$\mathbb{Q}$-Curves with Complex Multiplication

Ley Wilson

A thesis submitted in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy in Pure Mathematics

THE UNIVERSITY OF
SYDNEY

School of Mathematics and Statistics
June 2010

Abstract

In this work we study families of quadratic twists of abelian varieties with complex multiplication by means of the associated Hecke characters, focusing upon the special cases of elliptic curves and their Weil restrictions. Following Gross, we say that an elliptic curve E/F with complex multiplication is a $\mathbb{Q}$-curve if it is isogenous to all its Galois conjugates over F.

The Hecke character of an abelian variety A/F is an isogeny invariant and the Galois action is such that A is isogenous to its Galois conjugate A^σ if and only if the corresponding Hecke character is fixed by σ. The quadratic twist of A by an extension L/F corresponds to multiplication of the associated Hecke characters. This leads us to investigate the Galois groups of families of quadratic extensions L/F with restricted ramification which are normal over a given subfield k of F. Our most detailed results are given for the case where k is the field of rational numbers and F is a field of definition for an elliptic curve with complex multiplication by K. In this case the groups which occur as $\mathrm{Gal}(L/K)$ are closely related to the 4-torsion of the class group of K.

We analyze the structure of the local unit groups of quadratic fields to find conditions for the existence of curves with good reduction everywhere. After discussing the question of finding models for curves of a given Hecke character, we use twists by 3-torsion points to give an algorithm for constructing models of curves with known Hecke character and good reduction outside 3. The endomorphism algebra of the Weil restriction of an abelian variety A may be determined from the Grössencharacter of A. We describe the computation of these algebras and give examples in which A has dimension 1 or 2 and its Weil restriction has simple abelian subvarieties of dimension ranging between 2 and 24.

Acknowledgements

I am deeply appreciative of the mathematical enthusiasm and insight, as well as the encouragement and patience shown by my supervisor David Kohel and my associate supervisor Claus Fieker. Thanks are also due to others in the School of Mathematics and Statistics, especially Steve Donnelly and Mike Harrison, and to all the other students of David Kohel, in particular David Gruenewald who braved an early draft of this thesis.

This thesis contains no material which has been accepted for the award of any other degree or diploma. All work in this thesis, except where duly attributed to another person, is believed to be original.

Contents

Introduction

In this work we study abelian varieties with complex multiplication by means of the associated Hecke characters, focusing upon the special cases of elliptic curves and their Weil restrictions.

Let F be an algebraic number field. The Dedekind ζ-function of F,

$$\zeta_F(s) := \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^s}\right)^{-1} \tag{0.1}$$

converges for all $s \in \mathbb{C}$ with $\Re(s) > 1$. There is an analytic continuation of $\zeta_F(s)$ to the whole complex plane and setting

$$Z_F(s) := \left(2^{-r_2}\pi^{-n/2}\sqrt{|D_F|}\right)^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2}\zeta_F(s),$$

where r_1 and r_2 are respectively the numbers of real and complex infinite places of F, $n := r_1 + 2r_2$ and D_F is the discriminant of the maximal order of F, we have the functional equation

$$Z_F(s) = Z_F(1-s).$$

In 1920, Hecke [**21**] proved that similar properties held for L-series of the form

$$L(\chi, s) := \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^s}\right)^{-1} \tag{0.2}$$

where χ belongs to a class of a homomorphisms from the ideal group of F to $\mathbb{C}^*$ containing, but not limited to, those corresponding to characters of $\mathrm{Gal}(F^{ab}/F)$ via the Artin mapping. In the language of ideles, these χ are continuous homomorphisms from the idele group of F to $\mathbb{C}$ which are trivial on F^*. We shall call such homomorphisms *Hecke characters*.

Deuring [**7**, 1953] proved that if E is an elliptic curve defined over F such that the ring of F-rational endomorphisms of E is an order in an imaginary quadratic field, there exists a Hecke character χ such that

$$L(E/F, s) = L(\chi, s)L(\overline{\chi}, s), \tag{0.3}$$

and an analogous result was found for abelian varieties of CM type by Shimura and Taniyama [**57**, 1961].

Serre and Tate [**51**, 1969], used ℓ-adic representations to prove that if A is an abelian variety of CM type of dimension g then the conductor of A is the $2g$th power of the conductor of the associated Hecke character χ_A.

In [**55**, 1971], Shimura studied abelian varieties A/F of CM type associated with Hecke characters of the form

$$\chi_A := \chi_0 \circ \mathrm{N}_{F/k} \tag{0.4}$$

for some subfield k of F. Such varieties are interesting from a class field theoretic perspective because the group of torsion points of A defined over an algebraic closure F^{alg} of F generates an abelian extension of k. They also have the property that for every element σ of $\mathrm{Gal}(F/k)$ there exists an F-rational isogeny from A to A^σ. In analogy with our use of the term $\mathbb{Q}$-curve (see below), we shall call such abelian varieties k-varieties, and say that a k-variety is of type 1 or type 2 according to whether the associated Hecke character satisfies (0.4) or not.

The conjecture of Birch and Swinnerton-Dyer for elliptic curves is that if the group of F-rational points of E modulo torsion has rank r then $L(E/F, s)$ has a zero at $s = 1$ of order r. If E has complex multiplication and is associated with a Hecke character with 'nice' properties, the conjecture is very much more approachable than in the general case. This was partial motivation for work of Gross and Rohrlich in the early eighties.

Gross [**16**] looked in detail at elliptic curves with complex multiplication by $k := \mathbb{Q}(\sqrt{-p})$ for p a rational prime congruent to 3 modulo 4 corresponding to Hecke characters satisfying (0.4) where F is the Hilbert class field of k and the additional properties that

$$\chi_A^\sigma = \chi_A \text{ for all } \sigma \in \mathrm{Gal}(F/\mathbb{Q}) \tag{0.5}$$

and that χ_A is ramified only at primes of F dividing p. The term $\mathbb{Q}$-*curve* for elliptic curves satisfying (0.5) stems from the work of Gross.

Motivated by Gross's work, Rohrlich studied the functional equation of abelian varieties with complex multiplication by k satisfying (0.4) such that

$$\chi_0^\rho = \chi_0, \tag{0.6}$$

where ρ denotes complex conjugation on k.

If A and B are $\mathbb{Q}$-curves defined over F then we say that A is $\mathbb{Q}$-*equivalent* to B if

$$\chi_A \chi_B^{-1} = \eta \circ \mathrm{N}_{F/\mathbb{Q}} \tag{0.7}$$

where η is a quadratic Hecke character of $\mathfrak{I}_{\mathbb{Q}}$. There is a unique element in each $\mathbb{Q}$-equivalence class with minimal conductor and the endomorphism algebra of the Weil restriction of A is determined up to isomorphism by the equivalence class of A.

Nakamura [**33, 34**] described the equivalence classes of $\mathbb{Q}$-curves over F, and determined the possible endomorphism algebras of their Weil restrictions. These articles form the starting point for the investigations of the present work.

Given an elliptic curve A defined over a field F and associated with a given Hecke character χ_A, we are interested in families of twists of A by quadratic extensions L/F. The general theory is very similiar when A is a simple abelian variety of CM type but as the conditions for a Hecke character to correspond to an abelian variety simplify considerably in dimension one and any elliptic curve is defined over a ring class field, which has a well known structure over $\mathbb{Q}$, detailed results and examples are easier to obtain.

If the study of abelian varieties of CM type has been dominated by that of elliptic curves, the study of elliptic curves (especially in those branches including explicit examples) has been dominated by curves having a model over the rationals. Part of the attraction of studying $\mathbb{Q}$-curves of type 1 is that they share many of the properties of curves defined over a quadratic field, without the limitation on the CM field. Advances in technology have also made the general case more amenable to computational investigation. One of the aims of this work is to make more explicit the study of elliptic curves with complex multiplication by quadratic fields with non-trivial class groups.

Overview

The first two chapters are essentially introductory. Some acquaintance with algebraic number fields and class field theory is assumed, as well as some algebraic geometry, particularly in the discussion of the Néron model.

In **Chapter 1** we begin with a discussion of elliptic curves in which we outline aspects of the theory we will draw upon later, notably good and bad reduction and complex multiplication. The second and third sections treat similar topics for abelian varieties of general dimension, focusing upon abelian varieties of CM type.

Chapter 2 is devoted to Hecke characters. In the first section we give the basic definitions and properties of general Hecke characters of an algebraic number field F and then describe the subgroup corresponding to field extensions. In Section 2.2 we use local field theory and genus theory to gain more detailed information about the Hecke characters of quadratic fields, and in Section 2.3 we study the Hecke characters associated with abelian varieties.

The raison d'être of **Chapter 3** is the twisting of abelian varieties defined over a number field F by quadratic extensions L/F. We study the

Galois groups of families of quadratic extensions with restricted ramification which are normal over a given subfield k of F. Our most detailed results are given for the case where k is an imaginary quadratic field and F is a field of definition for an elliptic curve with complex multiplication by an order of k.

Let $G := \mathrm{Gal}(F/k)$. If L is a quadratic extension of F normal over k then L determines a cohomology class in $H^2(F/k, \pm 1) := H^2(G, \pm 1)$. The subgroup $G[2] := \{g \in G : g^2 = 1\}$ is isomorphic to $C_2^{\times n}$ for some integer $n \geq 0$, and we define k' to be the fixed field $F^{G[2]}$. Let $\mathcal{G}$ be a maximal set of quadratic extensions L/F such that L/k' is normal and no two elements of $\mathcal{G}$ represent the same class in $H^2(F/k', \pm 1)$ and let $\mathcal{A}$ be the subset of $\mathcal{G}$ consisting of L such that L/k is abelian. It is known (see Massy [**27**]), that

$$|\mathcal{A}| \leq 2^n - 1 \text{ and } |\mathcal{G}| \leq 2^m - 1 \text{ where } m = \binom{n+1}{2}. \qquad (0.8)$$

In Section 3.2.2 we describe the groups which may occur as $\mathrm{Gal}(L/k')$ for L in $\mathcal{G}$ and, under the assumption that equality holds in both equations of (0.8), determine the number of elements of $\mathcal{G}$ which have a given Galois group over k'.

