the elements $1-\zeta_N^i$ with $1 \leq i < N$.

THEOREM 2.1.23. *For any positive integer N, the group C_N is of finite index in E_N. We have*

$$h^+_{\mathbb{Q}(\mu_N)} \sim [E_N : C_N],$$

and this is an equality if N is a prime power.

Let us now specialize back to our fields of interest, the fields $F_n = \mathbb{Q}(\mu_{p^n})$ for a prime p, which for now we shall not require to be odd. The Galois group $\mathrm{Gal}(F_n/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$ via the modulo p^n cyclotomic character that is determined by the power to which an element raises ζ_{p^n}. As such, it breaks up as a product $\Delta \times \Gamma_n$, where if p is odd, $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and Γ_n is a cyclic p-group. If $p = 2$, we take Δ to be the order 2 subgroup generated by complex conjugation and Γ_n to be the cyclic 2-group generated by elements which are 1 modulo 4. We let

$$q = \begin{cases} p & \text{if } p \text{ is odd} \\ 4 & \text{if } p = 2, \end{cases}$$

and we set $F = \mathbb{Q}(\mu_q)$.

DEFINITION 2.1.24. Let ω denote the homomorphism $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ that is the composition

$$\mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/q\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times$$

of reduction modulo q and the unique homomorphism splitting it. We also denote by ω the Dirichlet character of modulus q induced by the latter injection.

PROPOSITION 2.1.25. *We have*

$$B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \bmod p\mathbb{Z}_p$$

for any positive integer $k \geq 2$ with $k \not\equiv 0 \bmod p-1$.

As $B_{1,\omega^{-1}}$ has p-adic valuation -1, Theorem 2.1.20 has the following corollary.

COROLLARY 2.1.26. *The class number h_F^- is divisible by p if and only if p divides B_k for some positive even integer $k < p-1$.*

DEFINITION 2.1.27. We say that a prime p is regular if $p \nmid h_F$. Otherwise p is said to be irregular.

By a result of Kummer, p is regular if and only if $p \nmid h_F^-$. Thus, p is regular if and only if p divides the numerator of some B_k for a positive even $k < p-1$.

It is known that there are infinitely many irregular primes, and though heuristically speaking there are more regular primes than irregular primes less than any given bound, it is still an open question as to whether there are infinitely many regular primes.

EXAMPLE 2.1.28. The smallest irregular primes are 37, 59, 67, 101, and 103. For instance, $37 \mid B_{32}$, $59 \mid B_{44}$, and $67 \mid B_{58}$.

DEFINITION 2.1.29. The index of irregularity of a prime is the number of positive even $k < p-1$ such that $p \mid B_k$.

EXAMPLE 2.1.30. The smallest prime having index of irregularity greater than one is 157, which divides B_{62} and B_{110}. The prime 691 divides B_{12} and B_{200}.

Kummer made the following conjecture regarding h_F^+ in 1849 in a letter to Kronecker, and it was later rediscovered by Vandiver around 1920, after whom it is typically named. It has been verified for primes $p < 39 \cdot 2^{22} = 163557355$ by Buhler and Harvey [**BuHa**].

CONJECTURE 2.1.31 (KUMMER-VANDIVER CONJECTURE). *The p-part of the class number of F^+ is 1.*

Since it provides an interesting example, we remark that Weber conjectured the following for $p = 2$ in 1886, and Coates has asked whether its generalization to odd p holds.

CONJECTURE 2.1.32. *For any prime p, let $\mathbb{Q}_n$ denote the maximal (cyclic) p-extension of $\mathbb{Q}$ in F_n. Then $h_{\mathbb{Q}_n} = 1$.*

2.2. The Herbrand-Ribet Theorem

Now let us suppose that p is odd. Let A denote the p-part of the class group of $F = \mathbb{Q}(\mu_p)$. Let $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, which we identify with $(\mathbb{Z}/p\mathbb{Z})^\times$. We let ω also denote the unique character $\Delta \to \mathbb{Z}_p^\times$ with reduction modulo p equal to the mod p cyclotomic character.

The group A has an action of Δ, so being that A is a p-group, it has the structure of a $\mathbb{Z}_p[\Delta]$-module. Like all $\mathbb{Z}_p[\Delta]$-modules, the group A has a canonical decomposition as a direct sum

$$A = \bigoplus_{i=0}^{p-2} A^{(i)},$$

where

$$A^{(i)} = \{a \in A \mid \delta(a) = \omega(\delta)^i a \text{ for all } \delta \in \Delta\}.$$

Note that $A^{(i)} = A^{(j)}$ if $i \equiv j \bmod p-1$.

The following theorem of Leopoldt [**Leo**] is known as Leopoldt's reflection theorem (or "Spiegelungsatz").

THEOREM 2.2.1 (LEOPOLDT). *For even k, we have*

$$\dim_{\mathbb{F}_p}(A/pA)^{(k)} \leq \dim_{\mathbb{F}_p}(A/pA)^{(1-k)} \leq \dim_{\mathbb{F}_p}(A/pA)^{(k)} + 1.$$

EXERCISE 2.2.2. Prove this using Kummer theory (see the method of the proof of Theorem 2.3.18 below).

In particular, this theorem implies that if $A^{(1-k)} = 0$, then $A^{(k)} = 0$. If Vandiver's conjecture holds so that $A^{(k)} = 0$, the theorem tells us that $A^{(1-k)}$ is cyclic. In 1932, Herbrand proved that if $A^{(1-k)} \neq 0$, then $p \mid B_k$ [**Her**]. The converse was proven by Ribet in 1976 [**Rib**].

THEOREM 2.2.3 (HERBRAND-RIBET). *Let p be an odd prime, and let k be even with $2 \leq k \leq p-3$. We have $A^{(1-k)} \neq 0$ if and only if $p \mid B_k$.*

We explain how Herbrand's theorem follows from a result of Stickelberger's.

SKETCH OF PROOF OF HERBRAND'S THEOREM. The Stickelberger element of $\mathbb{Q}_p[\Delta]$ is

$$\theta = \frac{1}{p}\sum_{a=1}^{p-1} a[a]^{-1},$$

and the Stickelberger ideal of $\mathbb{Z}_p[\Delta]$ is the intersection $\mathcal{I} = \mathbb{Z}_p[\Delta]\theta \cap \mathbb{Z}_p[\Delta]$. Stickelberger proved that $\mathcal{I}$ annihilates A. Moreover, it is easy to see that $([b]-b)\theta \in \mathcal{I}$ for all $b \in \mathbb{Z}$ prime to p, where $[b]$ denotes the group element of b. The action of this element on $x \in A^{(1-k)}$ is given by

$$([b]-b)\theta x = (\omega^{1-k}(b)-b)B_{1,\omega^{k-1}}x,$$

but it is also zero. Since $k \not\equiv 0 \bmod p$, the element $\omega^{1-k}(b)-b$ is a unit for some b, and therefore $B_{1,\omega^{k-1}}$ annihilates x. In particular, if $A^{(1-k)} \neq 0$, then $B_{1,\omega^{k-1}} \notin \mathbb{Z}_p^\times$. By the Kummer congruence of Proposition 2.1.25, we have the result. □

We sketch a proof of the opposite implication which uses the theory of modular forms, and in particular congruences between cusp forms and Eisenstein series. We use this sketch as motivation for these concepts, which we elaborate upon in the following chapter. The reader may wish to return to this proof anew after reviewing those concepts. Our sketch is in the spirit of Ribet's proof, but what we write is more along the lines of the approach of Kurihara [**Kur**] and Harder-Pink [**HaPi**]. For an algebraic extension K of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$, let us use $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ to denote its absolute Galois group.

SKETCH OF PROOF OF RIBET'S THEOREM. Suppose that p divides B_k. Consider the weight k, level 1 Eisenstein series

$$E_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sum_{d|n} d^{k-1}q^n. \tag{2.2.1}$$

Modulo p, the Eisenstein series E_k has trivial constant term and so is a cusp form, being that ∞ is the only cusp of $\mathrm{SL}_2(\mathbb{Z})$. This cusp form lifts to a weight k newform $f = \sum_{n=1}^{\infty} a_n q^n$ on $\mathrm{SL}_2(\mathbb{Z})$. Attached to this f is an irreducible 2-dimensional Galois representation $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ that is unramified outside of p and characterized by the properties that $\det(\rho_f(\varphi_\ell)) = \ell^{k-1}$ and $\mathrm{Tr}(\rho_f(\varphi_\ell)) = a_\ell$ for any Frobenius φ_ℓ at ℓ for all primes $\ell \neq p$. In fact, this representation takes values in the $\mathrm{GL}_2(K_f)$, where K_f is the field of coefficients of f over $\mathbb{Q}_p$. Let V_f denote the corresponding 2-dimensional vector space over K_f.

For us, it is easiest to twist V_f by the $(1-k)$th power of the cyclotomic character: i.e., we consider $V_f' = V_f(1-k)$ and the resulting representation $\rho_f' \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ with determinant χ_p^{1-k} for the p-adic cyclotomic character $\chi_p \colon G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$. There exists a basis of V_f' such that the restriction of ρ_f' to a decomposition group D_p at a given prime over p is lower-triangular, and invariant group of $(V_f')^{I_p}$ of the inertia subgroup I_p is 1-dimensional.

In order to consider a residual representation associated to ρ_f, we must first choose a Galois stable lattice L_f in V_f', which is to say a free module of rank 2 over the valuation ring $\mathcal{O}_f$ of K_f. In fact, V_f' is itself constructed out of a canonical such lattice H_f, for instance as a certain subquotient group of a first étale cohomology group of a modular curve. Let π_f denote a uniformizer of $\mathcal{O}_f$, and let $\mathbb{F}_f = \mathcal{O}_f/\pi_f\mathcal{O}_f$ be the residue field. If f were not congruent to an Eisenstein series, then the residual representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_f}(H_f/\pi_f H_f)$ would be irreducible, and every Galois stable lattice in V_f' would have an isomorphic residual representation. However, in our case, every residual representation is reducible, and different choices of lattices can yield non-isomorphic residual representations.

The irreduciblity of ρ_f precludes the residual representations attached to Galois-stable lattices in V_f from all being semisimple, i.e., direct sums of two 1-dimensional representations. There exist smallest and largest non-split Galois-stable lattices with I_p-invariant group equal to $(H_f)^{I_p}$. The smallest such, which is our L_f, has $H_f^{I_p}/\pi_f H_f^{I_p}$ as a global quotient, hence is $G_{\mathbb{Q}_p}$-split. One can show that this quotient has trivial $G_{\mathbb{Q}}$-action, noting that $a_p(f) \equiv a_p(E_k) \equiv 1 \bmod \pi_f$ to get the triviality of the action of a Frobenius at p. Thus, $\bar{\rho}_f' \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_f}(L_f/\pi_f L_f)$ is a nontrivial unramified homomorphism upon restriction to the kernel of ω^{1-k}. In particular, $\bar{\rho}_f'$ has the form

$$\begin{pmatrix} \omega^{1-k} & * \\ 0 & 1 \end{pmatrix}$$

for a good choice of basis, where $*$ is a 1-cocycle that restricts to an unramified character on $G_{\mathbb{Q}(\mu_p)}$. The image of this homomorphism is a nontrivial quotient of A by class field theory, and the action of Δ on this quotient through lifting and conjugating is given by ω^{1-k}, as required. $\square$

2.3. Iwasawa modules

We continue to let p be an odd prime. Let A_n denote the p-part of the class group of F_n, which is a module over $\mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$. For $n \geq m$, we may consider the maps $A_m \to A_n$ and $A_n \to A_m$ induced by the inclusion of ideal groups and the norm map on ideals, respectively. These maps respect the $\mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$-actions on both groups, viewing $(\mathbb{Z}/p^m\mathbb{Z})^\times$ as a quotient of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. We let

$$A_\infty = \varinjlim_n A_n \quad \text{and} \quad X_\infty = \varprojlim_n A_n,$$

with the direct and inverse limits taken with respect to these maps.

Endowing A_∞ with the discrete topology and X_∞ with the profinite topology, these groups become continuous modules over the completed group ring

$$\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] = \varprojlim_n \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times],$$

which is endowed with the (profinite) topology of the inverse limit. Here, the action is the Galois action through the group $\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$, where $F_\infty = \mathbb{Q}(\mu_{p^\infty})$, the isomorphism being given by the p-adic cyclotomic character $\chi_p \colon G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, defined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_p(\sigma)}$ for $\sigma \in G_{\mathbb{Q}}$ and all $n \geq 1$.

The group $\Gamma = 1 + p\mathbb{Z}_p$ is procyclic, generated for instance by $1 + p$. We fix what may seem a rather unusual choice of generator for later purposes: let $\upsilon \in \Gamma$ be such that

$$(1 - p^{-1}) \log \upsilon = 1, \tag{2.3.1}$$

where $\log\colon 1 + p\mathbb{Z}_p \to \mathbb{Z}_p$ is the p-adic logarithm defined by the Taylor series expansion about 1 of the natural logarithm. The profinite $\mathbb{Z}_p$-algebra $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ is isomorphic to the completed group ring $\mathbb{Z}_p[\![T]\!]$ through such a choice of υ. Explicitly, we have

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![\Gamma]\!]$$

via the unique continuous $\mathbb{Z}_p$-linear isomorphism taking T to $\gamma - 1$, where $\gamma = [\upsilon]$ is the group element of υ.

Remark 2.3.1. In fact, there is no reason we cannot work in greater generality. That is, for any prime p and $n \geq 1$ or $n = \infty$, let $\mathbb{Q}_n$ denote the fixed field of $\Delta = (\mathbb{Z}/q\mathbb{Z})^\times$ in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Fixing a number field F, we can then set $F_n = F\mathbb{Q}_n$. We then have $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, and F_∞ is called the cyclotomic $\mathbb{Z}_p$-extension of F. Defining A_n as the p-part of the class group of F_n, we can define A_∞ and X_∞ as before. These are then modules over $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$, for $\Gamma = \mathrm{Gal}(F_\infty/F)$, which is again procyclic.

The group X_∞ is a finitely generated, torsion Λ-module. This follows by Nakayama's lemma from the fact that (at least for $F = \mathbb{Q}(\mu_p)$) its Γ-coinvariant group is isomorphic to the finite $\mathbb{Z}_p$-module A_1. The Pontryagin dual group $A_\infty^\vee = \mathrm{Hom}_{\mathrm{cts}}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is also a finitely generated Λ-module, where γ acts on an element f by precomposition with multiplication by γ^{-1}. (In fact, it is a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \Lambda[\Delta]$-module.)

The module theory of finitely generated Λ-modules is particularly nice, as every localization of Λ at a height one prime is a principal ideal domain, for which the structure theory of finitely generated modules is standard. A finitely generated torsion Λ-module M is as a consequence nearly isomorphic to the product of these localizations via the canonical inclusion: the kernel is the maximal finite Λ-submodule of M and the cokernel is finite as well.

Definition 2.3.2. A Λ-module homomorphism with finite kernel and cokernel is called a pseudo-isomorphism. We say that a Λ-module M is pseudo-isomorphic to a Λ-module N if there exists a pseudo-isomorphism $M \to N$ or a pseudo-isomorphism $N \to M$.

For general finitely generated Λ-modules, the existence of a pseudo-isomorphism does not imply the existence of a pseudo-isomorphism in the opposite direction.

Example 2.3.3. The maximal ideal of Λ is (p, T), which injects into Λ with finite cokernel, while there exists no pseudo-isomorphism $\Lambda \to (p, T)$.

For finitely generated-torsion modules, if $M \to N$ is a pseudo-isomorphism, then there does indeed exist a pseudo-isomorphism $N \to M$. That is, if we let $f \in \Lambda$ be an irreducible element outside of the support of M and N, then $M \otimes_\Lambda \Lambda[\frac{1}{f}] \to N \otimes_{\mathbb{Z}_p} \Lambda[\frac{1}{f}]$ is an isomorphism, and if we multiply the inverse by a suitably high power of f, the image of N will lie a finite index submodule of M inside $M \otimes_\Lambda \Lambda[\frac{1}{f}]$.

DEFINITION 2.3.4. A distinguished (or Weierstrass) polynomial in $\mathbb{Z}_p[T]$ is a nonconstant polynomial f satisfying $f \equiv T^{\deg f} \bmod p$

THEOREM 2.3.5 (WEIERSTRASS PREPARATION THEOREM). *Every nonzero element of Λ is the product of a unit, a power of p, and possibly a distinguished polynomial.*

Summarizing what we have said, we obtain the following [**Ser**].

THEOREM 2.3.6 (SERRE). *Every finitely generated Λ-module M is pseudo-isomorphic to a Λ-module of the form*

$$\Lambda^r \oplus \bigoplus_{i=1}^{g} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{h} \Lambda/(p^{\mu_j}), \tag{2.3.2}$$

where $r, g, h \geq 0$, the $f_i \in \Lambda$ are irreducible distinguished polynomials, $k_i \geq 1$ for $1 \leq i \leq g$, and $\mu_j \geq 1$ for $1 \leq j \leq h$. This decomposition is unique up ordering.

The nonnegative integer r in this theorem is the Λ-rank of M, i.e., $r = \dim_{Q(\Lambda)}(M \otimes_\Lambda Q(\Lambda))$, for $Q(\Lambda)$ the quotient field of Λ. Moreover, we may make the following definitions.

DEFINITION 2.3.7. For a finitely generated Λ-module M which is pseudo-isomorphic to a Λ-module as in (2.3.2), the quantities

$$\lambda(M) = \sum_{i=1}^{g} k_i \deg(f_i) \quad \text{and} \quad \mu(M) = \sum_{j=1}^{h} \mu_j$$

are known as the λ-invariants and μ-invariants of M, respectively.

REMARK 2.3.8. The λ-invariant of a finitely generated Λ-module M is the $\mathbb{Z}_p$-rank of the Λ-torsion subgroup of M.

DEFINITION 2.3.9. The characteristic polynomial of a finitely generated Λ-module M which is pseudo-isomorphic to a module as in (2.3.2) Theorem 2.3.6 is defined to be $p^{\mu(M)} \prod_{i=1}^{g} f_i^{k_i}$, and the characteristic ideal $\mathrm{char}(M)$ is the ideal of Λ which it generates.

DEFINITION 2.3.10. For a Λ-module M, we let M^ι denote the Λ-module that is M as a pro-p group and upon which $f \in \Lambda$ acts as multiplication by $\iota(f)$ on M, where

$$\iota(f)(T) = f((T+1)^{-1} - 1).$$

The following can be seen through a bit of commutative algebra.

PROPOSITION 2.3.11 (IWASAWA). *The Λ-modules X_∞^ι and $A_\infty^\vee$ are pseudo-isomorphic.*

In particular, we have $\mu(X_\infty) = \mu(A_\infty^\vee)$ and $\lambda(X_\infty) = \lambda(A_\infty^\vee)$, while if f is the characteristic polynomial of X_∞, then $\iota(f)$ is the characteristic polynomial of $A_\infty^\vee$.

The structure theorem for finitely generated, torsion Λ-modules has direct consequences for the growth of the orders of the groups A_n. That is, Iwasawa proved the following [**Iwa1**].

THEOREM 2.3.12 (IWASAWA). *We have*

$$|A_{n+1}| = p^{p^n\mu+n\lambda+\nu}$$

for $n \geq 0$ sufficiently large, where $\mu = \mu(X_\infty)$, $\lambda = \lambda(X_\infty)$, and $\nu \in \mathbb{Z}$.

IDEA OF PROOF. We explain the idea and leave the details to the reader. In our case of interest, the map $(X_\infty)_{\Gamma^{p^n}} \to A_{n+1}$ between the Γ^{p^n}-coinvariant group of X_∞ (i.e., the largest quotient on which $\Gamma^{p^n} = 1 + p^{n+1}\mathbb{Z}_p$ acts trivially) is an isomorphism. This is a consequence of the facts that p is the unique prime over p in $F = \mathbb{Q}(\mu_p)$ and totally ramified in F_∞. (In general, it will have kernel and cokernel bounded in n.). Since X_∞ is pseudo-isomorphic to a direct sum as in (2.3.2), we again obtain a map between the Γ^{p^n}-coinvariant groups with kernel and cokernel bounded (and eventually stable) in n. These kernels and cokernels will contribute to the integer ν. The result is the reduced to a statement about the growth of coinvariant groups of quotients of Λ by principal ideals. For example, $\mathbb{F}_p[\![T]\!]/((T+1)^{p^n} - 1)$ is an $\mathbb{F}_p$-vector space of dimension p^n, explaining the occurrence of $p^n\mu$ in the exponent. □

Regarding the μ-invariant, Ferrrero and Washington proved the following theorem [**FeWa**].

THEOREM 2.3.13 (FERRERO-WASHINGTON). *The μ-invariant of X_∞ is zero.*

REMARK 2.3.14. The Ferrero-Washington theorem applies more generally to abelian fields F. Iwasawa conjectured that $\mu(X_\infty) = 0$ for all number fields F.

By class field theory, the group A_n is isomorphic to the Galois group of the maximal unramified abelian p-extension of F_n. It follows that X_∞ is continuously isomorphic to the Galois group of the maximal unramified abelian pro-p extension L_∞ of $F_\infty = \mathbb{Q}(\mu_{p^\infty})$.

The isomorphism $X_\infty \cong \mathrm{Gal}(L_\infty/F_\infty)$ is one of Λ-modules with respect to the continuous action of $\sigma \in \Gamma$ on $\tau \in \mathrm{Gal}(L_\infty/F_\infty)$ given by lifting σ to $\tilde{\sigma} \in \mathrm{Gal}(L_\infty/\mathbb{Q})$ and conjugating:

$$\sigma \cdot \tau = \tilde{\sigma}\tau\tilde{\sigma}^{-1}.$$

This is independent of the choice of $\tilde{\sigma}$ as X_∞ is abelian.

DEFINITION 2.3.15. We refer to the Λ-module $X_\infty \cong \mathrm{Gal}(L_\infty/F_\infty)$ as the unramified Iwasawa module over F_∞. The Λ-module A_∞ is called the p-part of the class group of F_∞.

Similarly, we may define the p-ramified Iwasawa module over F_∞ as follows.

DEFINITION 2.3.16. The p-ramified Iwasawa module $\mathfrak{X}_\infty$ is the Galois group of the maximal pro-p, unramified outside p (and any real places) extension of F_∞, which is a Λ-module under the continuous action of Γ given by lifting and conjugating.

REMARK 2.3.17. The Λ-rank of $\mathfrak{X}_\infty$ is $\frac{p-1}{2}$ (for $F = \mathbb{Q}(\mu_p)$).

Any $\mathbb{Z}_p$-module M with a commuting action of an involution (e.g., a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-module, considering the element $-1 \in \mathbb{Z}_p$) has a decomposition into (± 1)-eigenspaces (or plus and minus parts) for its action: let us write these as $M^\pm$ so that $M = M^+ \oplus M^-$. (Such a decomposition does not in general exist if $p = 2$, but we can still speak of plus and minus parts.)

The plus part $\mathfrak{X}_\infty^+$ is in fact torsion. In fact, Kummer theory yields the following theorem of Iwasawa [**Iwa2**]. Recall that $\mathbb{Z}_p(1)$ is the compact $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-module (resp., $\mathbb{Z}_p[\![G_\mathbb{Q}]\!]$-module) that is $\mathbb{Z}_p$ as a compact $\mathbb{Z}_p$-module and upon which $a \in \mathbb{Z}_p^\times$ (resp., $\sigma \in G_\mathbb{Q}$) acts by multiplication by a (resp., by $\chi_p(\sigma)$).

THEOREM 2.3.18 (IWASAWA). *We have $\mathfrak{X}_\infty^+ \cong (A_\infty^-)^\vee(1)$ as $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-modules.*

PROOF. Any p-ramified Kummer extension of F_n that is cyclic of degree dividing p^n is generated by the p^nth root of an element $a \in F_n^\times$ such that $a\mathbb{Z}[\mu_{p^n}]$ is the product of a power of the prime over p and the p^nth power of a fractional ideal prime to p. Let $\mathcal{B}_n$ denote the subgroup of $F_n^\times$ consisting of such elements. By Kummer theory, we have

$$\mathcal{B}_n/(\mathcal{B}_n \cap F_n^{\times p^n}) \cong \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n}),$$

where $\mathfrak{X}_n$ is the Galois group of the maximal p-ramified extension of F_n. Our description of $\mathcal{B}_n$ therefore provides an exact sequence

$$0 \to \mathcal{E}_n/\mathcal{E}_n^{p^n} \to \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n}) \to A_n[p^n] \to 0, \tag{2.3.3}$$

where $\mathcal{E}_n = \mathbb{Z}[\frac{1}{p}, \mu_{p^n}]^\times \otimes_\mathbb{Z} \mathbb{Z}_p$ is the p-completion of the group of p-units in F_n. (With the identification just described, the surjection in the sequence takes $a \in \mathcal{B}_n$ to the class of the fractional ideal $\mathfrak{a}$ such that $\mathfrak{a}^{p^n} = a\mathbb{Z}[\frac{1}{p}, \mu_{p^n}]$.)

We consider the direct limit over n of the minus parts of the sequences (2.3.3). Note that $\mathcal{E}_n^- \cong (\mathcal{E}_n/\mathcal{E}_n^{p^n})^- \cong \mu_{p^n}$, and $\varinjlim \mu_{p^n} = 0$ here, since the maps in the direct system of these groups are p-power maps. Since

$$\varinjlim_n \mathrm{Hom}(\mathfrak{X}_n, \mu_{p^n})^- \cong \varinjlim_n (\mathfrak{X}_n^+/p^n\mathfrak{X}_n^+)^\vee(1) \cong \left(\varprojlim_n \mathfrak{X}_n^+/p^n\mathfrak{X}_n^+\right)^\vee(1) \cong (\mathfrak{X}_\infty^+)^\vee(1)$$

and $\varinjlim A_n[p^n]^- \cong A_\infty^-$, we obtain the result. □

REMARK 2.3.19. For an arbitrary CM field F and any prime p, the plus part is again torsion, and if F contains μ_q, then Theorem 2.3.18 holds for F_∞.

COROLLARY 2.3.20. *Let f denote the chara cteristic polynomial of X_∞^-. Then the characteristic polynomial of $\mathfrak{X}_\infty^+$ is $f(\upsilon(T+1)^{-1} - 1)$, where $\upsilon = \chi_p(\gamma)$.*

Iwasawa showed that X_∞^- has no nonzero finite Λ-submodule [**Iwa2**]. Between this and the Ferrero-Washington theorem, we have the following.

PROPOSITION 2.3.21. *The Λ-module X_∞^- is p-torsion free.*

REMARK 2.3.22. What we shall be most interested in below for $F = \mathbb{Q}(\mu_p)$ is a finer decomposition of $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$-modules. That is, if M is such a module, then as a $\mathbb{Z}_p[(\mathbb{Z}/p\mathbb{Z})^\times]$-module, it has a decomposition into eigenspaces as before. Each of these eigenspaces $M^{(i)}$ is then a Λ-module.

2.4. Kubota-Leopoldt p-adic L-functions

We have the following congruences among generalized Bernoulli numbers.

PROPOSITION 2.4.1. *For positive integers j and k with $j \equiv k \bmod p^{r-1}(p-1)$ for some $r \geq 1$, and a $\overline{\mathbb{Q}}_p$-valued primitive Dirichlet character χ with $\chi(-1) = (-1)^j$ and such that $\chi\omega^j \neq 1$, we have*

$$(1 - \chi(p)p^{j-1})\frac{B_{j,\chi}}{j} \equiv (1 - \chi(p)p^{k-1})\frac{B_{k,\chi}}{k} \bmod p^r$$

and for any $i \geq 1$, we have

$$\frac{B_{j,\chi}}{j} \equiv \frac{B_{i,\chi\omega^{j-i}}}{i} \bmod p.$$

These congruences can be used in proving the existence and continuity of p-adic L-functions, as constructed by Kubota and Leopoldt [**KuLe**].

THEOREM 2.4.2 (KUBOTA-LEOPOLDT). *Let χ be an even primitive Dirichlet character of conductor Mp^r for some $r \geq 0$ and $M \geq 1$ prime to p. Given an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$, there exists a unique p-adic analytic (aside from $s = 1$ if $\chi = 1$, where it has a pole with residue $1 - p^{-1}$) function $L_p(\chi, s)$ on $\mathbb{Z}_p$ satisfying*

$$L_p(\chi, 1 - i) = (1 - \chi\omega^{-i}(p)p^{i-1})L(\chi\omega^{-i}, 1 - i)$$

for all $i \geq 1$.

DEFINITION 2.4.3. The function $L_p(\chi, s)$ is the Kubota-Leopoldt p-adic L-function of χ.

Let us indicate briefly how the Kubota-Leopoldt p-adic L-function can be constructed.

DEFINITION 2.4.4. For each $n \geq 1$, the nth Bernoulli polynomial $B_n(X) \in \mathbb{Q}[x]$ is defined by the power series expansion

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!},$$

EXAMPLE 2.4.5. We have $B_0(X) = 1$, $B_1(X) = X - \frac{1}{2}$, and $B_2(X) = X^2 - X + \frac{1}{6}$.

The relationship between Bernoulli polynomials and Bernoulli numbers is seen in the following lemma.

LEMMA 2.4.6. *If χ is a Dirichlet character of modulus (dividing) N, then*

$$B_{k,\chi} = N^{k-1}\sum_{a=1}^{N} \chi(a)B_k\left(\frac{a}{N}\right).$$

Using the Bernoulli polynomials, we can construct a distribution on $\mathbb{Q}/\mathbb{Z}$ known as the Bernoulli distribution. That is, these polynomials have the property that

$$M^{k-1}B_k\left(\frac{a}{M}\right) = \sum_{j=0}^{N/M-1} N^{k-1}B_k\left(\frac{a + jM}{N}\right)$$

for M dividing N.

SKETCH OF CONSTRUCTION OF p-ADIC L-FUNCTIONS. For simplicity of presentation, we focus on the case that our Dirichlet character has conductor an odd prime p, i.e., is an even power of ω. Form the modified Stickelberger elements

$$\Theta_n = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \left(\frac{a}{p^n} - \frac{1}{2}\right)[a]^{-1} \in \mathbb{Q}[(\mathbb{Z}/p^n\mathbb{Z})^\times]$$

out of the values $B_1(\frac{a}{p^n}) = \frac{a}{p^n} - \frac{1}{2}$. These elements are compatible under the natural projection maps and thus define in the inverse limit an element Θ_∞ of the total quotient ring $\mathcal{Q}$ of $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$.

We can take the projection of Θ_∞ to $\mathcal{Q}^{(1-k)}$, obtaining an element $\Theta_\infty^{(k)}$. Identifying $\gamma - 1$ with T and Δ with $\mu_{p-1}(\mathbb{Z}_p)$, we have

$$\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^{(1-k)} \cong \Lambda[\Delta]^{(1-k)} \cong \Lambda \cong \mathbb{Z}_p[\![T]\!],$$

so $\Theta_\infty^{(k)}$ lies in the quotient field of Λ.

For $k \not\equiv 0 \bmod p-1$, the element $\Theta_\infty^{(k)}$ lies in $\mathbb{Z}_p[\![T]\!]$. For $k \equiv 0 \bmod p-1$, it can be made to have integral coefficients by multiplication by $[v] - v$, which is sufficient to avoid convergence issues, by premultiplying and then multiplying back in the factor after evaluation. (For such k, the numerator of $\Theta_\infty^{(k)}$ is a unit power series.) The p-adic L-function for the character ω^k is then defined by

$$L_p(\omega^k, s) = -\Theta_\infty^{(k)}(v^s - 1)$$

for $s \in \mathbb{Z}_p$. □

2.5. The Iwasawa main conjecture

We present the classical Iwasawa main conjecture here over the cyclotomic $\mathbb{Z}_p$-extension of $F = \mathbb{Q}(\mu_p)$, for p odd, which is a theorem of Mazur and Wiles. This conjecture was stated more generally for any abelian field F, and it was proven by Mazur and Wiles for odd p [**MaWi1**]. Wiles treated the case $p = 2$, as well as a generalization of the main conjecture to totally real fields [**Wil2**]. The only real difference from the case of $\mathbb{Q}(\mu_p)$ in the statement for more general abelian fields is the need for a discussion of "eigenspaces" for more general finite order characters. The reader might therefore be able to determine the appropriate formulation.

Let us set $f_k = -\Theta_\infty^{(k)}$ for $k \not\equiv 0 \bmod p-1$ so that

$$f_k(v^s - 1) = L_p(\omega^k, s).$$

For $k \equiv 0 \bmod p-1$, we set $f_k = 1$. Iwasawa stated in [**Iwa4**] and proved in [**Iwa5**] the following theorem under the condition that $A^{(k)} = 0$ (where $A = A_1$ is the p-part of the class group of F). It is alternately known as the Iwasawa main conjecture, Iwasawa's main conjecture, and the main conjecture of Iwasawa theory, or simply the main conjecture.

THEOREM 2.5.1 (IWASAWA MAIN CONJECTURE, MAZUR-WILES). *Let k be an even integer. Then*

$$\mathrm{char}(X_\infty^{(1-k)}) = (f_k).$$

REMARK 2.5.2. The analytic class number tells us that the orders $h_n^{(p)}$ of the groups in the tower can be expressed in terms of products of Bernoulli numbers. From this, one can conclude that

$$\lambda(X_\infty^-) = \sum_{j=0}^{(p-3)/2} \lambda(\Lambda/(f_{2j})),$$

as well as the corresponding equality of μ-invariants (which we already know to equal zero by the Ferrero-Washington theorem). Consequently, to prove the main conjecture, it suffices to show either that $\mathrm{char}(X_\infty^{(1-k)})$ divides (f_k) for all even k, or vice versa.

The approach to the main conjecture due to Mazur and Wiles, which exploits the geometry of modular curves near the cusps, is to show that (f_k) divides $\mathrm{char}(X_\infty^{(1-k)})$.

REMARK 2.5.3. Rubin gave another proof of the main conjecture by exhibiting the opposite divisibility, bounding the size of the unramified Iwasawa module by exploiting the method of Euler systems of Thaine and Kolyvagin (see the lectures of D. Loeffler and S. Zerbes). This uses norm relations among cyclotomic units in auxiliary cyclotomic extensions of the fields $\mathbb{Q}(\mu_{p^n})$. Our focus in these notes is on the approach of Mazur and Wiles. It's important, however, to be aware that analogues of the analytic class number formula are not generally available for the Selmer groups of Galois representations, and so proofs of more general main conjectures for these objects have required both the study of higher-dimensonal Galois representations and congruences and the method of Euler systems.

Let us next discuss some equivalent formulations of the Iwasawa main conjecture. The first describes the characteristic ideal of the p-ramified Iwasawa module $\mathfrak{X}_\infty$. Set

$$g_k(T) = f_k(\upsilon(1+T)^{-1} - 1),$$

so

$$g_k(\upsilon^s - 1) = L_p(\omega^k, 1-s)$$

for $k \not\equiv 0 \bmod p-1$. Then the main conjecture is equivalent to the following statement.

THEOREM 2.5.4 (IWASAWA MAIN CONJECTURE, VERSION 2). *Let k be an even integer. Then*

$$\mathrm{char}(\mathfrak{X}_\infty^{(k)}) = (g_k).$$

A third equivalent version of the main conjecture can be given in terms of the norm compatible sequences in the p-completions of the unit groups of the fields F_n. Let

$$\mathcal{E}_n = \mathbb{Z}_p[\tfrac{1}{p}, \mu_{p^n}]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

and set $\mathcal{E}_\infty = \varprojlim_n \mathcal{E}_n$, the transition maps being induced by the norm maps of the field extensions. Similarly, let $\mathcal{U}_n$ denote the pro-p completion of $\mathbb{Q}_p(\mu_{p^n})^\times$, and set $\mathcal{U}_\infty = \varprojlim_n \mathcal{U}_n$. Class field theory provides an exact sequence

$$0 \to \mathcal{E}_\infty \to \mathcal{U}_\infty \to \mathfrak{X}_\infty \to X_\infty \to 0,$$

the first map being injective by a theorem known as the weak Leopoldt conjecture (see the lectures of J. Coates).

Let $\mathcal{C}_n$ denote the subgroup of $\mathcal{E}_n$ topologically generated by the cyclotomic p-units $1-\zeta_{p^n}^i$ with $p \nmid i$, and set $\mathcal{C}_\infty = \varprojlim_n \mathcal{C}_n$. The abelian pro-$p$ group $\mathcal{E}_\infty/\mathcal{C}_\infty$ is a Λ-torsion module that is fixed under the action of complex conjugation.

The group $(\mathcal{U}_\infty/\mathcal{C}_\infty)^+$ has a very fascinating description by a result of Iwasawa. We describe Coleman's approach to it [**Col2**]. It begins with his construction of Coleman power series [**Col1**].

THEOREM 2.5.5 (COLEMAN). *Given a norm compatible sequence $u = (u_n)_n \in \mathcal{U}_\infty$, there exists a unique power series $f \in \mathbb{Z}_p[\![T]\!]$ with $f(\zeta_{p^n}-1) = u_n$ for all $n \geq 1$.*

The power series g_u attached to $u \in \mathcal{U}_\infty$ by Coleman's theorem is known as the Coleman power series of u. The modified logarithm

$$\ell_p(g_u) = \log(f(T)) - \frac{1}{p}\log(f((T+1)^p - 1))$$

of this f lies in $\mathbb{Z}_p[\![T]\!]$ as well. The completed group ring $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ acts on $\mathbb{Z}_p[\![T]\!]$ via the continuous $\mathbb{Z}_p$-linear action under which $a \in \mathbb{Z}_p^\times$ maps T to $(1+T)^a - 1$. We then define an injective homomorphism

$$\phi\colon \mathcal{U}_\infty \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$$

on $u \in \mathcal{U}_\infty$ by letting $\phi(u) \in \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ be the unique element such that $\phi(u)\cdot T = \ell_p(g_u)$. On the ω^k-eigenspace for $k \not\equiv 0 \bmod p-1$, the homomorphism has image in $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$. Coleman proved that

$$\phi((1-\zeta_{p^n})_n) = \Theta_\infty.$$

Consequently, we have the following theorem, originally due to Iwasawa [**Iwa3**].

THEOREM 2.5.6 (IWASAWA). *Let k be an even integer. Then there is a canonical isomorphism of Λ-modules*

$$\mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \cong \Lambda/(f_k).$$

For an even integer k, we have an exact sequence

$$0 \to \mathcal{E}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \to \mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \to \mathfrak{X}_\infty^{(k)} \to X_\infty^{(k)} \to 0 \tag{2.5.1}$$

of finitely generated Λ-torsion modules. The alternating product of characteristic ideals in an exact sequence of such modules is the unit ideal. By this and Theorem 2.5.6, we have the following equivalent form of the main conjecture.

THEOREM 2.5.7 (IWASAWA MAIN CONJECTURE, VERSION 3). *Let k be an even integer. Then the characteristic ideals of $\mathcal{E}_\infty^{(k)}/\mathcal{C}_\infty^{(k)}$ and $X_\infty^{(k)}$ are equal.*

Greenberg conjectured the following weaker form of Vandiver's conjecture [**Gre2**].

CONJECTURE 2.5.8 (GREENBERG). *The Iwasawa module X_∞^+ is finite.*

EXERCISE 2.5.9. Greenberg's conjecture has equivalent formulations in the statements that $A_\infty^+ = 0$ and that $\mathcal{E}_\infty = \mathcal{C}_\infty$.

REMARK 2.5.10. In fact, Greenberg conjectured that X_∞^+ is finite with F_∞ replaced by the cyclotomic $\mathbb{Z}_p$-extension of any totally real or CM field, in which case X_∞^+ is not in general zero. The first occurrence of the Iwasawa main conjecture for general abelian fields in print is found in a paper of Greenberg's [**Gre1**].

From Theorem 2.5.6, we conclude the following.

COROLLARY 2.5.11. *If Greenberg's conjecture that $X_\infty^{(k)}$ is finite holds, then the Iwasawa main conjecture holds for $X_\infty^{(1-k)}$, and the latter Λ-module is pseudo-cyclic, i.e., pseudo-isomorphic to $\Lambda/(f_k)$.*

REMARK 2.5.12. Iwasawa had proven that $X_\infty^{(1-k)}$ is cyclic if $X_\infty^{(k)} = 0$ in [**Iwa5**]. Coates and Lichtenbaum conjectured that $X_\infty^{(k)}$ is pseudo-cyclic (in fact, for even eigenspaces of general abelian fields of degree prime to p) [**CoLi**].

Finally, we remark that as a consequence of the main conjecture, Mazur and Wiles were able to prove a precise formula for the order of the odd eigenspaces of $A = A_1$. This provides a direct refinement of the Herbrand-Ribet theorem.

THEOREM 2.5.13 (MAZUR-WILES). *For every even integer k, we have*

$$|A^{(1-k)}| = p^{v_p(B_{1,\omega^{k-1}})},$$

where v_p denotes the p-adic valuation.

CHAPTER 3

Theory of modular forms

In this chapter, we briefly review the theory of modular curves and modular forms, tailored to our study. Our interest in these notes is in modular curves as they apply to the study of the arithmetic of cyclotomic fields.

We can only hope in these subsections to give an overly short and hurried description of the theory, presuming that the reader is already somewhat familiar with the subject, as we shall assume more completely in the lectures themselves. We recommend that the reader unfamiliar with the subject consult a good textbook (e.g., [**DiSh, Lan, Shi2, Hid4**]) and other available sources rather than to attempt to gain anything close to a full understanding solely through these notes.

3.1. Modular curves over $\mathbb{C}$

The group $\mathrm{GL}_2(\mathbb{R})_+$ of invertible matrices with positive determinant acts on the complex upper half-plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

by Möbius transformations: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$, then

$$\gamma \cdot z = \frac{az+b}{cz+d} \in \mathbb{H}.$$

This group acts by the same formula on $\mathbb{R} \cup \{\infty\}$, but in fact what we shall be interested in is $\mathbb{Q} \cup \{\infty\}$, which is also preserved under the action.

Definition 3.1.1. The extended upper half-plane is $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

We give $\mathbb{H}^*$ a topology extending the usual Euclidean topology on $\mathbb{H}$ by declaring a basic open neighborhood of a rational number to be the set consisting of said point and an open disk tangent to it and a basic open neighborhood of infinity to be the set consisting of it and all complex numbers with imaginary part at least some fixed nonnegative number. The group $\mathrm{GL}_2(\mathbb{Q})_+ = \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2(\mathbb{R})_+$ then acts continuously on $\mathbb{H}^*$.

Definition 3.1.2. Let N be a positive integer.

(1) The principal congruence subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, i.e., the matrices congruent to 1 modulo N.
(2) A congruence subgroup of level N is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ but not $\Gamma(M)$ for any proper divisor M of N.
(3) The congruence subgroup $\Gamma_0(N)$ is the subgroup of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that are upper-triangular modulo N.

(4) The congruence subgroup $\Gamma_1(N)$ is the subgroup of matrices in $\Gamma_0(N)$ that are unipotent modulo N.

DEFINITION 3.1.3. For a congruence subgroup Γ, we have the open and closed modular curves $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ and $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$, respectively. The cusps of $X(\Gamma)$ are the points of the finite set

$$C(\Gamma) = X(\Gamma) - Y(\Gamma) = \Gamma\backslash(\mathbb{Q} \cup \{\infty\}).$$

DEFINITION 3.1.4. For $j \in \{0, 1\}$, we set $Y_j(N) = Y(\Gamma_j(N))$ and $X_j(N) = X(\Gamma_j(N))$ for $j \in \{0, 1\}$, and we let $C_j(N)$ denote their sets of cusps.

REMARK 3.1.5. The closed curves are compactifications of the open curves. The modular curves can be given the structure of Riemann surfaces, taking care of the charts around the cusps and the elliptic points, the latter being the classes of the points i, $e^{\pi i/3}$, and $e^{2\pi i/3}$ in a manner that we omit here.

For the most part, we will be concerned with the modular curve $X_1(N)$. The following lemma describes its cusps.

LEMMA 3.1.6. *Two fractions $\frac{a}{c}$ and $\frac{a'}{c'}$ in reduced form represent the same cusp of $X_1(N)$ if and only if $c \equiv \pm c' \bmod N$ and $a \equiv \pm a' \bmod (c, N)$ for the same choice of sign.*

Modular curves have fundamental domains in $\mathbb{H}^*$, which (we shall not define but) in particular are connected subsets of $\mathbb{H}^*$ that project bijectively onto $X(\Gamma)$.

EXAMPLE 3.1.7. The set $\{z \in \mathbb{H} \mid \mathrm{Re}(z) \le \frac{1}{2},\ |z| \ge 1\} \cup \{\infty\}$ is the closure of a fundamental domain for $X(\mathrm{SL}_2(\mathbb{Z}))$.

We next turn to Hecke operators. Consider the divisor group $\mathrm{Div}(X_1(N))$ that is the free abelian group on the points of $X_1(N)$. Note that the action of $\mathrm{GL}_2(\mathbb{Q})_+$ on $X_1(N)$ extends additively to an action on divisors.

DEFINITION 3.1.8. For $j \in \mathbb{Z}$ prime to the level N, the diamond operator

$$\langle j \rangle \colon \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$$

is the map induced by the Möbius transformation associated to any matrix $\delta_j \in \Gamma_0(N)$ with lower right entry congruent to j modulo N. For j sharing a common divisor with N, we set $\langle j \rangle = 0$.

The nth Hecke operators T_n for $n \ge 1$ may be defined via correspondences. That is, we consider the correspondence on the level N modular curve that is represented by the diagram

$$\begin{array}{ccc} & X(\Gamma_1(N) \cap \Gamma_0(Nn)) & \\ {\scriptstyle \epsilon_1}\swarrow & & \searrow{\scriptstyle \epsilon_n} \\ X_1(N) & & X_1(N). \end{array} \tag{3.1.1}$$

For $d \ge 1$ (dividing n), the degeneracy map ϵ_d is induced by the map $d \colon \mathbb{H}^* \to \mathbb{H}^*$ given by multiplication by d.

DEFINITION 3.1.9. For $n \geq 1$, the nth Hecke operator $T_n \colon \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$ is the unique homomorphism that on the class $\{x\}$ of $x \in X_1(N)$ is given by

$$T_n(\{x\}) = \sum_{y \in \epsilon_1^{-1}(x)} \{\epsilon_n(y)\},$$

That is, T_n is given by pulling back by ϵ_1 and then pushing forward by ϵ_n.

EXERCISE 3.1.10. For a prime p, the application of T_p to a $\mathbb{C}$-point represented by $z \in \mathbb{H}^*$ is the divisor given by the sum over the application to z of the right coset representatives of the $\Gamma_1(N)$-double cosets of the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. One set of such representatives consists of the matrices $\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)$ for $0 \leq j \leq p-1$ and, if $p \nmid N$, the matrix $\delta_p \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (given a choice of δ_p as above).

REMARK 3.1.11. It may seem a bit silly at first, but we may also think of $\langle j \rangle$ for j prime to N as defined by a correspondence $X_1(N) \xleftarrow{\mathrm{id}} X_1(N) \xrightarrow{\delta_j} X_1(N)$ given by pulling back by the identity and pushing forward by the action of δ_j.

EXERCISE 3.1.12. The Hecke operators and the diamond operators defined above are all mutually commutative.

Now we turn to general Hecke operators.

EXERCISE 3.1.13. For a prime p and $n \geq 1$, the p^{n+1}th Hecke operator satisfies

$$T_{p^{n+1}} = T_{p^n} T_p - p\langle p \rangle T_{p^{n-1}},$$

where $T_1 = 1$. Moreover, if m and n are relatively prime postiive integers, then $T_{mn} = T_m T_n$.

Given an operator defined by a correspondence, we may define its transpose as the operator given by switching the order of the two arrows in the diagram defining it.

DEFINITION 3.1.14. The nth adjoint Hecke operator T_n^* is the transpose of T_n, and the diamond operator $\langle j \rangle^*$ is the transpose of $\langle j \rangle$ for j prime to N (and zero otherwise).

One might note that $\langle j \rangle^* = \langle j \rangle^{-1}$ for j prime to N.

REMARK 3.1.15. Alternatively, the adjoint operator T_n^* to T_n is given by $T_n^* = w_N T_n w_N^{-1}$, where w_N is the Atkin-Lehner operator induced by the action of the matrix $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. We also have $\langle j \rangle^* = w_N \langle j \rangle w_N^{-1}$.

3.2. Moduli-theoretic interpretation

The modular curves we have defined are not just complex manifolds, but in fact varieties, cut out by polynomial equations. Even better, for small enough Γ, we can define them as the $\mathbb{C}$-points of schemes over $\mathbb{Z}$.

