University of Cambridge
Department of Pure Mathematics and Mathematical Statistics

# The Coates-Wiles Theorem

Alexandre Daoud
Homerton College

Submitted in part fulfilment of the requirements for the degree of
Master in Advanced Studies in Mathematics of the University of Cambridge, May 2017

# Abstract

Let $E$ be an elliptic curve with complex multiplication by an order in an imaginary quadratic field $K$ of class number 1 and $\psi_E$ its associated Hecke character. The Coates-Wiles Theorem states that if the Hecke $L$-function $L(\overline{\psi_E}, s)$ is non-vanishing at $s = 1$ then $E(K)$ is finite. This theorem fits into the larger framework of the Birch and Swinnerton-Dyer conjecture which remains open to this day. In this essay we will explore Rubin's proof of the Coates-Wiles Theorem via the machinery of abstract Euler systems. In particular, we will construct the Euler system of elliptic units by using torsion points of $E$ to generate global units in abelian extensions of $K$. We will then use a modified Selmer group to reduce the problem down to studying a particular ideal class group and the group of global units of $K$. Using the Euler system, we will be able to annihilate this class group whence the Coates-Wiles Theorem will follow via an application of the well-known Chebotarev Density Theorem and Mordell-Weil Theorem.

# Contents

# Chapter 1

# Introduction

The Birch and Swinnerton-Dyer conjecture has tantalised mathematicians for the better part of five decades. Its difficulty and importance is surely confirmed by its current status as one of the Clay Mathematics Insitute Millennium Problems. It was first put forward by Bryan Birch and Peter Swinnerton-Dyer in the mid 1960s in light of numerical evidence gathered using the early computers of the era. To date it remains the most well-verified open problem in Number Theory due mostly to its exact formulation rather than asymptotic nature. The Birch and Swinnerton-Dyer conjecture, henceforth BSD conjecture, usually takes the form of two statements known as the weak and strong BSD conjectures which are stated as follows

**Conjecture** (Weak BSD). *Let $E$ an elliptic curve defined over $\mathbb{Q}$ and $L(E,s)$ its $L$-function. Then the rank of the abelian group $E(K)$ is equal to the order of vanishing $L(E,s)$ at $s=1$.*

**Conjecture** (Strong BSD). *Let $E$ an elliptic curve defined over $\mathbb{Q}$ of rank $r$ and $L(E,s)$ its $L$-function. Then*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\frac{\Omega_E \mathrm{Reg}(E)|Ш(E)|\prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}$$

*where $\Omega_E=\int_{E(\mathbb{R})}|\omega_E|$, $\mathrm{Reg}(E)$ is the elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, $Ш(E)$ is the Tate-Shafarevich group of $E$ and $c_p=|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$ is the Tamagawa number of $E/\mathbb{Q}_p$.*

It is perhaps not very surprising that the strong BSD conjecture remains unproven considering the appearance of the cardinality of the Tate-Shafarevich group in the above formula. This quantity has been proven finite for certain elliptic curves such that $L(E,1)\neq 0$ by the work of Karl Rubin ([Rub87]). Moreover, Victor Kolyvagin ([Kol89]) showed that if the order of vanishing of $L(E,1)$ is either 0 or 1 then the weak BSD conjecture holds and the Tate-Shafarevich group is finite. The finiteness of the Tate-Shafarevich group remains, however, an open problem in the general case.

Rubin's work on the finiteness of the Tate-Shafarevich group built upon the earlier work of John Coates and Andrew Wiles in their paper [CW77] in which they proved the following result

**Theorem** (Coates-Wiles). *Let $K$ be an imaginary quadratic number field with class number 1 and $E$ an elliptic curve over $K$ with complex multiplication by an order in $\mathcal{O}_K$. If the Hecke $L$-function $L(\overline{\psi_E},s)$ is non-vanishing at $s=1$ then $E(K)$ is finite.*

It is immediately clear that the Coates-Wiles Theorem implies that the predictions made by the weak BSD conjecture (in the case of general number fields) hold. The goal of this essay shall be to provide a detailed exposition of Rubin's proof of the Coates-Wiles Theorem given in his paper [Rub99]. The proof is indeed a tour de force in the theory of complex multiplication and elliptic units along with abstract Euler systems and, as such, we will provide a comprehensive account of all the complex machinery involved.

Chapter 2 will be concerned with calculating a particular Selmer group. We will define a modified Selmer group in which we relax the usual cohomological conditions. We will be able to completely determine this modifed

Selmer group in the cases that are of interest to us which will then allow us to home in on the structure of the normal Selmer group. We will furthermore show that we can annihilate the true Selmer group using our modified one together with a certain Kummer pairing and a condition on a particular ideal class group.

In Chapter 3 we will construct the elliptic units which are a collection of global units in particular abelian extensions of an imaginary quadratic number field. We shall show that they satisfy a distribution relation analogous to that of cyclotomic units in cyclotomic fields. Moreover, we shall demonstrate a connection between such elliptic units and the Hecke $L$-function of an elliptic curve with complex multiplication.

Chapter 4 will see us constructing abstract Euler systems which axiomatise the phenomenae exhibited by the cyclotomic and elliptic units. In particular, we shall define a so-called $\mathfrak{p}$-system which shall act as a framework to which we may attach a *universal* Euler system. After proving some useful properties of Euler systems, we will go on to constructing principal ideals in $\mathfrak{p}$-systems. We then go on to showing how to bound and annihilate an ideal class group using these principal ideals as relations.

In Chapter 5, we will finally provide the proof of the Coates-Wiles Theorem by exploiting the machinery developed over the course of the essay, together with the Chebotarev Density Theorem of class field theory and the Mordell-Weil Theorem.

Throughout this essay we shall assume that the reader is familiar with the elementary theory of elliptic curves, complex multiplication and global class field theory. This being said, an appendix has been provided which provides an account of well-known and important statements in the aforementioned fields used in this essay. Should the reader find any confusion with notation, he or she is invited to view the Notation Index at the end of this document and, indeed, the appendix.

# Chapter 2

# Calculation of the Selmer Group

The aim of this chapter is to calculate the $\pi^n-$Selmer group $\mathrm{S}^{(\pi^n)}(E/K)$ where $K$ is an imaginary quadratic field with class number one and $\pi$ is the generator of some finite prime $\mathfrak{p}$ of K. We shall do this via slightly relaxing the conditions on the classical Selmer group to give us a modified Selmer group which contains the original one. Through cohomological methods and class field theory, we will be able to completely determine $\mathrm{S}^{(\pi^n)}(E/K)$ in terms of homomorphisms of subgroups of the idèle class group of a certain finite extension of $K$. In consequence, we will be able to give a simple condition for when the $\pi$-Selmer group is trivial in terms of the ideal class group and global units of $K(E[\mathfrak{p}])$.

## 2.1 Galois Cohomology of Torsion Points

*Assumptions.* Throughout this section, we shall assume that $F$ is a field of characteristic zero and $E/F$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ for some quadratic imaginary number field $K$.

We begin by proving a well-known Lemma in the elementary theory of group cohomology.

**Lemma 2.1.1** (Sah's Lemma). *Let $G$ be a group, $M$ a $G$-module and $h$ an element of the centre of $G$. Then $H^n(G, M)$ is annihilated by the endomorphism*

$$\begin{aligned} \sigma : M &\to M \\ x &\mapsto x^h - x \end{aligned}$$

*of $M$ for all $n \geq 0$. In particular, if $\sigma$ is an automorphism then $H^n(G, M) = 0$ for all $n \geq 0$.*

*Proof.* Consider the endomorphism of $M$ given by the action of $h$. Write $h^*$ for the induced homomorphism $h^* : H^*(G, M) \to H^*(G, M)$ of cohomology groups. It is a standard fact of the cohomology of groups that $h^* = \mathrm{id}$ and so $h^* - \mathrm{id} = 0$. On the other hand, let $f \in C^n(G, M)$. Then $h^n$ acts on $f$ by

$$h^n(f) = f(h^{-1}g_1h, \ldots, h^{-1}g_nh)^h = f(g_1, \ldots, g_n)^h$$

where we have used the fact that $h$ is in the centre of $G$. Hence $h^*$ is simply given on the cohomology groups by the action of $h$. Therefore, given a cohomology class $[f] \in H^*(G, M)$, we have

$$[0] = (h^* - \mathrm{id})[f] = h[f] - f$$

as desired. □

**Proposition 2.1.2.** *Let $p > 3$ be a rational prime and $\mathfrak{p}$ a finite prime of $K$ lying above $p$. Given $n \in \mathbb{N}$, let $C_n$ be a subgroup of $(\mathcal{O}_K/\mathfrak{p}^n)^\times$ and consider $\mathcal{O}_K/\mathfrak{p}^n$ as a $C_n$-module via the natural multiplicative action. If $C_n$ is cyclic or not a $p$-group then for all $i \in \mathbb{N}$ we have $H^i\left(C_n, \mathcal{O}_K/\mathfrak{p}^n\right) = 0$.*

*Proof.* First suppose that $C_n$ is cyclic. Fix $h \neq 1$ in $C_n$. Then $x \mapsto hx - x$ is an automorphism of $\mathcal{O}_K/\mathfrak{p}^n$. Appealing to Sah's Lemma, we see that $H^1(C_n, \mathcal{O}_K/\mathfrak{p}^n) = 0$.

Now suppose that $C_n$ is not a $p$-group. Let $C_n'$ be its prime-to-$p$ part. Then for all $i \in \mathbb{N}$ we have $H^i(C_n', \mathcal{O}_K/\mathfrak{p}^n) = 0$ since the order of $C_n'$ is prime to the order of $\mathcal{O}_K/\mathfrak{p}^n$. By the inflation-restriction sequence, we have

$$0 \longrightarrow H^1\left(C_n/C_n', (\mathcal{O}_K/\mathfrak{p}^n)^{C_n'}\right) \longrightarrow H^1(C_n, \mathcal{O}_K/\mathfrak{p}^n) \longrightarrow H^1(C_n', \mathcal{O}_K/\mathfrak{p}^n)$$

whence $H^1(C_n, \mathcal{O}_K/\mathfrak{p}^n) = 0$. □

**Proposition 2.1.3.** *Let $p > 3$ be a rational prime, $\mathfrak{p}$ a finite prime of $K$ lying over $p$ and $n \in \mathbb{N}$. If either $\mathcal{O}_{K,\mathfrak{p}} = \mathbb{Z}_p$ or $E[\mathfrak{p}] \not\subseteq E(F)$ then the cohomological restriction map induces an isomorphism*

$$H^1(F, E[\mathfrak{p}^n]) \cong H^1(F(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^{\mathrm{Gal}(F(E[\mathfrak{p}^n])/F)}$$

*Proof.* By Theorem A.7.2, we have $E[\mathfrak{p}^n] \cong \mathcal{O}_K/\mathfrak{p}^n$. This Theorem furthermore implies that $G = \mathrm{Gal}(F(E[\mathfrak{p}^n])/F) \subseteq (\mathcal{O}_K/\mathfrak{p}^n)^\times$. Now, in the case that $\mathcal{O}_{K,\mathfrak{p}} = \mathbb{Z}_p$, we have that $G$ is cyclic. Indeed,

$$\mathcal{O}_K/\mathfrak{p}^n \cong \mathcal{O}_{K,\mathfrak{p}^n}/\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}^n} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

which is cyclic. In the case that $E[\mathfrak{p}] \not\subseteq E(F)$ then $G$ is not a $p$-group since it has order prime to $p$.

Now consider the inflation-restriction sequence

$$0 \longrightarrow H^1(G, E[\mathfrak{p}^n]^G) \longrightarrow H^1(F, E[\mathfrak{p}^n]) \longrightarrow H^1(F(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^G \longrightarrow H^2(G, E[\mathfrak{p}^n]^G)$$

By Proposition 2.1.2, the second and last terms in this sequence are 0 and so we obtain the desired isomorphism. □

**Proposition 2.1.4.** *Let $p > 3$ be a rational prime, $\mathfrak{p}$ a finite prime of $K$ lying over $p$ and $n \in \mathbb{N}$. Let $l \neq p$ be a rational prime and $F$ a finite extension of $\mathbb{Q}_l$. Then the cohomological restriction map induces an injection*

$$H^1(F, E)_{\mathfrak{p}^n} \hookrightarrow H^1(F(E[\mathfrak{p}^n]), E)_{\mathfrak{p}^n}$$

*Proof.* For notational convenience, denote $F_n = F(E[\mathfrak{p}^n])$. Using the inflation-restriction sequence we obtain an exact sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(F_n/F), E(F_n))_{\mathfrak{p}^n} \longrightarrow H^1(F, E)_{\mathfrak{p}^n} \longrightarrow H^1(F_n, E)_{\mathfrak{p}^n}$$

By Theorem A.7.3, $E$ has good reduction over $F_n$ so $\overline{E} = \overline{E}_{\mathrm{ns}}$ and $E_0(F_n) = E(F_n)$. Proposition A.5.1 then yields an exact sequence

$$0 \longrightarrow E_1(F) \longrightarrow E(F_n) \longrightarrow \overline{E}(\mathbb{F}_n) \longrightarrow 0$$

where $\mathbb{F}_n$ is the residue field of $F_n$. Now consider the logarithm map $\lambda_E : E_1(F_n) \to \mathcal{O}_{F_n}$. This has finite kernel of $l$-power order and maps $E_1(F_n)$ onto an open subgroup of $\mathcal{O}_{F_n}$. Hence $E_1(F_n)$ is a finitely generated profinite $\mathbb{Z}_l$-module. We may view $E_1(F_n)$ as an $\mathcal{O}_K$-module which is still profinite[1] as restricting to an $\mathcal{O}_K$-module does not change the topology on $E_1(F_n)$.

We now claim that $E_1(F_n)$ is a pro-$\mathfrak{p}$ $\mathcal{O}_K$-module. Indeed, Proposition A.5.7 implies that every $\alpha \in \mathcal{O}_K$ prime to $l$ is an automorphism of $E_1(F_n)$. Fix such an $\alpha \in \mathcal{O}_K$. Then for all subgroups $G$ of $E_1(F_n)$, $\alpha$ acts as a

[1] Recall that a topological group is profinite if and only if it is compact, Hausdorff and totally-disconnected.

surjective endomorphism of $E_1(F_n)/G$. If $G$ has finite index in $E_1(F_n)$ then $\alpha$ is moreover an automorphism of $E_1(F_n)/G$. Since this holds for all $\alpha \in \mathcal{O}_K$ prime to $l$, $E_1(F_n)/G$ is a $p$-group and so $E_1(F_n)$ is pro-$\mathfrak{p}$.

From the exact sequence above, we see that $E_1(F)$ has finite index in $E(F_n)$ and so the pro-$\mathfrak{p}$ part of $E(F_n)$ is finite, say $E[\mathfrak{p}^m]$ for some $m \geq n$. We thus have an inclusion

$$H^1(F_n/F, E(F_n))_{\mathfrak{p}^n} \subseteq H^1(F_n/F, E[\mathfrak{p}^m]) = H^1(F(E[\mathfrak{p}^m])/F, E[\mathfrak{p}^m])$$

Now note that if $E[\mathfrak{p}] \not\subseteq E(F)$ then $\mathrm{Gal}(F(E[\mathfrak{p}^m])/F, E[\mathfrak{p}^m])$ is not a $p$-group. Conversely, if $E[\mathfrak{p}] \subseteq E(F)$ then $E$ has good reduction by Theorem A.7.3 and that the residue characteristic is greater than 3. Appealing to Corollary 3.17, $F_n/F$ is an unramified extension so, in particular, its Galois group is cyclic. Hence either case yields $H^1(F(E[\mathfrak{p}^m])/F, E[\mathfrak{p}^m]) = 0$ upon applying Lemma 2.1.2. □

## 2.2 The Relaxed Selmer Group

*Assumptions.* Throughout this section, we shall assume that $L$ is a number field and $E/L$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ for some quadratic imaginary number field $K$.

Recall for all non-constant $\alpha \in \mathcal{O}_K$ we have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & E(L)/\alpha E(L) \arrow[r] \arrow[d] & H^1(L, E[\alpha]) \arrow[r] \arrow[d, "\text{res}"] \arrow[dr, dotted] & H^1(L, E)_\alpha \arrow[r] \arrow[d, "\text{res}"] & 0 \\
0 \arrow[r] & E(L_\mathfrak{q})/\alpha E(L_\mathfrak{q}) \arrow[r] & \prod_{\mathfrak{q} \in M_K} H^1(L_\mathfrak{q}, E[\alpha]) \arrow[r] & \prod_{\mathfrak{q} \in M_K} H^1(L_\mathfrak{q}, E)_\alpha \arrow[r] & 0
\end{tikzcd}$$

where we define the $\alpha$-Selmer group $\mathrm{S}^{(\alpha)}(E)$ to be the kernel of the dotted homomorphism. In his paper [Coa83], Coates defined a slightly larger Selmer group which can be calculated relatively easily using cohomological methods coupled with class field theory.

**Definition 2.2.1.** Let $\alpha \in \mathcal{O}_K$. We define the **relaxed $\alpha$-Selmer group** to be

$$\mathcal{S}^{(\alpha)}(E) = \{\, c \in H^1(L, E[\alpha]) \mid \mathrm{res}_\mathfrak{q}(c) = 0 \text{ in } H^1(L_\mathfrak{q}, E) \text{ for all } \mathfrak{q} \in M_L^{\nmid\infty} \text{ with } (\mathfrak{q}, (\alpha)) = 1 \,\}$$

It is immediate from the definitions that $\mathrm{S}^{(\alpha)}(E) \subseteq \mathcal{S}^{(\alpha)}(E)$. Furthermore, by the usual exactness of the second row of the above diagram, we also have the equivalent definition

$$\mathcal{S}^{(\alpha)}(E) = \{\, c \in H^1(L, E[\alpha]) \mid \mathrm{res}_\mathfrak{q}(c) = 0 \text{ in } H^1(L_\mathfrak{q}, E(\overline{L_\mathfrak{q}})) \text{ for all } \mathfrak{q} \in M_L^{\nmid\infty} \text{ with } (\mathfrak{q}, (\alpha)) = 1 \,\}$$

**Proposition 2.2.2.** *Let $n \in \mathbb{N}_{\geq 1}$ and $\mathfrak{p}$ a finite prime of $K$ prime to 6 and lying over a rational prime $p$. Suppose that $\mathfrak{p}^n$ is principal with generator $\alpha$ and that $E[\mathfrak{p}^n] \subseteq E(L)$. Then*

$$\mathcal{S}^{(\alpha)}(E/L) = \mathrm{Hom}(\mathrm{Gal}(\mathcal{M}/L), E[\mathfrak{p}^n]))$$

*where $\mathcal{M}$ is the maximal $p$-extension*[2] *of $L$ unramified outside of primes lying above $\mathfrak{p}$.*

*Proof.* We first observe that since $E(\mathfrak{p}^n) \subseteq E(L)$, the $G_L$ and $G_{L_\mathfrak{q}}$-actions on $E[\mathfrak{p}^n]$ are trivial for all finite primes $\mathfrak{q}$ of $L$ and so

$$H^1(L, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_L, E[\mathfrak{p}^n])$$
$$H^1(L_\mathfrak{q}, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_{L_\mathfrak{q}}, E[\mathfrak{p}^n])$$

[2] Recall that a $p$-extension of fields is a Galois extension whose Galois group is pro-$p$

Now fix a prime $\mathfrak{q}$ of $L$ not lying over $\mathfrak{p}$. Theorem A.7.3 and the fact that the residue characteristic is greater than 3 imply that $E$ has good reduction at $\mathfrak{p}$. Appealing to Proposition A.5.8, we see that $L_{\mathfrak{q}}(E[\alpha])/L_{\mathfrak{q}}$ is unramified. Letting $I_{\mathfrak{q}}$ denote the absolute inertia group of $L_{\mathfrak{q}}$, we see that $I_{\mathfrak{q}}$ acts trivially on $E[\alpha]$ whence the image of $E(L_{\mathfrak{q}})/\alpha E(L_{\mathfrak{q}})$ under the Kummer map is contained in $\mathrm{Hom}(G_{L_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$.

Let $\mathbb{F}_{\mathfrak{q}}$ be the residue field of $L_{\mathfrak{q}}$ and $q = \mathbf{N}_{L/\mathbb{Q}}\,\mathfrak{q}$. We next observe that

$$G_{L_{\mathfrak{q}}}\big/I_{\mathfrak{q}} \cong \mathrm{Gal}\left(\overline{\mathbb{F}_{\mathfrak{q}}}/\mathbb{F}_{\mathfrak{q}}\right) \cong \varprojlim_{n\in\mathbb{N}_{\geq 1}} \mathrm{Gal}\left(\mathbb{F}_{q^n}/\mathbb{F}_q\right) \cong \varprojlim_{n\in\mathbb{N}_{\geq 1}} \mathbb{Z}\big/n\mathbb{Z} \cong \prod_{\text{rational } p} \mathbb{Z}_p$$

Suppose we are given a homomorphism $\varphi \in \mathrm{Hom}(G_{L_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$. Since the finite homomorphic image of a pro-$p$ group is a $p$-group, only the $\mathbb{Z}_p$-part of $G_{L_{\mathfrak{q}}}/I_{\mathfrak{q}}$ can contribute to $\varphi$. By Lagrange's Theorem, only the $\mathbb{Z}/p^i\mathbb{Z}$-parts of $\mathbb{Z}_p$ for $1 \leq i \leq \mathbf{N}\mathfrak{p}^n$ contribute to $\varphi$. We may thus conclude that

$$\mathrm{Hom}\left(G_{L_{\mathfrak{q}}}\big/I_{\mathfrak{q}}, E[\mathfrak{p}^n]\right) \cong \mathrm{Hom}\left(G_{L_{\mathfrak{q}}}\big/I_{\mathfrak{q}}, \mathcal{O}_K\big/\mathfrak{p}^n\right) \cong \mathcal{O}_K\big/\mathfrak{p}^n$$

Conversely, appealing to Proposition A.5.7 yields

$$E(L_{\mathfrak{q}})/\alpha E(L_{\mathfrak{q}}) \cong \overline{E}(\mathbb{F}_{\mathfrak{q}})/\alpha\overline{E}(\mathbb{F}_{\mathfrak{q}}) \cong \mathcal{O}_K\big/\mathfrak{p}^n$$

Therefore, the image of $E(L_{\mathfrak{q}})/\alpha E(L_{\mathfrak{q}})$ under the Kummer map is equal to $\mathrm{Hom}(G_{L_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$. We then have that

$$\mathcal{S}^{(\alpha)}(E/F) = \{\, \sigma \in \mathrm{Hom}(G_L, E[\alpha]) \mid \sigma \in \mathrm{Hom}(G_{L_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\alpha]) \text{ for all } \mathfrak{q} \in M_L^{\nmid\infty} \text{ with } (\mathfrak{q}, (\alpha)) = 1 \,\}$$

But this is exactly $\mathrm{Hom}(\mathrm{Gal}(\mathcal{M}/F), E[\mathfrak{p}^n])$ as desired. □

**Corollary 2.2.3.** *Suppose that $E$ is defined over $K$ and let $n \geq 1$ and $\mathfrak{p}$ be a finite prime of $K$ prime to 6. Furthermore, suppose that $\mathfrak{p}^n$ is principal with generator $\alpha$. Denoting $K_n = K(E[\mathfrak{p}^n])$ and $G_n = \mathrm{Gal}(K_n/K)$ we have*

$$\mathcal{S}^{(\alpha)}(E/K) = \mathrm{Hom}(\mathrm{Gal}(\mathcal{M}_n, K_n), E[\mathfrak{p}^n])^{G_n}$$

*where $\mathcal{M}_n$ is the maximal abelian $p$-extension of $K_n$ unramified outside of primes lying above $\mathfrak{p}$.*

*Proof.* We claim that $\mathcal{S}^{(\alpha)}(E/K) = \mathcal{S}^{(\alpha)}(E/K_n)^{G_n}$. If this were indeed the case then Proposition 2.2.2 would imply that $\mathcal{S}^{(\alpha)}(E/K_n) = \mathrm{Hom}(\mathrm{Gal}(\mathcal{M}_n/K_n), E[\mathfrak{p}^n])^{G_n}$ and the Corollary then follows.

We now prove the aforementioned claim. Since $\mathfrak{p}$ is prime to 6 (and, in particular, 2 and 3) the map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p})^\times$ is not surjective. Appealing to Proposition A.7.8 shows that $E[\mathfrak{p}] \not\subseteq E(L)$. We may thus apply Proposition 2.1.3 to establish an isomorphism

$$H^1(K, E[\mathfrak{p}^n]) \cong H^1(K_n, E[\mathfrak{p}^n])^{G_n}$$

It is then immediately clear that the image of $\mathcal{S}^{(\alpha)}(E/K)$ under this isomorphism is contained in $\mathcal{S}^{(\alpha)}(E/K)$.

On the other hand, Proposition 2.1.4 implies that the restriction map

$$H^1(K_{\mathfrak{q}}, E(\overline{K_{\mathfrak{q}}}))_{\mathfrak{p}^n} \to H^1(K_{\mathfrak{q}}(E[\mathfrak{p}^n]), E(\overline{K_{\mathfrak{q}}}))_{\mathfrak{p}^n}$$

is injective for all primes $\mathfrak{q}$ such that $(\mathfrak{q}, \mathfrak{p}) = 1$. From this we may deduce that every element of $H^1(K, E[\mathfrak{p}^n])$ whose image under $\mathrm{res}_{\mathfrak{q}}$ is an element of $\mathcal{S}^{(\alpha)}(E/K_n)$ is also a member of $\mathcal{S}^{(\alpha)}(E/K)$. This shows that $\mathcal{S}^{(\alpha)}(E/K) = \mathcal{S}^{(\alpha)}(E/K_n)^{G_n}$ and so the claim is proven. □

This concludes the cohomological calculations needed for the relaxed Selmer group. We observe that by calculating these relaxed Selmer groups, we have managed to establish $\mathfrak{q}$-adic control over the classical $\alpha$-Selmer groups for all finite primes $\mathfrak{q}$ not dividing $\alpha$. In the sequel, we shall make use of a certain pairing to establish the remaining $\mathfrak{p}$-adic control (for $\mathfrak{p}$ dividing $\alpha$) over the classical $\alpha$-Selmer group.

## 2.3 The Kummer Pairing

In this section we shall introduce a Kummer pairing which is an analogue of the classical one arising in the theory of elliptic curves over number fields. We refer the interested reader to [Sil09, p.209] where he or she may find a construction of the classical Kummer pairing.

*Assumptions.* Throughout this section, we shall assume that $E$ is an elliptic curve defined over an imaginary quadratic number field $K$ with complex multiplication by $\mathcal{O}_K$. By Proposition A.7.4, this implies that $K$ has class number one. Furthermore $\mathfrak{p} = \pi\mathcal{O}_K$ shall be a finite prime of $K$, prime to $\mathfrak{f}$, for some generator $\pi$. Finally, $[\cdot, F^{\text{ab}}/F]$ shall refer to the local Artin map; when necessary, we shall write $\sigma_x = [x, F^{\text{ab}}/F]$ to ease notation.

**Lemma 2.3.1.** *Let $\lambda_E : E_1(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_{\mathfrak{p},K}$ be the logarithm map. Then $\lambda_E$ extends uniquely to a surjective map $E(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_{\mathfrak{p},K}$ whose kernel is finite and has no $\mathfrak{p}$-torsion.*

*Proof.* Recall that $\lambda_E : E_1(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_{\mathfrak{p},K}$ is an isomorphism. Since $\mathfrak{p}$ is prime to $\mathfrak{f}$, $K$ has good reduction at $\mathfrak{p}$. Appealing to Proposition A.5.1 we obtain an exact sequence

$$0 \longrightarrow E_1(K_\mathfrak{p}) \longrightarrow E(K_\mathfrak{p}) \longrightarrow \overline{E}(\mathbb{F}_\mathfrak{p}) \longrightarrow 0$$

where $\mathbb{F}_\mathfrak{p}$ is the residue field of $K_\mathfrak{p}$. We thus see that $E(K_\mathfrak{p})/E_1(K_\mathfrak{p})$ is finite. Finally from Proposition A.5.4 we conclude that $E(K_\mathfrak{p})/E_1(K_\mathfrak{p})$ has no $\mathfrak{p}$-torsion. □

**Definition 2.3.2.** Let $n \in \mathbb{N}_{\geq 1}$ and denote $K_{\mathfrak{p},n} = K_\mathfrak{p}(E[\mathfrak{p}^n])$. We define the **$\boldsymbol{\pi^n}$-Kummer pairing** to be the map

$$\begin{aligned} \langle \cdot, \cdot \rangle_{\pi^n} : E(K_\mathfrak{p}) \times K_{\mathfrak{p},n}^\times &\to E[\mathfrak{p}^n] \\ (P, x) \quad &\mapsto [x, K_{\mathfrak{p},n}^{\text{ab}}/K_{\mathfrak{p},n}]Q - Q \end{aligned}$$

for some $Q \in E(\overline{K_\mathfrak{p}})$ such that $P = \pi^n Q$.

For the rest of this section, we fix the notation in use in the above definition.

**Proposition 2.3.3.** *The Kummer pairing $\langle \cdot, \cdot \rangle_{\pi^n}$ is bilinear and well-defined in the following sense:*

1. *$[x, K_{\mathfrak{p},n}^{\text{ab}}/K_{\mathfrak{p},n}]$ acts on $Q$.*

2. *The definition of the pairing is independent of the choice of $Q$.*

3. *$[x, K_{\mathfrak{p},n}^{\text{ab}}/K_{\mathfrak{p},n}]Q - Q \in E[\mathfrak{p}^n]$.*

*Proof.* We first show that the Kummer pairing is bilinear. Observe that linearity in the first argument is immediate so it suffices to show that for $x, y \in K_{\mathfrak{p},n}^\times$ and $P \in E(K_\mathfrak{p})$ we have $\langle P, xy \rangle_{\pi^n} = \langle P, x \rangle_{\pi^n} + \langle P, y \rangle_{\pi^n}$. Then

$$\langle P, xy \rangle_{\pi^n} = Q^{\sigma_x \sigma_y} - Q = (Q^{\sigma_x} - Q)^{\sigma_y} - (Q^{\sigma_y} - Q) = \langle P, x \rangle_{\pi^n}^{\sigma_y} + \langle P, y \rangle_{\pi^n}$$

Now, $\langle P, x\rangle_{\pi^n} \in E[\mathfrak{p}^n]$ and so, in particular, it is fixed by $\sigma_y$ whence the linearity claim follows.

To see the first part of the well-definedness claim, it suffices to realise that the extension of $K_{\mathfrak{p},n}$ defined by adjoining a pre-image of $P$ under the multiplication-by-$\pi^n$ map is abelian. For the second part of the claim, we observe that any other choice of pre-image of $P$ is of the form $Q + R$ for some $R \in E[\mathfrak{p}^n]$. We then have

$$(Q+R)^{\sigma_x} - (Q+R) = Q^{\sigma_x} - R^{\sigma_x} - Q - R = Q^{\sigma_x} - Q$$

where we have used the fact that $R$ is fixed by $\sigma_x$. Finally, we have

$$\pi^n \langle P, x\rangle_{\pi^n} = \pi^n Q^{\sigma_x} - \pi^n Q = P^{\sigma_x} - P$$

Now, $P$ is fixed by $\sigma_x$ so we see that $\langle P, x\rangle_{\pi^n}$ is a $\mathfrak{p}^n$-torsion point which establishes the third part of the claim. □

**Proposition 2.3.4.** *Given $n \in \mathbb{N}_{\geq 1}$, define the* ***$\pi^n$-reciprocity*** *map*

$$\begin{aligned} \delta_n : K_{\mathfrak{p},n} &\to E[\mathfrak{p}^n] \\ x &\mapsto \langle R, x\rangle_{\pi^n} \end{aligned}$$

*where $R \in E(K_{\mathfrak{p}})$ satisfies $\lambda_E(R) = \pi$. Then $\delta_n$ is a surjective $\mathrm{Gal}(K_{\mathfrak{p},n}/K_{\mathfrak{p}})$-equivariant homomorphism and is the unique such map satisfying*

$$\langle P, x\rangle_{\pi^n} = (\pi^{-1}\lambda_E(P))\delta_n(x) \tag{2.1}$$

*for all $(P, x) \in E(K_{\mathfrak{p}}) \times K_{\mathfrak{p},n}^{\times}$. Moreover, $\delta_n$ also maps $\mathcal{O}_{\mathfrak{p},n}^{\times} = \mathcal{O}_{\mathfrak{p},K_{\mathfrak{p},n}}^{\times}$ onto $E[\mathfrak{p}^n]$.*

*Proof.* The fact that $\delta_n$ is a homomorphism follows immediately from the linearity of the Kummer pairing in the second argument. Fix $(P, x) \in E(K_{\mathfrak{p}}) \times K_{\mathfrak{p},n}^{\times}$. By definition we have

$$\langle P, x\rangle_{\pi^n} = [x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q - Q$$

for some $Q \in E(\bar{K})$ satisfying $\pi^n Q = P$. We have that $\lambda_E(\pi^n Q) = \lambda_E(P) = \pi^m$ for some $m \geq 1$. Then $\lambda_E(\pi\lambda_E(P)^{-1}\pi^n Q) = \pi$. Define $Q' = \pi\lambda_E(P)^{-1}Q$ so that $\lambda_E(\pi^n Q') = \pi$. Then

$$\begin{aligned} \langle P, x\rangle_{\pi^n} &= (\pi^{-1}\lambda_E(P)Q')^{\sigma_x} - \pi^{-1}\lambda_E(P)Q' \\ &= \pi^{-1}\lambda_E(P)(Q'^{\sigma_x} - Q') \\ &= \pi^{-1}\lambda_E(P)\delta_n(x) \end{aligned}$$

thereby proving Equation 2.1. The uniqueness of $\delta_n$ then follows immediately from this formula. We next prove the Galois-equivarience of the reciprocity map. To this end, fix $\sigma \in \mathrm{Gal}(K_{\mathfrak{p},n}/K_{\mathfrak{p}})$. Then

$$\begin{aligned} \delta_n(x^\sigma) &= [x^\sigma, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q - Q \\ &= \sigma[x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]\sigma^{-1}Q - Q^{\sigma^{-1}\sigma} \\ &= ([x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q^{\sigma^{-1}} - Q^{\sigma^{-1}}) \\ &= \delta_n(x)^\sigma \end{aligned}$$

where we have used the fact that $\pi^n Q^{\sigma^{-1}} = (\pi^n Q)^{\sigma^{-1}} = R^{\sigma^{-1}} = R$ together with the conjugation property of Frobenius elements.

It remains to prove the surjection assertions. Since the local Artin maps glue together to give the global Artin map, Theorem A.7.5 implies that if $x \in \mathcal{O}_{\mathfrak{p}}^{\times}$ then $[x^{\sigma}, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]$ acts on $E[\mathfrak{p}^n]$ via multiplication by $x^{-1}$. Indeed, $\mathfrak{p}$ is prime to $\mathfrak{f}$ and so $E$ has good reduction at $\mathfrak{p}$ whence $\psi_E(x) = 1$. It then follows that $E(K_{\mathfrak{p}})$ admits no $\mathfrak{p}$-torsion and $E[\mathfrak{p}^n]$ has no proper $G_{K_{\mathfrak{p}}}$-stable subgroups.

Now note that the Kummer pairing induces a map

$$\begin{aligned} \varphi_n : E(K_{\mathfrak{p}}) &\to \mathrm{Hom}(K_{\mathfrak{p},n}^{\times}, E[\mathfrak{p}^n]) \\ P &\mapsto \langle P, \cdot \rangle_{\pi^n} \end{aligned}$$

It is easy to see that $\ker \varphi_n = \pi^n E(K_{\mathfrak{p}})$. Indeed,

$$\begin{aligned} \varphi_n(P) = 0 &\iff \langle P, x \rangle_{\pi^n} = 0 \text{ for all } x \in K_{\mathfrak{p},n}^{\times} \\ &\iff [x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q = Q \text{ for some } Q \in E(\bar{K_{\mathfrak{p}}}) \text{ with } \pi^n Q = P \text{ and for all } x \in K_{\mathfrak{p},n}^{\times} \\ &\iff Q \in E(K_{\mathfrak{p},n}) \text{ for some } Q \in E(\bar{K_{\mathfrak{p}}}) \text{ with } \pi^n Q = P \\ &\iff P = 0 \text{ with } Q \in E[\mathfrak{p}^n] \text{ or } P \neq 0 \text{ with } Q \in E(K_{\mathfrak{p}}) \\ &\iff P \in \pi^n E(K_{\mathfrak{p}}) \end{aligned}$$

and so we get an injection $E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \hookrightarrow \mathrm{Hom}(K_{\mathfrak{p},n}^{\times}, E[\mathfrak{p}^n])$. By Lemma 2.3.1, $E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \cong \mathcal{O}_K/\mathfrak{p}^n$ and we may thus conclude that $\mathrm{im}\, \delta_n \not\subseteq E[\mathfrak{p}^{n-1}]$. Since the image of $\delta_n$ is $G_{K_{\mathfrak{p}}}$-invariant, we must therefore have that $\mathrm{im}\, \delta_n = E[\mathfrak{p}^n]$.