When k is an imaginary quadratic field and F is the Hilbert class field of k, Nakamura [**34**] proved that $|\mathcal{G}| + 1 = 2^{m-n}(|\mathcal{A}| + 1)$, so that the upper bound on $|\mathcal{G}|$ will be attained whenever the upper bound on $|\mathcal{A}|$ is. Studying $\mathcal{A}$ with the same restrictions on F and k, we find that its cardinality is almost entirely determined by the 4-torsion in the class group of k. Let r be the 4-rank of the class group of k, and let D be the discriminant of k. We prove in Proposition 3.3.23 that $|\mathcal{A}| = 2^d - 1$ where

$$n - r - 1 \leq d \leq n - \max\{r, 1\}$$

and in particular that $d = n - r$ except possibly if D is congruent to 4 modulo 8 and is divisible by some prime $p \equiv 3 \bmod 4$. Since the density of imaginary quadratic fields with $r = 0$ is close to $1/3$ (Gerth [**12**], Fouvry and Klüners [**9**]), this shows that there is a large class of field extensions to which we may apply the results of Section 3.2.2.

In **Chapter 4** we apply the theory developed in the first three chapters to K and $\mathbb{Q}$-curves with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field K. Combining material from Chapters 2 and 3 we describe the Hecke characters associated with a set of representatives of each $\mathbb{Q}$-equivalence class of $\mathbb{Q}$-curves over $H_{\mathcal{O}}$, the ring class field of $\mathcal{O}$. If the discriminant of K is less than -4 then any K-curve of type 2 may be realized as the quadratic twist of a type 1 curve by an extension $L/H_{\mathcal{O}}$ which is normal over K.

If 3 either splits or is ramified in $\mathcal{O}$ then any elliptic curve E with CM by $\mathcal{O}$ has at least one 3-torsion point $P = (x_P, y_P)$ with x_P defined over $H_{\mathcal{O}}$. In Section 4.3.1 we investigate the quadratic twist E' of E by y_P^2 and show that E' is a K-curve of type 1 with good reduction at all primes of $H_{\mathcal{O}}$ coprime to 3. These curves are of particular interest to us because they offer a simple algorithm for finding a model of an elliptic curve associated with an easily described Hecke character. This is the converse to the problem of determining the Hecke character associated with a curve described by a given model, a question first studied by Weil [**64**, 1952], before it was known that all elliptic curves with CM could be associated to a Hecke character.

In Section 4.4 we consider $\mathbb{Q}$-curves with good reduction everywhere. We prove that there exists a CM elliptic curve with good reduction everywhere over H if and only if the discriminant D_K of K is divisible by at least two primes congruent to 3 mod 4, and that in this case there exists a $\mathbb{Q}$-curve with this property. This complements work of Rohrlich [**42**] which showed that this condition was necessary and sufficient for the existence of a CM elliptic curve E with j-invariant j_E having good reduction everywhere over $\mathbb{Q}(j_E)$.

Let F/k be a normal extension of number fields with Galois group G and let A be an abelian variety defined over F. The *Weil restriction* of A from F to k is an abelian variety $\mathfrak{W}_{F/k}(A)$ defined over k with the property that $\mathfrak{W}_{F/k}(A) \times_k F$ is isomorphic to $\prod_{\sigma \in G} A^\sigma$. These varieties form the subject matter of **Chapter 5**. Suppose that A/F is a simple abelian variety of CM type, which is F-isogenous to its Galois conjugate A^σ for all σ in $\mathrm{Gal}(F/k)$. We investigate the structure of $W := \mathfrak{W}_{F/k}(A)$, up to isogeny, as a product of simple factors and the relationship between the algebra of k-rational endomorphisms of W and the Hecke character χ_A associated with A. Theorem 5.2.16, which extends results of Goldstein and Schappacher [**13**] and Nakamura [**33**], shows among other things that if A is a k-variety of type 1 then $\mathfrak{W}_{F/k}(A)$ is k-isogenous to a product of simple non-isogenous abelian varieties of CM type. Suppose that K is an imaginary quadratic field with Hilbert class field H and let E/H be an elliptic curve with CM by K. Nakamura [**33, 34**] determined the possible endomorphism algebras for $\mathfrak{W}_{H/k}(E)$ when E is a k-curve and k is either K or $\mathbb{Q}$, in particular showing that if E is of type 1 then $\mathfrak{W}_{H/K}(E)$ is simple over K. If E is of K-type 1 and has CM by a non-maximal order $\mathcal{O}$ of K then we derive a necessary condition on the discriminants of K and $\mathcal{O}$ for $\mathfrak{W}_{H/K}(E)$ to be simple. We describe the computation of the endomorphism algebras $\mathrm{End}_k^0(\mathfrak{W}_{F/k}(A))$ using cohomological and group theory developed in Chapter 3 and give a number of examples in which A is an elliptic curve including an application to abelian varieties with CM by biquadratic fields.

The chapter concludes with a discussion of the analogous case where A has CM by a cyclic quartic CM field.

Notation

We outline some of our basic conventions and notations below. A page reference for the definition of the main symbols used is given in the List of Symbols at the end of this document.

Number fields. Let F be an algebraic number field, with maximal order $\mathcal{O}_F$. We denote by I_F the group of fractional ideals of $\mathcal{O}_F$ and by $\mathfrak{A}_F$ and $\mathfrak{I}_F$ the ring of adeles and the idele group of F respectively. A *prime* $\mathfrak{p}$ of F is a prime ideal of $\mathcal{O}_F$, and $v_\mathfrak{p}$ is the associated additive valuation of F. The completion of F with respect to $v_\mathfrak{p}$ will be denoted $F_\mathfrak{p}$, its maximal order $\mathcal{O}_\mathfrak{p}$ and residue class field $\overline{F}_\mathfrak{p} = F_\mathfrak{p}/\pi\mathcal{O}_\mathfrak{p}$ where π is an element of $F_\mathfrak{p}$ with $v_\mathfrak{p}(\pi) = 1$.

Let v be an additive valuation of $\mathcal{O}_F$, and let $\mathfrak{p}_v$ be the place of F associated with v. If v is non-archimedean, then $\mathfrak{p}_v$ is a *finite* place of F and hence a prime, and *infinite* otherwise. An infinite place of F is *real* or *complex* according to whether $F_{\mathfrak{p}_v}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

Ideals are generally denoted by gothic script, $\mathfrak{a}, \mathfrak{p}, \mathfrak{m} \ldots$ and ideles by lowercase Greek symbols, $\boldsymbol{\alpha} = (\alpha_\mathfrak{p})$. Let F/k be an abelian extension of algebraic number fields. The Artin map $\mathfrak{I}_k \to \mathrm{Gal}(F/k)$ resp. $I_k \to \mathrm{Gal}(F/k)$ is denoted $(F/k; \cdot)$ and we use the same symbol $\mathrm{N}_{F/k}$ to denote the norm mapping on field elements, ideles and ideals of F.

If F/k is a normal extension of algebraic number fields then we shall say that k is a normal subfield of F.

Local fields are denoted F_v where v is the associated additive valuation. For valuations in both local and global fields we adopt the convention that the valuation of a uniformizing element is always 1.

By a *quadratic field* we always mean a quadratic extension of $\mathbb{Q}$. The discriminant of a quadratic field K, which we shall consider as an integer, is denoted D_K. The discriminant of a general field extension F/k is denoted $D_{F/k}$.

Abelian varieties. The symbol E is reserved for elliptic curves. A and B denote abelian varieties, except in Chapter 3 where (after the introduction) A is used exclusively to denote an extension $A/F/k$ which is *abelian* over the base field k. The symbol E/F denotes an elliptic curve defined over a field F. Endomorphism rings and algebras are denoted by R, S and T. Isomorphism is denoted by $\cong$ and isogeny by $\simeq$.

We say that an abelian variety A/F is a *k-variety* if k is a normal subfield of F such that there are F-rational isogenies between A and A^σ for all $\sigma \in \mathrm{Gal}(F/k)$. We say that A *descends* to k if there exists an abelian variety B defined over k such that $B \times_k F$ is isomorphic to A. If A descends to k then A is clearly a k-variety, but a k-variety need not descend to k.

Groups and Galois action. The cyclic group of order n is written C_n and $C_n^{\times m}$ denotes the direct product of m copies of C_n. If A/F is an abelian variety, k is a subfield of F and σ an element of $\mathrm{Gal}(F/k)$ we denote by A^σ the Galois conjugate of A by F. The subfield of F fixed by a subgroup G of $\mathrm{Gal}(F/k)$ is denoted F^G. In particular, if G is a cyclic group generated by σ we usually denote its fixed field by $F^{\langle\sigma\rangle}$. If F is a CM field, or if $F = \mathbb{C}$ we denote the complex conjugate of a field element x by x^ρ or $\bar{x}$.

Hecke characters. There is considerable diversity of notation regarding Hecke characters in the literature. Our main conventions are as follows: Let F be a number field with idele group $\mathfrak{I}_F$. A *Hecke character* of $\mathfrak{I}_F$ is a continuous homomorphism

$$\chi : \mathfrak{I}_F \to \mathbb{C}^*.$$

which is trivial on F^*. If the image of χ is contained in the unit circle of $\mathbb{C}^*$ then we say that χ is an *ordinary* Hecke character. If there exists some finite abelian extension L/F such that χ is the character of $\mathfrak{I}_F$ corresponding to L/F by class field theory then we say that χ is a *Dirichlet character* of $\mathfrak{I}_F$ (Definition 2.1.14). Let A be an abelian variety of CM type. A Hecke character determined by A is called a *Grössencharacter* of A (Definition 2.3.4).

Magma. The computations in this work have been done in versions of Magma ranging from 2.13 to 2.15.

CHAPTER 1

Abelian Varieties

In this chapter we outline aspects of the theory of abelian varieties over algebraic number fields, focusing upon abelian varieties with potential good reduction everywhere, especially those with complex multiplication.