For $N \geq 4$, the modular curve $Y_1(N)$ is the moduli space with S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S equal to the set of isomorphism classes of pairs (E, P), where E is an elliptic curve over S and P is a point of E of order N, which we take to mean given by an injective morphism $(\mathbb{Z}/N\mathbb{Z})_{/S} \to E[N]_{/S}$ of S-schemes from the constant group scheme $\mathbb{Z}/N\mathbb{Z}$ over S to the

subgroup scheme $E[N]$ of E of N-torsion points, viewed as an S-scheme. In fact, it is a fine moduli scheme, which is to say that it represents the functor that takes S to the aforementioned set, and it is smooth of finite type over $\mathbb{Z}[\frac{1}{N}]$.

Similarly, $Y_0(N)$ over $\mathbb{Z}[\frac{1}{N}]$ is the "course" moduli space with S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S equal to the set of isomorphism classes (E, C), where E is an elliptic curve over S and C is a cyclic subgroup of order N, i.e., an S-subgroup scheme of $E[N]$ that is (étale) locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})_{/S}$. (We shall not define these notions more precisely.)

REMARK 3.2.1. There is an implicit choice of "model" made here so that we can define $Y_1(N)$ over a ring without Nth roots of unity, i.e., we take a constant subscheme as part of the moduli data, rather than the S-scheme $(\mu_N)_{/S}$.

The closed modular curves $X_1(N)$ and $X_0(N)$ of level N are smooth, proper curves over $\mathbb{Z}[\frac{1}{N}]$ containing the corresponding open modular curve as an open subscheme. These again have a moduli interpretation using generalized elliptic curves in place of elliptic curves, which is necessary at the cusps [**DeRa**]. These cusps are points defined over cyclotomic integer rings with N inverted.

REMARK 3.2.2. Our choice of model insures that the cusp 0 on $X_1(N)$ is rational, defined over $\operatorname{Spec}\mathbb{Z}[\frac{1}{N}]$, whereas ∞ is a $\operatorname{Spec}\mathbb{Z}[\mu_N, \frac{1}{N}]^+$-point of $X_1(N)$.

REMARK 3.2.3. In fact, the modular curves $Y_1(N)$ and $X_1(N)$ can be defined over $\mathbb{Z}$ by taking the normalizations of the affine and projective j-lines over $\mathbb{Z}$ inside the $\mathbb{Z}[\frac{1}{N}]$-schemes, though we must modify the moduli interpretation, using Drinfeld level structures in the place of points [**KaMa**]. These schemes are still flat over $\mathbb{Z}$, though no longer étale. (See [**Con**] for more information, stronger results, and a much more careful treatment.)

The Hecke operators on the group $\operatorname{Div}(X_1(N)(S))$ of formal sums of S-points for a $\mathbb{Z}[\frac{1}{N}]$-scheme S are also defined via correspondences as in (3.1.1), i.e., T_n is defined as $(\epsilon_n)_*\epsilon_1^*$ once we define degeneracy maps. The diamond operator $\langle j\rangle$ is defined more simply by

$$\langle j\rangle(E, P) = (E, jP).$$

On S-points of the open modular curves for a $\mathbb{Z}[\frac{1}{Nn}]$-scheme S, the degeneracy maps have the following description. Let d divide n. For an elliptic curve E over S, a point P of order N on E, and cyclic subgroup C of E of order Nn containing P, in the senses defined above, the triple (E, P, C) defines a point of $X(\Gamma_1(N) \cap \Gamma_0(n))(S)$. The degeneracy map

$$\epsilon_d \colon X(\Gamma_1(N) \cap \Gamma_0(n)) \to X_1(N)$$

for d dividing n is defined on the S-point (E, P, C) by

$$\epsilon_d(E, P, C) = (E/C', P' + C'),$$

where C' is the cyclic subgroup scheme of order d in C and P' is any point of E with $P = dP'$. The resulting formula for $(\epsilon_n)_*\epsilon_1^*$ works for points of any $\mathbb{Z}[\frac{1}{N}]$-scheme S.

THEOREM 3.2.4 (KATZ-MAZUR). *There exists a smooth $\mathbb{Z}[\frac{1}{N}]$-scheme called the universal elliptic curve $\mathcal{E}_1(N)$ over $Y_1(N)$, the fiber above a point $(E,P) \in Y_1(N)(S)$ being the elliptic curve E itself.*

REMARK 3.2.5. The scheme $\mathcal{E}_1(N)$ is an open subscheme of a universal generalized elliptic curve over $X_1(N)$, which has generalized elliptic curves as fibers.

For later use, we recall theta functions and Siegel units (see [**Kat**, Section 1]).

DEFINITION 3.2.6. Let $\mathcal{E} = \mathcal{E}_1(N)$. For an integer $c > 1$ and prime to 6, the theta function

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

is the unique element with Cartier divisor $c^2(0) - \mathcal{E}[c]$ that is invariant under norm maps attached to multiplication by a, for a prime to c.

EXERCISE 3.2.7. Let $c, d > 1$ be prime to 6. Then $d^*(\theta_c)\theta_c^{-d^2} = c^*(\theta_d)\theta_d^{-c^2}$ in $\mathcal{O}(\mathcal{E}\backslash\mathcal{E}[cd])^\times$.

DEFINITION 3.2.8. Let $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, and let $c \geq 1$ be prime to $6N$. The Siegel unit ${}_cg_u \in \mathcal{O}(Y_1(N))^\times$ is the pullback of ${}_c\theta$ by the section of $\mathcal{E}_1(N) \to X_1(N)$ taking $(E,P) \in X_1(N)(S)$ for a $\mathbb{Z}[\frac{1}{N}]$-scheme S to the point uP on its fiber E in $\mathcal{E}_1(N)(S)$.

DEFINITION 3.2.9. For $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, the Siegel unit

$$g_u \in \mathcal{O}(Y_1(N))^\times \otimes_{\mathbb{Z}} \mathbb{Z}[\tfrac{1}{6N}]$$

is the unique element with the property that for any $c > 1$ prime to $6N$, we have

$$ {}_cg_u = \frac{g_u^{c^2}}{g_{cu}}.$$

REMARK 3.2.10. Over $\mathbb{C}$, the Siegel unit g_u has the q-expansion

$$(-\zeta_N)^{-\frac{u}{2}} q^{\frac{1}{12}} \prod_{n=0}^{\infty}(1-q^n\zeta_N^u)\prod_{n=1}^{\infty}(1-q^n\zeta_N^{-u}). \tag{3.2.1}$$

(The power of $-\zeta_N$ is placed here somewhat artificially, but one gets the q-expansion of ${}_cg_u$ without tensoring with $\mathbb{Z}[\frac{1}{6N}]$ from it.)

3.3. Modular forms

DEFINITION 3.3.1. A modular form of weight k and level N is a holomorphic function $f\colon \mathbb{H}^* \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ and $z \in \mathbb{H}^*$.

Since $f(z+1) = f(z)$ for all $z \in \mathbb{H}$, to say that f is holomorphic at ∞ is to say that it has a Fourier expansion in $q = e^{2\pi iz}$ (or q-expansion) given by

$$f(q) = \sum_{n=0}^{\infty} a_n(f) q^n \tag{3.3.1}$$

for some $a_n(f) \in \mathbb{C}$. The $a_n(f)$ are known as its Fourier coefficients. A modular form f is uniquely determined by its Fourier expansion.

DEFINITION 3.3.2. If a modular form f vanishes on $\mathbb{Q} \cup \{\infty\}$, then f is said to be a cusp form.

If f is a cusp form, then $a_0(f) = 0$, though the converse need not hold if its level is greater than 1.

DEFINITION 3.3.3. We let $M_k(N)$ (resp., $S_k(N)$) denote the $\mathbb{C}$-vector space of modular forms (resp., cusp forms) of weight k and level N.

The space $M_k(N)$ breaks up into a direct sum of subspaces corresponding to the Dirichlet characters of modulus N.

DEFINITION 3.3.4. For a character $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, we define the subspace $M_k(N, \chi)$ of modular forms with Nebentypus (or character) χ to be the set of $f \in M_k(N)$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \chi(d) f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. We set

$$S_k(N, \chi) = S_k(N) \cap M_k(N, \chi).$$

The following is then easily verified.

LEMMA 3.3.5. *We have*

$$M_k(N) = \bigoplus_\chi M_k(N, \chi) \quad \text{and} \quad S_k(N) = \bigoplus_\chi S_k(N, \chi),$$

where the direct sums are taken over $\mathbb{C}$-valued characters χ of $(\mathbb{Z}/N\mathbb{Z})^\times$.

We mention a couple of constructions that are useful to us.

DEFINITION 3.3.6. For $f \in M_k(N)$, the L-function $L(f, s)$ is the analytic continuation to $\mathbb{C}$ of the L-series

$$L_p(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}$$

that converges uniformly for $\mathrm{Re}(s) > k$ (or $\frac{k}{2} + 1$ if f is a cusp form). If χ is a Dirichlet character, we may define $L_p(f, \chi, s)$ as the analytic continuation of $\sum_{n=1}^{\infty} a_n(f)\chi(n)n^{-s}$.

EXAMPLE 3.3.7. The Eisenstein series E_k has L-function $L(E_k, s) = \zeta(s)\zeta(s-k+1)$.

We next explore the action of Hecke operators on spaces of modular forms. For this, we make the following definition.

DEFINITION 3.3.8. The group $\mathrm{GL}_2(\mathbb{Q})_+$ acts on $f \in M_k(N)$ on the right by

$$(f|_\gamma)(z) = (cz+d)^{-k} (\det \gamma)^{k-1} f(\gamma z)$$

for $\gamma \in \mathrm{GL}_2(\mathbb{Q})_+$.

This action induces an action of the operator corresponding to the double coset $\Gamma_1(N)\gamma\Gamma_1(N)$ which is given by summing over the applications of the matrices representing the right cosets in its decomposition.

DEFINITION 3.3.9. For $n \geq 1$, the nth Hecke operator T_n on $M_k(N)$ is the $\Gamma_1(N)$-double coset operator associated to $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$.

Diamond operators $\langle j \rangle$ on $M_k(N)$ are defined by the action of δ_j. We have

$$M_k(N, \chi) = \{f \in M_k(N) \mid \langle j \rangle(f) = \chi(j)f\}.$$

We may define the action of general Hecke operators by the recursive formulas of Definition 3.1.13.

EXERCISE 3.3.10. For any prime p, the action of T_p is given on the Fourier expansion of $f \in M_k(N, \chi)$ for a Dirichlet character χ of modulus N is given by

$$a_n(T_p f) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f), \tag{3.3.2}$$

taking $a_{n/p} = 0$ if $p \nmid n$.

DEFINITION 3.3.11. We say that $f \in M_k(N)$ is an eigenform if it is an eigenform (i.e., eigenvector) for all of the Hecke operators T_n and diamond operators $\langle j \rangle$ simultaneously (this latter condition saying that $f \in M_k(N, \chi)$ for some χ).

EXERCISE 3.3.12. If f is an eigenform with $a_1(f) = 1$, then $T_n(f) = a_n(f)f$ for all $n \geq 1$.

DEFINITION 3.3.13. An eigenform with q-coefficient equal to 1 is said to be normalized.

EXAMPLE 3.3.14. Let χ be a p-adic Dirichlet character of of modulus N with $\chi(-1) = (-1)^k$. Suppose that $k > 2$ if $N = 1$. The weight k Eisenstein series $E_{k,\chi} \in M_k(N, \chi)$ with character χ is the level N eigenform

$$E_{k,\chi} = -\frac{B_{k,\chi}}{2k} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1}\chi(d)q^n.$$

REMARK 3.3.15. There is a complement to $S_k(N)$ in $M_k(N)$ with a basis consisting of slightly more general Eisenstein series (see [**DiSh**, Section 3]).

EXERCISE 3.3.16. If f is a normalized eigenform in $M_k(N, \chi)$, then the L-series $L(f, s)$ has an Euler product expansion

$$L(f, s) = \prod_{p \text{ prime}} (1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

DEFINITION 3.3.17. The Petersson inner product

$$\langle\ ,\ \rangle \colon M_k(N) \times S_k(N) \to \mathbb{C}$$

is the positive definite Hermitian pairing defined by

$$\langle f, g \rangle = \frac{1}{\mathrm{Vol}(X_1(N))} \int_{X_1(N)} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2},$$

where the integral is taken over $z = x + iy$ in a fundamental domain in $\mathbb{H}^*$ of the modular curve $X_1(N)$, and $\mathrm{Vol}(X_1(N))$ is the volume of this fundamental domain under the hyperbolic measure $y^{-2}dxdy$.

REMARK 3.3.18. The adjoint Hecke operator T_n^* on $S_k(N)$ is in fact adjoint to T_n under the Petersson inner product, hence its name. If n is prime to N, it satisfies $T_n^* = \langle n\rangle^{-1}T_n$. Recall that $\langle j\rangle^* = \langle j\rangle^{-1}$ for j prime to N.

Since the Hecke operators T_n for n prime to N are normal operators that commute with each other (and the diamond operators), they are simultaneously diagonalizable, and hence we have the following.

THEOREM 3.3.19. *The spaces $M_k(N)$ and $S_k(N)$ have bases consisting of eigenforms for all Hecke operators T_n with n prime to N.*

Next, reusing notation, let us consider degeneracy maps $\epsilon_d\colon X_1(Nn) \to X_1(N)$ for $d \geq 1$ dividing n. On $\mathbb{C}$-points, which is all we require here, ϵ_d is induced by multiplication-by-d on $\mathbb{H}^*$. The degeneracy maps induce degeneracy maps $\epsilon_d\colon M_k(N) \to M_k(Nn)$ on spaces of modular forms given by $\epsilon_d(f)(z) = f(dz)$. These clearly preserve the subspaces of cusp forms.

DEFINITION 3.3.20. The subspace of oldforms $M_k(N)^{\mathrm{old}}$ in $M_k(N)$ is the span of all images $\epsilon_1(M_k(Np^{-1}))$ and $\epsilon_p(M_k(Np^{-1}))$ for primes p dividing N.

DEFINITION 3.3.21. The new subspace $S_k(N)^{\mathrm{new}}$ of $S_k(N)$ is the orthogonal complement of $S_k(N)^{\mathrm{old}} = M_k(N)^{\mathrm{old}} \cap S_k(N)$ under the Petersson inner product.

DEFINITION 3.3.22. An eigenform in $S_k(N)$ is said to be a newform if lies in $S_k(N)^{\mathrm{new}}$ and is normalized, i.e., has q-coefficient 1.

EXERCISE 3.3.23. For an eigenform to be a newform, it suffices that it have primitive nebentypus.

THEOREM 3.3.24. *The space $S_k(N)^{\mathrm{new}}$ has a basis consisting of eigenforms.*

We can also consider forms with coefficients in a commutative ring A.

DEFINITION 3.3.25. We define $M_k(N, \mathbb{Z}) \subseteq M_k(N)$ to be the subset of modular forms with q-expansions having coefficients in $\mathbb{Z}$, and we let $S_k(N, \mathbb{Z})$ be its subgroup of cusp forms.

EXERCISE 3.3.26. The ranks of the groups of modular forms with $\mathbb{Z}$-coefficients agree with the dimensions of the vector spaces of modular forms over $\mathbb{C}$:

$$\mathrm{rank}_{\mathbb{Z}}\, M_k(N, \mathbb{Z}) = \dim_{\mathbb{C}} M_k(N) \quad \text{and} \quad \mathrm{rank}_{\mathbb{Z}}\, S_k(N, \mathbb{Z}) = \dim_{\mathbb{C}} S_k(N).$$

DEFINITION 3.3.27. For a commutative ring A (with 1), we set

$$M_k(N, A) = M_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A \quad \text{and} \quad S_k(N, A) = S_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A.$$

DEFINITION 3.3.28. The full modular Hecke algebra $\mathfrak{H}_k(N, A)$ of weight k and level N is the A-subalgebra of the A-linear endomorphisms of $M_k(N, A)$ generated by the diamond operators $\langle j \rangle$ with $j \in (\mathbb{Z}/N\mathbb{Z})^\times$ and the Hecke operators T_n for $n \geq 1$. The cuspidal Hecke algebra $\mathfrak{h}_k(N, A)$ of weight k and level N is the image of $\mathfrak{H}_k(N, A)$ in $\mathrm{End}_A(S_k(N, A))$ upon restriction. If $A = \mathbb{Z}$, we omit the ring from the notation.

REMARK 3.3.29. We can also define full and cuspidal adjoint Hecke algebras $\mathfrak{H}_k^*(N, A)$ and $\mathfrak{h}_k^*(N, A)$. These are isomorphic as A-algebras to $\mathfrak{H}_k(N, A)$ and $\mathfrak{h}_k(N, A)$, respectively, via the map that takes a Hecke or diamond operator to its adjoint, which is well-defined for instance by the description of this map as conjugation by the Atkin-Lehner involution w_N. We write T^* for the adjoint of an operator T in $\mathfrak{H}_k(N, A)$ or $\mathfrak{h}_k(N, A)$

We shall also need a slight variation on $M_k(N, A)$.

DEFINITION 3.3.30. For a domain A with quotient field Q, we set

$$M_k'(N, A) = \{f \in M_k(N, Q) \mid a_n(f) \in A \text{ for all } n \geq 1\}.$$

EXAMPLE 3.3.31. For $k \geq 4$, the Eisenstein series E_k has integral coefficients aside from its constant term $-\frac{B_k}{2k}$, so lies in $M_k'(1, \mathbb{Z})$.

The Hecke algebra $\mathfrak{H}_k(N, A)$ acts on $M_k(N, Q)$ and preserves $M_k'(N, A)$. The following can be proven directly for $A = \mathbb{C}$, in some cases by construction of explicit bases of the spaces of modular forms, and then in general using the results of the next section.

THEOREM 3.3.32 (HIDA). *For any domain A, for each level N and weight $k \geq 2$, there is a perfect pairing*

$$M_k'(N, A) \times \mathfrak{H}_k(N, A) \to A, \qquad (f, T_n) \mapsto a_1(T_n f),$$

where $a_1(F)$ denotes the q-coefficient of a modular form F, and it induces a perfect pairing

$$S_k(N, A) \times \mathfrak{h}_k(N, A) \to A.$$

We may conclude from this the following.

PROPOSITION 3.3.33. *Let $f \in M_k(N, \chi)$ be an eigenform. The ring generated by the coefficients of f and the values of χ is an order in a number field K_f.*

PROOF. Note that $M_k(N, \mathbb{Z})$ is a finitely generated abelian group upon which $\mathfrak{H}_k(N)$ acts. The characteristic polynomial of any T_n acting on $M_k(N)$ is therefore monic with integral coefficients. In particular, if $f \in M_k(N, \chi)$ is an eigenform, then $a_n(f)$ is a root of this polynomial, so is an algebraic integer. The ring of coefficients is a quotient of $\mathfrak{H}_k(N, \mathbb{Z})$ via the homomorphism that sends T_n to $a_n(f)$ and $\langle j \rangle$ to $\chi(j)$. Being therefore an integral extension of $\mathbb{Z}$ of finite rank, we have the result. □

REMARK 3.3.34. The field K_f of an eigenform f as in Proposition 3.3.33 is generated over $\mathbb{Q}$ by its Fourier coefficients, as can be seen from (3.3.2).

3.4. Homology and cohomology

Until noted otherwise, we again treat $X_1(N)$ as a compact Riemann surface in this section. In fact, at first, we shall only need to think of its structure as a real manifold. That is, we first discuss its usual (i.e., singular, or "Betti") homology and cohomology.

First, note that we have an exact sequence of relative homology groups

$$0 \to H_1(X_1(N), \mathbb{Z}) \to H_1(X_1(N), C_1(N), \mathbb{Z}) \xrightarrow{\partial} \mathbb{Z}[C_1(N)] \to \mathbb{Z} \to 0, \tag{3.4.1}$$

where the latter two groups are 0th cohomology groups of $C_1(N)$ and $X_1(N)$, respectively.

REMARK 3.4.1. Pushforward by the action of $\delta_j \in \Gamma_0(N)$ on $X_1(N)$ gives rise to a diamond operator $\langle j \rangle = (\delta_j)_*$ on homology and cohomology groups. Similarly, we may define T_n via as a correspondence via $(\epsilon_n)_* \epsilon_1^*$, via pullback and pushforward by degeneracy maps, and we may define T_n^* as $(\epsilon_1)_* \epsilon_n^*$, as before. The sequence (3.4.1) is equivariant for these actions.

The definitions of homology and cohomology using dual complexes of singular chains and cochains give rise to perfect pairings

$$\begin{array}{ccc}
H_1(X_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & \xrightarrow{\cup} & \mathbb{Z} \\
\downarrow & & \| \\
H_1(X_1(N), C_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & & \| \\
\uparrow\uparrow & & \| \\
H^1(X_1(N), C_1(N), \mathbb{Z}) \times H_c^1(Y_1(N), \mathbb{Z}) & \xrightarrow{\cup} & \mathbb{Z}
\end{array}$$

that are equivariant for the actions of Hecke operators.

We also have Poincaré duality, given by perfect cup product pairings

$$\begin{array}{ccccc}
H^1(X_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & \xrightarrow{\cup} & H^2(X_1(N), \mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z} \\
\downarrow & & & & \| \\
H^1(Y_1(N), \mathbb{Z}) \times H^1(X_1(N), \mathbb{Z}) & & \downarrow \wr & & \| \\
\uparrow\uparrow & & & & \| \\
H^1(Y_1(N), \mathbb{Z}) \times H_c^1(Y_1(N), \mathbb{Z}) & \xrightarrow{\cup} & H_c^2(Y_1(N), \mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z}.
\end{array}$$

where $H_c^i(Y_1(N), \mathbb{Z})$ denotes the ith compactly supported cohomology group. Hecke operators are adjoint to the adjoint operators under the cup product.

REMARK 3.4.2. More precisely, the definitions of homology and cohomology in terms of singular (co)chains, as well as Poincaré duality, give a Pontraygin duality between (co)homology with $\mathbb{Z}$-coefficients and compactly supported cohomology with $\mathbb{Q}/\mathbb{Z}$-coefficients (or vice versa for the coefficients). With $\mathbb{Z}$-coefficients on both sides, this can be reinterpreted as convergent spectral sequences

$$\mathrm{Ext}_{\mathbb{Z}}^i(H_j(X_1(N), C_1(N), \mathbb{Z}), \mathbb{Z}) \Rightarrow H_c^{i+j}(Y_1(N), \mathbb{Z})$$
$$\mathrm{Ext}_{\mathbb{Z}}^i(H^{2-j}(Y_1(N), \mathbb{Z}), \mathbb{Z}) \Rightarrow H_c^{i+j}(Y_1(N), \mathbb{Z})$$

and similarly with the groups reversed, or with taking instead the (co)homology of $X_1(N)$. Since all of our cohomology groups in question are free over $\mathbb{Z}$, the spectral sequences degenerate to give the above dualities.

Summarizing, we have a commutative diagram

$$\begin{array}{ccc} H_1(X_1(N),\mathbb{Z}) & \hookrightarrow & H_1(X_1(N),C_1(N),\mathbb{Z}) \\ \varphi\downarrow\wr & & \varphi\downarrow\wr \\ H^1(X_1(N),\mathbb{Z}) & \hookrightarrow & H^1(Y_1(N),\mathbb{Z}), \end{array}$$

where $\varphi(Tx) = T^*\varphi(x)$ for a Hecke (or diamond) operator T and its adjoint T^*.

REMARK 3.4.3. There is an involution τ on the homology and cohomology groups of modular curves induced by complex conjugation, which we can view as descended from the action $z \mapsto -\bar{z}$ on $\mathbb{H}^*$. Therefore, we can speak of plus and minus parts. The isomorphisms of Poincaré duality yield isomorphisms

$$H_1(X_1(N),C_1(N),\mathbb{Z})^{\pm} \xrightarrow{\sim} H^1(Y_1(N),\mathbb{Z})^{\mp}. \tag{3.4.2}$$

Next, let us compare with group (co)homology. Since $N \geq 4$, the group $\Gamma_1(N)$ contains no nontrivial elements of finite order, and it acts freely on the complexes of singular cochains for $\mathbb{H}$ with trivial coefficients (e.g., in $\mathbb{Z}$). It follows that we have a spectral sequence

$$H^i(\Gamma_1(N), H^j(\mathbb{H},\mathbb{Z})) \Rightarrow H^{i+j}(Y_1(N),\mathbb{Z}).$$

Since $\mathbb{H}$ is contractible, this quickly yields isomorphisms

$$H^i(\Gamma_1(N),\mathbb{Z}) \cong H^i(Y_1(N),\mathbb{Z}) \tag{3.4.3}$$

for all i, compatible with Hecke operators, which can be defined on the left by double cosets. The stabilizer $\Gamma_1(N)_x$ of a cusp x is the (infinite cyclic) intersection of a Borel subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with $\Gamma_1(N)$, and with the identification of (3.4.3), we have

$$H_1(X_1(N),\mathbb{Z}) \cong \ker\left(H_1(\Gamma_1(N),\mathbb{Z}) \to \bigoplus_{x\in C_1(N)} H_1(\Gamma_1(N)_x,\mathbb{Z}) \right).$$

DEFINITION 3.4.4. For $\alpha,\beta \in \mathbb{Q}\cup\{\infty\}$, the modular symbol $\{\alpha\to\beta\}_N$ is the class in the relative homology group $H_1(X_1(N),C_1(N),\mathbb{Z})$ of the geodesic from α to β in $\mathbb{H}^*$ (with respect to the hyperbolic metric $y^{-2}(dx^2+dy^2)$).

The boundary map ∂ of (3.4.1) satisfies

$$\partial(\{\alpha\to\beta\}) = \{\beta\} - \{\alpha\},$$

where for $x \in \mathbb{Q}\cup\{\infty\}$, the symbol $\{x\}$ denotes the class of x in the divisor group $\mathbb{Z}[C_1(N)]$. Since $\mathbb{H}$ is contractible, the modular symbols are independent of the chosen path with interior in $\mathbb{H}$, and they generate relative homology.

Cohomology with $\mathbb{C}$-coefficients has a decomposition into Hecke submodules via Hodge theory:

$$H^1(X_1(N),\mathbb{C}) \cong H^0(X_1(N),\Omega^1_{X_1(N)}) \oplus H^1(X_1(N),\mathcal{O}_{X_1(N)}). \tag{3.4.4}$$

Here, $\mathcal{O}_{X_1(N)}$ is the structure sheaf and $\Omega^1_{X_1(N)}$ is the sheaf of holomorphic differential 1-forms on $X_1(N)$. The summands are interchanged by complex conjugation, and they are isotropic under the cup product pairing of Poincaré duality. The Hecke module $H^0(X_1(N),\Omega^1_{X_1(N)})$ can be identified with $S_2(N)$ by viewing a weight 2 modular form f as the holomorphic differential on the curve induced by $2\pi i f(z)dz$. Hence $H^1(X_1(N),\mathcal{O}_{X_1(N)})$ can be identified with the antiholomorphic forms $\overline{S_1(N)}$. The group $H^1(Y_1(N),\mathbb{C})$ has a compatible decomposition to that of (3.4.4), where the second term is the same but the first is replaced by a sheaf of differentials with log poles at the cusps, and it is now isomorphic to $M_2(N)$. Consequently, we have the following.

Proposition 3.4.5. *The Hecke algebras generated by the diamond and Hecke operators inside the rings of endomorphisms of $H_1(X_1(N),\mathbb{Z})$ and $H_1(X_1(N),C_1(N),\mathbb{Z})$ are canonically isomorphic to the Hecke algebras $\mathfrak{h}_2(N)$ and $\mathfrak{H}_2(N)$.*

The decomposition (3.4.4) arises from the comparison of two cohomology theories: the Betti cohomology we have been considering, and de Rham cohomology. Rational structures on these isomorphic cohomology groups are compared by a period matrix with transcendental entries (see below).

The Betti and p-adic étale cohomology groups of modular curves with $\mathbb{Z}_p$-coefficients are also isomorphic, dependent upon a choice of embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Since $X_1(N)$ is smooth and proper over $\mathbb{Z}[\frac{1}{N}]$, the absolute Galois group of $\mathbb{Q}$ acts on its étale cohomology with $\mathbb{Z}_p$-coefficients (as well as the étale cohomology of $Y_1(N)$) via an action that is unramified outside of the primes dividing Np. It is the Galois action on étale cohomology we shall use in the next section. Poincaré duality provides an isomorphism between the Tate module of the Jacobian of $X_1(N)$ and $H^1_{\text{ét}}(X_1(N),\mathbb{Z}_p(1))$ that is both Galois equivariant and equivariant for the usual and adjoint Hecke actions on the respective sides.

We turn momentarily to modular symbols of higher weight. We may identify $\mathrm{Sym}^{k-2}\mathbb{Z}^2$ as the homogeneous, degree $k-2$ polynomials in two variables X and Y such that the (right) action of $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ takes $P(X,Y)$ to $P(aX+bY, cX+dY)$. The following definition is somewhat convoluted due to potential issues of torsion.

Definition 3.4.6. For $\alpha,\beta \in \mathbb{Q}\cup\{\infty\}$ and $P \in \mathrm{Sym}^{k-2}\mathbb{Z}^2$, the weight k and level N modular symbol $P\{\alpha\to\beta\}$ is defined to be the class of $P\otimes\{\alpha\to\beta\}$ in

$$\mathrm{Sym}^{k-2}\mathbb{Z}^2 \otimes_{\mathbb{Z}[\Gamma_1(N)]} H_1(\mathbb{H}^*,\mathbb{P}^1(\mathbb{Q}),\mathbb{Z}).$$

The modular symbols $X^{i-1}Y^{k-i-1}\{\alpha\to\beta\}$ with $\alpha,\beta\in\mathbb{P}^1(\mathbb{Q})$ and $1\le i\le k-1$ span a lattice $\mathcal{M}_k(N,\mathbb{Z})$ called the group of weight k, level N modular symbols. The intersection of this lattice with the kernel of the boundary to $H_0(\mathbb{P}^1(\mathbb{Q}),\mathbb{Z})\otimes_{\mathbb{Z}[\Gamma_1(N)]}\mathrm{Sym}^{k-2}\mathbb{Z}^2$ is the subgroup $\mathcal{S}_k(N,\mathbb{Z})$ of cuspidal modular symbols. For any commutative ring R, we set $\mathcal{M}_k(N,R)=\mathcal{M}_k(N,\mathbb{Z})\otimes_{\mathbb{Z}}R$ and similarly for $\mathcal{S}_k(N,R)$.

Note that $\mathcal{M}_2(N,\mathbb{Z}) \cong H_1(X_1(N), C_1(N), \mathbb{Z})$ and $\mathcal{S}_2(N,\mathbb{Z}) \cong H_1(X_1(N),\mathbb{Z})$.

EXERCISE 3.4.7. Formulate Definition 3.4.6 in arbitrary weight $k \geq 2$ in terms of group cohomology, or relative homology.

EXERCISE 3.4.8. Formulate and prove the extension of Proposition 3.4.5 to arbitrary weight $k \geq 2$.

REMARK 3.4.9. The action of a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ with nonzero, positive determinant on a formal symbol $P\{\alpha \to \beta\}$ is given by

$$P\{\alpha \to \beta\} = (P\gamma^{-1})\{\gamma\alpha \to \gamma\beta\}.$$

This allows us to define Hecke operators on $\mathcal{M}_k(\mathbb{Z})$ as double coset operators.

A theorem of Eichler and Shimura [**Shi1**], as extended by Shokurov [**Sho1**] (see [**Mer**]), yields the following.

THEOREM 3.4.10. *We have an integration pairing of $\mathbb{C}$-vector spaces*

$$\langle\ ,\ \rangle \colon \mathcal{M}_k(N,\mathbb{C}) \times (S_k(N) \oplus \overline{S_k(N)}) \to \mathbb{C}$$

$$\langle P(X,Y)\{\alpha \to \beta\}, (f,g)\rangle = \int_\alpha^\beta f(z)P(z,1)dz + \int_\alpha^\beta f(z)P(\bar{z},1)d\bar{z},$$

where $P \in \mathbb{C}[X,Y]$ is homogeneous of degree $k-2$. This integration pairing is perfect upon restricting the first variable to elements of $\mathcal{S}_k(N,\mathbb{C})$, and the usual and adjoint operators are adjoint under this pairing.

EXERCISE 3.4.11. Compare this with Poincaré duality, for instance in weight 2 when the left-hand side is restricted to $H_1(X_1(N),\mathbb{C})$.

REMARK 3.4.12. The integration pairing of Theorem 3.4.10 provides the special values

$$L(f,j) = \frac{(-2\pi i)^j}{(j-1)!} r_j(f), \qquad r_j(f) = \langle X^{j-1}Y^{k-j-1}\{0 \to \infty\}, f\rangle.$$

of $f \in S_k(N)$ for $1 \leq j \leq k-1$.

EXERCISE 3.4.13. For a normalized eigenform $f \in S_k(N)$, there exist periods $\Omega_f^\pm$ such that the values of the pairing on classes in $\mathcal{M}_k(N,\mathbb{Q})^\pm$ all lie in $K_f\Omega_f^\pm$, where K_f is the field of coefficients of f.

EXERCISE 3.4.14. Show how to obtain special values of an appropriately defined L-function $L(f,\chi,s)$ for $f \in S_k(N)$ and a Dirichlet character χ of modulus dividing N via the integration pairing of Theorem 3.4.10.

EXAMPLE 3.4.15. Of particular interest to us are the L-values of weight k eigenforms at odd integers in the interior of the critical strip $[1, k-1]$. In weights k among 12, 16, 18, 20, 22, and

26, the spaces $S_k(1)$ are one-dimensional, and hence the unique normalized cusp form f_k in this space is already an eigenform, which is congruent to the Eisenstein series

$$E_k = -\frac{B_k}{4k} + \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n$$

at any prime p dividing the numerator of $\frac{B_k}{4k}$. Let us write out the table of these values $\frac{r_j(f_k)}{r_1(f_k)}$ for odd $3 \leq j \leq \frac{k-1}{2}$, for k up to 22. (It is reproduced from [**Man2**], after some rearranging, and the subscripts were a bit hard to read at points, so they could contain inaccuracies.)

k	$(\frac{r_3(f_k)}{r_1(f_k)}, \frac{r_5(f_k)}{r_1(f_k)}, \frac{r_7(f_k)}{r_1(f_k)}, \ldots)$
12	$\frac{691}{2^3 3^4 5 \cdot 7}(-2 \cdot 7, 3^2)$
16	$\frac{3617}{2^3 3^3 5 \cdot 7 \cdot 11 \cdot 13}(-2 \cdot 3 \cdot 11, 3 \cdot 7, -11)$
18	$\frac{43867}{2^6 3^3 5^4 7 \cdot 11 \cdot 13}(-2^2 \cdot 7 \cdot 11 \cdot 13, 3 \cdot 5^2 \cdot 11, -3^2 \cdot 13)$
20	$\frac{283 \cdot 617}{2^3 3^5 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17}(-2 \cdot 3 \cdot 11 \cdot 13, 143, -3 \cdot 11, 2 \cdot 13)$
22	$\frac{131 \cdot 593}{2^5 3^3 5^4 7 \cdot 13 \cdot 17 \cdot 19}(-2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 17, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13, -2 \cdot 13 \cdot 17, 5 \cdot 17)$

The primes p such that $p \mid B_k$ appear in the numerators on the left of the right-hand columns. For each, we have a mod p congruence between $r_j(f_k)$ and the $r_j(E_k) = \frac{(j-1)!}{(-2\pi i)^j} L(E_k, j)$ for odd j with $3 \leq j \leq k-3$, the latter being zero by Example 3.3.7.

We end this section with the Manin-Drinfeld theorem.

THEOREM 3.4.16. *There exists a canonical, Hecke-equivariant splitting of the injection* $\mathcal{S}_k(N, \mathbb{Q}) \hookrightarrow \mathcal{M}_k(N, \mathbb{Q})$.

This was proven in weight 2 for $\Gamma_0(N)$ by use of the integration pairing of Theorem 3.4.10 and the operators $T_p - 1 - p$ for primes p not dividing N in a paper of Drinfeld [**Dri**], and the weight 2 analogue for $\Gamma_1(N)$ is proven by Manin in [**Man1**, Theorem 3.3]. In the general case, note that as the integration pairing is nondegenerate upon restriction to $\mathcal{S}_k(N, \mathbb{C})$, it immediately gives a $\mathbb{C}$-linear splitting of $\mathcal{S}_k(N, \mathbb{C}) \to \mathcal{M}_k(N, \mathbb{C})$. In [**Sho2**], Shokurov produces a basis in $\mathcal{M}_k(N, \mathbb{Z})$ of the left kernel of the pairing, which implies the theorem.

REMARK 3.4.17. The Manin-Drinfeld theorem is also a consequence of the Ramanujan-Petersson conjecture that $|a_p(f)| \leq 2p^{(k-1)/2}$ for all $p \nmid N$ (which Deligne showed follows from the Weil conjectures that he later proved). This says in particular that the Hecke eigenvalues of Eisenstein series and cuspidal eigenforms for primes p not dividing N are distinct.

3.5. Galois representations

Let $f \in S_k(N, \chi)$ be a newform, and fix a prime p. By a shift in notation, let $\mathcal{O}_f$ denote the valuation ring of the field K_f its coefficients generate over $\mathbb{Q}_p$, fixing an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$. Via the duality between cusp forms and the Hecke algebra, the normalized eigenform f gives rise to a ring homomorphism

$$\phi_f \colon \mathfrak{h}_k(N, \mathbb{Z}_p) \to \mathcal{O}_f$$

with $\phi_f(T_n) = a_n(f)$ and $\phi_f(\langle a \rangle) = \chi(a)$. Let $I_f = \ker \phi_f$.

REMARK 3.5.1. To give an idea of what the kernel I_f is, note that we may extend ϕ_f to a homomorphism $\mathcal{O}_f$-linearly to a map $\mathfrak{h}_k(N, \mathcal{O}_f) \to \mathcal{O}_f$, and the kernel of this map is generated by $T_n - a_n(f)$ for $n \geq 1$ and $\langle j \rangle - \chi(j)$ for all $j \in (\mathbb{Z}/N\mathbb{Z})^\times$.

The étale cohomology group

$$H^1(N) = H^1_{\text{ét}}(X_1(N)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)).$$

of the modular curve $X_1(N)$ over $\overline{\mathbb{Q}}$ is a Galois module that is unramified outside the primes dividing Np and which has a commuting Hecke action of adjoint Hecke operators.

REMARK 3.5.2. From now on, we use the convention that $T \in \mathfrak{H}_k(N, \mathbb{Z}_p)$ acts on cohomology through its adjoint T^*, so as to avoid speaking of adjoint operators below.

Suppose that $k = 2$. In this case, we set

$$V_f = H^1(N)/I_f H^1(N) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

which is a 2-dimensional K_f-vector space. This is isomorphic to the Galois representation attached to f by Shimura [**Shi1**].

DEFINITION 3.5.3. The p-adic Galois representation $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{Aut}_{K_f}(V_f)$ attached to f is the two-dimensional representation over K_f determined by the action of $G_{\mathbb{Q}}$ on V_f.

One typically fixes a choice of basis so that we can view ρ_f as a homomorphism $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f)$. A different choice yields a conjugate Galois representation.

THEOREM 3.5.4 (SHIMURA). *For any Frobenius φ_ℓ at a prime $\ell \nmid Np$, we have*

$$\det(\rho_f(\varphi_\ell)) = \ell\chi(\ell) \quad \textit{and} \quad \mathrm{Tr}(\rho_f(\varphi_\ell)) = a_\ell(f).$$

EXERCISE 3.5.5. The Galois representation ρ_f is characterized up to conjugacy by its trace and determinant on Frobenius elements φ_ℓ at primes $\ell \nmid Np$.

In [**Del**], Deligne constructed Galois representations ρ_f attached to newforms $f \in S_k(N, \chi)$ of arbitrary weight $k \geq 2$. For this, he takes the tensor product with $\mathbb{Q}_p$ of the quotient of an étale cohomology group by I_f, for instance of

$$H^1_{\text{ét}}(Y_1(N)_{/\overline{\mathbb{Q}}}, \mathrm{Sym}^{k-2}(\mathrm{Ta}_p\mathcal{E})(1)).$$

Here, $\mathrm{Ta}_p\mathcal{E}$ is the p-adic Tate module of the universal elliptic curve $\mathcal{E}_1(N)$, viewed as a sheaf over $X_1(N)_{/\overline{\mathbb{Q}}}$ (i.e., we take the first right-derived functor of the pushforward of $\mathbb{Z}_p(1)$). The trace of ρ_f on a Frobenius is again the corresponding Fourier coefficient, while $\det \rho_f = \chi_p^{k-1}\chi$.

REMARK 3.5.6. By the Manin-Drinfeld theorem, one obtains the same Galois representation from a modular form using cohomology of the open or closed curve, but not in general the same lattice (e.g., when f is p-adically congruent to an Eisenstein series).

CHAPTER 4

Hida theory and the main conjecture

4.1. Ordinary forms

Suppose in this section that N is divisible by p. For any prime ℓ dividing the level, the Hecke operator T_ℓ is frequently denoted U_ℓ, and we will also use this notation.

DEFINITION 4.1.1. A normalized eigenform f is said to be ordinary if $a_p(f) \in \mathcal{O}_f^\times$, i.e., is a p-adic unit.

Let $f \in S_k(N, \chi)$ be an ordinary newform. The property of being ordinary has important implications for the restriction of the Galois representation ρ_f to $G_{\mathbb{Q}_p}$, which is to say that it too is what is known as "ordinary", but as a Galois representation. In particular, there exists a basis of V_f with respect to which $\rho_f|_{G_{\mathbb{Q}_p}}$ is upper-triangular. On σ in the inertia subgroup I_p of $G_{\mathbb{Q}_p}$, it has the form

$$\rho_f(\sigma) = \begin{pmatrix} \chi_p\chi(\sigma) & * \\ 0 & 1 \end{pmatrix}.$$

Since we already know the determinant, another way of saying this is that V_f has a 1-dimensional inertia-fixed $G_{\mathbb{Q}_p}$-quotient.

Hida defined an idempotent of the Hecke algebra that projects to the "ordinary parts" of Hecke modules, which are the maximal submodules upon which U_p acts invertibly [**Hid1**].

PROPOSITION 4.1.2 (HIDA). *The element*

$$e^{\mathrm{ord}} = \lim_{n\to\infty} U_p^{n!}$$

is a well-defined idempotent of $\mathfrak{H}(N, \mathbb{Z}_p)$.

SKETCH OF PROOF. The $\mathbb{Z}_p$-algebra $\mathfrak{H}(N, \mathbb{Z}_p)$ is $\mathbb{Z}_p$-torsion free of finite rank, and as such, it is a product of complete noetherian local rings, each of which has semisimplification (i.e., quotient by nilradical) with quotient field a finite extension of $\mathbb{Q}_p$. Let u_p denote the projection of U_p to such a factor R. If u_p lies in the maximal ideal $\mathfrak{m}$ of R, then the limit of the $u_p^{n!}$ must approach 0. If, on the other hand, $u_p \in R^\times$, then $n!$ is divisible by the order of the residue field $R/\mathfrak{m}$ for sufficiently large n. Then $u_p^{n!} \equiv 1 \bmod \mathfrak{m}$, and as we further increase n, the quantity $n!$ becomes divisible by increasingly higher powers of p, which makes $u_p^{n!}$ congruent to 1 modulo increasing powers of $\mathfrak{m}$, forcing the limit of the $u_p^{n!}$ to be 1. Consequently, e^{ord} is an idempotent in $\mathfrak{H}(N, \mathbb{Q}_p)$. □

REMARK 4.1.3. The ring $e^{\mathrm{ord}}\mathfrak{H}(N, \mathbb{Z}_p)$ is a finite product of finite reduced $\mathbb{Z}_p$-algebras that are domains. The image of U_p in this ordinary Hecke algebra, which we also denote by U_p, is invertible.

DEFINITION 4.1.4. For an $\mathfrak{H}(N,\mathbb{Z}_p)$-module A, we define its ordinary part by $A^{\mathrm{ord}} = e^{\mathrm{ord}}A$.

REMARK 4.1.5. The perfect pairings between modular forms and Hecke algebras restrict to perfect pairings between their ordinary parts.

To indicate something of how we obtain the upper-triangular form of $\rho_f|_{G_{\mathbb{Q}_p}}$, we mention the following result that implies it. This result is a consequence of work of Mazur-Wiles, Tilouine, and Ohta (cf. [**Oht1**]) and is particularly suited for Hida theory.

THEOREM 4.1.6. *There is an exact sequence of $\mathfrak{h}_2(N,\mathbb{Z}_p)^{\mathrm{ord}}[G_{\mathbb{Q}_p}]$-modules*

$$0 \to H^1(N)^{\mathrm{ord}}_{\mathrm{sub}} \to H^1(N)^{\mathrm{ord}} \to H^1(N)^{\mathrm{ord}}_{\mathrm{quo}} \to 0,$$

that are free over $\mathbb{Z}_p$ and of rank one over $\mathfrak{h}_2(N,\mathbb{Z}_p)^{\mathrm{ord}}$, with $H^1(N)^{\mathrm{ord}}_{\mathrm{quo}}$ the maximal $\mathbb{Z}_p$-torsion-free quotient of $H^1(N)^{\mathrm{ord}}$ on which I_p acts trivially.

The theorem is proven by construction of an appropriate quotient the Jacobian $J_1(N)$ of $X_1(N)$ (typically) with good reduction at p. The application of Hida's idempotent to the ordinary part of the p-divisible group of its Neron model is of multiplicative type, and the injective image of its Tate module in the ordinary part of the Tate module $\mathrm{Ta}_p J_1(N)$ of $J_1(N)$ is dual under a twisted Weil pairing on $e^{\mathrm{ord}}\mathrm{Ta}_p J_1(N)$ to the resulting cokernel (on which I_p then acts trivially). The sequence is then the $\mathbb{Z}_p$-dual of the resulting exact sequence.

4.2. Hida theory

The ordinary parts of Hecke algebras, spaces of modular forms, and cohomology groups of modular curves (all with $\mathbb{Z}_p$-coefficients) have remarkable regularity properties as we increase the power of p that occurs in the level. In this way and others we shall soon see, Hida theory and Iwasawa theory have more than just superficial similarities. Contrary to the previous section, we now take N to be an integer prime to an odd prime p.

Hida theory deals with the behavior of modules over the ordinary part of the Hecke algebra as we increase r, i.e., the p-power in the level. Let $\mathcal{O}$ be the valuation ring of a finite extension of $\mathbb{Q}_p$, and set $\Lambda = \mathcal{O}[\![T]\!]$. We again identify Λ with $\mathcal{O}[\![1+p\mathbb{Z}_p]\!]$ by identifying T with $\gamma - 1$, where γ is the group element of our fixed topological generator υ. Recall that $Q(\Lambda)$ denotes the quotient field of Λ. We have a map $\kappa\colon \mathbb{Z}_p^\times \to \Lambda$ that is the projection to $1+p\mathbb{Z}_p$ followed by the map induced by the latter identification.

DEFINITION 4.2.1. A Λ-adic modular form of weight k, tame level N is a power series

$$f = \sum_{n=0}^{\infty} a_n(f) q^n \in Q(\Lambda) + q\Lambda[\![q]\!]$$

such that its specializations $f(\epsilon(\upsilon)\upsilon^{k-2}-1)$ at $T = \epsilon(\upsilon)\upsilon^{k-2}-1$ for a character $\epsilon\colon \Gamma \to \overline{\mathbb{Q}}_p^\times$ with kernel $\Gamma^{p^{r-1}}$ are modular forms of weight k, level Np^r, and character ϵ on the 1-units in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ for almost all such ϵ.

We may think of a Λ-adic modular form as a family of modular forms of varying (p-adic) weight.

DEFINITION 4.2.2. A Λ-adic modular form is a cusp form if all but finitely many of its specializations are cusp forms.

DEFINITION 4.2.3. We let $\mathfrak{M}'(N,\Lambda)$ and $\mathfrak{S}(N,\Lambda)$ denote the spaces of Λ-adic modular forms and Λ-adic cusp forms of weight 2 and tame level N, respectively. Let

$$\mathfrak{M}(N,\Lambda) = \mathfrak{M}'(N,\Lambda) \cap \Lambda[\![q]\!].$$

EXAMPLE 4.2.4. Let χ be an even $\mathcal{O}$-valued Dirichlet character of modulus Np. The Λ-adic Eisenstein series $\mathcal{E}_\chi \in \mathfrak{M}'(N,\Lambda)$ is

$$\mathcal{E}_\chi = \frac{1}{2}h_{\chi\omega^2} + \sum_{n=1}^{\infty}\sum_{\substack{d|n \\ p\nmid d}} \chi(d)(1+T)^{\log_\upsilon(d)}q^n,$$

where $h_{\chi\omega^2} \in Q(\Lambda)$ satisfies $h_{\chi\omega^2}(\upsilon^s - 1) = L_p(\chi\omega^2, -1-s)$ for $s \in \mathbb{Z}_p$ (with $h_{\chi\omega^2} \in \Lambda$ for $\chi\omega^2 \neq 1$), and where $\log_\upsilon(d)$ is taken to be the unique p-adic integer such that $\kappa(d) = \upsilon^{\log_\upsilon(d)}$. For all $k \geq 2$, we have $\mathcal{E}_\chi(\upsilon^{k-2} - 1) = E_{k,\chi\omega^{2-k}}$.