Moreover, $\delta_n(K_{\mathfrak{p},n})/\delta_n(\mathcal{O}_{\mathfrak{p},n}^{\times})$ is a quotient of $E[\mathfrak{p}^n]$ admitting a trivial $G_{K_{\mathfrak{p}}}$-action. Since there are no proper subgroups of $E[\mathfrak{p}^n]$ which are $G_{K_{\mathfrak{p}}}$-stable, we must have that this quotient group is trivial whence $\delta_n(\mathcal{O}_{\mathfrak{p},n}^{\times}) = E[\mathfrak{p}^n]$ as asserted. □

## 2.4 Establishing $\mathfrak{p}$-adic control

In this section we will use the Kummer pairing to establish $\mathfrak{p}$-adic control over the $\alpha$-Selmer group for the remaining finite prime $\mathfrak{p}$ dividing $\alpha$. We will then combine this with the results for the relaxed $\alpha$-Selmer group to fully determine the classical $\alpha$-Selmer group under our working conditions.

*Assumptions.* Throughout this section, we shall assume that $E$ is an elliptic curve defined over a quadratic imaginary number field $K$ with complex multiplication by $\mathcal{O}_K$ so that $K$ has class number one. $\mathfrak{p} = \pi\mathcal{O}_K$ shall continue to be a finite prime of $K$, prime to $\mathfrak{f}$, for some generator $\pi$. We shall write $K_n = K(E[\mathfrak{p}^n])$ with ring of integers $\mathcal{O}_n$ and $K_{\mathfrak{p},n}$ and $\mathcal{O}_{\mathfrak{p},n}$ for the corresponding structures completed at $\mathfrak{p}$. Finally, $[\cdot, F^{\mathrm{ab}}/F]$ shall still refer to the local Artin map.

**Theorem 2.4.1.** *Let $C_{K_n}$ be the idèle class group of $K_n$ and consider the subgroup of $\mathbb{I}_{K_n}$ given by*

$$U_n = \ker(\delta_n) \prod_{\mathfrak{q}|\infty} K_{\mathfrak{p},n}^{\times} \prod_{\mathfrak{q}\nmid\mathfrak{p},\infty} \mathcal{O}_{\mathfrak{p},n}^{\times}$$

*Then*

$$\mathrm{S}^{(\pi^n)}(E/K) = \mathrm{Hom}\left( {}^{C_{K_n}}\!/_{U_n}, E[\mathfrak{p}^n] \right)^{\mathrm{Gal}(K_n/K)}$$

*Proof.* As in the proof of 2.3.4, we have an injection

$$\begin{aligned} \varphi_n : E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) &\to \mathrm{Hom}(K_{\mathfrak{p},n}^\times, E[\mathfrak{p}^n]) \\ [P] &\mapsto \langle P, \cdot \rangle_{\pi^n} \end{aligned}$$

Note that by Equation 2.1, it follows that every element of $\mathrm{im}(\varphi_n)$ descends to a homomorphism on $K_{\mathfrak{p},n}^\times/\ker(\delta_n)$ so in fact we have an injection

$$E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \hookrightarrow \mathrm{Hom}(K_{\mathfrak{p},n}^\times/\ker(\delta_n), E[\mathfrak{p}^n])$$

Since $\mathfrak{p}$ is prime to $\mathfrak{f}$, $E$ has good reduction at $\mathfrak{p}$ and so Proposition A.5.8 implies that $K_{\mathfrak{p},n}/K_\mathfrak{p}$ is unramified whence $\mathrm{Gal}(K_{\mathfrak{p},n}/K_\mathfrak{p})$ is abelian. Fix $\sigma \in \mathrm{Gal}(K_{\mathfrak{p},n}/K_\mathfrak{p})$. Then

$$\begin{aligned} \langle P, x \rangle_{\pi^n}^\sigma &= \sigma[x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q - Q^\sigma \\ &= [x, K_{\mathfrak{p},n}^{\mathrm{ab}}/K_{\mathfrak{p},n}]Q^\sigma - Q^\sigma \\ &= \langle P, x \rangle_{\pi^n} \end{aligned}$$

and so we get an injection

$$E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \hookrightarrow \mathrm{Hom}\left(K_{\mathfrak{p},n}^\times/\ker(\delta_n), E[\mathfrak{p}^n]\right)^{\mathrm{Gal}(K_{\mathfrak{p},n}/K_\mathfrak{p})}$$

Conversely, appealing to Lemma 2.3.1 and Proposition 2.3.4 yields $E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \cong \mathcal{O}_K/\mathfrak{p}^n \cong E[\mathfrak{p}^n]$ and $K_{\mathfrak{p},n}^\times/\ker(\delta_n) \cong E[\mathfrak{p}^n]$. By Part 2 of A.7.5, $\mathrm{Hom}(E[\mathfrak{p}^n], E[\mathfrak{p}^n])^{\mathrm{Gal}(K_{\mathfrak{p},n}/K_\mathfrak{p})}$ are exactly the $\mathcal{O}_K$-module homomorphisms $\mathrm{Hom}_{\mathcal{O}_K}(E[\mathfrak{p}^n], E[\mathfrak{p}^n]) \cong E[\mathfrak{p}^n]$. Hence this injection is in fact an isomorphism.

Now let $\mathcal{M}_n$ be the maximal $p$-extension of $K_n$ unramified outside of $p$. Proposition 2.2.3 now tells us that $\mathrm{S}^{(\pi^n)}(E/K)$ consists exactly of the elements of $H^1(F, E[\mathfrak{p}^n])$ that are in

$$\mathrm{Hom}(\mathrm{Gal}(\mathcal{M}_n/K_n), E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

under $\mathrm{res}_\mathfrak{q}$ for $(\mathfrak{q}, \mathfrak{p}) = 1$ and in $\mathrm{Hom}(K_{\mathfrak{p},n}^\times/\ker(\delta_n), E[\mathfrak{p}^n])^{\mathrm{Gal}(K_{\mathfrak{p},n}/K_n)}$ under $\mathrm{res}_\mathfrak{p}$. By class field theory, this is exactly $\mathrm{Hom}(C_{K_n}/U_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$ as desired. □

**Corollary 2.4.2.** *Let $\mathcal{C}_{K_1}$ be the ideal class group of $K_1 = K(E[\mathfrak{p}])$ and $\mathcal{O}_1^\times$ its group of units. Then $\mathrm{S}^{(\pi)}(E/K)$ is trivial if and only if $\mathrm{Hom}(\mathcal{C}_{K_1}, E[\mathfrak{p}])^{\mathrm{Gal}(K(E[\mathfrak{p}]/K)}$ is trivial and $\delta_1(\mathcal{O}_1^\times) \neq 0$.*

*Proof.* Theorem A.7.9 implies that $K_1/K$ is a degree $N\mathfrak{p} - 1$ degree extension which is totally ramified above $\mathfrak{p}$; suppose $\mathfrak{P}$ is the unique prime of $K(E[\mathfrak{p}])$ lying above $\mathfrak{p}$. Let $V = \ker(\delta_1) \cap \mathcal{O}_{\mathfrak{p},1}^\times$, $\overline{\mathcal{O}_1}$ the closure of $\mathcal{O}_1$ in $\mathcal{O}_{\mathfrak{p},1}$ and $G = \mathrm{Gal}(K_1/K)$.

Recall the idealifier $\mathfrak{I} : \mathbb{I}_{K_1} \to I_{K_1}$ which sends an idèle to its associated fractional ideal and let $\pi : I_{K_1} \to \mathcal{C}_{K_1}$ be the canonical map sending an ideal to its class in $\mathcal{C}_{K_1}$. Write $U = (\pi \circ \mathfrak{I})(K_1^\times U_1)$ and consider the diagram with exact rows

$$\begin{tikzcd}
 & \overline{\overline{\mathcal{O}_1}}V \arrow[r] \arrow[d, hook] & K_1^\times U_1 \arrow[r, two heads, "\pi\circ\mathfrak{I}"] \arrow[d, hook] & U \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & \mathcal{O}_{\mathfrak{p},1}^\times \arrow[r, hook] & \mathbb{I}_{K_1} \arrow[r, two heads, "\pi\circ\mathfrak{I}"] & \mathcal{C}_{K_1} &
\end{tikzcd}$$

Applying the Snake Lemma to this diagram yields a short exact sequence

$$1 \longrightarrow \mathcal{O}_{\mathfrak{p},1}^{\times}/_{\overline{\mathcal{O}_1}V} \longrightarrow C_{K_1}/_{U_1} \longrightarrow \mathcal{C}_{\mathfrak{p}}/_{U} \longrightarrow 1$$

where $C_{K_1}$ is the idèle class group of $K_1$. Expicitly, $U$ is a subgroup of $\mathcal{C}_{K_1}$ generated by some power of the class of $\mathfrak{P}$. Now, $\mathfrak{P}^{\mathbf{N}\mathfrak{p}-1} = \mathfrak{p}$ is principal and so

$$\operatorname{Hom}\left(\mathcal{C}_{K_1}/_{U}, E[\mathfrak{p}]\right) = \operatorname{Hom}(\mathcal{C}_{K_1}, E[\mathfrak{p}])$$

Combining this with Theorem 2.4.1 and the fact that the functor $\operatorname{Hom}(\cdot, E[\mathfrak{p}])$ is left-exact, we see that

$$\begin{aligned} \mathrm{S}^{(\pi)}(E/K) = 0 &\iff \operatorname{Hom}\left(C_{K_1}/_{U_1}, E[\mathfrak{p}]\right)^G = 0 \\ &\iff \operatorname{Hom}(\mathcal{C}_{K_1}, E[\mathfrak{p}])^G = 0 \text{ and } \operatorname{Hom}\left(\mathcal{O}_{\mathfrak{p},1}^{\times}/_{\overline{\mathcal{O}_1}V}, E[\mathfrak{p}]\right)^G = 0 \end{aligned}$$

Now, Proposition 2.3.4 implies that $\delta_1 : \mathcal{O}_{\mathfrak{p},1}^{\times}/V \to E[\mathfrak{p}]$ is an isomorphism. Recall that $E[\mathfrak{p}]$ has no proper Galois-stable submodules and so

$$\begin{aligned} \operatorname{Hom}\left(\mathcal{O}_{\mathfrak{p},1}^{\times}/_{\overline{\mathcal{O}_1}V}, E[\mathfrak{p}]\right)^G = 0 &\iff \operatorname{Hom}\left(E[\mathfrak{p}]/_{V}, E[\mathfrak{p}]\right)^G = 0 \\ &\iff \overline{\mathcal{O}_1} \not\subseteq V = \ker(\delta_1) \cap \mathcal{O}_{\mathfrak{p},1} \\ &\iff \delta_1(\mathcal{O}_1) \neq 0 \end{aligned}$$

Putting these two conditions together yields

$$\mathrm{S}^{(\pi)}(E/K) = 0 \iff \operatorname{Hom}(\mathcal{C}_{K_1}, E[\mathfrak{p}])^G = 0 \text{ and } \delta_1(\mathcal{O}_1) \neq 0$$

whence the Corollary follows. □

It is worth noting that this is indeed a very powerful result. In normal circumstances, the determination of the Selmer group can be quite difficult. In this case, however, we have a condition that the Selmer group is trivial in terms of two simpler objects $\operatorname{Hom}(\mathcal{C}_{K_1}, E[\mathfrak{p}])^G$ and $\mathcal{O}_1$. The former consists of three finite groups, namely an ideal class group, a quotient of $\mathcal{O}_K$ and the Galois group of a finite Galois extension of number fields. The first condition is thus effectively computable considering the existence of algorithms with well-determined complexity to calculate all of these groups involved. The structure of the global units of a number field $K$ is well-known by Dirichlet's unit theorem and a fundamental system of units for $K$ is also effectively computable given $\mathcal{O}_K$. We note that while $\mathcal{O}_K$ is effectively computable, it is not known if it is computable in polynomial-time. We refer the enthusiastic reader to [Len92] which gives an account of elementary Algorithmic Number Theory and provides details of the aforementioned algorithms.

In the sequel we shall make use of this Corollary as the final step in the proof of the Coates-Wiles Theorem. In particular, we shall use the Euler system of elliptic units to bound particular ideal class groups and show that the above hypothesis of the above Corollary is satisfied. We will then be able to conclude that $E(K)$ is finite by the exact sequence of Proposition A.6.2 and the Mordell-Weil Theorem.

# Chapter 3

# Elliptic Units

This chapter will be concerned with elliptic units which are particular global units in abelian extensions of an imaginary number field $K$. In some sense, these are a generalisation of cyclotomic units in abelian extensions of $\mathbb{Q}$. We shall construct them using particular rational functions of torsion points of elliptic curves with complex multiplication by $\mathcal{O}_K$. We shall moreover justify our claim that elliptic units are a generalisation of the cyclotomic units by showing that they satisfy analogues of well-known properties of the latter. The importance of these units will become evident when we go on to show their connection with the $L$-function attached to an elliptic curve.

In the first two sections, we shall study the algebraic theory of these units; in particular their construction and their properties. In the latter two sections we shall pass to the analytic theory and demonstrate, through the study of elliptic functions, that we can recover certain values of the $L$-function in terms of elliptic units.

## 3.1 The Θ-function

*Assumptions.* Throughout this section, we shall assume that $E$ is an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ for some imaginary quadratic number field $K$ of class number 1. We shall denote by $\mathfrak{a} \lhd \mathcal{O}_K$ a non-trivial ideal of $\mathcal{O}_K$ prime to 6; we shall sometimes refer to this ideal as the **auxillary ideal**. To ease notation, if $\mathfrak{b} \lhd \mathcal{O}_K$ is any ideal then we shall write $E[\mathfrak{b}]^* := E[\mathfrak{b}] \backslash \{ O_E \}$.

**Definition 3.1.1.** Let $x$ and $y$ be Weierstrass coordinate functions for a particular Weierstrass model of $E$. Suppose that $\alpha \in \mathcal{O}_K$ is a generator for $\mathfrak{a}$. We define the **Θ-function** of $E$ with respect to the auxillary ideal $\mathfrak{a}$ to be the rational function

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

**Proposition 3.1.2.** *The $\Theta$-function of $E$ is well-defined in the sense that it is independent of the choice of generator of $\mathfrak{a}$ and of the choice of Weierstrass model of $E$. Furthermore, if $L$ is a number field and $E$ is defined over $L$ then $\Theta_{E,\mathfrak{a}}$ is defined over $L$.*

*Proof.* First assume that $\alpha'$ is any other generator of $\mathfrak{a}$. Then $\alpha' = \mu\alpha$ for some $\mu \in \mathcal{O}_K^\times$. By Proposition A.1.7 we know that the exponent of $\mathcal{O}_K^\times$ is 12 and so $\alpha'^{-12} = \alpha^{-12}$.

To demonstrate the independence from the choice of Weierstrass model, we first suppose that $E$ has Weierstrass equation $y^2 = x^3 + ax + b$. We now fix another Weierstrass model $E'$ with coordinate functions $x'$ and $y'$ . Then

$x = u^2x'$ and $y = u^3y'$ for some $u \in \mathbb{C}^\times$. Furthermore, we have $\Delta(E) = u^{12}\Delta(E')$ and $|E[\mathfrak{a}]^*| = \mathbf{N}\mathfrak{a} - 1$. Therefore

$$\begin{aligned}\Theta_{E',\mathfrak{a}}(Q) &= \alpha^{-12}\Delta(E')^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(x'(Q)-x'(P))^{-6}\\ &= \alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}u^{12(\mathbf{N}\mathfrak{a}-1)}\prod_{P\in E[\mathfrak{a}]^*}(x'(Q)-x'(P))^{-6}\\ &= \alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(u^2x'(Q)-u^2x'(P))^{-6}\\ &= \alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(x(Q)-x(P))^{-6}\\ &= \Theta_{E,\alpha}(Q)\end{aligned}$$

Finally, suppose that $E$ is defined over $L$. To show that $\Theta_{E,\mathfrak{a}}$ is also defined over $L$, we need to show that it is fixed by $G_L$. But $\alpha$ and $\Delta(E)$ are both elements of $L$ so they are fixed by $G_L$. Furthermore, $E[\mathfrak{a}]^*$ is stable under the action of $G_L$ and so the product is also fixed whence $\Theta_{E,\mathfrak{a}}$ is defined over $L$. □

*Remark.* We note that the independence of $\Theta_{E,\mathfrak{a}}$ of the choice of Weierstrass model for $E$ is equivalent to $\Theta_{E,\mathfrak{a}}$ commuting with isomorphisms of elliptic curves.

The following Theorem will be the first key ingredient in the construction of elliptic units. In particular, it demonstrates that the Θ-function of $E$ can be used to generate points in abelian extensions of $K$. Furthermore, it will show that the action of the Galois group of such an extension on these points is again given by the Θ-function.

**Theorem 3.1.3.** *Let $\mathfrak{b} \lhd \mathcal{O}_K$ be a non-trivial ideal prime to $\mathfrak{a}$ and $Q \in E[\mathfrak{b}]$ an $\mathcal{O}_K$-gnerator of $E[\mathfrak{b}]$. Then*

1. *$\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.*
2. *Given an ideal $\mathfrak{c} \lhd \mathcal{O}_K$ prime to $\mathfrak{b}$ and $c$ a generator of $\mathfrak{c}$ we have*

$$[\mathfrak{c}, K(\mathfrak{b})/K]\Theta_{E,\mathfrak{a}}(Q) = \Theta_{E,\mathfrak{a}}(cQ)$$

*Proof.* Without loss of generality, we may assume that $E$ is defined over $K$. Indeed, by the hypotheses of this section, $K$ has class number 1 and so, in particular, it is its own Hilbert class field. Hence $E$ is isomorphic to an elliptic curve with Weierstrass model defined over $K$ by Proposition A.7.4; Proposition 3.1.2 further shows us that it suffices to consider the Θ-function of this curve which is defined over $K$.

Part 1: Now consider $\mathfrak{b}$ as a modulus and given a finite prime $\mathfrak{p} \in M_K$, define the set

$$U^{\mathfrak{b}(\mathfrak{p})} = \begin{cases} 1 + \mathfrak{p}^{\mathfrak{b}(\mathfrak{p})} & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{b}(\mathfrak{p}) > 0 \\ \mathcal{O}_{\mathfrak{p},K^\times} & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{b}(\mathfrak{p}) = 0 \\ \mathbb{C}^\times & \text{if } \mathfrak{p} \mid \infty \end{cases}$$

Let $U^{\mathfrak{b}} = \prod_{\mathfrak{p}\in M_K} U^{\mathfrak{b}(\mathfrak{p})}$ which is a subgroup of $\mathbb{I}_K$. Fix an idèle $x \in U^{\mathfrak{b}}$ and, to simplify notation, write $\sigma_x = [x, K^{\mathfrak{ab}}/K]$. By Theorem 5.15, we have that $\psi_E(x)$ is an automorphism of $E$ and $Q^{\sigma_x} = \psi_E(Q)$. By Part 1 of Theorem 3.1.2, we thus have

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_x} = \Theta_{E,\mathfrak{a}}(Q^{\sigma_x}) = \Theta_{E,\mathfrak{a}}(\psi(x)Q) = \Theta_{E,\mathfrak{a}}(Q)$$

But by class field theory, $[U^{\mathfrak{b}}, K^{\mathrm{ab}}/K] = \mathrm{Gal}(\overline{K}/K(\mathfrak{b}))$ and so $\Theta_{E,\mathfrak{a}}(Q)$ is fixed by every $K(\mathfrak{b})$-automorphism of

$\overline{K}$ whence $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.

Part 2: Fix an idèle $x \in \mathbb{I}_K$ such that $\mathfrak{I}(x) = \mathfrak{c}$. Since $(\mathfrak{b}, \mathfrak{c}) = 1$, we have $x_\mathfrak{p} = 1$ for all finite primes $\mathfrak{p} \mid \mathfrak{b}$. By Theorem A.7.5 we have that $\psi_E(x) \in c\mathcal{O}_K^\times$ and that $Q^{\sigma_\mathfrak{c}} = \psi_E(x)Q$. Now, recall that the ray class field $K(\mathfrak{b})$ is the maximal abelian extension of $K$ unramified outside of primes dividing $\mathfrak{b}$. In particular, the Artin map $[\mathfrak{c}, K(\mathfrak{b})/K]$ makes sense and so, by the compatibility of the ideal and idèlic versions of the Artin map, we have that

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}(Q)^{\sigma_x} = \Theta_{E,\mathfrak{a}}(Q^{\sigma_x}) = \Theta_{E,\mathfrak{a}}(\psi_E(x)Q) = \Theta_{E,\mathfrak{a}}(cQ) \qquad \square$$

As in the proof of the Theorem 3.1.3 we may assume, without loss of generality, for the rest of this section that $E$ is defined over $K$.

**Lemma 3.1.4.** *Let $\mathfrak{p}$ be a finite prime of $K$ prime to $\mathfrak{f}$ and let $E$ be endowed with a Weierstrass model that is minimal at $\mathfrak{p}$. Suppose that $\mathfrak{b}$ and $\mathfrak{c}$ are non-trivial ideals of $\mathcal{O}_K$ such that $(\mathfrak{b}, \mathfrak{c}) = 1$. Let $B \in E[\mathfrak{b}]$ have exact order $\mathfrak{b}$ and $C \in E[\mathfrak{c}]$ with exact order $\mathfrak{c}$. Then*

1. *If $\mathfrak{b} = \mathfrak{p}^n$ for some $n \in \mathbb{N}_{\geq 1}$ then*

$$v_\mathfrak{p}(x(B)) = \frac{-2}{\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1)}$$

2. *If $\mathfrak{b}$ is not a power of $\mathfrak{p}$ then $v_\mathfrak{p}(x(B)) \geq 0$.*

3. *$\mathfrak{b}\mathfrak{c}$ is not a power of $\mathfrak{p}$ then $v_\mathfrak{p}(x(B) - x(C)) = 0$.*

*Proof.*

Part 1: Let $\hat{E}$ be the formal group associated to $E$ over $\mathcal{O}_{\mathfrak{p},K}$. Let $\pi$ be the endomorphism of $E$ given by $\psi_E(\mathfrak{p})$ and $[\pi]$ be the corresponding endomorphism of $\hat{E}$. Consider the power series

$$f(X) = \frac{[\pi^n](X)}{[\pi^{n-1}](X)}$$

in $\mathcal{O}_{\mathfrak{p},K}[[X]]$. Now, Theorem A.7.6 implies that $\pi$ acts as Frobenius on $\overline{E}$. Since $\mathfrak{p}$ is prime to $\mathfrak{f}$, $E$ has good reduction at $\mathfrak{p}$ so appealing to Proposition A.5.6 shows that $f(X) \equiv X^{\mathbf{N}\mathfrak{p}^n - \mathbf{N}\mathfrak{p}^{n-1}} \pmod{\mathfrak{p}}$. Moreover, Proposition 3.14 implies that $f(X) \equiv \pi \pmod{X}$. Hence by the Weierstrass Preparation Theorem (see [Ger83]), there exists a distinguished polynomial $e(X) \in \mathcal{O}_{\mathfrak{p},K}[X]$ of degree $\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1)$ and a unit $u(X) \in \mathcal{O}_{\mathfrak{p},K}[X]$ such that $f(X) = e(X)u(X)$. The two previous conditions imply that $e(X)$ is in fact an Eisenstein polynomial at $\mathfrak{p}$.

Now, the reduction of $\pi$ is the Frobenius endomorphism which is a purely inseparable endomorphism of $\overline{E}$. Hence, Proposition A.5.4 implies that $E[\mathfrak{p}^n] \subseteq E_1(\overline{K_\mathfrak{p}}) \cong \hat{E}(\mathfrak{p})$ via the logarithm map $\lambda_{\hat{E}}$. It then follows that $-x(B)/y(B)$ is a zero of $f(X)$ and, in particular, it is a root of $e(X)$. By the fact that $e(X)$ is an Eisenstein polynomial and Proposition A.5.2 we then have that

$$\frac{1}{\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1)} = v_\mathfrak{p}\left(\frac{x(B)}{y(B)}\right) = v_\mathfrak{p}(x(B)) - v_\mathfrak{p}(y(B)) = v_\mathfrak{p}(x(B)) - \frac{3}{2}v_\mathfrak{p}(x(B)) = -\frac{1}{2}v_\mathfrak{p}(x(B))$$

and so

$$v_\mathfrak{p}(x(B)) = \frac{-2}{\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1)}$$

as desired.

Part 2: Now suppose that $\mathfrak{b}$ is not a power of $\mathfrak{p}^n$. Appealing to Proposition A.5.7, we see that $B \notin E_1(\overline{K_\mathfrak{p}})$ and so Proposition A.5.2 implies that $v_p(x(B)) \geq 0$.

Part 3: Let $\overline{B}, \overline{C} \in \overline{E}(\overline{\mathbb{F}_\mathfrak{p}})$ be the reductions of $B$ and $C$. Suppose, for a contradiction, that $v_\mathfrak{p}(x(B)-x(C)) > 0$. Then

$$\begin{aligned} v_\mathfrak{p}(x(B)-x(C)) > 0 &\iff x(B) \equiv x(Q) \pmod{\mathfrak{p}} \\ &\iff x(\overline{B}) = x(\overline{C}) \\ &\iff \overline{B} = \pm\overline{C} \\ &\iff \overline{B \mp C} = O_{\overline{E}} \\ &\iff B \mp C \in E_1(\overline{K_\mathfrak{p}}) \end{aligned}$$

On the other hand, $\mathfrak{b}$ is prime to $\mathfrak{c}$ and so the order of $B \mp C$ is not a power of $\mathfrak{p}$. Applying Proposition A.5.7 then yields $B \mp C \notin E_1(\overline{K_\mathfrak{p}})$ which is clearly a contradiction. We must therefore have that $v_\mathfrak{p}(x(B)-x(C)) = 0$. □

The next theorem is the second key part of the recipe in the construction of the elliptic units. In particular, it provides a way to generate global units of abelian extensions of $K$, namely those that coincide with certain ray class fields of $K$.

**Theorem 3.1.5.** *Let $\mathfrak{b} \lhd \mathcal{O}_K$ be a non-trivial ideal prime to $\mathfrak{a}$ and $B \in E[\mathfrak{b}]$ an $\mathcal{O}_K$-generator of $E[\mathfrak{b}]$. If $\mathfrak{b}$ is a power of some finite prime $\mathfrak{p}$ of $K$ then $\Theta_{E,\mathfrak{a}}(B) \in K(\mathfrak{b})$ is a $\mathfrak{P}$-unit for all finite primes $\mathfrak{P}$ of $K(\mathfrak{b})$ not lying over $\mathfrak{p}$. Moreover, if $\mathfrak{b}$ is not a prime power then $\Theta_{E,\mathfrak{a}}(B)$ is a global unit of $K(\mathfrak{b})$.*

*Proof.* Fix a finite prime $\mathfrak{q}$ of $K$ such that $\mathfrak{b}$ is not a power of $\mathfrak{q}$. Let $\mathfrak{P}$ be any finite prime of $K(\mathfrak{b})$ lying over $\mathfrak{q}$. By Proposition A.7.7, $E$ isomorphic over $\overline{K}$ to an elliptic curve with good reduction at $\mathfrak{q}$. We may thus, in light of Proposition 3.1.2, assume that $E$ has good reduction at $\mathfrak{q}$. In this case, $\mathfrak{q} \nmid \Delta(E)$ and so $v_\mathfrak{P}(\Delta(E)) = 0$. Let $n = v_\mathfrak{P}(\alpha)$ for some generator $\alpha$ of $\mathfrak{a}$. Then

$$\begin{aligned} v_\mathfrak{P}(\Theta_{E,\mathfrak{a}}(B)) &= -12n - 6 \sum_{P \in E[\mathfrak{a}]^*} v_\mathfrak{P}(x(B)-x(P)) \\ &= -12n - 6 \sum_{P \in E[\mathfrak{p}^n]^*} v_\mathfrak{P}(x(B)-x(P)) - 6 \sum_{P \in E[\mathfrak{a}] \backslash E[\mathfrak{p}^n]} v_\mathfrak{P}(x(B)-x(P)) \end{aligned} \tag{3.1}$$

First consider the third term of the above expansion. By hypothesis, $B$ does not have order a prime power. Moreover, neither can $P$ since $n$ is the greatest power of $\mathfrak{p}$ dividing $\mathfrak{a}$. Part 3 of Lemma 3.1.4 then implies that this term vanishes.

Now consider the second term of the expansion. We observe that we can write it in the form

$$\sum_{P \in E[\mathfrak{p}^n]^*} v_\mathfrak{P}(x(B)-x(P)) = \sum_{i=1}^{n} \sum_{P \in E[\mathfrak{p}^i] \backslash E[\mathfrak{p}^{i-1}]} v_\mathfrak{P}(x(B)-x(P))$$

where we understand $E[\mathfrak{p}^0] = \{ O_E \}$. Now, $B$ does not have order exactly a power of $\mathfrak{p}$ and so $v_\mathfrak{P}(x(Q)) \geq 0$ by Lemma 3.1.4. Furthermore, each $P \in E[\mathfrak{p}^i] \backslash E[\mathfrak{p}^{i-1}]$ has order exactly $\mathfrak{p}^i$. Appealing once more to Lemma 3.1.4

and using the valuation axioms, we then have that

$$\begin{aligned}\sum_{P\in E[\mathfrak{p}^n]^*} v_{\mathfrak{P}}(x(B)-x(P)) &= \sum_{i=1}^{n} \sum_{E[\mathfrak{p}^i]\backslash E[\mathfrak{p}^{i-1}]} \frac{-2}{\mathbf{N}\mathfrak{p}^{i-1}(\mathbf{N}\mathfrak{p}-1)} \\ &= \sum_{i=1}^{n}(\mathbf{N}\mathfrak{p}^{i-1}(\mathbf{N}\mathfrak{p}-1))\frac{-2}{\mathbf{N}\mathfrak{p}^{i-1}(\mathbf{N}\mathfrak{p}-1)} \\ &= -2n\end{aligned}$$

where we have used Proposition A.7.2 to calculate the cardinality of $E[\mathfrak{p}^i]\backslash E[\mathfrak{p}^{i-1}]$. Inserting this back into Equation 3.1 yields $v_{\mathfrak{P}}(\Theta_{E,\mathfrak{a}}(B)) = 0$ and so $\Theta_{E,\mathfrak{a}}(B)$ is a $\mathfrak{P}$-unit. In the case that $\mathfrak{b}$ is a power of a finite prime $\mathfrak{p}$ of $K$, we see that $\Theta_{E,\mathfrak{a}}(B)$ is a $\mathfrak{P}$-unit for all finite primes $\mathfrak{P}$ of $K(\mathfrak{b})$ not lying over $\mathfrak{p}$. In the case that $\mathfrak{b}$ is not a prime power then $\Theta_{E,\mathfrak{a}}(B)$ is a $\mathfrak{P}$-unit for all finite primes $\mathfrak{P}$ of $K(\mathfrak{b})$. But this is exactly what it means for $\Theta_{E,\mathfrak{a}}(B)$ to be a global unit and so the Theorem is proven. □

## 3.2 A Distribution Relation

We will now show that the Θ-function satisfies an analogue of the so-called distribution relation of cyclotomic units. We recall that a cyclotomic unit is a unit in a number field given by a product of terms $\zeta_n^a - 1$ where $\zeta_n$ is an $n^{th}$ root of unity and $0 < a < n$. In particular, the group of cyclotomic units forms a subgroup of finite index in the global units of a cyclotomic field. If we define $g_a = e^{2\pi i a} - 1$ where $a$ is a rational number prime to some rational prime $p$ then we have the distribution relation $\prod_{bp=a} g_b = g_a$. For more details on cyclotomic units, we encourage the reader to see [Lan90, §6.3].

*Assumptions.* Throughout this section, we shall assume that $K$ is an imaginary quadratic field and $E$ is an elliptic curve defined over $K$ with complex multiplication by $\mathcal{O}_K$. As before we may assume, without loss of generality, that $K$ has class number 1. We let $\mathfrak{a} \lhd \mathcal{O}_K$ be the auxilliary ideal prime to 6.

**Lemma 3.2.1.** $\Theta(E,\mathfrak{a})$ *admits the divisor*

$$\operatorname{div}(\Theta_{E,\mathfrak{a}}) = 12\mathbf{N}\mathfrak{a}[O_E] - 12\sum_{P\in E[\mathfrak{a}]}[P]$$

*Proof.* Fix a Weierstrass model of $E$ with coordinate functions $x$ and $y$. By the elementary theory of elliptic curves (see [Sil09, III.3.1]), the $x$-coordinate is an even rational function with exactly one pole at $O_E$ of order 2. We therefore see that the factor $x - x(P)$ in the Θ-function admits the divisor $[P] + [-P] + 2[O_E]$. It follows that

$$\begin{aligned}\operatorname{div}(\Theta_{E,\mathfrak{a}}) &= -6\sum_{P\in E[\mathfrak{a}]^*}[P]+[-P]-2[O_E] \\ &= 12\sum_{P\in E[\mathfrak{a}^*}[O_E] - 6\sum_{P\in E[\mathfrak{a}]^*}[P]+[-P] \\ &= 12(\mathbf{N}\mathfrak{a}-1)[O_E] - 12\sum_{P\in E[\mathfrak{a}]^*}[P] \\ &= 12\mathbf{N}\mathfrak{a}[O_E] - 12\sum_{P\in E[\mathfrak{a}]}[P]\end{aligned}$$

□

**Theorem 3.2.2** (Distribution Relation)**.** *Let* $(\beta) = \mathfrak{b} \lhd \mathcal{O}_K$ *be an ideal prime to* $\mathfrak{a}$*. Then for all* $Q \in E(\overline{K})$ *we* *have*

$$\prod_{B\in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(Q+B) = \Theta_{E,\mathfrak{a}}(\beta Q)$$

*Proof.* We first consult Proposition 3.1.2 to see that both sides of the above equation are rational functions of $E$ defined over $K$. We claim that they, in fact, have the same divisor. If this were the case, then their ratio would be a constant in $\mathbb{C}^\times$. It would then suffice to show that such a constant would be equal to 1 to establish the Theorem. Applying Lemma 3.2.1 to the left hand side yields

$$\begin{aligned}\operatorname{div}\left(\prod_{B\in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(Q+B)\right) &= \sum_{B\in E[\mathfrak{b}]} \operatorname{div}(\Theta_{E,\mathfrak{a}}(Q+B))) \\ &= \sum_{B\in E[\mathfrak{b}]} \left(12\mathbf{N}\mathfrak{a}[B] - 12\sum_{P\in E[\mathfrak{a}]}[P+B]\right) \\ &= 12\mathbf{N}\mathfrak{a}\sum_{B\in E[\mathfrak{b}]}[B] - 12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}[Q]\end{aligned}$$

On the other hand, we immediately have

$$\operatorname{div}(\Theta_{E,\mathfrak{a}}(\beta Q)) = 12\mathbf{N}\mathfrak{a}\sum_{B\in E[\mathfrak{b}]}[B] - 12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}[Q]$$

Hence, by the reasoning above, the quotient of the left hand side by the right hand side is some constant $\lambda \in \mathbb{C}^\times$. Now let $\alpha$ be a generator of $\mathfrak{a}$. We have that

$$\begin{aligned}\lambda &= \frac{\prod_{B\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(Q+B)}{\Theta_{E,\mathfrak{a}}(\beta Q)} \\ &= \frac{\prod_{B\in E[\mathfrak{b}]}\alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(x(Q+B)-x(P))^{-6}}{\alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(x(\beta Q)-x(P))^{-6}} \\ &= \frac{\alpha^{-12\mathbf{N}\mathfrak{b}}\Delta(E)^{\mathbf{N}\mathfrak{b}(\mathbf{N}\mathfrak{a}-1)}\prod_{B\in E[\mathfrak{b}]}\prod_{P\in E[\mathfrak{a}]^*}(x(Q+B)-x(P))^{-6}}{\alpha^{-12}\Delta(E)^{\mathbf{N}\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]^*}(x(\beta Q)-x(P))^{-6}} \\ &= \frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)}\prod_{B\in E[\mathfrak{b}]}\prod_{P\in E[\mathfrak{a}]^*}(x(Q+B)-x(P))^{-6}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)}\prod_{P\in E[\mathfrak{a}]^*}(x(\beta Q)-x(P))^{-6}}\end{aligned}$$

Evaluating this ratio at $Q = O_E$ shows that

$$\lambda = \frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)}\beta^{12(\mathbf{N}\mathfrak{a}-1)}}\prod_{B\in E[\mathfrak{b}]^*}\prod_{P\in E[\mathfrak{a}]^*}(x(B)-x(P))^{-6}$$

where we considered the Laurent expansion of the $x$-coordinate function to pull out the $\beta$ term. Now write $\lambda = \gamma^w$ where

$$\gamma = \frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)/w}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)/w}\beta^{12(\mathbf{N}\mathfrak{a}-1)/w}}\prod_{\substack{B\in E[\mathfrak{b}]^* \\ P\in E[\mathfrak{a}]^*/\pm 1}}(x(B)-x(P))^{-12/w}$$

where we have used the fact that $(\mathfrak{a}, 6) = 1$ to write the product in its compact form. Denote $w = |\mathcal{O}_K^\times|$. By Proposition A.1.7, we know that $w$ is either $2, 4$ or $6$ and that $\mathcal{O}_K^\times$ is annihilated by exponentiation by $w$. It therefore suffices to show that $\gamma \in \mathcal{O}_K^\times$.