In Section 1.1 we recall some basic facts about elliptic curves, further details of which may be found in Gross [**16**] and Silverman [**58**]. Most of the abelian varieties we shall encounter later will be isogenous over $\mathbb{C}$ to powers of elliptic curves, however over their minimal fields of definition they may look very different. One of the broad aims of this chapter is to gain some understanding of the behaviour of abelian varieties under the extension and restriction of their base fields.

The introduction to abelian varieties over general fields in Section 1.2 follows Chapters II and IV of Mumford [**31**], while that of abelian varieties over $\mathbb{C}$ and of CM types draws on Lang [**26**] and various works of Shimura [**54, 55, 56**]. Our treatment of good reduction in Section 1.3 largely follows the article of Serre-Tate [**51**]. The central theme of this section is the manner in which the local geometry of an abelian variety A is determined by the ℓ-adic representation. For abelian varieties of CM type, this will be reinterpreted in terms of Grössencharacters in Section 2.3.

1.1. Preliminaries on Elliptic Curves

In this section, F will be an algebraic number field, k a subfield of F, and E an elliptic curve defined over F. The symbol K will be used to denote an imaginary quadratic field. We consider any algebraic number field as a subfield of $\mathbb{C}$. If L/F is a field extension, then E_L is the lift of E to L. Let E_1 and E_2 be elliptic curves defined over F. A non-zero homomorphism $\lambda : E_1 \to E_2$ is an *isogeny* and if λ is defined over F then we say that E_1 and E_2 are *isogenous over* F or F*-isogenous*.

Definition 1.1.1. *Let k be a subfield of F such that F/k is normal. We say that E is a k*-curve *if E^σ is isogenous to E over F for all σ in* $\mathrm{Gal}(F/k)$.

A homomorphism $E \to E$ is called an *endomorphism* of E, and the ring of F-rational endomorphisms is denoted $\mathrm{End}_F(E)$.

Let K be an imaginary quadratic field. An elliptic curve E has *complex multiplication*, or *CM* by an order $\mathcal{O}$ of K if

$$\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}, \tag{1.1}$$

and if this is the case, $K(j_E) = H_{\mathcal{O}}$, where j_E is the j-invariant of E and $H_{\mathcal{O}}$ is the ring class field of $\mathcal{O}$. If E does not have complex multiplication by an order of any imaginary quadratic field then $\mathrm{End}_{\mathbb{C}}(E) \cong \mathbb{Z}$. The invertible elements of the endomorphism ring of E form the *automorphism group* $\mathrm{Aut}(E)$ of E. If E does not have complex multiplication by either $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-4})$ then $\mathrm{Aut}(E) = \{\pm 1\}$.

Proposition 1.1.2. *Let E be an elliptic curve defined over a number field F and let L/F be a quadratic extension. There exists a unique elliptic curve E^L defined over F such that E and E^L are non-isomorphic over F but become isomorphic over L.*

Proof. See Propositions X.5.3 and X.5.4 of Silverman [**58**]. □

We say that E^L is the *quadratic twist* of E by L and if m is an element of F with the property that $L = F(\sqrt{m})$, then we also call E^L the quadratic twist of E by m.

Example 1.1.3. Suppose that E has a model $y^2 = x^3 + ax + b$ over F, and $L = F(\sqrt{m})$. Then E^L has a model $y^2 = x^3 + m^2ax + m^3b$.

Proposition 1.1.4. *Let K be an imaginary quadratic field with discriminant $D_K \neq -3, -4$, and let $\mathcal{O}$ be an order of K. Let $F/\mathbb{Q}$ be normal, and suppose that E/F and E'/F are non-F-isogenous elliptic curves with CM by $\mathcal{O}$. Then there exists a unique quadratic extension L/F such that E and E' are isogenous over L and if E and E' are both $\mathbb{Q}$-curves, then $L/\mathbb{Q}$ is normal.*

Conversely, let E be a $\mathbb{Q}$-curve and let L be any quadratic extension of F. Then E^L is a CM elliptic curve defined over F which is a $\mathbb{Q}$-curve if and only if $L/\mathbb{Q}$ normal.

Proof. This is a special case of Corollary 2.3.13 which we prove in the next chapter. □

Let $E(F)$ denote the points of E with F-rational coordinates. It is well known that $E(F)$ has the structure of an abelian group. (See Section III.2 of Silverman [**58**] for a description of the group structure.) The subgroup of $E(F)$ consisting of points of finite order is denoted by $E_{tors}(F)$ and by the Mordell-Weil theorem (see Silverman [**58**] Theorem VIII.6.7), $E(F)$ is finitely generated.

Definition 1.1.5. *The* Mordell-Weil *rank of E/F is the integer r such that*

$$E(F) \cong E_{tors}(F) \times \mathbb{Z}^r.$$

1.1.1. Good Reduction of Elliptic Curves. Let E be an elliptic curve defined over a number field F. A general Weierstrass equation for E/F has the form

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

and discriminant

$$\Delta_{\mathcal{E}} := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \tag{1.3}$$

where

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, \\ b_4 &:= 2a_4 + a_1a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

We say that $\mathcal{E}$ is *integral* if each coefficient a_i belongs to $\mathcal{O}_F$ and $\mathfrak{p}$-*minimal* if

$$v_{\mathfrak{p}}(\Delta_{\mathcal{E}}) = \min\{v_{\mathfrak{p}}(\Delta)\},$$

where Δ runs through the discriminants of integral Weierstrass equations for E.

Let $\mathfrak{p}$ be a prime of F. Let $E_{\mathfrak{p}}$ be the curve defined by reduction of a $\mathfrak{p}$-minimal Weierstrass equation modulo $\mathfrak{p}$. Then E has *good reduction* at $\mathfrak{p}$ if $E_{\mathfrak{p}}$ is an elliptic curve over $F_{\mathfrak{p}}$. Otherwise, $E_{\mathfrak{p}}$ has a singularity and we say that E has *bad reduction* at $\mathfrak{p}$.

Definition 1.1.6. *Suppose that E/F has bad reduction at $\mathfrak{p}$ and let $E_{\mathfrak{p}}^{ns}$ be the non-singular part of $E_{\mathfrak{p}}$. Then E has* multiplicative reduction *at $\mathfrak{p}$ if*

$$E_{\mathfrak{p}}^{ns}(\overline{F}_{\mathfrak{p}}) \cong \overline{F}_{\mathfrak{p}}^{*}$$

and additive reduction *at $\mathfrak{p}$ if*

$$E_{\mathfrak{p}}^{ns}(\overline{F}_{\mathfrak{p}}) \cong \overline{F}_{\mathfrak{p}}^{+}.$$

Definition 1.1.7. *Suppose that E has multiplicative reduction at $\mathfrak{p}$. Then the singularity of $E_{\mathfrak{p}}$ is a node, and we say that E has* split *multiplicative reduction if the slopes to the tangent lines of this node are in $F_{\mathfrak{p}}$.*

The most well known criterion for good reduction at $\mathfrak{p}$ is that $\mathfrak{p}$ must not divide the discriminant of a minimal Weierstrass equation for E. We shall discuss some other criteria in Section 1.3.

1.1.2. Lattices and Elliptic Curves.

Definition 1.1.8. *We shall use the term* lattice *in two closely related senses:*

a) *Let V be a finite dimensional vector space over $\mathbb{R}$. A* lattice in V *is a finitely generated $\mathbb{Z}$-module contained in V which spans V over $\mathbb{R}$.*
b) *Let R be a Dedekind domain with field of fractions F and let V be a finite-dimensional vector space over F. An* R-lattice in V *is a finitely generated R-module contained in V which spans V over F.*

The symbol Λ will be used for lattices of both kinds.

Lemma 1.1.9 (Weil [**66**] p. 81)**.** *Let Λ be a $\mathbb{Z}$-lattice in a number field F. Then the subring of elements a of F such that $a\Lambda \subseteq \Lambda$ is an order $\mathcal{O}_\Lambda$ of F.*

Let F be an algebraic number field, Λ a $\mathbb{Z}$-lattice in F and p a rational prime. If $F_p := F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\Lambda_p := \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p$, then Λ_p is a $\mathbb{Z}_p$-lattice in F_p. We can consider any element x of F_p as a vector $(x_1, \dots x_n)$ with x_i in $F_{\mathfrak{p}_i}$, where $\mathfrak{p}_i$ runs through the primes of F dividing p. Let $\mathfrak{A}_F$ denote the ring of adeles of F, and $\mathfrak{I}_F$ the group of ideles. Since $\mathfrak{A}_F = \mathfrak{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} F$, we can express any finite idele $\boldsymbol{\alpha}$ of $\mathfrak{I}_F$ as a product

$$\boldsymbol{\alpha} = \prod_p \alpha_p$$

with each α_p in F_p.

Proposition 1.1.10. *Let F, Λ and $\boldsymbol{\alpha}$ be as above. There exists a unique $\mathbb{Z}$-lattice Λ' in F such that*

$$\Lambda'_p = \alpha_p \Lambda_p, \tag{1.4}$$

for all rational primes p. We set $\boldsymbol{\alpha}\Lambda := \Lambda'$.

Proof. By Theorem V.2 of Weil [**66**], there exists such a $\mathbb{Z}$-lattice Λ' in F if and only if $\Lambda'_p = \Lambda_p$ for all but finitely many primes p, and if it exists Λ' is uniquely defined. Let $\mathcal{O}_\Lambda$ be the order of F defined in Lemma 1.1.9 and let D be the discriminant of $\mathcal{O}_\Lambda$. If p is coprime to D, and u is an element of F such that $u_\mathfrak{p}$ is a local unit of $F_\mathfrak{p}$ for all $\mathfrak{p}$ dividing p then u belongs to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ hence $u\Lambda_p \subseteq \Lambda_p$. The set of all primes p such that $p|D$ or $v_\mathfrak{p}(\alpha_\mathfrak{p}) > 0$ for some $\mathfrak{p}$ dividing p is finite, so we are done. □

Definition 1.1.11. *Let U_F be the subgroup of ideles $\boldsymbol{\alpha}$ of $\mathfrak{I}_F$ with trivial infinite components such that $v_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ at every finite place $\mathfrak{p}$ of F, and let F^*_∞ be the subgroup of ideles $\boldsymbol{\alpha}$ for which $\alpha_\mathfrak{p} = 1$ for all finite places $\mathfrak{p}$ of F. We define*

$$U_\Lambda := \{\boldsymbol{\alpha} \in U_F : \boldsymbol{\alpha}\Lambda = \Lambda\}. \tag{1.5}$$

If $\mathcal{O}_\Lambda = \mathcal{O}_F$ then by the argument in the proof of Proposition 1.1.10 it follows that $U_\Lambda = U_F$.