Set

$$\mathbb{Z}_{p,N} = \varprojlim_r \mathbb{Z}/Np^r\mathbb{Z}.$$

The nth Hecke operator for a prime n is then defined by the usual formula for its action on Fourier coefficients (see (3.3.2) for n prime). Each $j \in \mathbb{Z}_{p,N}^\times$ also yields a diamond operator $\langle j\rangle$ on $\mathfrak{M}(N,\Lambda)$, preserving the cusp forms, characterized by the property that it is compatible with the diamond operators on specializations. In particular, $\langle\upsilon\rangle$ acts as multiplication by $T+1$.

As before, we may define Hida's idempotent e^{ord} that acts on $\mathfrak{S}(N,\Lambda)$ and $\mathfrak{M}(N,\Lambda)$ and therefore the ordinary parts of the spaces of Λ-adic forms. Hida proved that these ordinary parts are free over Λ in [**Hid2**, Theorem 3.1] with a slightly different definition: the next result is found in Wiles [**Wil1**, Theorem 1.2.2]).

THEOREM 4.2.5 (HIDA, WILES). *The spaces $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ of ordinary Λ-adic forms are free of finite rank over Λ.*

We will concern ourselves here only with the well-behaved ordinary parts of Hecke algebras of Λ-adic forms.

DEFINITION 4.2.6. We let $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ denote the full modular and cuspidal ordinary Λ-adic Hecke algebras, which are the Λ-algebras generated by the Hecke and diamond operators inside the Λ-linear endomorphism rings of $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$, respectively.

Hida proved the following duality between ordinary modular forms and Hecke algebras [**Hid2**, Theorem 2.2].

THEOREM 4.2.7 (HIDA). *There is a perfect pairing of free, finite rank Λ-modules*

$$\mathfrak{M}'(N,\Lambda)^{\mathrm{ord}} \times \mathfrak{H}(N,\Lambda)^{\mathrm{ord}} \to \Lambda, \qquad (f, T_n) \mapsto a_1(T_n f),$$

that induces a perfect pairing

$$\mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \times \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \to \Lambda.$$

REMARK 4.2.8. It follows from Hida's duality theorem that $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ is a Cohen-Macaulay ring with dualizing module $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$, and $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ is Cohen-Macaulay with dualizing module $\mathfrak{M}'(N,\Lambda)^{\mathrm{ord}}$. If

$$\mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \cong \mathrm{Hom}_\Lambda(\mathfrak{h}(N,\Lambda)^{\mathrm{ord}},\Lambda)$$

is free over $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$, then $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ has the stronger property of being a Gorenstein ring. On the other hand, Wake showed that $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$ are not always Gorenstein [**Wak**]. However, they become Gorenstein upon tensor product with $Q(\Lambda)$, and in particular $\mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathfrak{M}(N,\Lambda)^{\mathrm{ord}}$ have rank one over their Hecke algebras.

For $r \geq 1$, let

$$\omega_{k,r} = (1+T)^{p^{r-1}} - \upsilon^{p^{r-1}(k-2)}.$$

The ordinary parts of the spaces of Λ-adic modular and cusp forms have a remarkable regularity, a sort of "perfect control" as the p-power in the level increases, whereby we can recover the spaces of ordinary forms of weight k and level Np^r simply by taking the quotient by $\omega_{k,r}$ [**Hid2**, Corollary 3.2].

THEOREM 4.2.9 (HIDA). *For all $r \geq 1$, we have*

$$\mathfrak{M}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong M_k(Np^r,\mathcal{O})^{\mathrm{ord}} \quad \text{and} \quad \mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong S_k(Np^r,\mathcal{O})^{\mathrm{ord}}$$

via isomorphisms that are equivariant with respect to the Hecke actions on both sides.

As a corollary, we have that ordinary Λ-adic forms and Hecke algebras are independent of the weight used, which explains our restriction to weight 2.

COROLLARY 4.2.10. *The spaces of ordinary Λ-adic modular forms of each weight $k \geq 2$ are all isomorphic via maps equivariant with respect to the corresponding ordinary Λ-adic Hecke algebras.*

REMARK 4.2.11. Note that under the identification of Λ with $\mathcal{O}[\![\Gamma]\!]$ for $\Gamma = 1 + p\mathbb{Z}_p$, the quotient of a Λ-module M by $\omega_{2,r}$ is equal to the $\Gamma^{p^{r-1}}$-coinvariant group of M, which is a $\mathcal{O}[\Gamma_r]$-module for $\Gamma_r = \Gamma/\Gamma^{p^{r-1}}$. One might compare this with the good control of p-parts of class groups described in our sketch of the proof of Theorem 2.3.12.

As a corollary of these two theorems, we obtain the following.

COROLLARY 4.2.12. *For all $r \geq 1$, we have*

$$\mathfrak{H}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathfrak{H}_k(Np^r,\mathcal{O})^{\mathrm{ord}} \quad \text{and} \quad \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathfrak{h}_k(Np^r,\mathcal{O})^{\mathrm{ord}}.$$

We have a similar regularity of ordinary parts of homology and cohomology groups of modular curves. That is, on homology, the canonical quotient maps on modular curves induce Hecke-equivariant surjections

$$H_1(X_1(Np^{r+1}),C_1(Np^{r+1}),\mathcal{O}) \to H_1(X_1(Np^r),C_1(Np^r),\mathcal{O})$$

which likewise induce (not necessarily surjective) maps on the first homology of the closed curves. On cohomology, the corresponding maps are the trace maps

$$H^1(Y_1(Np^{r+1}),\mathcal{O}) \to H^1(Y_1(Np^r),\mathcal{O})$$

that on the level of group cohomology correspond to corestriction. The latter maps are Hecke-equivariant for the dual action that we consider on cohomology. Again, we have perfect control of ordinary parts in the following sense [**Hid3**].

THEOREM 4.2.13 (HIDA). *The group* $\varprojlim_r H_1(X_1(Np^r),C_1(Np^r),\mathcal{O})^{\mathrm{ord}}$ *is free of finite rank over* Λ *and satisfies*

$$\left(\varprojlim_r H^1(X_1(Np^r),C_1(Np^r),\mathcal{O})^{\mathrm{ord}}\right)\otimes_\Lambda \Lambda/(\omega_{k,r}) \cong \mathcal{M}_k(\mathcal{O})^{\mathrm{ord}}$$

as $\mathfrak{H}(N,\Lambda)^{\mathrm{ord}}$*-modules. The analogous statement holds with usual homology and cuspidal modular symbols.*

Hida uses this theorem applied to étale cohomology in order to construct the Galois representations attached to ordinary Λ-adic cuspidal eigenforms. We can speak of such an eigenform as being a newform if its specializations, which are also eigenforms, are new at primes dividing N.

For a Λ-algebra $\mathcal{A}$, let us set $\mathfrak{S}(N,\mathcal{A}) = \mathfrak{S}(N,\Lambda)\otimes_\Lambda \mathcal{A}$. For a finitely generated profinite module $L = \varprojlim_\alpha L_\alpha$ over a complete commutative local ring A, we shall give $\mathrm{Aut}_A(L)$ the profinite topology as the inverse limit $\varprojlim_\alpha \mathrm{Aut}_A(L_\alpha)$ of finite groups. The following is the main theorem of [**Hid3**].

THEOREM 4.2.14 (HIDA). *Let* $\mathcal{F}\in\mathfrak{S}(N,\mathcal{A})^{\mathrm{ord}}$ *be a newform with character* χ *on* $(\mathbb{Z}/Np\mathbb{Z})^\times$*, where* $\mathcal{A}$ *is the integral closure of* Λ *in a finite extension* $\mathcal{Q}$ *of* $Q(\Lambda)$*. Then there exists a continuous Galois representation*

$$\rho_{\mathcal{F}}\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{A}}(\mathcal{L})$$

that is unramified outside of places dividing $Np\infty$*, where* $\mathcal{L}$ *is an* $\mathcal{A}$*-lattice in* $\mathcal{Q}^2$*, such that setting* $P_{k,\epsilon} = \epsilon(v)(1+T)^{k-2}-1$*, the resulting representation*

$$\rho_{\mathcal{F},k,\epsilon}\colon G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{A}/(P_{k,\epsilon})}(\mathcal{L}/P_{k,\epsilon}\mathcal{L})$$

is isomorphic to the Galois representation attached to $f_{k,\epsilon} = \mathcal{F}(\epsilon(v)v^{k-2}-1)$*, for every* $k\geq 2$ *and continuous homomorphism* $\epsilon\colon 1+p\mathbb{Z}_p \to \overline{\mathbb{Q}}_p^\times$ *with finite image. This representation* $\rho_{\mathcal{F}}$ *has the property that*

$$\det(\rho_{\mathcal{F}}(\varphi_\ell)) = \ell\chi(\ell)(1+T)^{\log_v(\ell)} \quad\text{and}\quad \mathrm{Tr}(\rho_{\mathcal{F}}(\varphi_\ell)) = a_\ell(\mathcal{F})$$

for all primes $\ell\nmid Np$*, where* φ_ℓ *is an arithmetic Frobenius at* ℓ*.*

In fact, the construction proceeds in much the same way as the construction of Galois representations attached to a single form. That is, setting $\mathcal{O}=\mathbb{Z}_p$, we may consider

$$\mathcal{T}(N)^{\mathrm{ord}} = \varprojlim_r H^1(Np^r)^{\mathrm{ord}} = \varprojlim_r H^1_{\text{ét}}(X_1(Np^r),\mathbb{Z}_p(1))^{\mathrm{ord}},$$

with the inverse limit taken with respect to trace maps, which is of rank 2 over $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$ (which is to say it is free of rank 2 over the total quotient ring) and free of finite rank over Λ. The lattice $\mathcal{L}$ can be taken to be $\mathcal{T}(N)^{\mathrm{ord}}/I_{\mathcal{F}}\mathcal{T}(N)^{\mathrm{ord}}$, where $I_{\mathcal{F}}$ is the kernel of the map $\phi_{\mathcal{F}}\colon \mathfrak{h}(N,\Lambda)^{\mathrm{ord}} \to \mathcal{A}$ taking T_n to $a_n(\mathcal{F})$ for $n \geq 1$.

The representation $\rho_{\mathcal{F}}$ is again upper-triangular with respect to a good choice of basis when restricted to $G_{\mathbb{Q}_p}$. This is a consequence of the following general result. We use $\mathfrak{h}^{\iota}$ to denote the Galois module on which an element of $G_{\mathbb{Q}}$ acts as $\langle \chi_p(\sigma)\rangle$, where χ_p is the p-adic cyclotomic character.

THEOREM 4.2.15 (OHTA, FUKAYA-KATO). *For $p \geq 5$, there is an exact sequence of $\mathfrak{h}^{\mathrm{ord}}[\![G_{\mathbb{Q}_p}]\!]$-modules*

$$0 \to \mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}} \to \mathcal{T}(N)^{\mathrm{ord}} \to \mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \to 0,$$

where $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}}$ and $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}} \cong (\mathfrak{h}(N,\Lambda)^{\mathrm{ord}})^{\iota}(1)$ as $\mathfrak{h}[\![I_p]\!]$-modules, where I_p is the inertia subgroup of $G_{\mathbb{Q}_p}$. Here, $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}$ is the maximal Λ-torsion-free quotient of $\mathcal{T}(N)^{\mathrm{ord}}$ on which I_p acts trivially, and U_p acts as a Frobenius φ_p on $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}$.

In fact, what Ohta shows using p-adic Hodge theory is that there is a $G_{\mathbb{Q}_p}$-equivariant isomorphism

$$\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \hat{\otimes}_{\mathbb{Z}_p} R \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}} \hat{\otimes}_{\mathbb{Z}_p} R$$

after extending scalars from $\mathcal{O} = \mathbb{Z}_p$ to the completion R of the ring generated over $\mathbb{Z}_p$ by all roots of unity (cf. [**Oht1, Oht2**]). For this, Ohta identifies $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}} \hat{\otimes}_{\mathbb{Z}_p} R$ with an inverse limit over r of cotangent spaces of semistable quotients of the Jacobians of the curves $X_1(Np^r)$ constructed by Mazur-Wiles [**MaWi2**] and Tilouine [**Til**]. Fukaya and Kato point out in [**FuKa**, Proposition 1.7.9] that this descends to a canonical isomorphism

$$D(\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{quo}}) \cong \mathfrak{S}(N,\Lambda)^{\mathrm{ord}},$$

where D is the functor given on compact $\mathfrak{h}[\![G_{\mathbb{Q}_p}]\!]$-modules T for a compact Λ-algebra $\mathfrak{h}$ by the submodule

$$D(T) = \{x \in T \hat{\otimes}_{\mathbb{Z}_p} W \mid (\varphi_p \otimes \varphi_p)(x) = x\}$$

of the completed tensor product, for W the completion of the integer ring of the maximal unramified extension of $\mathbb{Q}_p$ and φ_p the Frobenius map. The functor D is functorially but not canonically isomorphic to the forgetful functor from compact, unramified $\mathfrak{h}[\![G_{\mathbb{Q}_p}]\!]$-modules to compact $\mathfrak{h}$-modules, so $D(T) \cong T$ as $\mathfrak{h}$-modules. It is useful to note that this natural isomorphism is canonical upon restriction to the subcategory of modules with trivial $G_{\mathbb{Q}_p}$-action.

The result on $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}}$ is obtained by twisted Weil (or Poincaré) duality, which takes place through a perfect $\Lambda[G_{\mathbb{Q}}]$-equivariant pairing

$$\langle\ ,\ \rangle\colon \mathcal{T}(N)^{\mathrm{ord}} \times \mathcal{T}(N)^{\mathrm{ord}} \to \Lambda^{\iota}(1) \tag{4.2.1}$$

of Ohta's under which $\mathcal{T}(N)^{\mathrm{ord}}_{\mathrm{sub}}$ is its own annihilator [**Oht1**, Definition 4.1.17]. To obtain this pairing, one must modify the usual Poincaré duality pairing (using powers of U_p) to make it compatible with trace maps and by application of an Atkin-Lehner involution at each stage so that it has the property that $(Tx, y) = (x, Ty)$ for all $x, y \in \mathcal{T}(N)^{\mathrm{ord}}$ and $T \in \mathfrak{h}(N,\Lambda)^{\mathrm{ord}}$.

4.3. Proof of the main conjecture

We now review the proof of the main conjecture in the spirit of Mazur-Wiles [**MaWi1**]. As in its statement, we restrict our discussion to fields of p-power roots of unity (so tame level $N = 1$), and let us suppose in our discussion that $p \geq 5$. We are only interested in irregular primes, so this restriction on p makes no difference to us. The approach we shall take is that of M. Ohta [**Oht2**].

Let us fix an even integer k.

DEFINITION 4.3.1. The Eisenstein ideal I_k of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ is the ideal generated by $U_p - 1$, the elements $T_\ell - 1 - \ell\langle\ell\rangle$ for all primes $\ell \neq p$, and $\langle j\rangle - \omega^{k-2}(j)$ for all $j \in \mu_{p-1}(\mathbb{Z}_p)$.

Consider the maximal ideal

$$\mathfrak{m}_k = I_k + (p, \langle \upsilon\rangle - 1)$$

containing I_k, where $\upsilon \in 1 + p\mathbb{Z}_p$ is as in (2.3.1). We can localize $\mathfrak{h}(1,\Lambda)$ at $\mathfrak{m}_k$, obtaining a local ring $\mathfrak{h}_k$ that is a direct factor of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$.

REMARK 4.3.2. We consider $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$, where $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ as a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \Lambda[\Delta]$-algebra for the inverses of diamond operators, where $\Delta = \mu_{p-1}(\mathbb{Z}_p)$. (This rather strange convention of taking inverse diamond operators will be convenient later.) As $\langle -1\rangle = 1$, the nontrivial eigenspaces of $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ are all even. The algebra $\mathfrak{h}_k$ defined above is free of finite rank over Λ and by our convention has an ω^{2-k}-action of Δ.

For an even integer k, the algebra $\mathfrak{h}_k$ is nonzero if and only if $\mathfrak{h}(1,\Lambda)^{\mathrm{ord}}$ properly contains I_k. This in turn occurs if and only if the constant term $\frac{1}{2}h_{\omega^k}$ of the Λ-adic Eisenstein series $\mathcal{E}_{\omega^{k-2}}$ is not a unit, which is to say exactly when $p \mid B_{2,\omega^{k-2}}$. From now on, we suppose that this divisibility holds.

For simplicity of notation, we set $\mathfrak{h} = \mathfrak{h}_k$, we use $\mathcal{T}$ for $\mathcal{T}_{\mathfrak{m}_k}$, we use $\mathfrak{S}$ for $\mathfrak{S}(1,\Lambda)_{\mathfrak{m}_k}$, we use I for the image of I_k in $\mathfrak{h}$, and so on.

By a result of Manin and Drinfeld, the exact sequence

$$0 \to \mathfrak{S} \to \mathfrak{M} \to \Lambda \to 0 \tag{4.3.1}$$

is nearly split as a sequence of $\mathfrak{H}$-modules: that is, it splits if we first tensor the sequence over Λ with the quotient field $Q(\Lambda)$. Explicitly, this splitting takes $1 \in \Lambda$ to $\frac{2}{h_{\omega^k}}\mathcal{E}_k$. If s denotes this splitting and t denotes the corresponding splitting of $\mathfrak{S} \otimes_\Lambda Q(\Lambda) \to \mathfrak{M} \otimes_\Lambda Q(\Lambda)$, then the congruence module of the sequence (4.3.1) is defined to be

$$t(\mathfrak{M})/\mathfrak{S} \cong s(\Lambda)/(s(\Lambda) \cap \mathfrak{M}),$$

and it is isomorphic to $\Lambda/(\xi)$, where $\xi \in \Lambda$ satisfies $\xi(\upsilon^s - 1) = L_p(\omega^k, s-1)$ for $s \in \mathbb{Z}_p$. From this, we can conclude the following. The proof we give is due to Emerton [**Eme**].

THEOREM 4.3.3 (MAZUR-WILES). *We have an isomorphism $\mathfrak{h}/I \cong \Lambda/(\xi)$ of Λ-modules.*

PROOF. The Λ-adic Eisenstein series $\mathcal{E}_{\omega^{k-2}}$ has integral constant term since $k \not\equiv 0 \bmod p-1$, and one can show that every element of $\mathfrak{M}'$ does as well. By the duality of Hida, the modules $\mathfrak{M}$ and $\mathfrak{H}$ are Λ-dual to each other. In particular, $\mathcal{E}_{\omega^{k-2}}$ gives rise to a surjective homomorphism

$\mathfrak{H} \to \Lambda$ of Λ-algebras with kernel the Eisenstein ideal $\mathcal{I}$ in $\mathfrak{H}$. On the other hand, the surjection $\mathfrak{M} \to \Lambda$ that takes the involution ι applied to constant terms provides an element $T_0 \in \mathfrak{H}$ with kernel $\mathfrak{S}$ on $\mathfrak{M}$. The image of T_0 under $\mathfrak{H} \to \mathfrak{H}/I \cong \Lambda$ is then $\frac{1}{2}\xi$. We then have $\mathfrak{H}/(T_0) \cong \mathfrak{h}$, and if we take the quotient of both sides by the Eisenstein ideal (noting that I is the image of $\mathcal{I}$ in $\mathfrak{h}$), we obtain $\Lambda/(\xi)$. □

At p, we have an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules

$$0 \to \mathcal{T}_{\mathrm{sub}} \to \mathcal{T} \to \mathcal{T}_{\mathrm{quo}} \to 0, \tag{4.3.2}$$

This sequence is split as an exact sequence of $\mathfrak{h}$-modules. That is, by Theorem 4.2.15, the actions of $G_{\mathbb{Q}_p}$ on $\mathcal{T}_{\mathrm{sub}}$ and $\mathcal{T}_{\mathrm{quo}}$ factor through the maximal abelian quotient $G_{\mathbb{Q}_p}^{\mathrm{ab}}$. The unique order $p-1$ subgroup of its inertia group acts on $\mathcal{T}_{\mathrm{quo}}$ trivially and on $\mathcal{T}_{\mathrm{sub}}$ by ω^{k-1}, which is not the trivial character modulo p, allowing us to distinguish the two $\mathfrak{h}$-module summands.

Now, $\mathcal{T}_{\mathrm{sub}} \cong \mathfrak{h}$ and $\mathcal{T}_{\mathrm{quo}} \cong \mathfrak{S}$ as $\mathfrak{h}$-modules. Let $\mathcal{Q}$ denote the quotient field of $\mathfrak{h}$, and note that $V_- = \mathcal{T}_{\mathrm{sub}} \otimes_{\mathfrak{h}} \mathcal{Q}$ and $V_+ = \mathcal{T}_{\mathrm{quo}} \otimes_{\mathfrak{h}} \mathcal{Q}$ are 1-dimensional subspaces of $V = \mathcal{T} \otimes_{\mathfrak{h}} \mathcal{Q}$. Let us fix an ordered basis of V consisting of an element of V_- and an element of V_+, in that order, yielding a p-ramified representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{Q}), \qquad \rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

which is upper-triangular on $G_{\mathbb{Q}_p}$ and for $\tau \in I_p$ has the form

$$\rho(\tau) = \begin{pmatrix} \chi_p(\tau)\langle\chi_p(\tau)\rangle & b(\tau) \\ 0 & 1 \end{pmatrix}.$$

Both $a(\sigma)$ and $d(\sigma)$ lie in $\mathfrak{h}$ inside $Q(\mathfrak{h})$: for this, note that $\mathrm{Hom}_{\mathfrak{h}}(\mathfrak{S}, \mathfrak{S}) \cong \mathfrak{h}$. Since $\det \rho(\sigma) \in \mathfrak{h}$ as well, we also have $b(\sigma)c(\sigma) \in \mathfrak{h}$. In fact, we have the following lemma of Kurihara and Harder-Pink, which was applied to the Λ-adic setting by Ohta.

Lemma 4.3.4. *The elements $a(\sigma) - \det \rho(\sigma)$, $d(\sigma) - 1$, and $b(\sigma)c(\tau)$ are contained in I for all $\sigma, \tau \in G_{\mathbb{Q}}$.*

Proof. By plugging 1 into the characteristic polynomial for (the adjoint action of) the ℓth Hecke operator, which is also that of the Frobenius φ_ℓ for $\ell \neq p$, we have

$$1 - (a(\varphi_\ell) + d(\varphi_\ell)) + \det \rho(\varphi_\ell) = 1 - T_\ell + \ell\langle\ell\rangle \in I$$

By the Čebotarev density theorem, the φ_ℓ are dense in $G_{\mathbb{Q}}$, so by continuity of our Galois representation, we have

$$1 - a(\sigma) - d(\sigma) + \det \rho(\sigma) \in I \tag{4.3.3}$$

for all $\sigma \in G_{\mathbb{Q}}$. Let $\theta \in I_p$ restrict to $-1 \in \mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. By construction, we have $\rho(\theta) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so replacing σ with $\theta\sigma$ in (4.3.3), we obtain

$$1 + a(\sigma) - d(\sigma) - \det \rho(\sigma) \in I$$

and taking the sum and difference of the two equations gives us the first two containments. We then need only note that

$$c(\tau)b(\sigma) = (d(\tau\sigma) - 1) - (d(\tau)d(\sigma) - 1) \in I.$$

□

Now, let B and C denote the $\mathfrak{h}$-spans in $Q(\mathfrak{h})$ of the images of b and c, respectively. Then $BC \subseteq I$ is an ideal of $\mathfrak{h}$ independent of the choice of basis that we made. Another application of Cebotarev density shows that a positive density of Frobenius elements satisfy $d(\varphi_\ell) - 1 \in BC$, which implies that a similar positive density of elements $T_\ell - 1 - \ell\langle\ell\rangle$ lie in BC. From this, we may conclude that BC is a faithful $\mathfrak{h}$-module, and therefore B and C are as well.

Now, let us consider the map

$$\psi_c \colon G_{\mathbb{Q}} \to C/IC, \qquad \psi_c(\sigma) = (\det \rho(\sigma))^{-1} c(\sigma) + IC.$$

This is a cocycle, as matrix multiplication provides the equality

$$c(\sigma\tau) = \det(\rho(\tau))c(\sigma) + c(\tau)d(\tau)$$

for all $\sigma, \tau \in G_{\mathbb{Q}}$, and $d(\tau) - 1 \in I$. Moreover, the restriction of ψ_c to F_∞ is clearly a homomorphism, and by definition it is unramified at p, hence everywhere. Also, for any $\sigma \in G_{\mathbb{Q}}$ and $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$, we have

$$\psi_c(\sigma\tau\sigma^{-1}) = \det \rho(\sigma)^{-1}\psi_c(\tau) = \omega^{1-k}(\sigma)\kappa(\sigma)^{-1}\langle\kappa(\sigma)\rangle^{-1}\psi_c(\tau) = \chi_p(\sigma)^{-1}\sigma\psi_c(\tau)$$

Thus the restriction of ψ_c factors through $X_\infty^{(1-k)}$, and if we twist the source by $\mathbb{Z}_p(1)$, the resulting map

$$\bar{c} \colon X_\infty^{(1-k)}(1) \to C/IC$$

is a homomorphism of Λ-modules for the Λ-module structures arising from the Galois actions on both sides. On C/IC, this Λ-module structure agrees with that coming from the action of inverses of diamond operators.

By construction, the span of the image of ψ_c is C/IC. By considering the images of commutators with the element θ considered in the proof of Lemma 4.3.4, one may check that $\bar{c}$ is itself surjective. The surjectivity of $\bar{c}$ tells us that the characteristic ideal of $X_\infty^{(1-k)}(1)$ is divisible by the characteristic ideal of C/IC. Since C is a faithful $\mathfrak{h}$-module, one can use the theory of Fitting ideals to show that the Eisenstein quotient C/IC has characteristic ideal divisible by the characteristic ideal of $\mathfrak{h}/I$, which is of course (ξ). For the element f_k that appears in the main conjecture, we have $f_k(v^s - 1) = \xi(v^{s+1} - 1)$. Thus, we may conclude that $f_k \mid \mathrm{char}(X_\infty^{(1-k)})$ for all k, which implies equality by the analytic class number formula, as noted in Remark 2.5.2.

4.4. The map ϒ

We continue with the notation of the previous section. We will view $\overline{\mathbb{Q}}$ as the algebraic numbers in $\mathbb{C}$, which fixes in particular a complex conjugation, a generator of the Tate module $\mathbb{Z}_p(1)$, and isomorphisms between Betti and étale cohomology groups of modular curves.

In the proof of the main conjecture, we in essence used the $\mathfrak{h}$-lattice in $\mathcal{T} \otimes_{\mathfrak{h}} \mathcal{Q}$ that is given by the $\mathfrak{h}[G_{\mathbb{Q}}]$-module span of $\mathcal{T}_{\mathrm{sub}}$. This has the form $\mathcal{T}_{\mathrm{sub}} \oplus C'$, for $C' \subset \mathcal{T}_{\mathrm{quo}} \otimes_{\mathfrak{h}} \mathcal{Q}$, where C is identified with $\mathrm{Hom}_{\mathfrak{h}}(\mathcal{T}_{\mathrm{sub}}, C')$. By choosing this lattice, we insure that the homomorphism $\bar{c}$ is surjective. This may seem rather unnatural, and from our perspective it is. Therefore, in this section, we construct a related map Υ using the lattice $\mathcal{T}$ arising from the homology of the closed modular curves, as first defined in [**Sha3**].

We shall play two decompositions of $\mathcal{T}$ into rank one $\mathfrak{h}$-module summands off of each other. These each arise by looking locally at a place of $\mathbb{Q}$: that corresponding to p which we have already discussed and the decomposition $\mathcal{T} = \mathcal{T}^+ \oplus \mathcal{T}^-$ corresponding to the real place. We view $\mathcal{T}/\mathcal{T}^+$ as $\mathcal{T}^-$ in what follows. Set

$$\mathcal{S} = \varprojlim_r H_1(X_1(p^r), \mathbb{Z}_p)^+_{\mathfrak{m}_k},$$

which is isomorphic by our choice of complex embedding to $\mathcal{T}^+$. Our goal is to show that $\mathcal{T}^+/I\mathcal{T}^+$ is both $G_{\mathbb{Q}}$-stable in and a $G_{\mathbb{Q}_p}$-summand of $\mathcal{T}/I\mathcal{T}$, so that we have an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}}]$-modules

$$0 \to \mathcal{T}^+/I\mathcal{T}^+ \to \mathcal{T}/I\mathcal{T} \to \mathcal{T}^-/I\mathcal{T}^- \to 0 \tag{4.4.1}$$

that is canonically locally split at p. Moreover, we claim that $\mathcal{T}^-/I\mathcal{T}^-$ is free of rank 1 over $\mathfrak{h}/I$ with a canonical generator z. Given these facts, we define a homomorphism

$$\Upsilon\colon X^{(1-k)}(1) \to \mathcal{S}/I\mathcal{S}$$

as the composition of the restriction of the 1-cocycle $G_{\mathbb{Q}} \to \mathrm{Hom}_{\mathfrak{h}}(\mathcal{T}^-/I\mathcal{T}^-, \mathcal{T}^+/I\mathcal{T}^+)$ defined by (4.4.1) with evaluation at z. Explicitly, if $q\colon \mathcal{T}/I\mathcal{T} \to \mathcal{T}^-/I\mathcal{T}^-$ denotes the projection, then the cocycle is given on $x \in \mathcal{T}^-/I\mathcal{T}^- \subset \mathcal{T}/I\mathcal{T}$ by

$$x \mapsto \sigma(q(\sigma^{-1}x)) - x.$$

Since $G_{\mathbb{Q}}$ acts nontrivially on $\mathcal{T}^-/I\mathcal{T}^-$, the continuous homomorphism Υ is not $G_{\mathbb{Q}}$-equivariant, but it is still a map of $\Lambda[\Delta]$-modules if we take the Galois action of $\mathbb{Z}_p^\times$ on the left and the action of inverse diamond operators in $\mathbb{Z}_p^\times$ on the right.

Lemma 4.4.1. *The $\mathfrak{h}[G_{\mathbb{Q}}]$-module $Z = \mathcal{T}/I\mathcal{T}$ has a quotient Q canonically isomorphic to $(\Lambda/(\xi))^\iota(1)$.*

Proof. We consider the inverse limit

$$\tilde{\mathcal{T}} = \varprojlim_r H^1_{\text{ét}}(Y_1(p^r), \mathbb{Z}_p(1))_{\mathfrak{m}_k}$$

of the Eisenstein part of cohomology groups of the open modular curves of increasing p-power level. This $\mathfrak{H}$-module $\tilde{\mathcal{T}}$ has the properties that $\tilde{\mathcal{T}}_{\mathrm{sub}} = \mathcal{T}_{\mathrm{sub}}$, while $\tilde{\mathcal{T}}/\mathcal{T} \cong \Lambda$ is generated as a Λ-module by image of the compatible sequence of modular symbols $\{0 \to \infty\}$ at levels p^r. By Theorem 4.2.15 and its analogue for $\tilde{\mathcal{T}}$, we also have $\tilde{\mathcal{T}}/\mathcal{T} \cong \mathfrak{M}/\mathfrak{S}$.

Recall that we have a splitting $t\colon \mathfrak{M} \to \mathfrak{S} \otimes_\Lambda Q(\Lambda)$ of $\mathfrak{H} \otimes_\Lambda Q(\Lambda)$-modules. This induces a splitting $\tilde{\mathcal{T}}_{\mathrm{quo}} \to \mathcal{T}_{\mathrm{quo}} \otimes_\Lambda Q(\Lambda)$ and therefore a splitting $t\colon \tilde{\mathcal{T}} \to \mathcal{T} \otimes_\Lambda Q(\Lambda)$ (via our splitting of $\mathcal{T} \to \mathcal{T}_{\mathrm{quo}}$ and the compatible splitting for $\tilde{\mathcal{T}}$). We then have an isomorphism $t(\tilde{\mathcal{T}})/\mathcal{T} \cong \Lambda/(\xi)$

sending the image of $\{0 \to \infty\}$ to 1. In particular, we have that $x = \xi t(\{0 \to \infty\})$ is part of a Λ-basis of $\mathcal{T}$, and the Λ-module homomorphism

$$\pi\colon \mathcal{T} \to \Lambda, \qquad \pi(a) = \langle x, a \rangle$$

given by Ohta's pairing (4.2.1) is surjective. Note that $t(\tilde{\mathcal{T}})/\mathcal{T}$ is a Galois module upon which $G_{\mathbb{Q}}$ acts trivially. The image of x in Z is then also fixed by $G_{\mathbb{Q}}$, so lies in Z^+. By the Galois equivariance of Ohta's pairing $\mathcal{T} \times \mathcal{T} \to \Lambda^\iota(1)$, the map π induces a surjection of $\Lambda[G_{\mathbb{Q}}]$-modules $\bar{\pi}\colon Z^- \to Q$ for $Q = (\Lambda/(\xi))^\iota(1)$. □

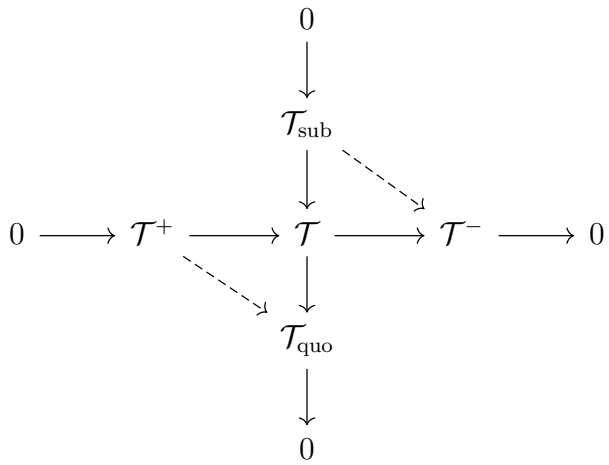
Let $P = \ker(Z \to Q)$, so we have a global exact sequence

$$0 \to P \to Z \to Q \to 0. \tag{4.4.2}$$

The second half of the following proposition now implies that this sequence agrees with (4.4.1) and is locally split, allowing us to construct Υ in the manner already described above.

Proposition 4.4.2 (Fukaya-Kato). *The composite maps $\mathcal{T}^+ \to \mathcal{T} \to \mathcal{T}_{\mathrm{quo}}$ and $\mathcal{T}_{\mathrm{sub}} \to \mathcal{T} \to \mathcal{T}^-$ are isomorphisms. Moreover, $P = Z^+$, the $\mathfrak{h}/I$-module Z^- is free with a canonical generator, and* (4.4.2) *is canonically split as an exact sequence of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules.*

That is, we have a commutative diagram



where the diagonal arrows are isomorphisms.

Proof. The first isomorphism follows from the second. For the second, since $\mathcal{T}_{\mathrm{sub}} \cong \mathfrak{h}$ and $\mathcal{T}^-$ has $\mathfrak{h}$-rank 1, it suffices to verify the surjectivity of $\mathcal{T}_{\mathrm{sub}} \to \mathcal{T}^-$. By Nakayama's lemma, this is further reduced to the surjectivity of $\mathcal{T}_{\mathrm{sub}} \to Z^-$.

Set $Z_{\mathrm{sub}} = \mathcal{T}_{\mathrm{sub}}/I\mathcal{T}_{\mathrm{sub}}$ and $Z_{\mathrm{quo}} = \mathcal{T}_{\mathrm{quo}}/I\mathcal{T}_{\mathrm{quo}}$. We claim that the composite map $Z_{\mathrm{sub}} \to Z \to Q$ of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules is an isomorphism. Since both the source and target are free of rank 1 over $\mathfrak{h}/I$, it suffices to show surjectivity. The cokernel is isomorphic to an $\mathfrak{h}[G_{\mathbb{Q}_p}]$-module quotient of Z_{quo}, but every lift of an element of $\Delta \cong \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ to I_p fixes Z_{quo} but no nonzero element of Q, proving the claim.

Since $Z_{\mathrm{sub}} \to Q$ is an isomorphism, $P \to Z_{\mathrm{quo}}$ is an isomorphism as well. The global exact sequence (4.4.2) is therefore locally split at p by the composite map $Z \to Z_{\mathrm{quo}} \xrightarrow{\sim} P$, as claimed.

It remains, then, only to verify that $P = Z^+$, as this implies that the surjection $Z^- \to Q$ is an isomorphism with a canonical generator z satisfying $\bar{\pi}(z) = 1$. Since $d(\sigma) - 1 \in I$ for all $\sigma \in G_{\mathbb{Q}}$, any complex conjugation acts trivially on Z_{quo}. In other words, P is contained in, and hence equal to, Z^+ inside Z. □

REMARK 4.4.3. Note that $Z^+ \cong \mathcal{S}/I\mathcal{S}$ as Λ-modules as well, as Frobenius acts as U_p on $\mathcal{T}_{\mathrm{quo}}$ (see [**FuKa**, Prop. 1.8.1]), hence trivially on Z_{quo}.

CHAPTER 5

Modular symbols and arithmetic

5.1. Galois cohomology and cup products

We begin this chapter by delving a bit deeper into our study of the arithmetic of cyclotomic fields. For this, we first review some Galois cohomology, which is already quite useful in what we have summarized above. Let K be a number field, and let p be a prime. We suppose that p is odd or K has no real places. We fix a finite set S of finite places of K that contains all places dividing primes over p.

DEFINITION 5.1.1. We use $G_{K,S}$ to denote the Galois group of the maximal S-ramified (or in more usual terminology, unramified outside S and any real places) extension Ω of K.

Let us use A to denote a discrete $\mathbb{Z}[G_{K,S}]$-module. We consider the Galois cohomology groups $H^i(G_{K,S}, A)$ defined by continuous cochains.

REMARK 5.1.2. The group $G_{K,S}$ is a finitely topologically generated profinite group of cohomological dimension 2. That is, the profinite cohomology groups $H^i(G_{K,S}, A)$ are trivial for $i \geq 3$.

REMARK 5.1.3. If K is Galois over some subfield E and A is a discrete $\mathbb{Z}[\mathrm{Gal}(\Omega/E)]$-module, then $\mathrm{Gal}(K/E)$ acts on the groups $H^i(G_{K,S}, A)$. That is, we let $\sigma \in \mathrm{Gal}(K/E)$ act on an inhomogenous i-cochain $f\colon G^i \to A$ by

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

for $g \in G_{K,S}^i$ and $\tilde{\sigma} \in \mathrm{Gal}(\Omega/E)$, and this induces an action on cohomology independent of the choice of lift.

Of particular interest is the case of μ_{p^n}-coefficients, for which the following objects are useful.

DEFINITION 5.1.4.

- Let $\mathcal{O}_{K,S}$ denote the ring of S-integers of K, i.e., elements of K which can be expressed as quotients of elements in $\mathcal{O}_K$ with denominators divisible only by primes in S.
- Let $\mathcal{E}_{K,S} = \mathcal{O}_{K,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ denote the p-completion of the group of S-units of K.
- Let $\mathrm{Cl}_{K,S}$ denote the S-class group of K, i.e., the quotient of the class group Cl_K by the classes of the primes in S, or alternatively, the class group of $\mathcal{O}_{K,S}$.

PROPOSITION 5.1.5. *For all $n \geq 1$, we have canonical exact sequences*

$$0 \to \mathcal{E}_{K,S}/\mathcal{E}_{K,S}^{p^n} \to H^1(G_{K,S}, \mu_{p^n}) \to \mathrm{Cl}_{K,S}[p^n] \to 0$$

$$0 \to \mathrm{Cl}_{K,S}/p^n\mathrm{Cl}_{K,S} \to H^2(G_{K,S}, \mu_{p^n}) \to \textstyle\bigoplus_{v \in S} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Z}/p^n\mathbb{Z} \to 0.$$

The first of these sequences can be derived by Kummer theory, just as in the derivation of (2.3.3). In fact, $H^1(G_{K,S}, \mu_{p^n})$ is the quotient by $K^{\times p^n}$ of the subgroup $\mathcal{B}_{n,K,S}$ of $K^\times$ consisting of those elements a such that the fractional ideal $a\mathcal{O}_{K,S}$ is a p^nth power. The second employs Kummer theory and/or the Poitou-Tate sequence, which we shall not review here, but see [**NSW**, Chapter 8].

REMARK 5.1.6. If K is Galois over E, then the exact sequences of Proposition 5.1.5 are of $\mathbb{Z}_p[\mathrm{Gal}(K/E)]$-modules.

EXAMPLE 5.1.7. Set $F_r = \mathbb{Q}(\mu_{p^r})$ for $r \geq 1$, and let S denote the set of its primes over p. Then S consists of the single principal ideal $(1 - \zeta_{p^r})$, so $\mathrm{Cl}_{F_r,S} \cong \mathrm{Cl}_{F_r}$, and for $n \geq 1$, we have isomorphisms

$$H^2(G_{F_r,S}, \mu_{p^n}) \cong A_r/p^n A_r,$$

where $A_r = \mathrm{Cl}_{F_r} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as before.

We are particularly interested in the cup products

$$H^1(G_{K,S}, \mu_{p^n}) \otimes H^1(G_{K,S}, \mu_{p^n}) \xrightarrow{\cup} H^2(G_{K,S}, \mu_{p^n}^{\otimes 2})$$

If $\mu_{p^n} \subset K$, then the Galois action on $\mu_{p^n}^{\otimes 2}$ is trivial, so as modules over $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$, we have

$$H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}) \cong H^2(G_{K,S}, \mu_{p^n}) \otimes_{\mathbb{Z}_p} \mu_{p^n},$$

allowing us to use the description of $H^2(G_{K,S}, \mu_{p^n})$ in (5.1.5). These cup products induce pairings

$$(\ ,\ )_{p^n,K,S} \colon \mathcal{B}_{n,K,S} \times \mathcal{B}_{n,K,S} \to H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}),$$

which again are $\mathrm{Gal}(K/E)$-equivariant if K is Galois over a subfield E. Composition with the restriction map

$$H^2(G_{K,S}, \mu_{p^n}^{\otimes 2}) \to H^2(G_{K_v}, \mu_{p^n}^{\otimes 2}) \xrightarrow{\sim} \mu_{p^n},$$

where K_v is the completion of K at v and the latter map is the invariant map of class field theory, is the restriction of the Hilbert norm residue symbol

$$(\ ,\ )_{p^n,K_v} \colon K_v^\times \times K_v^\times \to \mu_{p^n}.$$

McCallum and the author proved the following formula for this pairing [**McSh**].

THEOREM 5.1.8 (MCCALLUM-S.). *Suppose that $\mu_{p^n} \subset K^\times$, and let $a, b \in \mathcal{O}_{K,S}^\times$ be such that the norm residue symbols $(a,b)_{p^n,K_v}$ vanish for all $v \in S$. Let α be an p^nth root of a, let $L = K(\alpha)$, and let $G = \mathrm{Gal}(L/K)$. We may write $b = N_{L/K}y$ for some $y \in L^\times$ and $y\mathcal{O}_{L,S} = \mathfrak{c}^{1-\sigma}$ with $\mathfrak{c}$ an ideal of $\mathcal{O}_{L,S}$ and $\sigma \in G$. Then*

$$(a,b)_{p^n,K,S} = N_{L/K}\mathfrak{c} \otimes \alpha^{\sigma-1} \in \mathrm{Cl}_{K,S} \otimes_{\mathbb{Z}} \mu_{p^n}.$$

COROLLARY 5.1.9. *If $a, 1-a \in \mathcal{O}_{K,S}^\times$, then $(a, 1-a)_{p^n,K,S} = 0$.*

PROOF. In the notation of the theorem, we have $1 - a = N_{L/K}(1-\alpha)$, and $1 - \alpha \in \mathcal{O}_{L,S}^\times$. $\square$

Again take $F_n = \mathbb{Q}(\mu_{p^n})$, with S the set of primes over p. In this case, we restrict our cup product to the cyclotomic p-units and then extend it to the p-completion $\mathcal{C}_n$ to yield an antisymmetric, $\mathrm{Gal}(F_n/\mathbb{Q})$-equivariant, bilinear pairing

$$(\ ,\ )_n \colon \mathcal{C}_n \times \mathcal{C}_n \to A_n \otimes_{\mathbb{Z}} \mu_{p^n}.$$

By Corollary 5.1.9 and the fact that $\mathcal{C}_n \cong \mathcal{C}_n^+ \oplus \mu_{p^n}$, we have $(\zeta_{p^n}, 1-\zeta_{p^n}^i)_{p^n,F_n,S} = 0$ for all $1 \leq i < p^n$, so our pairing factors through $\mathcal{C}_n^+$ in each variable and therefore lands in $(A_n \otimes_{\mathbb{Z}} \mu_{p^n})^+ \cong A_n^- \otimes \mu_{p^n}$.

Remark 5.1.10. From Corollary 5.1.9, one can already find a number of interesting pairs on which the pairing vanishes. For instance, we have

$$\frac{1-x^a}{1-x^{a+b}} + x^a \frac{1-x^b}{1-x^{a+b}} = 1 \tag{5.1.1}$$

$$\frac{(1-x^{2a})(1-x^{a+b})}{(1-x^a)(1-x^{2(a+b)})} - x^a \frac{(1-x^b)(1-x^{a+b})}{1-x^{2(a+b)}} = 1 \tag{5.1.2}$$

$$x^b \frac{(1-x^{3a})(1-x^{a+b})}{(1-x^a)(1-x^{3(a+b)})} + \frac{(1-x^b)(1-x^{a+b})(1-x^{2a+b})}{1-x^{3(a+b)}} = 1 \tag{5.1.3}$$

for $a, b \geq 1$, which we can apply to $x = \zeta_{p^n}$ (with appropriate conditions on a and b).

Consider $n = 1$. The eigenspaces $\mathcal{C}_1^{(1-i)}$ for i odd are isomorphic to $\mathbb{Z}_p$, generated by elements η_i that are the projections of $1-\zeta_p$ to these spaces. For any even k, set

$$e_{i,k} = (\eta_i, \eta_{k-i})_1 \in A^{(1-k)} \otimes_{\mathbb{Z}} \mu_p,$$

where $A = A_1$. Note that the eigenspaces here match up as $A^{(1-k)} \otimes_{\mathbb{Z}} \mu_p \cong (A \otimes_{\mathbb{Z}} \mu_p)^{(2-k)}$. These elements $e_{i,k}$ generate the span of the image of the pairing.

Note that if $p \mid B_k$, then in all known cases, $A^{(1-k)} \cong \mathbb{F}_p$ as a group, which is to say for $p < 39 \cdot 2^{22}$ [**BuHa**]. In these cases, one might think of the values $e_{i,k}$ as i varies as lying in $\mathbb{F}_p$ via a choice of generator. Via a computation, we showed in [**McSh**] that for $p < 25000$ and k with $p \mid B_k$, there exists up to scalar a unique nontrivial, antisymmetric, Galois-equivariant pairing $\mathcal{C}_1 \times \mathcal{C}_1 \to \mathbb{F}_p(2-k)$ that satisfies the relations (5.1.2) in Remark 5.1.10.

Example 5.1.11. Here is a table of the relative values of the $e_{i,k}$, normalized so that $e_{1,k} = 1$. (From what we have said, it is not clear that these values are nonzero, but as we shall explain later, they are.). The full tables for $p < 25000$ may be found on the author's webpage.

p	k	$(e_{1,k}, e_{3,k}, \ldots, e_{p-2,k})$
37	32	(1 26 0 36 1 35 31 34 3 6 2 36 1 0 11 36 11 26)
59	44	(1 45 21 30 14 35 5 0 48 57 7 52 2 11 0 54 24 45 29 38 14 58 27 32 15 0 44 27 32)
67	58	(1 45 38 56 0 47 62 9 29 15 65 26 45 57 0 10 22 41 2 52 38 58 5 20 0 11 29 22 66 2 24 43 65)
101	68	(1 56 40 96 26 63 0 61 81 71 35 92 73 64 6 88 0 0 13 95 37 28 9 66 30 20 40 0 38 75 5 61 45 100 17 17 12 66 72 53 86 31 70 15 48 29 35 89 84 84)
691	12	(1 222 647 44 469 690 177 81 234 351 224 0 78 250 507 149 363 359 177 2 250 451 . . .)

The last row is given so one can compare two of its entries with the periods of the normalized weight 12 cuspidal eigenform Δ with Fourier coefficients given by the Ramanunjan τ-function. It might be surprising that $\frac{e_{3,k}}{e_{5,k}}$ and $\frac{r_3(\Delta)}{r_5(\Delta)} = -\frac{14}{9}$ (see Example 3.4.15) are the same modulo 691!