To this end, fix any finite prime $\mathfrak{p}$ of $K$ along with an extension $v_\mathfrak{p}$ of the $\mathfrak{p}$-adic valuation to $\overline{K}$. By Proposition A.7.7 and Proposition 3.1.2, we may assume that $E$ has good reduction at $\mathfrak{p}$ so that $v_\mathfrak{p}(\Delta(E)) = 0$. Since $\mathfrak{a}$ and $\mathfrak{b}$

are coprime, we may assume, without loss of generality, that $\mathfrak{p} \nmid \mathfrak{a}$. Denote $m = v_{\mathfrak{p}}(\beta)$. Then

$$\frac{wv_{\mathfrak{p}}(\gamma)}{12} = -(\mathbf{N}\mathfrak{a} - 1)m - \sum_{\substack{B \in E[\mathfrak{b}]^* \\ P \in E[\mathfrak{a}]^*/\pm 1}} v_{\mathfrak{p}}(x(B) - x(P))$$

We observe that for $P \in E[\mathfrak{a}]^*/\pm 1$ we have

$$\sum_{B \in E[\mathfrak{b}]^*} v_{\mathfrak{p}}(x(B) - x(P)) = \sum_{B \in E[\mathfrak{p}^{\mathfrak{m}}]^*} v_{\mathfrak{p}}(x(B) - x(P)) + \sum_{B \in E[\mathfrak{b}] \setminus E[\mathfrak{p}^{\mathfrak{m}}]} v_{\mathfrak{p}}(x(B) - x(P))$$

Since $\mathfrak{a}$ is prime to $\mathfrak{p}$, Part 2 of Lemma 3.1.4 immediately implies that the term

$$\sum_{\substack{B \in E[\mathfrak{b}] \setminus E[\mathfrak{p}^{\mathfrak{m}}] \\ P \in E[\mathfrak{a}]^*/\pm 1}} v_{\mathfrak{p}}(x(B) - x(P))$$

vanishes. The Lemma furthermore gives us

$$\begin{aligned} \sum_{\substack{B \in E[\mathfrak{p}^m]^* \\ P \in E[\mathfrak{a}]^*/\pm 1}} v_{\mathfrak{p}}(x(B) - x(P)) &= \sum_{P \in E[\mathfrak{a}]^*/\pm 1} \left[ \sum_{i=1}^{m} \sum_{B \in E[\mathfrak{p}^i] \setminus E[\mathfrak{p}^{i-1}]} v_{\mathfrak{p}}(x(B) - x(P)) \right] \\ &= \sum_{\substack{1 \le i \le m \\ P \in E[\mathfrak{a}]^*/\pm 1}} \frac{-2(\mathbf{N}\mathfrak{p}^i - \mathbf{N}\mathfrak{p}^{i-1})}{(\mathbf{N}\mathfrak{p}^i - \mathbf{N}\mathfrak{p}^{i-1})} \\ &= -m(\mathbf{N}\mathfrak{a} - 1) \end{aligned}$$

Putting this together shows that $v_{\mathfrak{p}}(\gamma) = 0$. But $\mathfrak{p}$ was arbitrary and so $\gamma \in \mathcal{O}_K^\times$ whence $\lambda = 1$ as claimed. □

**Corollary 3.2.3.** *Let $\mathfrak{b} \lhd \mathcal{O}_K$ be an ideal prime to $\mathfrak{a}$ and $B \in E[\mathfrak{b}]$ of order exactly $\mathfrak{b}$. Given a finite prime $(\pi) = \mathfrak{p}$ of $K$ dividing $\mathfrak{b}$, define the ideal $\mathfrak{b}'$ to be the one given by dividing $\mathfrak{b}$ out by $\mathfrak{p}$. If the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{b}')^\times$ is injective then*

$$\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\, \Theta_{E,\mathfrak{a}}(B) = \begin{cases} \Theta_{E,\mathfrak{a}}(\pi B) & \text{if } \mathfrak{p} \mid b' \\ \Theta_{E,\mathfrak{a}}(\pi B)^{1-((K(\mathfrak{b}')/K),\mathfrak{p})^{-1}} & \text{if } \mathfrak{p} \nmid \mathfrak{b}' \end{cases}$$

*Proof.* To ease notation, denote $\mathfrak{B} = (\mathcal{O}_K/\mathfrak{b})^\times$ and $\mathfrak{B}' = (\mathcal{O}_K/\mathfrak{b}')^\times$. Consider the diagram with exact rows

$$\begin{tikzcd} & 1 \arrow[r] \arrow[d] & \mathcal{O}_K^\times \arrow[r] \arrow[d] & \mathcal{O}_K^\times \arrow[r] \arrow[d, hook] & 1 \\ 1 \arrow[r] & 1 + \mathfrak{b}'\mathfrak{B} \arrow[r] & \mathfrak{B} \arrow[r, two heads] & \mathfrak{B}' & \end{tikzcd}$$

By the Snake Lemma, we then have a short exact sequence

$$1 \longrightarrow 1 + \mathfrak{b}'\mathfrak{B} \longrightarrow {}^{\mathfrak{B}}\!/_{\mathcal{O}_K^\times} \longrightarrow {}^{\mathfrak{B}'}\!/_{\mathcal{O}_K^\times} \longrightarrow 1$$

On the other hand, $K$ has class number one and so by Theorem A.1.2 we have a short exact sequence[1]

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow \mathfrak{B} \longrightarrow C_K^{\mathfrak{b}} \longrightarrow 1$$

where we are viewing $\mathfrak{b}$ as a modulus of $K$. We also obtain a similar sequence for $\mathfrak{b}'$. We thus see that $\mathfrak{B}/(\mathcal{O}_K^\times)$ and $\mathfrak{B}'/(\mathcal{O}_K^\times)$ are the ray class groups modulo $\mathfrak{b}$ and $\mathfrak{b}'$ respectively. In light of this, we now have a short exact sequence

[1] Note that in both exact sequences, we are slightly abusing notation - we intend to quotient out by the image of $\mathcal{O}_K^\times$ in the corresponding quotient groups.

$$1 \longrightarrow 1+\mathfrak{b}'\mathfrak{B} \longrightarrow C_K^{\mathfrak{b}} \longrightarrow C_K^{\mathfrak{b}'} \longrightarrow 1$$

By Galois Theory, we thus see that $1+\mathfrak{b}'\mathfrak{B} \cong \mathrm{Gal}(K(\mathfrak{b})/K(\mathfrak{b}')) = G$. Given $g \in 1+\mathfrak{b}'\mathfrak{B}$, denote by $\sigma_g$ the element of $G$ under this correspondence. By Part 2 of Theorem 3.1.3 and the definition of the norm we have

$$\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\,\Theta_{E,\mathfrak{a}}(B) = \prod_{g\in G}\Theta_{E,\mathfrak{a}}(B)^{\sigma_g} = \prod_{g\in G}\Theta_{E,\mathfrak{a}}(gB)$$

We now observe that

$$\{\, gB \mid g \in G \,\} = \{\, Q \in E[\mathfrak{b}] \mid \pi Q = \pi B, Q \notin E[\mathfrak{b}'] \,\}$$

In the case that $\mathfrak{p} \mid \mathfrak{b}'$ then the above set equals $\{\, B+Q \mid Q \in E[\mathfrak{p}] \,\}$ and so the distribution relation implies that

$$\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\,\Theta_{E,\mathfrak{a}}(B) = \prod_{Q\in E[\mathfrak{p}]}\Theta_{E,\mathfrak{a}}(B+Q) = \Theta_{E,\mathfrak{a}}(\pi B)$$

Now in the case that $\mathfrak{p} \nmid \mathfrak{b}'$ then the above set equals $\{\, B+Q \mid Q \in E[\mathfrak{p}], Q \not\equiv -B \pmod{E[\mathfrak{b}']} \,\}$. Choosing $P \in E[\mathfrak{p}]$ such that $B+P \in E[\mathfrak{b}']$, we have

$$\Theta_{E,\mathfrak{a}}(B+P)\,\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\,\Theta_{E,\mathfrak{a}}(B) = \Theta_{E,\mathfrak{a}}(B+P)\prod_{\substack{Q\in E[\mathfrak{p}]\\ Q\not\equiv -B \pmod{E[\mathfrak{b}']}}}\Theta_{E,\mathfrak{a}}(B+Q) = \Theta_{E,\mathfrak{a}}(\pi B)$$

Appealing to Part 2 of Theorem 3.1.3, we have that

$$\Theta_{E,\mathfrak{a}}(B+P)^{((K(\mathfrak{b}')/K),\mathfrak{p})} = \Theta_{E,\mathfrak{a}}(\pi B+\pi P) = \Theta_{E,\mathfrak{a}}(\pi B)$$

whence

$$\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\,\Theta_{E,\mathfrak{a}}(B) = \Theta_{E,\mathfrak{a}}(\pi B)^{1-((K(\mathfrak{b}')/K),\mathfrak{p})^{-1}}$$

as required. □

We end this section by noting that the above Corollary is yet another generalisation of a particular property of cyclotomic units. Indeed, let $\zeta_n$ be a primtive $n^{th}$ root of unity for some $n \in \mathbb{N}_{>1}$. Then for any rational prime $p$ we have

$$\mathbf{N}_{\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)}\,\zeta_{mp}-1 = \begin{cases} \zeta_m - 1 & \text{if } p \mid m \\ (\zeta_m-1)^{1-((\mathbb{Q}(\zeta_m)/\mathbb{Q}),p)^{-1}} & \text{if } p \nmid m \end{cases}$$

This striking similarity between cyclotomic units and the units we have constructed in this chapter is exactly what will motivate our definition of Euler systems. The axomatisation of these phenomenae will allow us to study these objects in full generality.

That being said, we would like to further build upon this theory before we fully define elliptic units. Indeed, we would like for our units to be related, in some way, to certain values of the Hecke $L$-function attached to an elliptic curve with complex multiplication. This is exactly what we shall accomplish in the rest of this chapter.

## 3.3 The Eisenstein-Weierstrass Connection

In the spirit of Grothendieck's philosophy of *Géométrie Algébrique et Géométrie Analytique* we now shift perspective to the analytic theory. In this section, we will study the connection between the Weierstrass and Eisenstein theories of elliptic functions. In particular, we shall show that we can express the $\Theta$-function in terms of certain Eisenstein series.

*Assumptions.* Throughout this section, we shall assume that $K$ is an imaginary quadratic field and $E$ is an elliptic curve defined over $K$ with complex multiplication by $\mathcal{O}_K$ so that $K$ has class number 1. We continue to let $(\alpha) = \mathfrak{a} \triangleleft \mathcal{O}_K$ be the auxiliary ideal prime to 6. We let $\Lambda \subseteq \mathbb{C}$ be the lattice associated to $E$ under the correspondence of Theorem A.4.2.This correspondence also implies that $\mathcal{O}_K\Lambda = \Lambda$ so we can choose $\Omega \in \mathbb{C}^\times$ so that $\Lambda = \Omega\mathcal{O}_K$. Furthermore, by Proposition A.7.2, we have that $E[\mathfrak{a}]$ corresponds to $\mathfrak{a}^{-1}\Lambda/\Lambda$. To once again ease notation, we shall write $\mathfrak{a}^{-1}\Lambda/\Lambda^* = (\mathfrak{a}^{-1}\Lambda/\Lambda)\backslash\{\,0\,\}$. After choosing a Weierstrass model of $E$, we fix an an analytic isomorphism

$$\begin{aligned}\xi : {}^{\mathbb{C}}\!/_{\Lambda} &\to E(\mathbb{C})\\ z &\mapsto (\wp(z;\Lambda), \wp'(z;\Lambda)/2)\end{aligned}$$

and denote

$$\Theta_{\Lambda,\mathfrak{a}}(z) = (\Theta_{E,\mathfrak{a}} \circ \xi)(z) = \alpha^{-12}\Delta(\Lambda)^{\mathbf{N}\mathfrak{a}-1} \prod_{u\in\mathfrak{a}^{-1}\Lambda/\Lambda^*} (\wp(z;\Lambda) - \wp(u;\Lambda))^{-6}$$

**Definition 3.3.1.** Let $L \subseteq \mathbb{C}$ be a lattice. We define the **fundamental $\boldsymbol{\theta}$-function** of $L$ to be

$$\theta(z;L) = \Delta(L)e^{-6\eta(z;L)z}\sigma(z;L)^{12}$$

**Lemma 3.3.2.** *Let $L \subseteq \mathbb{C}$ be a lattice. Then $\theta(z;L)$ is $L$-perioidic.*

*Proof.* We need to show that for all $w \in L$ we have $\theta(z+w;L) = \theta(z;L)$. To this end, fix $w \in L$. By Proposition A.4.1 we have

$$\begin{aligned}\theta(z+w;L) &= \Delta(L)e^{-6\eta(z+w;L)(z+w)}\sigma(z+w;L)^{12}\\ &= \Delta(L)e^{-6\eta(z+w;L)(z+w)}\psi(w)^{12}e^{12\eta(w)(z+w/2)}\sigma(z;L)^{12}\end{aligned}$$

where $\psi(w) = 1$ if $w \in 2L$ and $-1$ if $w \notin 2L$. A routine, yet somewhat lengthy, calculation shows that the exponent of the exponential reduces to $-6\eta(z;L)z$ □

**Proposition 3.3.3.** *Consider the function*

$$f(z) = \frac{\theta(z;\Lambda)^{\mathbf{N}\mathfrak{a}}}{\theta(z;\mathfrak{a}^{-1}\Lambda)}$$

*Then $f(z)$ is a rational function on $E$ defined over $\mathbb{C}$ and is equal to $\Theta_{\Lambda,\mathfrak{a}}(z)$.*

*Proof.* By Lemma 3.3.2, $f(z)$ is $\Lambda$-periodic. By inspection and the properties of the other functions involved in $f$, we see that $f$ is holomorphic and so, in particular, it is an elliptic function. Appealing to Proposition A.4.3 shows that $f(z)$ is a rational function of $E$, defined over $\mathbb{C}$.

To prove the second claim, we first note that by Proposition A.4.1, $\sigma(z;\Lambda)$ has a simple zero for every $z \in \Lambda$ and no other zeroes. Hence $f$ admits the divisor

$$12\mathbf{N}\mathfrak{a}[0] - 12\sum_{u\in\mathfrak{a}^{-1}\Lambda/\Lambda}[u]$$

as a function on $\mathbb{C}/\Lambda$. By Lemma 3.2.1, this divisor is equal to that of $\Theta_{\Lambda,\mathfrak{a}}$ and so their ratio must be some constant $\lambda \in \mathbb{C}^\times$. Furthermore, $\Delta(\mathfrak{a}^{-1}\Lambda) = \alpha^{12}\Delta(\Lambda)$ and from this we deduce that $f(z)$ has Laurent expansion with first term

$$\alpha^{-12}\Delta(\Lambda)^{\mathbf{N}\mathfrak{a}-1}z^{12(N\mathfrak{a}-1)}$$

On the other hand, it is immediately obvious from Lemma 3.2.1 that $\Theta_{\Lambda,\mathfrak{a}}$ also has Laurent expansion with the same first term whence $\lambda = 1$ and $f(z) = \Theta_{\Lambda,\mathfrak{a}}(z)$ as desired. □

**Definition 3.3.4.** Let $L \subseteq \mathbb{C}$ be a lattice. For all $k \in \mathbb{N}_{\geq 1}$, we define the **Eisenstein series** attached to $L$ of weight $k$ to be the function

$$E_k(z; L) = \lim_{s\to k}\sum_{w\in L}\frac{(\overline{z}+\overline{w})^k}{|z+w|^{2s}}$$

where we understand the limit to mean evaluation of the analytic continuation of the series at $s = k$. We note that if $k \geq 3$ then

$$E_k(z; L) = \sum_{w\in L}\frac{1}{(z+w)^k}$$

**Proposition 3.3.5.** *Let $L \subseteq \mathbb{C}$ a lattice. Then for all $k \in \mathbb{N}_{\geq 3}$, we have*

$$\begin{aligned}
E_1(z; L) &= \zeta(z; L) - s_2(L)z - A(L)^{-1}\overline{z}\\
E_2(z; L) &= \wp(z; L) + s_2(L)\\
E_k(z; L) &= \frac{(-1)^k}{(k-1)!}\left(\frac{d}{dz}\right)^{(k-2)}\wp(z; L)
\end{aligned}$$

*Proof.* We shall only provide a sketch of the proof of this Proposition; for further details, see [GS81, Proposition 1.5].

First suppose that $k = 1$. Consider the function

$$\phi_s(z; L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{0\neq w\in L}\left(\frac{\bar{z}+\bar{w}}{|z+w|^{2s}} - \frac{\bar{w}}{|w|^{2s}}\left[1 - \frac{sz}{w} + \frac{\bar{z}}{\bar{w}}(1-s)\right]\right)$$

Then $\phi_s$ is convergent for $\Re(s) > 1/2$ and $\zeta(z; L) = \lim_{s\to 1^+}\phi_s(z; L)$. When $\Re(s) > 3/2$, we can rearrange the terms of the series. In particular,

$$\sum_{0\neq w\in L}\bar{w}|w|^{-2s} = 0$$

since we may pair up terms with opposite signs. Moreover, the series $\sum_{0\neq w\in L}|w|^{-2s}$ has a simple pole at $s = 1$ with residue $A(L)^{-1}$. Then

$$\begin{aligned}
\zeta(z; L) - zs_2(L) &= \lim_{s\to 1^+}\sum_{w\in L}\frac{(\bar{z}+\bar{w})^{-2s}}{|z+w|^{2s}} + \bar{z}A(L)^{-1}\\
&= E_1(z; L) + \bar{z}A(L)^{-1}
\end{aligned}$$

which proves the case where $k = 1$.

Now suppose that $k = 2$. By [Wei76, VIII §14] we have that $d/dzE_1(z; L) = -E_2(z; L)$ whence this case follows from the previous one.

The case where $k \in \mathbb{N}_{\geq 3}$ is immediate from the definition of the Weierstrass $\wp$-function. □

The next theorem provides us with the connection between the Eisenstein and Weierstrass points of view.

Coupled with results in the next section, this will demonstrate the power of the Eisenstein series as the middleman between the Θ-function and the $L$-function.

**Theorem 3.3.6.** *Given $n \in \mathbb{N}_{\geq 1}$ we have that*

$$\left(\frac{d}{dz}\right)^k \log \Theta_{\Lambda,\mathfrak{a}}(z) = 12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a}E_k(z;\Lambda) - E_k(z;\mathfrak{a}^{-1}\Lambda))$$

*Proof.* By Proposition 3.3.3, we can write the Θ-function in terms of the fundamental $\theta$-function of $\Lambda$ and so

$$\begin{aligned}\left(\frac{d}{dz}\right)^k \log \Theta_{\Lambda,\mathfrak{a}}(z) &= \left(\frac{d}{dz}\right)^k \log \frac{\theta(z;\Lambda)^{\mathbf{N}\mathfrak{a}}}{\theta(z;\mathfrak{a}^{-1}\Lambda)} \\ &= \left(\frac{d}{dz}\right)^{(k-1)} \left[\mathbf{N}\mathfrak{a}\frac{d}{dz}\log\theta(z;\Lambda) - \frac{d}{dz}\log\theta(z;\mathfrak{a}^{-1}\Lambda)\right] \qquad (3.2)\end{aligned}$$

Assume that $k = 1$. Then by the definition of $\theta(z;\Lambda)$ we have

$$\frac{d}{dz}\log\theta(z;\Lambda) = -12s_2(\Lambda)z - 12A(\Lambda)^{-1}\bar{z} + 12\zeta(z;\Lambda) = 12E_1(z;\Lambda)$$

Now assume that $k = 2$. Then differentiating the above, we have

$$\left(\frac{d}{dz}\right)^2 \log\theta(z;\Lambda) = -12s_2(\Lambda) - 12\wp(z;\Lambda) = -12E_2(z;\Lambda)$$

Finally, suppose that $k \in \mathbb{N}_{\geq 3}$. Then

$$\begin{aligned}\left(\frac{d}{dz}\right)^k \log\theta(z;\Lambda) &= \left(\frac{d}{dz}\right)^{(k-2)} (-12s_2(\Lambda) - 12\wp(z;\Lambda)) \\ &= -12\left(\frac{d}{dz}\right)^{(k-2)} \wp(z;\Lambda) \\ &= -12\frac{(k-1)!}{(-1)^k}E_k(z;\Lambda) \\ &= 12(-1)^{k-1}(k-1)!E_k(z;\Lambda)\end{aligned}$$

These calculations hold completely analogously for $\mathfrak{a}^{-1}\Lambda$ and so the Theorem follows upon substituting each case back into Equation 3.2. □

## 3.4 The Eisenstein-Hecke Connection and the Φ-function

In this section we shall make good on our promise to complete the other half of the puzzle and demonstrate the connection between the Eisenstein series defined in the previous section and the Hecke $L$-function. We recall that by Proposition 3.1.2, the value of the Θ-function of an elliptic curve $E$ depends only on the isomorphism class of $E$ over $\mathbb{C}$. In order to have any hope of expressing the $L$-function of $E$ (which is dependent on $E$ itself) in terms of the Eisenstein series, we shall have to equip Θ with data dependent on $E$. We shall do this via constructing a new rational function Φ on $E$ which is a product of certain translates of the Θ-function. We will then show that this is enough to determine the desired connection.

*Assumptions.* We continue to use the assumptions from the last section. We recall that $L(\bar{\psi}^k, s)$ is the $L$-function associated to powers of $\bar{\psi}$. Furthermore, if $\mathfrak{m} \lhd \mathcal{O}_K$ is an ideal divisible by $\mathfrak{f}$ and $\mathfrak{c}$ is prime to $\mathfrak{m}$ then $L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c})$ is the partial $L$-function whose defining series is restricted to ideals of $\mathcal{O}_K$ prime to $\mathfrak{m}$ such that $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$.

**Definition 3.4.1.** Let $F$ be an $\mathcal{O}_K$-generator of $E[\mathfrak{f}]$. We define the Φ-function of $E$ to be the rational function defined over $K$ given by

$$\Phi_{E,\mathfrak{a}}(Q) = \Phi_{E,\mathfrak{a},F}(Q) = \prod_{\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)} (\Theta_{E,\mathfrak{a}} \circ \tau_{F^\sigma})(Q)$$

where we understand $\tau_P : E \to E$ to be the translation-by-$P$ map on $E$.

*Remark.* We note that the action of $\mathrm{Gal}(K(\mathfrak{f})/K)$ on $F \in E[\mathfrak{f}]$ is well-defined since Part 1 of Theorem A.7.9 implies that $F \in E(K(\mathfrak{f}))$.

**Proposition 3.4.2.** *Let $B_\mathfrak{f}$ be a collection of ideals of $\mathcal{O}_K$ that are prime to $\mathfrak{af}$ such that the Artin map induces a bijection between $B_\mathfrak{f}$ and $\mathrm{Gal}(K(\mathfrak{f})/K)$. Then*

$$\Phi_{E,\mathfrak{a}}(P) = \prod_{\mathfrak{b} \in B_\mathfrak{f}} \Theta_{E,\mathfrak{a}}(\psi_E(\mathfrak{b})F + Q)$$

*Furthermore, if $\mathfrak{c} \lhd \mathcal{O}_K$ is an ideal and $Q \in E[\mathfrak{c}]$ that is not an $\mathfrak{f}$-torsion point then $\Phi_{E,\mathfrak{a}}(Q)$ is a global unit of $K(E[\mathfrak{c}])$.*

*Proof.* The first assertion follows immediately from Corollary 5.16ii which asserts that the action of $[\mathfrak{b}, K(\mathfrak{f})/K] \in \mathrm{Gal}(K(\mathfrak{f})/K)$ is given by multiplication by $\psi_E(\mathfrak{b})$.

To see the second assertion, it suffices to realise that $\psi_E(\mathfrak{b})F + Q$ generates a torsion group given by an ideal that is not a prime power whence Theorem 3.1.5 implies that $\Phi_{E,\mathfrak{a}}(Q)$ is a global unit. □

Similar to the Θ-function, we also have an analytic definition for the Φ-function in the form of the following definition.

**Definition 3.4.3.** Let $f$ be a generator of $\mathfrak{f}$. We define the Φ-function of $\mathbb{C}/\Lambda$ to be

$$\Phi_{\Lambda,\mathfrak{a}}(z) = \Phi_{\Lambda,\mathfrak{a},f}(z) = \Phi E, \mathfrak{a}, \xi(\omega/f)(\xi(z))$$

The following theorem gives us the connection between the Hecke $L$-function and the Eisenstein series.

**Theorem 3.4.4.** *Let $\mathfrak{m} \lhd \mathcal{O}_K$ be an ideal divisible by $\mathfrak{f}$ and $v \in \mathfrak{m}^{-1}\Lambda/\Lambda$ an $\mathfrak{m}$-torsion point of exact order $\mathfrak{m}$. Then for all $k \in \mathbb{N}_{\geq 1}$ we have*

$$E_k(v; \Lambda) = v^{-k}\psi_E(\mathfrak{c})^k L_\mathfrak{m}(\overline{\psi_E}^k, k, \mathfrak{c})$$

*where $\mathfrak{c} = \Omega^{-1}v\mathfrak{m}$.*

*Proof.* Let $\mu$ be a generator of $\mathfrak{m}$ so that we may write $v = \gamma\Omega/\mu$ for some $\gamma \in \mathcal{O}_K$ not divisible by $\mathfrak{m}$. For sufficiently large $s$ we have

$$\begin{aligned}
\sum_{w \in \Lambda} \frac{(\bar{v} + \bar{w})^k}{|v + w|^{2s}} = \sum_{w \in \Omega\mathcal{O}_K} \frac{(\overline{\gamma\Omega/\mu} + \bar{w})^k}{|\gamma\Omega/\mu + w|^{2s}} &= \sum_{w \in \mathcal{O}_K} \frac{(\overline{\gamma\Omega/\mu} + \overline{\Omega w})^k}{|\gamma\Omega/\mu + \Omega w|^{2s}} \\
&= \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \sum_{w \in \mathcal{O}_K} \frac{(\overline{\gamma/\mu} + \bar{w})^k}{|\gamma/\mu + w|^{2s}} \\
&= \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \frac{|\mu|^{2s}}{\bar{\mu}^k} \sum_{w \in \mathcal{O}_K} \frac{(\bar{\gamma} + \overline{\mu w})^k}{|\gamma + \mu w|^{2s}} \\
&= \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \frac{|\mu|^{2s}}{\bar{\mu}^k} \sum_{\substack{\beta \in \mathcal{O}_K \\ \beta \equiv \gamma \pmod{\mathfrak{m}}}} \frac{\bar{\beta}^k}{|\beta|^{2s}} \qquad (3.3)
\end{aligned}$$

By Theorem A.7.6, $\psi_E(\beta\mathcal{O}_K) = \beta\mathcal{O}_K$ so that $\psi_E(\mathcal{O}_K)/\beta \in \mathcal{O}_K^\times$. Let $Z = \{\,\beta \in \mathcal{O}_K \mid ((\beta), \mathfrak{f}) = 1\,\}$ and define a multiplicative map

$$\begin{aligned} \varepsilon : Z &\to \mathcal{O}_K^\times \\ \beta &\mapsto \frac{\psi_E(\beta\mathcal{O}_K)}{\beta} \end{aligned}$$

By the definition of the conductor $\mathfrak{f}$, $\epsilon$ must factor through $(\mathcal{O}_K/\mathfrak{f})^\times$. Hence for all $\beta \in \mathcal{O}_K$ such that $\beta \equiv \gamma \pmod{\mathfrak{m}}$ we must have that

$$\bar{\beta} = \overline{\psi_E}(\beta\mathcal{O}_K)\frac{\psi_E(\gamma\mathcal{O}_K)}{\gamma}$$

To ease notation, denote $\sigma_{\mathfrak{b}} = [\mathfrak{b}, K(\mathfrak{m})/K)]$. It then follows that

$$\sum_{\substack{\beta\in\mathcal{O}_K \\ \beta\equiv\gamma \pmod{\mathfrak{m}}}} \frac{\bar{\beta}^k}{|\beta|^{2s}} = \sum_{\substack{\beta\in\mathcal{O}_K \\ \beta\equiv\gamma \pmod{\mathfrak{m}}}} \frac{\overline{\psi_E}^k(\beta\mathcal{O}_K)\psi_E^k(\gamma\mathcal{O}_K)}{|\beta|^{2s}\gamma^k} = \frac{\psi_E^k(\gamma\mathcal{O}_K)}{\gamma^k}\sum_{\substack{\mathfrak{b}\lhd\mathcal{O}_K \\ \sigma_{\mathfrak{b}}=\sigma_{\mathfrak{c}}}} \frac{\overline{\psi_E}^k(\mathfrak{b})}{\mathbf{N}\mathfrak{b}^s} = \frac{\psi_E^k(\mathfrak{c})}{\gamma^k}L_{\mathfrak{m}}(\overline{\psi_E}^k, s, \mathfrak{c})$$

Substituting this back into equation 3.3 yields

$$\begin{aligned} \sum_{w\in\Lambda}\frac{(\bar{v}+\bar{w})^k}{|v+w|^{2s}} &= \frac{\bar{\Omega}^k}{|\Omega|^{2s}}\frac{|\mu|^{2s}}{\bar{\mu}^k}\frac{\psi_E^k(\mathfrak{c})}{\gamma^k}L_{\mathfrak{m}}(\overline{\psi_E}^k, s, \mathfrak{c}) \\ &= \frac{\bar{\Omega}^k}{|\Omega|^{2s}}\frac{|\mu|^{2s}}{\bar{\mu}^k}\frac{\psi_E^k(\mathfrak{c})}{v^k\Omega^{-k}\mu}L_{\mathfrak{m}}(\overline{\psi_E}^k, s, \mathfrak{c}) \\ &= \frac{|\Omega|^{2k}}{|\Omega|^{2s}}\frac{|\mu|^{2s}}{|\mu|^{2k}}v^{-k}\psi_E^k(\mathfrak{c})L_{\mathfrak{m}}(\overline{\psi_E}^k, s, \mathfrak{c}) \end{aligned}$$

The Theorem then follows upon passing to the analytic continuation and evaluating at $s = k$. □

**Lemma 3.4.5.** *Let $\mathfrak{a} \lhd \mathcal{O}_K$ be an ideal prime to $\mathfrak{f}$. Then for all $k \in \mathbb{N}_{\geq 1}$ we have*

$$E_k(z; \mathfrak{a}^{-1}\Lambda) = \psi_E(\mathfrak{a})^k E_k(\psi_E(\mathfrak{a})z; \Lambda)$$

*Proof.* Fix a generator $\alpha$ of $\mathfrak{a}$ and first suppose that $k = 1$. Then

$$\begin{aligned} E_1(z; \mathfrak{a}^{-1}\Lambda) &= \zeta(z; \mathfrak{a}^{-1}\Lambda) - s_2(\mathfrak{a}^{-1}\Lambda)z - A(\mathfrak{a}^{-1}\Lambda)^{-1}\bar{z} \\ &= \frac{1}{z} + \sum_{0\neq w\in\Lambda}\left(\frac{1}{z-\alpha^{-1}w} + \frac{1}{\alpha^{-1}w} + \frac{z}{(\alpha^{-1}w)^2}\right) \\ &\quad - \left[\lim_{s\to 0^+}\sum_{0\neq w\in\Lambda}(\alpha^{-1}w)^{-2}|\alpha^{-1}w|^{-2s}\right]z - \left[\pi^{-1}\operatorname{covol}\left(\mathbb{C}/\alpha^{-1}\Lambda\right)\right]\bar{z} \\ &= \frac{1}{z} + \alpha\sum_{0\neq w\in\Lambda}\left(\frac{1}{\alpha z - w} + \frac{1}{w} + \frac{\alpha z}{w^2}\right) \\ &\quad - \alpha\left[\lim_{s\to 0^+}\sum_{0\neq w\in\Lambda}w^{-2}|w|^{-2s}\right](\alpha z) - |\alpha|\left[\pi^{-1}\operatorname{covol}\left(\mathbb{C}/\Lambda\right)\right]\bar{z} \\ &= \alpha E_1(\alpha z, \Lambda) \end{aligned}$$

Now suppose that $k = 2$. We then have that

$$\begin{aligned} E_2(z;\alpha^{-1}\Lambda) &= \frac{1}{z^2} + \sum_{0\neq w\in\Lambda}\left(\frac{1}{(z+\alpha w)^2} - \frac{1}{(\alpha w)^2}\right) + \lim_{s\to 0^+}\sum_{0\neq w\in\Lambda}(\alpha w)^{-2}|\alpha w|^{-2s} \\ &= \frac{1}{z^2} + \alpha^2\sum_{0\neq w\in\Lambda}\left(\frac{1}{(\alpha z+w)^2} - \frac{1}{w^2}\right) + \alpha^2\lim_{s\to 0+}\sum_{0\neq w\in\Lambda} w^{-2}|w|^{-2s} \\ &= \alpha^2 E_2(\alpha z;\Lambda) \end{aligned}$$

Finally, suppose that $k = 3$. It stands that

$$E_k(z;\mathfrak{a}^{-1}\Lambda) = \sum_{w\in\Lambda}\frac{1}{(z+\alpha^{-1}w)^k} = \alpha^k\sum_{w\in\Lambda}\frac{1}{(\alpha z+w)^k} = \alpha^k E_k(\alpha z;\Lambda)$$

Appealing to Theorem A.7.6 shows that $\alpha = \psi_E(\mathfrak{a})$ whence the Lemma follows. □

**Proposition 3.4.6.** *Let $f$ be a generator of the conductor $\mathfrak{f}$. Then for all $k \in \mathbb{N}_{\geq 1}$ we have*

$$\left(\frac{d}{dz}\right)^k \log\Phi_{\Lambda,\mathfrak{a}}(z)\Bigg|_{z=0} = 12f^k\Omega^{-k}(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a} - \psi_E(\mathfrak{a})^k)L(\overline{\psi_E}^k, k)$$

*Proof.* As usual, fix a collection $B_\mathfrak{f}$ of ideals of $\mathcal{O}_K$ prime to $\mathfrak{af}$ such that the Artin map induces a bijection between $B_\mathfrak{f}$ and $\mathrm{Gal}(K(\mathfrak{f})/K)$. To ease the exposition, let $u = \Omega/f$. By the definition of the Φ-function, Theorem 3.3.6 and Lemma 3.4.5, we have that

$$\begin{aligned} \left(\frac{d}{dz}\right)^k \log\Phi_{\Lambda,\mathfrak{a}}(z)\Bigg|_{z=0} &= \left(\frac{d}{dz}\right)^k \log\prod_{\mathfrak{b}\in B_\mathfrak{f}}\Theta_{\Lambda,\mathfrak{a}}(\psi_E(\mathfrak{b})u+z)\Bigg|_{z=0} \\ &= \sum_{\mathfrak{b}\in B_\mathfrak{f}}\left(\frac{d}{dz}\right)^k\log\Theta_{\Lambda,\mathfrak{a}}(z)\Bigg|_{z=\psi_E(\mathfrak{b})u} \\ &= \sum_{\mathfrak{b}\in B_\mathfrak{f}}(12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a}E_k(\psi_E(\mathfrak{b})u;\Lambda) - E_k(\psi_E(\mathfrak{b});\mathfrak{a}^{-1}\Lambda))) \\ &= 12(-1)^{k-1}(k-1)!\left(\mathbf{N}\mathfrak{a}\sum_{\mathfrak{b}\in B_\mathfrak{f}}E_k(\psi_E(\mathfrak{b})u;\Lambda) - \psi_E(\mathfrak{a})^k\sum_{\mathfrak{b}\in B_\mathfrak{f}}E_k(\psi_E(\mathfrak{ab})u;\Lambda)\right) \end{aligned}$$

We next observe that the multiplicativity of the Artin map implies that the collection $\mathfrak{a}B_\mathfrak{f}$ is also in bijection with $\mathrm{Gal}(K(f)/K)$. We may thus assume, without loss of generality, that the $\psi_E(\mathfrak{a})$ factor does not occur in the first argument of the Eisenstein series in the second term above. Appealing to Theorem 3.4.4 shows that

$$\begin{aligned} \left(\frac{d}{dz}\right)^k \log\Phi_{\Lambda,\mathfrak{a}}(z)\Bigg|_{z=0} &= 12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a} - \psi_E(\mathfrak{a})^k)\sum_{\mathfrak{b}\in B_\mathfrak{f}}E_k(\psi_E(\mathfrak{b})u,\Lambda) \\ &= 12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a} - \psi_E(\mathfrak{a})^k)\sum_{\mathfrak{b}\in B_\mathfrak{f}}((\psi_E(\mathfrak{b})u)^{-k})\psi_E(\mathfrak{b})^k L_\mathfrak{f}(\overline{\psi_E}^k, k, \mathfrak{b}) \\ &= 12f^k\Omega^{-k}(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a} - \psi_E(\mathfrak{a})^k)L(\overline{\psi_E}^k, k) \end{aligned}$$

and so the Proposition is proven. □

This Proposition forms a key component in the proof of the Coates-Wiles Theorem. Indeed, it will aid us in demonstrating the connection between the value of $L(\overline{\psi_E}, 1)$ and the elliptic units.