Let E be an elliptic curve defined over $\mathbb{C}$. There is a lattice Λ of $\mathbb{C}$ and a complex analytic isomorphism of groups $f : E(\mathbb{C}) \to \mathbb{C}/\Lambda$. For any isogeny $\lambda : E \to E'$ there exists an analytic homomorphism ζ such that the diagram

$$\begin{tikzcd}
E(\mathbb{C}) \arrow[r, "f"] \arrow[d, "\lambda"] & \mathbb{C}/\Lambda \arrow[d, "\zeta"] \\
E'(\mathbb{C}) \arrow[r, "f'"] & \mathbb{C}/\Lambda'
\end{tikzcd}$$

commutes. We identify E with the complex torus $\mathbb{C}/\Lambda$.

Definition 1.1.12. *Two lattices (resp. $\mathbb{Z}$-lattices) Λ_1 and Λ_2 in $\mathbb{C}$ (resp. F) are* homothetic *if there exists some element x of $\mathbb{C}^*$ (resp. F^*) such that $\Lambda_1 = x\Lambda_2$.*

Proposition 1.1.13. *Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$ and let E_1 and E_2 be elliptic curves defined over $\mathbb{C}$ such that $E_i \cong \mathbb{C}/\Lambda_i$ for $i = 1, 2$. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are homothetic.*

Proof. See Silverman [**58**] Corollary VI.4.1.1. □

The following theorem relates $\mathbb{Z}$-lattices in an imaginary quadratic field K with elliptic curves with complex multiplication by an order of K via an embedding of K in $\mathbb{C}$.

Theorem 1.1.14 (Lang [**26**] Theorem 1.4.1)**.** *Let K be an imaginary quadratic field, let θ be an embedding of K in $\mathbb{C}$ and let Λ be a lattice in K. Then $\theta(\Lambda)$ is a lattice in $\mathbb{C}$ and $\mathbb{C}/\theta(\Lambda)$ is isomorphic to an elliptic curve with CM by an order of K.*

Let $E/\mathbb{C}$ be an elliptic curve with CM by an order $\mathcal{O}$ of K. Then there exists a lattice Λ in K such that $\mathbb{C}/\theta(\Lambda) \cong E$, and $\mathcal{O}$ is the subring of elements x of K such that $x\Lambda \subset \Lambda$.

Let N_Λ be the open subgroup $U_\Lambda K_\infty^* K^*$ of $\mathfrak{I}_K/K^*$. By the Existence Theorem of global class field theory, (see Tate [**61**] p. 172), there exists a unique abelian extension F/K such that

$$\mathrm{N}_{F/K}(\mathfrak{I}_F/F^*) = N_\Lambda. \tag{1.6}$$

Proposition 1.1.15 (Shimura [**56**] Theorem 5.5)**.** *Let Λ be a lattice in an imaginary quadratic field K, let E be an elliptic curve which is isomorphic to $\mathbb{C}/\theta(\Lambda)$, and let F be the abelian extension of K defined in* (1.6)*. Then $F = K(j_E)$, where j_E is the j-invariant of E.*

Since $K(j_E)$ is the ring class field of the order $\mathcal{O}$ of K isomorphic to $\mathrm{End}_{\mathbb{C}}(E)$ we can set

$$U_{\mathcal{O}} := U_\Lambda \text{ and } N_{\mathcal{O}} := N_\Lambda. \tag{1.7}$$

1.1.3. Reduction of Isogenies. This section develops theory which we will need for the definition of the Grössencharacter of an elliptic curve with complex multiplication. The central result is Proposition 1.1.22. Similar results for abelian varieties of CM type of any dimension will be discussed in Section 1.3. See Definition 1.2.2 and below for basic definitions concerning isogenies.

Lemma 1.1.16. *Let F be a number field, $\mathfrak{p}$ an ideal of $\mathcal{O}_F$ and suppose E and E' are elliptic curves defined over F with good reduction at $\mathfrak{p}$. Then if $\phi : E \to E'$ is an isogeny of degree m defined over F^{alg}, reduction at $\mathfrak{p}$ defines an isogeny of degree m*

$$\phi_{\mathfrak{p}} : E_{\mathfrak{p}} \to E'_{\mathfrak{p}},$$

defined over $\overline{F}_{\mathfrak{P}}^{alg}$ where $\mathfrak{P}$ is a prime of F^{alg} dividing $\mathfrak{p}$.

Proof. See Silverman [**59**] Proposition II.4.4. □

Let $L := F^{alg}$. As a consequence of the preservation of degrees, reduction at $\mathfrak{p}$ defines an injection ϑ of $\mathrm{Hom}_L(E, E')$ into $\mathrm{Hom}_{\overline{L}_{\mathfrak{P}}}(E_{\mathfrak{p}}, E'_{\mathfrak{p}})$.

Lemma 1.1.17. *An endomorphism of $E_{\mathfrak{p}}$ is in the image of ϑ if and only if it commutes with every element of $\vartheta(\mathrm{End}_L(E))$.*

Proof. This is a special case of Proposition 1.3.22. See Lemma II.5.2 of Silverman [**59**] for proof in the elliptic curve case. □

Definition 1.1.18. *Let E be a curve with CM by an order $\mathcal{O}$ of K. Let $H_{\mathcal{O}}$ be the ring class field associated with $\mathcal{O}$ and let $h := [H_{\mathcal{O}} : K]$. Let $\{j_1, \ldots j_h\}$ run through the set of possible j-invariants of elliptic curves with CM by $\mathcal{O}$, and for $1 \le i < k \le h$, let $n_{i,k} := \mathrm{N}_{H_{\mathcal{O}}/\mathbb{Q}}(j_i - j_k)$.*

*We say that a rational prime p is E-*excluded *if p satisfies one or more of the following conditions:*

a) *p is ramified in $H_{\mathcal{O}}/\mathbb{Q}$,*
b) *E has bad reduction at a prime lying over p,*
c) *p divides $n_{i,k}$ for some i, k.*

Let Λ be a lattice in K corresponding to an elliptic curve E, let $\mathfrak{a}$ be a non-zero fractional ideal of $\mathcal{O}_K$, and let $\bar{\mathfrak{a}}$ denote the ideal class of $\mathfrak{a}$. If $\mathfrak{b}$ is another ideal in $\bar{\mathfrak{a}}$ the lattices $\mathfrak{b}^{-1}\Lambda$ and $\mathfrak{a}^{-1}\Lambda$ are homothetic, and hence correspond to isomorphic elliptic curves. We write $\bar{\mathfrak{a}} * E$ for the curve corresponding to $\mathfrak{a}^{-1}\Lambda$.

If $\mathfrak{a}$ is an integral ideal, then $\Lambda \subset \mathfrak{a}^{-1}\Lambda$ and so the map sending $z+\Lambda$ to $z+\mathfrak{a}^{-1}\Lambda$ is a homomorphism $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$ which induces an isogeny

$$E \to \bar{\mathfrak{a}} * E \tag{1.8}$$

of degree $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$, (see Silverman [**59**] Corollary II.1.5).

For the remainder of this section, we let H be the Hilbert class field of K.

Lemma 1.1.19. *Let E/H be an elliptic curve with CM by $\mathcal{O}_K$ and let p be a rational prime which is not E-excluded, lying under the degree 1 prime $\mathfrak{p}$ of $\mathcal{O}_K$. Let $\mathfrak{P}$ be a prime of H lying over $\mathfrak{p}$. Let $\phi : E \to \bar{\mathfrak{p}} * E$ be the isogeny of* (1.8)*. Then $\phi_{\mathfrak{P}}$ is purely inseparable of degree p.*

Proof. See Silverman [**59**] p. 127. □

Lemma 1.1.20. *Let $\mathfrak{a}$ be a non-zero fractional ideal of K and let $\sigma := (H/K;\mathfrak{a})$ be the Artin automorphism of H/K associated with $\mathfrak{a}$. Then $j_E^\sigma = j_{\bar{\mathfrak{a}}*E}$ and hence over H^{alg}*

$$E^\sigma \cong \bar{\mathfrak{a}} * E.$$

Proof. See Silverman [**59**] Theorem II.4.3. □

Lemma 1.1.21 (Silverman [**58**] Corollary II.2.12)**.** *Let C and C' be smooth algebraic curves defined over a field of characteristic $p > 0$ and suppose that $\eta : C \to C'$ is a map of inseparable degree m, and let f be the mth-power Frobenius. Then η factors as $\eta = \zeta \circ f$ where ζ is separable.*

Proposition 1.1.22 (Silverman [**59**] Proposition II.5.3.)**.** *Let E be an elliptic curve with CM by $\mathcal{O}_K$ and let p be a rational prime which is not E-excluded, lying under the degree 1 prime $\mathfrak{p}$ of K. Let $\mathfrak{P}$ be a prime of H lying over $\mathfrak{p}$ and set $\sigma := (H/K;\mathfrak{p})$. Then there exists an isogeny $\phi_{\sigma,p} : E \to E^\sigma$ whose reduction modulo $\mathfrak{P}$ is the pth power Frobenius map f.*

Proof. Let $\phi : E \to E^\sigma$ be the isogeny obtained by composing

$$\begin{tikzcd} E \arrow[r, "\lambda"] & \bar{\mathfrak{p}} * E \arrow[r, "\eta"] & E^\sigma, \end{tikzcd}$$

where λ and η are the maps defined in (1.8) and Lemma 1.1.20 respectively. Then $\phi_{\mathfrak{P}}$ is a purely inseparable map of degree p by Lemma 1.1.19, and by Lemma 1.1.21, factors as $\phi_{\mathfrak{P}} = \zeta \circ f$, where $\zeta : E_{\mathfrak{P}}^{(p)} \to E_{\mathfrak{P}}^\sigma$ is a separable isogeny of degree 1.