The existence of an essentially unique nontrivial pairing in our computations led us to the following conjecture [**McSh**].

CONJECTURE 5.1.12 (MCCALLUM-S.). *The elements $e_{i,k}$ for odd i and even k generate $A^- \otimes_{\mathbb{Z}} \mu_p$. In other words, the map*

$$\mathcal{C}_1 \otimes_{\mathbb{Z}_p} \mathcal{C}_1 \to A_1^- \otimes_{\mathbb{Z}} \mu_{p^n}$$

induced by the pairing $(\ ,\ )_1$ is surjective.

Let's take a short detour to explain some reasons the values of this pairing are interesting. First, they give the powers appearing in commutators in relations in a presentation of the Galois group $G_{F,S}$ of the maximal pro-p, p-ramified extension of F.

REMARK 5.1.13. Let $\mathcal{G}$ denote the maximal pro-p quotient of $G_{F,S}$. Being a finitely generated pro-p group, it fits in an exact sequence

$$1 \to \mathcal{R} \to \mathcal{F} \to \mathcal{G} \to 1,$$

where $\mathcal{F}$ is a free pro-p group on a minimal finite number d of generators, and $\mathcal{R}$ is a free pro-p subgroup that is generated as a normal subgroup of $\mathcal{F}$ by a minimal finite number r of elements.

Suppose that p is odd and F contains μ_p. As groups, we then have

$$H^i(G_{F,S}, \mu_p^{\otimes i}) \cong H^i(\mathcal{G}, \mathbb{F}_p) \cong \mathrm{Hom}(\mathcal{F}/\mathcal{F}_1, \mathbb{F}_p)$$

for $i \in \{1, 2\}$, where $\mathcal{F}_1 = \mathcal{F}^p[\mathcal{F}, \mathcal{F}]$. Fixing a set of d generators x_i of $\mathcal{G}$, we have a dual basis x_i^* to their images in the maximal elementary abelian p-quotient $\mathcal{F}/\mathcal{F}_1 \cong \mathcal{G}/\mathcal{G}_1$ inside the latter homomorphism group. The cup products $x_i^* \cup x_j^*$ give a collection elements of

$$H^2(\mathcal{G}, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathcal{G}}(\mathcal{R}, \mathbb{F}_p),$$

the latter isomorphism being the inverse of the transgression map in the Hochschild-Serre spectral sequence. This allows us to evaluate $x_i^* \cup x_j^*$ at a relation $r \in \mathcal{R}$. The result $r_{i,j}$ is the power of $[x_i, x_j]$ occuring the expression of the relation $r \in \mathcal{F}_1$ modulo pth powers and triple commutators:

$$r \in \left(\prod_{1 \le i < j \le d} [x_i, x_j]^{r_{i,j}} \right) \mathcal{F}^p[\mathcal{F}, [\mathcal{F}, \mathcal{F}]],$$

where one might note that the ordering of the product does not matter.

For our second application, we want to consider continuous Galois cohomology groups $H^1(G_{K,S}, T)$ with coefficients in a finitely generated module T over a compact local $\mathbb{Z}_p$-algebra R with finite residue field (e.g., $R = \mathbb{Z}_p$). This cohomology, defined via continuous cochains, has the property that

$$H^i(G_{K,S}, T) \cong \varprojlim_n H^i(G_{K,S}, T/\mathfrak{m}^n T)$$

for all $i \ge 0$, where $\mathfrak{m}$ is the maximal ideal of R.

REMARK 5.1.14. Since $G_{K,S}$ has cohomological dimension 2, we always have

$$H^2(G_{K,S}, T/\mathfrak{m}^n T) \cong H^2(G_{K,S}, T) \otimes_R R/\mathfrak{m}^n R.$$

EXAMPLE 5.1.15. Upon taking inverse limits of the exact sequences of Proposition 5.1.5, we obtain a canonical isomorphism

$$H^1(G_{K,S}, \mathbb{Z}_p(1)) \cong \mathcal{E}_{K,S}$$

and a canonical exact sequence

$$0 \to \mathrm{Cl}_{K,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^2(G_{K,S}, \mathbb{Z}_p(1)) \to \bigoplus_{v \in S} \mathbb{Z}_p \xrightarrow{\sum} \mathbb{Z}_p \to 0.$$

REMARK 5.1.16. Since $G_{K,S}$ has cohomological dimension 2, if L/K is any Galois extension with Galois group G and we use S also to denote the primes over S in K, then for any T as above we have an isomorphism

$$H^2(G_{L,S}, T)_G \xrightarrow{\sim} H^2(G_{K,S}, T)$$

from the coinvariant group of $H^2(G_{L,S}, T)$, i.e., the maximal quotient of $H^2(G_{L,S}, T)$ on which G acts trivially. Note that the coinvariant group M_G of an $R[G]$-module M is isomorphic to $M/I_G M$, where I_G is the augmentation ideal in $R[G]$.

It is often remarkably useful to think of cup products as connecting homomorphisms.

LEMMA 5.1.17. *Let L/K be an S-ramified abelian pro-p extension of K with Galois group G. The connecting homomorphism*

$$\Psi_{L/K,S} \colon H^1(G_{K,S}, \mathbb{Z}_p(1)) \to H^2(G_{K,S}, G(1))$$

in the long exact sequence associated to the short-exact sequence

$$0 \to G \xrightarrow{g \mapsto g-1} \mathbb{Z}_p[G]/I_G^2 \xrightarrow{g \mapsto 1} \mathbb{Z}_p \to 0 \tag{5.1.4}$$

satisfies $a \mapsto a \cup \pi_G$, where $\pi_G \colon G_{K,S} \to G$ is the projection map.

DEFINITION 5.1.18. We call the map $\Psi_{L/K,S}$ the S-recriprocity map for L/K. When L is taken to be the maximal abelian pro-p S-ramified extension of K, we write $\Psi_{K,S}$ for $\Psi_{L/K,S}$ and refer to it simply as the S-reciprocity map for K.

Using S-reciprocity maps, we can give the following description of the second graded quotient of $H^2(G_{L,S}, \mathbb{Z}_p(1))$ in its augmentation filtration (cf. [**Sha1**]).

PROPOSITION 5.1.19. *Let L/K be an S-ramified abelian pro-p extension. Then we have a canonical isomorphism*

$$\frac{I_G H^2(G_{L,S}, \mathbb{Z}_p(1))}{I_G^2 H^2(G_{L,S}, \mathbb{Z}_p(1))} \cong \frac{H^2(G_{K,S}, G(1))}{\Psi_{L/K,S}(\mathcal{E}_{K,S})}.$$

In our specific case of interest, we have the following. Let $A_{K,S}$ denote the p-part of the S-class group $\mathrm{Cl}_{K,S}$.

COROLLARY 5.1.20. *Let Φ be a subgroup of $\mathcal{B}_{n,F_n,S}$, and let E_n be the Kummer extension of F_n obtained by adjoining all p^nth roots of elements of Φ. Suppose that E_n/F_n is totally ramified*

at the unique prime over p. Set $G = \mathrm{Gal}(E_n/F_n)$. The norm map induces an isomorphism $(A_{E_n,S})_G \xrightarrow{\sim} A_n$, and we have an isomorphism

$$\frac{I_G A_{E_n,S}}{I_G^2 A_{E_n,S}} \cong \frac{A_n \otimes_{\mathbb{Z}_p} G}{\Psi_{E_n/F_n,S}(\mathcal{E}_n)}$$

These are isomorphisms of $\mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$-modules if $E_n/\mathbb{Q}$ is Galois, i.e., if $\Phi F_n^{\times p^n}$ is preserved by $\mathrm{Gal}(F_n/\mathbb{Q})$.

Note in the above that while $A_{E_n,S}$ does not have a canonical $\mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$-module structure, its graded quotients in the augmentation filtration do.

EXAMPLE 5.1.21. Consider the extension $E = F(\eta_i^{1/p})$ of F for an odd integer i. It has Galois group $G \cong \mu_p^{\otimes i}$ as a $\mathbb{Z}_p[\Delta]$-module. Suppose that Vandiver's conjecture holds at p and that $i \not\equiv \pm(k-1) \bmod p$ for all even integers k with $p \mid B_{1,\omega^{k-1}}$. If $e_{i,k} \neq 0$ for all such k (i.e., if pairing with η_i is surjective), then $A_E \cong A_F$ via the norm map.

This is shown using Corollary 5.1.20. The key point beyond its application is that if $I_G A_E / I_G^2 A_E = 0$, then $A_E \cong (A_E)_G$, and since E/F is ramified at p, the norm map induces an isomorphism $(A_E)_G \cong A_F$. The condition that $i \not\equiv 1-k \bmod p-1$ insures this ramification, and the condition that $i \not\equiv k-1 \bmod p-1$ then insures that $A_{E,S} \cong A_E$.

5.2. Iwasawa cohomology

We maintain the notation of Section 5.1. Note that since K cannot contain all p-power roots of unity, the groups $H^2(G_{K,S}, \mathbb{Z}_p(1))$ and $H^2(G_{K,S}, \mathbb{Z}_p(2))$ need not be isomorphic. In fact, while $H^2(G_{K,S}, \mathbb{Z}_p(2))$ is a finite group, the group $H^2(G_{K,S}, \mathbb{Z}_p(1))$ need not be finite, as Remark (5.1.15) shows. This presents a problem if we wish to consider the application of cup products

$$H^1(G_{K,S}, \mathbb{Z}_p(1)) \times H^1(G_{K,S}, \mathbb{Z}_p(1)) \to H^2(G_{K,S}, \mathbb{Z}_p(2))$$

to the structure of class groups. This can be remedied to an extent by passing up the cyclotomic $\mathbb{Z}_p$-extension under corestriction maps. Recall the notation for cyclotomic $\mathbb{Z}_p$-extensions from Remark 2.3.1.

DEFINITION 5.2.1. Let T be a compact $R[\![G_{K,S}]\!]$-module, where R is a compact $\mathbb{Z}_p$-algebra. For $i \geq 0$, the ith Iwasawa cohomology group of K_∞ with T-coefficients is the $R[\![\Gamma]\!]$-module

$$H^i_{\mathrm{Iw},S}(K_\infty, T) = \varprojlim_n H^i(G_{K_n,S}, T),$$

where the inverse limit is taken with respect to corestriction maps.

EXERCISE 5.2.2. Show that $H^0_{\mathrm{Iw},S}(K_\infty, T) = 0$.

REMARK 5.2.3. For $R = \mathbb{Z}_p$, we have

$$H^2_{\mathrm{Iw},S}(K_\infty, T) \cong \varprojlim_n H^2(G_{K_n,S}, T/p^n T),$$

If $\mu_q \subset K$, then $\mu_{p^r} \subset K_n$, so G_{F_n} acts trivially on μ_{p^n}. We can then pull Tate twists out of the groups: i.e., we have isomorphisms

$$H^2_{\mathrm{Iw},S}(F_\infty, T(i)) \cong H^2_{\mathrm{Iw},S}(F_\infty, T)(i)$$

of $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$-modules for all $i \in \mathbb{Z}$. Each group $H^2(G_{K,S}, T(i))$ is then determined by the group $H^2_{\mathrm{Iw},S}(K_\infty, T)$ as a coinvariant group of the ith Tate twist:

$$H^2(G_{K,S}, T(i)) \cong (H^2_{\mathrm{Iw},S}(K_\infty, T)(i))_\Gamma$$

Example 5.2.4. We have in the notation of Section 2.5 that

$$H^1_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(1)) \cong \mathcal{E}_\infty \quad \text{and} \quad H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(1)) \cong X_\infty.$$

In particular, $H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2)) \cong X_\infty(1)$.

If we replace F by any number field, the first isomorphism holds for the inverse limit of p-completions of p-units in the fields K_n, but for the second, one has an exact sequence as in Example 5.1.15.

$$0 \to X'_\infty \to H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \to \bigoplus_{v \in S} \mathbb{Z}_p[\Gamma/\Gamma_v] \to \mathbb{Z}_p \to 0,$$

where X'_∞ denotes the completely split Iwasawa module over K_∞, which is to say the Galois group of the maximal abelian pro-p extension of K_∞ in which all primes (over p) split completely, and Γ_v denotes the decomposition group at v in $\Gamma = \mathrm{Gal}(K_\infty/K)$.

We can define S-reciprocity maps at the level of K_∞. Let $\mathcal{E}_{K_\infty} = \varprojlim_n \mathcal{E}_{K_n,S}$ under norm maps (which is independent of S containing the primes over p).

Definition 5.2.5. Let L_∞ be an S-ramified abelian pro-p extension of K_∞ with Galois group G. The S-reciprocity map

$$\Psi_{L_\infty/K_\infty,S} \colon \mathcal{E}_{K_\infty} \to H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \hat{\otimes}_{\mathbb{Z}_p} G,$$

where $\hat{\otimes}_{\mathbb{Z}_p}$ denotes the completed tensor product (i.e., inverse limit of tensor products of quotients by closed subgroups) is the map induced by the connecting homomorphism

$$H^1_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \to H^2_{\mathrm{Iw},S}(K_\infty, G(1))$$

for the long exact sequence attached to the short exact sequence of (5.1.4). If L_∞ is the maximal S-ramified abelian pro-p extension of K_∞, we write $\Psi_{K_\infty,S}$ for $\Psi_{L_\infty/K_\infty,S}$.

Exercise 5.2.6. Determine how this map interpolates (inverse limits of) cup products.

The analogues to Proposition 5.1.19 and Corollary 5.1.20 for Iwasawa cohomology are then as follows.

Proposition 5.2.7. *Let L_∞/K_∞ be an S-ramified abelian pro-p extension with Galois group $G = \mathrm{Gal}(L_\infty/K_\infty)$. Then we have a canonical isomorphism*

$$\frac{I_G H^2_{\mathrm{Iw},S}(L_\infty, \mathbb{Z}_p(1))}{I_G^2 H^2_{\mathrm{Iw},S}(L_\infty, \mathbb{Z}_p(1))} \cong \frac{H^2_{\mathrm{Iw},S}(K_\infty, \mathbb{Z}_p(1)) \hat{\otimes}_{\mathbb{Z}_p} G}{\Psi_{L_\infty/K_\infty,S}(\mathcal{E}_{K_\infty})},$$

which is of Λ-modules if L_∞/K is Galois.

Specializing to our specific case of interest that $F = \mathbb{Q}(\mu_p)$ and $S = \{(1-\zeta_p)\}$, we have the following.

COROLLARY 5.2.8. *Suppose that Φ is a closed $\mathrm{Gal}(F_\infty/\mathbb{Q})$-stable subgroup of the p-completion of the p-unit group of F_∞. Let E_∞ be the Kummer extension of F_∞ obtained by adjoining all p-power roots of elements of Φ, which is then Galois over $\mathbb{Q}$, and suppose it is totally ramified at the unique prime over p. Set $G = \mathrm{Gal}(E_\infty/F_\infty)$. Let X'_{E_∞} denote the inverse limit of p-parts of S-class groups of number fields in E_∞. If E_∞ has a unique prime over p, then $(X'_{E_\infty})_G \cong X_\infty$, and we have a canonical isomorphism*

$$\frac{I_G X'_{E_\infty}}{I_G^2 X'_{E_\infty}} \cong \frac{X_\infty \otimes_{\mathbb{Z}_p} G}{\Psi_{E_\infty/K_\infty,S}(\mathcal{E}_\infty)}$$

of $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!]$-modules.

EXAMPLE 5.2.9. We may for instance take E_∞ to be given by adjoining to F_∞ all p-power roots of $\eta_i \in \mathcal{E}_\infty$ for some i as in Example 5.1.21. Note that $\mathrm{Gal}(E_\infty/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ for a particular choice of semi-direct product. In this case, under the assumptions of said example (i.e., pairing with η_i is surjective), we have $X_{E_\infty} \cong X_{F_\infty}$, as can be seen by Nakayama's lemma. In particular, it would appear to be typical behavior that the unramified Iwasawa module X_{E_∞} is finitely generated over $\mathbb{Z}_p$, though in principle it could be much larger! It's reasonable to ask the open question of whether this is always the case.

5.3. K-groups and Steinberg symbols

We can interpret the Galois cohomology groups in question as K-groups of S-integer rings via a standard description of K_1 and a theorem of Tate. We keep the assumptions and notations of the previous two sections. For definitions and properties of the lower (resp., higher) K-groups, see the book of Milnor [**Mil**] (resp., Weibel [**Wei**]).

We have $K_1(\mathcal{O}_{K,S}) \cong \mathcal{O}_{K,S}^\times$, so

$$K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^1(G_{K,S}, \mathbb{Z}_p(1)),$$

and Tate showed the existence of a canonical isomorphism

$$K_2(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^2(G_{K,S}, \mathbb{Z}_p(2)).$$

We have product maps in K-theory, in particular

$$K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} K_1(\mathcal{O}_{K,S}) \to K_2(\mathcal{O}_{K,S}),$$

the image of $a \otimes b$ being what is known as the Steinberg symbol $\{a, b\}$ (see Milnor's book).

PROPOSITION 5.3.1. *We have a commutative diagram*

$$\begin{array}{ccc} K_1(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} K_1(\mathcal{O}_{K,S}) & \xrightarrow{\{\,,\,\}} & K_2(\mathcal{O}_{K,S}) \\ \downarrow & & \downarrow \\ H^1(G_{K,S}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(G_{K,S}, \mathbb{Z}_p(1)) & \xrightarrow{\cup} & H^2(G_{K,S}, \mathbb{Z}_p(2)). \end{array}$$

REMARK 5.3.2. At primes in S, we have tame symbols on $K_2(\mathcal{O}_{K,S})$, which for any $v \in S$ (which we treat as an additive valuation) with residue field k_v, which are given by the composition of $K_2(\mathcal{O}_{K,S}) \to K_2(K)$ with the map

$$K_2(K) \to k_v^\times, \qquad \{a,b\} \mapsto (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}},$$

recalling that $K_2(K)$ is generated by Steinberg symbols by the theorem of Matsumoto. There is a canonical exact sequence

$$0 \to K_2(\mathcal{O}_K) \to K_2(\mathcal{O}_{K,S}) \to \bigoplus_{v \in S} k_v^\times \to 0.$$

Note that $k_v^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0$ if v lies over p.

More generally, the Quillen-Lichtenbaum conjecture, which was proven as a consequence of the work of Voevodsky and Rost, gives us the following isomorphisms.

THEOREM 5.3.3. *For $j \in \{1,2\}$ and any $i \geq 1$, there are canonical isomorphisms*

$$c_{i,j} \colon K_{2i-j}(\mathcal{O}_{K,S}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} H^j(G_{K,S}, \mathbb{Z}_p(i))$$

compatible with products in K-theory and cup products.

EXAMPLE 5.3.4. Suppose that p is odd. For even $k \geq 2$, the quotient of the p-parts of the orders of $K_{2k-2}(\mathbb{Z})$ and $K_{2k-1}(\mathbb{Z})$ is $p^{v_p(B_k/k)}$. Explicitly, for any $i \geq 1$, we have

$$K_{2i-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^2(G_{\mathbb{Q},S}, \mathbb{Z}_p(i)) \cong (X_\infty^{(1-i)}(i-1))_\Gamma,$$
$$K_{2i-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p(i)) \hookleftarrow (\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma,$$

where the latter injection has cokernel $(X_\infty^{(1-i)}(i-1))^\Gamma$. If i is odd and $X^{(1-i)} = 0$, then $(\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma \cong \mathbb{Z}_p$ is generated by the image of a certain limit of cyclotomic p-units. If i is even, then $(X_\infty^{(1-i)}(i-1))^\Gamma = 0$, and $(\mathcal{E}_\infty^{(1-i)}(i-1))_\Gamma$ is isomorphic to the finite group $\mathbb{Z}_p(i-1)_{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})}$. It follows that, under Vanidver's conjecture at p, the nonvanishing of $e_{i,k}$ is equivalent to the surjectivity of the products

$$K_{2i-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} K_{2(k-i)-1}(\mathbb{Z}) \to K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

for odd $i \geq 1$ and even $k \geq 2$.

5.4. The map ϖ

We begin by defining a special class of modular symbols inside the first homology group of a modular curve relative to its cusps. Let N be a positive integer. Recall that $\mathcal{M}_2(N) = H_1(X_1(N), C_1(N), \mathbb{Z})$.

DEFINITION 5.4.1. For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, the Manin symbol $[u:v]_N \in \mathcal{M}_2(N)$ is

$$[u:v]_N = \left\{ \frac{b}{d} \to \frac{a}{c} \right\}_N,$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $u = c \bmod N$ and $v = d \bmod N$.

The reader can check that $[u:v]_N$ exists and is well-defined. Note that $[u:v]_N = \gamma\{0 \to \infty\}_N$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is as in the definition of $[u:v]_N$. Manin proved the follwing [**Man1**].

THEOREM 5.4.2 (MANIN). *The group $\mathcal{M}_2(N)$ is generated by the Manin symbols $[u:v]_N$ with $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, and it is presented by these symbols subject to the relations*

$$[u:v]_N = [-u:-v]_N = -[-v:u]_N = [u:u+v]_N + [u+v:v]_N$$

for all such u and v.

PROOF THAT THE RELATIONS HOLD. The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. Note that $S^2 = T^3 = -I$, and $-I$ fixes all cusps, thus all modular symbols. The latter implies the first equality. Note that

$$\{0 \to \infty\}_N + S\{0 \to \infty\}_N = \{0 \to \infty\}_N + \{\infty \to 0\}_N = 0$$

and

$$\{0 \to \infty\}_N + T\{0 \to \infty\}_N + T^2\{0 \to \infty\}_N = \{0 \to \infty\}_N + \{-1 \to 0\}_N + \{\infty \to -1\}_N = 0.$$

Applying $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to these relations yields the relations on Manin symbols. □

REMARK 5.4.3. There is also a presentation of $\mathcal{M}_k(N)$ in terms of Manin symbols, again having the form

$$X^{i-1}Y^{k-i-1}[u:v] = \gamma \cdot X^{i-1}Y^{k-i-1}\{0 \to \infty\}$$

with $u, v \in \mathbb{Z}/N\mathbb{Z}$ and $(u,v) = (1)$, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $(u,v) = (c,d) \bmod N\mathbb{Z}^2$ (cf. [**Mer**]).

DEFINITION 5.4.4. Set $\mathbb{Z}' = \mathbb{Z}[\frac{1}{2}]$. For a $\mathbb{Z}$-module M with a commuting action of a complex conjugation τ (i.e., an involution) and $m \in M$, we set $M^+ = (M \otimes_{\mathbb{Z}} \mathbb{Z}')^+$ and $m^+ = \frac{1}{2}(m + \tau(m)) \in M^+$.

For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, we have

$$[u:v]_N^+ = \frac{1}{2}([u:v]_N + [-u:v]_N) \in \mathcal{M}_2(N)^+.$$

DEFINITION 5.4.5. For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$, we set

$$[u:v]_N^* = w_N[u:v]_N^+ = \left\{\frac{d}{bN} \to \frac{c}{aN}\right\}^+ \in \mathcal{M}_2(N)^+.$$

DEFINITION 5.4.6. The non-zero cusps $C_1^\circ(N)$ of $X_1(N)$ are the cusps that do not lie over the cusp $0 \in X_0(N)$.

The zero cusps in $X_1(N)$, i.e., those that map to $0 \in X_0(N)$, are exactly those represented by a reduced fraction $\frac{a}{c}$ with c prime N. We have the following corollary of Theorem 5.4.2 for the relative homology group

$$\mathcal{S}_2^\circ(N) = H_1(X_1(N), C_1^\circ(N), \mathbb{Z}).$$

COROLLARY 5.4.7. *The group $\mathcal{S}_2^\circ(N)^+$ is generated by the $[u:v]_N^*$ with $u,v \in \mathbb{Z}/N\mathbb{Z} - \{0\}$ and $(u,v) = (1)$, subject to the relations*

$$[u:v]_N^* = [-u:v]_N^* = -[v:u]_N^* = [u:u+v]_N^* + [u+v:v]_N^*$$

for u, v as above (noting that the last term is zero if $u+v=0$).

Let us use a subscript N when denoting Steinberg symbols in $K_2(\mathbb{Z}[\frac{1}{N}, \mu_N])$. The following was proven independently in nearly this form by Busuioc [**Bus**] and the author [**Sha3**].

PROPOSITION 5.4.8 (BUSUIOC, SHARIFI). *There exists a map*

$$\Pi_N^\circ \colon \mathcal{S}_2^\circ(N)^+ \to K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N])^+$$

satisfying

$$\Pi_N^\circ([u:v]_N^*) = \{1-\zeta_N^u, 1-\zeta_N^v\}_N^+$$

for all $u, v \in \mathbb{Z}/N\mathbb{Z} - \{0\}$ with $(u,v) = (1)$.

PROOF. We need only show that Π_N° respects the relations of Corollary 5.4.7. Dirichlet's unit theorem tells us that

$$\mathbb{Z}[\mu_N]^\times \cong \mu_M \oplus (\mathbb{Z}[\mu_N]^+)^\times / \langle -1 \rangle.$$

where $M = N$ or $2N$ depending on whether N is even or odd, respectively. For $\zeta \in \mu_M$, we have $\{\zeta, \zeta\}_N = 0$ by antisymmetry, and we have $\{\zeta, u\}_N^+ = 0$ for all $u \in (\mathbb{Z}[\mu_N]^+)^\times$ as $\{\zeta, u\}_N$ is inverted by complex conjugation. Thus, $\{\zeta, v\}_N^+ = 0$ for all $v \in \mathbb{Z}[\mu_N]^\times$.

Now, note that $1 - \zeta_N^u = -\zeta_N^u(1-\zeta_N^{-u})$, so we have

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = \{1-\zeta_N^{-u}, 1-\zeta_N^v\}_N^+,$$

Moreover, Steinberg symbols are antisymmetric, so in particular we have

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = -\{1-\zeta_N^v, 1-\zeta_N^u\}_N^+.$$

Finally, we note that

$$\frac{1-\zeta_N^u}{1-\zeta_N^{u+v}} + \zeta_N^u \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}} = 1,$$

so

$$\left\{ \frac{1-\zeta_N^u}{1-\zeta_N^{u+v}}, \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}} \right\}_N^+ = 0,$$

which yields

$$\{1-\zeta_N^u, 1-\zeta_N^v\}_N^+ = \{1-\zeta_N^u, 1-\zeta_N^{u+v}\}_N^+ + \{1-\zeta_N^{u+v}, 1-\zeta_N^v\}_N^+$$

by bilinearity and antisymmetry. □

REMARK 5.4.9. The map Π_N° satisfies $\Pi_N^\circ(\langle j \rangle^{-1} x) = \sigma_j \Pi^\circ(x)$ for all $x \in \mathcal{S}^\circ(2)(N)^+$ and all $j \in (\mathbb{Z}/N\mathbb{Z})^\times$.

The following lemma was proven by Fukaya and Kato on p-completions for p dividing N.

LEMMA 5.4.10. *The map Π_N° restricts to a map*

$$\Pi_N \colon \mathcal{S}_2(N)^+ \to K_2(\mathbb{Z}[\mu_N])^+.$$

PROOF. For a prime ℓ, let q_ℓ denote the order of the residue field of a fixed prime over ℓ in $\mathbb{Q}(\mu_N)$. We claim that there exists a map f as in the diagram

$$\begin{array}{ccc} H_1(X_1(N), C_1^\circ(N), \mathbb{Z}') & \longrightarrow & \mathbb{Z}'[C_1^\circ(N)] \\ \downarrow{\scriptstyle \Pi_N^\circ} & & \downarrow{\scriptstyle f} \\ K_2(\mathbb{Z}[\frac{1}{N}, \mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}' & \longrightarrow & \bigoplus_{\ell | N} \mathbb{F}_{q_\ell}^\times \otimes_{\mathbb{Z}} \mathbb{Z}' \end{array} \tag{5.4.1}$$

that makes it commute, where the upper horizontal arrow is the boundary map, the lower horizontal arrow is the sum of tame symbols (see Remark 5.3.2) at our fixed primes over $\ell \mid N$. (Here, we consider Π_N° to be zero on the minus part of homology.)

We define the projection f_ℓ of the map f to the ℓ-coordinate of the direct sum. For an integer n, let n_ℓ denote the ℓ-part of (n, N), and let $n'_\ell = \frac{n}{n_\ell}$. For a non-zero cusp $\{\frac{c}{aN}\}$, where $\frac{a}{c}$ is in reduced form and a is prime to N, set $f_\ell(\{\frac{c}{aN}\}) = 1$ unless (c, N) is a power of ℓ, and otherwise set

$$f_\ell\left(\left\{\frac{c}{aN}\right\}\right) = \begin{cases} (1 - \zeta_{N'_\ell}^{(aN_\ell)^{-1}})^{-c_\ell} & \text{if } N'_\ell \neq 1 \\ c'_\ell & \text{if } N'_\ell = 1. \end{cases}$$

The commutativity is now left as an exercise. □

Merel provided rather nice formulas for the action of Hecke operators on Manin symbols [**Mer**].

THEOREM 5.4.11 (MEREL). *For a positive integer n and $u, v \in \mathbb{Z}/n\mathbb{Z}$ with $(u, v) = (1)$, we have*

$$T_n([u : v]_N) = \sum_{\substack{a,b,c,d \geq 0 \\ ad-bc=n \\ a>b,\, d>c}} [au + cv : bu + dv]_N,$$

where we take $[x : y]_N$ to be zero if $(x, y) \neq (1)$.

EXAMPLE 5.4.12. We have

$$T_2([u : v]_N) = [2u : v]_N + [2u : u + v]_N + [u + v : 2v]_N + [u : 2v]_N. \tag{5.4.2}$$

and

$$\begin{aligned} T_3([u : v]_N) = {} & [3u : v]_N + [3u : u + v]_N + [3u : 2u + v]_N \\ & + [2u + v : u + 2v]_N + [u + 2v : 3v]_N + [u + v : 3v]_N + [u : 3v]_N. \end{aligned} \tag{5.4.3}$$

The reader might try the fun computation that the relations (5.1.2) and (5.4.2) (resp., (5.1.3) and (5.4.3)) yield the cases $\ell = 2, 3$ in the following theorem of Fukaya and Kato, which was conjectured in a slightly weaker form (that Π_N is Eisenstein in the same sense as what follows) in [**Sha3**, Conjecture 5.8].

THEOREM 5.4.13 (FUKAYA-KATO). *Suppose that $p \mid N$ is an prime greater than 3. For every prime $\ell \geq 1$, the map*

$$\Pi_N^\circ \colon \mathcal{S}_2^\circ(N)^+ \otimes \mathbb{Z}_p \to K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N])^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

satisfies

$$\Pi_N^\circ \circ (T_\ell - 1 - \ell\langle\ell\rangle) = 0$$

for all primes $\ell \nmid N$ *and* $\Pi_N^\circ(U_\ell - 1) = 0$ *for all primes* $\ell \mid N$.

Sketch of proof of Theorem 5.4.13. Via a regulator computation, Fukaya and Kato exhibit the Hecke-equivariance of a map

$$z_N^\sharp \colon \mathcal{S}_2^\circ(N) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to H^2_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Q}_p(2))^{\text{ord}}$$

that takes a symbol $[u : v]^*$ to a Beilinson-Kato element $g_u \cup g_v$, where g_u and g_v are the Siegel units on $Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}$ of Remark 3.2.9. This map is not in general integral, but the growth of its denominators can be controlled in the tower of increasing p-power levels (and the maps are compatible with degeneracy maps and corestriction), so for the purpose of this sketch, we can suppose it takes values in $H^2_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2))^{\text{ord}}$.

For any $i \geq 0$, there exists a map

$$\infty \colon H^i_{\text{ét}}(Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2)) \to H^i(G_{\mathbb{Q}(\mu_N),S}, \mathbb{Z}_p(2)),$$

where S is the set of primes of $\mathbb{Q}(\mu_N)$ over N, associated to pullback by the cusp at infinity, which is not quite a point on $Y_1(N)$ but may be viewed as a morphism

$$\infty \colon \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}, \mu_N]^+(\!(q)\!) \to Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]}.$$

The map is pullback followed by a composition

$$H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N](\!(q)\!), \mathbb{Z}_p(2))^+ \to H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N][\![q]\!], \mathbb{Z}_p(2))^+ \xrightarrow{q \mapsto 0} H^i_{\text{ét}}(\mathbb{Z}[\tfrac{1}{N}, \mu_N], \mathbb{Z}_p(2))^+,$$

the first map being a splitting of the canonical surjection. We note that the latter étale cohomology group is isomorphic to $H^i(G_{\mathbb{Q}(\mu_N),S_N}, \mathbb{Z}_p(2))^+$ for S_N the set of primes of $\mathbb{Q}(\mu_N)$ over N. These maps are compatible with cup products.

The effect of ∞ on g_u is to forget about the power of q that occurs in its q-expansion and then evaluate it at 0, which results in a root of unity times $1 - \zeta_N^u$. Thus, $\infty \circ z_N^\sharp([u : v]_N) = \{1-\zeta_N^u, 1-\zeta_N^v\}_N$. The result then follows from the Hecke-equivariance of $z^\sharp$ and the computable facts that for any ℓ prime to N, one has $\infty \circ (T_\ell - 1 - \ell\langle\ell\rangle) = 0$, while for all ℓ dividing N, one has $\infty((U_\ell - 1)(g_u \cup g_v)) = 0$, which in particular implies that $z_N^\sharp([u : v]_N)$ and its ordinary projection have the same image under ∞. Thus $\Pi_N^\circ = \infty \circ z^\sharp$, and it is Eisenstein in the sense defined in the theorem. □

In particular, Π_N° and Π_N factor through maps

$$\varpi_N^\circ \colon \mathcal{S}_2^\circ(N)^+/I\mathcal{S}_2^\circ(N)^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to (K_2(\mathbb{Z}[\tfrac{1}{N}, \mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^+$$

and

$$\varpi_N \colon \mathcal{S}_2(N)^+/I\mathcal{S}_2(N)^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to (K_2(\mathbb{Z}[\mu_N]) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^+.$$

For any prime ℓ dividing N, a Manin-type symbol $[\ell u : v]^*_{N\ell} \in \mathcal{S}_2(N\ell)$ maps to $[u : v]^*_N$ under the degeneracy map ϵ_1 on homology, and $\{1-\zeta_N^u, 1-\zeta_{N\ell}^v\}_{N\ell}$ has norm $\{1-\zeta_N^u, 1-\zeta_N^v\}_N$. That is, the maps $\varpi_{N\ell}$ and ϖ_N are compatible.

5.5. A conjecture and known results

We now return to the Hida-theoretic and Iwasawa-theoretic settings, again restricting to the modular tower $X_1(p^r)$ and the cyclotomic tower $F_r = \mathbb{Q}(\mu_{p^r})$ for a fixed irregular prime p. Let $k \geq 2$ be an even integer such that $p \mid B_{2,\omega^{k-2}}$. We adopt the notation of Section 4.3 and work on the modular side with localizations at the Eisenstein maximal ideal $\mathfrak{m}_k$.

We recall our map Υ and define a map ϖ out of the maps ϖ_{p^r} of the previous section. For S the set consisting of the prime over p in F, let us set

$$Y = H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2))^{(2-k)} \cong X_\infty^{(1-k)}(1),$$

as in Example 5.2.4. The map Υ then becomes a map $\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$.

Using the isomorphisms

$$(K_2(\mathbb{Z}[\mu_{p^r}]) \otimes \mathbb{Z}_p)^+ \xrightarrow{\sim} H^2(\mathbb{Z}[\tfrac{1}{p}, \mu_{p^r}], \mathbb{Z}_p(2))^+$$

that are compatible with norms and corestriction, we may view $\varprojlim_r (\varpi_r \otimes_{\mathbb{Z}} \mathrm{id}_{\mathbb{Z}_p})$ as a map to $X_\infty(1)$ from the inverse limit of the groups $\mathcal{S}_2(p^r)/I\mathcal{S}_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ under the degeneracy maps induced by the identity on $\mathbb{H}$. We define $\varpi\colon \mathcal{S}/I\mathcal{S} \to Y$ to be the resulting map on ω^{2-k}-eigenspaces.

Remark 5.5.1. In our current setting, it makes no difference whether we work with the maps ϖ_{p^r} or $\varpi^\circ_{p^r}$, as

$$(\mathfrak{S}_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\mathrm{ord}} = (\mathfrak{S}^\circ_2(p^r) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\mathrm{ord}}.$$

In fact, repeated application of U_p to a cusp $\left\{\frac{a}{b}\right\}$ with p dividing b yields a formal sum of cusps with increasing power of p in the denominator, until that power reaches p^r, at which point each application multiplies the sum by p. Therefore, any such non-zero cusp must have trivial image in the ordinary part of the $\mathbb{Z}_p$-modular symbols.

The following conjecture can be viewed as a refinement of the main conjecture of Iwasawa theory (cf. [**Sha3**, Conjecture 4.12]).

Conjecture 5.5.2. *The maps $\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$ and $\varpi\colon \mathcal{S}/I\mathcal{S} \to Y$ are inverse to each other.*

Fukaya and Kato have proven strong results towards Conjecture 5.5.2, most importantly [**FuKa**, Theorem 7.2.3(1)]. Let $\xi' \in \Lambda$ be the power series in Λ that satisfies

$$\xi'(\upsilon^s - 1) = (1 - p^{-1})L'_p(\omega^k, s-1)$$

for all $s \in \mathbb{Z}_p$. As a power series in T, it equals $(T+1)\frac{d\xi}{dT}$.

Theorem 5.5.3 (Fukaya-Kato, Fukaya-Kato-S.). *The identity $\xi'\Upsilon \circ \varpi = \xi'$ holds on $\mathcal{S}/I\mathcal{S}$.*

Specifically, Fukaya and Kato proved that $\xi'\Upsilon \circ \varpi = \xi'$ on $\mathcal{S}/I\mathcal{S} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, but it since it was not at that time a priori clear that $\mathcal{S}/I\mathcal{S}$ has no p-torsion, this original result was ostensibly weaker. The result is strengthened to the above statement as a consequence of [**FKS2**]. In a recent preprint [**Oht4**], Ohta proves the following theorem, which shows that $\mathcal{S}/I\mathcal{S}$ indeed has no p-torsion.

THEOREM 5.5.4 (OHTA). *The map Υ is an isomorphism.*

When the tame level is not 1, certain characters are excluded from Ohta's result, but in our situation it has this simple form. Wake and Wang-Erickson had previously proven, using the theory of pseudo-deformations, that Υ is a pseudo-isomorphism under Greenberg's conjecture (without Ohta's condition on the character) and an isomorphism under Vandiver's conjecture [**WWE1, WWE2**]. In fact, what they show is that under Vandiver's conjecture is that the two Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ are Gorenstein, and under Greenberg's conjecture, they are weakly Gorenstein in a specific sense. In [**Sha3**, Proposition 4.10], it had been pointed out that if $\mathfrak{H}$ is Gorenstein, then Υ is an isomorphism.

COROLLARY 5.5.5. *If ξ and ξ' are relatively prime in Λ, then Conjecture 5.5.2 holds.*

PROOF. If ξ and ξ' are relatively prime, then in that (ξ) is its characteristic ideal, the Λ-module Y must be pseudo-cyclic. By the main conjecture and the fact that Y is p-torsion free by Proposition 2.3.21, there then exists an injective pseudo-isomorphism $Y \to \Lambda/(\xi)$. The map $\xi' \colon Y \to Y$ given by multiplication by ξ' is then injective, and since Υ is an isomorphism by Theorem 5.5.4, the map $\xi' \colon \mathcal{S}/I\mathcal{S} \to \mathcal{S}/I\mathcal{S}$ is injective as well. By Theorem 5.5.3, we then have that $\Upsilon \circ \varpi = 1$, so given that Υ is an isomorphism, the maps Υ and ϖ are inverse to each other. □

REMARK 5.5.6. If Greenberg conjecture fails, then ξ and ξ' necessarily have a common factor. If Greenberg's conjecture holds, then Y is pseudo-cyclic as a Λ-module, but it is possible that ξ has a square factor.

REMARK 5.5.7. If $X_\infty^{(1-k)}$ is merely supposed to be pseudo-cyclic, which is a consequence of Greenberg's conjecture, then we may conclude from the above theorems that ϖ is an isomorphism and $\Upsilon \circ \varpi$ and $\varpi \circ \Upsilon$ are multiplication by a unit in Λ that, modulo the annihilator of Y, is independent of all choices. The latter statement is actually the original form of the conjecture in [**Sha3**]: that is, the author strongly suspected at the time that the unit can be taken to be 1 (at least up to sign, with which the careful reader might realize we have been somewhat incautious in this write-up).

REMARK 5.5.8. There are no known cases where ξ and ξ' are not relatively prime, or even in which the λ-invariant of $X_\infty^{(1-k)}$ is greater than 1. (This was checked by Buhler and Harvey for primes $p < 39 \cdot 2^{22}$ in [**BuHa**].) It seems more than likely that ξ never has multiple factors, so Conjecture 5.5.2 in its stated form appears quite reasonable.

Let us very roughly indicate for the interested reader how the two derivatives ξ' appear in the theorem of Fukaya and Kato. On the left, ξ' arises from a rather fascinating computation which says that we have canonical isomorphisms

$$H^i_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \cong Y$$

for both $i = 1$ and $i = 2$, where S is the set consisting of the prime over p in $F = \mathbb{Q}(\mu_p)$. Moreover, the composition

$$Y \xrightarrow{\sim} H^1_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \to H^2_{\mathrm{Iw},S}(F_\infty, (\Lambda/(\xi))^\iota(2)) \xrightarrow{\sim} Y,$$

is ξ', where the second map is cup product with $(1-p^{-1})\log\chi_p \in H^1(G_{\mathbb{Q},S},\mathbb{Z}_p)$. Here, $\log$ denotes the p-adic logarithm defined by the usual power series (which is trivial on roots of unity).

On the right, Fukaya and Kato compute that the composition of a map formed from $z^\sharp$ with a certain p-adic regulator $H^1(G_{\mathbb{Q}_p},\mathcal{T}_{\mathrm{quo}}(1)) \xrightarrow{\sim} \mathfrak{S}$ is, upon reduction modulo I, multiplication by ξ'. (To get to the latter local cohomology group, one must first apply a map in Hochschild-Serre spectral sequence and then restrict.) Here, we use the fact that $\mathcal{S}/I\mathcal{S}$ and $\mathfrak{S}/I\mathfrak{S}$ are canonically isomorphic (given our choice of complex embedding). Though it is rather beyond the scope of these lectures, the point is that

$$L_p'(\omega^k, s-1) = \lim_{t\to 0} \zeta_p(t+1)(L_p(\omega^k, s+t-1) - L_p(\omega^k, s-1)),$$

where ζ_p is the p-adic Riemann-zeta function. The two-variable power series interpolating $\zeta_p(t+1)L_p(\omega^k, s+t-1)$ appears in a p-adic regulator computation on the value $z(\{0\to\infty\})$ of a map $z\colon \mathcal{M} \to H^1_{\mathrm{Iw},S}(F_\infty, \tilde{\mathcal{T}}(1))$ constructed using Beilinson-Kato elements on the curves $Y(p^r)$, and which descends to $(1-U_p)z^\sharp$ under corestriction maps, upon restriction to $\mathcal{S}$. The p-adic regulator of (or Coleman map applied to) $z(\{0\to\infty\})$ is a power series attached to a two-variable p-adic L-function valued in modular forms, and at $t=0$ it is a product of two Λ-adic Eisenstein series (one suitably diagonalized), the constant term of which is the above product of L-functions. The derivative appears in applying the Manin-Drinfeld splitting (which allows us to subtract off $\zeta_p(t+1)L_p(\omega^k, s-1)$) and in letting t tend to zero, which amounts to descending down the cyclotomic tower.

We end by describing an alternate form of Conjecture 5.5.2, which by Corollary 5.2.8 gives an analytic invariant (conjecturally) describing the structure of the second graded quotient in the augmentation filtration of the completely split Iwasawa module over the maximal p-ramified abelian pro-p extension of F_∞.

Definition 5.5.9. We define a map $\phi\colon \mathfrak{X}_\infty^- \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times/\langle -1\rangle]\!](1)$ by

$$\phi(\sigma) = \varprojlim_n \sum_{\substack{i=1\\ p\nmid j}}^{p^r-1} \chi_{i,n}(1-\zeta_{p^n}^i)[i]_n,$$

where $\chi_{i,n}\colon \mathfrak{X}_\infty \to \mu_{p^n}$ denotes the Kummer character attached to a p^nth root of $1-\zeta_{p^r}^i$ and $[i]_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times/\langle -1\rangle$ denotes the group element attached to i. Let $\Phi\colon \mathfrak{X}_\infty^-(-1) \to \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+$ be its twist by $\mathbb{Z}_p(-1)$.

Remark 5.5.10. The map ϕ has kernel isomorphic to the quotient of the Tate twist of the "Iwasawa adjoint" $\alpha(X_\infty^+)$, which is p-torsion free and pseudo-isomorphic to $(X_\infty^+)^\iota(1)$, and cokernel isomorphic to $(X_\infty^+[p^\infty])^\vee(1)$. In particular, it is an injective pseudo-isomorphism under Greenberg's conjecture at p and an isomorphism under Vandiver's conjecture at p.

Let $1-\zeta = (1-\zeta_{p^r})_r \in \mathcal{E}_\infty$. Let $\Psi_\infty\colon \mathcal{E}_\infty \to X_\infty^{(1-k)} \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^+$ denote the composition of the S-reciprocity map $\Psi_{K_\infty,S}$ with projection to the appropriate eigenspaces.

DEFINITION 5.5.11. We define the universal ordinary Mazur-Tate element (cf. [**MaTa**]) by

$$\mathcal{L} = \varprojlim_n \sum_{\substack{j=0 \\ p\nmid j}}^{p^r-1} U_p^{-r}[j:1]_r^\star \otimes [j]_r \in \mathcal{T}_{\mathfrak{m}}^+ \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+,$$

and we let $\overline{\mathcal{L}}$ denote its image in $\mathcal{S}/I\mathcal{S} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]^+$.

The universal ordinary Mazur-Tate element gives rise to (as written, the plus part of) the two-variable p-adic L-function of Mazur-Kitagawa by specialization at a Λ-adic (or A-adic for a Λ-algebra A) eigenform [**Kit**].

Note that $X_\infty^{(1-k)} \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^- \cong X_\infty^{(1-k)}(1) \otimes_{\mathbb{Z}_p} \mathfrak{X}_\infty^-(-1)$, so it makes sense to apply $\Upsilon \otimes \Phi$ to the former tensor product. We arrive at the following alternate form of Conjecture 5.5.2.

CONJECTURE 5.5.12. *We have* $(\Upsilon \otimes \Phi) \circ \Psi_\infty(1-\zeta) = \overline{\mathcal{L}}$.

APPENDIX A

Project descriptions

A.1. First project

Let N be a integer prime to an odd prime p. We consider the prime-to-p part Δ' of the group $\Delta = (\mathbb{Z}/Np\mathbb{Z})^\times/\langle -1\rangle$. Let $\theta\colon \Delta' \to \overline{\mathbb{Q}}_p^\times$ be a character. We consider $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ as a compact $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-module by allowing a group element j to acts as $\langle j\rangle^{-1}$. Let $F = \mathbb{Q}(\mu_{Np})$ and F_∞ be its cyclotomic $\mathbb{Z}_p$-extension, and note that $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_{p,N}^\times$. Set

$$Y = H^2_{\mathrm{Iw},S}(F_\infty, \mathbb{Z}_p(2))_\theta,$$

where S is the set of primes of F over p.

For a $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-module M, we may consider its θ-eigenspace for the group Δ':

$$M_\theta = M \otimes_{\mathbb{Z}_p[\Delta']} \mathcal{O}_\theta,$$

where $\mathcal{O}_\theta$ is the $\mathbb{Z}_p$-algebra generated by the image of θ. This is (noncanonically) a direct summand of M, and it is an $\mathcal{O}_\theta[\![T]\!]$-module.

Consider the Hecke algebra $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ for $\Lambda = \mathbb{Z}_p[\![T]\!]$, and define an Eisenstein ideal I to be generated by the images of $T_\ell - 1 - \ell\langle\ell\rangle$ for $\ell \nmid Np$ and $U_\ell - 1$ for $\ell \mid Np$. There is a unique maximal ideal $\mathfrak{m}$ of $\mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_\theta$ containing I. We still have the group

$$\mathcal{T} = \varprojlim_r H^1_{\text{ét}}(X_1(Np^r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))_{\mathfrak{m}},$$

which fits in an $\mathcal{O}_\theta[\![G_{\mathbb{Q}_p}]\!]$-exact sequence as in (4.3.2) with $D(\mathcal{T}_{\mathrm{quo}}) \cong \mathfrak{S} = S(N,\Lambda)_{\mathfrak{m}}$ and its Λ-dual $\mathcal{T}_{\mathrm{sub}}$ free of rank 1 over $\mathfrak{h} = \mathfrak{h}(N,\Lambda)^{\mathrm{ord}}_{\mathfrak{m}}$.