Armed with this result, we are now finally able to define our desired collection of units. These will be at the very heart of the proof and, as such, we will study them in further generality in the next Chapter.

Let $\mathfrak{p}$ be a finite prime of $K$ prime to $(f) = \mathfrak{f}$ and to 6. Let $\mathcal{R}$ be the collection of square-free integral ideals of $\mathcal{O}_K$ prime to $6\mathfrak{a}\mathfrak{f}\mathfrak{p}$. Let $K_n = K(E[\mathfrak{p}^n])$ and, given $\mathfrak{r} \in \mathcal{R}$, write $K_n^{\mathfrak{r}} = K_n(E[\mathfrak{r}])$.

**Definition 3.4.7.** For all $n \in \mathbb{N}_{n \geq 0}$ and $\mathfrak{r} \in \mathcal{R}$, we define the **elliptic units** of $K$ to be the elements of $\overline{K}$ given by

$$\eta_n(\mathfrak{r}) = \Phi_{\Lambda,\mathfrak{a},f}(\psi_E(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)$$

**Proposition 3.4.8.** *Let $n \in \mathbb{N}_{n \geq 0}$ and $\mathfrak{r} \in \mathcal{R}$. Then $\eta_n(\mathfrak{r})$ is a global unit in $K_n^{\mathfrak{r}}$ and the elliptic units satisfy the norm compatibility relations*

1. *For all primes $\mathfrak{q} \in \mathcal{R}$ not dividing $\mathfrak{r}$ we have*

$$\mathbf{N}_{K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}}\, \eta_n(\mathfrak{q}\mathfrak{r}) = \eta_n(\mathfrak{r})^{1-((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}}$$

2. $\mathbf{N}_{K_{n+1}^{\mathfrak{r}}/K_n^{\mathfrak{r}}}\, \eta_{n+1}(\mathfrak{r}) = \eta_n(\mathfrak{r})$

*Proof.* The fact that $\eta_n(\mathfrak{r})$ is a global unit follows immediately from Proposition 3.4.2.

To prove the first relation, we first observe that by Theorem A.7.9 we have that $G = \mathrm{Gal}(K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}) \cong \mathrm{Gal}(K_n^{\mathfrak{q}\mathfrak{f}\mathfrak{r}}/K_n^{\mathfrak{f}\mathfrak{r}})$. Expanding the definitions, we have

$$\mathbf{N}_{K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}}\, \eta_n(\mathfrak{q}\mathfrak{r}) = \prod_{\sigma \in G} \Lambda_{E,\mathfrak{a},\xi(\omega/f)}(\xi(\psi_E(\mathfrak{p}^n\mathfrak{q}\mathfrak{r})^{-1}\Omega))$$

In order to switch to the algebraic perspective, write $F = \xi(\Omega/f)$ and note that $Q = \xi(\psi_E(\mathfrak{p}^n\mathfrak{q}\mathfrak{t})^{-1}\Omega) \in E[\mathfrak{p}^n\mathfrak{q}\mathfrak{t}]$ has order exactly $\mathfrak{p}^n\mathfrak{q}\mathfrak{t}$. Let $B_{\mathfrak{f}}$ be a collection of ideals of $\mathcal{O}_K$, prime to $\mathfrak{a}\mathfrak{f}$, that is in bijection with $\mathrm{Gal}(K(\mathfrak{f})/K)$ under the Artin map. Furthermore, recall that $\psi_E(\mathfrak{q})$ is a generator for $\mathfrak{q}$. By Proposition A.7.8, the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p}^n\mathfrak{r}\mathfrak{f})^\times$ is injective. We may thus appeal to Corollary 3.2.3 to see that

$$\begin{aligned}
\mathbf{N}_{K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}}\, \eta_n(\mathfrak{q}\mathfrak{r}) &= \prod_{\sigma \in G} \Phi_{E,\mathfrak{a},\xi(\omega/f)}(\xi(\psi_E(\mathfrak{p}^n\mathfrak{q}\mathfrak{r})^{-1}\Omega)) \\
&= \prod_{\sigma \in G} \prod_{\mathfrak{b} \in B_{\mathfrak{f}}} \Theta_{E,\mathfrak{a}}(\psi_E(\mathfrak{b})F + Q) \\
&= \prod_{\mathfrak{b} \in B_{\mathfrak{f}}} \Theta(\psi_E(\mathfrak{b}\mathfrak{q}) + \psi_E(\mathfrak{q})Q)^{1-((K(\mathfrak{p}^n\mathfrak{f}\mathfrak{r})/K),\mathfrak{q})^{-1}} \\
&= \Phi_{\Lambda,\mathfrak{a}}(\psi_E(\mathfrak{q})\psi_E(\mathfrak{p}^n\mathfrak{q}\mathfrak{r})^{-1}\Omega)^{1-((K(\mathfrak{p}^n\mathfrak{f}\mathfrak{r})/K),\mathfrak{q})^{-1}} \\
&= \eta_n(\mathfrak{r})^{1-((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}}
\end{aligned}$$

Where in the last equality we used Proposition 3.4.2 to see that $\Phi_{\Lambda,\mathfrak{a}}(\psi_E(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)$ is a global unit in $K(E[\mathfrak{p}^n\mathfrak{r}])$ after which we applied the consistency property of the Artin symbol $((K(\mathfrak{p}^n\mathfrak{f}\mathfrak{r})/K),\mathfrak{q})|_{K_n^{\mathfrak{r}}} = ((K_n^{\mathfrak{r}}/K),\mathfrak{q})$. The second relation follows in exactly the same fashion using the first case of Corollary 3.2.3 rather than the second. □

## 3.5 The $\mathfrak{p}$-adic $\Phi$-function

Our final task of this chapter shall be to determine the nature of the $\Phi$-function locally. In particular, we will show that at primes of good reduction $\mathfrak{p}$, $\Phi$ is an element of $\mathcal{O}_{K,\mathfrak{p}}[[Z]]^\times$.

*Assumptions.* We continue to use the assumptions from the last section. Furthermore, we let $\mathfrak{p}$ be a finite prime of $K$ prime to $6\mathfrak{f}$ and we introduce the constraint that the auxiliary ideal is also prime to $\mathfrak{p}$. Recall that $\widehat{E}$ is the formal group associated with $E$, $x(Z), y(Z) \in \mathcal{O}_{K,\mathfrak{p}}[[X]]$ are the formal coordinate functions and $\widehat{\omega}_E(Z) \in 1 + Z\mathcal{O}_{K,\mathfrak{p}}[[X]]$ is the formal differential.

**Definition 3.5.1.** We define the **derivative operator** on $K_{\mathfrak{p}}((X))$ to be

$$D = \frac{1}{\widehat{\omega}_E(Z)} \frac{d}{dZ}$$

The following lemma will show us that the above notion of the derivative operator is the correct one to adopt.

**Lemma 3.5.2.** *The derivative operator induces a commutative diagram*

$$\begin{tikzcd}
K(x(Z), y(Z)) \arrow[r, hook] \arrow[d, "D"] & K_{\mathfrak{p}}((Z)) \arrow[d, "D"] \\
K(x(Z), y(Z)) \arrow[r, hook] & K_{\mathfrak{p}}((Z))
\end{tikzcd}$$

*Proof.* We have the following diagram with first two squares commuting

$$\begin{tikzcd}
K(\wp(z), \wp'(z)) \arrow[r, "\sim"] \arrow[d, "\frac{d}{dz}"] & K(E) \arrow[r, "\sim"] \arrow[d] & K(x(Z), y(Z)) \arrow[r, hook] \arrow[d, "D"] & K_{\mathfrak{p}}((Z)) \arrow[d, "D"] \\
K(\wp(z), \wp'(z)) \arrow[r, "\sim"] & K(E) \arrow[r, "\sim"] & K(x(Z), y(Z)) \arrow[r, hook] & K_{\mathfrak{p}}((Z))
\end{tikzcd}$$

which is obtained by identifying the coordinate functions in the analytic, algebraic and formal settings. Substituting the Weierstrass coordinate functions into the Weierstrass equation yields the relation

$$\wp'(z)^2 = 4\wp(z)^3 + 4a\wp(z) + 4b$$

Differentiating this relation gives $\wp''(z) = 6\wp(z)^2 + 2a$. But this relation also holds in $K_{\mathfrak{p}}(\wp(z), \wp'(z))$ so it suffices to prove that $D(x(Z)) = 2y(Z)$ and $D(y(Z)) = 3x(Z)^2 + a$. Indeed, we have

$$D(x(Z)) = \frac{2y(Z)}{d/dzx(Z)} \frac{d}{dz} x(Z) = 2y(Z)$$

Similarly,

$$D(y^2(Z)) = \frac{1}{\widehat{\omega}_E} \frac{d}{dz} y^2(Z) = 2y(Z)D(y(Z))$$

However, on the other hand we have

$$D(y^2(Z)) = D(x^3(Z) + ax(Z) + b) = 6x^2(Z)y(Z) + 2ay(Z)$$

whence $D(y(Z)) = 3x(Z)^2 + a$ as desired. Hence the right hand square in the above diagram also commutes. □

**Theorem 3.5.3.** *Fix an embedding of $K$ into $K_{\mathfrak{p}}$ and let $\Phi_{\mathfrak{p},\mathfrak{a}}$ be the image of $\Phi_{E,\mathfrak{a}}$ under the induced embedding of $K(x(Z), y(Z))$ into $K_{\mathfrak{p}}((Z))$. Then $\Phi_{\mathfrak{p},\mathfrak{a}} \in \mathcal{O}_{K,\mathfrak{p}}[[Z]]^{\times}$. Moreover, for all $k \in \mathbb{N}_{\geq 1}$*

$$D^k \log(\Phi_{\mathfrak{p},\mathfrak{a}}(z))\big|_{z=0} = 12(-1)^{k-1}(k-1)! f^k (\mathbf{N}\mathfrak{a} - \psi_E(\mathfrak{a})^k)\Omega^{-k} L(\overline{\psi_E}^k, k)$$

*Proof.* Let $\mathcal{O}$ be the ring of integers of $\overline{K_{\mathfrak{p}}}$. It suffices to show that $\Phi_{\mathfrak{p},\mathfrak{a}} \in \mathcal{O}[[X]]^{\times}$. Indeed, by definition of the chosen embedding, we have that $\Phi_{\mathfrak{p},\mathfrak{a}} \in K_{\mathfrak{p}}((X))$ so from the claim we would then be able to deduce that $\Phi_{\mathfrak{p},\mathfrak{a}} \in \mathcal{O}_{K,\mathfrak{p}}[[X]]^{\times}$.

Let $F$ be an $\mathcal{O}_K$-generator of $E[\mathfrak{f}]$ and $B_{\mathfrak{f}}$ a collection of ideals of $\mathcal{O}_K$, prime to $\mathfrak{af}$, which is in bijection with $\text{Gal}(K(\mathfrak{f})/K)$ via the Artin map. Let $Q \in E[\mathfrak{a}]^*$ and consider the factor $(\psi_E(\mathfrak{b})F + P) - x(Q)$ in the formula for

$\Theta_{E,\mathfrak{a}}(P)$. The addition law on $E$ gives

$$x(\psi_E(\mathfrak{b}F)+P)-x(Q)=\frac{(y(P)-y(\psi_E(\mathfrak{b})F))^2}{(x(P)-x(\psi_E(\mathfrak{b})F))^2}-x(P)-x(\psi_E(\mathfrak{b})F)-x(Q)$$

Now, $\psi_E(\mathfrak{b})F$ is not in the kernel of reduction modulo $\mathfrak{p}$ and so Proposition A.5.2 implies that $v_{\mathfrak{p}}(x(\psi_E(\mathfrak{b}F)))\geq 0$ and similarly for the $y$ coordinate. Moreover, Part 2 of Lemma 3.1.4 shows that $v_{\mathfrak{p}}(x(Q))\geq 0$. We now switch to the formal perspective by replacing $x(P)$ and $y(P)$ with the formal Laurent series $x(Z),y(Z)\in\mathcal{O}_{K,\mathfrak{p}}((X))$. By definition of these series, we have that $x(\psi_E(\mathfrak{b})F+Z)-x(Q)\in\mathcal{O}[[X]]$. Evaluating this at $Z=0$ yields $x(\psi_E(\mathfrak{b})F)-x(Q)$ which is an element of $\mathcal{O}^\times$ by Part 3 of Lemma 3.1.4.

Recall that $\mathfrak{p}\nmid\mathfrak{af}$ and so $\Delta(E),\alpha\in\mathcal{O}_{K,\mathfrak{p}}^\times$. Hence

$$\Phi_{\mathfrak{p},\mathfrak{a}}(Z)=\alpha^{-12|B_{\mathfrak{f}}|}\Delta(E)^{|B_{\mathfrak{f}}|\mathbf{N}\mathfrak{a}-1}\prod_{\substack{\mathfrak{b}\in B_{\mathfrak{f}}\\ Q\in E[\mathfrak{a}]^*}}(x(\psi_E(\mathfrak{b})F+Z)-x(Q))^{-6}$$

The second assertion follows immediately upon combining Proposition 3.4.6 with Lemma 3.5.2. □

# Chapter 4

# Euler Systems

Euler systems were introduced by Kolyvagin in his paper [Kol90] in order to place bounds on the ideal class groups of certain number fields. More concretely, he used the Euler system of cyclotomic units in number fields of the form $F(\boldsymbol{\mu}_n)$ to bound the ideal class group of $F$. In [Rub91], Rubin was able to use Kolyvagin's method with the Euler system of elliptic units to bound the ideal class groups of abelian extensions of an imaginary quadratic number field.

In this chapter we shall define Euler systems in enough generality to encompass both the cyclotomic and elliptic cases. We will then go on to demonstrate properties about these abstract Euler systems which we will then use to construct certain principle ideals in abelian extensions of our base field. We will then show how these principle ideals can be used to bound ideal class groups. This theory forms another key part of the proof of the Coates-Wiles Theorem and we shall make heavy use of it in the sequel in order to calculate certain Selmer groups.

## 4.1 Axiomatising the norm-compatibility relations

Our goal in this section shall be to provide an axiomatic framework for Euler systems. We aim to capture, as much as possible, the behaviour that both the cyclotomic and elliptic units exhibit. In particular, we would like for our abstract Euler systems to mimic the norm-compatibility relations as seen in Proposition 3.4.8. We shall introduce the so-called universal Euler system of particular number fields $K$ which is an object from which all Euler systems on $K$ can be constructed[1].

*Assumptions.* Throughout this section, we shall assume that $K$ is a number field. Let $\mathfrak{p}$ be a finite prime of $K$ lying above the rational prime $p$ and define $\mathcal{R}^{\mathfrak{e}}$ to be the collection of all square-free ideals of $\mathcal{O}_K$ that are prime to both $\mathfrak{p}$ and the so-called exceptional ideal $\mathfrak{e}$. We shall use $\mathfrak{q}$ to refer to a prime ideal in $\mathcal{R}^{\mathfrak{e}}$. If $\mathfrak{r}, \mathfrak{s} \in \mathcal{R}^{\mathfrak{e}}$, we shall write $\mathfrak{r}/\mathfrak{s}$ to mean the ideal of $\mathcal{R}^{\mathfrak{e}}$ given by dividing $\mathfrak{r}$ out by the primes dividing $\mathfrak{s}$. Finally, except in cases of ambiguity, we shall simply write $\mathcal{R} = \mathcal{R}^{\mathfrak{e}}$.

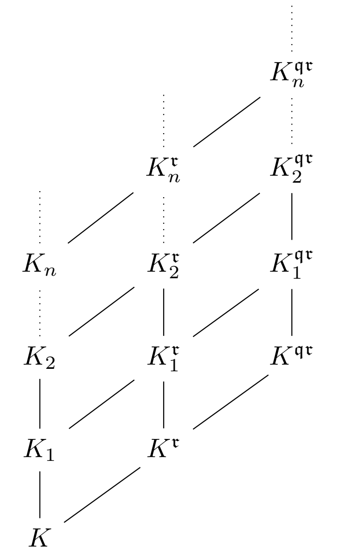
**Definition 4.1.1.** We define a **$\mathfrak{p}$-system** of $K$ to be a tower of abelian extensions

$$K = K_0 \subseteq K_1 \subseteq \cdots K_n \subseteq \cdots$$

together with abelian extensions[2] $K_n^{\mathfrak{r}}/K_n$ for every $n \in \mathbb{N}_{\geq 0}$ and $\mathfrak{r} \in \mathcal{R}$ such that we have the following diagram of field extensions

[1] This is a slight exaggeration - we will be able to construct all Euler systems that are of immediate interest. The general theory of Euler systems is vast and far outside the scope of this essay. The interested reader is encouraged to see Rubin's book [Rub14].

[2] Note that we are taking the convention $K_n^{1} = K_n$.


$K_n^{\mathfrak{q}\mathfrak{r}}$
$K_n^{\mathfrak{r}}$
$K_2^{\mathfrak{q}\mathfrak{r}}$
$K_n$
$K_2^{\mathfrak{r}}$
$K_1^{\mathfrak{q}\mathfrak{r}}$
$K_2$
$K_1^{\mathfrak{r}}$
$K^{\mathfrak{q}\mathfrak{r}}$
$K_1$
$K^{\mathfrak{r}}$
$K$

and satisfying $\mathrm{Gal}(K_n^{\mathfrak{r}}/K) = (\mathcal{O}_K/\mathfrak{p}^n\mathfrak{r})^\times$ and for all primes $\mathfrak{q} \neq \mathfrak{p}$, the extension $K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}$ has degree $\mathbf{N}\mathfrak{q} - 1$, is totally ramified above primes lying over $\mathfrak{q}$ and unramified everywhere else.

For the rest of this chapter, unless otherwise stated, we fix an arbitrary $\mathfrak{p}$-system of $K$. We observe that, using the notation above, we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(K_n^{\mathfrak{r}}/K_n) \longrightarrow \mathrm{Gal}(K_n^{\mathfrak{r}}/K) \longrightarrow \mathrm{Gal}(K_n/K) \longrightarrow 1$$

So that $G_{\mathfrak{r}} = \mathrm{Gal}(K_n^{\mathfrak{r}}/K_n) = (\mathcal{O}_K/\mathfrak{r})^\times$. Applying the Chinese Remainder Theorem we obtain a commutative diagram of isomorphisms

$$\begin{tikzcd}
G_{\mathfrak{r}} \arrow[r] \arrow[d] & \prod_{\mathfrak{q}|\mathfrak{r}} \arrow[d] \\
(\mathcal{O}_K/\mathfrak{r})^\times \arrow[r] & \prod_{\mathfrak{q}|\mathfrak{r}}(\mathcal{O}_K/\mathfrak{q})^\times
\end{tikzcd}$$

**Definition 4.1.2.** Let $\mathfrak{q} \in \mathcal{R}$ be a prime ideal. We define the **$\mathfrak{q}$-norm operator** in $\mathbb{Z}[G_{\mathfrak{q}}]$ to be

$$N_{\mathfrak{q}} = \sum_{\sigma \in G_{\mathfrak{q}}} \sigma$$

Moreover, if $\mathfrak{r} \in \mathcal{R}^{\mathfrak{c}}$ is any ideal then we also define the **$\mathfrak{r}$-norm operator** in $\mathbb{Z}[G_{\mathfrak{r}}]$ to be

$$N_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{t}} N_{\mathfrak{q}} \in$$

**Definition 4.1.3.** Let $\mathfrak{q} \in \mathcal{R}$ be a prime ideal. We define the **$\mathfrak{q}$-derivative operator** in $\mathbb{Z}[G_{\mathfrak{q}}]$ to be

$$D_{\mathfrak{q}} = \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i$$

Moreover, if $\mathfrak{r} \in \mathcal{R}^{\mathfrak{c}}$ is any ideal then we also define the **$\mathfrak{r}$-derivative operator** in $\mathbb{Z}[G_{\mathfrak{r}}]$ to be

$$D_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} D_{\mathfrak{q}}$$

**Lemma 4.1.4** (Telescoping Identity)**.** *Let $\mathfrak{q} \in \mathcal{R}$ be a prime and $\sigma_{\mathfrak{q}}$ a generator of $G_{\mathfrak{q}}$. Then*

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = \mathbf{N}\mathfrak{q} - 1 - N_{\mathfrak{q}}$$

*Proof.* Expanding the definition of $D_{\mathfrak{q}}$, we have that

$$\begin{aligned}(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^{i+1} - \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^{i} &= \sigma_{\mathfrak{q}}^2 - \sigma_{\mathfrak{q}} - 2\sigma_{\mathfrak{q}}^3 - 2\sigma_{\mathfrak{q}}^2 + \cdots + (\mathbf{N}\mathfrak{q} - 2) + (\mathbf{N}\mathfrak{q} - 2)\sigma_{\mathfrak{q}}^{\mathbf{N}\mathfrak{q}-2} \\ &= \mathbf{N}\mathfrak{q} - 2 - \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} \sigma_{\mathfrak{q}}^{i} = \mathbf{N}\mathfrak{q} - 1 - N_{\mathfrak{q}}\end{aligned}$$

□

We now make a series of definitions in order to construct Euler systems. In particular, we shall obtain a universal Euler system via the direct limit of individual so-called Euler modules. These Euler modules, together with the connecting homomorphisms of the direct system that they form, will provide an axiomatisation of the norm-compatibility relations manifest in elliptic units.

**Definition 4.1.5.** Given $n \in \mathbb{N}$ and $\mathfrak{r} \in \mathcal{R}^{\mathfrak{e}}$, let $x_{n,\mathfrak{r}}$ be an indeterminate. Let $Y_{n,\mathfrak{r}}$ be the free $\mathbb{Z}[\mathrm{Gal}(K_n^{\mathfrak{r}}/K)]$-module on the indeterminates $\{\, x_{n,\mathfrak{s}} \mid \mathfrak{s} \mid \mathfrak{r} \,\}$ and $Z_{n,\mathfrak{r}}$ the $\mathbb{Z}[\mathrm{Gal}(K_n^{\mathfrak{r}}/K)]$-submodule of $Y_{n,\mathfrak{t}}$ generated by the relations

1. $G_{\mathfrak{r}/\mathfrak{s}}$ acts trivially on the indeterminate $x_{n,\mathfrak{s}}$.

2. If $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$ then $N_{\mathfrak{q}} x_{n,\mathfrak{q}\mathfrak{s}} = (1 - ((K_n^{\mathfrak{s}}/K), \mathfrak{q})^{-1}) x_{n,\mathfrak{s}}$

We define the **(n,𝔯)-Euler module** to be the $\mathrm{Gal}(K_n^{\mathfrak{t}}/K)$-module

$$X_{n,\mathfrak{r}} = {}^{Y_{n,\mathfrak{r}}}\!/\!_{Z_{n,\mathfrak{r}}}$$

**Definition 4.1.6.** Consider the directed set $I = \mathbb{N} \times \mathcal{R}$ with partial order $\leq$ given by the usual ordering on $\mathbb{N}$ and ideal divisibility on $\mathcal{R}^{\mathfrak{e}}$. For every $(n, \mathfrak{s}) \leq (m, \mathfrak{r})$ we define a homomorphism of Euler modules

$$\begin{aligned}\varphi_{(n,\mathfrak{s})}^{(m,\mathfrak{r})} : X_{n,\mathfrak{s}} &\to X_{m,\mathfrak{r}} \\ x_{n,\mathfrak{t}} &\mapsto \mathbf{N}_{K_m^{\mathfrak{r}}/K_n^{\mathfrak{r}}}\, x_{n,\mathfrak{t}}\end{aligned}$$

for $\mathfrak{t} \mid \mathfrak{s}$. Clearly, $\varphi_{(n,\mathfrak{s})}^{(n,\mathfrak{s})} = \mathrm{id}$ and $\varphi_{(l,\mathfrak{r})}^{(n,\mathfrak{t})} = \varphi_{(m,\mathfrak{s})}^{(n,\mathfrak{t})} \circ \varphi_{(l,\mathfrak{r})}^{(m,\mathfrak{s})}$ for all $(l, \mathfrak{r}) \leq (m, \mathfrak{s}) \leq (n, \mathfrak{t})$ and so the $X_{n,\mathfrak{r}}$ form a directed system with respect to the connecting homomorphisms $\varphi$. We define the **universal Euler system** with respect to the fixed $\mathfrak{p}$-system to be

$$\mathcal{X} = \varinjlim_{(n,\mathfrak{t}) \in I} X_{n,\mathfrak{r}}$$

with the direct limit taken with respect to the $\varphi$.

**Definition 4.1.7.** We define an **Euler system** of $K$ to be a $G_K$-equivariant map

$$\boldsymbol{\eta} : \varinjlim_{(n,\mathfrak{r}) \in I} X_{n,\mathfrak{r}} \to \bigcup_{n,\mathfrak{r}} K_n^{\mathfrak{r}\,\times}$$

such that $\boldsymbol{\eta}([X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}])$ is a global unit for all $n \in \mathbb{N}_{\geq 0}$ and $\mathfrak{t} \in \mathcal{R}^{\mathfrak{e}}$.

**Proposition 4.1.8.** *Specifying an Euler system* $\boldsymbol{\eta} : \varinjlim_{(n,\mathfrak{r}) \in I} X_{n,\mathfrak{r}} \to \bigcup_{n,\mathfrak{r}} K_n^{\mathfrak{r}\,\times}$ *is equivalent to specifying a collection of global units*

$$\{\, \boldsymbol{\eta}(n, \mathfrak{r}) \in K_n^{\mathfrak{r}\,\times} \mid \mathbb{N}_{\geq 1}, \mathfrak{r} \in \mathcal{R} \,\}$$

*such that*

*1.* $\mathbf{N}_{K_n^{\mathfrak{q}\mathfrak{r}}/K_n^{\mathfrak{r}}}\, \boldsymbol{\eta}(n, \mathfrak{q}\mathfrak{t}) = \boldsymbol{\eta}(n, \mathfrak{r})^{1 - ((K_n^{\mathfrak{r}}/K), \mathfrak{q})^{-1}}$

*2.* $\mathbf{N}_{K^{\mathfrak{r}}_{n+1}/K^{\mathfrak{r}}_n}\,\boldsymbol{\eta}(n+1,\mathfrak{r}) = \boldsymbol{\eta}(n,\mathfrak{r})$

*Proof.* First suppose that we are given an Euler system $\boldsymbol{\eta} : \varinjlim_{(n,\mathfrak{r})\in I} X_{n,\mathfrak{r}} \to \bigcup_{n,\mathfrak{r}} K^{\mathfrak{r}\,\times}_n$. Let $[X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}]$ be an equivalence class in the universal Euler system. It is clear by the definition of $\boldsymbol{\eta}$ that the image of this equivalence class is a global unit in $K^{\mathfrak{r}}_n$ so it suffices to demonstrate the norm-compatibility relations. By definition of the direct limit, we have that $x_{n,\mathfrak{r}} \sim \varphi^{(n+1,\mathfrak{r})}_{(n,\mathfrak{r})}(x_{n+1,\mathfrak{r}})$ and so

$$[X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}] = [X_{n+1,\mathfrak{r}}, \mathbf{N}_{K^{\mathfrak{r}}_{n+1}/K^{\mathfrak{r}}_n}\, x_{n_1,\mathfrak{r}}]$$

Appealing to the $G_K$-equivariance of $\boldsymbol{\eta}$ we then have that

$$\begin{aligned}\boldsymbol{\eta}(n,\mathfrak{r}) = \boldsymbol{\eta}([X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}]) &= \boldsymbol{\eta}([X_{n+1,\mathfrak{r}}, \mathbf{N}_{K^{\mathfrak{r}}_{n+1}/K^{\mathfrak{r}}_n}\, x_{n_1,\mathfrak{r}}]) \\ &= \mathbf{N}_{K^{\mathfrak{r}}_{n+1}/K^{\mathfrak{r}}_n}\,\boldsymbol{\eta}([X_{n+1,\mathfrak{r}}, x_{n,\mathfrak{r}}]) \\ &= \mathbf{N}_{K^{\mathfrak{r}}_{n+1}/K^{\mathfrak{r}}_n}\,\boldsymbol{\eta}(n+1,\mathfrak{r})\end{aligned}$$

Now suppose that $\mathfrak{q} \in \mathcal{R}^{\mathfrak{e}}$ is a prime ideal that does not divide $\mathfrak{r} \in \mathcal{R}$. $G_K$-equivariance again shows that

$$\begin{aligned}\mathbf{N}_{K^{\mathfrak{qr}}_n/K^{\mathfrak{r}}_n}\,\boldsymbol{\eta}(n,\mathfrak{qr}) = \mathbf{N}_{K^{\mathfrak{qr}}_n/K^{\mathfrak{r}}_n}\,\boldsymbol{\eta}([X_{n,\mathfrak{qr}}, x_{n,\mathfrak{qr}}]) &= \boldsymbol{\eta}([X_{n,\mathfrak{qr}}, \mathbf{N}_{K^{\mathfrak{qr}}_n/K^{\mathfrak{r}}_n}\, x_{n,\mathfrak{qr}}]) \\ &= \boldsymbol{\eta}([X_{n,\mathfrak{qr}}, N_{\mathfrak{q}} x_{n,\mathfrak{qr}}]) \\ &= \boldsymbol{\eta}([X_{n,\mathfrak{qr}}, (1-((K^{\mathfrak{r}}_n/K),\mathfrak{q})^{-1}) x_{n,\mathfrak{r}}]) \\ &= (1-((K^{\mathfrak{r}}_n/K),\mathfrak{q})^{-1})\boldsymbol{\eta}([X_{n,\mathfrak{qr}}, x_{n,\mathfrak{r}}]) \\ &= \boldsymbol{\eta}(n,\mathfrak{r})^{1-((K^{\mathfrak{r}}_n/K),\mathfrak{q})^{-1}}\end{aligned}$$

Conversely, suppose that we are given a collection of global units

$$\{\, \boldsymbol{\eta}(n,\mathfrak{r}) \in K^{\mathfrak{r}\,\times}_n \mid \mathbb{N}_{\geq 1}, \mathfrak{r} \in \mathcal{R} \,\}$$

satisfying the above conditions. Define a map

$$\boldsymbol{\eta} : \varinjlim_{(n,\mathfrak{r})\in I} X_{n,\mathfrak{r}} \to \bigcup_{n,\mathfrak{r}} K^{\mathfrak{r}\,\times}_n$$

by $\boldsymbol{\eta}([X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}]) = \boldsymbol{\eta}(n,\mathfrak{r})$ and then extending linearly. By construction, $\boldsymbol{\eta}([X_{n,\mathfrak{r}}, x_{n,\mathfrak{r}}])$ is a global unit for all $n \in \mathbb{N}_{\geq 0}$ and $\mathfrak{r} \in \mathcal{R}^{\mathfrak{e}}$ and is $G_K$-equivariant by linearity. This map is clearly compatible with the structure of the universal Euler system and so $\boldsymbol{\eta}$ is an Euler system. □

*Remark.* From now on we shall suppress the use of the equivalence class in the argument of the Euler system and simply write $\boldsymbol{\eta}(x_{n,\mathfrak{r}})$ or $\boldsymbol{\eta}(n,\mathfrak{r})$.

We will now show that our usual notions of the cyclotomic and elliptic units are subsumed by the definition of an Euler system.

**Example 4.1.9.** Let $K = \mathbb{Q}, \mathfrak{e} = 1$ and $(p) = \mathfrak{p}$ for some rational prime $p$. For every integer $m > 1$, let $\zeta_m$ be a primitive $m^{th}$ root of unity in $\overline{\mathbb{Q}}$. We define a $p$-system on $\mathbb{Q}$ by setting $K_n = \mathbb{Q}(\zeta_{p^n})$ and for every integer $r \in \mathcal{R}^1$ we set $K^r_n = K_n(\zeta_r) = K(\zeta_{p^n r})$. By the elementary theory of cyclotomic fields, this is indeed a $p$-system since $\mathrm{Gal}(K^r_n/K) = (\mathbb{Z}/p^n r)^\times$ and for every rational prime $q \neq l$ we have that the extension $K^{qr}_n/K^r_n$ is totally ramified above primes of $K^r_n$ lying above $q$ and unramified everywhere else.

Now define $\boldsymbol{\eta}(n,r) = \zeta_{p^n r} - 1$. This is indeed guaranteed to be an Euler system by the usual norm-compatibility relations for cyclotomic units.

**Example 4.1.10.** Let $K$ be an imaginary quadratic number field and $E$ an elliptic curve defined over $K$ with complex multiplication by $\mathcal{O}_K$. Let $\mathfrak{e} = 6\mathfrak{a}\mathfrak{f}$ where $\mathfrak{a} \lhd \mathcal{O}_K$ is an auxiliary ideal prime to $6\mathfrak{f}$ where $\mathfrak{f}$ is the conductor of the Hecke character $\Psi_E$ attached to $E$. We define a $\mathfrak{p}$-system on $K$ by setting $K_n = K(E[\mathfrak{p}^n])$ and for all $\mathfrak{r} \in \mathcal{R}$ we set $K_n^{\mathfrak{r}} = K_n(E[\mathfrak{r}]) = K_n(E[\mathfrak{p}^n\mathfrak{r}])$. This is guaranteed to be a $\mathfrak{p}$-system by Theorem A.7.9. Let $\Lambda$ be the lattice associated to $E$ and $\Omega \in \mathbb{C}^\times$ such that $\Lambda = \Omega\mathcal{O}_K$. Then by Proposition 3.4.8

$$\boldsymbol{\eta}(n, \mathfrak{r}) = \Phi_{\Lambda,\mathfrak{a}}(\psi_E(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)$$

is an Euler system of $K$ where $\Phi$ is the $\Phi$-function of $E$.

*Remark.* We note that by a result of Yin (see [Yin00]), our theory will be proper only to $\mathbb{Q}$ and imaginary quadratic number fields. Indeed, we shall soon restrict $\mathcal{R}$ to ideals $\mathfrak{r}$ such that every prime dividing $\mathfrak{r}$ splits completley in $K_n$. Yin showed that only $\mathbb{Q}$ and imaginary quadratic number fields possess abelian extensions $K_n^{\mathfrak{q}}/K_n$ for such a prime $\mathfrak{q}$ such that

1. $K_n^{\mathfrak{q}}/K$ is abelian.
2. $[K_n^{\mathfrak{q}} : K_n] = \mathbf{N}\mathfrak{q} - 1$.
3. $K_n^{\mathfrak{q}}/K_n$ is totally ramified above primes lying over $\mathfrak{q}$ and unramified everywhere else.

## 4.2 Properties

*Assumptions.* We continue to use the notations and assumptions from the previous section. Furthermore, if $n \in \mathbb{N}_{\geq 1}$, and $M$ is a power of $p$, we define $\mathcal{R}_{n,M} \subseteq \mathcal{R}$ to be those ideals $\mathfrak{r}$ such that for every prime $\mathfrak{q}|\mathfrak{r}$ we have that $\mathfrak{q}$ splits completely in $K_n/K$ and $N\mathfrak{q} - 1 \equiv 0 \pmod{M}$.

**Proposition 4.2.1.** *Let $\mathfrak{r} \in \mathcal{R}_{n,M}$ be an ideal. Then $X_{n,\mathfrak{r}}$ is a free $\mathbb{Z}$-module of rank $[K_n^{\mathfrak{r}} : K]$. In particular, $X_{n,\mathfrak{r}}$ has no $\mathbb{Z}$-torsion.*

*Proof.* We may assume, without loss of generality, that $G_{\mathfrak{q}}$ is not trivial for all primes $\mathfrak{q} \mid \mathfrak{r}$. Indeed given such a $\mathfrak{q}$ with $G_{\mathfrak{q}}$ trivial, let $\mathfrak{r}' = \mathfrak{r}/\mathfrak{q}$. Then $K_n^{\mathfrak{r}'} = K_n^{\mathfrak{r}}$ and $X_{n,\mathfrak{r}'} = X_{n,\mathfrak{r}}$.