Since $E_{\mathfrak{P}}^\sigma = E_{\mathfrak{P}}^{(p)}$ by definition, we are done if we can show that ζ is the reduction of an automorphism of E^σ. Since reduction of endomorphisms preserves degree, it is enough to show that ζ is the reduction of an endomorphism of E^σ. By Lemma 1.1.17 this is true if and only if ζ commutes with the reduction modulo $\mathfrak{P}$ of every element of $\mathrm{End}(E^\sigma)$. Let α be an element of $\mathrm{End}(E)$. We may regard α^σ as the corresponding element of $\mathrm{End}(E^\sigma)$. Now by Silverman [**59**] p. 132,

$$f \circ \alpha_{\mathfrak{P}} = (\alpha^\sigma)_{\mathfrak{P}} \circ f, \tag{1.9}$$

and by Corollary II.1.1.1 of Silverman [**59**]

$$\phi \circ \alpha = \alpha^\sigma \circ \phi$$

hence

$$\phi_{\mathfrak{P}} \circ \alpha_{\mathfrak{P}} = (\alpha^\sigma)_{\mathfrak{P}} \circ \phi_{\mathfrak{p}}$$

and the result follows since $\phi_{\mathfrak{P}} = \zeta \circ f$.

Let ξ be the automorphism of E^σ such that $\xi_{\mathfrak{P}} = \zeta$. We define

$$\phi_{\sigma,p} := \xi^{-1} \circ \phi = \xi^{-1} \circ \eta \circ \lambda.$$

□

Proposition 1.1.23. *Retaining the notation of Proposition 1.1.22, suppose that E is a $\mathbb{Q}$-curve. Then for any element σ of $\mathrm{Gal}(H/K)$ there exists a rational prime p such that $\phi_{\sigma,p} : E \to E^\sigma$ is an H-isogeny.*

Proof. We let p be a prime which is not E-excluded and consider the factors of $\phi_{\sigma,p} = \xi^{-1} \circ \eta \circ \lambda$ one by one. From the definitions we can see that ξ is an H-endomorphism of E^σ and that the map λ of (1.8) from E to $\bar{\mathfrak{p}} * E$ is defined over H.

It remains to check the isomorphism $\eta : \bar{\mathfrak{p}} * E \to E^\sigma$. We know that $\bar{\mathfrak{p}} * E$ is isogenous to E over H and that E is isogenous to E^σ over H, hence composing the isogenies and applying Lemma 1.1.20 gives the desired H-rational isogeny. □

1.2. Abelian Varieties

Let k be a field. In this section k may be either an algebraic number field, the completion of an algebraic number field, or a finite field.

Let V be an algebraic variety defined over k. We denote by $V(k)$ the set of points of V defined over k. We say that V is a *group variety* over k if the set of points $V(k^{alg})$ admits a group law $m : V \times V \to V$ such that m and the inverse map are both morphisms of varieties.

Definition 1.2.1. *An* abelian variety *is a projective group variety.*

The group law on an abelian variety is commutative (see Mumford [**31**] p. 44), hence it is customary to write it additively.

If a subvariety of A is an abelian variety, then we call it an abelian subvariety. We say that A is *simple* if none of its proper subvarieties are non-trivial abelian varieties.

Definition 1.2.2. *Let A and B be abelian varieties over k. A homomorphism $\varphi : A \to B$ is an* isogeny *if it is surjective, with finite kernel.*

In particular if A and B are isogenous, written $A \simeq B$, then they have the same dimension.

The *degree* of an isogeny is the degree of the extension $k(A)/k(\varphi^*(B))$, where φ^* denotes the pullback of φ. The separable degree of φ is the degree of the separable part of the extension and the cardinality of the kernel of φ.

Definition 1.2.3. *Let k and A be as above and let M be a normal subfield of k. We shall say that A is an M-variety if there exists a k-rational isogeny $\lambda_\sigma : A \to A^\sigma$ for all σ in $\mathrm{Gal}(k/M)$.*

For any positive integer m, let m_A denote multiplication by m on A, that is, the map sending a point P of A to the point

$$\underbrace{P + \cdots + P}_{m \text{ times}}$$

and let $A[m] := \ker m_A$.

Proposition 1.2.4 (Mumford [**31**] p. 63)**.** *Let k be a field of characteristic p, let m be a positive integer, and let A/k be an abelian variety of dimension g. The map $m_A : A \to A$ is an isogeny of degree m^{2g} which is separable if and only if m is coprime to p (including when $p = 0$).*

It follows that for all m, $A[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^i$ over k^{alg} for some integer $i \leq 2g$ with equality when m and p are coprime.

Let $\varphi : A \to B$ be an isogeny, and let m be an integer such that $\ker \varphi \subseteq A[m]$. Such an m must exist, since $\ker \varphi$ is finite and closed under $+$. Then there exists an isogeny $\hat{\varphi} : B \to A$ such that

$$\varphi \circ \hat{\varphi} = m_B,\ \hat{\varphi} \circ \varphi = m_A.$$

Theorem 1.2.5 (Poincaré's Complete Reducibility Theorem)**.**
If A is an abelian variety and B is an abelian subvariety of A then there exists an abelian subvariety B' such that A is isogenous to $B \times B'$.

Proof. See p. 173 of Mumford [**31**]. □

It follows that for any abelian variety A of dimension g there exist simple, pairwise non-isogenous abelian varieties $A_1, \ldots, A_n$ such that

$$A \simeq A_1^{a_1} \times \cdots A_n^{a_n}.$$

The group of endomorphisms of A defined over k is denoted $\mathrm{End}_k(A)$. Since $\mathrm{End}_k(A)$ contains a subring isomorphic to $\mathbb{Z}$, we can consider the *endomorphism algebra* of A,

$$\mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

For any ring T we let $\mathbb{M}_a(T)$ denote the ring of $a \times a$ matrices over T.

Proposition 1.2.6. *If A is simple then $\mathrm{End}_k^0(A)$ is a division algebra. If A is isogenous to a product $A_1^{a_1} \times \cdots \times A_n^{a_n}$ with the A_i simple and pairwise non-isogenous, then*

$$\mathrm{End}_k^0(A) \cong \sum_{i=1}^{n} \mathbb{M}_{a_i}(T_i),$$

where $T_i = \mathrm{End}_k^0(A_i)$.

Proof. If A is simple, then any non-zero endomorphism of A is an isogeny and hence has an inverse in $\mathrm{End}_k^0(A)$. It is clear that $\mathrm{Hom}(A_i, A_j) = 0$ for all $i \neq j$ and the result follows. □

Proposition 1.2.7 (Mumford [**31**] p. 176)**.** *Let A and B be any two abelian varieties. Then $\mathrm{Hom}(A, B)$ is a finitely generated free abelian group of rank at most $4 \dim A \dim B$.*

In particular, if A is an abelian variety of dimension g then $\mathrm{End}_k^0(A)$ is an algebra of dimension at most $4g^2$ over $\mathbb{Q}$.

Proposition 1.2.8 (Mumford [**31**] p. 182)**.** *Let A be a simple abelian variety of dimension g over k and let K be the centre of $\mathrm{End}_k^0(A)$. Suppose that $[K : \mathbb{Q}] = n$ and $[\mathrm{End}_k^0(A) : K] = d^2$. Then nd divides $2g$ and if $\mathrm{char}\, k = 0$ then nd^2 divides $2g$.*

A *CM field* K is an imaginary quadratic extension of a totally real field K_0. If K and L are CM fields, so are the normal closure of K and the compositum LK.

Lemma 1.2.9 (Shimura [**54**] p. 38)**.** *Let A and K be as in the previous proposition. Then K is either a totally real number field, or a CM field.*

Definition 1.2.10. *If A/k is an abelian variety of dimension g, we say that A is* of CM type *if $\mathrm{End}_k^0(A)$ contains a CM field K of degree $2g$.*

Proposition 1.2.11 (Shimura [**54**] Proposition 3)**.** *Let k be a number field and let A/k be an abelian variety of CM type. There exists a simple abelian variety B of CM type such that $A \times_k \mathbb{C}$ is isogenous to B^n for some integer n.*

1.2.1. CM Types. For any algebraic number field F, we consider the algebraic closure F^{alg} of F to be embedded in the complex numbers. Let ι be an embedding $F \hookrightarrow \mathbb{C}$. If F is normal over $\mathbb{Q}$ then any other embedding will have the form ι_σ for some $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ where $\iota_\sigma(x) := \iota(x^\sigma)$ for any element x of F.

Definition 1.2.12. *A* CM type *is a pair* (K, Φ) *such that* K *is a CM field of degree* $2g$ *over* $\mathbb{Q}$ *and* $\Phi = \{\phi_1, \ldots, \phi_g\}$ *is a set of embeddings of* K *into* $\mathbb{C}$ *such that no two* ϕ_i *are complex conjugate.*

We frequently identify Φ with the $g \times g$ diagonal matrix with entries $\{\phi_1, \ldots, \phi_g\}$. This allows us to define

$$\begin{aligned} \det \Phi(x) &:= \prod \phi_i(x), \\ \operatorname{tr} \Phi(x) &:= \sum \phi_i(x). \end{aligned}$$

Suppose that k is a subfield of K which is also a CM field, and let (k, Ψ) be a CM type. Let $\Psi_{K/k}$ be the set of homomorphisms $K \to \mathbb{C}$ which induce an element of Ψ on k. Then $(K, \Psi_{K/k})$ is a CM type, which we call the CM type lifted from (k, Ψ). A CM type (K, Φ) is *simple* if it has not been lifted from a proper subfield of K.