In **[Sha3]**, it is shown that if $p \geq 5$, $p \nmid \varphi(N)$, and the character θ is primitive, satisfies $\theta\omega^{-1}(p) \neq 1$ when considered as primitive Dirichlet character, then we can as before construct out of $\mathcal{T}$ a Λ-module homomorphism

$$\Upsilon\colon Y \to \mathcal{S}/I\mathcal{S}$$

that is conjectured to be an isomorphism, inverse to $\varpi = \varprojlim_r (\varpi_{Np^r})_\theta$. (Here, we consider the p-part of ϖ_{Np^r} as it was defined before, and we view it as a map to $H^2(G_{F_r,S}, \mathbb{Z}_p(2))^+$.) The conditions we placed on θ were sufficient to insure that the canonical map $X_\infty(1)_\theta \to Y$ is an isomorphism, where X_∞ is the unramified Iwasawa module.

The project:

(1) Remove the condition $p \nmid \varphi(N)$ from the construction of Υ.
(2) Construct Υ for as wide a class of θ as possible: note that $\mathcal{T}$ may not quite be the right object for this! It should be helpful to think of Υ as a connecting homomorphism **[Sha4]**.
(3) Formulate the analogous conjecture to Conjecture 5.5.2 in the θ-eigenspace.

A.2. Second project

Let K be an imaginary quadratic field, and fix $N \geq 4$. We consider the ray class field $K(N)$ of K. Let (E, P) be the canonical CM pair of modulus N over $K(N)$ in the sense of [**Kat**, (15.3.1)]. In particular, E has CM by $\mathcal{O}_K$ and $E(\mathbb{C}) \cong \mathbb{C}/N\mathcal{O}_K$ under an isomorphism taking P to 1. For a nontrivial integral ideal $\mathfrak{c}$ of $\mathcal{O}_F$ prime to $6N$, we have a θ-function ${}_{\mathfrak{c}}\theta_E$. (If $\mathfrak{c} = (c)$ for some $c > 1$, then this is simply the pullback from the universal elliptic curve of the θ-function ${}_c\theta$ of Definition 3.2.6.) For a nonzero $u \in \mathbb{Z}/N\mathbb{Z}$, we obtain an elliptic N-unit ${}_{\mathfrak{c}}\Theta_N(u) = {}_{\mathfrak{c}}\theta_E(uP)^{-1} \in \mathcal{O}_{K(N)}[\frac{1}{N}]^\times$, which is in fact a unit unless $N\mathcal{O}_K$ is a prime power. For the Galois element $\sigma_{\mathfrak{c}} \in G_K^{\mathrm{ab}}$ corresponding to $\mathfrak{c}$ by class field theory, the element

$$\Theta_N(u) = {}_{\mathfrak{c}}\Theta_N(u) \otimes (N(\mathfrak{c}) - \sigma_{\mathfrak{c}})^{-1} \in \mathcal{O}_{K(N)}[\tfrac{1}{N}]^\times \otimes_{\mathbb{Z}} \mathcal{Q},$$

where $\mathcal{Q}$ is the total quotient ring of $\mathbb{Z}_p[\mathrm{Gal}(K(N)/K)]$, is independent of $\mathfrak{c}$. If one ignores this issue of integrality, one could ask if there exists a well-defined map

$$\Pi_N^\circ \colon H_1(X_1(N), C_1^\circ(N), \mathbb{Z}_p) \to K_2(\mathcal{O}_{K(N)}[\tfrac{1}{N}]) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \qquad [u : v]_N^\star \mapsto \{\Theta_N(u), \Theta_N(v)\}_N,$$

where we use a slightly different notation for symbols here by not projecting to "plus parts". Note that the K_2-group is finite, which creates an apparent issue given the denominators used in the definition of the $\Theta_N(u)$.

The project:

(1) Show that Π_N° is a well-defined map under assumptions on the level or to certain eigenspaces for the action of Galois. (Here, it may be best to look at elliptic units arising as specializations of Siegel units on $Y_1(N)$, assuming the Heegner hypothesis on N.)
(2) Determine whether the restriction of Π_N° to $H_1(X_1(N), \mathbb{Z}_p)$ takes image in cohomology of $G_{K(N),S_p}$, for S_p the set of primes over p.
(3) Show that Π_N arises as specialization of the map $z_N^\sharp$ of Fukaya-Kato at the CM point (E, P). Determine whether this specialization factors through the quotient of homology by a certain CM ideal I_N, producing a map ϖ_N.
(4) Can there be an equivariance of ϖ_N for diamond operators and Galois elements, and if so, what is it? Determine whether or not this map should be expected to be surjective (or injective).
(5) What difference does the ramification behavior of p in K make? Perform computations in examples.

The methods of [**FKS2**] could be helpful in the first part. The passage to an inverse limit over increasing p-power in the levels, as in [**FuKa**], could also be helpful in avoiding issues of torsion. For the last part, we note that a more natural map might arise by replacing the homology of $X_1(N)$ with the (first relative) homology of the Bianchi space of level N, which for Euclidean fields has nice Manin-type generators and relations, with the generator indexed by pairs of relatively prime elements of $\mathcal{O}_F/N$, as proven by Cremona [**Cre**]. (This could also be investigated.) In comparison, the map above only uses a limited set of pairs of elliptic N-units.

A.3. Third project

This project has as its goal the exploration of the relationship between Massey products of units of cyclotomic fields and the Iwasawa theory of Kummer extensions (see [**Sha2**]). There are numerous possibilities here. First, let us recall the definition of Massey products.

For a profinite group G and a commutative ring R, a defining system for an n-fold Massey product $(\chi_1, \dots, \chi_n)$ of n continuous homomorphisms $\chi_i \colon G \to R$ is a homomorphism $\rho \colon G \to N_{n+1}/Z_{n+1}$, where N_{n+1} denotes the group of upper-triangular unipotent matrices in $\mathrm{GL}_{n+1}(R)$ and Z_{n+1} denotes the subgroup of matrices which are zero above the diagonal aside from the $(1, n+1)$-entry, such that the character $\rho_{i,i+1}$ given by the $(i, i+1)$-entry of ρ is χ_i for $1 \leq i \leq n$. Given such a defining system, the Massey product $(\chi_1, \dots, \chi_n)$ is taken to be the class of the 2-cocycle

$$\kappa_{1,n}(\sigma, \tau) \mapsto \sum_{i=2}^{n} \rho_{1,i}(\sigma)\rho_{n+2-i,n+1}(\tau).$$

The Massey product is therefore only defined if there exists such a defining system, and if so, its value depends upon the choice of defining system. Thus, it may be viewed as an element of a quotient of $H^2(G, R)$. Note that we may also extend the definition to R-coefficients upon which G acts by a character to $R^\times$ by placing products of the characters along the diagonal and requiring that the resulting map to the upper-triangular Borel be a homomorphism.

Now, let us focus for the moment on Massey triple products (a_1, a_2, a_3) of elements of $\mathcal{E}_{F,S}$ for a number field F containing μ_p and S a set of primes containing those dividing p. (We omit subscripts for simplicity of notation.) Taken with $\mathbb{Z}_p(1)$-coefficients, such a Massey product will exist if and only if $(a_1, a_2) = (a_2, a_3) = 0$, in which case it will have image in the quotient of $H^2(G_{F,S}, \mathbb{Z}_p(3))$ by all cup products of the form (a_1, c) and (c, a_3) where $c \in H^1(G_{F,S}, \mathbb{Z}_p(2))$.

The project:

(1) By definition, the Massey product (a_1, a_2, a_3) provides an obstruction to the existence of a certain p-ramified extension. Under what circumstance does the vanishing of such products correspond to the existence of a (different) unramified extension of a p-extension of F in the sense of Corollary 5.1.20 (for $F = \mathbb{Q}(\mu_p)$)? What about higher Massey products? Study the implications for the structure of unramified Iwasawa modules.

(2) Consider Massey products of the form $(\chi_p, \dots, \chi_p, a_1, \dots, a_n)$ as elements of quotients of $H^2(G_{F,S}, \mathbb{Z}_p(n))$, where $\chi_p \in H^1(G_{F,S}, \mathbb{Z}_p)$ is the cyclotomic character. What are these measuring? (For $n = 1$, one might compare with [**McSh**, Section 4] for $F = \mathbb{Q}(\mu_p)$ and μ_p-coefficients.)

(3) In Iwasawa theory (taking $F = \mathbb{Q}(\mu_p)$), we have a duality between $\mathfrak{X}_\infty^+$ and X_∞^- (see, e.g., (2.3.18)). Do we have related duality for the second graded quotient of an unramified Iwasawa module of a Kummer extension that is controlled by cup products with a Kummer generator? What about for higher Massey products? The paper [**LiSh**] might be a good reference for duality.

For an extra fun challenge, see if n-fold Massey products of cyclotomic units can be interpreted in terms of some variant of modular symbols for GL_n. (This can be discussed if we come to it.)

A.4. Fourth project

The goal of this project is to formulate a higher weight version of Conjecture 5.5.2 at level one (or tame level), relating Steinberg symbols of Soulé (or cyclotomic) elements in higher K-groups and higher weight modular symbols. Set $\mathbb{Z}' = \mathbb{Z}[\frac{1}{2}]$, as before.

The project:

(1) For even $k \geq 2$, construct a map

$$\Pi_k \colon \mathcal{S}_k(1, \mathbb{Z}') \to K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}'$$

the projection of which to $K_{2k-2}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ takes $X^{i-1}Y^{k-i-1}\{0 \to \infty\}$ for $3 \leq i \leq k-3$ and odd i to a Steinberg symbol $\{\kappa_i, \kappa_{k-i}\}$ of elements $\kappa_j \in K_{2j-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for odd j that are constructed out of cyclotomic p-units, known as Soulé elements [**Sou**].

(2) Determine whether an alternate construction of Π_k can be made without reference to individual primes.

(3) Show that Π_k factors through the quotient of $\mathcal{S}_k(1, \mathbb{Z}')$ by an Eisenstein ideal I_k generated by $T_\ell - 1 - \ell^{k-1}$ for all primes ℓ, inducing a map ϖ_k.

(4) Construct a map $\Upsilon_k \colon K_{2k-2}(\mathbb{Z}) \otimes \mathbb{Z}' \to \mathcal{S}_k(1, \mathbb{Z}')/I_k\mathcal{S}_k(1, \mathbb{Z}')$ out of the Galois action on the higher weight p-adic étale cohomology groups of a modular curve.

(5) Show that $\xi_k' \Upsilon_k \circ \varpi_k = \xi_k'$ for a particular number ξ_k'.

(6) Compare the above with the Λ-adic weight 2 constructions in the notes.

(7) Repeat the previous steps allowing an arbitrary tame level N.

Bibliography

[BuHa] J. P. Buhler, D. Harvey, Irregular primes up to 163 million, *Math. Comp.* **80** (2011), 2435–2444.

[Bus] C. Busuioc, The Steinberg symbol and special values of L-functions, *Trans. Amer. Math. Soc.* **360** (2008), 5999–6015.

[CoLi] J. Coates, S. Lichtenbaum, On ℓ-adic zeta functions, *Ann. of Math* **98** (1973), 498–550.

[Col1] R. Coleman, Division values in local fields, *Invent. Math.* **53** (1979), 91–116.

[Col2] R. Coleman, Local units modulo cyclotomic units, *Proc. Amer. Math. Soc.* **89** (1983), 1–7.

[Con] B. Conrad, Arithmetic moduli of generalized elliptic curves, *J. Inst. Math. Jussieu* **6** (2007), 209–278.

[Cre] J. Cremona, Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields, *Compos. Math.* **51** (1984), 275–324.

[Del] P. Deligne, Formes modulaires et représentations l-adiques, *Séminaire Bourbaki*, Exp. 355, *Lecture Notes in Math.* **175**, Springer, Berlin, 1971, 139–172.

[DeRa] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), *Lecture Notes in Math.* **349**, Springer, Berlin, 1973, 143–316.

[DiSh] F. Diamond, J. Shurman, A first course in modular forms, *Grad. Texts in Math.* **228**, Springer, New York, 2005.

[Dri] V. Drinfeld, Two theorems on modular curves, *Funkcional. Anal. i Priložen* **7** (1973), 83–84.

[Eme] M. Emerton, The Eisenstein ideal in Hida's ordinary Hecke algebra. *Int. Math. Res. Not. IMRN* **1999** (1999), 793–802.

[FeGr] B. Ferrero, R. Greenberg, On the behavior of p-adic L-functions at s=0. *Invent. Math.* **50** (1978/79), 91–102.

[FeWa] B. Ferrero, L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.

[FuKa] T. Fukaya, K. Kato, On conjectures of Sharifi, preprint, version August 15, 2012.

[FKS1] T. Fukaya, K. Kato, R. Sharifi, Modular symbols in Iwasawa theory, In: Iwasawa Theory 2012 - State of the Art and Recent Advances, *Contrib. Math. Comput. Sci.* **7**, Springer, 2014, 177–219.

[FKS2] T. Fukaya, K. Kato, R. Sharifi, Modular symbols and the integrality of zeta elements, *Ann. Math. Qué.* **40** (2016), 377–395.

[Gre1] R. Greenberg, On p-adic L-functions and cyclotomic fields, *Nagoya Math. J.* **56** (1974), 61–77.

[Gre2] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.

[HaPi] G. Harder, R. Pink, Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbf{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen, *Math. Nachr.* **159** (1992), 83–99.

[Hid1] H. Hida, On congruence divisors of cusp forms as factors of the special values of their zeta functions, *Invent. Math.* **64** (1981), 221–262.

[Hid2] H. Hida, Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup.* **19** (1986), 231–273.

[Hid3] H. Hida, Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[\![X]\!])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986), 545–613.

[Hid4] H. Hida, Elementary theory of L-functions and Eisenstein series, London Math. Soc. Stud. Texts **26**, Cambridge Univ. Press, Cambridge, 1993.

[Her] J. Herbrand, Sur les classes des corps circulaires, *J. Math. Pures Appl.* (9) **11** (1932), 417–441.

[Iwa1] K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.

[Iwa2] K. Iwasawa, On the theory of cyclotomic fields, *Ann. of Math.* **70** (1959), 530–561.

[Iwa3] K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964), 42–82.

[Iwa4] K. Iwasawa, Analogies between number fields and function fields, Some Recent Advances in the Basic Sciences, Vol. 2 (Proc. Annual Sci. Conf., Belfer Grad. School Sci., Yeshiva Univ., New York, 1965-1966), Belfer Graduate School of Science, Yeshiva Univ., New York, 203–208.

[Iwa5] K. Iwasawa, On p-adic L-functions, *Ann. of Math.* **89** (1969), 198–205.

[Kat] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, In: Cohomologies p-adiques et applications arithmétiques, III, *Astérisque* **295** (2004), 117–290.

[KaMa] N. Katz, B. Mazur, Arithmetic moduli of elliptic curves. *Ann. of Math. Stud.* **108**, Princeton Univ. Press, Princeton, NJ, 1985.

[Kit] K. Kitagawa, On standard p-adic L-functions of families of elliptic cusp forms, In: p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), *Contemp. Math.* **65**, Amer. Math. Soc., Providence, RI, 1994, 81–110.

[KuLe] T. Kubota, H. Leopoldt, Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.* **214/215** (1964), 328–339.

[Kur] M. Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1. *J. Number Theory* **45** (1993), 281–294.

[Lan] S. Lang, Introduction to modular forms, Grundlehren math. Wiss. **222**, Springer, Berlin-New York, 1976.

[Leo] H. Leopoldt, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, *J. Reine Angew. Math.* **199** (1958), 165–174.

[LiSh] M. Lim, R. Sharifi, Nekovář duality in p-adic Lie extensions of global fields, *Doc. Math.* **18** (2013), 621–678.

[Man1] Y. Manin, Parabolic points and zeta functions of modular curves, *Izv. Ross. Akad. Nauk Ser. Mat.* **36** (1972), 19–66.

[Man2] Y. Manin, Periods of cusp forms, and p-adic Hecke series. *Mat. Sb.* **92(134)** (1973), 378–401, 503.

[MaTa] B. Mazur, J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* **54** (1987), 711–750.

[MaWi1] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.

[MaWi2] B. Mazur, A. Wiles, On p-adic analytic families of Galois representations, *Compos. Math.* **59** (1986), 231–264.

[McSh] W. McCallum, R. Sharifi, A cup product in the Galois cohomology of number fields. *Duke Math. J.* **120** (2003), 269–310.

[Mer] L. Merel, Universal Fourier expansions of modular forms, *On Artin's conjecture for odd 2-dimensional representations*, *Lecture Notes in Math.* **1585**, Springer, Berlin, 1994, 59–94.

[Mil] J. Milnor, Introduction to algebraic K-theory, *Ann. of Math. Stud.* **72**, Princeton Univ. Press, Princeton, NJ, 1971.

[NSW] J. Neurkirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Second Edition, *Grundlehren Math. Wiss.* **323**, Springer-Verlag, Berlin, 2008.

[Oht1] M. Ohta, On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms, *J. reine angew. Math.* **463** (1995), 49–98.

[Oht2] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II, *Math. Ann.* **318** (2000), 557–583.

[Oht3] M. Ohta, Congruence modules related to Eisenstein series, *Ann. Éc. Norm. Sup.* **36** (2003), 225–269.

[Oht4] M. Ohta, μ-type subgroups of $J_1(N)$ and application to cyclotomic fields, preprint, 84 pages.

[Rib] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[Rub] K. Rubin, Appendix to: S. Lang, Cyclotomic fields I and II, Combined second edition, *Grad. Texts in Math.* **121**, Springer-Verlag, New York, 1990, 397–419.

[Ser] J-P. Serre, Classes des corps cyclotomiques (d'après K. Iwasawa), *Séminaire Bourbaki*, Exp. 174, Soc. Math. France, Paris, 1959, 83–93.

[Sha1] R. Sharifi, Massey products and ideal class groups, *J. Reine Angew. Math.* **603** (2007), 1–33.

[Sha2] R. Sharifi, Iwasawa theory and the Eisenstein ideal, *Duke Math. J.* **137** (2007), 63–101.

[Sha3] R. Sharifi, A reciprocity map and the two variable p-adic L-function, *Ann. of Math.* **173** (2011), 251–300.

[Sha4] R. Sharifi, Reciprocity maps with restricted ramification, preprint, arXiv:1609.03616.

[Sha5] R. Sharifi, Iwasawa theory, unpublished lecture notes, http://math.ucla.edu/∼sharifi/iwasawa.pdf.

[Shi1] G. Shimura, Sur les intégrales attachées aux formes automorphes, *J. Math. Soc. Japan* **11** (1959), 291–311.

[Shi2] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Princeton Univ. Press, Princeton, NJ, 1994.

[Sho1] V. Shokurov, A study of the homology of Kuga varieties, *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 443–464, 480.

[Sho2] V. Shokurov, Shimura integrals of cusp forms, *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 670–718, 720.

[Sou] C. Soulé, On higher p-adic regulators, Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), *Lecture Notes in Math.* **854**, Springer, Berlin-New York, 1981, 372–401.

[Sti] L. Stickelberger, Uber eine Verallgemeinerung der Kreistheilung, *Math. Ann.* **37** (1890), 321–367.

[Tat] J. Tate, Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257–274.

[Til] J. Tilouine, Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke, *Bull. Soc. Math. France* **115** (1987), 329–360.

[Was] L. Washington, Introduction to cyclotomic fields, 2nd Ed. *Grad. Texts in Math.* **83**, Springer, New York, 1997.

[Wak] P. Wake, Eisenstein Hecke algebras and conjectures in Iwasawa theory, *Algebra Number Theory* **9** (2015), 53–75.

[WWE1] P. Wake, C. Wang-Erickson, Pseudo-modularity and Iwasawa theory, to appear in *Amer. J. Math.* arXiv:1505.05128.

[WWE2] P. Wake, C. Wang-Erickson, Ordinary pseudorepresentations and modular forms, to appear in *Proc. Amer. Math. Soc.*, arXiv:1510.01661.

[Wei] C. Weibel, The K-book. An introduction to algebraic K-theory, *Grad. Stud. Math.* **145**, Amer. Math. Soc., Providence, RI, 2013.

[Wil1] A. Wiles, On ordinary λ-adic representations associated to modular forms, *Invent. Math.* **94** (1988), 529–573.

[Wil2] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540.

COURSE OUTLINE: IWASAWA THEORY OF ELLIPTIC CURVES ARIZONA WINTERS SCHOOL 2017

CHRISTOPHER SKINNER

1. Course Outline

Iwasawa theory was introduced around 1960 in the context of class groups of cyclotomic and other $\mathbb{Z}_p$-extensions of number fields. The 'main conjecture' of Iwasawa theory proposed a remarkable connection between the p-adic L-functions of Kubota and Leopoldt and these class groups, including among its consequences certain refined class number formulas for values of Dirichlet L-functions. This main conjecture was proved by Mazur and Wiles in the early 1980s.

Beginning with work of Mazur and Swinnerton-Dyer in the 1970s and especially in subsequent papers of Greenberg, the ideas of Iwasawa theory were extended to elliptic curves and – having been suitably recast in the language of Selmer groups – other p-adic Galois representations. Each instance has it's own 'main conjecture' (at least conjecturally!) relating certain Galois cohomology groups (the algebraic side) with p-adic L-functions (the analytic side).

The aim of this course will be to describe the Iwasawa theory of elliptic curves and – possibly – modular forms, state the associated main conjectures, and report on some of the progress that has been made on proving these conjectures and especially some of the arithmetic consequences. A rough outline of the course:

- Selmer groups of elliptic curves
- Main Conjectures
- recent results (and their proofs)
- arithmetic applications (to BSD, etc.)

2. Projects

Possible projects include:

1. *Missing cases of the main conjecture for elliptic curves.*
2. *Relating different main conjectures.*
3. *The structure of Selmer groups.*

LECTURES ON THE IWASAWA THEORY OF ELLIPTIC CURVES

CHRISTOPHER SKINNER

Abstract. These are a preliminary set ot notes for the author's lectures for the 2018 Arizona Winter School on Iwasawa Theory.

Contents

1. Introduction

Iwasawa theory was introduced around 1960 in the context of class groups of cyclotomic and other $\mathbb{Z}_p$-extensions of number fields. The Main Conjecture of Iwasawa theory proposed a remarkable connection between the p-adic L-functions of Kubota and Leopoldt and these class groups [19, §1], [12, §5], including among its consequences certain refined class number formulas for values of Dirichlet L-functions. This Main Conjecture was proved by Mazur and Wiles [47] in the early 1980's.

Beginning with work of Mazur and Swinnerton-Dyer [45] in the 1970's and especially in subsequent papers of Greenberg [20] [21] [22], the ideas of Iwasawa theory were extended to elliptic curves and – having been suitably recast in the language of Selmer groups – other p-adic Galois representations. Each instance has its own Main Conjecture (at least conjecturally!) relating certain Galois cohomology groups (the algebraic side) with p-adic L-functions (the analytic side). And like the original Main Conjecture of Iwasawa, these Main Conjectures have consequences for the (expected) related special value formulas. In the case of an elliptic curve E this can include the p-part of the Birch–Swinnerton-Dyer formula when the analytic rank is at most one.

The aim of these lectures is to describe the Iwasawa theory of elliptic curves, stating the associated Main Conjectures and reporting on some of the progress that has been made toward proving these conjectures and especially some of the arithmetic consequences.

Prerequisites. These notes are prepared with the expectation that the reader will have a solid background in algebraic number theory and be comfortable with Galois cohomology and Tate's duality theorems ([49, I] is a good reference for the latter). These notes focus on the case of elliptic curves, but this course was chosen with the expectation that the reader will be more comfortable with this case than with that of a general eigenform and because this is probably the case of most interest (and it also simplifies some notation). While very little specific to elliptic curves is used, it could also be helpful to have a familiarity with their basic arithmetic ([61] would be more than sufficient).

Additional readings for details. Those seeking more details should be able to easily find some in the literature. In particular, in addition to the earlier cited papers of Greenberg, [23], [24], and [25] contain a wealth of foundational material (and many examples). Kato's paper [33] is an introduction to the circle of ideas carried out in [34] for elliptic curves and modular forms, while [59], [60], and [14] help illuminate aspects of [34]. However, for details of the proofs of many of the more recent results (such as [64]) the best current resources may be the original papers themselves.

Some notational preliminaries. We let $\overline{\mathbb{Q}}$ be a fixed separable algebraic closure of $\mathbb{Q}$. Given a subfield $F \subset \overline{\mathbb{Q}}$ we let $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. For a set Σ of places of F, we write $G_{F,\Sigma}$ for the Galois group $\mathrm{Gal}(F_\Sigma/F)$ of the maximal extension $F_\Sigma \subset \overline{\mathbb{Q}}$ of F that is unramified outside Σ. If $F = \mathbb{Q}$ then we may drop the subscript '$\mathbb{Q}$' from our notation (writing G_Σ for $G_{\mathbb{Q},\Sigma}$). For a place v of F we let $\overline{F}_v$ be a separable algebraic closure of the completion F_v and let $G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v)$. We let $I_v \subset G_{F_v}$ be the inertia subgroup and, when the residue field of F_v is finite, $\mathrm{Frob}_v \in G_{F_v}/I_v$ an arithmetic Frobenius. Generally, we will assume that we have chosen an F-embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{F}_v$, which identifies G_{F_v} as a subgroup of G_F.

We fix conventions for the reciprocity laws of class field theory as follows: For a number field F and a place v of F we let $\mathrm{rec}_{F_v} : F_v^\times \to G_{F_v}^{ab}$ be the reciprocity map of local class field theory, normalized so that uniformizers map to lifts of the arithmetic Frobenius. Similarly, we let $\mathrm{rec}_F : F^\times \backslash \mathbb{A}_F^\times \to G_F^{ab}$ be the reciprocity map of global class field theory, normalized so that $\mathrm{rec}_F|_{F_v^\times} = \mathrm{rec}_{F_v}$.

Throughout, p is a prime number (usually assumed > 2). We let $\epsilon : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character.

At times it will be useful to view elements of $\overline{\mathbb{Q}}$ as both complex numbers and p-adic numbers. To this end we fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ which will be tacitly in use in all that follows.

Finally, one last bit of general notation about modules: Suppose M is a module for a ring R. If $\phi : M \to M$ is an R-linear endomorphism of M, then we write $M[\phi]$ to mean the kernel of ϕ. A commonly used variation of this will be to write $M[r]$ for $M[\phi]$ when ϕ is just the multiplication by r map.

Acknowledgments. It is a pleasure to thank all those who provided feedback and corrections to these notes, particulary Francesc Castella – who carefully read earlier drafts – as well as Kim Tuan Do. The author's work has been supported by grants from the National Science Foundation and a Simons Investigator grant.

2. Selmer groups

We begin by recalling the usual Selmer groups of an elliptic curve as well as some generalizations.

2.1. Selmer groups of elliptic curves.

Let E be an elliptic curve over a number field F.

2.1.1. *The Weak Mordell–Weil Theorem.* One of the fundamental results about the arithmetic of E is the celebrated theorem of Mordell and Weil:

$$E(F) \text{ is a finitely-generated abelian group.}$$

An important step in the proof of this theorem is the Weak Mordell–Weil Theorem: for any positive integer $m \geq 2$, $E(F)/mE(F)$ is a finite group. This yields the Mordell–Weil Theorem when combined with the theory of heights on elliptic curves, especially Tate's canonical height.

The Weak Mordell–Weil Theorem is generally proved by realizing $E(F)/mE(F)$ as a subgroup of another group that is more readily recognized as having finite order. This makes use of the Kummer map for elliptic curves. Let $P \in E(F)$ be a point and let $Q \in E(\overline{F})$ be a point such that $mQ = P$. The map $\phi_Q : G_F \to E[m]$, $\sigma \mapsto \sigma(Q) - Q$, is a 1-cocycle. Let $c_P = [\phi_Q]$ be

the class of ϕ_Q in the Galois cohomology group $H^1(F, E[m])$. If Q' is another point such that $mQ' = P$, then the difference $\phi_Q - \phi_{Q'}$ is a coboundary, so c_P depends only on P. The map $E(F) \to H^1(F, E[m])$, $P \mapsto c_P$, is clearly a homomorphism. A point $P \in E(F)$ is in the kernel of this homomorphism if and only if c_P is a coboundary, that is, if and only if there exists $R \in E[m]$ such that $\sigma(Q) - Q = \sigma(R) - R$ for all $\sigma \in G_F$. But this is so if and only if $\sigma(Q - R) = Q - R$ for all $\sigma \in G_F$, and so if and only if $Q - R \in E(F)$. But then $P = m(Q - R) \in mE(F)$. This shows that there is in fact an injection

$$E(F)/mE(F) \overset{\kappa}{\hookrightarrow} H^1(F, E[m]), \quad \kappa(P) = c_P.$$

The map κ is the Kummer map for the multiplication by m endomorphism of E. It is just the boundary map in the long exact Galois cohomology sequence associated with the short exact sequence $0 \to E[m] \to E \overset{m}{\to} E \to 0$. However, we have not yet achieved what we wanted: the group $H^1(F, E[m])$ is infinite. We seem to have gone in the wrong direction! To finish the proof of the Weak Mordell–Weil Theorem one makes a closer analysis of the image of κ.

Let v be a finite place of F not dividing m and such that E has good reduction at v. This only excludes a finite subset Σ of all the places of F. Let k_v be the residue field of v and let ℓ be the characteristic of k_v. Let $\overline{E}$ be the reduction of E modulo v; this is an elliptic curve over k_v. As $\ell \nmid m$, the reduction map is an isomorphism on m-torsion: $E[m] \overset{\sim}{\to} \overline{E}[m]$. Let $\sigma \in I_v$. Then σ acts trivially on $\overline{E}$ and so $\sigma(Q)$ and Q have the same image in $\overline{E}$. In particular, $\sigma(Q) - Q$ reduces to the origin in $\overline{E}$. But $\sigma(Q) - Q \in E[m]$ and so it follows from the injectivity of the reduction map on $E[m]$ that $\sigma(Q) - Q = 0$. In particular, the restriction of c_Q to the inertia group I_v is a coboundary. This means that the image of κ is contained in

$$\ker \left\{ H^1(F, E[m]) \overset{res}{\to} \prod_{v \notin \Sigma} H^1(I_v, E[m]) \right\},$$

the kernel of the product of the restriction maps to the inertia subgroups of all the places v not in the finite set Σ. Another way of writing this kernel is $H^1(G_{F,\Sigma}, E[m])$. So we have

$$E(F)/mE(F) \overset{\kappa}{\hookrightarrow} H^1(G_{F,\Sigma}, E[m]), \quad \kappa(P) = c_P.$$

This is better: the group $H^1(G_{F,\Sigma}, E[m])$ is finite (and hence $E(F)/mE(F)$ is also finite). The finiteness of $H^1(G_{F,\Sigma}, E[m])$ can be seen as follows. Let $L = F(E[m]) \subset F_\Sigma$ be the finite Galois extension of F obtained by adjoining the coordinates of points in $E[m]$. The inflation restriction sequence gives a left-exact sequence

$$0 \to H^1(\mathrm{Gal}(L/F), E[m]^{G_L}) \to H^1(G_{F,\Sigma}, E[m]) \overset{res}{\to} H^1(\mathrm{Gal}(F_\Sigma/L), E[m]).$$

The group $H^1(\mathrm{Gal}(L/F), E[m]^{G_L})$ is clearly finite (as both $\mathrm{Gal}(L/F)$ and $E[m]$ are finite groups). Since $\mathrm{Gal}(F_\Sigma/L)$ acts trivially on $E[m]$, $H^1(\mathrm{Gal}(F_\Sigma/L), E[m]) = \mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$. Any element of $\mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$ factors through the Galois group over L of the maximal abelian extension of L of exponent m that is unramified outside the finitely many places of L dividing a place in Σ. This extension is finite, and hence so is $\mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$. We have sandwiched $H^1(G_{F,\Sigma}, E[m])$ between two finite groups.

By realizing $E(F)/mE(F)$ as a subgroup of $H^1(G_{F,\Sigma}, E[m])$ we reduced its finiteness to the ostensibly easier problem of the finiteness of certain extensions of number fields. This demonstrates one utility of cohomology groups.

2.1.2. *The Selmer group for multiplication by m.* The Selmer group for the multiplication by m map on E refines the inclusion $E(F)/mE(F) \hookrightarrow H^1(G_{F,\Sigma}, E[m])$. It is essentially the smallest subgroup of $H^1(F, E[m])$ containing the image of $E(F)/mE(F)$ that can be defined by more-or-less obvious local constraints ('local conditions') on the cohomology classes.

The Kummer map $P \overset{\kappa}{\mapsto} c_P$ that we recalled earlier makes sense for E over any field and in particular over the completion F_v of F at a place of F.

For each place v of F the inclusion of F in the completion F_v induces a commutative diagram

$$\begin{array}{ccc} E(F)/mE(F) & \xrightarrow{\kappa} & H^1(F, E[m]) \\ \downarrow & & \downarrow res \\ E(F_v)/mE(F_v) & \xrightarrow{\kappa_v} & H^1(F_v, E[m]), \end{array}$$

where κ_v is just the Kummer map for E over F_v. The Selmer group $\mathrm{Sel}_m(E/F)$ for the multiplication by m on E is

$$\mathrm{Sel}_m(E/F) = \left\{ c \in H^1(F, E[m]) \ : \ res_v(c) \in \mathrm{im}(\kappa_v) \ \forall v \right\}.$$

This clearly contains the image of κ. Furthermore, by the argument explained above, if v does not divide m and E has good reduction at v then $\mathrm{im}(\kappa_v) \subset \ker\left\{ H^1(F_v, E[m]) \overset{res}{\to} H^1(I_v, E[m]) \right\}$. In particular, $\mathrm{Sel}_m(E/F) \subseteq H^1(G_{F,\Sigma}, E[m])$.

The maps κ and κ_v are part of short exact sequences

$$0 \to E(F)/mE(F) \overset{\kappa}{\to} H^1(F, E[m]) \to H^1(F, E)[m] \to 0$$

and

$$0 \to E(F_v)/mE(F_v) \overset{\kappa_v}{\to} H^1(F_v, E[m]) \to H^1(F_v, E)[m] \to 0$$

that come from the long exact Galois cohomology sequences associated with the short exact sequence $0 \to E[m] \to E \overset{m}{\to} E \to 0$. In particular, we can rewrite the definition of $\mathrm{Sel}_m(E/F)$ as

$$\mathrm{Sel}_m(E/F) = \ker\left\{ H^1(F, E[m]) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}.$$

And we see that the image of κ is just $\ker\left\{ \mathrm{Sel}_m(E/F) \to H^1(F, E) \right\}$. In particular, there is a fundamental exact sequence

$$0 \to E(F)/mE(F) \overset{\kappa}{\to} \mathrm{Sel}_m(E/F) \to Ш(E/F)[m] \to 0,$$

where

$$Ш(E/F) = \ker\left\{ H^1(F, E) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}$$

is the Tate-Shafarevich group of E over F.

If $m \mid m'$ then the inclusion $E[m] \subset E[m']$ induces a surjection $H^1(F, E[m]) \twoheadrightarrow H^1(F, E[m'])[m]$ and so a surjection $\mathrm{Sel}_m(E/F) \to \mathrm{Sel}_{m'}(E/F)[m]$. The kernel is just $E[\frac{m'}{m}](F)/mE[m'](F)$. If F'/F is a finite extension, then the restriction map $H^1(F, E[m]) \to H^1(F', E[m])$ induces a homomorphism $\mathrm{Sel}_m(E/F) \to \mathrm{Sel}_m(E/F')$. Furthermore, if F'/F is a Galois extension, then the action of $\mathrm{Gal}(F'/F)$ on $H^1(F', E[m])$ defines an action on $\mathrm{Sel}_m(E/F')$, and the maximal $\mathrm{Gal}(F'/F)$-fixed subgroup contains the image of $\mathrm{Sel}_m(E/F)$.

Remark 2.1.2.a. Suppose that $m = p$. It is expected that $Ш(E/F)[p^\infty]$ is finite, in which case it is known that $Ш(E/F)[p]$ has even dimension as a vector space over $\mathbb{F}_p$. It then follows from the fundamental exact sequence that

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) \equiv \dim_{\mathbb{F}_p} E(F)/pE(F) \bmod 2.$$

In particular, if $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) = 1$, then is expected that $\dim_{\mathbb{F}_p} E(F)/pE(F) = 1$. If $\dim_{F_p} E(F)/pE(F) = 1$ but $E[p](F) = 0$, then $\mathrm{rank}_{\mathbb{Z}} E(F) = 1$. This suggests

$$(\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) = 1 \text{ and } E[p](F) = 0) \overset{?}{\Longrightarrow} \mathrm{rank}_{\mathbb{Z}} E(F) = 1.$$

2.1.3. *Vista: Selmer groups of Abelian varieties and their isogenies.* The group $\mathrm{Sel}_m(E/F)$ is a special case of a definition that can be made for any non-zero isogeny

$$A \overset{\phi}{\to} B$$

of abelian varieties over F. The natural generalization of the Kummer map yields an injection $A(F)/\phi(B(F)) \hookrightarrow H^1(F, A[\phi])$, which leads to the definition of a Selmer group $\mathrm{Sel}_\phi(A/F) \subset H^1(G_{F,\Sigma}, A[\phi])$ (for Σ containing all places that divide $\#A[\phi]$ and at which A – and so also B – has bad reduction). These Selmer groups play an equally important role in our understanding of the arithmetic of the abelian varieties A and B.

Elliptic curves can have isogenies that are not just multiplication by an integer m. For example, if E has an F-rational point $P \in E[m]$, then the quotient map $E \to E' = E/\langle P \rangle$ is an isogeny. And if E is an elliptic curve with complex multiplication by an order in an imaginary quadratic field K contained in F, then E will have many F-rational endomorphisms that are not just multiplication by an integer. The Selmer groups for these endomorphisms have featured prominently in most efforts to understand the arithmetic of elliptic curves with complex multiplication, such as the Coates–Wiles theorem [13] or Rubin's proof of the first known cases of elliptic curves with a finite Tate-Shafarevich group [57].

2.1.4. *The p^∞-Selmer group.* The p^∞-Selmer group of E is obtained by taking the direct limits over n of the p-power Selmer groups $\mathrm{Sel}_{p^n}(E/F)$:

$$\mathrm{Sel}_{p^\infty}(E/F) = \varinjlim_n \mathrm{Sel}_{p^n}(E/F).$$

Since $\varinjlim_n H^1(F, E[p^n]) = H^1(F, E[p^\infty])$ the p^∞-Selmer group can also be directly defined as

$$\mathrm{Sel}_{p^\infty}(E/F) = \ker \left\{ H^1(F, E[p^\infty]) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}.$$

The natural surjection $H^1(F, E[p^n]) \twoheadrightarrow H^1(F, E[p^\infty])[p^n]$ induces a surjection $\mathrm{Sel}_{p^n}(E/F) \twoheadrightarrow \mathrm{Sel}_{p^\infty}(E/F)[p^n]$ with kernel $E[p^\infty](F)/p^n E[p^\infty](F)$.

Taking the direct limit over the fundamental exact sequences for the multiplication by p^n maps yields the fundamental exact sequence for the p^∞-Selmer groups:

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)[p^\infty] \to 0.$$

Remark 2.1.4.b. The group $Ш(E/F)[p^\infty]$ is expected to be finite, in which case it follows from the fundamental exact sequence for $\mathrm{Sel}_{p^\infty}(E/F)$ that

$$\mathrm{rank}_{\mathbb{Z}} E(F) \overset{?}{=} \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/F),$$

the $\mathbb{Z}_p$-corank of a discrete module S being the $\mathbb{Z}_p$-rank of its Pontryagin dual $\mathrm{Hom}_{cts}(S, \mathbb{Q}_p/\mathbb{Z}_p)$.

2.1.5. *The p^∞-Selmer group in terms of $E[p^\infty]$ only.* The p^∞-Selmer group of E can be defined solely in terms of the p-divisible group $E[p^\infty]$. We start by noting that if $v \nmid p$, then $\varinjlim_n E(F_v)/p^n E(F_v) = E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. The key point here is that $E(F_v)/p^n E(F_v)$ has order either 1 or 2 if $v \mid \infty$ and if $v \nmid \infty$ then $E(F_v)$ contains a pro-ℓ-subgroup of finite index, where ℓ is the residue characteristic of v. It follows that the local condition at v defining a class in $\mathrm{Sel}_{p^\infty}(E/F)$ is just that its restriction to $H^1(F_v, E[p^\infty])$ is 0. If in addition v is a prime of good reduction, then the kernel of the restriction map $H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])$ is $H^1(G_{F_v}/I_v, E[p^\infty]) \cong E[p^\infty]/(\mathrm{Frob}_v - 1)E[p^\infty] = 0$ (since $E[p^\infty]$ is divisible and 1 is not an eigenvalue for the action of Frob_v on the p-adic Tate module of the elliptic curve E/k_v). So for such v, vanishing in $H^1(F_v, E[p^\infty])$ is equivalent to vanishing in $H^1(I_v, E[p^\infty])$, that is, the local condition at v defining a class in $\mathrm{Sel}_{p^\infty}(E/F)$ can also be expressed as the class being unramified at v. Already, this means

$$\begin{aligned}\mathrm{Sel}_{p^\infty}(E/F) &= \ker\left\{ H^1(F, E[p^\infty]) \overset{res}{\to} \prod_{v\nmid p} H^1(F_v, E[p^\infty]) \times \prod_{v\mid p} H^1(F_v, E)\right\} \\ &= \ker\left\{ H^1(G_{F,\Sigma}, E[p^\infty]) \overset{res}{\to} \prod_{v\in\Sigma, v\nmid p} H^1(F_v, E[p^\infty]) \times \prod_{v\mid p} H^1(F_v, E[p^\infty])/\mathrm{im}(\kappa_v)\right\}.\end{aligned}$$

The situation for $v \mid p$ is more complicated. We want to express $\mathrm{im}(\kappa_v)$ in terms of $E[p^\infty]$ only (without reference to the full curve E). Let $T = T_p E = \varprojlim_n E[p^n]$ be the p-adic Tate-module of E (really just of the p-divisible group $E[p^\infty]$). Note that there is a canonical isomorphism $T_p E \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{\to} E[p^\infty]$ (given by $(P_n) \otimes \frac{1}{p^m} \mapsto P_m$).

Suppose first that E has good ordinary or multiplicative reduction at v. Then T has a G_{F_v}-filtration $0 \subset T_v^+ \subset T$ with T_v^+ a rank-one $\mathbb{Z}_p$-summand such that T/T_v^+ is unramified with Frob_v acting as multiplication by the unit root α_p of $x^2 - a_v(E)x + p$ (if E has good reduction at v) or by $a_v(E)$ (if E has multiplicative reduction at v). Then

$$\begin{aligned}\mathrm{im}(\kappa_v) &= \mathrm{im}\left\{H^1(F_v, T_v^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(F_v, E[p^\infty])\right\}_{\mathrm{div}} \\ &= \ker\left\{H^1(F_v, E[p^\infty]) \to H^1(F_v, T/T_v^+ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)\right\}_{\mathrm{div}},\end{aligned}$$

where the subscript 'div' denotes the maximal divisible subgroup. In the case of good reduction, the divisible subgroup is the whole group unless $a_v(E) \equiv 1 \bmod p$ (the index of the divisible subgroup is $\#\mathbb{Z}_p/(\alpha_p - 1)\mathbb{Z}_p$). In the case of split multiplicative reduction, the divisible subgroup is everything. In the case of non-split multiplicative reduction, the divisible subgroup is everything if $p > 2$, and if $p = 2$ then the index of the divisible subgroup is either 1 or 2 (and equals the 2-part of the Tamagawa factor for E/F_v). All this follows from analyzing $E[p^\infty]$ and its cohomology using the formal group when E has good reduction at v and using the Tate parameterization in the cases of multiplicative reduction.

More generally, Bloch and Kato [5, Ex. 3.11] described the image of κ_v, $v \mid p$, in a manner that also covers the cases of supersingular and additive reduction. Let $V = T \otimes \mathbb{Q}_p$. This is a two-dimensional $\mathbb{Q}_p$-representation of G_F. Note that $V/T = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{\to} E[p^\infty]$. Letting

$$H^1_f(F_v, V) = \ker\left\{H^1(F_v, V) \to H^1(F_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})\right\},$$

they show that

$$\mathrm{im}(\kappa_v) = \mathrm{im}\left\{H^1_f(F_v, V) \to H^1(F_v, E[p^\infty])\right\}.$$

It is a good exercise of one's understanding of basic p-adic Hodge theory to deduce the description of $\mathrm{im}(\kappa_v)$ given above in the cases of ordinary and multiplicative reduction from that of Bloch and Kato.

Remark 2.1.5.c. The question of whether the Selmer group $\mathrm{Sel}_{p^n}(E/F)$ is determined by the Galois module $E[p^n]$ has been studied by Česnavičius [11]; a positive answer is given in terms of flat cohomology under mild conditions on p.

2.1.6. *Selmer groups and The Birch–Swinnerton-Dyer Conjecture.* As already noted, the Selmer groups $\mathrm{Sel}_m(E/F)$ and $\mathrm{Sel}_{p^\infty}(E/F)$ encapsulate information about the Mordell–Weil group $E(F)$ and the Tate–Shafarevich group $Ш(E/F)$. Information about both these groups should also be encoded in the L-function $L(E/F,s)$ of E, as explained in the Birch–Swinnerton-Dyer Conjecture. Combining this we can extract some expected connections between $L(E/F,s)$ and Selmer groups of E.

The Birch and Swinnerton-Dyer Conjecture, as stated by Tate [68]:

Conjecture 1 (Birch and Swinnerton-Dyer Conjecture)**.** *Let F be a number field and let E/F be an elliptic curve.*

(a) *The Hasse–Weil L-function $L(E/F,s)$ has analytic continuation to the entire complex plane and*

$$\mathrm{ord}_{s=1}L(E/F,s) = \mathrm{rk}_{\mathbb{Z}}\, E(F). \tag{BSD}$$

(b) *The Tate–Shafarevich group $Ш(E/F)$ has finite order, and*

$$\frac{L^{(r)}(E/F,1)}{r!\cdot \Omega_{E/F}\cdot \mathrm{Reg}(E/F)\cdot |\Delta_F|^{-1/2}} = \frac{\#Ш(E/F)\cdot \prod_{v\nmid\infty} c_v(E/F)}{(\#E(F)_{\mathrm{tors}})^2}, \tag{BSD-f}$$

where $r = \mathrm{ord}_{s=1}L(E/F,s)$, $c_v(E/F) = [E(F_v) : E^0(F_v)]$ is the Tamagawa number at v for a finite place v of F, $\mathrm{Reg}(E/F)$ is the regulator of the Néron-Tate height pairing on $E(F)$, Δ_F is the discriminant of F, and $\Omega_{E/F}\in\mathbb{C}^\times$ is the period defined by

$$\Omega_{E/F} = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{a}_\omega)\cdot \prod_{\substack{v|\infty\\ v\text{-real}}} \int_{E(F_v)} |\omega| \cdot \prod_{\substack{v|\infty\\ v\text{-complex}}} \left(2\cdot \int_{E(F_v)} \omega\wedge\overline{\omega}\right). \tag{Ω}$$

Here $\omega\in\Omega^1(\tilde{E}/\mathcal{O}_F)$ is any non-zero differential on the Néron model $\tilde{E}$ of E over $\mathcal{O}_F$, and $\mathfrak{a}_\omega\subset F$ is the fractional ideal such that $\mathfrak{a}_\omega\cdot\omega = \Omega^1(\tilde{E}/\mathcal{O}_F)$. Also, for a finite place v, $E^0(F_v)\subset E(F_v)$ denotes the subgroup of local points that specialize to the identity component of the Néron model of E at the place v.

When $F=\mathbb{Q}$ we will write Ω_E for $\Omega_{E/\mathbb{Q}}$.