Now for every prime $\mathfrak{q} \mid \mathfrak{r}$ and divisor $\mathfrak{s} \mid \mathfrak{r}$ define

$$B_1 = \mathrm{Gal}(K_n/K)$$
$$B_{\mathfrak{q}} = G_{\mathfrak{q}} - \{1\}$$
$$B_{\mathfrak{s}} = \prod_{\mathfrak{q}|\mathfrak{s}} B_{\mathfrak{q}}$$

We claim that $B = \bigcup_{\mathfrak{s}|\mathfrak{r}} B_{\mathfrak{s}} x_{n,\mathfrak{s}}$ is a $\mathbb{Z}$-basis for $X_{n,\mathfrak{t}}$. To this end, we first observe that $B_{\mathfrak{q}} \cup \{N_{\mathfrak{q}}\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[G_{\mathfrak{q}}]$. Indeed, $\mathbb{Z}[G_{\mathfrak{q}}]$ has rank $|G_{\mathfrak{q}}|$ as a $\mathbb{Z}$-module and $|B_{\mathfrak{q}} \cup \{N_{\mathfrak{q}}\}| = |G_{\mathfrak{q}}|$ also. Furthermore, the elements of $B_{\mathfrak{q}} \cup \{N_{\mathfrak{q}}\}$ are $\mathbb{Z}$-linearly independent as they are a collection of field automorphisms contained in $G_K$. From this it follows that for all $\mathfrak{s} \mid \mathfrak{r}$

$$\prod_{\mathfrak{q}|\mathfrak{s}} B_{\mathfrak{q}} \cup \{N_{\mathfrak{q}}\}$$

is a $\mathbb{Z}$-basis for $\mathbb{Z}[G_{\mathfrak{s}}]$. By induction on the number of primes dividing $\mathfrak{r}$, we then see that $X_{n,\mathfrak{r}}$ is finitely generated over $\mathbb{Z}$ by $B$. Indeed, if $\mathfrak{r} = 1$ there is nothing to prove so assume that $\mathfrak{q}$ divides $\mathfrak{r}$ and write $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$. By the induction hypothesis, $X_{n,\mathfrak{s}}$ is finitely generated over $\mathbb{Z}$ by $\bigcup_{\mathfrak{t}|\mathfrak{s}} B_\mathfrak{t} x_{n,\mathfrak{t}}$. Since $N_\mathfrak{q} x_{n,\mathfrak{q}} = 1 - ((K_n/K),\mathfrak{q})^{-1} x_{n,1}$, it follows that $X_{n,\mathfrak{q}}$ is finitely generated over $\mathbb{Z}$ by $\bigcup_{\mathfrak{s}|\mathfrak{q}} B_\mathfrak{s} x_{n,\mathfrak{s}}$ and so the claim is proven.

To see that $X_{n,\mathfrak{r}}$ is infact a free $\mathbb{Z}$-module we first observe that

$$|B| \leq \sum_{\mathfrak{s}|\mathfrak{r}} |B_\mathfrak{s}| = \prod_{\mathfrak{q}|\mathfrak{r}} |B_\mathfrak{q} + 1| = \prod_{\mathfrak{q}|\mathfrak{r}} |G_\mathfrak{q}| = [K_n^\mathfrak{r} : K]$$

Conversely, we claim that $X_{n,\mathfrak{r}}$ has rank at least $[K_n^\mathfrak{r} : K]$ as a $\mathbb{Z}$-module. The Proposition would then follow immediately.

Consider the homomorphism

$$\begin{aligned} \varphi : Y_{n,\mathfrak{r}} &\to \mathbb{Z}[\mathrm{Gal}(K_n^\mathfrak{r}/K)] \\ x_{n,\mathfrak{s}} &\mapsto \prod_{\mathfrak{q}|(\mathfrak{r}/\mathfrak{s})} N_\mathfrak{q} \prod_{\mathfrak{q}|\mathfrak{s}} \left( |G_\mathfrak{q}| + (1 - ((K_n^\mathfrak{q}/K),\mathfrak{q})^{-1} - |G_\mathfrak{q}|) \frac{N_\mathfrak{q}}{|G_\mathfrak{q}|} \right) \end{aligned}$$

for $\mathfrak{s} \mid \mathfrak{r}$ which is trivial on $Z_{n,\mathfrak{r}}$. This then induces an homomorphism

$$\Phi : X_{n,\mathfrak{t}} \otimes_\mathbb{Z} \mathbb{Q} \to \mathbb{Q}[\mathrm{Gal}(K_n^\mathfrak{r}/K)]$$

It can be shown using the theory of Galois characters that $\Phi$ is surjective (see the proof of [Rub14, Proposition 3.1]) so that

$$\mathrm{rank}_\mathbb{Z}(X_{n,\mathfrak{r}}) = \dim_\mathbb{Q}(X_{n,\mathfrak{r}} \otimes_\mathbb{Z} \mathbb{Q}) \geq [K_n^\mathfrak{r} : K] \geq |B|$$

as desired. □

**Proposition 4.2.2.** *Let $\mathfrak{r} \in \mathcal{R}_{n,M}$ be an ideal. Then $D_\mathfrak{r} x_{n,\mathfrak{r}} \in (X_{n,\mathfrak{r}}/MX_{n,\mathfrak{r}})^{G_\mathfrak{r}}$.*

*Proof.* Given a prime $\mathfrak{q} \mid \mathfrak{r}$, let $\sigma_\mathfrak{q}$ be a generator of $G_\mathfrak{q}$. Since the $\sigma_\mathfrak{q}$ generate $G_\mathfrak{r}$, it suffices to show that for all $\mathfrak{q}$ we have $(\sigma_\mathfrak{q} - 1)D_\mathfrak{r} x_{n,\mathfrak{r}} \in MX_{n,\mathfrak{r}}$. We shall prove this by induction on the number of primes dividing $\mathfrak{r}$. If $\mathfrak{r} = 1$ then the claim is trivial. Now suppose that $\mathfrak{r} = \mathfrak{qs}$ for some prime $\mathfrak{q} \in R_{n,M}$. Then by the Telescoping Identity 4.1.4 we have that

$$\begin{aligned} (\sigma_\mathfrak{q} - 1)D_\mathfrak{r} x_{n,\mathfrak{r}} &= (\sigma_\mathfrak{q} - 1)D_\mathfrak{q} D_\mathfrak{s} x_{n,\mathfrak{r}} \\ &= (\mathbf{N}\mathfrak{q} - 1)D_\mathfrak{s} x_{n,\mathfrak{r}} - N_\mathfrak{q} D_\mathfrak{s} x_{n,\mathfrak{s}} \\ &= (\mathbf{N}\mathfrak{q} - 1)D_\mathfrak{s} x_{n,\mathfrak{r}} - (1 - ((K_n^\mathfrak{s}/K),\mathfrak{q})^{-1})D_\mathfrak{s} x_{n,\mathfrak{s}} \end{aligned}$$

Now, $((K_n^\mathfrak{s}/K),\mathfrak{q})^{-1} \in G_\mathfrak{s}$ whence $(1 - ((K_n^\mathfrak{s}/K),\mathfrak{q})^{-1})D_\mathfrak{s} x_{n,\mathfrak{s}} \in MX_{n,\mathfrak{s}}$ by the induction hypothesis. Moreover, $\mathbf{N}\mathfrak{q} - 1 \equiv 0 \pmod{M}$ and so it follows that

$$(\sigma_\mathfrak{q} - 1)D_\mathfrak{r} x_{n,\mathfrak{r}} \equiv 0 \pmod{MX_{n,\mathfrak{r}}}$$

as required. □

The following congruence relation was part of Kolyvagin's original definition of an Euler system. In the following proof, Rubin showed that it in fact follows from the axioms that we have given above.

**Proposition 4.2.3.** *Let $\boldsymbol{\eta}$ be an Euler system and $\mathfrak{q} \in \mathcal{R}$ a prime. Suppose that $k$ is the largest power of $p$ dividing $\mathbf{N}\mathfrak{q} - 1$ so that $\mathbf{N}\mathfrak{q} - 1 = dp^k$ such that $(d,p) = 1$. Given $n \in \mathbb{N}_{\geq 1}$ and $\mathfrak{r} \in \mathcal{R}$ we have*

$$\boldsymbol{\eta}(n,\mathfrak{qr})^d \equiv \boldsymbol{\eta}(n,\mathfrak{r})^{d((K_n^\mathfrak{r}/K),\mathfrak{q})^{-1}} \pmod{\mathfrak{Q}}$$

*for all primes $\mathfrak{Q}$ lying over $\mathfrak{q}$.*

*Proof.* Suppose that $m \geq n$ and write $G = \mathrm{Gal}(K_m^{\mathfrak{qt}}/K_n^{\mathfrak{qt}})$. Given a prime $\mathfrak{Q}$ of $K_m^{\mathfrak{qt}}$ lying over $\mathfrak{q}$, let $\mathcal{D}_{\mathfrak{q}}$ be the decomposition group of $\mathfrak{q}$ in $G$. In other words, $\mathcal{D}_{\mathfrak{q}}$ is the intersection of $G$ with the decomposition group of $\mathfrak{q}$ in $K_m^{\mathfrak{qt}}$. Fix a set $\mathcal{D}'$ of representatives for the factor group $G/\mathcal{D}_{\mathfrak{q}}$ and let $N_{\mathcal{D}_{\mathfrak{q}}} = \sum_{\gamma \in \mathcal{D}_{\mathfrak{q}}} \gamma$ and $N_{\mathcal{D}'} = \sum_{\gamma \in H'} \gamma$. By construction we clearly have that $N_{\mathcal{D}_{\mathfrak{q}}} N_{\mathcal{D}'} = \sum_{\gamma \in G} \gamma$.

Now, every prime lying above $\mathfrak{q}$ in $K_m^{\mathfrak{r}}$ ramifies totally in $K_m^{\mathfrak{qr}}$ and so the Galois group $G$ is equal to the decomposition group relative to $\mathfrak{Q}$ and also the inertia group relative to $\mathfrak{Q}$. Reducing the left-hand side of the first norm-compatibility relation, we then have that

$$\mathbf{N}_{K_m^{\mathfrak{qr}}/K_n^{\mathfrak{qr}}} \boldsymbol{\eta}(m, \mathfrak{qr}) = \boldsymbol{\eta}(m, \mathfrak{qr})^{\mathbf{N}\mathfrak{q}-1} \pmod{\mathfrak{Q}}$$

On the other hand, we claim that

$$\boldsymbol{\eta}(m, \mathfrak{r})^{1-((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}} \equiv (\boldsymbol{\eta}(m, \mathfrak{r})^{((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}})^{\mathbf{N}\mathfrak{q}-1}$$

Indeed, this follows immediately by starting with the definition of the Artin symbol, dividing through by $\boldsymbol{\eta}(m, \mathfrak{r})$ then applying the inverse of the Artin symbol.

Let $f$ be the inertial degree of $\mathfrak{q}$ in $K_n^{\mathfrak{r}}/K$. Since the Artin symbol $((K_n^{\mathfrak{t}}/K), \mathfrak{q})$ is a generator of $\mathcal{D}_{\mathfrak{q}}$ we have the following reduction relation

$$N_{\mathcal{D}_{\mathfrak{q}}} = \sum_{i=0}^{|\mathcal{D}_{\mathfrak{q}}|-1} (\mathbf{N}\mathfrak{q}^f)^i \pmod{\mathfrak{Q}}$$

If we denote this reduction by $r$ then reducing the second norm-compatibility relation modulo $\mathfrak{Q}$ yields

$$\begin{aligned} \boldsymbol{\eta}(n, \mathfrak{r}) &= \boldsymbol{\eta}(m, \mathfrak{r})^{N_{\mathcal{D}_{\mathfrak{q}}} N_{\mathcal{D}'}} \equiv \boldsymbol{\eta}(m, \mathfrak{r})^{r N_{\mathcal{D}'}} \pmod{\mathfrak{Q}} \\ \boldsymbol{\eta}(n, \mathfrak{qr}) &= \boldsymbol{\eta}(m, \mathfrak{qr})^{N_{\mathcal{D}_{\mathfrak{q}}} N_{\mathcal{D}'}} \equiv \boldsymbol{\eta}(m, \mathfrak{qr})^{r N_{\mathcal{D}'}} \pmod{\mathfrak{Q}} \end{aligned}$$

It is immediate that $r \equiv |\mathcal{D}_{\mathfrak{q}}| \pmod{\mathbf{N}\mathfrak{q} - 1}$. Letting $m \to \infty$, $\mathcal{D}_{\mathfrak{q}}$ becomes arbitrarily large so we can always find an $m$ such that $p^k | r$. Fix such an $m \geq n$ and write $r = p^k s$ so that

$$\begin{aligned} \boldsymbol{\eta}(n, \mathfrak{qr})^d &\equiv (\boldsymbol{\eta}(m, \mathfrak{qr}))^{N_{\mathcal{D}'} d p^k s} \pmod{\mathfrak{Q}} \\ &= (\boldsymbol{\eta}(m, \mathfrak{qr})^{(\mathbf{N}\mathfrak{q}-1)})^{s N_{\mathcal{D}'}} \\ &= (\boldsymbol{\eta}(m, \mathfrak{r})^{((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}})^{(\mathbf{N}\mathfrak{q}-1) s N_{\mathcal{D}'}} \\ &= (\boldsymbol{\eta}(m, \mathfrak{r})^{N_{\mathcal{D}'}})^{s d ((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}} \\ &= \boldsymbol{\eta}(n, \mathfrak{r})^{d((K_n^{\mathfrak{t}}/K),\mathfrak{q})^{-1}} \end{aligned}$$

□

## 4.3 Constructing Principal Ideals of $\mathfrak{p}$-systems

Our next task shall be to employ Euler systems in order to construct certain principal ideals in our $\mathfrak{p}$-systems. In the next section, we will then go onto use these ideals as relations in order to place bounds - and in some cases annihilate - certain parts of the ideal class group of $K_1$.

*Assumptions.* We continue to use the notations and assumptions from the previous section. Furthermore, we assume that the base field of our $\mathfrak{p}$-system has class number 1[3]. Finally, fix an integer $n \geq 1$ and an ideal

[3] Recall that the only interesting cases are when the base field is $\mathbb{Q}$ or an imaginary quadratic field $K$. The former clearly has class

$\mathfrak{r} \in \mathcal{R}_{M,\mathfrak{r}}$.

**Definition 4.3.1.** Let $\boldsymbol{\eta}$ be an Euler system. We define a map

$$\begin{aligned} c_{\boldsymbol{\eta},n,\mathfrak{r}} : G_{\mathfrak{r}} &\to K_n(\mathfrak{r})^{\times} \\ \sigma &\mapsto \boldsymbol{\eta}\left(\frac{(\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) \end{aligned}$$

which is well-defined by Proposition 4.2.2.

**Proposition 4.3.2.** *Let $\boldsymbol{\eta}$ be an Euler system. Then $c_{\boldsymbol{\eta},n,\mathfrak{r}}$ is a 1-cocycle.*

*Proof.* To ease notation, write $c = c_{\boldsymbol{\eta},n,\mathfrak{r}}$. By definition of a 1-cocycle, we are required to show that for all $\sigma, \tau \in G_{\mathfrak{r}}$ we have $c(\sigma\tau) = c(\sigma) + c(\tau)^{\sigma}$. Note that by Proposition 4.2.1, $X_{n,\mathfrak{r}}$ has no $\mathbb{Z}$-torsion and so, in particular, we have canonical $M^{th}$-roots of $\boldsymbol{\eta}((\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}})$. It then follows that,

$$\begin{aligned} c(\sigma\tau) &= \boldsymbol{\eta}\left(\frac{(\sigma\tau-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) \\ &= \boldsymbol{\eta}\left(\frac{(\sigma\tau+\sigma-\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) \\ &= \boldsymbol{\eta}\left(\frac{(\tau-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right)^{\sigma} + \boldsymbol{\eta}\left(\frac{(\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) \\ &= c(\sigma) + c(\tau)^{\sigma} \end{aligned}$$

as claimed. □

**Corollary 4.3.3.** *Let $\boldsymbol{\eta}$ be an Euler system. Then there exists a $\beta_{\mathfrak{r}} \in K_n^{\mathfrak{r}\,\times}$ unique modulo $K_n^{\times}$ such that*

$$\frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{M}} \in K_n^{\times}$$

*Proof.* Since $G_{\mathfrak{r}}$ is independent of $n$ we observe that, by Hilbert's Theorem 90, $H^1(G_{\mathfrak{r}}, K_n^{\mathfrak{r}})$ is trivial. In particular, the 1-cocycle $c = c_{\boldsymbol{\eta},n,\mathfrak{r}}$ defined above is also a 1-coboundary. We can thus find $\beta_{\mathfrak{r}} \in K_n^{\mathfrak{r}\,\times}$ such that $c(\sigma) = \beta_{\mathfrak{r}}^{\sigma-1}$ for all $\sigma \in G_{\mathfrak{r}}$. We first claim that such a $\beta_{\mathfrak{r}}$ is unique modulo $K_n^{\times}$. Indeed, let $\beta'_{\mathfrak{r}}$ be another element of $K_n^{\mathfrak{r}}$ such that $c(\sigma) = \beta_{\mathfrak{r}}'^{\sigma-1}$ for all $\sigma \in G_{\mathfrak{r}}$. Then $(\beta'_{\mathfrak{r}}/\beta_{\mathfrak{r}})^{\sigma} = \beta'_{\mathfrak{r}}/\beta_{\mathfrak{r}}$ whence $\beta'_{\mathfrak{r}}/\beta_{\mathfrak{r}} \in K_n^{\times}$ and so $\beta'_{\mathfrak{r}} \equiv \beta_{\mathfrak{r}} \pmod{K_n^{\times}}$. We now claim that such a $\beta_{\mathfrak{r}}$ satisfies the assertion of the Corollary.

To this end, fix an automorphism $\sigma \in G_{\mathfrak{r}}$. Then

$$\sigma\left(\frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{M}}\right) = \frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{\sigma D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{\sigma M}} = \frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{\sigma D_{\mathfrak{r}}}}{(\beta_{\mathfrak{r}}\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{(\sigma-1)D_{\mathfrak{r}}/M})^{M}} = \frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{M}}$$

as desired. □

**Definition 4.3.4.** Let $\boldsymbol{\eta}$ be an Euler system. We define a map

$$\begin{aligned} \kappa_{n,M} : \mathcal{R}_{n,M} &\to K_n^{\times}/(K_n^{\times})^{M} \\ \mathfrak{r} &\mapsto \left[\frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{M}}\right] \end{aligned}$$

where $\beta_{\mathfrak{r}}$ is the element of $K_n^{\mathfrak{r}\,\times}$ as provided by the previous Corollary.

Our motivation in defining such a map $\kappa_{n,M}(\mathfrak{r})$ is that we will be able to give a simple description for the ideal that it generates in terms of the primes dividing $\mathfrak{r}$. In particular, we will construct a map $\phi_{\mathfrak{q}}$ which will describe

number 1 and we may assume the latter has class number 1 as is the running theme throughout this essay.

the $\mathfrak{q}$-part of the ideal generated by $\kappa_{n,M}(\mathfrak{r})$ when $\mathfrak{q}$ divides $\mathfrak{r}$. In order to formalise this, we first define some useful notations.

To ease the exposition, we denote $L = K_n$. We let $I_L$ be the group of fractional ideals of $L$ written additively as follows

$$I_L = \bigoplus_{\mathfrak{Q} \in M_L^{\nmid\infty}} \mathbb{Z}\mathfrak{Q}$$

Furthermore given a finite prime $\mathfrak{q}$ of $K$, we let $I^{\mathfrak{q}} = I_L^{\mathfrak{q}}$ be similarly defined, with the direct sum ranging over the finite primes $\mathfrak{Q}$ of $L$ lying above $\mathfrak{q}$. If $x \in L^\times$ let $(x)_\mathfrak{q}$ denote the projection of $(x)$ to $I_\mathfrak{q}$, $[x]$ the projection of $(x)$ to $I_L/MI_L$ and $[x]_\mathfrak{q}$ the projection of $(x)$ to $I^\mathfrak{q}/MI^\mathfrak{q}$.

**Proposition 4.3.5.** *Let $\mathfrak{q} \in \mathcal{R}_{n,M}$ be a prime of $K$ and denote $\mathfrak{O} = \mathcal{O}_L/\mathfrak{q}\mathcal{O}_L$. Then there exists a* Gal$(L/K)$-*equivariant homomorphism*

$$\phi_\mathfrak{q} : {L^\times}\big/{(L^\times)^M} \to {I^\mathfrak{q}}\big/{MI^\mathfrak{q}}$$

*which induces an isomorphism*

$$\phi_\mathfrak{q} : {\mathfrak{O}^\times}\big/{(\mathfrak{O}^\times)^M} \to {I^\mathfrak{q}}\big/{MI^\mathfrak{q}}$$

*Proof.* Let $\mathfrak{Q}$ be a finite prime of $L$ lying above $\mathfrak{q}$ and $\overline{\mathfrak{Q}}$ a prime of $\overline{K}$ lying above $\mathfrak{Q}$. We recall that $\mathfrak{q}$ splits completely in $L/K$ and that $\mathfrak{Q}$ totally ramifies in $L^\mathfrak{q}/L$. Denote by $\sigma_\mathfrak{Q}$ a lift of the generator $\sigma_\mathfrak{q}$ of $G_\mathfrak{q}$ to $G_K$ so that $\sigma_\mathfrak{Q}$ is contained in the inertia group of $\overline{\mathfrak{Q}}$.

Our first task is to construct a homomorphism

$$\phi_\mathfrak{Q} : {L_\mathfrak{Q}^\times}\big/{(L_\mathfrak{Q}^\times)^M} \to {\mathbb{Z}}\big/{M\mathbb{Z}}$$

To this end, define an isomorphism

$$\begin{aligned} \psi : {\mathbb{Z}}\big/{M\mathbb{Z}} &\to \boldsymbol{\mu}_M \\ [a] &\mapsto (\pi^{a/M})^{1-\sigma_\mathfrak{Q}} \end{aligned}$$

where we understand $a$ to be the least positive representative of $[a]$ and $\pi$ is a generator of $\mathfrak{q}$. Now choose a Frobenius element $\tau$ in the Artin symbol $((\overline{L}/L), \mathfrak{Q})$. Recall that $\tau$ is an element of the the decomposition group of $\mathfrak{Q}$ in $\overline{L}/L$ which is isomorphic to the Galois group of the extension of local fields $\overline{L_\mathfrak{Q}}/L_\mathfrak{Q}$. Furthermore, any such $\tau$ is conjugate to the other elements of the Artin symbol. We define

$$\phi_\mathfrak{Q} : L_\mathfrak{Q}^\times \to {\mathbb{Z}}\big/{M\mathbb{Z}}$$

to be the image of $\tau$ under the composition

$$\begin{aligned} G_{L_\mathfrak{Q}} &\to \operatorname{Hom}(L_\mathfrak{Q}^\times, \boldsymbol{\mu}) \to \operatorname{Hom}(L_\mathfrak{Q}^\times, \mathbb{Z}/M\mathbb{Z}) \\ \sigma &\mapsto \left(x \mapsto x^{\frac{\sigma-1}{M}}\right) \end{aligned}$$

where the second map of hom-sets is the one induced by the isomorphism $\psi$. This is well-defined as it is clearly independent of the choice of Frobenius element $\tau$. Moreover, $\phi_\mathfrak{Q}$ is trivial on $(L_\mathfrak{Q}^\times)^M$ so $\phi_\mathfrak{Q}$ descends to a homomorphism

$$\phi_\mathfrak{Q} : {L_\mathfrak{Q}^\times}\big/{(L_\mathfrak{Q}^\times)^M} \to {\mathbb{Z}}\big/{M\mathbb{Z}}$$

We can give an explicit description for this map as follows. Let $\alpha \in L_{\mathfrak{Q}}^{\times}$ and let $\overline{\mathfrak{Q}}$ denote the maximal ideal of the ring of integers of $L_{\mathfrak{Q}}$. Since $\sigma_{\mathfrak{Q}}$ reduces to the trivial automorphism modulo $\overline{\mathfrak{Q}}$ we have that

$$(\alpha^{1/M})^{((\overline{L}/L),\mathfrak{Q})-1} \equiv (\beta^{1/M})^{1-\sigma_{\mathfrak{Q}}} \pmod{\overline{\mathfrak{Q}}} \tag{4.1}$$

for some $\beta \in \overline{L_{\mathfrak{Q}}}^{\times}$. Let $a = v_{\mathfrak{Q}}(\beta)$. Then

$$(\alpha^{1/M})^{((\overline{L}/L),\mathfrak{Q})-1} = (\pi^{a/M})^{1-\sigma_{\mathfrak{Q}}} \tag{4.2}$$

and so $\phi_{\mathfrak{Q}}(\alpha) = a$. We next use this to define a map

$$\begin{aligned} \phi_{\mathfrak{q}} : {}^{L^{\times}}\!\!\diagup_{(L^{\times})^M} &\to {}^{I^{\mathfrak{q}}}\!\!\diagup_{MI^{\mathfrak{q}}} \\ \alpha &\mapsto \sum_{\mathfrak{Q}/\mathfrak{q}} \phi_{\mathfrak{Q}}(\alpha)\mathfrak{Q} \end{aligned}$$

Finally, this then induces a well-defined isomorphism

$$\phi_{\mathfrak{q}} : {}^{\mathfrak{O}^{\times}}\!\!\diagup_{(\mathfrak{O}^{\times})^M} \to {}^{I^{\mathfrak{q}}}\!\!\diagup_{MI^{\mathfrak{q}}}$$

Gal$(L/K)$-equivariance then follows immediately from the definition upon recalling that Gal$(L/K)$ permutes the primes $\mathfrak{Q}$ lying over $\mathfrak{q}$. □

**Theorem 4.3.6.** *Let $\boldsymbol{\eta}$ be an Euler system and $\mathfrak{q} \in \mathcal{R}_{n,M}$ a prime. Then*

$$[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \begin{cases} \phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{r}/\mathfrak{q})) & \text{if } \mathfrak{q} \mid \mathfrak{r} \\ 0 & \text{if } \mathfrak{q} \nmid \mathfrak{r} \end{cases}$$

*Proof.* First suppose that $\mathfrak{q} \nmid \mathfrak{r}$. Then by the definition of the $\mathfrak{p}$-system, we have that $\mathfrak{q}$ is unramified in $L^{\mathfrak{r}}/L$. Hence for all primes $\mathfrak{Q}'$ of $L^{\mathfrak{r}}$ lying above primes $\mathfrak{Q}/\mathfrak{q}$ in $L$ we have that $v_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r})) = v_{\mathfrak{Q}'}(\kappa_{n,M}(\mathfrak{r}))$. It then follows that for all $\mathfrak{Q}/\mathfrak{q}$ we have $v_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r})) \equiv 0 \pmod{M}$ where we have used the fact that $\kappa_{n,M}(\mathfrak{r})$ is a global unit times an $M^{th}$ power in $L^{\mathfrak{r}\times}$. Therefore, $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = 0$.

Now suppose that $\mathfrak{q} \mid \mathfrak{r}$, and write $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$. Let $\mathfrak{Q}$ be a prime of $L$ lying above $\mathfrak{q}$ and $\sigma_{\mathfrak{Q}}$ a lift of $\sigma_{\mathfrak{q}}$ so that $\sigma_{\mathfrak{Q}}$ is contained in the inertia group of $\overline{\mathfrak{Q}}$ where $\overline{\mathfrak{Q}}$ is a prime of $\overline{L}$ lying above $\mathfrak{Q}$. Furthermore, let $k$ be the highest power of $p$ dividing $\mathbf{N}\mathfrak{q} - 1$ so that $\mathbf{N}\mathfrak{q} - 1 = dp^k$ with $(d, p) = 1$. We claim that

$$(\kappa_{n,M}(\mathfrak{r})^{d/M})^{1-\sigma_{\mathfrak{Q}}} \equiv (\kappa_{n,M}(\mathfrak{s})^{d/M})^{((L^{\mathfrak{s}}/L),\mathfrak{Q})-1} \pmod{\mathfrak{Q}'}$$

where $\mathfrak{Q}'$ is any prime of $L^{\mathfrak{r}}$ lying above $\mathfrak{Q}$. By the definition of the map (in particular, Equations 4.1 and 4.2), we would then have that

$$d\phi_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{s}) = dv_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r}))$$

Since $d$ is prime to $M$, it would then follow that $\phi_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{s}) = v_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r}))$ which proves the Theorem.

To deduce the claim, we first expand the definition of $\kappa_{n,M}$. We have that

$$\kappa_{n,M}(\mathfrak{r}) = \frac{\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^M}, \kappa_{n,M}(\mathfrak{s}) = \frac{\boldsymbol{\eta}(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}}}{\beta_{\mathfrak{s}}^M} \tag{4.3}$$

for some $\beta_{\mathfrak{r}} \in L^{\mathfrak{r}\times}$ and $\beta_{\mathfrak{s}} \in L^{\mathfrak{s}\times}$ satisfying

$$\beta_{\mathfrak{r}}^{\sigma-1} = \boldsymbol{\eta}((\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M), \beta_{\mathfrak{s}}^{\sigma-1} = \boldsymbol{\eta}((\sigma-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M) \tag{4.4}$$

for all $\sigma \in G_{\mathfrak{r}}$ and $\sigma \in G_{\mathfrak{s}}$ respectively. To ease notation, let $\tau_{\mathfrak{q}} = ((L^{\mathfrak{s}}/K), \mathfrak{q})$ and $\tau_{\mathfrak{Q}} = ((L^{\mathfrak{s}}/L), \mathfrak{Q})$. We now observe that

$$\begin{aligned}
(\kappa_{n,M}(\mathfrak{r})^{d/M})^{1-\sigma_{\mathfrak{Q}}} &= ((\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}})^{1/M}/\beta_{\mathfrak{r}})^{d(1-\sigma_{\mathfrak{Q}})} && \text{(by Equation 4.3)}\\
&\equiv \beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)} \pmod{\mathfrak{Q}'} && \text{(since } \boldsymbol{\eta}(x_{n,\mathfrak{r}}) \text{ is a global unit)}\\
&= \boldsymbol{\eta}((\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M)^d && \text{(Equation 4.4)}\\
&= \boldsymbol{\eta}((\mathbf{N}\mathfrak{q}-1-N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d && \text{(Lemma 4.1.4)}\\
&= \boldsymbol{\eta}((\mathbf{N}\mathfrak{q}-1)D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d\boldsymbol{\eta}(\tau_{\mathfrak{q}}^{-1}-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M)^d\\
&= (\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d(\mathbf{N}\mathfrak{q}-1)/M}/\beta_{\mathfrak{s}}^{d(1-\tau_{\mathfrak{q}}^{-1})} && \text{(Equation 4.3)}\\
&= (\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d\tau_{\mathfrak{q}}\tau_{\mathfrak{q}}^{-1}(\mathbf{N}\mathfrak{q}-1)/M}/\beta_{\mathfrak{s}}^{d(1-\tau_{\mathfrak{q}}^{-1})}\\
&\equiv (\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d\tau_{\mathfrak{q}}(1-\tau_{\mathfrak{q}}^{-1})/M}/\beta_{\mathfrak{s}}^{d(1-\tau_{\mathfrak{q}}^{-1})} \pmod{\mathfrak{Q}'}\\
&\equiv \boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}d(1-\tau_{\mathfrak{Q}}^{-1})/M}/\beta_{\mathfrak{s}}^{d(1-\tau_{\mathfrak{Q}}^{-1})} \pmod{\mathfrak{Q}'} && \text{(Proposition 4.2.3)}\\
&= ((\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}}/\beta_{\mathfrak{s}}^{M})^{1/M})^{d(1-\tau_{\mathfrak{Q}}^{-1})}\\
&\equiv (\kappa_{n,M}(\mathfrak{s})^{d/M})^{\tau_{\mathfrak{Q}}-1} \pmod{\mathfrak{Q}'}
\end{aligned}$$

thereby proving the claim. □

## 4.4 Bounding the Ideal Class Group of $K(E[\mathfrak{p}])$

After constructing the machinery of abstract Euler systems, we now look to applying our theory in the case of $\mathfrak{p}$-systems coming from the running theme throughout this essay: an elliptic curve with complex multiplication. In particular, we will show how the results from the previous section allow us to place bounds on the Galois-eigenspaces of a certain ideal class group. This will form yet another key component of the proof of the Coates-Wiles Theorem. The interested reader is encouraged to view Rubin's appendix in [Lan90] for the case of cyclotomic units and the $\mathfrak{p}$-system defined over $\mathbb{Q}$.

*Assumptions.* Throughout this section, we shall assume that $E$ is an elliptic curve defined over an imaginary quadratic number field $K$ with complex multiplication by $\mathcal{O}_K$ so that $K$ has class number 1. We fix a prime $\mathfrak{p}$ of $K$ prime to $\mathfrak{f}$, $\mathfrak{a} \lhd \mathcal{O}_K$ an auxiliary ideal prime to $6\mathfrak{f}$ and we fix the $\mathfrak{p}$-systemof $K$ as defined in Example 4.1.10. As before, $\mathcal{R} = \mathcal{R}_{n,M}^{\mathfrak{c}}$ will denote the ideals in $\mathcal{R}^{\mathfrak{c}}$ whose prime divisors $\mathfrak{q}$ split completely in $K_n/K$ and such that $\mathbf{N}\mathfrak{q} - 1 \equiv 0 \pmod{M}$.

Furthermore, we write $L = K_1 = K(E[\mathfrak{p}])$, $\boldsymbol{\mu}_L$ the group of roots of unity in $L$ and $L_M = L(\boldsymbol{\mu}_M)$ where $\boldsymbol{\mu}_M$ are the $M^{th}$ roots of unity in an algebraic closure of $L$. We have that $G = \mathrm{Gal}(L/K)$ so that $G$ is cyclic of order $p-1$ or $p^2-1$, depending on how $p$ ramifies in $K$. In order to simplify the exposition, we shall assume that $p$ splits completely in $K$ so that in fact $|G| = p-1$. This restriction is not too severe since, as we shall see in the sequel, it turns out that this case is enough to deduce the Coates-Wiles Theorem[4].

Consider all irreducible $\mathbb{Z}_p$-representations of $G$. Since $p$ splits completely in $K$, all such representations are 1-dimensional and so, in particular, they are in one-to-one correspondence with the elements of the character group

[4] The reasoning for this restriction is that if $|G| = p^2-1$ then there exist irreducible $\mathbb{Z}_p$-representations of $G$ of dimension 2 which do not correspond to elements of the character group of $G$ (in other words, their characters are not linear characters).

$\widehat{G}$. By Proposition A.3.2 we thus get a decomposition of the group ring

$$\mathbb{Z}_p[G] \cong \bigoplus_{\chi \in \widehat{G}} R_\chi$$

where each $R_\chi$ is isomorphic to $\mathbb{Z}_p$. If $M$ is a $\mathbb{Z}[G]$-module then we shall write $M^\chi$ for $(M \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\chi$, the $\chi$-eigenspace of the $p$-adic completion of $M$.

**Lemma 4.4.1.** *Let $\mathcal{C}_L$ be the ideal class group of $L$ and $M$ a power of $p$. Then we have injections*

$$\mathrm{Hom}\,(\mathcal{C}_L, \mathbb{Z}/M\mathbb{Z}) \hookrightarrow \mathrm{Hom}(G_{L_M}, \mathbb{Z}/M\mathbb{Z})$$
$$L^\times/(L^\times)^M \hookrightarrow L_M^\times/(L_M^\times)^M$$

*Proof.* Let $L(1)$ be the Hilbert class field of $L$ and $\phi : \mathrm{Gal}(L(1)/L) \to \mathcal{C}_L$ the inverse of the Artin map. Then the composition

$$\begin{tikzcd} G_L \arrow[r] & \mathrm{Gal}(L(1)/L) \arrow[r] & \mathcal{C}_L \\ \sigma \arrow[r, mapsto] & \sigma|_{L(1)} \arrow[r, mapsto] & \phi(\sigma|_{L(1)}) \end{tikzcd}$$

induces an injection

$$\mathrm{Hom}(\mathcal{C}_L, \mathbb{Z}/M\mathbb{Z}) \hookrightarrow \mathrm{Hom}(G_L, \mathbb{Z}/M\mathbb{Z})$$

Now the kernel of the natural map $\mathrm{Hom}(G_L, \mathbb{Z}/M\mathbb{Z}) \to \mathrm{Hom}(G_{L_M}, \mathbb{Z}/M\mathbb{Z})$ is $\mathrm{Hom}(\mathrm{Gal}(L_M/L), \mathbb{Z}/M\mathbb{Z})$ so it suffices to show that there does not a non-trivial homomorphism $\mathrm{Gal}(L_M/L) \to \mathbb{Z}/M\mathbb{Z}$. In other words, we need to show that there does not exist an unramified $p$-extension of $L$ in $L_M$. We observe that the $p$-part of $\mathrm{Gal}(L_M/L)$ is $\mathrm{Gal}(L_M/L(\boldsymbol{\mu}_p))$. But this extension is totally ramified at all primes of $L(\boldsymbol{\mu}_p)$ above $p$ and so the first injection is proven.