Let L be the field generated by the elements $\{\operatorname{tr} \Phi(x) : x \in K\}$. Let F be the normal closure of K, set $G = \operatorname{Gal}(F/\mathbb{Q})$, and let G_K and G_L be the subgroups of G corresponding to K and L respectively. We consider the ϕ_i in Φ as elements σ of G by identifying ι_σ with σ. Let $S := \cup G_K \phi_i$ and $S^{-1} := \{s^{-1} : s \in S\}$. By definition, G_L consists of the elements of G which fix S, and consequently there exist elements ψ_i for $i = 1, \ldots, m$ of G such that $S^{-1} = \cup G_L \psi_i$.

Definition 1.2.13. *Let* L *be as above and let* $\Psi := \{\psi_1, \ldots, \psi_m\}$*. The pair* (L, Ψ) *is a CM type, which we call the* reflex *of* (K, Φ).

We observe that $\det \Psi(x)$ is an element of K^* for all x in L^*.

If $K/\mathbb{Q}$ is abelian then the reflex of a simple CM type $(K, \{\phi_i\})$ is $(K, \{\phi_i^{-1}\})$ where as above, we identify the ϕ_i with elements of $\operatorname{Gal}(K/\mathbb{Q})$. In particular, if K is an imaginary quadratic field, then (K, Φ) is its own reflex.

Proposition 1.2.14 (Shimura [**54**] p. 63)**.** *Let* (K, Φ) *be a CM type with reflex* (L, Ψ)*. Then* (L, Ψ) *is simple, and if* (K, Φ) *is simple, it is the reflex of* (L, Ψ).

1.2.2. Abelian Varieties over $\mathbb{C}$**.** Let A be an abelian variety of dimension g defined over $\mathbb{C}$. Then there exists a lattice Λ_g in $\mathbb{C}^g$ and a holomorphic map f such that the sequence

$$0 \to \Lambda_g \to \mathbb{C}^g \xrightarrow{f} A \to 0, \tag{1.10}$$

is exact. It follows that any element γ of $\operatorname{End}^0_{\mathbb{C}}(A)$ corresponds to a $\mathbb{C}$-linear transformation Γ of $\mathbb{C}^g$, such that

$$\Gamma(\Lambda_g) \subseteq \Lambda_g \text{ and } f \circ \Gamma = \gamma \circ f. \tag{1.11}$$

The map sending γ to Γ can be uniquely extended to a representation S of $\mathrm{End}_{\mathbb{C}}(A)$ in $\mathbb{M}_g(\mathbb{C})$, known as the *analytic representation*. This induces a representation R on $\mathrm{End}_{\mathbb{Q}}(\Lambda \otimes \mathbb{Q}) \cong \mathbb{M}_{2g}(\mathbb{Q})$ known as the *rational representation*, and R is equivalent to the direct sum of S and its complex conjugate $\bar{S}$, (see for example Shimura [**54**] Section 3.2). Suppose that $\mathrm{End}^0_{\mathbb{C}}(A)$ contains a subalgebra isomorphic to a CM field K of degree $2g$ and let θ be an embedding of K in $\mathrm{End}^0_{\mathbb{C}}(A)$.

Lemma 1.2.15 (Shimura [**54**] p. 39)**.** *Let $\{\phi_1, \ldots, \phi_{2g}\}$ be the full set of embeddings of K into $\mathbb{C}$. The representation $R \circ \theta$ is equivalent to the direct sum of the ϕ_i.*

It follows that $S \circ \theta$ must be equivalent to the direct sum of g distinct ϕ_i say $\{\phi_1, \ldots, \phi_g\}$ no two of which are complex conjugate.

Definition 1.2.16. *Let $\Phi := \{\phi_1, \ldots, \phi_g\}$. We say that (A, θ) is of CM type (K, Φ).*

By (1.10), $S(\gamma)$ maps $\mathbb{Q}\Lambda_g$ to itself for all γ in $\mathrm{End}^0_{\mathbb{C}}(A)$, and because $[\mathbb{Q}\Lambda_g : \mathbb{Q}] = 2g$, there is an isomorphism $h : K \to \mathbb{Q}\Lambda_g$, which extends to an $\mathbb{R}$-linear isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}^g$. Let $\Lambda := h^{-1}(\Lambda_g)$. Then Λ is a $\mathbb{Z}$-lattice in K, and the following diagram is commutative, with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & \Lambda \arrow[r] \arrow[d] & K_{\mathbb{R}} \arrow[r] \arrow[d, "h"'] & K_{\mathbb{R}}/\Lambda \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Lambda_g \arrow[r] & \mathbb{C}^g \arrow[r, "f"] & A \arrow[r] & 0
\end{tikzcd}$$

Proposition 1.2.17. *If (A, θ) and (A', θ') are varieties of the same CM type (K, Φ) then A and A' are isogenous over $\mathbb{C}$.*

Proof. Let f and h be as in the diagram above, let Λ and Λ' be $\mathbb{Z}$-lattices in K corresponding to A and A' respectively, and let m be an integer such that $m\Lambda \subset \Lambda'$. Then $mh(\Lambda) \subset h(\Lambda')$ so there is a surjective homomorphism λ from $\mathbb{C}^g/h(\Lambda)$ to $\mathbb{C}^g/h(\Lambda')$ and $f \circ \lambda$ is an isogeny. □

Proposition 1.2.18 (Lang [**26**] Proposition 1.3.4)**.** *Let (A, θ) be an abelian variety of CM type (K, Φ), and suppose that B is a simple abelian variety with CM by a subfield K_0 of K such that $A_{\mathbb{C}}$ is isogenous to B^n for some integer $n \geq 1$. Then the CM type of A is lifted from the CM type of B.*

By Proposition 1.2.14 such a B always exists. This means that if a CM type is simple then the varieties of that type are simple over $\mathbb{C}$.

Theorem 1.2.19. *Let (K, Φ) be a CM type, let $g := [K : \mathbb{Q}]/2$ and let Λ be a $\mathbb{Z}$-lattice in K. Then $\Phi(\Lambda)$ is a lattice in $\mathbb{C}^g$ and $\mathbb{C}^g/\Phi(\Lambda)$ is complex-analytically isomorphic to an abelian variety A of CM type (K, Φ).*

Proof. This is a composite of Lang [**26**] Theorems 1.4.1 and 1.4.4. □

Combining this theorem with Proposition 1.2.17 shows that every CM type defines a unique isogeny class of abelian varieties over $\mathbb{C}$.

Definition 1.2.20. *Let F/k be a field extension and let A be an abelian variety defined over F. We say that A* descends *to k if there exists an abelian variety A_0 defined over k such that A_0 and A are isomorphic over F.*

Proposition 1.2.21 (Lang [**26**] Proposition 5.1.1)**.** *For any abelian variety $A/\mathbb{C}$ of CM type (K, Φ) there exists an algebraic number field k such that A descends to k.*

Definition 1.2.22. *Let F be an absolutely normal algebraic number field and let (A, θ) be an abelian variety defined over F of CM type (K, Φ). Let G be the subgroup of* $\mathrm{Gal}(F/\mathbb{Q})$ *consisting of the elements σ such that $(A^\sigma, \theta^\sigma)$ is isomorphic to (A, θ) over $\mathbb{C}$. Let k be the fixed field of G. We say that k is the* field of moduli *of A.*

Remark 1.2.23. The field of moduli of an elliptic curve E with complex multiplication by an order of K is $K(j_E)$. This classical result is a consequence of the Main Theorem of Complex Multiplication: see for example Silverman [**59**] for the theorem when $g = 1$ or Shimura [**54, 56**] for general g.

Proposition 1.2.24 (Shimura [**54**] Proposition 30)**.** *Let (K, Φ) be a CM type with reflex (K', Φ'), and suppose that A is an abelian variety defined over k such that $(A_{\mathbb{C}}, \theta)$ is of type (K, Φ). If* $\mathrm{End}_k^0(A)$ *is isomorphic to K then k contains K'. If A is simple over k then the converse holds.*

1.3. Good Reduction of Abelian Varieties

Given an elliptic curve E defined over a number field k, we defined the reduction of E at a prime $\mathfrak{p}$ of k in terms of a $\mathfrak{p}$-minimal Weierstrass model $\mathcal{E}$ for E. Given an abelian variety A/k we can follow a similar procedure using a scheme N called the local Néron model for A at $\mathfrak{p}$. Just as we said that E had good reduction at $\mathfrak{p}$ if $\mathcal{E}$ defined an elliptic curve over $F_{\mathfrak{p}}$, if the special fibre of N is an abelian variety then A has good reduction at $\mathfrak{p}$. We shall follow this path in Section 1.3.2.

It is also possible to take a very different approach via the ℓ-adic representation of A which is a homomorphism $\rho_\ell : \mathrm{Gal}(k^{alg}/k) \to \mathbb{M}_{2g}(\mathbb{Q}_\ell)$, where ℓ is a rational prime coprime to $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$. Let $\mathfrak{P}$ be a prime of k^{alg} dividing $\mathfrak{p}$. In this case, we say that A has good reduction at $\mathfrak{p}$ if ρ_ℓ maps the inertia group at $\mathfrak{P}$ to 1. To develop the tools for this approach we review the theory of ramification, inertia and decomposition groups in Section 1.3.1, and in Section 1.3.3 we look at Tate modules and ℓ-adic representations, and define the conductor of A/k in the case where A has good reduction everywhere over a finite extension of k.

1.3.1. Local Ramification Groups. Let F_v be a local field with residue characteristic p. Let x_v be a uniformizing element for the unique prime ideal of $\mathcal{O}_v$. We take v to be the additive valuation on F such that $v(x_v) = 1$. Similarly, if F is a number field and $\mathfrak{p}$ is a prime ideal of F with uniformizing element $x_{\mathfrak{p}}$ we normalize the valuation $v_{\mathfrak{p}}$ by setting $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = 1$.