As already noted, the finiteness of $Ш(E/F)$ (or even of just the p-primary part $Ш(E/F)[p^\infty]$) implies that the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F)$ equals the rank of $E(F)$. So one expects

$$\mathrm{ord}_{s=1}L(E/F,s) \overset{?}{=} \mathrm{corank}_{\mathbb{Z}_p}\,\mathrm{Sel}_{p^\infty}(E/F). \tag{BSD-crk}$$

This suggests that one might first ask:

$$L(E/F,1)=0 \overset{?}{\iff} \#\mathrm{Sel}_{p^\infty}(E/F)=\infty. \tag{Sel-van}$$

It also suggests the question:

$$\text{(Sel-par)} \qquad \operatorname{ord}_{s=1} L(E/F,s) \equiv \frac{1-w(E/F)}{2} \stackrel{?}{\equiv} \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/F) \bmod 2.$$

Here $w(E/F) \in \{\pm 1\}$ is the root number of E/F (the sign of the expected functional equation of $L(E/F)$). If $L^{\mathrm{alg}}(E/F,1) = L(E/F,1)/\Omega_{E/F}|\Delta_F|^{-1/2}$ is a rational number, then a refined form of (Sel-van), incorporating the BSD formula (BSD-f) when $r=0$, is

$$\text{(BSDp-0)} \qquad \left|L^{\mathrm{alg}}(E/F,1)\right|_p \stackrel{?}{=} \left| \frac{\#\operatorname{Sel}_{p^\infty}(E/F) \cdot \prod_{v \nmid \infty} c_v(E/F)}{(\#E(F)_{\mathrm{tors}})^2} \right|_p .$$

Here we understand the right-hand side to equal 0 if $\#\operatorname{Sel}_{p^\infty}(E/F) = \infty$. As explained below, some progress has been made on all these problems (and a few others) for an elliptic curve $E/\mathbb{Q}$.

2.2. **Bloch–Kato Selmer groups.** Bloch and Kato [5] actually defined Selmer groups in a very general setting, starting with a p-adic Galois representation of G_F.

In keeping with our arithmetic conventions for class field theory, we also adopt arithmetic conventions for p-adic Hodge–Tate weights. In particular, the p-adic cyclotomic character has Hodge–Tate weight 1.

2.2.1. *The definition.* Let L be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$. Let V be a finite-dimensional L-space equipped with a continuous L-linear action of G_F. We assume that V is a *geometric* representation of G_F. This means that the action of G_F on V is unramified away from a finite set of places and that for each place $v \mid p$ the representation of G_{F_v} on V is potentially semistable (equivalently, de Rham). Let $T \subset V$ be a G_F-stable $\mathcal{O}$-lattice (so in particular, $V = T \otimes_{\mathcal{O}} L$). Such a lattice always exists by a simple compactness argument. Let $W = V/T$. Bloch and Kato defined subgroups (Selmer groups) $H^1_f(F,V) \subset H^1(F,V)$, $H^1_f(F,T) \subset H^1(F,T)$, and $H^1_f(F,W) \subset H^1(F,W)$ as follows.

First they defined local subgroups for a place v of F:

$$H^1_f(F_v,V) = \begin{cases} H^1(\mathrm{Gal}(F_v^{\mathrm{ur}}/F_v), V^{I_v}) = \ker\left\{H^1(F_v,V) \to H^1(I_v,V)\right\} & v \nmid p \\ \ker\left\{H^1(F_v,V) \to H^1(F_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})\right\} & v \mid p. \end{cases}$$

The exact sequence $0 \to T \to V \to W \to 0$ yields an exact sequence

$$H^1(F_v,T) \stackrel{i}{\to} H^1(F_v,V) \stackrel{j}{\to} H^1(F_v,W),$$

and $H^1_f(F_v,T)$ and $H^1_f(F_v,W)$ are defined to be

$$H^1_f(F_v,T) = i^{-1}(H^1_f(F_v,V)) \ \text{ and } \ H^1_f(F_v,W) = j(H^1_f(F_v,V)).$$

Note that $H^1_f(F_v,W)$ is L-divisible, being the image of the L-space $H^1_f(F_v,V)$.

The Bloch–Kato Selmer groups are then defined by

$$H^1_f(F,?) = \ker\left\{ H^1(F,?) \stackrel{res}{\to} \prod_v H^1(F_v,?)/H^1_f(F_v,?) \right\}, \quad ? = T, V, \text{ or } W.$$

The Bloch–Kato analog of the Tate–Shafarevich group is

$$Ш_f(W/F) = H^1_f(F,W)/H^1_f(F,W)_{\mathrm{div}},$$

the quotient of $H^1_f(F,W)$ by its maximal divisible subgroup.

2.2.2. *Examples.* We describe some examples, a few of which figure in subsequent results:

Example 2.2.2.a (Elliptic curves: $V = V_pE$). Then $T = T_pE$ is a G_F-stable $\mathbb{Z}_p$-lattice and $W \cong E[p^\infty]$. If $v \nmid p$ then it is relatively easy to see that $H^1_f(F_v, V) = 0$. Then $H^1_f(F_v, W) = 0$, which agrees with $\mathrm{im}(\kappa_v)$. As already noted above, Bloch and Kato proved that $H^1(F_v, W) = \mathrm{im}(\kappa_v)$ even when $v \mid p$. It follows that $H^1_f(F, W) = \mathrm{Sel}_{p^\infty}(E/F)$. The group $Ш_f(E[p^\infty]/F)$ is then the quotient of the p-primary part $Ш(E/F)[p^\infty]$ of the usual Tate–Shafarevich group by its maximal divisible subgroup. In particular, $Ш_f(E[p^\infty]/F)$ equals $Ш(E/F)[p^\infty]$ if and only if the latter is finite.

Example 2.2.2.b (Algebraic Hecke characters). Let $\psi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times$ be an algebraic Hecke character. This means that there exists an algebraic character $\rho : F^\times \to \overline{\mathbb{Q}}^\times$ such that the restriction of ψ to the identity component $(F \otimes \mathbb{R})_1^\times \subset (F \otimes \mathbb{R})^\times$ is given by ρ. Concretely, this is so if and only if there exist $[F : \mathbb{Q}]$ integers $(n_\tau)_\tau$, indexed by the embeddings $\tau : F \hookrightarrow \mathbb{C}$, such that for $\alpha = \sum_i x_i \otimes r_i \in (F \otimes \mathbb{R})_1^\times$, $\psi(\alpha) = \prod_\tau (\sum_i \tau(x_i) r_i)^{n_\tau}$. The character $\mathbb{A}_F^\times \to \mathbb{C}^\times$, $\alpha \mapsto \rho(\alpha_\infty)^{-1}\psi(\alpha)$ takes values in $\overline{\mathbb{Q}}^\times$ (and even in a finite extension of $\mathbb{Q}$). The p-adic Galois character associated with ψ is just

$$\rho_\psi : G_F \to \overline{\mathbb{Q}}_p^\times, \quad \rho_\psi(\sigma) = \rho(x_p)\rho(x_\infty)^{-1}\psi(x) \ \text{ for } \ \sigma = \mathrm{rec}_F(x).$$

Note that if $\psi = |\mathrm{N}_{F/\mathbb{Q}}(\cdot)|_{\mathbb{Q}}^{-1}$, then $\sigma_\psi = \epsilon$, the p-adic cyclotomic character.

Serre proved that $\psi \mapsto \sigma_\psi$ is a bijection between algebraic Hecke characters of F and p-adic characters $\chi : G_F \to \overline{\mathbb{Q}}_p^\times$ that are unramified outside a finite set of places and Hodge–Tate at each $v \mid p$.

The Hodge–Tate weights of ρ_ψ can be read off from the algebraic representation ρ. The simplest case is when p splits completely in F. Then the places of v are indexed by the embeddings τ. In particular, if v is the place determined by the embedding $F \overset{\tau}{\hookrightarrow} \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, then the Hodge–Tate weight of $\sigma_\psi|_{G_{F_v}}$ is $-n_\tau$. Let $n_v = n_\tau$. Let $L \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}_p$ containing the values of ρ_ψ. It follows that in this case

$$H^1_f(F_v, L(\rho_\psi)) = \begin{cases} H^1(F_v, L(\rho_\psi)) & n_v < -1 \\ 0 & n_v > 0. \end{cases}$$

In particular, for $W = L/\mathcal{O}(\rho_\psi)$ with each n_v either > 0 or < -1,

$$H^1_f(F, W) = \ker \left\{ H^1(F, W) \overset{res}{\to} \prod_{v \nmid p} \frac{H^1(F_v, W)}{H^1_f(F_v, W)} \prod_{v \mid p, n_v > 0} H^1(F_v, W) \times \prod_{v \mid p, n_v < -1} \frac{H^1(F_v, W)}{H^1(F_v, W)_{\mathrm{div}}} \right\}.$$

Example 2.2.2.c (Twists of V_pE by characters). Suppose $\chi : G_F \to \overline{\mathbb{Q}}_p^\times$ is a continuous character that is unramified away from finitely many places and Hodge–Tate at all places $v \mid p$. Let $L = \mathbb{Q}_p[\chi]$ be the finite extension of $\mathbb{Q}_p$ obtained by adjoining the values of χ. Then χ takes values in $\mathcal{O}^\times$. Let $V = V_pE \otimes_{\mathbb{Q}_p} L(\chi)$ and $T = T_pE \otimes_{\mathbb{Z}_p} \mathcal{O}(\chi)$ (so if ρ denotes the action of G_F on T_pE, then G_F acts on T as $\rho \otimes \chi$). We then let

$$\mathrm{Sel}(E/F, \chi) = H^1_f(F, W).$$

It will be useful to have a description of $H^1(F_v, V)$, $v \mid p$, in some cases. Suppose first that all the Hodge-Tate weights of $\chi|_{G_{F_v}}$ are zero (equivalently, the restriction $\chi|_{I_v}$ has finite order).

Suppose also that E has good ordinary or multiplicative reduction at v. Then

$$H^1_f(F_v, V) = \ker\left\{H^1(F_v, V) \to H^1(I_v, V/V_v^+)\right\},$$

where V_v^+ is $(V_pE)_v^+ \otimes_{\mathbb{Q}_p} L(\chi)$. It follows that $H^1_f(F_v, W)$ is just the maximal divisible subgroup of $\ker\left\{H^1(F_v, W) \to H^1(I_v, W/W_v^+)\right\}$, where $W_v^+ = T_v^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

If all the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are > 1, then all the Hodge–Tate weights of V at v are > 1 and so $H^1_f(F_v, V) = H^1(F_v, V)$. But if all the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are < -1, then all the Hodge–Tate weights of V at v are < 0 and so $H^1_f(F_v, V) = 0$. Suppose then that for each $v \mid p$ the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are either all > 1 or all < -1, and let $S_p^{\pm}$ denote the set of $v \mid p$ such that the Hodge–Tate weight of χ at v has sign $\pm$. Then

$$H^1_f(F, W) = \ker\left\{H^1(F, W) \overset{res}{\to} \prod_{v\nmid p} \frac{H^1(F_v, W)}{H^1_f(F_v, W)} \times \prod_{v\in S_p^-} H^1(F_v, W) \times \prod_{v\in S_p^+} \frac{H^1(F_v, W)}{H^1(F_v, W)_{\mathrm{div}}}\right\}.$$

In particular, the reduction type of E at v does not really intervene in the description of the Bloch–Kato Selmer groups in this case.

Example 2.2.2.d (Eigenforms). Let $f \in S_k(N, \chi)$ be a newform of weight k, level N, and character χ. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be the q-expansion of f at the cusp at infinity. The coefficients a_n (equivalently, the eigenvalues of the action of the usual Hecke operators on f) are algebraic integers and generate a (possibly non-maximal) order in the ring of integers of the finite extension $\mathbb{Q}(f) \subset \mathbb{C}$ obtained by adjoining the a_n's. Let $L \subset \overline{\mathbb{Q}}_p$ be a finite extension of $\mathbb{Q}_p$ containing the image of $\mathbb{Q}(f)$. Let $\mathcal{O} \subset L$ be the ring of integers of L.

Associated with f and L (and the embedding $\mathbb{Q}(f) \hookrightarrow L$) is a two-dimensional L-space V_f and an absolutely irreducible continuous $G_{\mathbb{Q}}$-representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{Aut}_L(V_f)$ such that ρ_f is unramified at all primes $\ell \nmid Np$ and $\det(1 - X \cdot \rho_f(\mathrm{frob}_\ell)) = 1 - a_\ell X + \chi(\ell)\ell^{k-1}X^2$ for such ℓ. In particular, $\mathrm{trace}\,\rho_f(\mathrm{frob}_\ell) = a_\ell(f)$ if $\ell \nmid pN$, and $\det \rho_f = \chi\epsilon^{k-1}$.

Suppose $k \geq 2$ and $a_p \in \mathcal{O}^\times$. Let $\alpha_p \in \mathbb{Q}^\times$ be the unit root of $x^2 - a_p x + \chi(p)p^{k-1}$ if $p \nmid N$ and otherwise let $\alpha_p = a_p$. Then V has a $G_{\mathbb{Q}_p}$-filtration $V^+ \subset V$, with $\dim_L V^+ = 1$ and $G_{\mathbb{Q}_p}$ acting on V via the character $\epsilon^{k-1}\alpha^{-1}$, where $\alpha : G_{\mathbb{Q}_p} \to \mathcal{O}^\times$ is unramified and $\alpha(\mathrm{frob}_p) = \alpha_p$. Let $V^- = V/V^+$. In this case

$$H^1_f(\mathbb{Q}_p, V) = \ker\left\{H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, V^-)\right\}.$$

Letting $T \subset V$ be any $G_{\mathbb{Q}}$-stable $\mathcal{O}$-lattice and $W = V/T$, we let $T^+ = T \cap V^+$, $T^- = T/T^+$, $W^+ = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ and $W^- = W/W^+$. Then

$$H^1_f(\mathbb{Q}_p, W) = \ker\left\{H^1(\mathbb{Q}_p, W) \to H^1(\mathbb{Q}_p, W^-)\right\}_{\mathrm{div}} = \mathrm{im}\left\{H^1(\mathbb{Q}_p, W^+) \to H^1(\mathbb{Q}_p, W)\right\}_{\mathrm{div}}.$$

Example 2.2.2.e (Twists of Eigenforms). Let V be the Galois representation associated to some newform of weight k, and let $\chi : G_F \to L^\times$ be a character as in Example 2.2.2.c. Everything in that example carries over to the G_F-representations $V(\chi)$ with the only change being that we now require the Hodge–Tate weights to be either > 1 or $< 1 - k$ in the latter part.

2.2.3. *Vista: The Bloch–Kato conjectures for L-functions and Selmer groups.* In addition to defining Selmer groups very generally, Bloch and Kato [5] also formulated conjectures generalizing (BSD-crk) and (BSDp-0) (see also [18]).

2.3. **Selmer structures.** Mazur and Rubin [48, Ch. 2] introduced a general setup for Selmer groups.

2.3.1. *The structures.* Let $\mathcal{O}$ be the ring of integers of a finite extension $L/\mathbb{Q}_p$. Let M be a topological $\mathcal{O}$-module equipped with a continuous $\mathcal{O}$-linear action of G_F that is unramified outside a finite set of places.

A Selmer structure for M is a collection of $\mathcal{O}$-submodules

$$\mathcal{L} = (\mathcal{L}_v)_v, \quad \mathcal{L}_v \subset H^1(F_v, M),$$

indexed by the places v of M. To be a Selmer structure this collection must satisfy

$$\mathcal{L}_v = H^1_{\mathrm{ur}}(F_v, M) = \ker\left\{H^1(F_v, M) \to H^1(I_v, M)\right\} \quad \text{for almost all } v.$$

The asssociated Selmer group is then defined to be

$$H^1_{\mathcal{L}}(F, M) = \left\{c \in H^1(F, M) \ : \ \ res_v(c) \in \mathcal{L}_v \ \forall v\right\}.$$

If Σ is any finite set of places containing all those at which M is ramified or for which $\mathcal{L}_v \neq H^1_{\mathrm{ur}}(F_v, M)$, then

$$H^1_{\mathcal{L}}(F, M) = \ker\left\{H^1(G_{F,\Sigma}, M) \stackrel{res}{\to} \prod_{v\in\Sigma} H^1(F_v, M)/\mathcal{L}_v\right\}.$$

Let $M^* = \mathrm{Hom}_{cts}(M, \mathbb{Q}_p/\mathbb{Z}_p(1)) = \mathrm{Hom}_{cts}(M, \mu_{p^\infty})$ be the arithmetic dual of M, equipped with the natural $\mathcal{O}$-module structure (so $(a \cdot f)(m) = f(am)$ for $a \in \mathcal{O}$, $f \in M^\vee$, and $m \in M$). Suppose M is either a direct or projective limit of finite-order G_F-stable $\mathcal{O}$-modules. The same is then true of M^* (the dual of a direct limit is an inverse limit, etc.). In this case, local Tate duality provides us with a perfect pairing

$$(\cdot,\cdot)_v : H^i(F_v, M) \times H^{2-i}(F_v, M^*) \to \mathbb{Q}_p/\mathbb{Z}_p, \quad i = 0, 1, 2.$$

This is just the cup-product combined with the canonical pairing $M \otimes M^* \to \mu_{p^\infty}$ and the identification $H^2(F_v, \mu_{p^\infty}) = \mathbb{Q}_p/\mathbb{Z}_p$. Furthermore, if $v \nmid p\infty$, then $H^1_{\mathrm{ur}}(F_v, M)$ and $H^1_{\mathrm{ur}}(F_v, M^*)$ are mutual annihilators under $(\cdot,\cdot)_v$. It follows that if $\mathcal{L} = (\mathcal{L}_v)$ is a Selmer structure for M, then

$$\mathcal{L}^* = (\mathcal{L}_v^*), \quad \mathcal{L}_v^* \text{ the annihilator of } \mathcal{L}_v \text{ under } (\cdot,\cdot)_v,$$

is a Selmer structure for M^*.

2.3.2. *Examples.* The Selmer groups we have considered so far are all defined by Selmer structures.

Example 2.3.2.a ($\mathrm{Sel}_{p^n}(E/F)$). Take $\mathcal{O} = \mathbb{Z}_p$, $M = E[p^n]$, and

$$\mathcal{L}_v = \mathrm{im}(E(F_v)/p^n E(F_v) \stackrel{\kappa_v}{\to} H^1(F_v, E[p^n]).$$

As noted before, if $v \nmid p$ is a prime of good reduction, then $\mathrm{im}(\kappa_v) = H^1_{\mathrm{ur}}(F_v, E[p^n])$, so $(\mathcal{L}_v)_v$ is a Selmer structure for $E[p^n]$.

The Weil pairing $(\cdot,\cdot)_{\mathrm{Weil}} : E[p^n] \times E[p^n] \to \mu_{p^n}$ identifies M^* with $E[p^n]$. Furthermore, for each place v, $\mathrm{im}(\kappa_v)$ is its own annihilator under $(\cdot,\cdot)_v$, and so $\mathcal{L}^* = \mathcal{L}$.

Example 2.3.2.b ($H^1_f(F,T)$ and $H^1_f(F,W)$). The Bloch–Kato Selmer groups $H^1_f(F,?)$, $? = T, W$, are just the Selmer groups for the Selmer structures

$$\mathcal{L}_f = (H^1_f(F_v,?)).$$

To see that $\mathcal{L}_f$ is a Selmer structure, it suffices to note that if V is unramified at some $v \nmid p$, then $H^1_f(F_v,?) = H^1_{\mathrm{ur}}(F_v,?)$. For $? = T$ this is so since $H^1(F_v,T)_{\mathrm{tor}}$ is the image of $W^{G_{F_v}} = W^{G_{F_v}/I_v}$ and so belongs to $H^1_{\mathrm{ur}}(F_v,T)$. And for $? = W$, $H^1_{\mathrm{ur}}(F_v,W) = H^1(G_{F_v}/I_v,W)$ is the image of $H^1_{\mathrm{ur}}(F_v,V) = H^1(G_{F_v}/I_v,V)$ as $H^2(G_{F_v}/I_v,T) = 0$, the pro-cyclic group $G_{F_v}/I_v \cong \widehat{\mathbb{Z}}$ having cohomological dimension 1.

2.3.3. *An important exact sequence.* We impose a partial ordering on the Selmer structures on M, writing $\mathcal{L}_1 \leq \mathcal{L}_2$ if $\mathcal{L}_{1,v} \subseteq \mathcal{L}_{2,v}$ for all v. In this case $H^1_{\mathcal{L}_1}(F,M) \subseteq H^1_{\mathcal{L}_2}(F,M)$. Note that we also have $\mathcal{L}_2^* \leq \mathcal{L}_1^*$.

Let $\mathcal{L}_1 \leq \mathcal{L}_2$ be Selmer structures for M and let S be the finite set of places where $\mathcal{L}_{1,v} \neq \mathcal{L}_{2,v}$. Then global duality implies that there is an exact sequence [48, Thm. 2.3.4]:

$$\text{(SES)} \qquad 0 \to H^1_{\mathcal{L}_1}(F,M) \to H^1_{\mathcal{L}_2}(F,M) \overset{res}{\to} \prod_{v\in S} \frac{\mathcal{L}_{2,v}}{\mathcal{L}_{1,v}} \overset{res^\vee}{\to} H^1_{\mathcal{L}_1^*}(F,M^*)^\vee \to H^1_{\mathcal{L}_2}(F,M^*)^\vee \to 0.$$

The map $res^\vee$ is the dual of

$$H^1_{\mathcal{L}^*}(F,M^*) \overset{res}{\to} \prod_{v\in S} \mathcal{L}_v^* = \prod_{v\in S} \left(\frac{H^1(F_v,M)}{\mathcal{L}_v} \right)^\vee,$$

where the final identification comes via Tate local duality.

2.3.4. *An important formula.* Suppose that M has finite order. Let $\mathcal{L}$ be a Selmer structure for M. Then by combining the exact sequence (SES) with global duality and the global Euler characteristic yields (cf. [15, Thm. 2.19] and [48, Prop. 2.3.5]):

$$\text{(SF)} \qquad \frac{\#H^1_{\mathcal{L}}(F,M)}{\#H^1_{\mathcal{L}^*}(F,M^*)} = \frac{\#H^0(F,M)}{\#H^0(F,M^*)} \prod_v \frac{\#\mathcal{L}_v}{\#H^1(F_v,M)}.$$

3. Iwasawa modules for elliptic curves

For simplicity we assume from hereon that

$$\text{(odd)} \qquad p > 2.$$

Among other things this ensures the triviality of all the H^1-cohomology groups for all archimedean local fields that appear herein.

3.1. **The extension F_∞/F.** Let F_∞/F be a $\mathbb{Z}_p^d$-extension of F, $d \geq 1$. This is an (infinite) pro-finite abelian extension of F such that $\Gamma = \mathrm{Gal}(F_\infty/F)$ (which is a $\widehat{\mathbb{Z}}$-module) is isomorphic to $\mathbb{Z}_p^d$. Let

$$\Lambda = \mathbb{Z}_p[\![\Gamma]\!],$$

be the completed group ring of Γ over $\mathbb{Z}_p$. If $\gamma_1, ..., \gamma_d \in \Gamma$ are topological generators, then the map $\Lambda \overset{\sim}{\to} \mathbb{Z}_p[\![T_1, ..., T_d]\!]$, $\gamma_1 \mapsto 1 + T_i$, identifies Λ with the power series ring in d variables over $\mathbb{Z}_p$. In particular, Λ is a $d+1$-dimensional regular complete local ring. The maximal ideal of Λ is $\mathfrak{m} = (p, \gamma_1 - 1, ..., \gamma_d - 1)$. If $d = 1$, then we will just write γ for a topological generator of Γ.

The examples of most interest to us will be:

3.1.1. $F = \mathbb{Q}$. In this case there is exactly one possibility for F_∞, namely the cyclotomic $\mathbb{Z}_p$-extension, which we will denote by $\mathbb{Q}_\infty$. This is defined as follows.

For each $n \geq 1$ let ζ_{p^n} be a primitive p^nth root of unity. The field $\mathbb{Q}(\zeta_{p^{n+1}})$ is a Galois extension of $\mathbb{Q}$ with Galois group $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ canonically isomorphic to $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, the isomorphism being $\sigma \mapsto a \bmod p^{n+1}$ for $\sigma(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^a$. The groups G_n decompose compatibly as $G_n = \Delta \times \Gamma_n$ with Δ cyclic of order $p-1$ and Γ_n cyclic of order p^n. The subgroup Δ projects isomorphically onto $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$. Put $\mathbb{Q}(\zeta_{p^\infty}) = \cup_{n=0}^\infty \mathbb{Q}(\zeta_{p^{n+1}})$. Then there is a canonical isomorphism of profinite groups:

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n G_n \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

The Galois group G then decomposes as $G = \Delta \times \Gamma$ with $\Gamma = \varprojlim_n \Gamma_n$. The group Γ is a cyclic pro-p-group and identified with $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ while Δ is just the subgroup $\mu_{p-1} \subset \mathbb{Z}_p^\times$. The cyclotomic $\mathbb{Z}_p$-extension is just $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$. The group Γ projects isomorphically onto $\Gamma_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, which indentifies these two groups. Note that a convenient topological generator of Γ (and hence of $\Gamma_\mathbb{Q}$) is the element γ identified with $1 + p \in 1 + p\mathbb{Z}_p$ (since $p > 2$, $1 + p\mathbb{Z}_p = (1+p)^{\mathbb{Z}_p}$).

3.1.2. $F = K$, *an imaginary quadratic extension of* $\mathbb{Q}$. In this case there are three extensions of interest to us. The first of these is the unique $\mathbb{Z}_p^2$-extension K_∞/K; this is maximal among the $\mathbb{Z}_p^d$-extensions of K (for all d). The other two are the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^{\mathrm{cyc}}/K$ and the anticyclotomic $\mathbb{Z}_p$-extension K_∞^{ac}.

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\Gamma_K = \mathrm{Gal}(K_\infty/K)$ by conjugation. In particular, Γ_K decomposes under the action of the non-trivial automorphism $c \in \mathrm{Gal}(K/\mathbb{Q})$ as $\Gamma_K = \Gamma_K^+ \times \Gamma_K^-$ with c acting on $\Gamma_K^\pm$ as $c^{-1}gc = g^{\pm 1}$. Then $K_\infty^{\mathrm{cyc}} = K_\infty^{\Gamma_K^-}$ and $K_\infty^{\mathrm{ac}} = K_\infty^{\Gamma_K^+}$. In particular, the canonical projections $\mathrm{Gal}(K_\infty/K) \twoheadrightarrow \mathrm{Gal}(K_\infty^?/K)$ induce isomporphisms

$$\Gamma_K^+ \xrightarrow{\sim} \Gamma_K^{\mathrm{cyc}} = \mathrm{Gal}(K_\infty^{\mathrm{cyc}}/K) \quad \text{and} \quad \Gamma_K^- \xrightarrow{\sim} \Gamma_K^{\mathrm{ac}} = \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K).$$

Of course, the cyclotomic $\mathbb{Z}_p$-extension is just $K_\infty^{\mathrm{cyc}} = K \cdot \mathbb{Q}_\infty$, and the canonical projection $\Gamma_K^{\mathrm{cyc}} = \mathrm{Gal}(K_\infty^{\mathrm{cyc}}/K) \xrightarrow{\sim} \Gamma_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is an isomorphism.

3.1.3. *Back to the general case.* In general, the extension F_∞/F is unramified at each place $v \nmid p$ of F, and the finiteness of the class group of F implies that it must be ramified at at least one place $v \mid p$. For simplicity we will assume that

(p-ram) $\qquad\qquad F_\infty$ is ramified at each place $v \mid p$.

This is true of each of our examples of interest. However, there are many $\mathbb{Z}_p$-extensions of arithmetic interest for which this hypothesis does not hold. Another nice property that an extension F_∞/F can have is

(fs) there are only finitely many places of F_∞ over each finite place of F.

This can only hold for $\mathbb{Z}_p$-extensions (that is, for $d = 1$), and even then it does not always hold. Property (fs) holds for the cyclotomic $\mathbb{Z}_p$-extensions $\mathbb{Q}_\infty$ and K_∞^{cyc}. It does not hold for the anticyclotomic extension K_∞^{ac}: while each prime that splits in K has only finitely many places over it in K_∞^{ac}, every prime that is inert in K splits completely in K_∞^{ac}.

3.2. **Selmer groups over F_∞.** Perhaps the most natural way to define a Selmer group over F_∞ is

$$S(E/F_\infty) = \varinjlim_{F \subseteq F' \subset F_\infty} \mathrm{Sel}_{p^\infty}(E/F'),$$

where F' runs over the finite extensions of F in F_∞. This realizes $S(E/F_\infty)$ as a subgroup of $H^1(F_\infty, E[p^\infty])$. However, for our purposes it is convenient to take a slightly different point of view. Following Greenberg, instead of varying the fields F', we enlarge the Galois module $E[p^\infty]$.

As before let $T = T_pE = \varprojlim_n E[p^n]$ be the p-adic Tate-module of E. Then T is a free $\mathbb{Z}_p$-module of rank two with a continuous $\mathbb{Z}_p$-linear action of G_F. We denote this action by ρ. Let $\Lambda^\vee = \mathrm{Hom}_{cts}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontryagin dual of Λ with the Λ-action given by $(x \cdot f)(y) = f(xy) = f(yx)$. Let

$$\Psi : G_F \twoheadrightarrow \mathrm{Gal}(F_\infty/F) = \Gamma \subset \Lambda^\times$$

be the canonical projection. Put

$$M = T \otimes \Lambda^\vee$$

and let G_F act via $\rho \otimes \Psi^{-1}$. Note that the canonical isomorphism $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} E[p^\infty]$ induces an isomorphism $M \xrightarrow{\sim} \mathrm{Hom}_{cts}(\Lambda, E[p^\infty])$, and this is a G_F-equivariant isomorphism if we let G_F act on Λ via Ψ. The module M can be viewed as built out of the W arising from twist of T_pE as in Example 2.2.2.c. If $\chi : G_\mathbb{Q} \twoheadrightarrow \Gamma \to \mathcal{O}^\times$ is a character, $\mathcal{O}$-being the ring of integers of a finite extension L of $\mathbb{Q}_p$, then

$$(M \otimes_{\mathbb{Z}_p} \mathcal{O})[\gamma - \chi(\gamma)] = T_pE \otimes_{\mathbb{Z}_p} (\Lambda^\vee \otimes_{\mathbb{Z}_p} \mathcal{O})[\gamma - \chi(\gamma)] = T_p \otimes_{\mathbb{Z}_p} L/\mathcal{O}(\chi^{-1}).$$

3.2.1. $S(E/F_\infty)$. Let Σ be a finite set of places of F containing all those divide p or at which E has bad reduction. We will define $S(E/F_\infty)$ as a subgroup of $H^1(G_{F,\Sigma}, M)$. To do this we make the following additional simplifying hypothesis:

(sst) E has either good ordinary, multiplicative, or supersingular reduction at each $v \mid p$

(that is, E has semistable reduction at each $v \mid p$). Let S_p^{ord} be the set of $v \mid p$ at which E has good ordinary or multiplicative reduction. Then assuming (p-ram) and (sst) we have

$$S(E/F_\infty) = \ker \left\{ H^1(G_{F,\Sigma}, M) \overset{res}{\to} \prod_{v \in \Sigma, v \nmid p} H^1(F_v, M) \times \prod_{v \in S_p^{\mathrm{ord}}} H^1(I_v, T/T_v^+ \otimes_{\mathbb{Z}_p} \Lambda^\vee) \right\}.$$

Note that no condition is imposed at places $v \mid p$ at which E has supersingular reduction. If (fs) also holds, then we can replace the product $\prod_{v \in \Sigma, v \nmid p} H^1(F_v, M)$ with $\prod_{v \in \Sigma, v \nmid p} H^1(I_v, M)$. It can be shown that this definition of $S(E/F_\infty)$ is identified with the natural definition proposed above via the map $H^1(F, M) \to H^1(F_\infty, E[p^\infty])$ given by restriction to G_{F_∞} followed by evaluation at $1 \in \Gamma$.

Along the way toward the Main Conjectures and their applications we will need some variations on $S(E/F_\infty)$.

3.2.2. $S_{\mathrm{Gr}}(E/K_\infty)$. Let $K \subset \overline{\mathbb{Q}}$ be an imaginary quadratic field. We assume that

(split) $$p \text{ splits in } K\text{: } p = v\bar{v},$$

where v corresponds to the valuation determined by $K \subset \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Letting $F_\infty = K_\infty$, we write $\mathcal{M}$ for the G_K-module M defined above. Let Σ be a finite set of places of K containing all those that dividing p or at which E has bad reduction. We put

$$S_{\mathrm{Gr}}(E/K_\infty) = \ker\left\{ H^1(G_{K,\Sigma}, \mathcal{M}) \overset{res}{\to} \prod_{w\in\Sigma, w\nmid p} H^1(I_w, \mathcal{M}) \times H^1(K_{\bar{v}}, \mathcal{M}) \right\}.$$

This Selmer group is supposed to capture the Selmer groups of the twists of T_pE by characters whose Hodge–Tate weight at v is > 1 and at $\bar{v}$ is < -1.

3.2.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. This is essentially a variation on $S_{\mathrm{Gr}}(E/K_\infty)$. Taking $F_\infty = K_\infty^{\mathrm{ac}}$, the anticyclomtomic $\mathbb{Z}_p$-extension of K, we let M_{ac} be the corresponding G_K-module M. We put

$$S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = \ker\left\{ H^1(G_{K,\Sigma}, M_{\mathrm{ac}}) \overset{res}{\to} \prod_{w\in\Sigma, w\nmid p} H^1(K_w, M_{\mathrm{ac}}) \times H^1(K_{\bar{v}}, M_{\mathrm{ac}}) \right\}.$$

Note that for an inert prime $q \in \Sigma$, since (fs) does not hold, we cannot always replace $H^1(K_q, M_{\mathrm{ac}})$ with $H^1(I_q, M_{\mathrm{ac}})$.

3.2.4. $S_\pm(E/\mathbb{Q}_\infty)$. Suppose $E/\mathbb{Q}$ has supersingular reduction at p. Then the definition of $S(E/\mathbb{Q}_\infty)$ has no restriction on the classes at p. This results in a Λ-module that is too big to be useful. If $a_p(E) = 0$ (which will always be the case if $p \geq 5$), then Kobayashi [38] defined two subgroups $S_\pm(E/\mathbb{Q}_\infty) \subset S(E/\mathbb{Q}_\infty)$ which, building on work of Kato [34], can be shown to be co-torsion in the sense described in §3.3 below.

Let $\mathbb{Q}_n \subset \mathbb{Q}_\infty$ be the finite extension of $\mathbb{Q}$ with $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ (the last isomorphism depends on the choice of γ; the identification with $1 + p\mathbb{Z}_p/1 + p^{n+1}\mathbb{Z}_p$ is canonical). The extension $\mathbb{Q}_n/\mathbb{Q}$ is totally ramified at p and we denote by $\mathbb{Q}_{n,p}$ the completion of $\mathbb{Q}_n$ at the unique prime above p. Then $\mathbb{Q}_{n,p}/\mathbb{Q}_p$ has Galois group Γ_n. Let

$$E^\pm(\mathbb{Q}_{n,p}) = \left\{ P \in E(\mathbb{Q}_{n,p}) \ : \ \mathrm{Tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_{m+1,p}} P \in E(\mathbb{Q}_{m,p}) \forall 0 \leq m < n, m \equiv \frac{1 \mp (-1)}{2} \bmod 2 \right\}.$$

Then we let

$$\mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) = \left\{ c \in \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \ : \ res_p(c) \in \kappa_p(E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \right\},$$

where res_p denotes restriction at the unique prime above p and κ_p is the Kummer map at this prime. The Selmer groups Kobayashi defined are

$$S_\pm(E/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n).$$

Shapiro's lemma gives an identification

$$H^1(\mathbb{Q}_{p,n}, E[p^\infty]) = H^1(\mathbb{Q}_p, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Gamma_n], E[p^\infty])),$$

where the $G_{\mathbb{Q}_p}$ action on $\mathbb{Z}_p[\Gamma_n]$ is $g \cdot \sum n_\gamma \gamma = \sum n_\gamma \gamma g^{-1}$. Let

$$H^1_\pm(\mathbb{Q}_p, M) = \varinjlim_n \kappa_p(E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \subset \varinjlim_n H^1(\mathbb{Q}_p, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Gamma_n], E[p^\infty])) = H^1(\mathbb{Q}_p, M).$$

Then $H^1_\pm(\mathbb{Q}_p, M)$ is a Λ-submodule of $H^1(\mathbb{Q}_p, M)$. We can rewrite the definition of $S_\pm(E/\mathbb{Q}_\infty)$ as

$$S_\pm(E/\mathbb{Q}_\infty) = \left\{ c \in S(E/\mathbb{Q}_\infty) \ : \ res_p(c) \in H^1_\pm(\mathbb{Q}_p, M) \right\}.$$

3.2.5. *Vista: Iwasawa cohomology and Coleman maps.* The cohomology group

$$H^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(\mathbb{Q}_{p,n}, T),$$

where the inverse limit is taken with respect to the corestriction maps, is often called the Iwasawa cohomology of T. The group $H^1_{\mathrm{Iw}}(T)$ can be identified with $H^1(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda)$, where the $G_{\mathbb{Q}_p}$-action on $T \otimes \Lambda$ is just $\rho \otimes \Psi$. One can define a local subgroup $\mathcal{L}_p \subset H^1(\mathbb{Q}_p, M)$ – to be part of a Selmer structure for M, say – by first defining a subgroup $L_p \subset H^1_{\mathrm{Iw}}(T)$ and taking $\mathcal{L}_p$ to be the annihilator of L_p under the pairing of local Tate duality. In many cases of interest, the group L_p is the kernel of a Λ-homomorphism $H^1_{\mathrm{Iw}}(T) \to \Lambda$ (or something similar) which is often called a Coleman map. This is true, for example, of the local conditions at p defining the Selmer groups $S(E/\mathbb{Q}_\infty)$, when E has ordinary reduction at p, and $S_\pm(E/\mathbb{Q}_\infty)$, when E has supersingular reduction at p. For the latter see [38], and for a more general discussion see [40].

3.3. $S_?(E/F_\infty)$ **as a Λ-module.** The group $H = H^1(G_{F,\Sigma}, M)$ has a natural structure as a discrete Λ-module. So its Pontryagin dual $X = \mathrm{Hom}_{cts}(H, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact Λ-module, with the Λ-action being $(\lambda \cdot f)(x) = f(\lambda x)$. Similarly, the submodule $S(E/\mathbb{Q}_\infty) \subset H$ is a discrete Λ-module and its Pontryagin dual

$$X_?(E/F_\infty) = \mathrm{Hom}_{cts}(S_?(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p), \quad ? = \emptyset, \mathrm{Gr}, \mathrm{BDP}, \text{ or } \pm,$$

which is a quotient of X, is a compact Λ-module. (Of course, by $? = \emptyset$ we mean no subscript.)

Proposition 2. *X is a finitely-generated Λ-module.*

Proof. We will prove this by induction on the $\mathbb{Z}_p$-rank d of $\Gamma \cong \mathbb{Z}_p^d$.

Suppose first that $d = 0$. Then $H = H^1(G_{F,\Sigma}, E[p^\infty])$ and we want to show that $X = \mathrm{Hom}_{cts}(H, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely-generated $\mathbb{Z}_p$-module. By the compactness of X and Nakayama's lemma, it suffices to show that X/pX is a finite. And by duality the latter is equivalent to the finiteness of $H[p]$. From the short exact sequence $0 \to E[p] \to E[p^\infty] \xrightarrow{p} E[p^\infty] \to 0$ we obtain a surjection $H^1(G_{F,\Sigma}, E[p]) \twoheadrightarrow H^1(G_{F,\Sigma}, E[p^\infty])[p] = H[p]$. We have already observed that $H^1(G_{F,\Sigma}, E[p])$ is finite, hence $H[p]$ is finite.

For the induction step, let γ belong to a topological generating set of Γ. Then $\Gamma' = \Gamma/\overline{\langle\gamma\rangle} \cong \mathbb{Z}_p^{d-1}$, and $\Lambda/(\gamma-1)\Lambda = \mathbb{Z}_p[\![\Gamma']\!] = \Lambda'$. Note that $M[\gamma-1] = T \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{cts}(\Lambda/(\gamma-1)\Lambda, \mathbb{Q}_p/\mathbb{Z}_p) = T \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{cts}(\Lambda', \mathbb{Q}_p/\mathbb{Z}_p) = M'$. From the short exact sequence $0 \to M' \to M \xrightarrow{\gamma-1} M \to 0$ we obtain a surjection $H^1(G_{F,\Sigma}, M') \to H^1(G_{F,\Sigma}, M)[\gamma-1]$, and so by duality an injection $X/(\gamma-1)X \hookrightarrow \mathrm{Hom}_{cts}(H^1(G_{F,\Sigma}, M'), \mathbb{Q}_p/\mathbb{Z}_p) = X'$. By the induction hypothesis, X' is a finitely-generated Λ'-module, hence $X/(\gamma-1)X$ is a finitely-generated Λ'-module (by the Noetherian-ness of Λ'). That X is a finitely-generated Λ-module follows from Nakayama's lemma as before. □

Corollary 3. *Let $\mathcal{S} \subset H^1(G_{F,\Sigma}, M)$ be a Λ-submodule. Its Pontryagin dual $\mathcal{X} = \mathrm{Hom}_{cts}(\mathcal{S}, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely-generated Λ-module. In particular, $X_?(E/F_\infty)$ is a finitely-generated Λ-module.*

There is a structure theorem for finitely-generated Λ-modules that is reminiscent of finitely-generated modules over a PID. Such a Λ-module X admits a Λ-homomorphism

$$X \to \Lambda^r \oplus \prod_{i=1}^s \Lambda/(f_i), \quad f_i \neq 0,$$

with pseudonull kernel and cokernel. Pseudonull means that the localizations at all height one primes of Λ are zero; if $d = 1$, then finitely-generated and pseudonull is equivalent to finite order. The integer r is uniquely determined and is called the Λ-rank of X; we will denote it by $r(X)$. The ideal $\xi(X) = (f_1 \cdots f_s) \subset \Lambda$ is also uniquely determined. The characteristic ideal $\xi(X) \subseteq \Lambda$ of the Λ-module X is 0 if $r > 0$ and is the ideal $(f_1 \cdots f_s)$ if $r = 0$.

One useful result, which points to the utility of this structure theorem is:

Lemma 4. *Suppose $d = 1$ (so $\Lambda \cong \mathbb{Z}_p[\![T]\!]$). Let X be a finitely-generated, torsion Λ-module with no non-zero pseudonull submodule. Let $0 \neq \lambda \in \Lambda$. Then*

$$\#X/\lambda X = \#\Lambda/(\xi(X), \lambda).$$

In particular, if $f \in \xi(X)$ is a generator, then

$$\#X/(\gamma - 1)X = \#\mathbb{Z}_p/f(0).$$

These equalities should be understood to mean that if one side is infinite then so is the other.

The proof of this lemma essentially amounts to multiplying the exact sequence

$$0 \to X \to \prod_{i=1}^{s} \Lambda/(f_i) \to \text{coker} \to 0$$

by λ and appealing to the snake lemma and noting that coker has finite order and so $\#\text{coker}[\lambda] = \#\text{coker}/\lambda\text{coker}$.

Some natural questions to ask about $X = X(E/F_\infty)$:

- What is $r(X)$? Is it ever 0? positive?
- What is $\xi(X)$?
- Does X have a non-zero pseudonull Λ-submodule?

The Iwasawa theory of elliptic curves is partly focused on answering these questions. The arithmetic significance of the answers will become more clear as we go on.

3.3.1. *Vista: Selmer groups of p-adic deformations.* The Iwasawa modules $S_?(E/F_\infty)$ that we have defined are some of the simplest examples of Selmer groups for p-adic deformations. In this case the deformation is $T_pE \otimes_{\mathbb{Z}_p} \Lambda$ (with G_F acting as $\rho \otimes \Psi^{-1}$), which deforms the twist of T_pE by the trivial character by the universal G_F-character that factors through Γ. Other possible deformations could include deforming T_pE. Here we use 'deformation' in the sense of Greenberg [22]; the reader should consult *op. cit.* for more on Selmer groups in this context.

3.3.2. *Horizon: Selmer complexes.* Nekovář [51] developed a formalism for Iwasawa theory based on 'big Galois representations' (such as $T \otimes \mathbb{Z}_p\Lambda$) and their cohomological invariants, working within the framework of derived categories. This both recovers and extends many of the results about Selmer groups, leading to generalized Cassels–Tate pairings and generalized p-adic height pairings, among many others. The epigraph following the introduction: '*Selmer groups are dead. Long live Selmer complexes.*'

3.4. **Control theorems.** It is natural to ask whether the group $\mathrm{Sel}_{p^\infty}(E/F)$ can be recovered from $S(E/F_\infty)$. Certainly, there is a canonical map $\mathrm{Sel}_{p^\infty}(E/F) \to S(E/F_\infty)$ with image in the Γ-invariants $S(E/F_\infty)^\Gamma = S(E/F_\infty)[\gamma_1 - 1, \cdots, \gamma_d - 1]$. How are these two groups related? The answer to this is a case of what is often called a 'control theorem.'

Instead of proving the most general theorems, we concentrate on some important cases. To make our task easier, we will always assume

$$(\mathrm{irred}_F) \qquad\qquad E[p] \text{ is an irreducible } G_F\text{-representation.}$$

Under this assumption it is not hard to deduce that if $x_1, ..., x_j \in \Lambda$, then the natural map

$$H^1(G_\Sigma, M[x_1, ..., x_j]) \xrightarrow{\sim} H^1(G_\Sigma, M)[x_1, ..., x_j]$$

is an isomorphism. And using that F_∞/F is unramified at each $v \nmid p$ one can also deduce that if $x_1, ..., x_j$ is a regular sequence, then

$$H^1(I_v, M[x_1, ..., x_j]) \xrightarrow{\sim} H^1(I_v, M)[x_1, ..., x_j], \quad v \nmid p.$$

3.4.1. $S(E/\mathbb{Q}_\infty)$*: ordinary case.* Suppose that $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p. Let $M^- = T/T^+ \otimes_{\mathbb{Z}_p} \Lambda^\vee$, and let

$$\mathcal{P}_\Sigma = \prod_{\ell \in \Sigma} \mathcal{P}_\ell, \quad \mathcal{P}_\ell = \begin{cases} H^1(I_\ell, M)^{G_{\mathbb{Q}_\ell}} & \ell \neq p \\ H^1(I_p, M^-)^{G_{\mathbb{Q}_p}} & \ell = p. \end{cases}$$

Then $S(E/\mathbb{Q}_\infty) = \ker\left\{H^1(G_\Sigma, M) \xrightarrow{res} \mathcal{P}_\Sigma\right\}$. Let

$$P_\Sigma = \prod_{\ell \in \Sigma} P_\ell, \quad P_\ell = \begin{cases} H^1(\mathbb{Q}_\ell, E[p^\infty]) & \ell \neq p \\ \frac{H^1(\mathbb{Q}_p, E[p^\infty])}{\mathrm{im}\left\{H^1(\mathbb{Q}_p, T^+ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathbb{Q}_p, E[p^\infty])\right\}_{\mathrm{div}}} & \ell = p. \end{cases}$$

Then there is an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \mathrm{im}\left\{H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} P_\Sigma\right\} \cap \ker\left\{P_\Sigma \to \mathcal{P}_\Sigma[\gamma - 1]\right\}.$$

If $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module, then using global Tate duality one can show that $H^1(G_\Sigma, M) \xrightarrow{res} \mathcal{P}_\Sigma$ is surjective, hence $S(E/\mathbb{Q}_\infty)[\gamma - 1] = \ker\left\{H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} \mathcal{P}_\Sigma[\gamma - 1]\right\}$. It follows that the displayed sequence is exact on the right. And if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, then one can similarly show that $H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} P_\Sigma$ is surjective. This yields:

Proposition 5 (Control Theorem for the ordinary case)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \ker\left\{P_\Sigma \to \mathcal{P}_\Sigma[\gamma - 1]\right\} \to 0.$$

To be precise, the arguments above actually show that if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, then $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module.