To prove the second injection, note that Proposition A.2.4 provides us with isomorphisms

$$L^\times/(L^\times)^M \cong H^1(L, \boldsymbol{\mu}_M)$$
$$L_M^\times/(L_M^\times)^M \cong H^1(L_M, \boldsymbol{\mu}_M)$$

It hence suffices to show that the cohomological restriction map

$$H^1(L, \boldsymbol{\mu}_M) \to H^1(L_M, \boldsymbol{\mu}_M)$$

is injective. We note that the kernel of this map is $H^1(\mathrm{Gal}(L_M/L), \boldsymbol{\mu}_M)$. But Sah's Lemma implies that this is trivial since $\mathrm{Gal}(L_M/L)$ is cyclic, acts faithfully on $\boldsymbol{\mu}_M$ and $p > 2$. □

In the previous sections we defined $\mathcal{R} = \mathcal{R}_{n,M}$ to be the collection of all ideals in $\mathcal{R}$ whose prime divisors $\mathfrak{q}$ split completely in $K_n$ and satisfy $\mathbf{N}\mathfrak{q} - 1 \equiv 0 \pmod{M}$. Having proved many useful results with such ideals, we must ask ourselves whether any actually exist. The answer is a resounding yes (at least in the case $n = 1$) and the following Proposition will provide us with a healthy stock of primes in $\mathcal{R} = \mathcal{R}_{1,M}$. We will then go on to use these primes to place bounds on the size of $\mathcal{C}_L^\chi$.

**Proposition 4.4.2.** *Let $\kappa \in L^\times/(L^\times)^M$ and $\psi$ a non-trivial homomorphism in* $\mathrm{Hom}(\mathcal{C}_L, \mathbb{Z}/M\mathbb{Z})$*. Then there exists a prime ideal $\mathfrak{q} \in \mathcal{R}_{1,M}$ and a prime $\mathfrak{Q}$ of $L$ lying above $\mathfrak{q}$ such that*

1. *$[\kappa]_{\mathfrak{q}} = 0$ and $\psi([\mathfrak{Q}]) \neq 0$ where $[\mathfrak{Q}]$ is the class of $\mathfrak{Q}$ in $\mathcal{C}_L$.*

2. *For all $d \in \mathbb{Z}, d\phi_{\mathfrak{q}}(\kappa) = 0$ if and only if $\kappa^d \in (L^\times)^M$.*

*Proof.* Consider the Kummer map

$$\begin{aligned} L^\times/(L^\times)^M &\to \operatorname{Hom}(G_{L_M}, \boldsymbol{\mu}_M) \\ y &\mapsto (\sigma \mapsto (y^{1/M})^{\sigma-1}) \end{aligned}$$

and denote by $\varkappa$ the image of $\kappa$ under this map. Let $e$ be the order of $\kappa$ in $L^\times/(L^\times)^M$ and identify $\psi$ with its image in $\operatorname{Hom}(G_{L_M}, \mathbb{Z}/M\mathbb{Z})$ under the injection of Lemma 4.4.1. Consider the two subgroups

$$\begin{aligned} \mathcal{H}_1 &= \{\, \gamma \in G_{L_M} \mid \psi(\gamma) = 0 \,\} \\ \mathcal{H}_2 &= \{\, \gamma \in G_{L_M} \mid \varkappa(\gamma) \text{ is killed by } t < e \,\} \end{aligned}$$

It is immediate from the facts that $\psi \neq 0$ and $\operatorname{Hom}(\mathcal{C}_L, \mathbb{Z}/M\mathbb{Z})$ injects into $\operatorname{Hom}(G_{L_M}, \mathbb{Z}/M\mathbb{Z})$ that $\mathcal{H}_1$ is a proper subgroup of $G_{L_M}$. Moreover, appealing to Lemma 4.4.1 shows that $\mathcal{H}_2$ is also a proper subgroup of $G_{L_M}$ since injective homomorphisms preserve order. We may thus choose a $\gamma \in G_{L_M} \setminus \{\, \mathcal{H}_1 \cup \mathcal{H}_2 \,\}$.

Now, fix a finite Galois extension $N$ of $L$ containing $L_M$ and such that $\varkappa$ and $\psi$ are trivial on $G_L$. By the Chebotarev Density Theorem, there are infinitely many finite primes $\mathfrak{q}$ of $K$ that are unramified in $N$ and such that the Artin symbol of $\mathfrak{q}$ in $N/K$ coincides with the conjugacy class of $\gamma|_N$. We are thus free to choose such a prime $\mathfrak{q}$ not dividing $6\mathfrak{a}\mathfrak{f}\mathfrak{p}$ and such that $[\kappa]_{\mathfrak{q}} = 0$. Let $\mathfrak{Q}$ be a prime of $L$ lying above $\mathfrak{q}$. We claim that $\mathfrak{q}$ and $\mathfrak{Q}$ are the desired primes of the Proposition.

By construction $\gamma$ fixes $L(\boldsymbol{\mu}_m)$ so by Proposition A.1.1, $\mathfrak{p}$ splits completely in $L(\boldsymbol{\mu}_m)$. Therefore, *a foritiori*, $\mathfrak{p}$ splits completely in $L$ whence $\mathfrak{q} \in \mathcal{R}$.

To prove the second assertion, observe that the inclusion

$$\operatorname{Hom}(\mathcal{C}_L, \mathbb{Z}/M\mathbb{Z}) \hookrightarrow \operatorname{Hom}(G_L, \mathbb{Z}/M\mathbb{Z})$$

of Lemma 4.4.1 identifies $\psi([\mathfrak{Q}])$ with $\psi((\overline{L}/L), \mathfrak{Q}) = \psi(\gamma)$. Now, $\gamma \notin \mathcal{H}_1$ and so $\psi([\mathfrak{Q}]) \neq 0$.

Moreover, since $\gamma \notin \mathcal{H}_2$, it follows that $(\kappa^{1/M})^{((\overline{L}/L),\mathfrak{Q})-1}$ is a primitive $e^{th}$ root of unity. Hence $\kappa$ has order $e(\mathbf{N}\mathfrak{q} - 1)$ modulo $\mathfrak{Q}$ and so $\kappa$ has order $e$ in

$$(\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times/((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times)^M$$

By Proposition 4.3.5, $\phi_{\mathfrak{q}}$ is an isomorphism on this factor group whence the second assertion follows. □

**Lemma 4.4.3.** *Let $\chi \in \widehat{G}$ be a non-trivial character. Then*

$$\left(\mathcal{O}_L^\times/\boldsymbol{\mu}_L\right)^\chi \cong R_\chi$$

*Proof.* We first note that since $K$ is totally imaginary, $L$ must be as well. Hence $L$ admits $[L : \mathfrak{Q}] = 2[L : K] = 2|G|$ pairs of complex conjugate embeddings into $\overline{\mathbb{Q}}$ and no real embeddings. By Dirichlet's Unit Theorem, we have that

$$\mathcal{O}_L^\times/\boldsymbol{\mu}_L \cong \mathbb{Z}^{|G|-1}$$

Since $\mathbb{Q}[G] \cong \mathbb{Q}^{|G|}$, we have a short exact sequence of $\mathbb{Q}[G]$-modules

$$0 \longrightarrow \left( \mathcal{O}_L^\times \big/ \boldsymbol{\mu}_L \right) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q}[G] \longrightarrow \mathbb{Q} \longrightarrow 0$$

Since $\mathbb{Z}_p$ is a flat $\mathbb{Z}$-module, tensoring with $\mathbb{Z}_p$ will preserve this exact sequence. We may thus pass to the $\chi$-eigenspace to deduce the assertion of the Lemma. □

We now arrive at the main Theorem of this Chapter. Effectively, with this result under our belt, the morale of Kolyvagin and Rubin's theory can be phrased as follows: the machinery that we have constructed takes as input an Euler system corresponding to a $\mathfrak{p}$-system of $K$ and an irreducible $\mathbb{Z}_p$-representation $\chi$ of $G$ and outputs an upper bound on the $\chi$-eigenspace of the ideal class group of $L$. The proof of this Theorem is rather lengthy but the main idea will be to use Proposition 4.4.2 to construct a sequence of primes $\mathfrak{q}$ of $K$ and primes $\mathfrak{Q}/\mathfrak{q}$ of $L$ for which the images in $\mathcal{C}_L^\chi$ of their classes in $\mathcal{C}_L$ generate $\mathcal{C}_L^\chi$. The classes of these primes will give rise to interesting relations in $\mathcal{C}_L^\chi$ which will allow us to deduce an upper bound on the size of $|\,\mathcal{C}_L^\chi\,|$.

**Theorem 4.4.4.** *Let $\boldsymbol{\eta}$ be an Euler system and $\mathcal{U} = \mathcal{U}_{\boldsymbol{\eta}} = \langle \boldsymbol{\mu}_L, \boldsymbol{\eta}(1, \mathcal{O}_K) \rangle_{\mathbb{Z}_p[G]}$. If $\chi$ is an irreducible $\mathbb{Z}_p$-representation of $G$ then*

$$|\,\mathcal{C}_L^\chi\,| \leq \left| \left( \mathcal{O}_L^\times \big/ \mathcal{U}_{\boldsymbol{\eta}} \right)^\chi \right|$$

*Proof.* First suppose that $\chi$ is the trivial character. Let $P$ be the $p$-part of $\mathcal{C}_L$. We may identify $\mathcal{C}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ with $P$ considered as a $\mathbb{Z}_p$-module with module structure given by the scalar multiplication

$$\left( \sum_{i=0}^{\infty} a_i p^i \right) \cdot x \mapsto \sum_{i=0}^{\infty} a_i p^i x$$

which is well-defined since $P$ is annihilated by $p^n$ for sufficiently large $n$. $P$ clearly also has a natural action of $G$ so it is infact a $\mathbb{Z}_p[G]$-module. Since $\chi$ is the trivial character, the $\chi$-idempotent is

$$\varepsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1}$$

which is simply the norm from $L$ to $K$ map (up to a constant). Hence $P^\chi$ is in fact that $p$-part of $\mathcal{C}_K$. But $\mathcal{C}_K$ is trivial and so we must have that $|\,\mathcal{C}_L^\chi\,| = 0$.

Now suppose that $\chi$ is not the trivial character and denote

$$M = p \left| \left( \mathcal{O}_K^\times \big/ \mathcal{U} \right)^\chi \right| |\,\mathcal{C}_L^\chi\,|$$

Moreover, let $\overline{\mathcal{O}_K^\times}$,$\overline{\mathcal{U}}$ and $\overline{\boldsymbol{\mu}_L}$ denote the images of $\mathcal{O}_K^\times$,$\mathcal{U}$ and $\boldsymbol{\mu}_L$ in $L^\times/(L^\times)^M$. By Lemma 4.4.3, $(\overline{\mathcal{O}_K^\times}/\overline{\boldsymbol{\mu}_L})^\chi$ is a free $R_\chi/MR_\chi$-module of rank 1. Hence for some $t \mid M$ we have

$$\left( \mathcal{O}_K^\times \big/ \mathcal{U} \right)^\chi \cong \overline{\mathcal{O}_K^\times}^\chi \big/ \overline{\mathcal{U}}^\chi \cong R_\chi \big/ tR_\chi$$

Now let $\xi \in \overline{\mathcal{O}_K^\times}^\chi$ be an $R_\chi$-generator of $\overline{\mathcal{O}_K^\times}^\chi / \overline{\boldsymbol{\mu}}^\chi$ so that $\xi$ has order $M$ in $L^\times/(L^\times)^M$. Then $\xi^t \in \overline{\mathcal{U}}^\chi$. Fix a root of unity $\zeta \in \overline{\boldsymbol{\mu}_L}^\times$ so that

$$\xi^t = \zeta^a (\kappa_{1,M}(\mathcal{O}_K)^\chi)^b$$

for some $a, b \leq M$ where we have used the fact that $\kappa_{1,M}(\mathcal{O}_K)$ is the image of $\boldsymbol{\eta}(1, \mathcal{O}_K)^\chi$ in $L^\times/(L^\times)^M$. Let $t_0$ denote the order of $\kappa_{1,M}(\mathcal{O}_K)^\chi$. Then $\xi^{tt_0} = \zeta^a$ so that $M|t_0 t$.

Henceforth, given $\mathfrak{r} \in \mathcal{R}$, we write $\kappa(\mathfrak{r})$ for $\kappa_{n,M}(\mathfrak{r}) \in L^\times/(L^\times)^M$. Label the elements of $\mathrm{Hom}(\mathcal{C}_L^\chi, \mathbb{Z}/M\mathbb{Z})$ as

$\psi_1, \ldots, \psi_k$. By Proposition 4.4.2, we inductively define a sequence of prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_k \in \mathcal{R}$ of $K$ as follows. Suppose that we have constructed primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_{i-1}$ for $i-1 \leq k$. Let $\mathfrak{r}_i = \prod_{j \leq i} \mathfrak{q}_j$ where we understand $\mathfrak{q}_0 = \mathcal{O}_K$. We then define $\mathfrak{q}_i \in \mathcal{R}$ to be the prime of $K$ generated by the Proposition using the homomorphism $\psi_i$ and the element $\kappa(\mathfrak{r}_{i-1})^\chi$. If we let $\mathfrak{Q}_i/\mathfrak{q}_i$ be the primes of $L$ lying above the $\mathfrak{q}_i$ provided by the Proposition and $\mathfrak{c}_i$ the class of $\mathfrak{Q}_i$ in $\mathcal{C}_L$ then we have the following two properties:

1. $\alpha_i(\mathfrak{c}_i) \neq 0$

2. $d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi) = 0$ if and only if $(\kappa(\mathfrak{r}_{i-1})^\chi)^d$

For all $1 \leq i \leq k$. We now claim that $\mathfrak{c}_i^\chi, \ldots, \mathfrak{c}_k^\chi$ generate $\mathcal{C}_L^\chi$ as a $\mathbb{Z}_p[G]$-module. If this were not the case then let $H$ be the subgroup generated by the $\mathfrak{c}_i$ over $\mathbb{Z}_p[G]$. Then we would always be able to find a non-trivial homomorphism $\psi : \mathcal{C}_L^\chi / H \to \mathbb{Z}/M\mathbb{Z}$. Such a homomorphism would clearly be 0 on the $\mathfrak{c}_i^\chi$. On the other hand, we must have that $\psi = \psi_i$ for some $1 \leq i \leq k$ so $\psi(\mathfrak{c}_i) = 0$ which contradicts the first property stated above.

Next, let $s_i$ for $1 \leq i \leq k$ denote the order of $\mathfrak{c}_i^\chi$ in $\mathcal{C}_L^\chi / \langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_{i-1}^\chi \rangle$ and $t_i$ for $0 \leq i \leq k-1$ the order of $\kappa(\mathfrak{r}_i)^\chi$ in $L^\times/(L^\times)^M$. We claim that $t_{i-1} \mid t_i$. Observe that since $R_\chi$ is a free $\mathbb{Z}_p$-module of rank 1, we have

$$[\langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_i^\chi \rangle : \langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_{i-1}^\chi \rangle] = [R_\chi : s_i R_\chi]$$

By the fact that the $\mathfrak{c}_i$ generate $\mathcal{C}_L^\chi$ it then follows that

$$|\,\mathcal{C}_L^\chi\,| = \prod_{i=1}^{k} [R_\chi : s_i R_\chi]$$

By Theorem 4.3.6 we have that $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i} = \phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi)$. Furthermore, the second property stated above, we know that $d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi) = 0$ if and only if $(\kappa(\mathfrak{r}_{i-1})^\chi)^d = 0$. Hence $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$ has order $t_{i-1}$ in $I^{\mathfrak{q}_i}/MI^{\mathfrak{q}_i}$. On the other hand, $d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r})^\chi) = 0$ if and only if $(\kappa(\mathfrak{r}_i)^\chi)^d = 0$ and so $t_{i-1} | t_i$ as claimed.

We next claim that $(t_i/t_{i-1})\mathfrak{c}_i^\chi = 0$ in $\mathcal{C}_L^\chi / \langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_{i-1}^\chi \rangle$. Since $(\kappa(\mathfrak{r}_i)^\chi)^{t_i} \in (L^\times)^M$, we can choose $z_i \in L^\times/(L^\times)^M$ such that $z_i^{M/t_i} = \kappa(\mathfrak{r}_i)^\chi \zeta$ for some $\zeta \in \boldsymbol{\mu}_L$ so that

$$\left(\frac{M}{t_i}\right)[z_i]_{\mathfrak{q}_i} = [\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$$

and $[z_i]_{\mathfrak{q}_i}$ has order $t_{i-1}M/t_i$ in $(I^{\mathfrak{q}_i}/MI^{\mathfrak{q}_i})^\chi$. It is easy to see that $(I^{\mathfrak{q}_i}/MI^{\mathfrak{q}_i})^\chi \cong R_\chi/MR_\chi$. Indeed, we have an isomorphism of $\mathbb{Z}[G]$-modules

$$\begin{aligned} I^{\mathfrak{q}_i} &\to \mathbb{Z}[G] \\ \prod_{\sigma \in G} \sigma(\mathfrak{Q}_i)^{e_\sigma} &\mapsto \sum_{\sigma \in G} e_\sigma \sigma \end{aligned}$$

where $\mathfrak{Q}_i$ is some prime of $L$ lying above $\mathfrak{q}_i$. By Part 1 of Theorem 4.3.6 and the previous discussion, it follows that there exists a unit $u \in R_\chi^\times$ such that

$$(z_i) \equiv u \frac{t_i}{t_{i-1}} \mathfrak{q}_i^\chi \pmod{I^{\mathfrak{q}_1}, \ldots, I^{\mathfrak{q}_{i-1}}, t_i I_L}$$

Since $t_0 | t_i$ and $(M/t) | t_0$ it follows that $t_i$ annihilates $\mathcal{C}_L^\chi$ since $M/t$ does. Projecting the above congruence to $\mathcal{C}_L^\chi$, we then have that $(t_i/t_{i-1})\mathfrak{c}_i^\chi = 0$ in $\mathcal{C}_L^\chi / \langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_{i-1}^\chi \rangle$ as claimed.

Hence for all $1 \leq i \leq k$, $s_i$ divides $(t_i/t_{i-1})$ so that

$$|\,\mathcal{C}_L^\chi\,| = \prod_{i=1}^{k} [R_\chi : s_i R_\chi]$$

divides

$$\prod_{i=1}^{k}\left[R_\chi : \frac{t_i}{t_{i-1}}R_\chi\right] = \prod_{i=1}^{k}[t_{i-1}R_\chi : t_iR_\chi] = [t_0R_\chi : t_kR_\chi]$$

Now, $t_k \mid M$ and $M \mid tt_0$ whence $[t_0R_\chi : t_kR_\chi]$ divides $[R_\chi : tR\chi] = |(\mathcal{O}_L^\times/\mathcal{U})^\chi|$ and so the Theorem is proven. □

**Corollary 4.4.5.** *Let $\boldsymbol{\eta}(n,\mathfrak{r}) = \eta_n^{\mathfrak{a}}(\mathfrak{r})$ be the Euler system of elliptic units with respect to an auxiliary ideal $\mathfrak{a}$ prime to $6\mathfrak{f}$. If $\chi$ is an irreducible $\mathbb{Z}_p$-representation of $G$ and $\eta_1(\mathcal{O}_K) \notin \boldsymbol{\mu}_L^\chi((\mathcal{O}_L^\times)^\chi)^p$ then $\mathcal{C}_L^\chi$ is trivial.*

*Proof.* By Theorem 4.4.4, we know that

$$|\,\mathcal{C}_L^\chi\,| \leq \left|\left({}^{\mathcal{O}_L^\times}\!\big/_{\mathcal{U}_{\boldsymbol{\eta}}}\right)^\chi\right|$$

where $\mathcal{U}$ is the $\mathbb{Z}_p[G]$-module generated by $\boldsymbol{\mu}_L$ and $\eta_1(\mathcal{O}_K)$. Since $(\mathcal{O}_K^\times)^\chi$ is a $p$-group, the hypothesis $\eta_1(\mathcal{O}_K) \notin \boldsymbol{\mu}_L^\chi((\mathcal{O}_L^\times)^\chi)^p$ ensures that the factor group $(\mathcal{O}_L^\times/\mathcal{U})^\chi$ is trivial. □

# Chapter 5

# The Coates-Wiles Theorem

Our goal is finally in sight; we now have all the tools required in order to tackle the proof of the Coates-Wiles Theorem. Our plan of attack shall be as follows. We will define a homomorphism of the unit group of a completion $L_{\mathfrak{P}}$ of $L = K(E[\mathfrak{p}])$ for some prime $\mathfrak{P}$ above $\mathfrak{p}$ to $E[\mathfrak{p}]$ which will provide us with the connection between the non-vanishing of $L(\overline{\psi}, 1)$ and the elliptic units. This connection, along with Corollary 4.4.5 will allow us to annihilate $\mathcal{C}_L^{\chi_E}$ where $\chi_E$ is the representation of $G$ on $E[\mathfrak{p}]$. We will then show that we have an isomorphism $(\mathcal{O}_L^\times)^{\chi_E} \cong (\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$. An easy application of the Chebotarev Density Theorem will then allow us to employ these results, along with Corollary 2.4.2, to annihilate the Selmer group $\mathrm{S}^{(\psi_E(\mathfrak{p}))}(E)$ whence the Coates-Wiles Theorem will follow from the Mordell-Weil Theorem.

*Assumptions.* Throughout this section we shall assume that $K$ is an imaginary quadratic number field and $E/K$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ so that $K$ has class number 1. We fix the following objects

- $\Lambda$ a lattice in $\mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ via the analytic isomorphism $\xi$ and $\Omega \in \mathbb{C}^\times$ such that $\Omega\mathcal{O}_K = \Lambda$.
- $(f) = \mathfrak{f}$ the conductor of the Hecke character $\psi_E$ attached to E.
- $\mathfrak{p}$ a finite prime of $K$ not dividing $\mathfrak{f}$ lying above a rational prime $p > 7$ and $\mathfrak{P}$ the unique prime of $L$ lying above $\mathfrak{p}$.
- $M$ a power of $p$.
- The $\mathfrak{p}$-system of $K$ given by $K_n^{\mathfrak{r}} = K(E[\mathfrak{p}^n\mathfrak{r}])$ for some $\mathfrak{r} \in \mathcal{R} = \mathcal{R}_{n,M}^{6\mathfrak{af}}$ and denote $L = K_1$, $G = \mathrm{Gal}(L/K)$.
- $\eta$ the Euler system of elliptic units with respect to an auxiliary ideal $\mathfrak{a} \lhd \mathcal{O}_K$ prime to $6\mathfrak{pf}$.

**Proposition 5.1.** *There exists a $G$-equivariant isomorphism*

$$\gamma : E[\mathfrak{p}] \to (1 + \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}})/(1 + \mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}})$$

*that induces a homomorphism*

$$\delta : \mathcal{O}_{L,\mathfrak{P}}^\times \to E[\mathfrak{p}]$$

*by composing the natural projection $\mathcal{O}_{L,\mathfrak{P}}^\times \to (1 + \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}})/(1 + \mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}})$ with the inverse of $\gamma$.*

*Proof.* Since $E$ has good reduction at $\mathfrak{p}$, Proposition A.5.4 implies that $E[\mathfrak{p}] \subseteq E_1(K_{\mathfrak{p}}) \subseteq E_1(L_{\mathfrak{P}})$. By Proposition A.5.5, we have an isomorphism $\widehat{E}[\mathfrak{p}] \cong E_1(L_{\mathfrak{P}})$ with $E$ considered as defined over $L$. Restricting this to $K_{\mathfrak{p}}$ we get an isomorphism $\widehat{E}[\mathfrak{p}] \cong E[\mathfrak{p}]$. We then define $\gamma$ to be the composition

$$\begin{tikzcd} E[\mathfrak{p}] \arrow[r] & \widehat{E}[\mathfrak{p}] \arrow[r, "1+\cdot"] & (1 + \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}})/(1 + \mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}}) \\ P \arrow[r, mapsto] & -x(P)/y(P) & \end{tikzcd}$$

To show that it is injective, observe that

$$P \in \ker \gamma \iff \frac{-x(P)}{y(P)} \in \ker(1+\cdot) \iff \frac{x(P)}{y(P)} \in \mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}}$$

Now, the proof of Lemma 3.1.4 implies that $v_{\mathfrak{p}}(x(P)/y(P)) = (\mathbf{N}\mathfrak{p}-1)^{-1}$ whence $v_{\mathfrak{P}}(x(P)/y(P)) = (\mathbf{N}\mathfrak{p}-1)^{-2}$ since the ramification index of $\mathfrak{p}$ in $L/K$ is 2. This is clearly less than 2 so we must have that $P = 0$.

Since $|E[\mathfrak{p}]| = \mathbf{N}\mathfrak{p}$, the surjectivity of $\gamma$ will follow if we can show that $(1+\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}})/(1+\mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}})$ also has cardinality $\mathbf{N}\mathfrak{p}$. Indeed, the $\mathfrak{P}$-adic logarithm map provides an isomorphism

$$(1+\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}})/(1+\mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}}) \cong \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}/\mathfrak{P}^2\mathcal{O}_{L,\mathfrak{P}} \cong \mathcal{O}_{L,\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}} \cong \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$$

where we have used the fact that $\mathfrak{p}$ ramifies totally in $L/K$ so that the inertial degree of $\mathfrak{p}$ in $L/K$ is 1. The latter clearly has cardinality $\mathbf{N}\mathfrak{p}$ as claimed. The fact that $\gamma$ is $G$-equivariant now follows immediately from the definition. □

**Lemma 5.2.** *There exists a prime $\mathfrak{q}$ of $K$ not dividing $6\mathfrak{p}\mathfrak{f}$ such that $\mathbf{N}\mathfrak{q} \not\equiv \psi_E(\mathfrak{q}) \pmod{\mathfrak{p}}$.*

*Proof.* Since $p > 7$, Proposition A.7.8 implies that $E[\overline{\mathfrak{p}}] \subseteq E(K)$. We may therefore choose a prime $\mathfrak{q}$ of $K$ not dividing $6\mathfrak{p}\mathfrak{f}$, such that $[\mathfrak{q}, K(E[\overline{\mathfrak{p}}])/K] \neq 1$. We claim that such a prime $\mathfrak{q}$ satisfies the assertions of the Lemma. Indeed, by Thoerem A.7.6, the action of the Artin symbol on $E[\overline{\mathfrak{p}}]$ implies that $\psi_E(\mathfrak{q}) \not\equiv 1 \pmod{\overline{\mathfrak{p}}}$. Conjugating this congruence yields $\overline{\psi_E}(\mathfrak{q}) \not\equiv 1 \pmod{\mathfrak{p}}$. Since $\mathbf{N}\mathfrak{q} = \psi_E(\mathfrak{q})\overline{\psi_E}(\mathfrak{q})$, multiplying the congruence by $\psi_E(\mathfrak{q})$ shows that $\mathbf{N}\mathfrak{q} \not\equiv \psi_E(\mathfrak{q}) \pmod{\mathfrak{p}}$. □

Henceforth we shall assume that the auxiliary ideal defining the Euler system of elliptic units is any of the primes $\mathfrak{q}$ provided by Lemma 5.2.

**Proposition 5.3.** *The $L$-function of $E$ associated to $\psi_E$ satsifies the following properties*

1. $L(\overline{\psi_E}, 1)/\Omega \in K$
2. $L(\overline{\psi_E}, 1)/\Omega \in \mathcal{O}_{K,\mathfrak{p}}$
3. $L(\overline{\psi_E}, 1)/\Omega \equiv 0 \pmod{\mathfrak{p}}$ *if and only if* $\delta(\eta) = 0$

*where* $\eta = \eta_1^{\mathfrak{q}}(\mathcal{O}_K)$.

*Proof.* We recall that $\Phi_{\Lambda,\mathfrak{q}}$ is a rational function of $\wp(z;\Lambda)$ and $\wp(z;\Lambda)$ with $K$-rational coefficients. Fixing a Weierstrass model $y^2 = x^3 + ax + b$ of $E$ we may differentiate the Weierstrass equation

$$\wp'(z;\Lambda) = 4\wp(z;\Lambda)^3 + 4a\wp(z;\Lambda) + 4b$$

once to see that $\wp''(z;\Lambda)$ also belongs to $K(\wp(z;\Lambda), \wp'(z;\Lambda))$. From this it follows that
$\Phi_{\Lambda,\mathfrak{q}} \in K(\wp(z;\Lambda), \wp'(z;\Lambda))$ too. By Theorem 3.4.6 we have

$$\left.\frac{d}{dz}\log \Phi_{\Lambda,\mathfrak{q}}(z)\right|_{z=0} = 12f\Omega^{-1}(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1)$$

We therefore see that $L(\overline{\psi_E}, 1)/\Omega \in K$ so the first claim is proven.

To prove the second and third assertions, consider the $\mathfrak{p}$-torsion point

$$P = (\wp(\psi_E(\mathfrak{p})^{-1}\Omega;\Lambda), \wp'(\psi_E(\mathfrak{p})^{-1}\Omega;\Lambda)/2)$$

and let $z = -x(P)/y(P) \in \mathfrak{P}$ be the image of $P$ in $\widehat{E}[\mathfrak{p}]$ under the isomorphism $E[\mathfrak{p}] \cong \widehat{E}[\mathfrak{p}]$. By the definition of the Euler system of elliptic units, we have that $\eta = \Phi_{\mathfrak{p},\mathfrak{q}}(z)$. Now, Theorem 3.5.3 implies that $\Phi_{\mathfrak{p},\mathfrak{q}}(0), 12f\Omega^{-1}(N\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1) \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$. Furthemore we have that

$$D^1 \log(\Phi_{\mathfrak{p},\mathfrak{q}}(X))|_{X=0} = 12f\Omega^{-1}(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1)$$

On the other hand, we have

$$D^1 \log(\Phi_{\mathfrak{p},\mathfrak{q}}(X))|_{X=0} = \frac{(D^1\Phi_{\mathfrak{p},\mathfrak{q}}(X))|_{X=0}}{\Phi_{\mathfrak{p},\mathfrak{q}}(0)}$$

so that we obtain the expansion

$$\Phi_{\mathfrak{p},\mathfrak{a}}(X) \equiv \Phi_{\mathfrak{p},\mathfrak{q}}(0)(1 + 12f\Omega^{-1}(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1)X) \pmod{X^2}$$

From this, we see that

$$\eta = \Phi_{\mathfrak{p},\mathfrak{a}}(z) \equiv \Phi_{\mathfrak{p},\mathfrak{q}}(0)(1 + 12f\Omega^{-1}(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1)z) \pmod{\mathfrak{P}^2}$$

Applying the homomorphism $\delta : \mathcal{O}_{L,\mathfrak{P}}^{\times} \to E[\mathfrak{p}]$ yields

$$\delta(\eta) = (12f(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}))L(\overline{\psi_E}, 1)/\Omega)P$$

Now by Lemma 5.2, $\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q}) \not\equiv 1 \pmod{\mathfrak{p}}$ and so $12f(\mathbf{N}\mathfrak{q} - \psi_E(\mathfrak{q})) \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$. Hence we can have $\delta(\eta) = 0$ if and only if $L(\overline{\psi_E}, 1)/\Omega \equiv 0 \pmod{\mathfrak{p}}$ as required. □

*Remark.* We remark that the first assertion of the Proposition is a special case of Damerell's Theorem which states that for all $k \in \mathbb{N}_{\geq 1}$ we have $L(\overline{\psi_E}^k, k)\Omega^{-k} \in K$. The proof of the general case follows the exact same reasoning as the case in which $k = 1$ after differentiating the Weierstrass equation to show that, in fact, all derivatives of $\Phi_{\Lambda,\mathfrak{q}}$ are elements of $K(\wp(z;\Lambda), \wp(z;\Lambda))$.

**Definition 5.4.** Consider the representation of $G$ on $E[\mathfrak{p}]$. Then this is an irreducible $\mathbb{Z}_p$-representation of $G$ since $E[\mathfrak{p}]$ has no proper $G$-invariant subgroups. Let $\chi_E \in \widehat{G}$ be the corresponding character and $R_{\chi_E}$ the corresponding direct summand in the decomposition of the group ring $\mathbb{Z}_p[G]$. Then $E[\mathfrak{p}] \cong R_{\chi_E}/\mathfrak{p}R_{\chi_E}$.

**Lemma 5.5.** *$\boldsymbol{\mu}_L^{\chi_E}$ is trivial.*

*Proof.* Suppose, for a contradiction that $\boldsymbol{\mu}_L^{\chi_E}$ is not trivial. Let $P$ be the $p$-part of $\boldsymbol{\mu}_L$. In other words, $P$ is all the $(p^n)^{th}$ roots of unity contained in $L$ for $n \geq 1$. Explicitly, we may identify $\boldsymbol{\mu}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ with $P$ viewed as a $\mathbb{Z}_p[G]$-module with scalar multiplication by $\mathbb{Z}_p$ given by exponentiation and the usual action of $G$. This is well-defined since $P$ is killed by a large enough power of $p$. Then

$$\boldsymbol{\mu}_L^{\chi_E} = \{\, \zeta \in P \mid \sigma(\zeta) = \chi_E(\sigma)\zeta \text{ for all } \sigma \in G \,\}$$

by Part 3 of Proposition A.3.1. We claim that $\boldsymbol{\mu}_L^{\chi_E}$ consists of $p^{th}$ roots of unity. Indeed fix $\zeta \in \boldsymbol{\mu}_L^{\chi_E}$. Since $\chi_E(\sigma)$ is killed by $p$, we have that $\sigma(\zeta^p) = \zeta^p$ for all $\sigma \in G$. If $\zeta^p \neq 1$ then we would have a non-trivial $(p^n)^{th}$ root of unity $\zeta^p \in K$ for some $n \geq 1$. But this is impossible as $p > 7$ and $K$ is an imaginary quadratic number field whose only possible roots of unity are $\pm 1$ or $3^{rd}, 4^{th}$ or $6^{th}$ roots of unity. Now since $G$ is isomorphic to $E[\mathfrak{p}]^{\times}$, for all

$P \in E[\mathfrak{p}]^\times$ there exists $\sigma_P \in G$ such that $\chi_E(\sigma_P) = P$. Given $\zeta \in \boldsymbol{\mu}_L^{\chi_E}$ we define a homomorphism

$$\rho_\zeta : E[\mathfrak{p}] \to \boldsymbol{\mu}_p$$
$$P \mapsto \chi_E(\sigma_P)\zeta$$

where we set $\rho_\zeta(0) = O_E$ which is clearly $G_K$-equivariant and so is an element of $\mathrm{Hom}(E[\mathfrak{p}], \boldsymbol{\mu}_p)^{G_K}$. Now, the Weil pairing (see [Sil09, §III.8]) provides a $G_K$-equivariant isomorphism $E[p] \cong \mathrm{Hom}(E[p], \boldsymbol{\mu}_p)$. From the discussion above, there exists a non-trivial homomorphism in $\mathrm{Hom}(E[p], \boldsymbol{\mu}_p)^{G_K}$ and so $E[p]^{G_K}$ is non-trivial. But this is a contradiction to Proposition A.7.8. Hence $\boldsymbol{\mu}_L^{\chi_E}$ is trivial. □

**Theorem 5.6.** *Let $\mathcal{C}_L$ be the ideal class group of $L$. If $L(\overline{\psi_E}, 1)/\Omega \in \mathcal{O}_{K,\mathfrak{p}}^\times$ then $\mathcal{C}_L^{\chi_E}$ is trivial.*

*Proof.* Let $\eta = \eta_\mathfrak{q}(\mathcal{O}_K)$. We claim that $\eta^{\chi_E} \notin \boldsymbol{\mu}_L^{\chi_E}((\mathcal{O}_L^\times)^{\chi_E})^p$. If this were indeed the case then we would be able to conclude, by Corollary 4.4.5, that $\mathcal{C}_L^{\chi_E} = 0$. Appealing to Lemma 5.5, we see that $\boldsymbol{\mu}_L^{\chi_E}$ is trivial and so $\eta \notin \boldsymbol{\mu}_L^{\chi_E}$. We now show that $\eta^{\chi_E} \notin ((\mathcal{O}_L^\times)^{\chi_E})^p$. Indeed, since $\delta$ is $G$-equivariant, we have that $\delta(\eta^{\chi_E}) = \delta(\eta)^{\chi_E}$. Since the image of $\delta$ is contained in $E[\mathfrak{p}]$ and $E[\mathfrak{p}]^\chi = 0$ for any $\chi \neq \chi_E$ we have that $\delta(\eta)^{\chi_E} = \delta(\eta)$. Since $L(\overline{\psi}, 1)/\Omega$ is a $\mathfrak{p}$-adic unit, Part 3 of Proposition 5.3 implies that $\delta(\eta) \neq 0$. It follows that $\eta^{\chi_E}$ is not contained in the kernel of $\delta$ which certainly contains $((\mathcal{O}_L^\times)^{\chi_E})^p$ and so $\eta^{\chi_E} \notin ((\mathcal{O}_L^\times)^{\chi_E})^p$ as claimed. □

Theorem 5.6 gives us one half of the hypothesis of Corollary 2.4.2. In order to satisfy the second half, we prove the following Lemma and Theorem.