Definition 1.3.1. *Let k_w be a local field with residue characteristic p, and let F_v be a finite Galois extension of k_w with valuation v. The* ith ramification group *of F_v/k_w is*

$$G_i(F_v/k_w) := \{\sigma \in \mathrm{Gal}(F_v/k_w) : v(\sigma(x) - x) \geq i + 1, \textit{ for all } x \in \mathcal{O}_v\}.$$

We extend the definition of the ith ramification group of F_v/k_w to real numbers $t \geq -1$ by setting $G_t := G_i$ for all t in $(i-1, i]$. Let $[G_i : G_j]$ denote the index of G_j in G_i for $j \geq i$, and for $j < i$ set

$$[G_i : G_j] := [G_j : G_i]^{-1}.$$

We then define

$$\varphi(t) := \int_0^t \frac{1}{[G_0 : G_y]} dy. \tag{1.12}$$

By the Hasse-Arf Theorem (see p. 76 of Serre [**49**]), if i is an integer such that G_i does not equal G_{i+1} then $\varphi(i)$ is an integer. We refer to Serre [**49**] IV.3 for further discussion and proofs of the properties of φ and its inverse φ^{-1}, noting that $\varphi^{-1}(i)$ is an integer for all integers $i \geq -1$.

Definition 1.3.2. *The* ith ramification group *of F_v/k_w* in the upper numbering *$G^{(i)}(F_v/k_w)$ is equal to $G_j(F_v/k_w)$ where $j = \varphi^{-1}(i)$.*

If $L_{v'}$ is a profinite Galois extension of k_w, then we define the upper and lower ramification groups of $L_{v'}/k_w$ by

$$G_n(L_{v'}/k_w) := \varprojlim G_n(F_v/k_w) \text{ and } G^{(n)}(L_{v'}/k_w) := \varprojlim G^{(n)}(F_v/k_w),$$

where F_v runs through the finite Galois extensions of k_w contained in $L_{v'}$.

Let $\mathcal{O}_w$ be the ring of elements x of k_w with $w(x) \geq 0$ and let U_w be the group of invertible elements of $\mathcal{O}_w$. Set $U_w^{(0)} := U_w$ and for any positive integer i define

$$U_w^{(i)} := \{x \in k_w^* : w(x - 1) \geq i\}. \tag{1.13}$$

Proposition 1.3.3 (Serre [**49**] p. 228)**.** *Let F_v/k_w be a finite abelian extension of local fields of characteristic $p > 0$, set $G := \mathrm{Gal}(F_v/k_w)$ and let $\psi : k_w^* \to G$ be the local Artin homomorphism. Then*

$$\psi(U_w^{(i)}) = G^{(i)}(F_v/k_w).$$

Definition 1.3.4. *Let F be an algebraic number field with algebraic closure F^{alg} and let L be a profinite extension of F contained in F^{alg}. Let $\mathfrak{P}$ be a prime of L which divides $\mathfrak{p}$, and let $G := \mathrm{Gal}(L/F)$. The* decomposition *and* inertia *groups of $\mathfrak{P}$ are the subgroups of G given by*

$$\begin{aligned} G_D(\mathfrak{P}) &:= \{\sigma \in G : \mathfrak{P}^\sigma = \mathfrak{P}\}, \\ G_T(\mathfrak{P}) &:= \{\sigma \in G : v_{\mathfrak{P}}(\sigma(x) - x) \geq 1 \textit{ for all } x \in L\}, \end{aligned}$$

respectively.

We recall that

$$G_D(\mathfrak{P}) \cong \mathrm{Gal}(L_{\mathfrak{P}}/F_{\mathfrak{p}}),$$

and

$$G_D(\mathfrak{P})/G_T(\mathfrak{P}) \cong \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{F}_{\mathfrak{p}}).$$

1.3.2. Néron Models. Details and proofs of the material in this section may be found in Bosch, Lütkebohmert and Reynaud [**5**] or Artin [**3**]. In Chapter IV of [**59**] Silverman gives a detailed exposition of Néron models of elliptic curves.

Let k be a number field, let $\mathfrak{p}$ be a finite place of k, let $k_{\mathfrak{p}}$ be the completion of k with respect to $\mathfrak{p}$, let $\mathcal{O}_{\mathfrak{p}}$ be the maximal order of $k_{\mathfrak{p}}$, and $\overline{k}_{\mathfrak{p}}$ its residue class field. Let S be an $\mathcal{O}_{\mathfrak{p}}$-scheme, (strictly, a $\mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$-scheme). The *generic fibre* of S is

$$S \times_{\mathcal{O}_{\mathfrak{p}}} k_{\mathfrak{p}},$$

and the *special fibre* of S is

$$S \times_{\mathcal{O}} \overline{k}_{\mathfrak{p}}.$$

Definition 1.3.5. *Let S be a scheme. A* group scheme *over S is a scheme which represents a functor from the category of schemes over S to the category of groups.*

See Shatz [**53**] p. 30, or Silverman [**59**] p. 306 for more details. An *abelian scheme* is a group scheme which is a relatively compact continuously varying family of abelian varieties.

Definition 1.3.6. *Let A be an abelian variety defined over k. We say that A has* good reduction *at $\mathfrak{p}$ if there exists an abelian scheme $A_{\mathfrak{p}}$ defined over $\mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$ such that A is isomorphic to the generic fibre $A_{\mathfrak{p}} \times_{\mathcal{O}_{\mathfrak{p}}} k_{\mathfrak{p}}$.*

Definition 1.3.7. *A* Néron model for A at $\mathfrak{p}$ *is a smooth group scheme N of finite type over $\mathcal{O}_\mathfrak{p}$ such that*

$$N \times_{\mathcal{O}_\mathfrak{p}} k_\mathfrak{p} \cong A,$$

with the universal property that for any smooth $\mathcal{O}_\mathfrak{p}$-scheme Y, and $k_\mathfrak{p}$-rational map $\lambda : Y \to A$, there is a unique extension of λ to a morphism of schemes $\lambda : Y \to N$.

Theorem 1.3.8. *For any place $\mathfrak{p}$ of k there exists a local Néron model $N(A, \mathfrak{p})$ of A at $\mathfrak{p}$ which is unique up to isomorphism.*

By the universal property of the Néron model, it follows that A has good reduction at $\mathfrak{p}$ if and only if $N(A, \mathfrak{p})$ is an abelian scheme.

Lemma 1.3.9 (Artin [**3**] Lemma 1.16)**.** *Let S be a scheme and let N be a smooth group scheme over S. There exists an open subgroup N^0 called the* connected component *such that for any algebraically closed field k the fibres $N^0 \times_S k$ are the connected components of the fibres $N \times_S k$.*

If N is an abelian scheme then N is equal to N^0.

Proposition 1.3.10. *Let $N := N(A, \mathfrak{p})$. Then $N^0 \times_{\mathcal{O}_p} k_\mathfrak{p}$ is the extension of an abelian variety by a linear group $T \times U$ where T is a torus and U is unipotent. Moreover there exists a finite extension F/k such that if $\mathfrak{P}$ is a prime of F dividing $\mathfrak{p}$ and $N_F := N(A_F, \mathfrak{P})$ then*

$$N_F^0 \times_{\mathcal{O}_\mathfrak{P}} F_\mathfrak{P} \cong A' \times T',$$

where A' is an abelian variety and T' is a torus.

Proof. For the first statement, see Section 5 of Rosenlicht [**43**] and for the second, see Théorème 3.6 of Grothendieck [**18**]. □

Example 1.3.11. Let k be a number field, let E/k be an elliptic curve with bad reduction at $\mathfrak{p}$, and let $N := N(E, \mathfrak{p})$. Then $N^0(k_\mathfrak{p}) = E^{ns}(k_\mathfrak{p})$, and if E has multiplicative reduction then N^0 is a torus of dimension 1. (See Silverman [**59**] Corollary 9.1 and 9.2.) The second part of the proposition tells us that E_L has either good or multiplicative reduction at every prime of some finite extension F of k.

Definition 1.3.12. *An abelian variety A over k has* potential good reduction *at $\mathfrak{p}$ if there exists a finite extension F/k such that A_F has good reduction at every prime $\mathfrak{P}$ of F dividing $\mathfrak{p}$.*

If A has good reduction at every prime $\mathfrak{p}$ of k, then we say that A has *good reduction everywhere* or GRE.

1.3.3. Tate Modules. Let k be a field, and let A/k be an abelian variety of dimension g. By Proposition 1.2.4, and Mumford [**31**] Chapter IV, the group $A[m]$ of m-torsion points of A over k^{alg} is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2g$. We define

$$T_\ell(A) = \varprojlim A[\ell^n],\ V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell, \tag{1.14}$$

and call $T_\ell(A)$ the *ℓ-adic Tate module* of A. By the definition of the inverse limit there are isomorphisms

$$T_\ell(A) \cong \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} = \mathbb{Z}_\ell^{2g},\ V_\ell(A) \cong \mathbb{Q}_\ell^{2g}.$$

Definition 1.3.13. *Let $G := \mathrm{Gal}(k^{alg}/k)$ and let $\rho_\ell := \rho_\ell(A)$ be the representation*

$$\rho_\ell : G \to \mathrm{Aut}(T_\ell(A))$$

*defined by the action of G on $T_\ell(A)$. We call ρ_ℓ the ℓ-*adic representation associated with A.