Let $K_\ell = \ker\left\{P_\ell \to \mathcal{P}_\ell\right\}$. Then as a consequence of Proposition 5:

Corollary 6. *Under the assumptions of the preceding proposition,*

$$\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \cdot \prod_{\ell \in \Sigma} \#K_\ell.$$

The orders of the groups K_ℓ are readily computed. Suppose first that $\ell \nmid p$. Then from the earlier observation that $H^1(I_\ell, E[p^\infty]) \xrightarrow{\sim} H^1(I_\ell, M)[\gamma - 1]$, it follows that

$$\#K_\ell = \#H^1(\mathbb{F}_\ell, E[p^\infty]^{I_\ell}) = \begin{cases} |c_\ell(E/\mathbb{Q})|_p^{-1} & \ell \mid N_E, \ell \neq p \\ 1 & \ell \nmid N_E, \end{cases}$$

where N_E is the conductor of E, and $c_\ell(E/\mathbb{Q})$ is the Tamagawa factor at ℓ for $E/\mathbb{Q}$. Now suppose that E has good ordinary reduction at p. Then a straightforward but more involved calculation shows that

$$\#K_p = (\#\mathbb{Z}_p/(1 - \alpha_p))^2,$$

where again α_p is the p-adic unit root of $x^2 - a_p(E)x + p$. As $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = Ш(E/\mathbb{Q})[p^\infty]$ when Sel_{p^∞} is finite, we can now restate the preceding corollary as:

Corollary 7. *Under the assumptions of the preceding proposition and assuming that E has good ordinary reduction at p,*

$$\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \left| (1 - \alpha_p)^2 \cdot \#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell | N_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}.$$

More generally, let $\psi_\zeta : G_\mathbb{Q} \to \Gamma \xrightarrow{\gamma \mapsto \zeta} \overline{\mathbb{Q}}_p^\times$ be the finite order character sending γ (or any lift of it) to the pth-power root of unity ζ. One can also compare $(S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}[\zeta])[\gamma - \zeta]$ to $\mathrm{Sel}(E, \psi_\zeta^{-1})$ in a similar way. Doing so yields:

Proposition 8 (Control Theorem for twists in the ordinary case)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Let ζ be a pth-power root of unity. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}(E, \psi_\zeta^{-1})$ is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}(E, \psi_\zeta^{-1}) \to (S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}[\zeta])[\gamma - \zeta] \to \ker\left\{ P_{\Sigma,\zeta} \to (\mathcal{P}_\Sigma \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta])[\gamma - \zeta] \right\} \to 0.$$

Here $P_{\Sigma,\zeta} = \prod_{\ell \in \Sigma} P_{\ell,\zeta}$ with $P_{\ell,\zeta}$ defined just as P_ℓ but with $E[p^\infty]$ replaced with the group $W = E[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta]$ with $G_\mathbb{Q}$ acting as $\rho \otimes \psi_\zeta^{-1}$.

Both of these propositions are particularly useful if $X(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodule. If this is so, then by Lemma 4 the order of $S(E/\mathbb{Q}_\infty)[\gamma - 1]$, which is the order of $X(E/\mathbb{Q}_\infty)/(\gamma - 1)X(E/\mathbb{Q}_\infty)$, equals the order of $\mathbb{Z}_p/(g_E(0))$ for any generator g_E of $\xi(E/\mathbb{Q}_\infty)$. This highlights the utility of the next proposition.

Proposition 9 (No pseudonull submodule)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module. Then $X(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodules.*

Combining these results we conclude:

Proposition 10. *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Let g_E be a generator of the characteristic ideal $\xi(E/\mathbb{Q}_\infty)$. Then*

$$|g_E(0)|_p^{-1} = \#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \left| (1 - \alpha_p)^2 \cdot \#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell | N_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}.$$

This result can be extended to cover the case of multiplicative reduction and even to allow for $E[p^\infty]^{G_{\mathbb{Q}}} \neq 0$. This as well as many details can be found in the papers of Greenberg (see especially [23, Thm. 4.1] and also [63, § 3.2]).

3.4.2. $S_{\mathrm{Gr}}(E/K_\infty)$. Let $\gamma_\pm \in \Gamma_K^\pm \subset \Gamma_K = \mathrm{Gal}(K_\infty/K)$ be topological generators such that γ_+ maps to γ in $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. The next proposition relates $\mathrm{Sel}_{\mathrm{Gr}}(E/K_\infty)[\gamma_+ - 1]$ and $\mathrm{Sel}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. Let $\Lambda_K = \mathbb{Z}_p[\![\Gamma_K]\!]$ and $\Lambda_{\mathrm{ac}} = \mathbb{Z}_p[\![\Gamma^-]\!] = \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)]\!]$.

Proposition 11. *Suppose E has either good or multiplicative reduction at p and that* (irred_K) *holds. Suppose that* (split) *holds. Suppose also that $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module. Let Σ^- be the set of primes at which E has bad reduction and which are inert in K. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \to S_{\mathrm{Gr}}(E/K_\infty)[\gamma_+ - 1] \to \prod_{\ell \in \Sigma^-} H^1_{\mathrm{ur}}(K_\ell, M_{\mathrm{ac}}) \times H_{\bar{v}} \to 0,$$

where

$$H_{\bar{v}} = \ker\left\{H^1(K_{\bar{v}}, M_{\mathrm{ac}}) \to H^1(K_{\bar{v}}, \mathcal{M})[\gamma_+ - 1]\right\} \cong M^{G_{\bar{v}}}.$$

Note that $H_{\bar{v}}$ has finite order and is even trivial if E has supersingular reduction at p. On the other hand, for $\ell \in \Sigma^-$, $H^1_{\mathrm{ur}}(K_\ell, M^{\mathrm{ac}}) \cong \mathrm{Hom}_{cts}(\Lambda_{\mathrm{ac}}, E[p^\infty]^{I_\ell})$. The characteristic ideal of the dual of this last group is $(c_\ell(E/K)) \subset \Lambda_{\mathrm{ac}}$, the ideal generated by the Tamagawa number of E/K at the prime ℓ.

The proof of Proposition 11 proceeds along the lines of the proof of Proposition 5.

3.4.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. We assume that (split) holds. The Selmer group $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ was defined so as to closely interpolate the Selmer groups for twists of V_pE by anticyclotomic characters $\chi : G_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}} \to \mathcal{O}^\times$ with Hodge–Tate weight > 1 at v (and so < -1 at $\bar{v}$). So it would be natural to formulate a control theorem relating such a Selmer group to $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - \chi(\gamma)]$. We leave it to the interested reader to do so. Instead we consider the Selmer group $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ defined to be the group

$$\ker\left\{H^1(G_{K,\Sigma}, E[p^\infty]) \overset{res}{\to} \prod_{w \in \Sigma, w \nmid p} H^1(K_w, E[p^\infty]) \times \frac{H^1(K_v, E[p^\infty])}{H^1(K_v, E[p^\infty])_{\mathrm{div}}} \times H^1(K_{\bar{v}}, E[p^\infty])\right\}.$$

Note that $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ is not a Bloch–Kato Selmer group: the local condition at the places $w \mid p$ is not that imposed by the Bloch–Kato subgroup $H^1_f(K_w, E[p^\infty])$. However, $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ is defined by a Selmer structure.

The control theorem of interest to us is:

Proposition 12. *Suppose E has good reduction at p and that* (irred_K) *holds. Suppose that* (split) *holds. Suppose also that $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ has finite order. Let Σ^+ be the set of places of K of residue degree 1 at which E has bad reduction. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{\mathrm{BDP}}(E/K) \to S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - 1] \to \prod_{w \in \Sigma^+} H^1_{\mathrm{ur}}(I_w, E[p^\infty]) \times K_v \times K_{\bar{v}} \to 0,$$

where

$$H_v = H^1(K_v, E[p^\infty])/H^1(K_v, E[p^\infty])_{\mathrm{div}} \cong H^1(K_v, T_pE)^\vee_{\mathrm{tors}} \cong H^0(K_v, E[p^\infty])^\vee,$$

and

$$H_{\bar{v}} = \ker\left\{H^1(K_{\bar{v}}, E[^\infty]) \to H^1(K_{\bar{v}}, M_{\mathrm{ac}})[\gamma_- - 1]\right\} \cong M_{\mathrm{ac}}^{G_{K_{\bar{v}}}}/(\gamma_- - 1)M_{\mathrm{ac}}^{G_{K_{\bar{v}}}}.$$

Note that $\#H_{\bar{v}} = \#H^0(K_{\bar{v}}, E[p^\infty])$. In particular, both H_v and $H_{\bar{v}}$ are trivial if E has supersingular reduction at p and otherwise both have order equal to $\#\mathbb{Z}_p/(1 - a_p(E) + p)$.

Write $N_E = N^+N^-$ with N^+ divisible by primes split or ramified in K and N^- divisible by primes inert in K.

Corollary 13. *Under the hypotheses of the preceding proposition,*

$$|\#S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - 1]|_p^{-1} = \left|\#\mathrm{Sel}_{\mathrm{BDP}}(E/K) \cdot \prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2 \cdot \delta_p(E)^2\right|_p^{-1},$$

where $\delta_p(E) = 1$ if E has supersingular reduction at p, and $\delta_p(E) = 1 - a_p(E) + p$ if E has good ordinary reduction at p.

3.4.4. $S_\pm(E/\mathbb{Q}_\infty)$. Kobayashi established a control theorem for the $\pm$-Selmer groups $S_\pm(E/\mathbb{Q}_\infty)$ which is the obvious analog of Proposition 5.

Proposition 14 (Control Theorem for the supersingular case)**.** *Suppose $E/\mathbb{Q}$ has good supersingular reduction at p with $a_p(E) = 0$ and that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S_\pm(E/\mathbb{Q}_\infty)[\gamma - 1] \to \prod_{\ell\in\Sigma, \ell\neq p} \ker\{P_\ell \to \mathcal{P}_\ell[\gamma - 1]\} \to 0.$$

Under the hypothesis that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module, B.D. Kim [35] has shown that $X_\pm(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodule. As a consequence, just as in the ordinary case, we have

Proposition 15. *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p and that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Let $g_{E,\pm}$ be a generator of the characteristic ideal $\xi_\pm(E/\mathbb{Q}_\infty) = \xi(X_\pm(E/\mathbb{Q}_\infty))$. Then*

$$|g_{E,\pm}(0)|_p^{-1} = \#S_\pm(E/\mathbb{Q}_\infty)[\gamma - 1] = \left|\#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell|N_E} c_\ell\right|_p^{-1}.$$

4. Main Conjectures

The Main Conjectures for elliptic curves generally have two ingredients: the characteristic ideal of the dual of the Selmer group and a related p-adic L-function, ideally both in some Λ. Then the conjecture generally has two parts: the torsion-ness over Λ of the dual of the Selmer group (and hence the non-vanishing of the characteristic ideal) and the assertion that the p-adic L-function generates the characteristic ideal. In some cases it is also possible to formulate a Main Conjecture 'without L-functions.' This generally means that the p-adic L-function has been replaced with some appropriate element in an Iwasawa cohomology group (a universal norm). These elements often come from an Euler system. The Main Conjectures without L-functions have proven useful in relating different Main Conjectures.

Let E be an elliptic curve over $\mathbb{Q}$. In the preceding section we defined Selmer groups for E and certain $\mathbb{Z}_p^d$-extensions F_∞/F. In the following we recall the Main Conjectures for these groups. In order to do so it is helpful to recall some facts about E and its L-series.

Recall that E is modular. This means there is a weight 2 newform $f_E \in S_2(\Gamma_0(N_E))$, where N_E is the conductor of E, such that the Fourier expansion $f_E = \sum_{n=1}^\infty a_n q^n$ has coefficients in $\mathbb{Z}$ and $L(E,s) = L(f_E,s) = \sum_{n=1}^\infty a_n n^{-s}$. It also means that there exists a surjective morphism $\phi_E : X_0(N_E) \to E$ over $\mathbb{Q}$ under which the ∞ cusp is mapped to the identity element (that is, the point at infinity) of E. The pullback under ϕ_E of a Néron differential ω_E of E satisfies $\phi_E^*\omega_E = c2\pi i f_E(\tau)d\tau = c\omega_{f_E}$, for some non-zero constant c.

4.1. **p-adic L-functions.** We first recall the p-adic L-functions that appear in the statements of the Main Conjectures.

4.1.1. *$\mathcal{L}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}(E/K_\infty)$.* We begin with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We assume that E has good ordinary or multiplicative reduction at p.

Given a primitive p^tth-power root of unity ζ, recall that ψ_ζ is the finite order character of $G_\mathbb{Q}$ obtained by projecting to $\Gamma_\mathbb{Q}$ and composing with the character of $\Gamma_\mathbb{Q}$ that sends γ to ζ. Similarly, $\phi_\zeta : \Lambda \to \mathbb{Z}_p[\zeta] \subset \overline{\mathbb{Q}}_p$ is the homomorphism sending $\gamma \in \Gamma$ to ζ (so the homomorphism of $\Lambda_\mathbb{Q} = \mathbb{Z}_p[\![T]\!]$ sending T to $\zeta - 1$). We also denote by ψ_ζ the Dirichlet character of $(\mathbb{Z}/p^{t+1}\mathbb{Z})^\times$ such that image of $\gamma \in 1+p\mathbb{Z}_p$ is sent to ζ (unless $t = 0$, in which case ψ_1 is the trivial character).

There exists an element $\mathcal{L}(E/\mathbb{Q}_\infty) \in \Lambda_\mathbb{Q} = \mathbb{Z}_p[\![\Gamma_\mathbb{Q}]\!]$ such that for any primitive p^tth root of unity ζ,

$$\phi_\zeta(\mathcal{L}(E/\mathbb{Q}_\infty)) = e_p(\zeta)\frac{L(f_E,\psi_\zeta^{-1},1)}{\Omega_{f_E}},$$

where Ω_{f_E} is a certain (essentially canonical) period of f_E and

$$e_p(\zeta) = \begin{cases} \alpha_p^{-(t+1)}\frac{p^{t+1}}{G(\psi_\zeta^{-1})} & \zeta \neq 1 \\ \alpha_p^{-1}\left(1-\frac{1}{\alpha_p}\right)^{m_p} & \zeta = 1. \end{cases}$$

Here $L(f_E,\psi_\zeta^{-1},s)$ is the twist of the L-function of f_E by the Dirichlet character ψ_ζ^{-1}. Also, α_p is the p-adic unit root of $x^2 - a_p(E)X + p$ if E has good ordinary reduction at p and $\alpha = a_p(E) \in \{\pm 1\}$ if E has multiplicative reduction at p, $G(\psi_\zeta^{-1})$ is the Gauss sum, and $m_p = 2$ if E has good reduction at p and $m_p = 1$ if E has multiplicative reduction. This is the p-adic L-function of f_E first constructed by Amice-Vélu and Vishik (see also [46]).

Let K be an imaginary quadratic field and suppose that (split) holds (for simplicity). There exists an element $\mathcal{L}(E/K_\infty) \in \Lambda_K$ defined by an interpolation property for finite characters of Γ_K that is analogous to that of $\mathcal{L}(E/\mathbb{Q}_\infty)$. A construction of this p-adic L-function can be made through p-adic interpolation of Rankin–Selberg integrals, as done by Perrin-Riou [54] (see also [64]), or via modular symbols along the lines of the construction of $\mathcal{L}(E/\mathbb{Q}_\infty)$ by Amice-Vélu and Vishik (cf. [43]). The p-adic L-functions $\mathcal{L}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}(E/K_\infty)$ are related by

$$\mathcal{L}(E/\mathbb{Q}_\infty)\mathcal{L}(E^K/\mathbb{Q}_\infty) = \mathcal{L}(E/K_\infty) \bmod (\gamma_- - 1). \tag{L-fact}$$

Here E^K is the K-twist of E (so $L(E^K,s) = L(E,\chi_K,s)$, where χ_K is the quadratic Dirichlet character associated with $K/\mathbb{Q}$).

4.1.2. $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$. We assume that (split) holds. For simplicity we will assume that the conductor N_E of E and the discriminant $-D_K$ of K are relatively prime and neither is divisible by p (this just simplifies some formulas).

Let $\Xi_{\mathrm{Gr}} \subset \mathrm{Hom}_{cts}(\Gamma_K, \overline{\mathbb{Q}}_p^\times)$ be the subset of characters such that the composition $G_K \twoheadrightarrow \Gamma_K \xrightarrow{\chi} \overline{\mathbb{Q}}_p$ is crystalline at both v and $\bar{v}$ and such that the Hodge–Tate weight at v is < -1 and at $\bar{v}$ is > 1. These are the Galois characters associated with unramified algebraic Hecke characters ψ of K such that the restriction of ψ to $(K \otimes \mathbb{R})^\times = \mathbb{C}^\times$ is just $z^n \bar{z}^{-m}$ for integers $n, m > 1$ and such that $n, m \equiv 0 \bmod p-1$. Given $\chi \in \Xi_{\mathrm{Gr}}$ we will write χ_{alg} for the corresponding algebraic Hecke character (so $\sigma_{\chi_{\mathrm{alg}}} = \chi$).

Let $\Lambda_K^{\mathrm{ur}} = \Lambda_K \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$, where $\mathbb{Z}_p^{\mathrm{ur}}$ is the p-adic completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$. Let $\chi : \Gamma_K \to \overline{\mathbb{Q}}_p^\times$ be a continuous character. Then χ determines a $\mathbb{Z}_p^{\mathrm{ur}}$-homomorphism $\phi_\chi : \Lambda_K^{\mathrm{ur}} = \mathbb{Z}_p^{\mathrm{ur}}[\![\Gamma_K]\!] \to \widehat{\overline{\mathbb{Q}}}_p$ by linear extension (it is the unique $\mathbb{Z}_p^{\mathrm{ur}}$-homomorphism such that $\phi_\chi(\gamma) = \chi(\gamma)$ for all $\gamma \in \Gamma_K \subset \Lambda_K^\times$).

There exists an element $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty) \in \Lambda_K^{\mathrm{ur}}$ such that for any $\chi \in \Xi_{\mathrm{Gr}}$,

$$\phi_\chi(\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) = c(\chi) \cdot E(f, \chi) \cdot \pi^{2n-1} \left(\frac{\Omega_{K,p}}{\Omega_{K,\infty}} \right)^{2(n+m)} L(f_E, \chi_{\mathrm{alg}}^{-1}, 1),$$

where

$$E(f,\chi) = (1 - a_p(E)\chi_{\mathrm{alg}}(\varpi_v)^{-1}p^{-1} + \chi_{\mathrm{alg}}(\varpi_v)^{-2}p^{-1})(1 - a_p(E)\chi_{\mathrm{alg}}(\varpi_{\bar{v}})p^{-1} + \chi_{\mathrm{alg}}(\varpi_{\bar{v}})^2 p^{-1}),$$

with ϖ_v and $\varpi_{\bar{v}}$ respective uniformizers at v and $\bar{v}$, $c(\chi)$ is a product of powers of 2, i, N, and D_K that depend on on n and m but do not matter for our applications (as these factors are all prime to p), and $\Omega_{K,\infty}$ and $\Omega_{K,p}$ are, respectively, archimedean and p-adic CM periods associated to K. While the latter depend on choices, these choices only change the factors by a multiple of $(\mathbb{Z}_p^{\mathrm{ur}})^\times$.

As in the case of the p-adic L-function $\mathcal{L}(E/\mathbb{Q}_\infty)$, there exists an interpolation formula for characters $\chi : \Gamma_K \to \overline{\mathbb{Q}}_p^\times$ that are ramified at v or $\bar{v}$ but the same restrictions on Hodge–Tate weights. However, we will not go into this here.

There are essentially two constructions of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (and the two are closely related). The first realizes $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ as a special case of Hida's construction of p-adic Rankin–Selberg L-functions [29] involving a Hida family of CM eigenforms. The other realizes $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ as a p-adic L-function for a cuspform on a definite unitary group $U(2)$, constructed via the doubling method (see [70] and [16]).

Remark 4.1.2.a. It is possible to define a slight modification of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ that is actually an element of Λ_K and not just Λ_K^{ur}. This requires normalizing the L-values by a 'congruence period' for the anticyclotomic character $\chi_{\mathrm{alg}}^{\mathrm{c}}/\chi_{\mathrm{alg}}$, but the result is less canonical.

Remark 4.1.2.b. It is also possible to construct $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ when $p \mid N_E$ or when $(N_E, D_K) \neq 1$, but the result is more cumbersome to write down.

4.1.3. $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. We again assume that (split) holds and that the conductor N_E of E and the discriminant $-D_K$ of K are relatively prime, and neither is divisible by p. We also assume that $(\mathrm{irred})_{\mathbb{Q}}$ holds (as with the other hypotheses, this is mostly to simplify formulas). We make

the additional assumption that

(Heeg)
- $N_E = N^+N^-$ with N^+ divisible only by primes that split in K and N^- divisible only by primes that are inert in E;
- N^- is the squarefree product of an even number of distinct primes.

This is essentially the Heegner hypothesis. It ensures that the root number $w(E/K)$ equals -1, among other things. It also ensures that the sign of the functional equation of $L(f_E, \chi_{\mathrm{alg}}^{-1}, s)$ is $+1$ for any (anticyclotomic) character $\chi \in \Xi_{\mathrm{Gr}}$ that factors through Γ_K^{ac}.

Let $\Xi_{\mathrm{BDP}} \subset \mathrm{Hom}_{cts}(\Gamma_K^{\mathrm{ac}}, \overline{\mathbb{Q}}_p^\times)$ be the subset of characters such that the composition $G_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}} \xrightarrow{\chi} \overline{\mathbb{Q}}_p$ is crystalline at both v and $\bar{v}$ and such that the Hodge–Tate weight at v is < -1 and at $\bar{v}$ is > 1. These are the Galois characters associated with unramified algebraic Hecke characters ψ of K such that the restriction of ψ to $(K \otimes \mathbb{R})^\times = \mathbb{C}^\times$ is just $(z/\bar{z})^n$ for and integer $n > 1$ and such that $n \equiv 0 \bmod p-1$. Note that these are also just the $\chi \in \Xi_{\mathrm{Gr}}$ that factor through the projection $\Gamma_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}}$.

Let $\Lambda_{\mathrm{ac}}^{\mathrm{ur}} = \Lambda_{\mathrm{ac}} \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$. There exists an element $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \in \Lambda_{\mathrm{ac}}^{\mathrm{ur}}$ such that for any $\chi \in \Xi_{\mathrm{BDP}}$,

$$\phi_\chi(\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) = c(\chi) \cdot E(f,\chi) \cdot \pi^{2n-1} \left(\frac{\Omega_{K,p}}{\Omega_{K,\infty}}\right)^{4n} L(f_E, \chi_{\mathrm{alg}}^{-1}, 1) \prod_{\ell | N^-} c_\ell(E/K)^{-1},$$

where $E(f,\chi)$ and $c(\chi)$ are is in the interpolation formula for $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$, and $c_\ell(E/K)$ is the Tamagawa number for E/K at the prime ℓ of K.

This p-adic L-function was essentially constructed in [4] and [6] as the *square* of another p-adic funtion. This second p-adic L-function interpolates weighted sums of the values on CM points on a Shimura curve of powers of the Maass–Shimura operator applied to the modular form f_E (or of a Jacquet–Langlands transfer of f_E to the Shimura curve); the weights and the power of the operator vary with χ. This is just a p-adic interpolation of integral formulas of Waldspurger and Gross. The p-adic L-function resulting from the constructions in *op. cit.* may differ from the $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty)$ as we have described by multiplication by a unit in $\Lambda_{\mathrm{ac}}^{\mathrm{ur},\times}$. The factor $\prod_{\ell|N^-} c_\ell(E/K)^{-1}$ arises from the normalization of the Jacquet–Langlands transfer of f_E to the Shimura curve – it is at this point that we use the hypothesis that ($\mathrm{irred}_{\mathbb{Q}}$) holds.

Comparing interpolation formulas it is clear that:

Lemma 16. *Suppose* (split) *holds and that N_E is coprime to D_K and both are prime to p. Suppose also that* (Heeg) *and* ($\mathrm{irred}_{\mathbb{Q}}$) *hold. Then*

$$\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \cdot \prod_{\ell|N^-} c_\ell(E/K) = \mathcal{L}_{\mathrm{Gr}}(E/K_\infty) \bmod (\gamma_+ - 1).$$

We record two other important facts about $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. The first fact is of an Iwasawa-theoretic nature:

Theorem 17 ($\mu = 0$)**.** *Suppose all the hypotheses of Lemma 16 hold. Suppose also that N is squarefree. Then the μ-invariant of $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is 0, that is, $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is non-zero modulo p.*

This theorem was proved by Burungale [7, Thm. B]. Note that this includes the assertion that $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \neq 0$, which is far from obvious!

The second fact is of clear arithmetic import:

Theorem 18 (The BDP formula)**.** *Suppose all the hypotheses of Lemma 16 hold. Suppose also that N is squarefree if $N^- \neq 1$. Then*

$$\phi_1(\mathcal{L}_{\mathrm{BDP}}) = u \left(\frac{1 - a_p(E) + p}{p} \cdot \log_{E(K_v)} y_K \right)^2$$

for some $u \in (\mathbb{Z}_p^{\mathrm{ur}})^\times$.

Here $y_K \in E(K)$ is a Heegner point associated with K and the parametrization of E by the Shimura curve (the same curve that occurs in the construction of $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$), and $\log_{E(K_v)}$ is the log map on the p-adic Lie group $E(K_v)$ defined by the formal group logarithm. Note that the trivial character 1 of Γ_K^{ac} does not belong to Ξ_{BDP}. Theorem 18 follows from the main results of [4] and [6].

4.1.4. $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$. This begins with a closer look at the constructions of Amice-Vélu and Vishik. Let E be an elliptic curve with good reduction at p. Let α_p and β_p be the roots of $x^2 - a_p(E)x + p$. Then Amice-Vélu and Vishik constructed two power series (this construction is also explained in [46])

$$\mathcal{L}(E, \bullet; T) \in \mathcal{H}_{1,\mathbb{Q}_p} = \left\{ \sum_{n=0}^{\infty} a_n T^n \in \mathbb{Q}_p[\![T]\!] \ : \ \lim_{n\to\infty} \frac{|a_n|_p}{n} = 0 \right\}, \bullet \in \{\alpha_p, \beta_p\},$$

with the property that for a primitive p^tth root of unity ζ,

$$\mathcal{L}(E, \bullet; \zeta - 1) = e_p(\zeta, \bullet) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}},$$

where

$$e_p(\zeta, \bullet) = \begin{cases} (\bullet)^{-(t+1)} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} & \zeta \neq 1 \\ \left(1 - \frac{1}{\bullet}\right)^2 & \zeta = 1. \end{cases}$$

However, the $\mathcal{L}(E, \bullet; T)$ do not belong to $\Lambda_{\mathbb{Q}} = \mathbb{Z}_p[\![T]\!]$ unless $\bullet$ is a p-adic unit (which is the case when E has ordinary reduction and $\bullet = \alpha_p$ is the unit root).

Now suppose that $a_p(E) = 0$, so $\beta_p = -\alpha_p$. Let

$$\log_p^+(1+T) = \frac{1}{p} \prod_{n=1}^{\infty} \frac{\Phi_{p^{2n}}(1+T)}{p} \quad \text{and} \quad \log_p^-(1+T) = \frac{1}{p} \prod_{n=1}^{\infty} \frac{\Phi_{p^{2n-1}}(1+T)}{p},$$

where $\Phi_{p^m}(X)$ is the p^mth cyclotomic polynomial. Pollack [52] has shown that there exist $\mathcal{L}_\pm(E/\mathbb{Q}_\infty) \in \Lambda_{\mathbb{Q}}$ such that

$$\mathcal{L}(E, \pm\alpha_p; T) = \log_p^+(1+T) \cdot \mathcal{L}_-(E/\mathbb{Q}_\infty) \pm \alpha_p \log_p^-(1+T) \cdot \mathcal{L}_+(E/\mathbb{Q}_\infty).$$

The functions $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ have the following interpolation property. Suppose ζ is a primitive p^tth root of unity. If $t > 0$ is even, then

$$\phi_\zeta(\mathcal{L}_+(E/\mathbb{Q}_\infty)) = (-1)^{\frac{t+2}{2}} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} \left(\prod_{\text{odd } m=1}^{t-1} \Phi_{p^m}(\zeta)^{-1} \right) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}}.$$

If $t > 0$ is odd, then

$$\phi_\zeta(\mathcal{L}_-(E/\mathbb{Q}_\infty)) = (-1)^{\frac{t+1}{2}} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} \left(\prod_{\text{even } m=2}^{t-1} \Phi_{p^m}(\zeta)^{-1} \right) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}}.$$

Also,

$$\phi_1(\mathcal{L}_+(E/\mathbb{Q}_\infty)) = 2\frac{L(f_E,1)}{\Omega_{f_E}} \quad \text{and} \quad \phi_1(\mathcal{L}_-(E/\mathbb{Q}_\infty)) = (p-1)\frac{L(f_E,1)}{\Omega_{f_E}}.$$

Remark 4.1.4.c. Sprung [66] has extended Pollack's construction to cover the remaining supersingular cases, where $a_p(E) \neq 0$. It is also possible to extend the construction of $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ to two-variable L-functions in Λ_K, at least when (split) holds. This yields 'doubly-signed' p-adic L-functions as it involves the choice of a root of $x^2 - a_p(E)x + p$ for each of the primes above p. Such a construction can be found in [43] (see also [44]).

4.2. **The Main Conjectures.** We are now in a position to state the Main Conjectures we are interested in.

4.2.1. *$S(E/\mathbb{Q}_\infty)$ and $S(E/K_\infty)$.* Let E be an elliptic curve over $\mathbb{Q}$. The Main Conjecture for $S(E/\mathbb{Q}_\infty)$ is just:

Conjecture 19 (The cyclotomic Iwasawa–Greenberg Main Conjecture for E)**.** *Suppose E has good ordinary or multiplicative reduction at p. The Pontryagin dual $X(E/\mathbb{Q}_\infty)$ of $S(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_\mathbb{Q}$-module and its characteristic ideal $\xi(E/\mathbb{Q}_\infty) = \xi(X(E/\mathbb{Q}_\infty))$ is generated by $\mathcal{L}(E/\mathbb{Q}_\infty)$ in $\Lambda_\mathbb{Q} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in $\Lambda_\mathbb{Q}$ if* $(\text{irred}_\mathbb{Q})$ *holds.*

This conjecture can be partially motivated by the combination of control theorems such as Propositions 5 and 8 and the Bloch–Kato conjectures on special values. The latter predicts that $\#(S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta])[\gamma - \zeta]$ should equal $\#\mathbb{Z}_p[\zeta]/\phi_\zeta(\mathcal{L}(E/\mathbb{Q}_\infty))$ – upon using the control theorem to relate the first group order with the size of a Bloch-Kato Selmer group and using the interpolation properties of the p-adic L-function to relate the second group order to a special value of an L-function. And since the first group order should be (upon assuming torsion-ness and no non-zero pseudonull submodule) $\#\mathbb{Z}_p[\zeta]/\phi_\zeta(g_E)$, for $g_E \in \xi(E/\mathbb{Q}_\infty)$ a generator, the most optimistic (and reasonable) conjecture to make is that g_E can be taken to be $\mathcal{L}(E/\mathbb{Q}_\infty)$.

The main conjecture for $S(E/K_\infty)$ is:

Conjecture 20 (The 2-variable Iwasawa–Greenberg Main Conjecture for E/K)**.** *Suppose E has good ordinary or multiplicative reduction at p. The Pontryagin dual $X(E/K_\infty)$ of $S(E/K_\infty)$ is a torsion Λ_K-module and its characteristic ideal $\xi(E/K_\infty) = \xi(X(E/K_\infty))$ is generated by $\mathcal{L}(E/K_\infty)$ in $\Lambda_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_K if* (irred_K) *holds.*

4.2.2. *$S_{\text{Gr}}(E/K_\infty)$.* At this point it should be easy to guess what the main conjecture for $S_{\text{Gr}}(E/K_\infty)$ is:

Conjecture 21 (The two-variable Iwasawa–Greenberg Main Conjecture for $S_{\text{Gr}}(E/K_\infty)$)**.** *Suppose E has good reduction at p. Let K be an imaginary quadratic field such that* (split) *holds. The Pontryagin dual $X_{\text{Gr}}(E/K_\infty)$ of $S_{\text{Gr}}(E/K_\infty)$ is a torsion Λ_K-module and its characteristic ideal $\xi_{\text{Gr}}(E/K_\infty) = \xi(X_{\text{Gr}}(E/K_\infty))$ is generated by $\mathcal{L}_{\text{Gr}}(E/K_\infty)$ in $\Lambda_K^{\text{ur}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_K^{ur} if* (irred_K) *holds.*

Note that unlike Conjecture 19, this conjecture allows E to have supersingular reduction at p.

4.2.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. An obvious variant on Conjecture 21 is:

Conjecture 22 (The anticyclotomic Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$)**.** *Suppose E has good or multiplicative reduction at p. Let K be an imaginary quadratic field such that* (split) *holds. The Pontryagin dual $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ of $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module and its characteristic ideal $\xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = \xi(X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}))$ is generated by $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ in $\Lambda_{\mathrm{ac}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_{ac} if* (irred_K) *holds.*

Remark 4.2.3.a. Proposition 11 and Lemma 16 show that Conjectures 21 and 22 are closely connected. In particular, under the hypotheses of Lemma 16, it follows that Conjecture 21 implies Conjecture 22.

4.2.4. $S_\pm(E/\mathbb{Q}_\infty)$. Finally, we state the Main Conjecture for the $\pm$-Selmer groups:

Conjecture 23 (The cyclotomic $\pm$-Iwasawa Main Conjecture for E)**.** *Suppose E has supersingular reduction at p and $a_p(E) = 0$. The Pontryagin dual $X_\pm(E/\mathbb{Q}_\infty)$ of $S_\pm(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and its characteristic ideal $\xi_\pm(E/\mathbb{Q}_\infty) = \xi(X_\pm(E/\mathbb{Q}_\infty))$ is generated by $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ in $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in $\Lambda_{\mathbb{Q}}$ if* $(\mathrm{irred}_{\mathbb{Q}})$ *holds.*

4.3. **Main Conjectures without L-functions.** The classical Main Conjecture of Iwasawa theory has an equivalent formulation that does not involve p-adic L-functions. Following especially [34, §12], analogous formulations exist for the Main Conjectures of elliptic curves. In the rest of this section we give a rough description of this in some of the cases already considered in these lectures.

Let $E/\mathbb{Q}$ be an elliptic curve. We will assume that E has good ordinary reduction at p.

4.3.1. *The cyclotomic Main Conjecture.* For simplicity, we also assume $(\mathrm{irred}_{\mathbb{Q}})$ holds. Let

$$H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) = \ker\left\{ H^1(G_\Sigma, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) \overset{res}{\to} \prod_{\ell \in \Sigma, \ell \neq p} H^1(I_\ell, T \otimes \Lambda_{\mathbb{Q}}) \right\}.$$

Here we let $G_{\mathbb{Q}}$ act on $T \otimes \Lambda_{\mathbb{Q}}$ via $\rho \otimes \Psi$. Let

$$S_{\mathrm{str}}(E/\mathbb{Q}_\infty) = \ker\left\{ S(E/\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_p, M) \right\} \quad \text{and} \quad X_{\mathrm{str}}(E/\mathbb{Q}_\infty) = S_{\mathrm{str}}(E/\mathbb{Q}_\infty)^\vee.$$

Kato has constructed, more-or-less naturally, a free $\Lambda_{\mathbb{Q}}$-module $Z_{\mathrm{Kato}} \subset H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. The Main Conjecture without L-function in this case asserts that $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is a torsion-free rank one $\Lambda_{\mathbb{Q}}$-module, that $Z_{\mathrm{Kato}} \neq 0$, and that

$$\xi(H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) \overset{?}{=} \xi(X_{\mathrm{str}}(E/\mathbb{Q}_\infty)). \tag{IMC-noL}$$

The connection with Main Conjecture with L-function comes about as follows. Let

$$H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) = \frac{H^1(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{\mathrm{im}(H^1(\mathbb{Q}_p, T^+ \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}))} = \left(\mathrm{im}(H^1(\mathbb{Q}_p, M^+))\right)^\vee,$$

where the second $=$ is the identification coming from local duality. Then there is a Coleman isomorphism

$$\mathrm{Col} : H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) \overset{\sim}{\to} \Lambda_{\mathbb{Q}}$$

of $\Lambda_{\mathbb{Q}}$-modules, which essentially interpolates the dual Bloch–Kato exponential maps for all the specializations $T(\psi_\zeta)$ of $T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}$.

It is a consequence of global duality that there is an exact sequence

$$0 \to \frac{H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{Z_{\mathrm{Kato}}} \overset{res_p}{\to} \frac{H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{res_p(Z_{\mathrm{Kato}})} \overset{res_p^\vee}{\to} X(E/\mathbb{Q}_\infty) \to X_{\mathrm{str}}(E/\mathbb{Q}_\infty) \to 0.$$

Aside from the exactness on the left, this is just a special case of (SES). The left-exactness holds since $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is assumed to be a torsion-free $\Lambda_{\mathbb{Q}}$-module of rank one (part of the Main Conjecture without L-function) and since $\mathrm{Col}(res_p(Z_{\mathrm{Kato}})) = (\mathcal{L}(E/\mathbb{Q}_\infty))$, which has been proved by Kato, and since $\mathcal{L}(E/\mathbb{Q}_\infty) \neq 0$ by a result of Rohrlich [56]. Admitting the equality in the Main Conjecture without L-function and appealing to the previously mentioned results of Kato and Rohrlich, $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}$, $H^1_{/f}(\mathbb{Q}_p, T \otimes \Lambda_{\mathbb{Q}})/res_p(Z_{\mathrm{Kato}})$, and $X_{\mathrm{str}}(E/\mathbb{Q}_\infty)$ are all torsion $\Lambda_{\mathbb{Q}}$-modules, hence so too is $X(E/\mathbb{Q}_\infty)$. Moreover, since characteristic ideals behave well in exact sequences, we also have

$$\xi(E/\mathbb{Q}_\infty) = \xi(H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) = \xi(\Lambda_{\mathbb{Q}}/\mathrm{Col}(Z_{\mathrm{Kato}})) = (\mathcal{L}(E/\mathbb{Q}_\infty),$$

so the Main Conjecture with L-function follows.

Remark 4.3.1.a. The formulation of the cyclotomic Main Conjecture without L-function in (IMC-noL) makes sense even in the case of supersingular reduction at p. It is only in the connection to the Main Conjecture with L-function (Conjecture 19) that made use of ordinary reduction.

4.3.2. *The two-variable Main Conjectures for E/K_∞.* Let K be an imaginary quadratic field such that (split) holds. Let $H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_K)$ be defined in analogy with $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. Let

$$H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = \ker\left\{ H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_K) \overset{res}{\to} \frac{H^1(K_v, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)} \right\},$$

and let $S_{\mathrm{ord,str}}(E/K_\infty) \subset S(E/K_\infty)$ be the subgroup of classes whose restriction at the place $\bar{v}$ is trivial.

Lei, Loeffler, and Zerbes [42] have constructed a free Λ_K-submodule $Z_{\mathrm{LLZ}} \subset H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ (essentially norm-compatible systems of their Beilinson–Flach elements – this also requires varying them in Hida families (cf. [37])). The Main Conjecture without L-function in this case is that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ is a torsion-free Λ_K-module of rank one, that $Z_{\mathrm{LLZ}} \neq 0$, and

$$\xi(H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)/Z_{\mathrm{LLZ}}) \overset{?}{=} \xi(X_{\mathrm{ord,str}}(E/K_\infty)), \quad X_{\mathrm{ord,str}}(E/K_\infty) = S_{\mathrm{ord,str}}(E/K_\infty)^\vee.$$

One of the remarkable features of this Main Conjecture without L-function is that it is also related to the Main Conjecture with L-function for both $S_{\mathrm{Gr}}(E/K_\infty)$ and $S(E/K_\infty)$. It implies two distinct Main Conjectures!

The connection with the two-variable Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$ comes via the exact sequence:

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_v}{\to} \frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})} \overset{res_v^\vee}{\to} X_{\mathrm{Gr}}(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0.$$

Other than the exactness on the left, this sequence is just a special case of (SES). The exactness on the left follows from the assumption that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ is a torsion-free Λ_K-module of rank one together with $res_v(Z_{\mathrm{LLZ}})$ being non-torsion. The latter follows from a suitably normalized version of Perrin-Riou's 'big logarithm' map $\mathrm{Log}_v : \mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K) \otimes_{\Lambda_K} \Lambda_K^{\mathrm{ur}} \overset{\sim}{\to} \Lambda_K^{\mathrm{ur}}$ and the expectation (essentially proved by Lei, Loeffler, and Zerbes) that $\mathrm{Log}_v(Z_{\mathrm{LLZ}}) =$

($\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ together with the non-vanishing of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (which is easier to prove than for $\mathcal{L}(E/\mathbb{Q}_\infty)$). The argument concluding the Main Conjecture with L-functions now proceeds as before.

The connection with the two-variable Main Conjecture for $S(E/K_\infty)$ comes about via a second exact sequence:

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_{\bar{v}}}{\to} \frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))} \overset{res^\vee_{\bar{v}}}{\to} X(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0,$$

where as before $H^1_{/f}(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_K) = H^1(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_K)/\mathrm{im}(H^1(K_w, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)$. The key to this second sequence is the Coleman isomorphism $\mathrm{Col}_{\bar{v}} : H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K) \overset{\sim}{\to} \Lambda_K$ and the expectation that $\mathrm{Col}_{\bar{v}}(Z_{\mathrm{LLZ}}) = (\mathcal{L}(E/K_\infty))$ (essentially proved by Kings, Loeffler, and Zerbes) and the non-vanishing of $\mathcal{L}(E/K_\infty)$ (which follows from (L-fact) and the aforementioned result of Rohrlich). The argument again proceeds as before.

4.3.3. *The Heegner point Main Conjecture.* Before the work of Kato and Lei–Loeffler–Zerbes, Perrin-Riou [53] formulated an anticyclotomic Main Conjecture for $S(E/K^{\mathrm{ac}}_\infty)$ in cases where the Heegner hypotheses (such as (Heeg)) hold. Let

$$H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}}) = \ker \left\{ H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}}) \overset{res}{\to} \prod_{w|p} \frac{H^1(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})}{\mathrm{im}(H^1(K_w, T^+ \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})} \right\}.$$

The Heegner points over the ring class fields of $K[p^n]$ form norm-compatible sequences in $H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})$ that generate a free Λ_{ac}-submodule $Z_{\mathrm{Heeg}} \subset H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})$. In this case Perrin-Riou's anticyclotomic Main Conjecture is that $X(E/K^{\mathrm{ac}}_\infty) \sim \Lambda_{\mathrm{ac}} \oplus N \oplus N$ for N a torsion Λ_{ac}-module and that

$$\xi(N) \overset{?}{=} c_E^{-1} \xi(H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})/Z_{\mathrm{Heeg}}),$$

where c_E is the Manin constant for the modular parameterization of E (by the Shimura curve dictated by the hypothesis (Heeg)). This conjecture is closely connected with the Main Conjecture for $S_{\mathrm{BDP}}(E/K^{\mathrm{ac}}_\infty)$.

5. Theorems and ideas of their proofs

We recall a few of the results, some recent, towards proofs of the Main Conjectures stated earlier. We also try to give some idea of their proofs.

5.1. **Cyclotomic Main Conjectures: the ordinary case.** We begin, as always, with the case of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. One result that encompasses many instances of the Main Conjecture for this case is:

Theorem 24. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* ($\mathrm{irred}_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Then the Iwasawa–Greenberg Main Conjecture for $S(E/\mathbb{Q}_\infty)$ is true. In particular, $X(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and*

$$\xi(E/\mathbb{Q}_\infty) = (\mathcal{L}(E/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}.$$

The proof of this theorem is contained in [34] [64] [63].

5.1.1. *Remarks on related results.* Of course, there are many other interesting results toward this case of the Main Conjectures for elliptic curves. We comment on a few:

- The Main Conjecture for a CM elliptic curve with ordinary reduction at p (which is excluded by this theorem because of the hypothesis on some $\ell \,||\, N_E$) was proved much earlier by Rubin [58].
- Kato's divisibility ((Div-1) below) also holds, at least in $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, when (irred$_{\mathbb{Q}}$) fails to. Greenberg and Vatsal [26] exploited this and the classical Main Conjecture for Dirichlet characters to deduce the cyclotomic Main Conjecture for some elliptic curves E for which $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation. In the same paper Greenberg and Vatsal pioneered a method of showing that when the analytic and algebraic Iwasawa μ-invariants vanish, the Main Conjecture for one elliptic curve E (or eigenform f) implies the Main Conjecture for any congruent elliptic curve (or eigenform). These ideas were then further developed by Emerton, Pollack, and Weston [17].
- Results of Grigorov [27] and more recently of Kim, Kim, and Sun [36] make it possible to 'numerically verify' instances of the cyclotomic Main Conjecture (showing that is implied by some value being prime-to-p). This yields examples of the cyclotomic Main Conjecture for elliptic curves with, say, squarefull conductors.

5.1.2. *Idea of the proof of Theorem 24.* Theorem 24 was proved in two big steps and one smaller one.

In the first step, Kato proved that $X(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and that

$$(\mathcal{L}(E/\mathbb{Q}_\infty)) \subseteq \xi(E/\mathbb{Q}_\infty) \quad \text{if } E \text{ has good ordinary reduction at } p. \tag{Div-1}$$

This was done by an Euler system argument. To be precise, the argument requires that E have good reduction at p as well as the existence of an element $\sigma \in G_{\mathbb{Q}}$ that fixes $\mathbb{Q}_\infty$ and is such that $T/(\sigma - 1)T$ is a free $\mathbb{Z}_p$-module of rank 1. The hypothesis that $E[p]$ is ramified at some $\ell \,||\, N_E$, $\ell \neq p$, ensures the existence of such an element σ.

In the second step, Urban and the lecturer showed that if K is an imaginary quadratic field of discriminant $-D_K$ such that (a) $(D_K, 4Np) = 1$, (b) p splits in K, and (c) $N_E = N^- N^+$ with N^- (resp. N^+) divisible only by primes that are inert in K (resp. split in K) and N^- is the square-free product of an odd number of primes ℓ such that $E[p]$ is ramified at ℓ, then

$$\xi(E/\mathbb{Q}_\infty)\xi(E^K/\mathbb{Q}_\infty) \subseteq (\mathcal{L}(E/\mathbb{Q}_\infty)\mathcal{L}(E^K/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}. \tag{Div-2}$$

Here E^K is the K-twist of E.

Suppose now that E is as in the statement of the theorem. It is easy to see that it is always possible to choose K so that all the hypotheses required for (Div-2) are satisfied. If in addition E has good ordinary reduction, then combining (Div-1) (for both the curve E and its K-twist E^K, which will also have good ordinary reduction at p) with (Div-2) yields the Main Conjecture for E.

The final step is to extend this result to include those E with multiplicative reduction. This was done in [63]. The argument there uses the fact that the results in [34] and [64] actually prove the Main Conjecture for p-ordinary newforms $f \in S_k(\Gamma_0(N))$, $p \nmid N$, with $k \equiv 2 \bmod p - 1$. A simple congruence argument then shows that the Main Conjecture for an E with multiplicative reduction at p can be deduced from the Main Conjectures for such f. The key point is that f_E, the newform associated with E, is a p-adic limit of such newforms f.

As noted, Kato's proof of (Div-1) goes via Euler systems. In particular, it involves progress toward the Main Conjecture without L-function for E as in Section 4.3. More precisely, Kato constructs an Euler system for T. The base of this Euler system, when it is non-zero, is a rank one $\Lambda_{\mathbb{Q}}$-module $Z_{\mathrm{Kato}} \subset H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. The machinery of Euler systems then proves that in this case $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is a free $\Lambda_{\mathbb{Q}}$-module of rank one and that

$$\xi(H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) \subseteq \xi(X_{\mathrm{str}}(E/\mathbb{Q}_\infty)).$$

Furthermore, via a deep 'explicit reciprocity law' Kato also shows that $\mathrm{Col}(Z_{\mathrm{Kato}}) = (\mathcal{L}(E/\mathbb{Q}_\infty))$. Then arguing much as in Section 4.3.1 yields both that $X(E/\mathbb{Q}_\infty)$ is torsion and (Div-1).

To try to say much about the proof of (Div-2) would take us far afield of the focus of these lectures. So suffice it to say that the proof is an extensive generalization of the Eisenstein congruence arguments used in Wiles's proof [73] of the Iwasawa Main Conjecture for totally real fields. Moreover, (Div-2) is actually just a consequence of the main theorem in [64], which is in fact an inclusion towards a three-variable Main Conjecture: the extra variables come from including f_E, the newform associated with E, in a Hida family and working with the extension K_∞/K. The very rough idea is to first construct a three-variable p-adic family of Eisenstein series on $GU(2,2)$ whose constant term is divisible by this three-variable L-function. Then to show that this Eisenstein family is coprime to the p-adic L-function by showing that for any height one prime divisor of the p-adic L-function there is some Fourier coefficient that is not divisible by this height one prime. Finally, use the Galois representations associated to cuspidal families on $GU(2,2)$ that are congruent to this Eisenstein family (by the preceding steps, these congruences are 'measured' by the p-adic L-function) to construct classes in the appropriate Selmer group.