**Lemma 5.7.** *Suppose that $p$ splits completely in $K$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) \neq 1$. Then $\boldsymbol{\mu}_p \not\subseteq L_\mathfrak{P}$ and $(\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$ is a free $R_{\chi_E}$-module of rank one.*

*Proof.* Since the local Artin map is given in terms of the global one, Theorem A.7.5 implies that $[\psi_E(\mathfrak{p}), L_\mathfrak{P}/K_\mathfrak{p}] = 1$. Moreover, since $p$ is totally ramified in $\mathbb{Q}_p(\boldsymbol{\mu}_p)$, local Class Field Theory implies that $[p, \mathbb{Q}_p(\boldsymbol{\mu}_p)/\mathbb{Q}_p] = 1$.

Now suppose, for a contradiction, that $\boldsymbol{\mu}_p \subseteq L_\mathfrak{P}$ so that $K_\mathfrak{p}(\boldsymbol{\mu}_p) \subseteq L_\mathfrak{P}$. Note that $[K_\mathfrak{p}(\boldsymbol{\mu}_p) : K_\mathfrak{p}] = p-1$. But $p$ splits completely in $K$ so, in fact, $[K_\mathfrak{p}(\boldsymbol{\mu}_p) : K_\mathfrak{p}] = \mathbf{N}\mathfrak{p} - 1 = [L_\mathfrak{P} : K_\mathfrak{p}]$. It then follows that $[p/\psi_E(\mathfrak{p}), L_\mathfrak{P}/K_\mathfrak{p}] = 1$ whence $p/\psi_E(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$.

Observe that $\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) = \psi_E(\mathfrak{p}) + \overline{\psi_E}(\mathfrak{p}) = \psi_E(\mathfrak{p}) + p/\psi_E(\mathfrak{p})$ where we have used the norm map to obtain the relation $p = \psi_E(\mathfrak{p})\overline{\psi_E}(\mathfrak{p})$. Therefore,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) \equiv 1 \pmod{\mathfrak{p}}$$

On the other hand, Part 3 of Theorem A.7.6 implies that $\psi_E(\mathfrak{p})$ acts as Frobenius on $\overline{E}(\mathbb{F}_p)$. Hence by Hasse's Theorem (see [Sil09, §V.1]), we have that $|\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p}))| \leq 2\sqrt{p} < p-1$ so we must have that, in fact, $\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) = 1$. But this is a contradiction to the hypothesis of the Lemma and so $\boldsymbol{\mu}_p \not\subseteq L_\mathfrak{P}$.

Now, the $\mathfrak{P}$-adic logarithm map provides us with an isomorphism $\mathcal{O}_{L,\mathfrak{P}}^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathcal{O}_{L,\mathfrak{P}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. The latter is isomorphic to $L_\mathfrak{P}$ which is, in turn, isomorphic to $K_\mathfrak{p}[G]$. From this we deduce that $(\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$ is some quotient of $R_{\chi_E} \cong \mathbb{Z}_p$. But $\mathcal{O}_{L,\mathfrak{P}}^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong L_\mathfrak{P}^\times$ has no $p$-torsion since $\boldsymbol{\mu}_p \not\subseteq L_\mathfrak{P}$ whence $(\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E} \cong R_{\chi_E}$. □

**Theorem 5.8.** *Suppose that $p$ splits completely in $K$, $L(\overline{\psi_E}, 1)/\Omega \in \mathcal{O}_{K,\mathfrak{p}}^\times$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) \neq 1$. Then $(\mathcal{O}_L^\times)^{\chi_E} \cong (\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$.*

*Proof.* The natural inclusion map $(\mathcal{O}_L^\times)^{\chi_E} \hookrightarrow (\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$ is clearly injective so it suffices to show that it is surjective. Following the same argumentation of the proof of Theorem 5.6, Part 3 of Proposition 5.3 implies that $\eta^{\chi_E} \notin ((\mathcal{O}_L^\times)^{\chi_E})^p \subseteq ((\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E})^p$ and so $(\mathcal{O}_L^\times)^{\chi_E} \not\subseteq ((\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E})^p$.

Now, by Lemma 4.4.3, we have that $(\mathcal{O}_L^\times/\boldsymbol{\mu}_L)^{\chi_E}$ is a free $R_{\chi_E}$-module of rank one. Appealing to Lemma 5.5 we then see that $(\mathcal{O}_L^\times)^{\chi_E}$ is also a free $R_{\chi_E}$-module of rank one. Hence $(\mathcal{O}_L^\times)^{\chi_E}$ must be of the form $p^n\mathbb{Z}_p$ for some $n \geq 0$. By the above discussion, it follows that $n = 0$ and so the map must be a surjection. □

**Theorem 5.9** (Coates-Wiles)**.** *If $L(\overline{\psi_E}, 1) \neq 0$ then $E(K)$ is finite.*

*Proof.* By the Chebotarev Density Theorem, there are infinitely many primes $\mathfrak{p}$ of $K$ such that $((K/\mathbb{Q}), \mathfrak{p}) = 1$. We may choose such a prime $\mathfrak{p}$ not dividing

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot (L(\overline{\psi_E}, 1)/\Omega)\mathfrak{f}$$

and such that $\mathrm{Tr}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) \neq 1$. Let $p$ be the rational prime lying below $\mathfrak{p}$. Then $p > 7$ and splits completely in $K$ and $L(\overline{\psi_E}, 1)/\Omega$ is a unit at $\mathfrak{p}$. Let $\mathfrak{P}$ be the unique prime of $L$ lying above $\mathfrak{p}$. By Theorem 5.6, $\mathcal{C}_L^{\chi_E}$ is trivial. Moreover, Theorem 5.8 yields an isomorphism $(\mathcal{O}_L^\times)^{\chi_E} \cong (\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$.

We would now like to apply Corollary 2.4.2 in order to annihilate the Selmer group $\mathrm{S}^{(\psi_E(\mathfrak{p}))}(E)$. To this end, we must show that $\mathrm{Hom}(\mathcal{C}_L, E[\mathfrak{p}])^G = 0$ and $\delta_1(\mathcal{O}_L^\times) \neq 0$.

Let $f \in \mathrm{Hom}(\mathcal{C}_L, E[\mathfrak{p}])^G$ be a non-trivial homomorphism. We claim that $f$ can only be non-trivial on $\mathcal{C}_L^{\chi_E}$. Let $\chi \neq \chi_E$ be another irreducible $\mathbb{Z}_p$-representation of $G$ and let $x \in \mathcal{C}_L^{\chi}$. By $G$-equivariance and idempotency of $\varepsilon_\chi$ we have

$$f(x) = f(\varepsilon_\chi x) = \varepsilon_\chi f(x) = 0$$

since $E[\mathfrak{p}]^\chi = 0$. Combining this fact with the result that $\mathcal{C}_L^{\chi_E}$ is trivial shows that $\mathrm{Hom}(\mathcal{C}_L, E[\mathfrak{p}])^G$ is itself trivial.

Now, $\delta_1$ is also $G$-equivariant so that $\delta_1((\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}) = E[\mathfrak{p}]$. This, together with with the fact that $(\mathcal{O}_L^\times)^{\chi_E} \cong (\mathcal{O}_{L,\mathfrak{P}}^\times)^{\chi_E}$, implies that $\delta_1((\mathcal{O}_L^\times)^{\chi_E}) = E[\mathfrak{p}]$ and, in particular, $\delta_1(\mathcal{O}_L^\times) \neq 0$.

It then follows that $\mathrm{S}^{(\psi_E(\mathfrak{p}))}(E) = 0$ so by the exact sequence of Proposition A.6.2, we have $E(K)/\mathfrak{p}E(K) = 0$[1]. The Theorem now follows upon applying the Mordell-Weil Theorem. Indeed, suppose that $E(K)$ were infinite. Then the Mordell-Weil Theorem implies that $E(K) = E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$ for some $r \geq 1$. But then we would have that $E(K)/\mathfrak{p}E(K) \neq 0$ which is a contradiction. Hence $E(K)$ is finite as desired. □

The following Corollary shows that the Coates-Wiles Theorem holds even when we drop the assumption that $E$ has complex multiplication by the maximal order $\mathcal{O}_K$.

**Corollary 5.10.** *Let $K$ be a quadratic imaginary number field of class number 1 and $E/K$ an elliptic curve with complex multiplication by an order in $\mathcal{O}_K$. If $L(\overline{\psi_E}, 1) \neq 0$ then $E(K)$ is finite.*

*Proof.* By Proposition A.7.1, there exists an isogeny $\phi : E \to E'$ where $E'/K$ is an elliptic curve over $K$ that has complex multiplication by $\mathcal{O}_K$. Recall that the $L$-functions of isogenous elliptic curves are equal[2] (see [Kna92, Theorem 11.67]), so that $L(\overline{\psi_E}, 1) \neq 0$ if and only if $L(\overline{\psi_{E'}}, 1) \neq 0$. By the Coates-Wiles Theorem, $E'(K)$ is then

[1] This exact sequence also implies that the $\mathfrak{p}$-part of the Tate-Shafarevich group $\text{Ш}(E)_{\mathfrak{p}}$ is trivial.

[2] The idea behind this is that isogenous elliptic curves have the same reduction type and have the same number of $\mathbb{F}_{\mathfrak{p}}$-points for each prime $\mathfrak{p}$ of $K$. The Euler factors in the $L$-function then coincide.

finite. We now claim that the rank of elliptic curves is an isogeny invariant. Indeed, consider the exact sequence of abelian groups

$$0 \longrightarrow \ker\phi \longrightarrow E(K) \xrightarrow{\phi} E'(K) \longrightarrow 0$$

Since $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, we obtain an exact sequence

$$0 \longrightarrow \ker\phi \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\phi} E'(K) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow 0$$

But the kernel of an isogeny is necessarily finite and, in particular, torsion so $\ker\phi \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ whence $E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \cong E'(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. This implies that $\operatorname{rank}_{\mathbb{Z}}(E(K)) = \operatorname{rank}_{\mathbb{Z}}(E'(K))$ from which we may deduce that $E(K)$ is finite. □

*Remark.* The general case of an elliptic curve $E$ with complex multiplication by an order in an imaginary quadratic number field of non-trivial class number 1 can also be shown by similar techniques. The interested reader is encouraged to see [Sha87].

# Appendix

In this appendix we will give a brief exposition of definitions and well-known results from various fields which we employ in this essay. We shall only provide the proofs for results for which no suitable reference could be found. At the beginning of each section we shall mention relevant references where the reader may find all omitted proofs (and more).

## A.1 Class Field Theory

In this section we shall provide a concise exposition of the main results and concepts in global class field theory from both the ideal and idèlic perspectives. Class field theory is vast and we cannot hope to provide details of all the statements, let alone the proofs. That being said, the techniques and machinery provided by class field theory will be crucial to our proof of the Coates-Wiles Theorem and of the construction of elliptic units in general so it will be necessary to recall the most important elements of the theory. We shall not require much, if any, local class field theory but it will be useful for us to recall a few concepts from this theory as well. The main reference for this section will be [Dao17].

Let $K$ be a number field and denote by $\mathcal{O}_K$ its ring of integers. We shall write $G_K = \mathrm{Gal}(\bar{K}/K)$ for the absolute Galois group of $K$. By a *prime* $\mathfrak{p}$ of $K$, we mean an equivalence class of absolute values on $K$. Recall that by Ostrowski's Theorem, every absolute value $|\cdot|_\mathfrak{p}$ on $K$ is either a non-archimedean $\mathfrak{p}$-adic absolute value (with associated valuation $v_\mathfrak{p}$) or an archimedean absolute value. We may thus identify the primes of $K$ with prime ideals (henceforth the *finite primes*) of $\mathcal{O}_K$ and the field embeddings $K \hookrightarrow \mathbb{C}$ (henceforth the *infinite primes*). Given a prime $\mathfrak{p}$ of $K$, we shall write $K_\mathfrak{p}$ for its completion with respect to $\mathfrak{p}$. If $\mathfrak{p}$ is finite ($\mathfrak{p} \nmid \infty$) then we shall write $\mathcal{O}_{K,\mathfrak{p}}$ for its ring of integers. If $\mathfrak{p}$ is infinite ($\mathfrak{p} \mid \infty$) and corresponds to a real embedding we shall say that $\mathfrak{p}$ is *real*; if it corresponds to a complex embedding we shall say that $\mathfrak{p}$ is *complex*.

Let $L/K$ be a Galois extension of number fields and $\mathfrak{p}$ a finite prime of $K$. Then $\mathrm{Gal}(L/K)$ permutes the primes $\mathfrak{P}$ of $L$ lying over $\mathfrak{p}$ and this action is transitive. We define the *decomposition group* of $L/K$ relative to $\mathfrak{P}$ to be

$$\mathrm{Gal}(L/K)_\mathfrak{P} = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P} \,\}$$

It can be shown that $\mathrm{Gal}(L/K)_\mathfrak{P} \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Let $\mathbb{F}_\mathfrak{P} = \mathcal{O}_{L,\mathfrak{P}}/\mathfrak{P}$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_{K,\mathfrak{p}}$ be the residue fields of the completions. Then $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ surjects onto $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ via the reduction map.

Thanks to this surjection, we may make the following definitions. We define the *inertia group* $I_\mathfrak{P}$ of $L/K$ relative to $\mathfrak{P}$ to be the elements of $\mathrm{Gal}(L/K)_\mathfrak{P}$ that reduce to the trivial automorphism of $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. If $\mathfrak{p}$ is unramified in $L/K$ then $[L_\mathfrak{P} : K_\mathfrak{p}]$ is just the degree of the corresponding extension of residue fields and so $\mathrm{Gal}(L_\mathfrak{P}, K_\mathfrak{p}) \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}, \mathbb{F}_\mathfrak{p})$. In this case, we define the *Artin symbol* or *Frobenius element*, denoted $((L/K), \mathfrak{P})$ of $L/K$ relative to $\mathfrak{P}$ to be the unique element of $\mathrm{Gal}(L/K)_\mathfrak{P}$ that acts as Frobenius on $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$.

We recall that the Frobenius elements relative to primes above an unramified prime $\mathfrak{p}$ are conjugates. In other words, for all $\sigma \in \mathrm{Gal}(L/K)$ we have $((L/K), \sigma(\mathfrak{P})) = \sigma \circ ((L/K), \mathfrak{P}) \circ \sigma^{-1}$. We then define the Artin symbol of $\mathfrak{p}$ in $L/K$, denoted $((L/K), \mathfrak{p})$ to be the conjugacy class of $((L/K), \mathfrak{P})$ for any prime $\mathfrak{P}$ lying over $\mathfrak{p}$. We note that if $L/K$ is abelian then the conjugacy classes have a unique element and we identify $((L/K), \mathfrak{p})$ with its unique element.

Assume frome now on that $L/K$ is a finite abelian extension of number fields.

**Proposition A.1.1.** *Suppose that $\mathfrak{p}$ is a finite unramified prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Then $((L/K), \mathfrak{p}) = 1$ if and only if $\mathfrak{p}$ splits completely in $L$.*

Let $S$ be a set that contains all the primes of $K$ that ramify in $L$ and $I_K^S$ the subgroup of all fractional ideals of $K$ that do not contain a prime of $S$ in their factorisation. We define the *Artin map* to be the unique homomorphism $\varphi_{L/K}^S : I_K^S \to \mathrm{Gal}(L/K)$ that extends the Artin symbol.

Let $M_K$ be the set of all primes of $K$, $M_K^\infty$ the subset of infinite primes and $M_K^{\nmid\infty}$ the subset of finite primes. We define a **modulus** of $K$ to be a function $\mathfrak{m} : M_K \to \mathbb{Z}$ such that

1. $\mathfrak{m}(\mathfrak{p}) \geq 0$ for all $\mathfrak{p} \in M_K$ and $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p} \in M_K^{\nmid\infty}$.
2. $\mathfrak{m}(\mathfrak{p}) = 0$ or $1$ for all real primes $\mathfrak{p}$.
3. $\mathfrak{m}(\mathfrak{p}) = 0$ for all complex primes $\mathfrak{p}$.

We can write a modulus as a formal product $\mathfrak{m} = \prod_{\mathfrak{p} \in M_K} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$. Moreover, we can write $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ where $\mathfrak{m}_\infty$ is the real infinite part of $\mathfrak{m}$ and $\mathfrak{m}_0$ is the finite part of $\mathfrak{m}$ which can be identified with an integral ideal of $\mathcal{O}_K$. Given two moduli $\mathfrak{m}$ and $\mathfrak{n}$, we say that $\mathfrak{m}$ *divides* $\mathfrak{n}$ if $\mathfrak{m}(\mathfrak{p}) \leq \mathfrak{n}(\mathfrak{p})$ for all $\mathfrak{p} \in M_K$.

Let $\mathfrak{m}$ be a modulus of $K$ and $\alpha \in K^\times$. We say that $\alpha$ is *multiplicatively congruent* to 1 modulo $\mathfrak{m}$, denoted $\alpha \equiv 1 \pmod{^\times\, \mathfrak{m}}$, if

1. $\alpha \in 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_{\mathfrak{p},K}$ for all finite primes $\mathfrak{p}$ such that $\mathfrak{m}(\mathfrak{p}) > 0$.
2. $|\alpha|_\mathfrak{p} > 0$ for all real primes $\mathfrak{p}$ such that $\mathfrak{m}(\mathfrak{p}) > 0$.

We now define a series of notations. We let $I_K$ be the group of fractional ideals of $K$, $I_K^\mathfrak{m}$ the subgroup of fractional ideals of $K$ that are prime to a modulus $\mathfrak{m}$. Let $P_K$ be the subgroup of $I_K$ of principal ideals and similarly for $P_K^\mathfrak{m}$. Furthermore, we define $P_K^{\mathfrak{m},1} = \{ (\alpha) \in P_K^\mathfrak{m} \mid \alpha \equiv 1 \pmod{^\times\, \mathfrak{m}} \}$, $K^\mathfrak{m} = \{ \alpha \in K^\times \mid (\alpha) \in P_K^\mathfrak{m} \}$ and similarly for $K^{\mathfrak{m},1}$. Finally, we define the *ray class group* of $K$ modulo $\mathfrak{m}$ to be the factor group $C_K^\mathfrak{m} = I_K^\mathfrak{m}/P_K^{\mathfrak{m},1}$.

**Theorem A.1.2.** *Let $\mathfrak{m}$ be a modulus of $K$ and $\mathcal{C}_K$ the ideal class group of $K$. Then we have an exact sequence*

$$1 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}) \longrightarrow K^\mathfrak{m}/K^{\mathfrak{m},1} \longrightarrow C_K^\mathfrak{m} \longrightarrow \mathcal{C}_K \longrightarrow 1$$

*Furthermore, $K^\mathfrak{m}/K^{\mathfrak{m},1} \cong \{ \pm 1 \}^{|\mathfrak{m}_\infty|} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$. In particular, $C_K^\mathfrak{m}$ is finite.*

**Theorem A.1.3** (Class Field Theory)**.** *Let $\mathfrak{m}$ be a modulus for $K$. Then*

1. *(Existence) There exists an abelian extension of $K$, denoted $K(\mathfrak{m})$ and called the* ***ray class field*** *of $K$ modulo $\mathfrak{m}$, such that $C_K^\mathfrak{m} \cong \mathrm{Gal}(K(\mathfrak{m})/K)$ via the Artin map.*

2. *(Completeness) Every finite abelian extension of $K$ is contained in a ray class field of $K$ for some modulus $\mathfrak{m}$.*

3. *(Artin Recpirocity) For every intermediate field $L$ of $K(\mathfrak{m})/K$, the Artin map induces an isomorphism*

$$\varphi^{\mathfrak{m}}_{L/K} : \frac{I^{\mathfrak{m}}_K}{P^{\mathfrak{m},1}_K \mathbf{N}_{L/K} I^{\mathfrak{m}}_L} \to \mathrm{Gal}(L/K)$$

Consider the trivial modulus 1 of $K$. Then $H = K(1)$ is referred to as the *Hilbert class field* of $K$ and satisfies $\mathrm{Gal}(H/K) \cong \mathcal{C}_K$. It can be shown that $H$ is the maximal unramified abelian extension of $K$.

We now discuss the idèlic theory. Let $\{\, G_i \,\}_{i\in I}$ be a family of locally compact groups and $K_i \subseteq G_i$ an open compact subgroup for each $i \in S$ where $S \subseteq I$ is finite. We define the *restricted product* of the $G_i$ with respect to the $K_i$ to be

$$\prod_{i\in I\setminus S}^{K_i} G_i = \left\{ (g_i) \in \prod_{i\in I} G_i \;\middle|\; g_i \in K_i \text{ for all but finitely many } i \in I\setminus S \right\}$$

We equip the restricted product with the topology generated by the basis of open sets

$$\left\{ \prod_{i\in I} A_i \;\middle|\; A_i \text{ is open in } G_i \text{ and } A_i = K_i \text{ for all but finitely many } i \in I \right\}$$

It is an easy consequence of Tychonoff's Theorem that the restricted product is a locally compact group. We then define the *idèle group* of $K$ to be

$$\mathbb{I}_K = \prod_{\mathfrak{p}\in M_K\setminus M_K^\infty}^{\mathcal{O}^\times_{\mathfrak{p},K}} K^\times_{\mathfrak{p}}$$

It can be shown that $K^\times$ embeds as a discrete subgroup of $\mathbb{I}_K$ and so we define the *idèle class group* of $K$ to be $C_K = \mathbb{I}_K/K^\times$. An important result concerning $C_K$ is that its every open subgroup has finite index which is a consequence of the finiteness of the class number. If $x \in \mathbb{I}_K$, we define the *ideal associated* to $x$ to be $\prod_{\mathfrak{p}\in M_K^{\nmid\infty}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}$ and we define the *idealifier* to be the map $\mathfrak{J} : \mathbb{I}_K \to I_K$ sending an idèle to its associated ideal. Furthermore, we define the *idèle norm* to be the map $\mathbf{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ that sends $x \in \mathbb{I}_L$ to $y \in \mathbb{I}_K$ whose $\mathfrak{p}^{th}$ component is $\prod_{\mathfrak{P}/\mathfrak{p}} \mathbf{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} x_{\mathfrak{P}}$.

**Proposition A.1.4.** *Let $\mathfrak{m}$ be a modulus for $K$ and define the groups*

$$U_K^{\mathfrak{m}(\mathfrak{p})} = \begin{cases} \mathcal{O}^\times_{\mathfrak{p},K} & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{m}(\mathfrak{p}) = 0 \\ 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_{\mathfrak{p},K} & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{m}(\mathfrak{p}) > 0 \\ K^\times_{\mathfrak{p}} & \text{if } \mathfrak{p} \mid \infty, \mathfrak{m}(\mathfrak{p}) = 0 \\ \mathbb{R}^\times_{>0} & \text{if } \mathfrak{p} \text{ is real}, \mathfrak{m}(\mathfrak{p}) > 0 \end{cases}$$

*Denote $U_K^{\mathfrak{m}} = \prod_{\mathfrak{p}\in M_K} U_K^{\mathfrak{m}(\mathfrak{p})}$. Then*

1. *$U_K^{\mathfrak{m}}$ is an open subgroup of $\mathbb{I}_K$.*

2. *Every open subgroup of $\mathbb{I}_K$ contains $U_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.*

3. *$C_K/U_K^{\mathfrak{m}} \cong C_K^{\mathfrak{m}}$.*

**Theorem A.1.5** (Class Field Theory)**.** *Let $K^{\mathrm{ab}}$ be the maximal abelian extension of $K$. Then there is a continuous* *surjective homomorphism called the* ***Artin map***

$$[\cdot, K^{\mathrm{ab}}/K] : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

*For an intermediate abelian field $L$ of $K^{\mathrm{ab}}/K$ write $[\cdot, L/K] = [\cdot, K^{\mathrm{ab}}/K]|_L$. The Artin map satisfies the following properties:*

1. *(Artin Reciprocity) $[K^\times, K^{\mathrm{ab}}/K] = 1$ and so the Artin map descends to a homomorphism $C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ which induces an isomorphism*

$$[\cdot, K^{\mathrm{ab}}/K] : \widehat{C_K} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

*where $\widehat{C_K}$ is the profinite completion of $C_K$. Furthermore, for every finite abelian extension $L/K$, we have an isomorphism*

$$[\cdot, L/K] : C_K/\,\mathbf{N}_{L/K}\, C_L \to \mathrm{Gal}(L/K)$$

2. *(Existence) For every finite-index open subgroup $N$ of $C_K$, there exists a unique abelian extension $L/K$ such that $N = \mathbf{N}_{L/K}\, C_L$. In particular, for every modulus $\mathfrak{m}$ of $K$, the ray class field $K(\mathfrak{m})$ is the unique abelian extension such that $\mathbf{N}_{K(\mathfrak{m})/K}\, C_{K(\mathfrak{m})} = U_K^{\mathfrak{m}}$.*

3. *(Compatibility) Let $L/K$ be a finite abelian extension and $x \in \mathbb{I}_K$ be an idèle such that $\mathfrak{I}(x)$ is prime to all finite primes of $K$ that ramify in $L$. Then*

$$[x, L/K] = \left(\frac{L/K}{\mathfrak{I}(x)}\right)$$

4. *(Norm Restriction) Let $L/K$ be an extension of number fields. Then*

$$[x, L^{\mathrm{ab}}/L] = [\mathbf{N}_{L/K}\, x, K^{\mathrm{ab}}/K]$$

Let $K$ be a number field and $\mathfrak{p}$ a finite prime of $K$. We define the *local Artin map* $[\cdot, K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}}] : \widehat{K_{\mathfrak{p}}^{\times}} \to \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}})$ to be the restriction of the global Artin map to $K_{\mathfrak{p}}^{\times}$ considered as a subgroup of $\mathbb{I}_K$.

The following is a celebrated theorem from classical Class Field Theory. For a proof, see [Tri].

**Theorem A.1.6** (Chebotarev Density Theorem)**.** *Let $L/K$ be a Galois extension of number fields and $C \subseteq \mathrm{Gal}(L/K)$ a conjugacy class. Then there are infinitely many finite primes of $K$ that do not ramify in $L$ such that $((L/K), \mathfrak{p}) = C$.*

The following Proposition is not directly related to Class Field Theory but this is the most appropriate section for it to be included in. For a proof, see [Ash10, 6.3.1].

**Proposition A.1.7.** *Let $K$ be an imaginary quadratic number field. Then $|\mathcal{O}_K^\times| = 2, 4$ or 6.*

## A.2 Galois Cohomology

Our next discussion will be regarding Galois cohomology. The main references for this section are [Sil09, Appendix B] and [Ser97, §2].

Let $G$ be a profinite group and $M$ an abelian group equipped with the discrete topology on which $G$ acts. Denote by $m^\sigma$ the action of $\sigma \in G$ on $m \in M$. We say that $M$ is a *$G$-module* if the action of $G$ on $M$ is continuous and is compatible with the module structure of $M$. A *homomorphism* of $G$-modules $M$ and $N$ is a group homomorphism $M \to N$ that commutes with the action of $G$.

From now on, fix a $G$-module $M$. We define the group of *$n$-cochains*, denoted $C^n(G,M)$, to be the group of all continuous functions from $G^n \to M$. We define the *coboundary* homomorphisms to be the maps $d^{n+1} : C^n(G,M) \to C^{n+1}(G,M)$ given by the formula

$$\begin{aligned}(d^{n+1}\varphi)(g_1,\dots,g_{n+1}) = g_1\varphi(g_2,\dots,g_{n+1}) + \sum_{i=1}^{n}(-1)^i\varphi(g_1,\dots,g_{i-1},g_ig_{i+1},g_{i+2},\dots,g_{n+1})\\ + (-1)^{n+1}\varphi(g_1,\dots,g_n)\end{aligned}$$

It can be checked that $d^{n+1} \circ d^n = 0$. For all $n \geq 0$, we define the group of *$n$-cocycles* to be $Z^n(G,M) = \ker(d^{n+1})$ and the group of *$n$-cocycles* to be $B^n(G,M) = \mathrm{im}(d^n)$ for $n \geq 1$ and 0 when $n = 0$. We then define the *$n$-cohomology* group to be the factor group $H^n(G,M) = Z^n(G,M)/B^n(G,M)$. For our purposes, it will be sufficient to give explicit descriptions for the $0^{th}$ and $1^{st}$-cohomology groups. We have that

$$\begin{aligned}
&H^0(G,M) = M^G = \{\, m \in M \mid m^\sigma = m \text{ for all } \sigma \in G \,\}\\
&Z^1(G,M) = \{\, c \in C^1(G,M) : c(\sigma\tau) = c(\sigma)^\tau + c(\tau) \,\}\\
&B^1(G,M) = \{\, c \in C^1(G,M) \mid \text{ there exists } m \in M \text{ such that } c(\sigma) = m^\sigma - m \text{ for all } \sigma \in G \,\}
\end{aligned}$$

We observe that if $M$ is a $G$-module via the trivial action then $H^0(G,M) = M$ and $H^1(G,M) = \mathrm{Hom}_{\mathrm{cont}}(G,M)$.

**Proposition A.2.1.** *Let*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

*be a short exact sequence of $G$-modules. Then there exists a long exact sequence of cohomology groups*

$$\begin{tikzcd}
0 \arrow[r] & H^0(G,P) \arrow[r, "\phi^0"] & H^0(G,M) \arrow[r, "\psi^0"] & H(G,N) \arrow[dll, "\delta"] \\
& H^1(G,P) \arrow[r, "\phi^1"] & H^1(G,M) \arrow[r, "\psi^1"] & H^1(G,N)
\end{tikzcd}$$

*where the $\phi^*$ and $\psi^*$ are the induced homomorphisms of cohomology groups and $\delta$ is the connecting homomorphism defined as follows. Fix $n \in H^0(G,N)$ and choose $m \in M$ such that $\psi(m) = n$. Define the cochain $f \in C^1(G,M)$ by $f(\sigma) = m^\sigma - m$ and set $\delta(n) = [f]$.*

Let $H$ be a subgroup of $G$. Then any $G$-module is naturally an $H$-module via restriction of the group action. We define the *restriction* homomorphism of cohomology groups to be $\mathrm{res} : H^1(G,M) \to H^1(H,M)$ given by restriction of the domain of cochains to $H$. Now suppose that $H$ is normal in $G$. Then $M^H$ is naturally a $G/H$-module. Given a 1-cochain $f : G/H \to M^H$, we may compose $f$ with the projection $G \to G/H$ and the inclusion $M^H \subseteq M$ to obtain an *inflation* homomorphism of cohomology groups $\inf : H^1(G/H, M^H) \to H^1(G,M)$.

**Proposition A.2.2.** *Let $M$ be a $G$-module and $H$ a normal subgroup of $G$. Then we have an exact sequence*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\inf} H^1(G,M) \xrightarrow{\mathrm{res}} H^1(H,M)^{G/H} \longrightarrow H^2(G/H, M^H)$$

Let $K$ be a perfect field so that $G_K$ is a profinite group. Then a $G_K$-module is an abelian group with an action of the absolute Galois group $G_K$. We shall often write simply $H^1(K,M)$ in the place of $H^1(G_K,M)$.

**Proposition A.2.3** (Hilbert's Theorem 90)**.** *Let $K$ be a perfect field. Then $H^1(K, \overline{K}^\times) = 0$*

**Proposition A.2.4.** *Let $K$ be a perfect field such that* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K) \nmid m$*. Then $H^1(K, \boldsymbol{\mu}_m) \cong K^\times/(K^\times)^m$.*

## A.3 Character Theory

In this section we discuss certain key concepts concerning characters of finite groups. For any finite abelian group $G$, let $\widehat{G}$ denote its character group consisting of all characters of $G$ into an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Let $G$ be a finite abelian group and $\chi \in \widehat{G}$ a character. We define the *$\chi$-idempotent* in the group ring $\overline{\mathbb{Q}}[G]$ to be

$$\varepsilon_\chi = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}$$

The following Proposition provides us with the key properties of the $\chi$-idempotent. Since the proof is straightforward, we provide it for completeness.

**Proposition A.3.1.** *Let $G$ be a finite abelian group and $\chi \in \widehat{G}$ a character. Then the $\chi$-idempotent is indeed an idempotent element of the group ring $\overline{\mathbb{Q}}[G]$. Moreover,*

1. *Given another character $\chi \neq \psi \in \widehat{G}$ we have $\varepsilon_\chi\varepsilon_\psi = 0$.*
2. *$\sum_{\chi\in\widehat{G}}\varepsilon_\chi = 1$.*
3. *For all $\sigma \in G$ we have $\varepsilon_\chi\sigma = \chi(\sigma)\varepsilon_\chi$.*

*Proof.* We first show that $\varepsilon_\chi$ is idempotent. Indeed,

$$\begin{aligned}\varepsilon_\chi^2 = |G|^{-2}\left(\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\right)\left(\sum_{\tau\in G}\chi(\tau^{-1})\tau\right) &= |G|^{-2}\sum_{\sigma\in G}\sigma\left(\sum_{\tau\in G}\chi(\tau^{-1})\chi(\tau\sigma^{-1})\right)\\ &= |G|^{-2}\sum_{\sigma\in G}\sigma\left(|G|\chi(\sigma^{-1})\right)\\ &= \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma = \varepsilon_\chi\end{aligned}$$

Now suppose that $\psi$ is another character of $G$ distinct from $\chi$. By the orthogonality of characters, we have that

$$\begin{aligned}\varepsilon_\chi\varepsilon_\psi = |G|^{-2}\left(\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\right)\left(\sum_{\tau\in G}\psi(\tau^{-1})\tau\right) &= |G|^{-2}\sum_{\sigma\in G}\left(\sum_{\tau\in G}\chi(\tau^{-1})\psi(\tau\sigma^{-1})\right)\\ &= |G|^{-2}\sum_{\sigma\in G}\psi(\sigma^{-1})\left(\sum_{\tau\in G}\chi(\tau^{-1})\psi(\tau)\right) = 0\end{aligned}$$

Since $\sum_{\chi\in\widehat{G}}\chi(g) = |G|$ if $g = 1$ and $0$ otherwise, the summation assertion follows immediately. Finally, fix $\sigma \in G$. Then

$$\varepsilon_\chi\sigma = \frac{1}{G}\sum_{\tau\in G}\chi(\tau)\tau^{-1}\sigma = \frac{1}{|G|}\sum_{\gamma\in G}\chi(\gamma^{-1}\sigma)\gamma = \chi(\sigma)\varepsilon_\chi$$

which proves the final assertion. □

**Proposition A.3.2.** *Let $M$ be a $\overline{\mathbb{Q}}[G]$-module. Then $M$ admits a decomposition into $\overline{\mathbb{Q}}[G]$-submodules of $M$, $M = \bigoplus_{\chi\in\widehat{G}} M^\chi$ where $M^\chi = \varepsilon_\chi M$ is the so-called* ***$\chi$-eigenspace*** *of $M$.*

*Proof.* By Part 2 of Proposition A.3.1, it follows that $M$ is the sum of the $M^\chi$. To see that it is in fact a direct sum, suppose that $M^\chi$ and $M^\psi$ are two distinct eigenspaces. We need to show that $M^\chi \cap M^\psi = \{0\}$. To this end, suppose that $\alpha$ is an element of both $M^\chi$ and $M^\psi$. Then $\alpha = m^\chi$ and $\alpha = n^\psi$ for some $m, n \in M$ so that $m^\chi = n^\psi$. By the idempotency of $\varepsilon$, we have that $m^\chi = (n^\psi)^\chi$. Appealing to the orthogonality of $\varepsilon$ yields $m^\chi = 0$. □

*Remark.* We observe that if $R$ is a commutative ring containing the images of every $\chi \in \widehat{G}$ and in which $|G|$ is a unit, then the above results all hold completely analogously for the group ring $R[G]$.

## A.4 Elliptic Curves over the Complex Numbers

In this section we shall state results and definitions of the analytic theory of elliptic curves defined over $\mathbb{C}$. The main references for this section are [Sil09, Chapter VI] and [Sil94, §I.5]. Fix a lattice $L \subseteq \mathbb{C}$. We define the *Weierstrass functions*

$$\zeta(z; L) = \frac{1}{z} \sum_{0 \neq w \in L} \left( \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right)$$

$$\wp(z; L) = \frac{1}{z^2} \sum_{0 \neq w \in L} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

$$\sigma(z; L) = z \prod_{0 \neq w \in L} \left( 1 - \frac{z}{w} \right) e^{(z/w) + \frac{1}{2}(z/w)^2}$$

Furthermore, let $\mathrm{covol}(\mathbb{C}/L)$ be the covolume of a fundamental paralellogram for $L$. We define

$$A(L) = \pi^{-1} \, \mathrm{covol}(\mathbb{C}/L)$$

$$s_2(L) = \lim_{s \to 0^+} \sum_{0 \neq w \in L} w^{-2s} |w|^{-2s}$$

$$G_k(L) = \sum_{0 \neq w \in L} \frac{1}{w^k}, k \in \mathbb{N}_{\geq 4} \text{ and } k \text{ even}$$

We finally define the *quasi-period* map to be

$$\eta(z; L) = A(L)^{-1} \overline{z} + s_2(L) z$$

The main properties of the Weierstrass functions of interest to us are summarised in the following proposition.

**Proposition A.4.1.**

1. *$\sigma(z; \Lambda)$ defines a holomorphic function on $\mathbb{C}$ with simple zeroes on $L$ and no other zeroes.*

2. *For all $z \in \mathbb{C}$ we have*

$$\frac{d}{dz} \zeta(z; L) = -\wp(z; L), \quad \frac{d}{dz} \log(\sigma(z; L)) = \zeta(z; L)$$

3. *For all $z \in \mathbb{C}$ and $w \in L$ we have*

$$\sigma(z + w; L) = \psi(w) e^{\eta(w)(z + \frac{1}{2} w)} \sigma(z, L)$$

*where $\psi : L \to \{\pm 1\}$ is defined by $\psi(w) = 1$ if $w \in 2L$ and $\psi(w) = -1$ if $w \notin 2L$.*

**Theorem A.4.2.** *There is an equivalence of categories*

$$\left\{ \begin{array}{c} \textit{Objects: Elliptic curves defined over } \mathbb{C} \\ \textit{Morphisms: Isogenies} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{Objects: Lattices } L \subseteq \mathbb{C} \textit{ up to homothety} \\ \textit{Morphisms: } \operatorname{Hom}(L_1, L_2) = \{\, \alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2 \,\} \end{array} \right\}$$

This correspondence can be made explicit in the following way. Suppose that we are given a lattice $L \subseteq \mathbb{C}$. Then the Weierstrass equation $y^2 = x^3 - 15G_4(L)x - 35G_6(L)$ defines an elliptic curve $E/\mathbb{C}$ and we have an analytic isomorphism

$$\begin{aligned} \xi : \mathbb{C}/L &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z; L), \wp'(z; L)/2) \end{aligned}$$

Moreover, the discriminant and $j$-invariant of $E$ are given by

$$\begin{aligned} \Delta(L) &= (60G_4(L))^3 - 27(140G_6(L))^2 \\ j(L) &= -1728(60G_4(L))^3/\Delta(L) \end{aligned}$$

Conversely, suppose that we are given an elliptic curve $E/\mathbb{C}$ with a fixed Weierstrass model $y^2 = x^3 + ax + b$. Then the Uniformisation Theorem guarantees the existence of a lattice $L \subseteq \mathbb{C}$ such that $15G_4(L) = -a$ and $35G_6(L) = -b$.

We note that this correspondence identifies the holomorphic invariant differential of an elliptic curve $\omega_E$ with the differential $dz$.

Recall that en *elliptic function* relative to $L$ is a meromorphic function $f(z)$ on $\mathbb{C}$ that is periodic with respect to $L$. In other words, for all $z \in \mathbb{C}$ and $w \in L$ we have

$$f(z + w) = f(z)$$

We denote by $\mathbb{C}(L)$ the field of all elliptic functions relative to $L$.

**Proposition A.4.3.** *Let $L \subseteq \mathbb{C}$ be a lattice. Then*

$$\mathbb{C}(L) = \mathbb{C}(\wp(z), \wp'(z))$$

## A.5 Elliptic Curves over Non-Archimedean Local Fields

We will now recall key results concerning elliptic curves over local fields. The main references for this section are [Rub99, §3] and [Sil09, Chapter VII].

Fix a rational prime $p$ and a finite extension $F$ of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_F$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_F$ and $\pi$ a uniformiser for $\mathfrak{p}$ so that $\mathbb{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$ is the residue field of $F$. Let $v_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation on $F$, normalised so that $v_\mathfrak{p}(\pi) = 1$.

Let $E$ be an elliptic curve defined over $F$. We say that a particular Weierstrass model with coefficients in $\mathcal{O}_F$ of $E$ is *minimal* with respect to $v_\mathfrak{p}$ if the valuation of its discriminant is minimal amongst all the valuations of discriminants of such Weierstrass models. From now on, we fix a minimal model of $E$ with minimal discriminant $\Delta$. We define the *reduction* of $E$, denoted $\overline{E}$, to be the curve given by reducing the coefficients of the Weierstrass model of $E$ modulo $\mathfrak{p}$. It can be shown that such a curve is independent of the choice of minimal model of $E$ and has, at most, one singular point. We denote by $\overline{E}_{\mathrm{ns}}$ the quasi-projective curve obtained by removing the singular point from $\overline{E}$ which is also an abelian group. Denote by $E_0(F)$ all the points of $E$ with non-singular reduction and $E_1(F)$ the kernel of reduction.

**Proposition A.5.1.** *There exists an exact sequence of abelian groups*

$$0 \longrightarrow E_1(F) \longrightarrow E_0(F) \longrightarrow \overline{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \longrightarrow 0$$

**Proposition A.5.2.** *We have that*

$$E_1(F) = \{\, (x,y) \in E(F) \mid v_{\mathfrak{p}}(x) < 0 \,\} = \{\, (x,y) \in E(F) \mid v_{\mathfrak{p}}(y) < 0 \,\}$$

*Moreover, if $(x,y) \in E_1(F)$ then $3v(x) = 2v(y)$.*

We say that $E$ has *good reduction* if $\Delta \in \mathcal{O}_F^\times$ and $\overline{E}$ is non-singular. If not then $\overline{E}$ is always singular and we say that $E$ has *bad reduction.* Moreover, we say that $E$ has *potentially good reduction* if there exists a finite extension of $F$ over which $E$ has good reduction.

**Proposition A.5.3.** *Suppose that $E$ has good reduction. Then the reduction map $E(F) \to \overline{E}(\mathbb{F}_{\mathfrak{p}})$ induces an injection of endomorphism rings $\mathrm{End}_F(E) \to \mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\overline{E})$ which sends an endomorphism of $E$ to its corresponding endomorphism $\overline{\phi}$ of $E$.*

**Proposition A.5.4.** *Suppose that $E$ has good reduction and let $\phi \in \mathrm{End}_F(E)$ be such that $\overline{\phi}$ is purely inseparable. Then $\overline{\phi}$ is injective and $\ker(\phi) \subseteq E_1(F)$.*

Recall that $E$ admits a formal group $\widehat{E}$ with formal group law $\mathcal{F}_E \in \mathcal{O}_F[[Z,Z']]$. Moreover, we have a power series $w(Z) = Z^3 \sum_{i=0}^{\infty} A_i Z^i$ for some $A_i \in \mathbb{Z}[a_1,\ldots,a_6]$ and power series $x(Z) = Z/w(Z)$ and $y(Z) = -1/w(Z)$ giving an $F((Z))$-rational point $(x(Z), y(Z))$ of $E$. $x(Z)$ and $y(Z)$ are compatible with the formal group law in the following sense

$$(x(Z), y(Z)) + (x(Z'), y(Z')) = (x(\mathcal{F}_E(Z,Z')), y(\mathcal{F}_E(Z,Z')))$$

We also have a map $\mathrm{End}_F(E) \to \mathrm{End}(\widehat{E})$ that takes an endomorphism $\phi$ of $E$ and maps it to an endomorphism $\Phi$ of $\widehat{E}$ satisfying $\phi(x(Z), y(Z)) = (x(\Phi(Z)), y(\Phi(z))$. Given $n \in \mathbb{N}_{\geq 1}$, we let $\widehat{E}(\mathfrak{p}^n)$ be the abelian group on the set $\mathfrak{p}^n$ with group law given by $(x,x') \mapsto \mathcal{F}_E(x,x')$.

**Proposition A.5.5.** *We have an isomorphism*

$$\begin{aligned} \widehat{E}(\mathfrak{p}) &\to E_1(F) \\ Z &\mapsto (x(Z), y(Z)) \end{aligned}$$

*with inverse given by the map $(x,y) \mapsto -x/y$.*

**Proposition A.5.6.** *Suppose that $E$ has good reduction and let $q$ be the cardinality of the residue field of $F$. If $\phi \in End_F(E)$ reduces to the Frobenius endomorphism $\phi_q$ of $\overline{E}$ then $\Phi(Z) \equiv Z^q \pmod{\mathfrak{p}\mathcal{O}_F[[Z]]}$.*

We now recall that we have a formal analogue of the invariant differential given by

$$\widehat{\omega}(Z) = \frac{x'(Z)}{2y(Z) + a_1 x(Z) + a_3}$$

We next define the formal logarithm map $\lambda_{\widehat{E}}(Z)$ to be the unique power series such that $\lambda'_{\widehat{E}}(Z) = \widehat{w}(Z)$ which converges on $\mathfrak{p}$ and induces an isomorphism $\widehat{E}(\mathfrak{p}) \to \mathfrak{p}$ when $v_{\mathfrak{p}}(p) < p-1$. We furthermore define the logarithm map of $E$ $\lambda_E : E_1(F) \to F$ to be the composition of the isomorphism of Proposition A.5.5 with the inverse of the isomorphism of $\lambda_{\widehat{E}}$. Hence if $v_{\mathfrak{p}}(p) < p-1$ then $\lambda_E : E_1(F) \to \mathfrak{p}$ is an isomorphism.

Let $\mathcal{D}_F(E) \cong F$ be the vector space of one-dimensional holomorphic differentials on $E$ defined over F. Every endomorphism $\phi$ of $E$ induces an endomorphism $\phi^*$ of $\mathcal{D}_F(E)$ and we therefore have an injective homomorphism of abelian groups[1]

$$\iota : \mathrm{End}_F(E) \to \mathrm{End}_F(\mathcal{D}_F(E)) \cong F$$

**Proposition A.5.7.** *Let $\phi \in \mathrm{End}_F(E)$. If $\iota(\phi) \in \mathcal{O}_F^\times$ then $\phi$ is an automorphism of $E_1(F)$. Moreover, if $E$ has good reduction then the reduction homomorphism $E[\phi] \cap E(F) \to \overline{E}(\mathbb{F}_{\mathfrak{p}})$ is injective.*

**Proposition A.5.8.** *Suppose $E$ has good reduction and let $\phi \in \mathrm{End}_F(E)$ be an endomorphism such that $\iota(\phi) \in \mathcal{O}_F^\times$. If $P \in E(\overline{F}))$ is such that $\phi(P) \in E(F)$ then the extension $F(E[\phi], P)/F$ (obtained by adjoining the coordinates of the relevant points) is unramified.*

## A.6 Elliptic Curves over Global Fields

We next recall key results about elliptic curves over number fields. The main references for this section are [Sil09, §VIII.4] and [Sil09, §X.4].

Let $K$ be a number field and $E$ an elliptic curve defined over $K$. Let $\mathfrak{p}$ be a finite prime of $K$. We say that $E$ has *good* (respectively *bad* and *potentially good*) reduction at $\mathfrak{p}$ if $E/K_{\mathfrak{p}}$ does. Let $\Delta_{\mathfrak{p}}(E)$ be the minimal discriminant of $E/K_{\mathfrak{p}}$. Since $E$ has only finitely many primes of bad reduction, we may define the *minimal discriminant* of $K$ to be $\Delta(E) = \prod_{\mathfrak{p} \in M_K^{\nmid\infty}} \Delta_{\mathfrak{p}}(E)$.

**Theorem A.6.1** (Mordell-Weil). *$E(K)$ is a finitely generated abelian group.*

We now identify $\mathrm{End}_K(E)$ with its image $\mathcal{O} \subseteq K$ under the map $\iota$. It can be shown that $\mathcal{O}$ is either $\mathbb{Z}$ or an order in an imaginary quadratic number field[2] Fix a non-constant endomorphism $\alpha \in \mathcal{O}$ of $E$, let $E[\alpha]$ denote its kernel on $\overline{K}$ and $K(E[\alpha])$ the finite extension of $K$ gven by adjoining the coordinates of the points in $E[\alpha]$ to $K$. Since multiplication by $\alpha$ is surjective we have an exact sequence of abelian groups

$$0 \longrightarrow E[\alpha] \longrightarrow E(\overline{K}) \xrightarrow{\alpha} E(\overline{K}) \longrightarrow 0$$

Note that each of these abelian groups admits a natural $G_K$-action given by the $G_K$-action on the coordinates. In particular, they are $G_K$-modules so passing to $G_K$-cohomology yields a long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^0(K, E[\alpha]) \arrow[r] & E(K) \arrow[r, "\alpha^0"] & E(K) \arrow[dll, "\delta"] \\ & H^1(K, E[\alpha]) \arrow[r] & H^1(K, E) \arrow[r, "\alpha^1"] & H^1(K, E) \end{tikzcd}$$

where we have written $H^1(K, E) = H^1(K, E(\overline{K}))$ to ease notation. Writing $H^1(K, E)_\alpha$ for the kernel of $\alpha^1$, this may be written as a short exact sequence

[1] Note that this definition works for elliptic curves over arbitrary fields but it is only injective if the characteristic of the defining field is 0.

[2] This much is true for any elliptic curve over a characteristic 0 field. If the characteristic is not 0 then $\mathcal{O}$ may be an order in a quaternion algebra over $\mathbb{Q}$.

$$0 \longrightarrow E(K)/\alpha E(K) \xrightarrow{\delta} H^1(K, E[\alpha]) \longrightarrow H^1(K, E)_\alpha \longrightarrow 0$$

Given a prime $\mathfrak{p}$ of $K$, we may repeat the same process with $E$ considered as defined over $K_\mathfrak{p}$ to obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & E(K)/\alpha E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\alpha]) \arrow[r] \arrow[d, "\mathrm{res}"] \arrow[dr, dotted] & H^1(K, E)_\alpha \arrow[r] \arrow[d, "\mathrm{res}"] & 0 \\
0 \arrow[r] & \prod\limits_{\mathfrak{p} \in M_K} E(K_\mathfrak{p})/\alpha E(K_\mathfrak{p}) \arrow[r, "\delta"] & \prod\limits_{\mathfrak{p} \in M_K} H^1(K_\mathfrak{p}, E[\alpha]) \arrow[r] & \prod\limits_{\mathfrak{p} \in M_K} H^1(K_\mathfrak{p}, E)_\alpha \arrow[r] & 0
\end{tikzcd}$$

Explicitly, the second vertical map res is given coordinate-wise by the cohomological restriction map $H^1(K, E[\alpha]) \xrightarrow{\mathrm{res}_\mathfrak{p}} H^1(K_\mathfrak{p}, E[\alpha])$ and similarly for the third one. We define the *$\alpha$-Selmer group*, denoted $\mathrm{S}^{(\alpha)}(E)$, to be the kernel of the dotted homomorphism in the diagram above. Since the rows are exact, we have the following two equivalent definitions for the $\alpha$-Selmer group

$$\begin{aligned}
\mathrm{S}^{(\alpha)}(E) &= \ker\left( H^1(K, E[\alpha]) \to \prod_{\mathfrak{p} \in M_K} H^1(K_\mathfrak{p}, E[\alpha]) \right) \\
&= \{\, c \in H^1(K, E[\alpha]) \mid \mathrm{res}_\mathfrak{p} \in \mathrm{im}(\delta_\mathfrak{p}) \text{ for all } \mathfrak{p} \in M_K \,\}
\end{aligned}$$

It can be shown that the $\alpha$-Selmer group of $E$ is finite. Moreover, we define the *Tate-Shafarevich group* of $E$, denoted $\text{Ш}(E)$ to be

$$\text{Ш}(E) = \ker\left( H^1(K, E) \to \prod_{\mathfrak{p} \in M_K} H^1(K_\mathfrak{p}, E) \right)$$

The non-trivial elements of the Tate-Shafarevich group can be interpreted as the homogeneous spaces of $E$ that have $K_\mathfrak{p}$-rational points for every prime $\mathfrak{p}$ of $K$ but no $K$-rational points. In other words, the Tate-Shafarevich group is a measure of how well $E$ satisfies the Hasse principal - if $\text{Ш}(E)$ is trivial then the Hasse principle holds. It is an important and long-standing conjecture that the Tate-Shafarevich group is finite. Rubin verified this for particular elliptic curves with complex multiplication using many of the methods we develop in this essay.

**Proposition A.6.2.** *Let $\alpha \in \mathcal{O}$ be a non-constant endomorphism of $E$. Then there exists an exact sequence*

$$0 \longrightarrow E(K)/\alpha E(K) \longrightarrow \mathrm{S}^{(\alpha)}(E) \longrightarrow \text{Ш}(E)_\alpha \longrightarrow 0$$

*In particular, if $\mathrm{S}^{(\alpha)}(E)$ is trivial then so is $E(K)/\alpha E(K)$ and $\text{Ш}(E)_\alpha$.*

## A.7 Complex Multiplication

In this final preliminary section, we discuss results about elliptic curves with complex multiplication. The main reference for this section is [Rub99, §5].

Let $L$ be a subfield of $\mathbb{C}$ and $E/L$ an elliptic curve. We say that $E$ has *complex multiplication* if $\mathrm{End}_L(E) \supsetneq \mathbb{Z}$. In this case, $\mathrm{End}_L(E)$ is an order $\mathcal{O}$ in an imaginary quadratic number field. Let $K = \mathbb{Q}\mathcal{O}$ be the imaginary quadratic field containing $\mathcal{O}$. Given an ideal $\mathfrak{a} \lhd \mathcal{O}$, we write $E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} E[\alpha]$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ then we write $E[\mathfrak{p}^\infty] = \bigcup_{n \in \mathbb{N}_{\geq 1}} E[\mathfrak{p}^n]$. Via the correspondence in Theorem A.4.2, we may fix a lattice $\Lambda \subseteq \mathbb{C}$ and an analytic isomorphism $\mathbb{C}/\Lambda \xrightarrow{\xi} E(\mathbb{C})$. We may scale $\Lambda$ by a constant in $\mathbb{C}$ so that $\Lambda \subseteq K$ whence $\Lambda$ is a fractional ideal of $\mathcal{O}$.

**Proposition A.7.1.** *There exists an isogeny $\phi : E \to E'$ where $E'$ is an elliptic curve defined over $L$ with complex multiplication by the maximal order $\mathcal{O}_K$.*

In light of this Proposition, we may assume that $E$ has complex multiplication by $\mathcal{O}_K$.

**Theorem A.7.2.** *Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a non-trivial ideal. Then $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$ as $\mathcal{O}_K$-modules. Via the analytic isomorphism $\xi$ we then also have that $\mathfrak{a}^{-1}\Lambda/\Lambda \cong \mathcal{O}_K/\mathfrak{a}$. Moreover, this isomorphism induces an injection $\mathrm{Gal}(L(E[\mathfrak{a}])/L) \hookrightarrow \mathcal{O}_K/\mathfrak{a}^\times$. In particular, $L(E[\mathfrak{a}])/L$ is an abelian extension.*

**Theorem A.7.3.** *Let $l$ be a rational prime and $F$ a finite extension of $\mathbb{Q}_l$. Then*

1. *$E$ has potentially good reduction.*
2. *If $\mathfrak{p}$ is a prime of $K$ not dividing $l$ and $n \in \mathbb{N}_{\geq 1}$ is such that $1 + \mathcal{O}_{K,\mathfrak{p}}$ is torsion free then $E$ has good reduction when considered defined over $F(E[\mathfrak{p}^n])$ at all primes not dividing $\mathfrak{p}$.*

The next two Theorems are consequences of the Fundamental Theorem of Complex Multiplication (see [Rub99, Theorem 5.11]).

**Proposition A.7.4.** *Let $H$ be the Hilbert class field of $K$. Then there exists an elliptic curve defined over $H$ with complex multiplication by $\mathcal{O}_K$ which is isomorphic to $E$ over $\mathbb{C}$.*

Recall that a *Hecke character* of a number field $L$ is a homomorphism of groups $\psi : \mathbb{I}_L/L^\times \to \mathbb{C}^\times$. We say that $\psi$ is *unramified* at a prime $\mathfrak{P}$ of $K$ if $\psi(\mathcal{O}_{K,\mathfrak{P}}^\times) = 1$.

**Theorem A.7.5.** *There exists a Hecke character $\psi_E : \mathbb{I}_L/L^\times \to \mathbb{C}^\times$ associated to $E$ such that*

1. *The conductor $\mathfrak{f}$ of $\psi_E$ is divisible by exactly the primes of bad reduction of $E$.*
2. *If $x \in \mathbb{I}_L$ is an idèle and $y = \mathbf{N}_{L/K}(x) \in \mathbb{I}_K$ is the idèle norm of $x$ then*
$$\psi_E(x)\mathcal{O}_K = y_\infty^{-1}\mathfrak{J}(y)\mathcal{O}_K$$
*where $y_\infty$ is the component of $y$ corresponding to the unique complex prime of $K$.*
3. *If $x \in \mathbb{I}_L$ is an idèle taking the value 1 on all infinite primes of $L$ and $\mathfrak{p}$ is a finite prime of $K$ then $\psi_E(x)(\mathbf{N}_{L/K}(x))_\mathfrak{p}^{-1} \in \mathcal{O}_{K,\mathfrak{p}}^\times$. Moreover, for all $P \in E[\mathfrak{p}^\infty]$ we have*
$$[x, L^{\mathrm{ab}}/L]P = \psi_E(x)(\mathbf{N}_{L/K}(x))_\mathfrak{p}^{-1}P$$
4. *If $\mathfrak{P}$ is a finite prime of $L$ then $\psi_E$ is unramified at $\mathfrak{P}$ if and only if $E$ has good reduction at $\mathfrak{P}$.*

Any Hecke character of conductor $\mathfrak{f}$ yields a Hecke character in the classical sense $\psi : I_L^\mathfrak{f} \to \mathbb{C}^\times$ (see [CF67, §VIII.1]). We may thus translate the above Theorem to the classical sense as follows

**Theorem A.7.6.** *Let $\mathfrak{f} \lhd \mathcal{O}_L$ be ideal given by the product of all primes of bad reduction of $E$. Then there exists a Hecke character $\psi_E : I_L^\mathfrak{f} \to \mathbb{C}^\times$ such that*

1. *For all ideals $\mathfrak{b} \lhd \mathcal{O}_L$ prime to $\mathfrak{f}$ we have $\psi_E(\mathfrak{b})\mathcal{O}_K = \mathbf{N}_{L/K}(\mathfrak{b})\mathcal{O}_K$.*
2. *Given a finite prime $\mathfrak{P}$ of $L$ and an ideal $\mathfrak{b} \lhd \mathcal{O}_L$ both prime to $\mathfrak{f}$ then the action of $[\mathfrak{P}, L(E[\mathfrak{b}])/L]$ on $E[\mathfrak{b}]$ is given by multiplication by $\psi_E(\mathfrak{P})$.*

3. *If $\mathfrak{P}$ is a prime of good reduction of $E$ then the endomorphism $\psi_E(\mathfrak{P})$ acts as Frobenius on $\overline{E}(\mathbb{F}_q)$.*

**Proposition A.7.7.** *Let $\mathfrak{p}$ be a finite prime of $L$. Then there exists a curve isomorphic to $E$ over $\overline{L}$ with good reduction at $\mathfrak{p}$.*

**Proposition A.7.8.** *Suppose that $E$ is defined over $K$.*

1. *If $\mathfrak{p}$ is a finite prime of $K$ such that the reduction map $(\mathcal{O}_K)^\times \to (\mathcal{O}_K/\mathfrak{p})^\times$ is not surjective then $E[\mathfrak{p}] \not\subseteq E(K)$.*

2. *If $\mathfrak{f}$ is the conductor of $\psi_E$ then the reduction map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times$ is injective. In particular, $E$ does not have good reduction at all primes of $K$.*

The following Theorem is a collection of important results that (partially) show that elliptic curves with complex multiplication give an explicit description of class field theory for imaginary quadratic fields.

**Theorem A.7.9.** *Suppose that $E$ is defined over $K$, $\mathfrak{a} \lhd \mathcal{O}_K$ an ideal and $\mathfrak{p}$ a finite prime of $K$, both prime to $6\mathfrak{f}$. Then*

1. *$E[\mathfrak{a}\mathfrak{f}] \subseteq E(K(\mathfrak{a}\mathfrak{f})$ and $\mathrm{Gal}(K(E[\mathfrak{a}])/K) \cong (\mathcal{O}_K/\mathfrak{a})^\times$.*

2. *If $\mathfrak{b}$ divides $\mathfrak{a}$ then $\mathrm{Gal}(K(E[\mathfrak{a}])/K(E[\mathfrak{b}])) \cong \mathrm{Gal}(K(\mathfrak{a}\mathfrak{f})/K(\mathfrak{b}\mathfrak{f}))$.*

3. *$K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ is totally ramified above $\mathfrak{p}$.*

4. *If the reduction map $(\mathcal{O}_K)^\times \to (\mathcal{O}_K/\mathfrak{a})^\times$ is injective then $K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ is unramified outside of $\mathfrak{p}$.*

We define the *Hecke $L$-function* associated to powers of $\psi_E$ to be analytic continuation of the Dirichlet series

$$L(\psi_E^k, s) = \sum_{\substack{\mathfrak{b} \lhd \mathcal{O}_K \\ (\mathfrak{b}, \mathfrak{f}_k)=1}} \frac{\psi_E^k(\mathfrak{b})}{\mathbf{N}\mathfrak{b}^s}$$

where $\mathfrak{f}_k$ is taken to mean the conductor of $\psi_E^k$. It is a Theorem of Hecke that this Dirichlet series does indeed admit an analytic continuation. If $\mathfrak{m}$ is prime to $\mathfrak{f}$ and $\mathfrak{c}$ is prime to $\mathfrak{m}$ then we define the *partial* $L$-function $L_{\mathfrak{m}}(\psi_E^k, s, \mathfrak{c})$ similarly but with the summation restricted to ideals $\mathfrak{b} \lhd \mathcal{O}_K$ such that $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$. We note that if $L(E, s)$ is the $L$-function of $E$ in the usual sense then $L(E, s) = L(\psi_E, s)L(\overline{\psi_E}, S)$ (see [Sil09, §II.10]).

# Notation Index

| Symbol | Meaning | Page |
|---|---|---|
| $\mathcal{S}^{(\alpha)}(E)$ | Relaxed $\alpha$-Selmer group of the elliptic curve $E$ | 5 |
| $\langle\cdot,\cdot\rangle_{\pi^n}$ | $\pi^n$-Kummer pairing | 7 |
| $\delta_n$ | $\pi^n$-reciprocity map | 8 |
| $\Theta_{E,\mathfrak{a}}$ | $\Theta$-function of the elliptic curve $E/K$ with respect to the auxilliary ideal $\mathfrak{a}\in\mathcal{O}_K$ | 12 |
| $E[\mathfrak{b}]^*$ | $E[\mathfrak{b}]\setminus\{\,O_E\,\}$ | 12 |
| $\mathfrak{a}^{-1}\Lambda/\Lambda^*$ | $(\mathfrak{a}^{-1}\Lambda/\Lambda)\setminus\{\,0\,\}$ | 20 |
| $\theta(z;L)$ | Fundamental $\theta$-function of the lattice $L$ | 20 |
| $E_k(z;L)$ | Eisenstein series of weight $k$ attached to the lattice $L$ | 21 |
| $\Phi_{E,\mathfrak{a}}$ | $\Phi$-function of the elliptic curve $E/K$ with respect to the auxiliary ideal $\mathfrak{a}\lhd\mathcal{O}_K$ | 22 |
| $\eta_n(\mathfrak{r})$ | Elliptic unit of given by $n\in\mathbb{N}_{\geq 0}$ and $\mathfrak{r}\in\mathcal{R}$ | 26 |
| $D_\mathfrak{r}$ | $\mathfrak{r}$-derivative operator in $\mathbb{Z}[G_\mathfrak{r}]$ | 30 |
| $N_\mathfrak{r}$ | $\mathfrak{r}$-norm operator in $\mathbb{Z}[G_\mathfrak{r}]$ | 30 |
| $((L/K),\mathfrak{p})$ | Artin symbol of the unramified prime $\mathfrak{p}$ in the Galois extension $L/K$ | 51 |
| $\mathcal{C}_K$ | Ideal class group of the number field $K$ | 52 |
| $C_K^{\mathfrak{m}}$ | Ray class group of the number field $K$ modulo $\mathfrak{m}$ | 52 |
| $K(\mathfrak{m})$ | Ray class field of the number field $K$ modulo $\mathfrak{m}$ | 52 |
| $[\cdot,K^{\mathrm{ab}}/K]$ | Artin map of the global or local field $K$ | 53 |
| $\mathbb{I}_K$ | Idèle group of the number field $K$ | 53 |
| $\mathfrak{J}$ | Idealifier map $\mathfrak{J}:\mathbb{I}_K\to I_K$ | 53 |
| $C_K$ | Idèle class group of the number field $K$ | 53 |
| $H^n(K,M)$ | $n^{th}$-cohomology group of the $G_K$-module $M$ | 55 |
| $e_\chi$ | $\chi$-idempotent of a character $\chi:G\to\overline{\mathbb{Q}}$ | 56 |
| $\eta(z;L)$ | Quasi-period map associated to the lattice $L$ | 57 |
| $\sigma(z;L)$ | Weierstrass $\sigma$-function associated to the lattice $L$ | 57 |
| $\wp(z;L)$ | Weierstrass $\wp$-function associated to the lattice $L$ | 57 |
| $\zeta(z;L)$ | Weierstrass $\zeta$-function associated to the lattice $L$ | 57 |
| $\mathrm{S}^{(\alpha)}(E)$ | $\alpha$-Selmer group of the elliptic curve $E$ | 61 |
| $\text{Ш}(E)$ | Tate-Shafarevich group of the elliptic curve $E$ | 61 |
| $\mathfrak{f}$ | Conductor of the Hecke character $\psi_E$ associated to the elliptic curve $E$ | 62 |
| $\psi_E$ | Hecke character associated to the elliptic curve $E$ | 62 |
| $L(\psi_E^k,s)$ | Hecke $L$-function associated to $E$ | 63 |
| $L_\mathfrak{m}(\psi_E^k,s,\mathfrak{c})$ | Partial Hecke $L$-function associated to $E$ | 63 |

# Bibliography

[CF67] J. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (A Nato Advanced Study Institute W).* Academic Press, 1967. ISBN: 0121632512,9780121632519.

[Wei76] A. Weil. *Elliptic functions according to Kronecker and Eisenstein.* Springer-Verlag, Berlin and New York, 1976.

[CW77] J. Coates and A. Wiles. "On the Conjecture of Birch and Swinnerton-Dyer". In: *Inventiones mathematicae* 39 (1977), pp. 223–252. URL: `http://eudml.org/doc/142468`.

[Ser78] Serge Lang. *Elliptic Curves: Diophantine Analysis.* Springer-Verlag, 1978. ISBN: 978-3-642-05717-5.

[GS81] C. Goldstein and N. Schappacher. "Series d'Eisenstein et fonctions L de courbes elliptiques multiplication complexe." In: *Journal fr die reine und angewandte Mathematik* 327 (1981), pp. 184–218. URL: `http://eudml.org/doc/152388`.

[Coa83] J. Coates. "Infinite Descent on Elliptic Curves with Complex Multiplication". In: *Arithmetic and Geometry: Papers Dedicated to I.R. Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic.* Ed. by M. Artin and J. Tate. Boston, MA: Birkhäuser Boston, 1983, pp. 107–137. ISBN: 978-1-4757-9284-3.

[Ger83] S Gersten. "A short proof of the algebraic Weierstrass preparation theorem". In: *Proc. Amer. Math. Soc.* 88 (1983), pp. 751–752. DOI: `https://doi.org/10.1090/S0002-9939-1983-0702313-2`.

[Rub87] K. Rubin. "Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication". In: *Inventiones mathematicae* 89.3 (1987), pp. 527–559. ISSN: 1432-1297. DOI: `10.1007/BF01388984`. URL: `http://dx.doi.org/10.1007/BF01388984`.

[Sha87] E. D. Shalit. *Iwasawa theory of elliptic curves with complex multiplication: p-adic L functions.* Perspectives in mathematics 3. Academic Press, 1987. ISBN: 9780122102554,0-12-210255-X.

[Kol89] V. A. Kolyvagin. "Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil Curves". In: *Mathematics of the USSR-Izvestiya* 32.3 (1989), p. 523. URL: `http://stacks.iop.org/0025-5726/32/i=3/a=A04`.

[Kol90] V. Kolyvagin. "Euler Systems". In: *The Grothendieck Festschrift: A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck.* Ed. by P. Cartier et al. Boston, MA: Birkhäuser Boston, 1990, pp. 435–483. ISBN: 978-0-8176-4575-5. DOI: `10.1007/978-0-8176-4575-5_11`. URL: `http://dx.doi.org/10.1007/978-0-8176-4575-5_11`.

[Lan90] S. Lang. *Cyclotomic Fields I and II.* 2nd ed. Graduate Texts in Mathematics 121. Springer-Verlag New York, 1990. ISBN: 978-1-4612-6972-4,978-1-4612-0987-4.

[Rub91] K. Rubin. "The "main conjectures" of Iwasawa theory for imaginary quadratic fields". In: *Inventiones mathematicae* 103.1 (1991), pp. 25–68. ISSN: 1432-1297. DOI: `10.1007/BF01239508`. URL: `http://dx.doi.org/10.1007/BF01239508`.

[Kna92] A. Knapp. *Elliptic Curves*. 1992. ISBN: 0691085595,9780691085593.

[Len92] H. Lenstra. "Algorithms in algebraic number theory". In: *Bulletin of the American Mathematical Society* (Mar. 1992). URL: `https://arxiv.org/pdf/math/9204234.pdf`.

[Sil94] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1st ed. Graduate Texts in Mathematics 151. Springer-Verlag New York, 1994. ISBN: 978-0-387-94328-2,978-1-4612-0851-8.

[Ser97] J.-P. Serre. *Cohomologie Galoisienne*. 5 revised. Lecture Notes in Mathematics 5. Springer-Verlag, 1997. ISBN: 978-3-540-58002-7.

[Was97] L. Washington. *Introduction to Cyclotomic Fields*. 2nd ed. Graduate Texts in Mathematics 83. Springer-Verlag New York, 1997. ISBN: 0387906223,9780387906225.

[Rub99] K. Rubin. *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer*. 1999. URL: `http://swc.math.arizona.edu/aws/1999/99RubinCM.pdf` (Retrieved 08/04/2017).

[Yin00] L. Yin. "A note on Rubin's methods of the use of two Euler systems". In: *Science in China Series A: Mathematics* 43.8 (2000), pp. 792–794. ISSN: 1862-2763. DOI: `10.1007/BF02884177`. URL: `http://dx.doi.org/10.1007/BF02884177`.

[Sil09] J. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics 106. Springer-Verlag New York, 2009. ISBN: 0387094938,9780387094939.

[Ash10] R. Ash. *A Course in Algebraic Number Theory*. Dover Books on Mathematics. Dover Publications, 2010. ISBN: 0486477541,9780486477541.

[Kei12] S. Keil. "Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group". In: (June 2012). URL: `https://arxiv.org/pdf/1206.1822.pdf`.

[Rub14] K. Rubin. *Euler Systems.(AM-147)*. Vol. 147. Princeton University Press, 2014. URL: `http://swc-alpha.math.arizona.edu/swc-www/aws/1999/99RubinES.pdf`.

[JFN16] M. T.R. e. John Forbes Nash Jr. *Open Problems in Mathematics*. 1st ed. Springer International Publishing, 2016. ISBN: 978-3-319-32160-8,978-3-319-32162-2. URL: `http://gen.lib.rus.ec/book/index.php?md5=6D58FBF44315D5E836D43CCD5D249740`.

[AS17] A Angelakis and P Stevenhagen. *Adelic point groups of elliptic curves*. 2017. URL: `https://arxiv.org/pdf/1703.08427.pdf`.

[Dao17] A. Daoud. *Class Field Theory Notes*. 2017. URL: `http://www.p-adic.com/Class%20Field%20Theory.pdf`.

[Tri] N. Triantafillou. *The Chebotarev Density Theorem*. URL: `https://math.mit.edu/~ngtriant/notes/chebotarev.pdf`.