5.2. **The Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$.** Recently, progress has been made towards the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty^{\mathrm{ac}})$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. One result that encompasses some of this progress is:

Theorem 25. *Let E be either a semistable elliptic curve or a quadratic twist of such a curve. Suppose E has good reduction at p and that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Let K be an imaginary quadratic field with discriminant $-D_K$. Suppose* (split) *holds, $(D_K, N_E) = 1$, and ℓ is inert in K. Suppose also that* (Heeg) *holds.*

(i) *$X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K^{ur}-module and $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion $\Lambda_{\mathrm{ac}}^{\mathrm{ur}}$-module.*
(ii) *There exists an element $0 \neq a \in \Lambda_{\mathrm{cyc}}^{\mathrm{ur}} = \mathbb{Z}_p^{\mathrm{ur}}[\![\Gamma_K^{\mathrm{cyc}}]\!]$ such that $a \cdot \xi_{\mathrm{Gr}}(E/K_\infty)^{\mathrm{ur}} \subseteq (\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) \subset \Lambda_K^{\mathrm{ur}}$.*
(iii) *$\xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})^{\mathrm{ur}} \subseteq (\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) \subset \Lambda_{\mathrm{ac}}^{\mathrm{ur}}$.*
(iv) *If $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$, then* (i) *holds with $a = 1$.*

Here we have written $\xi_?(\cdot)^{\mathrm{ur}}$ to mean $\xi_?(\cdot)\Lambda_{??}^{\mathrm{ur}}$. Part (ii) of this theorem is essentially the main results of [70] and [71]. The element a in (i) can be taken to be divisible only by height one primes of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ that are of the form $P\Lambda_K^{\mathrm{ur}}$ for some height one prime $P \subset \Lambda_{\mathrm{cyc}}^{\mathrm{ur}}$.

Combining Theorem 25 with results toward the cyclotomic Main Conjecture, via arguments like those in Section 4.3.2, yields case of the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. For example:

Theorem 26. *Let E be either a semistable elliptic curve or a quadratic twist of such a curve. Suppose E has good ordinary reduction at p and that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Let K be an imaginary quadratic field with discriminant $-D_K$. Suppose* (split) *holds, $(D_K, N_E) = 1$, and ℓ is inert in K. Suppose also that* (Heeg) *holds and that $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$. Then $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K^{ur}-module and $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion $\Lambda_{\mathrm{ac}}^{\mathrm{ur}}$-module, and*

$$\xi_{\mathrm{Gr}}(E/K_\infty)^{\mathrm{ur}} = (\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) \subset \Lambda_K^{\mathrm{ur}} \quad \textit{and} \quad \xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})^{\mathrm{ur}} = (\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) \subset \Lambda_{\mathrm{ac}}^{\mathrm{ur}}.$$

That is, the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ hold.

5.2.1. *Idea of the proofs of Theorems 25 and 26.* Part (i) of Theorem 25 is a relatively easy consequence of work of Cornut and Vatsal [10] together with the theorems of Gross–Zagier and Kolyvagin (as extended by others to Heegner points coming from Shimura curve parameterizations). In particular, by [10, Thm. 1.5] there is some finite order character χ of Γ_K^{ac} such that $L'(f_E, \chi_{\mathrm{alg}}^{-1}, 1) \neq 0$. Let $\mathcal{O}$ be the ring of integers of the finite extension L of $\mathbb{Q}_p$ containing the values of χ. Let $W = E[p^\infty] \otimes_{\mathbb{Z}_p} \mathcal{O}(\chi^{-1})$. It then follows from the Gross–Zagier theorem and Kolyvagin's Euler system argument that $H_f^1(K, W)$ has $\mathcal{O}$-corank 1, with the $\mathcal{O}$-divisible part generated by the image of Heegner points. A simple Galois cohomology argument, such as appears in Section 6.2 below, then shows that $H^1_{\mathrm{BDP}}(K, W)$ is finite, where by $H^1_{\mathrm{BDP}}(K, W)$ we mean the group of classes that are trivial at all places except v. A control theorem argument like that of Proposition 12 shows that the dual $H^1_{\mathrm{BDP}}(K, W)^\vee$ is a quotient of $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \otimes_{\mathbb{Z}_p} \mathcal{O}$ mod $(\gamma_- - \chi(\gamma_-))$ with a finite order kernel. It follows that $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module. It then follows similarly from Proposition 11 that $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K-module.

Part (ii) is a consequence of the main results in [70] and [71], in much the same way that (Div-2) is a consequence of the main result in [64]. These main results are also inclusions toward three-variable main conjectures, the additional variable arising from including f_E in a Hida or Coleman family. Again, the very rough idea is to first construct a three-variable p-adic family of Eisenstein series, in this case on $GU(3,1)$, whose constant term is divisible by the three-variable L-function. Then to show that this Eisenstein family is coprime to the p-adic L-function. This step is complicated by the fact that forms on $GU(3,1)$ do not have Fourier expansions, only Fourier–Jacobi expansions. And then, once this is done, use the Galois representations associated to cuspidal families on $GU(3,1)$ that are congruent to this Eisenstein family (by the preceding steps, these congruences are 'measured' by the p-adic L-function) to construct classes in the appropriate Selmer group.

The passage from (ii) to (iii) follows from combining Proposition 11, Lemma 16, and Theorem 17. To make this work one must also note that Lemma 16 together with $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \neq 0$ (see Theorem 17) imply that $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (and hence a) is not divisible by $\gamma_+ - 1$.

The stronger conclusion of (iv) follows since if $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ had a divisor of the form $P\Lambda_K$ for some height one prime $P \subset \Lambda_{\mathrm{cyc}}^{\mathrm{ur}}$, then $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ mod $(\gamma_+ - 1)$ would be divisible by P mod $(\gamma_+ - 1)$, which is a power of p (we already observed that P mod $(\gamma_+ - 1)$ is non-zero when passing from (ii) to (iii)). But this would contradict Theorem 17.

To deduce Theorem 26 from Theorem 25, one can argue much as in Section 4.3.2. As $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K-module by part (i) of Theorem 25, so too is its quotient $X_{\mathrm{ord,str}}(E/K_\infty)$. The latter being torsion implies that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = 0$ (here we use (irred$_K$)). This in turn

implies that there is an exact sequence

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_v}{\to} \frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})} \overset{res_v^\vee}{\to} X_{\mathrm{Gr}}(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0.$$

Part (iv) of Theorem 25 implies that

$$\xi(X_{\mathrm{Gr}}(E/K_\infty)) \subseteq \xi(\frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})}),$$

hence

$$\xi(X_{\mathrm{ord,str}}(E/K_\infty)) \subseteq \xi(\frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}}).$$

Furthermore, each of these inclusions is an equality if the other is. We will explain that the second inclusion is an equality, hence so is the first.

By noting that $S(E/K_\infty)[\gamma_- - 1] \cong S(E/\mathbb{Q}_\infty) \oplus S(E^K/\mathbb{Q}_\infty)$, one readily sees that $X(E/K_\infty)$ is a torsion Λ_K-module (since $X(E/\mathbb{Q}_\infty)$ and $X(E^K/\mathbb{Q}_\infty)$ are both torsion $\Lambda_{\mathbb{Q}}$-modules). It follows that $H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = 0$ (here we again use that (Heeg$_K$) holds. It then follows that there is an exact sequence

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_{\bar{v}}}{\to} \frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))} \overset{res_{\bar{v}}^\vee}{\to} X(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0,$$

As $\xi(X_{\mathrm{ord,str}}(E/K_\infty)) \subseteq \xi(H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)/Z_{\mathrm{LLZ}}$, it follows that

$$\xi(X(E/K_\infty)) \subseteq \xi(\frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))}) = (\mathcal{L}(E/K_\infty)).$$

And again, each inclusion is an equality if the other is. But by reducing the last equation modulo $(\gamma_- - 1)$ and appealing to the cyclotomic Main Conjecture for both E and E^K (or even just Kato's divisibilities Div-1), we conclude that this last inclusion is an equality. Hence so are the others. This proves the Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$. The Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ essentially follows by reducing modulo $(\gamma_+ - 1)$.

5.2.2. *Remarks on related results.*

- Wan's results actually allow D_K and N to have prime factors in common. This is important for some applications.
- Wan also proved a version of Theorem 25(ii) when (Heeg) is replaced by a condition that allows the root number $w(E/K)$ to equal $+1$. In this case $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = 0$ and $X_{\mathrm{BDP}}(E/K_\infty)$ is not torsion.
- A careful read of the deduction of Theorem 26 from Theorem 25 shows that it actually gives a second proof of the cyclotomic Main Conjecture for E and E^K! (This is so, as one can get away with appealing to Kato's divisibility at the crucial step.)
- Wan has a modification of these results that allows many of the arguments to be applied to E with supersingular reduction at p [71]. A summary of some of this is in [9].

5.3. **Cyclotomic Main Conjectures: the supersingular case.** The work of Wan, in combination with the Beilinson–Flach elements of Lei–Loeffler–Zerbes, has provided a means to approach the cyclotomic Main Conjectures for $S_\pm(E/\mathbb{Q}_\infty)$ when E has supersingular reduction at p and $a_p(E) = 0$.

Theorem 27. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either a semistable curve or a quadratic twist of such. Let $p \geq 3$ be a prime at which E has supersingular reduction and $a_p(E) = 0$. Suppose that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Then the Main Conjecture for $S_{\pm}(E/\mathbb{Q}_\infty)$ is true. In particular, $X_{\pm}(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and*

$$\xi_{\pm}(E/\mathbb{Q}_\infty) = (\mathcal{L}_{\pm}(E/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}.$$

The proof of this theorem combines work of Kobayashi [38] and Wan [71]. The argument essentially follows as indicated in the third remark of Section 5.2.2, only everything is decorated with a subscript $\pm$ and Kato's divisibility is replaced with Kobayashi's.

5.3.1. *Remarks on related results.*

- The Main Conjecture for a *CM* elliptic curve with supersingular reduction at p was proved earlier by Pollack and Rubin [55].
- The Main Conjecture for $S_{\pm}(E/\mathbb{Q}_\infty)$ is equivalent to the Kato's Main Conjecture without L-functions for E; the equivalence runs along the same lines as described for the ordinary case in Section 4.3.1.
- Sprung [66] [67] has extended Theorem 27 to include those E with supersingular reduction at p but with $a_p(E) \neq 0$.

5.4. **Perrin-Riou's Heegner point Main Conjecture.** The proofs of the Main Conjectures with L-functions described so far have both invoked progress toward Main Conjectures *without* L-functions and resulted in the proof of such in many cases. This is one more.

Theorem 28. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E and good ordinary reduction at p. Suppose that N is either a semistable curve or a quadratic twist of a semistable curve. Suppose* (irred$_{\mathbb{Q}}$) *holds. Let K be an imaginary quadratic field of discriminant $-D_K$ such that* (split) *holds. Suppose that N_E and D_K are relatively prime and that* (Heeg) *holds. Suppose further that $N^- \neq 1$ and $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$. Then Perrin-Riou's Heegner point Main Conjecture is true. That is,*

(a) *$X(E/K_\infty^{\mathrm{ac}}) \sim \Lambda_{\mathrm{ac}} \oplus N \oplus N$ with N a torsion Λ_{ac}-module, and*
(b) *$\xi(N) = \xi(H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})/Z_{\mathrm{Heeg}})$.*

Here, the $\sim$ in (a) means that there is a Λ_{ac} homomorphism with pseudonull kernel and cokernel (this is reflexive). See Section 4.3.3 for definition of the terms in the statement of (b).

Part (a) of this theorem was known from earlier work of Bertolini, Cornut, and Nekovář, while Howard [30] [31] proved the inclusion $\supseteq$ in (b). Wan [72] showed that equality could be deduced from Howard's inclusion in combination with his work on the Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$.

Remark 5.4.0.a. Castella and Wan [9] have formulated and proved a version of the Heegner point Main Conjecture when E has supersingular reduction at p and $a_p(E) = 0$.

6. Arithmetic consequences

By this point the reader will have recognized that many of the theorems towards the Main Conjectures for elliptic curves have interesting consequences, especially for the (conjectured) Birch–Swinnerton-Dyer formula. We explain a few in the following.

6.1. **Results when $L(E,1) \neq 0$.** As an almost immediate consequence of Theorem 24 and the control theorems and especially Proposition 10, we have:

Theorem 29. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) \neq 0$, then*

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \cdot \prod_{\ell | N_E} c_\ell\right|_p^{-1}.$$

Additional argument is required when E has split multiplicative reduction at p due to the trivial zero of $\mathcal{L}(E/\mathbb{Q}_\infty)$ at $T = 0$. The details of this case are included in [63]. We have written $\#Ш(E/\mathbb{Q})$ and not just $\#Ш(E/\mathbb{Q})[p^\infty]$ as it is known by the work of Kolyvagin that when $L(E,1) \neq 0$ the Tate–Shafaravich group $Ш(E/\mathbb{Q})$ has finite order.

The corresponding result for the case of supersingular reduction, a consequence of Theorem 27 and Proposition 15 is just:

Theorem 30. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either semistable or a quadratic twist of a semistable curve. Let $p \geq 3$ be a prime at which E has good supersingular reduction with $a_p(E) = 0$. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) \neq 0$, then*

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \cdot \prod_{\ell | N_E} c_\ell\right|_p^{-1}.$$

6.2. **Results when $L(E,1) = 0$.** The Main Conjecture also has consequences when $L(E,1) = 0$. Again combining Theorem 24 and the control theorems, one can deduce:

Theorem 31. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) = 0$, then $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \infty$ and so its $\mathbb{Z}_p$-corank is at least one. Moreover, if E does not have split multiplicative reduction at p and $\mathrm{ord}_{s=1} L(E,s)$ is even and positive, then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is at least two.*

The key point here is that if $L(E,1) = 0$ then $g_E(0) = 0$, so by Lemma 4 we have $\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \infty$. By the arguments used to establish the control theorems we have an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \prod_{\ell \in \Sigma} K_\ell.$$

As the groups on the right are finite (at least if E does not have split multiplicative reduction), then $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ has infinite order if and only if $S(E/\mathbb{Q}_\infty)[\gamma - 1]$ does. The modifications of

this argument needed to handle the case of split multiplicative reduction at p are included in [63]. The claim about the $\mathbb{Z}_p$-corank being at least two follows from combining the result that the $\mathbb{Z}_p$-corank being positive with the proof of the parity conjecture by Nekovář [50].

The analog of this theorem in the supersingular case is:

Theorem 32. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either semistable or a quadratic twist of a semistable curve. Let $p \geq 3$ be a prime at which E has supersingular reduction and $a_p(E) = 0$. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) = 0$, then $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \infty$ and so its $\mathbb{Z}_p$-corank is at least one. Moreover, if E does not have split multiplicative reduction at p and $\mathrm{ord}_{s=1}L(E,s)$ is even and positive, then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is at least two.*

Remark 6.2.0.a. Theorems 31 and 32 provide some evidence toward the Birch–Swinnerton-Dyer Conjecture. This conjecture asserts that if $L(E,1) = 0$ then $E(\mathbb{Q})$ has positive rank, and the fundamental exact sequence $0 \to E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0$ then shows that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ must have $\mathbb{Z}_p$-corank at least one. Moreover, if the order of vanishing is at least two, then the rank of $E(\mathbb{Q})$ should be at least two and hence the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ should be at least two. So the conclusions of the theorems agree with implications of the Birch–Swinnerton-Dyer Conjecture. Furthermore, assuming that $Ш(E/\mathbb{Q})$ is finite, we can conclude the expected facts about the rank of $E(\mathbb{Q})$!

6.3. **Results when** $\mathrm{ord}_{s=1}L(E,s) = 1$**.** Suppose the analytic rank of E is 1, that is, the order of vanishing at $s = 1$ of the L-function $L(E,s)$ is 1. Then we know from the work of Gross, Zagier, and Kolyvagin that $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}) = 1$ and $Ш(E/\mathbb{Q})$ is finite. It is even known that $L'(E,1)/\Omega_E \cdot R(E/\mathbb{Q}) \in \mathbb{Q}^\times$. What can be said regarding its conjectured value (the Birch–Swinnerton-Dyer formula (BSD-f))? The following theorem is progress toward this:

Theorem 33. *Let E be a semistable elliptic curve and p a prime of good reduction such that $a_p(E) = 0$ if E has supersingular reduction at p. Suppose* $(\mathrm{irred})_{\mathbb{Q}}$ *holds. If E has analytic rank one, then*

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

A proof of this theorem is given in [32]. This proof combines the Gross–Zagier theorem [28] [74] with Kolyvagin's Euler system argument [41] and with the results toward the Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ and Theorems 29 and 30. These arguments have been extended to the case of multiplicative reduction by Castella [8].

6.3.1. *Remarks on related results.*

- Cases of Theorem 33 have also been proved by Zhang [75] and by Berti, Bertolini, and Venerucci [3]. Each of these imposes some restrictions on the primes $\ell \mid N_E$ at which p is allowed to divide $c_\ell(E/\mathbb{Q})$. Furthermore, each also appeals to Theorem 29.
- The supersingular case of Theorem 33 has also been proved by Kobayashi [39] as a consequence of a remarkable result on the non-vanishing of the p-adic height of the Heegner point when E has supersingular reduction at p. This proof, too, appeals to the Theorems 27 and 30.

6.3.2. *Idea of the proof of Theorem 33.* We give a quick sketch of the proof of Theorem 33.

One first chooses an auxiliary imaginary quadratic field such that the hypotheses of Theorem 25 hold and $L(E^K,1)\neq 0$ (so $\mathrm{ord}_{s=1}L(E/K,s)=1$). The theorems of Gross–Zagier and Kolyvagin then give a non-torsion Heegner point $y_K\in E(K)$ that generates a subgroup of finite index. From parts (i) and (iii) of Theorem 25 together with Corollary 13 one deduces that

$$\left|\frac{1-a_p(E)+p}{p}\cdot \log_{E(K_v)} y_K\right|_p^{-2} \leq \left|\#\mathrm{Sel}_{\mathrm{BDP}}(E/K)\cdot \prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2\cdot \delta_p(E)^2\right|_p^{-1}$$

Using that $\mathrm{Sel}_{p^\infty}(E/K)\twoheadrightarrow E(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ (since the image of y_K has infinite order in $E(K_v)$) together with $\mathrm{rank}_{\mathbb{Z}}E(K)=1$, a simple Galois cohomological argument shows that

$$\#\mathrm{Sel}_{\mathrm{BDP}}(E/K)=\#Ш(E/K)[p^\infty]\cdot[E(K_v)/E(K_v)_{\mathrm{tors}}:\mathbb{Z}_p\cdot y_K]^2.$$

Substituting this into the preceding inequality yields

$$[E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p\cdot y_K]^2\leq \left|\#Ш(E/K)[p^\infty]\cdot\prod_{\ell|N^+}c_\ell(E/\mathbb{Q})^2\right|_p^{-1}.$$

The Gross–Zagier formula expresses $\frac{L'(E,1)}{\Omega_{E/K}R(E/\mathbb{Q})}$ in terms of the square of the index $[E(K):\mathbb{Z}\cdot y_K]$ and ratio of the degree of the modular parametrization of E and the degree of the Shimura curve parametrization of E (the latter gives rise to y_K). Using a result of Ribet and Takahashi on the p-part of the latter, we can conclude that

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}R(E/K)}\right|_p^{-1}\leq \left|\#Ш(E/K)[p^\infty]\prod_{\ell|N_E}c_\ell(E/K)\right|_p^{-1}.$$

Since $L(E/K,s)$ factors as $L(E/K,s)=L(E,s)L(E^K,s)$, $L'(E/K,1)=L'(E,1)L(E^K,1)$. A comparison of periods shows that since (irred_K) holds, $\Omega_{E/K}$ is a p-adic unit multiple of $\Omega_E\Omega_{E^K}$. Furthermore, $R(E/\mathbb{Q})$ is just $R(E/K)$ since $E^K(\mathbb{Q})$ is finite. So we have

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}R(E/K)}\right|_p^{-1}=\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1}\cdot\left|\frac{L(E^K,1)}{\Omega_{E^K}}\right|_p^{-1}.$$

On the other hand, $Ш(E/K)[p^\infty]=Ш(E/\mathbb{Q})[p^\infty]\oplus Ш(E^K/\mathbb{Q})[p^\infty]$ and $\prod_{\ell|N_E}c_\ell(E/K)$ equals $\prod_{\ell|N_E}c_\ell(E/\mathbb{Q})\cdot\prod_{\ell|N_{E^K}}c_\ell(E^K/\mathbb{Q})$ up to a power of 2. It follows that

$$\left|\#Ш(E/K)[p^\infty]\prod_{\ell|N^+}c_\ell(E/K)\right|_p^{-1}=\left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E}c_\ell(E/\mathbb{Q})\right|_p^{-1}$$
$$\times\left|\#Ш(E^K/\mathbb{Q})[p^\infty]\prod_{\ell|N_{E^K}}c_\ell(E^K/\mathbb{Q})\right|_p^{-1}.$$

Combining the last three displayed equations with Theorems 29 and 30 for $L(E^K,1)$ we conclude that

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} \leq \left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

This is the upper bound predicted by the Birch–Swinnerton-Dyer formula.

To achieve the predicted lower bound, we choose a possibly *different* quadratic field K such that (split) and (Heeg) hold, $L(E^K,1)\neq 0$, and $p\nmid c_\ell(E/\mathbb{Q})$ for all $\ell \mid N^+$. Then Kolyvagin's Heegner point Euler system argument yields

$$[E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_p : \mathbb{Z}_p\cdot y_K]^2 \geq \left|\#Ш(E/K)[p^\infty]\cdot\prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2\right|_p^{-1}.$$

Arguing as above we now conclude that

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} \geq \left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

Equality follows.

Remark 6.3.2.a. For the argument sketched above to always apply, one actually needs to be able to choose K so that D_K and N_E are possibly not coprime (see the first remark in Section 5.2.2). This is primarily to be able to deal with the case where N_E is a prime (or E is a quadratic twist of a such a curve).

6.4. **Converses to Gross–Zagier/Kolyvagin.** If E has analytic rank one, then the theorems of Gross, Zagier, and Kolyvagin imply that $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})$ is one and $Ш(E/\mathbb{Q})$ is finite. In particular, the corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is one. Conversely, as noted (see (BSD-crk)), admitting the conjectures of Birch–Swinnerton-Dyer and the finiteness of the Tate-Shafarevich group, if the corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is one, then E has analytic rank one. Can this converse can be made unconditional?

The following theorem is an example of what one can prove about this:

Theorem 34. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E and good ordinary reduction at p. Suppose E is semistable. Suppose* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. If $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ has corank one, then $\mathrm{ord}_{s=1}L(E,s)=1$. In particular, $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})$ is finite.*

This is essentially in [72]. An analog for the case of supersingular reduction is proved in [9].

The idea of the proof of Theorem 34 is as follows. One begins by choosing an imaginary quadratic field K so that E and K satisfy the hypotheses of Theorem 28 and $L(E^K,1)\neq 0$. It follows from the theorems of Gross, Zagier, and Kolyvagin that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, so the corank of $\mathrm{Sel}_{p^\infty}(E/K)=\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})\oplus\mathrm{Sel}_{p^\infty}(E^K/\mathbb{Q})$ is also one. A control theorem argument shows that $\mathrm{Sel}_{p^\infty}(E/K)\subset S(E/K_\infty)[\gamma_- -1]$ with finite index, so $X(E/K_\infty^{\mathrm{ac}})/(\gamma_- -1)X(E/K_\infty^{\mathrm{ac}})$ has rank one. Then it follows from part (a) of Theorem 28 that $N/(\gamma_- -1)N$ is finite. It then follows from part (b) of the same theorem that the image of Z_{Heeg} in

$$H^1_{\mathrm{ord}}(K,T\otimes\mathbb{Z}_p\Lambda_{\mathrm{ac}})/(\gamma_- -1)H^1_{\mathrm{ord}}(K,T\otimes\mathbb{Z}_p\Lambda_{\mathrm{ac}})\hookrightarrow H^1_{\mathrm{ord}}(K,T)\cong\mathbb{Z}_p.$$

has finite index. But this image of Z_{Heeg} is spanned by the Heegner point y_K. So y_K is non-torsion. It then follows from the Gross–Zagier theorem that $\mathrm{ord}_{s=1}L(E/K,s) = 1$, and this, together with $L(E^K,1) \neq 0$, implies that $\mathrm{ord}_{s=1}L(E,s) = 1$.

Remark 6.4.0.a. Variants on this theorem have also been proved by the lecturer [62] and Zhang [75] [65] and Venerucci [69]. Such converses to Gross–Zagier were a key piece of the arguments in [1] and [2] that show that a positive proportion of elliptic curves have both algebraic and analytic rank one.

References

[1] Manjul Bhargava and Christopher Skinner, *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one*, J. Ramanujan Math. Soc. **29** (2014), no. 2, 221–242.
[2] Manjul Bhargava, Christopher Skinner, and Wei Zhang, *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one*, arXiv:1401.0233.
[3] Andrea Berti, Massimo Bertolini, and Rodolfo Venerucci, *Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 1–31.
[4] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148. With an appendix by Brian Conrad.
[5] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.
[6] Ernest Hunter Brooks, *Shimura curves and special values of p-adic L-functions*, Int. Math. Res. Not. IMRN **12** (2015), 4177–4241.
[7] Ashay 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** (2017), no. 1, 189–222.
[8] Francesc Castalla, *On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes*, Camb. J. Math. (to appear).
[9] Francesc Castella and Xin Wan, *Perrin-Riou's main conjecture for elliptic curves at supersingular primes*, arXiv:1607.02019.
[10] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186.
[11] Kęstutis Česnavičius, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), no. 1, 31–61.
[12] John Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 269–353.
[13] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.
[14] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294** (2004), ix, 251–319.
[15] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154.
[16] Ellen Eischen, Michael Harris, Jian-Shu Li, and Christopher Skinner, *p-adic L-functions for unitary groups*, arXiv:1602.01776.
[17] Matthew Emerton, Robert Pollack, and Tom Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), no. 3, 523–580.
[18] Jean-Marc Fontaine and Bernadette Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 599–706.
[19] Ralph Greenberg, *On p-adic L-functions and cyclotomic fields*, Nagoya Math. J. **56** (1975), 61–77.
[20] ———, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137.
[21] ———, *Iwasawa theory for motives*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 211–233.
[22] ———, *Iwasawa theory and p-adic deformations of motives*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 193–223.

[23] ———, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.
[24] ———, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464.
[25] ———, *On the structure of certain Galois cohomology groups*, Doc. Math. **Extra Vol.** (2006), 335–391.
[26] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.
[27] Grigor Tsankov Grigorov, *Kato's Euler system and the Main Conjecture*, ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–Harvard University.
[28] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.
[29] Haruzo Hida, *A p-adic measure attached to the zeta functions associated with two elliptic modular forms. II*, Ann. Inst. Fourier (Grenoble) **38** (1988), no. 3, 1–83.
[30] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.
[31] ———, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45.
[32] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434.
[33] Kazuya Kato, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* B_{dR}. *I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163.
[34] ———, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290. Cohomologies *p*-adiques et applications arithmétiques. III.
[35] Byoung Du Kim, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc. **95** (2013), no. 2, 189–200.
[36] C-H. Kim, M. Kim, and H-S. Sun, *On the indivisibility of derived Kato's Euler systems and the Main Conjecture for modular forms*, arXiv:1709.05780v2.
[37] Guido Kings, David Loeffler, and Sarah Livia Zerbes, *Rankin-Eisenstein classes and explicit reciprocity laws*, Camb. J. Math. **5** (2017), no. 1, 1–122.
[38] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.
[39] ———, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629.
[40] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528.
[41] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
[42] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for Rankin-Selberg convolutions of modular forms*, Ann. of Math. (2) **180** (2014), no. 2, 653–771.
[43] David Loeffler, *p-adic integration on ray class groups and non-ordinary p-adic L-functions*, Iwasawa theory 2012, Contrib. Math. Comput. Sci., vol. 7, Springer, Heidelberg, 2014, pp. 357–378.
[44] David Loeffler and Sarah Livia Zerbes, *Iwasawa theory and p-adic L-functions over* $\mathbb{Z}_p^2$*-extensions*, Int. J. Number Theory **10** (2014), no. 8, 2045–2095.
[45] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.
[46] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.
[47] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.
[48] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.
[49] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006.
[50] Jan Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104.
[51] ———, *Selmer complexes*, Astérisque **310** (2006), viii+559 (English, with English and French summaries).
[52] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.
[53] Bernadette Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456 (French, with English summary).
[54] ———, *Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire*, J. London Math. Soc. (2) **38** (1988), no. 1, 1–32 (French).

[55] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.
[56] David E. Rohrlich, *On L-functions of elliptic curves and anticyclotomic towers*, Invent. Math. **75** (1984), no. 3, 383–408.
[57] Karl Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), no. 3, 527–559.
[58] ———, *The "Main Conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.
[59] ———, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.
[60] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 379–460.
[61] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[62] Christopher Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, arXiv:1405.7294.
[63] ———, *Multiplicative reduction and the cyclotomic Main Conjecture for* GL_2, Pacific J. Math. **283** (2016), no. 1, 171–200.
[64] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.
[65] Christopher Skinner and Wei Zhang, *Indivisibility of Heegner points in the multiplicative case*, arXiv:1407.1099.
[66] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.
[67] ———, *The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes*, arXiv:1610.10017.
[68] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Dix exposés sur la cohomologie des schémas, Adv. Stud. Pure Math., vol. 3, North-Holland, Amsterdam, 1968, pp. 189–214.
[69] Rodolfo Venerucci, *On the p-converse of the Kolyvagin-Gross-Zagier theorem*, Comment. Math. Helv. **91** (2016), no. 3, 397–444.
[70] Xin Wan, *Iwasawa Main Conjecture for Rankin–Selberg p-adic L-functions*, arXiv:1408.4044.
[71] ———, *Iwasawa Main Conjecture for supersingular elliptic curves*, arXiv:1411.6352.
[72] ———, *Heegner point Kolyvagin system and Iwasawa Main Conjecture*, arXiv:1408.4043.
[73] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540.
[74] Shouwu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.
[75] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253.

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA

E-mail address: cmcls@princeton.edu

1. Projects: Propagating the Iwasawa main conjecture via congruences

1.1. **Goal of these projects.** Let $f, g \in S_k(\Gamma_0(N))$ be normalized eigenforms (not necessarily newforms) of weight $k \geqslant 2$, say with rational Fourier coefficients $a_n, b_n \in \mathbf{Q}$ for simplicity, and assume that

$$f \equiv g \pmod{p}$$

in the sense that $a_n \equiv b_n \pmod{p}$ for all $n > 0$. Roughly speaking, the goal of these projects is to study how knowledge of the Iwasawa main conjecture for f can be "transferred" to g.

For $k = 2$ and primes $p \nmid N$ of ordinary reduction, such study was pioneered by Greenberg–Vatsal [GV00], and in these projects we will aim to extend some of their results to:

- non-ordinary primes;
- certain anticyclotomic settings;
- (more ambitiously) some of the "residually reducible" cases which eluded the methods of [GV00], with applications to the p-part of the BSD formula in ranks 0 and 1.

1.2. **The method of Greenberg–Vatsal.** Before jumping into the specifics of each of those settings, let us begin with a brief outline of the method of Greenberg–Vatsal (which is beautifully explained in [GV00, §1]). Let F_∞/F be a $\mathbf{Z}_p$-extension of a number field F, and identify the Iwasawa algebra $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$ with the one-variable power series ring $\Lambda = \mathbf{Z}_p[[T]]$ in the usual fashion.

Recall that Iwasawa's main conjecture for f over F_∞/F posits the following equality between principal ideals of Λ:

$$(L_p^{\mathrm{alg}}(f)) \stackrel{?}{=} (L_p^{\mathrm{an}}(f)), \tag{1.1}$$

where

- $L_p^{\mathrm{alg}}(f) \in \Lambda$ is a characteristic power series of a Selmer group for f over F_∞/F.
- $L_p^{\mathrm{an}}(f) \in \Lambda$ is a p-adic L-function interpolating critical values for $L(f/F, s)$ twisted by certain characters of $\mathrm{Gal}(F_\infty/F)$.

By the Weierstrass preparation theorem, we may uniquely write

$$L_p^{\mathrm{alg}}(f) = p^{\mu^{\mathrm{alg}}(f)} \cdot Q^{\mathrm{alg}}(f) \cdot U,$$

with $\mu^{\mathrm{alg}}(f) \in \mathbf{Z}_{\geqslant 0}$, $Q^{\mathrm{alg}}(f) \in \mathbf{Z}_p[T]$ a distinguished polynomial, and $U \in \Lambda^\times$ an invertible power series. Letting

$$\lambda^{\mathrm{alg}}(f) := \deg Q^{\mathrm{alg}}(f),$$

and similarly defining $\mu^{\mathrm{an}}(f)$ and $\lambda^{\mathrm{an}}(f)$ in terms $L_p^{\mathrm{an}}(f)$, the strategy of [GV00] is based on the following three observations:

O1. The equality (1.1) amounts to having:
  (1) $(L_p^{\mathrm{alg}}(f)) \supseteq (L_p^{\mathrm{an}}(f))$,
  (2) $\mu^{\mathrm{alg}}(f) = \mu^{\mathrm{an}}(f)$,
  (3) $\lambda^{\mathrm{alg}}(f) = \lambda^{\mathrm{an}}(f)$.
  We shall place ourselves in a situation where one expects that $\mu^{\mathrm{alg}}(f) = \mu^{\mathrm{an}}(f) = 0$.

O2. For Σ any finite set of primes $\ell \neq p, \infty$, the equality (1.1) is *equivalent* to the equality

$$(L_{p,\mathrm{alg}}^{\Sigma}(f)) \stackrel{?}{=} (L_{p,\mathrm{an}}^{\Sigma}(f)), \tag{1.2}$$

  where $L_{p,\mathrm{alg}}^{\Sigma}(f)$ and $L_{p,\mathrm{an}}^{\Sigma}(f)$ are the "imprimitive" counterparts of $L_p^{\mathrm{alg}}(f)$ and $L_p^{\mathrm{an}}(f)$ obtained (roughly speaking) by relaxing the local conditions/removing the Euler factors at the primes $\ell \in \Sigma$.

O3. For appropriate Σ, the objects involved in (1.2) are well-behaved under congruences. Letting $\mu_{\mathrm{alg}}^{\Sigma}(f)$, $\lambda_{\mathrm{alg}}^{\Sigma}(f)$, etc. be the obvious invariants from the above discussion, this translates into:

2

Expectation 1. *Assume that $f \equiv g \pmod p$, and let $* \in \{\mathrm{alg}, \mathrm{an}\}$. If $\mu_*^\Sigma(f) = 0$, then $\mu_*^\Sigma(g) = 0$ and $\lambda_*^\Sigma(f) = \lambda_*^\Sigma(g)$.*

Now, if we are given $f \equiv g \pmod p$ and the divisibilities

$$(L_p^{\mathrm{alg}}(f)) \supseteq (L_p^{\mathrm{an}}(f)) \quad \text{and} \quad (L_p^{\mathrm{alg}}(g)) \supseteq (L_p^{\mathrm{an}}(g)), \tag{1.3}$$

we see that the equivalence of **O2** combined with **Expectation 1** yields the implication

$$(L_p^{\mathrm{alg}}(f)) = (L_p^{\mathrm{an}}(f)) \quad \Longrightarrow \quad (L_p^{\mathrm{alg}}(g)) = (L_p^{\mathrm{an}}(g)). \tag{1.4}$$

Note that this has interesting applications. Indeed, if for example the residual representation $\bar\rho_f$ is absolutely irreducible, then one can hope to establish (1.3) by an Euler/Kolyvagin system argument. Proving the opposite divisibility (either via Eisenstein congruences, or via a refined Euler/Kolyvagin system argument) often requires additional ramification hypotheses on $\bar\rho_f$ relative to the level of f (see below for specific examples), a restriction that could be ultimately removed thanks to (1.4).

1.3. **On the cyclotomic main conjectures for non-ordinary primes.** Here we let F_∞/F be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$, let $p \nmid N$ be a non-ordinary prime for $f \in S_k(\Gamma_0(N))$, and let α, β be the roots of the p-th Hecke polynomial of f. In this setting, Lei–Loeffler–Zerbes [LLZ10], [LLZ11], formulated[1] "signed" main conjectures:

$$(L_p^\sharp(f)) \stackrel{?}{=} \mathrm{Char}_\Lambda(\mathrm{Sel}_\sharp(f)^\vee), \qquad (L_p^\flat(f)) \stackrel{?}{=} \mathrm{Char}_\Lambda(\mathrm{Sel}_\flat(f)^\vee), \tag{1.5}$$

where $\mathrm{Sel}_\sharp(f)$ and $\mathrm{Sel}_\flat(f)$ are Selmer groups cut out by local condition at p more stringent that the usual ones, and $L_p^\sharp(f), L_p^\flat(f) \in \Lambda$ are related to the p-adic L-functions $L_p^\alpha(f), L_p^\beta(f)$ of Amice–Vélu and Vishik in the following manner:

$$\begin{pmatrix} L_p^\alpha(f) \\ L_p^\beta(f) \end{pmatrix} = Q_{\alpha,\beta}^{-1} M_{\log} \cdot \begin{pmatrix} L_p^\sharp(f) \\ L_p^\flat(f) \end{pmatrix}, \tag{1.6}$$

where $Q_{\alpha,\beta} = \left(\begin{smallmatrix} \alpha & -\beta \\ -p & p \end{smallmatrix}\right)$ and $M_{\log}$ is a certain "logarithm matrix".

Project A. *Show* **Expectation 1** *for the signed p-adic L-functions. More precisely, for each $\bullet \in \{\sharp, \flat\}$, show that if $f \equiv g \pmod p$, then*

$$\mu(L_p^\bullet(f)) = 0 \quad \Longrightarrow \quad \mu(L_p^\bullet(g)) = 0$$

and the λ-invariants of Σ-imprimitive versions of $L_p^\bullet(f)$ and $L_p^\bullet(g)$ are equal.

Say $k = 2$ for simplicity. Similarly as in [GV00], the proof of this result would follow from the equality

$$L_p^{\Sigma,\bullet}(f) \equiv u L_p^{\Sigma,\bullet}(g) \pmod{p\Lambda},$$

for some unit $u \in \mathbf{Z}_p^\times$, which in turn would follow from establishing the congruence

$$L_p^{\Sigma,\bullet}(f, \zeta - 1) \equiv u L_p^{\Sigma,\bullet}(g, \zeta - 1) \pmod{p\mathbf{Z}_p[\zeta]}, \tag{1.7}$$

for all $\zeta \in \mu_{p^\infty}$ and some $u \in \mathbf{Z}_p^\times$ independent of ζ. However, a point of departure here from the p-ordinary setting is that (unless $a_p = b_p = 0$) the signed p-adic L-functions $L_p^\bullet(f), L_p^\bullet(g)$ are not directly related to twisted L-values, and so the arguments of [GV00, §3] do not suffice to cover this case. Nonetheless, it should be possible to exploit the result of [Vat99, Prop. 1.7], which amounts to the congruence

$$L_p^{\Sigma,\star}(f, \zeta - 1) \equiv u L_p^{\Sigma,\star}(g, \zeta - 1) \pmod{p\mathbf{Z}_p[\zeta]}$$

for both $\star \in \{\alpha, \beta\}$, together with (1.6) to establish (1.7). This will involve a detailed analysis of the values of $M_{\log}$ at p-power roots of unity, for which some of the calculations in [LLZ17] (see esp. [*loc.cit.*, Lem. 3.7]) might be useful.

[1] Extending earlier work of Kobayashi, Pollack, Lei, and Sprung

Remark 1.1. The algebraic analogue of Project A has recently been established by Hatley–Lei (see [HL16, Thm. 4.6]). On the other hand, as shown in [LLZ11, Cor. 6.6], either of the main conjectures (1.5) is equivalent to Kato's main conjecture (see [LLZ11, Conj. 6.2]). Thus from the discussion of §1.2 and the main result of [KKS17], we see that a successful completion of Project A would yield[2] cases of the signed main conjectures beyond those covered by [Wan14] or [CÇSS17, Thm. B], where the following hypothesis is needed:

$$\text{there exists a prime } \ell \neq p \text{ with } \ell \| N \text{ such that } \bar{\rho}_f \text{ is ramified at } \ell.$$

(*cf.* [KKS17, §1.2.3]).

1.4. **On the anticyclotomic main conjecture of Bertolini–Darmon–Prasanna.** Here we let F_∞/F be the anticyclotomic $\mathbf{Z}_p$-extension of an imaginary quadratic field K in which

$$p = \mathfrak{p}\overline{\mathfrak{p}} \text{ splits},$$

let $f \in S_k(\Gamma_0(N))$, and let $p \nmid N$ be a prime. Assume also that every prime factor of N splits in K; so K satisfies the *Heegner hypothesis*, and $N^- = 1$ with the standard notation.

The Iwasawa–Greenberg main conjecture for the p-adic L-function $L_{\mathfrak{p}}(f) \in \overline{\mathbf{Z}}_p[[\mathrm{Gal}(F_\infty/F)]]$ introduced in [BDP13] predicts that

$$\mathrm{Char}_\Lambda(\mathrm{Sel}_{\mathfrak{p}}(f)^\vee)\Lambda_{\overline{\mathbf{Z}}_p} \stackrel{?}{=} (L_{\mathfrak{p}}(f)), \tag{1.8}$$

where $\Lambda_{\overline{\mathbf{Z}}_p} = \overline{\mathbf{Z}}_p[[T]]$ and $\mathrm{Sel}_{\mathfrak{p}}(f)$ is a Selmer group defined by imposing local triviality (resp. no condition) at the primes above $\mathfrak{p}$ (resp. $\overline{\mathfrak{p}}$).

Project B. *Show* **Expectation 1** *for the p-adic L-functions of* [BDP13]. *That is, if $f \equiv g \pmod p$, then $\mu(L_{\mathfrak{p}}(f)) = \mu(L_{\mathfrak{p}}(g)) = 0$[3] and the λ-invariants of Σ-imprimitive versions of $L_{\mathfrak{p}}(f)$ and $L_{\mathfrak{p}}(g)$ are equal.*

Similarly as for Project A, in weight $k = 2$ this problem can be reduced to establishing the congruence

$$L_{\mathfrak{p}}^{\Sigma}(f, \zeta - 1) \equiv u L_{\mathfrak{p}}^{\Sigma}(g, \zeta - 1) \pmod{p\overline{\mathbf{Z}}_p[\zeta]} \tag{1.9}$$

for all $\zeta \in \mu_{p^\infty}$ and some $u \in \overline{\mathbf{Z}}_p^\times$ independent of ζ. Now, by the p-adic Waldspurger formula of [BDP13, Thm. 5.13], the congruence of [KL16, Thm. 2.9] amounts to (1.9) for $\zeta = 1$, and so a promising approach to Project B would be based on extending the result of [KL16, Thm. 2.9] to ramified characters.

Remark 1.2. When p is a good *ordinary* prime, the algebraic analogue of Project B has recently been established by Hatley–Lei (see [HL17, Prop. 4.2 and Thm. 5.4]). On the other hand, one can show that Howard's divisibility towards Perrin-Riou's Heegner point main conjecture implies one of the divisibilities predicted by (1.8) (see [How04, Thm. B] and [Cas17b, App. A]). Similarly as in [KKS17], it should be possible to show (this is work in progress) that a suitable refinement of the Kolyvagin system arguments of [How04] combined with Wei Zhang's proof of Kolyvagin's conjecture [Zha14][4] yields the full equality (1.8). In particular, this would yield new cases of conjecture (1.8) with $N^- = 1$ (not currently available in the literature), and even more cases (under a somewhat weaker version of Hypothesis ♠ in [Zha14], still with $N^- = 1$) after a successful completion of Project B.

Finally, in line with the previous remark, we note that the following should be possible:

Project C. *Extend the results of* [HL17] *to the non-ordinary case.*

[2] Subject to the nonvanishing mod p of some "Kurihara number"

[3] Note that in this case the vanishing of μ-invariants is known under mild hypotheses by [Hsi14, Thm. B] and [Bur17, Thm. B]

[4] Which can be seen as proving "primitivity" in the sense of [MR04] of the Heeger point Kolyvagin system

1.5. **On the p-part of the Birch–Swinnerton-Dyer formula for residually reducible primes.** Here we consider the primes $p > 2$ for which the associated residual representation $\bar{\rho}_f$ is *reducible*. For simplicity, assume that f corresponds to an elliptic curve $E/\mathbf{Q}$ (admitting a rational p-isogeny with kernel Φ). The combination of [GV00, Thm. 3.12] (with a key input from [Kat04, Thm. 17.4]) and [Gre99, Thm.4.1] yields the p-part of the BSD formula for E in analytic rank 0, i.e., when $L(E,1) \neq 1$, provided the following holds:

(GV) the $G_{\mathbf{Q}}$-action on $\Phi \subset E[p]$ is either $\begin{cases} \text{ramified at } p \text{ and even, or} \\ \text{unramified at } p \text{ and odd.} \end{cases}$

Similarly as in the residually irreducible cases considered in [JSW17], the above result (applied to a suitable quadratic twist of E) would be an important ingredient in the following:

Project D. *Prove the p-part of the BSD formula in analytic rank* 1 *for elliptic curves E and primes $p > 2$ for which* (GV) *does not hold.*

Following the strategy of [JSW17] and [Cas17a], a key ingredient toward this[5] would be the proof of the relevant cases of the anticyclotomic main conjecture (1.8). By the discussion in §1.2, this could be approached in the following steps:

(1) establish the divisibility "$\supseteq$" in (1.8) (possibly after inverting p), based on a suitable refinement of the Kolyvagin system argument in [How04].
(2) show that $\mu(L_{\mathfrak{p}}(f)) = 0$ based on the congruence of [Kri16, Thm. 3] between $L_{\mathfrak{p}}(f)$ and an anticyclotomic Katz p-adic L-function, and Hida's results on the vanishing of μ for the latter.
(3) letting $L_{\mathfrak{p}}^{\mathrm{alg}}(f)$ be a generator of the characteristic ideal in (1.8), show that $\mu(L_{\mathfrak{p}}^{\mathrm{alg}}(f)) = 0$ and $\lambda(L_{\mathfrak{p}}^{\mathrm{alg}}(f)) = \lambda(L_{\mathfrak{p}}(f))$ based on an algebraic counterpart of [Kri16, Thm. 3] and the known cases of the main conjecture for the anticyclotomic Katz p-adic L-function.

After this is carried out, we could try to study the missing cases:

Project E. *Prove the p-part of the BSD formula for elliptic curves $E/\mathbf{Q}$ at residually reducible primes $p > 2$ when:*

- *$L(E,1) \neq 0$ and* (GV) *doesn't hold (complementing the cases that follow from* [GV00]*).*
- *$\mathrm{ord}_{s=1} L(E,s) = 1$ and* (GV) *holds (complementing the cases covered by* Project D*).*

Finally, we should note that $p = 2$ has been neglected throughout the above discussion, but one would of course like to understand this case as well. (See e.g. [CLZ17] for recent results in this direction.)

References

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148.

[Bur17] Ashay 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** (2017), no. 1, 189–222. MR 3591965

[Cas17a] Francesc Castella, *On the p-part of the Birch–Swinnerton-Dyer formula for multiplicative primes*, Camb. J. Math., to appear (2017).

[Cas17b] ———, *p-adic heights of Heegner points and Beilinson-Flach classes*, J. Lond. Math. Soc. (2) **96** (2017), no. 1, 156–180. MR 3687944

[CÇSS17] Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On two-variable main conjectures for modular forms at non-ordinary primes*, preprint (2017).

[CLZ17] Li Cai, Chao Li, and Shuai Zhai, *On the* 2*-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists fo elliptic curves*, preprint, `arXiv:1712.01271` (2017).

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[5] Note that there are other points where the residually irreducible hypothesis is used in [JSW17], e.g. in the "anticyclotomic control theorem" of [*loc.cit.*, §3.3], but handling these should be relatively easy.

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63. MR 1784796

[HL16] Jeffrey Hatley and Antonio Lei, *Arithmetic properties of signed Selmer groups at non-ordinary primes*, preprint, `arXiv:1608.00257` (2016).

[HL17] ———, *Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms*, preprint, `arXiv:1706.04531` (2017).

[How04] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472. MR 2098397 (2006a:11070)

[Hsi14] Ming-Lun Hsieh, *Special values of anticyclotomic Rankin-Selberg L-functions*, Doc. Math. **19** (2014), 709–767. MR 3247801

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434. MR 3684675

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III. MR 2104361 (2006b:11051)

[KKS17] Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun, *On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms*, preprint, `arXiv:1709.05780` (2017).

[KL16] Daniel Kriz and Chao Li, *Congruences between Heegner points and quadratic twists of elliptic curves*, preprint, `arXiv:1606.03172` (2016).

[Kri16] Daniel Kriz, *Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-function*, Algebra Number Theory **10** (2016), no. 2, 309–374. MR 3477744

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528.

[LLZ11] ———, *Coleman maps and the p-adic regulator*, Algebra Number Theory **5** (2011), no. 8, 1095–1131. MR 2948474

[LLZ17] ———, *On the asymptotic growth of Bloch-Kato-Shafarevich-Tate groups of modular forms over cyclotomic extensions*, Canad. J. Math. **69** (2017), no. 4, 826–850. MR 3679697

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR 2031496 (2005b:11179)

[Vat99] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419. MR 1695203

[Wan14] Xin Wan, *Iwasawa main conjecture for supersingular elliptic curves*, preprint, `arXiv:1411.6352` (2014).

[Zha14] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253. MR 3295917