Suppose that k is a number field, let $\mathfrak{p}$ be a prime of k, let $\mathfrak{P}$ be a prime of k^{alg} dividing $\mathfrak{p}$ and set

$$G^{(i)}(\mathfrak{p}) := G^{(i)}(k^{alg}_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

Proposition 1.3.14 (Serre-Tate [**51**] Theorems 1 and 2)**.** *Let ℓ be a rational prime which is coprime to $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$. The variety A has good reduction at $\mathfrak{p}$ if and only if $G_T(\mathfrak{p})$ acts trivially on $T_\ell(A)$, and potential good reduction at $\mathfrak{p}$ if and only if $\rho_\ell(G_T(\mathfrak{p}))$ is finite.*

We define

$$A_{\mathfrak{p}} := N(A,\mathfrak{p}) \times_{\mathcal{O}_{\mathfrak{p}}} k_{\mathfrak{p}},\ \text{and } \widetilde{A}_{\mathfrak{p}} := N(A,\mathfrak{p}) \times_{\mathcal{O}_{\mathfrak{p}}} \overline{k}_{\mathfrak{p}}. \tag{1.15}$$

Let $\mathfrak{p}$ be a prime of k at which A has good reduction and let ℓ be a rational prime which is coprime to $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$. Then

$$T_\ell(A) \cong T_\ell(\widetilde{A}_{\mathfrak{p}}). \tag{1.16}$$

Let A, k, $\mathfrak{p}$ and ℓ be as in Proposition 1.3.14 and suppose that A has potential good reduction at $\mathfrak{p}$. Let F be a finite Galois extension of k such that $B := A_F$ has good reduction at every prime $\mathfrak{P}$ of F dividing $\mathfrak{p}$. Then $G := \mathrm{Gal}(F_{\mathfrak{P}}/k_{\mathfrak{p}})$ acts on $\widetilde{B}_{\mathfrak{P}}$ via its action on $F_{\mathfrak{P}}$ and since there are canonical isomorphisms $T_\ell(\widetilde{B}_{\mathfrak{P}}) \cong T_\ell(B) \cong T_\ell(A)$ we can define an action of G on $T_\ell(A)$.

Let G_i be the ith ramification group of $F_{\mathfrak{P}}/k_{\mathfrak{p}}$, set $n_i := |G_i|$ and define

$$f_{\mathfrak{p}} := \sum_i \frac{n_i}{n_0}\left(2g - \dim T_\ell(A)^{G_i}\right), \tag{1.17}$$

where $g := \dim A$.

Lemma 1.3.15. *With notation as above, $f_{\mathfrak{p}}$ is a non-negative integer independent of the choice of ℓ.*

Proof. Let ϕ_A be the character of the ℓ-adic representation of G and let a_G denote the Artin character of G. By Theorem 4 of Serre-Tate [**51**] and its Corollary,

$$\langle a_G, \phi_A \rangle := \frac{1}{|G|} \sum_{\sigma \in G} a_G(\sigma^{-1}) \phi_A(\sigma),$$

is a non-negative integer independent of ℓ and by Corollary 1' on p. 100 of Serre [**49**], $f_{\mathfrak{p}} = \langle a_G, \phi_A \rangle$. □

Definition 1.3.16. *Let A/k be an abelian variety of CM type. The* local conductor *of A at a place $\mathfrak{p}$ of k is*

$$\mathfrak{f}_{A,\mathfrak{p}} := \mathfrak{p}^{f_{\mathfrak{p}}},$$

with $f_{\mathfrak{p}}$ as in Lemma 1.3.15, and the conductor *of A over k is*

$$\mathfrak{f}_A := \prod_{\mathfrak{p}\,\textit{finite}} \mathfrak{f}_{A,\mathfrak{p}}.$$

See for example Serre [**50**] for the definition of $\mathfrak{f}_{A,\mathfrak{p}}$ when A does not have potential good reduction at $\mathfrak{p}$.

Proposition 1.3.17 (Serre-Tate [**51**] Theorem 6(a) and (c))**.** *Let A/k be an abelian variety of CM type and set $G := \mathrm{Gal}(k^{alg}/k)$. Let $\mathfrak{p}$ be a place of k, let ℓ be coprime to $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$ and define $m_{\mathfrak{p}}$ to be the smallest non-negative integer m such that $\rho_\ell(G^{(m)}(\mathfrak{p})) = 1$. Then A has potential good reduction at $\mathfrak{p}$ and*

$$f_{\mathfrak{p}} = 2g \cdot m_{\mathfrak{p}}.$$

Let

$$\rho_\ell^* : G/G_T(\mathfrak{P}) \to \mathrm{Aut}(T_\ell(A)^{G_T(\mathfrak{P})})$$

be the natural representation of the quotient group afforded by ρ_ℓ. We define the *L-polynomial* of A at $\mathfrak{p}$ to be

$$L_{\mathfrak{p}}(A/F, T) := \det[1 - \rho_\ell^*(\pi_{\mathfrak{p}})T]. \tag{1.18}$$

where $\pi_{\mathfrak{p}}$ is the Frobenius endomorphism.

Definition 1.3.18. *With notation as above, the L-series of A/F is*

$$\begin{aligned} L(A/F, s) &:= \prod_{\mathfrak{p}} L_{\mathfrak{p}}(A/F, \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-1} \\ &= \prod_{\mathfrak{p}} \det\left[1 - \frac{\rho_\ell^*(\pi_{\mathfrak{p}})}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^s}\right]^{-1}, \end{aligned} \tag{1.19}$$

where ℓ is chosen to ensure $\ell \neq \operatorname{char}\overline{F}_{\mathfrak{p}}$.

Example 1.3.19. Let E be an elliptic curve over F with good reduction at $\mathfrak{p}$. Then $V_\ell(\widetilde{E_{\mathfrak{p}}})$ is isomorphic to $\mathbb{Q}_\ell^2$, hence $\rho_\ell^*(\pi_{\mathfrak{p}})$ can be represented by a matrix Π in $\mathbb{M}_2(\mathbb{Z})$ since it is independent of the choice of $\ell \neq p$. Then we have

$$\begin{aligned} L_{\mathfrak{p}}(E/F,T) &= 1-(\operatorname{tr}\Pi)T+(\det\Pi)T^2 \\ &= 1-a_{\mathfrak{p}}T+\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})T^2, \end{aligned}$$

where

$$a_{\mathfrak{p}} := 1+\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})-\#\widetilde{E_{\mathfrak{p}}}(\overline{F}_{\mathfrak{p}}).$$

If E has bad reduction at $\mathfrak{p}$ then

$$L_{\mathfrak{p}}(E/F,T)=\begin{cases} 1-T & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1+T & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{p}, \\ 1 & \text{if } E \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

See Silverman [**59**] Section II.10 for further details.

In Example 1.3.19 we gave two definitions for the local factors of the L-series of E at primes of good reduction, the second of which is purely determined by the cardinality of $\widetilde{E_{\mathfrak{p}}}(\overline{F}_{\mathfrak{p}})$. If C/F is a non-singular projective curve of genus g then one may similarly define the L-polynomial of C/F at primes of $\mathfrak{p}$ where $\widetilde{C_{\mathfrak{p}}}$ is non-singular, and if A is the Jacobian of C then these polynomials will coincide with $L_{\mathfrak{p}}(A/F,T)$ as defined in (1.18).

Now suppose that A/k has complex multiplication by an order $\mathcal{O}$ of a CM field K. Let ℓ be a rational prime, and define $K_\ell := K \otimes \mathbb{Q}_\ell$ and $\mathcal{O}_\ell := \mathcal{O} \otimes \mathbb{Z}_\ell$.

Lemma 1.3.20 (Serre-Tate [**51**] p. 503)**.** *If $\ell \neq \operatorname{char} k$ then the map*

$$\operatorname{End}(A) \otimes \mathbb{Q}_\ell \to \operatorname{End}(V_\ell(A))$$

is injective.

The action of $\mathcal{O}$ on $T_\ell(A)$ makes $T_\ell(A)$ an $\mathcal{O}_\ell$-module and $V_\ell(A)$ a K_ℓ-module. By Lemma 1.3.20, K_ℓ acts faithfully on $V_\ell(A)$, so, since they both have dimension $2g$ over $\mathbb{Q}_\ell$, $V_\ell(A)$ is a free K_ℓ-module of rank 1.

Lemma 1.3.21. *Let x be an element of K_ℓ. If $xT_\ell(A)$ is contained in $T_\ell(A)$, then x is an element of $\mathcal{O}_\ell$.*

Proof. Let x be as in the lemma, and let n be a non-negative integer such that $\ell^n x$ is in $\mathcal{O}_\ell$ and y an element of $\mathcal{O}$ such that $y \equiv \ell^n \bmod \ell^n\mathcal{O}_\ell$. Then $\ell^n xT_\ell(A) \subset \ell^n T_\ell(A)$ by our assumption on x, $yT_\ell(A) \subset \ell^n T_\ell(A)$. But then y vanishes on ℓ^n-torsion points of A, so there exists y_0 in $\mathcal{O}$ such that $y = \ell^n y_0$ and $y_0 \equiv x \bmod \mathcal{O}_\ell$, hence x is an element of $\mathcal{O}_\ell$. □

Proposition 1.3.22. *Considering $\mathcal{O}_\ell$, K_ℓ and $\mathrm{End}(T_\ell(A))$ to be subrings of $\mathrm{End}(V_\ell(A))$,*

a) *The commutator of $\mathcal{O}$ in $\mathrm{End}(V_\ell(A))$ is K_ℓ.*
b) *The commutator of $\mathcal{O}$ in $\mathrm{End}(T_\ell(A))$ is $\mathcal{O}_\ell$.*
c) *The commutator of $\mathcal{O}$ in $\mathrm{End}(A)$ is $\mathcal{O}$.*

The proof follows directly from Lemma 1.3.20 and Lemma 1.3.21.

Corollary 1.3.23. *The image of the ℓ-adic representation ρ_ℓ is a subgroup of the group of invertible elements of $\mathcal{O}_\ell$.*

Proof. Let σ be an element of $\mathrm{Gal}(k^{alg}/k)$. Since $\rho_\ell(\sigma)$ commutes with every element of $\mathcal{O}$, by part b) of Proposition 1.3.22, it must be an element of $\mathcal{O}_\ell$. □

CHAPTER 2

Character Theory

In this chapter we investigate continuous homomorphisms from the idele group $\mathfrak{I}_F$ of a number field F into the multiplicative group of $\mathbb{C}$ which are trivial on F^*. We call such homomorphisms *Hecke characters* of $\mathfrak{I}_F$.

In the first section, which largely follows the exposition of Heilbronn [**23**], we establish some basic definitions and properties and then focus upon the subset of Hecke characters which correspond, via the Artin mapping, to characters of $\mathrm{Gal}(F^{ab}/F)$. We call these characters *Dirichlet characters* of $\mathfrak{I}_F$. In Section 2.2 we describe in detail the quadratic Dirichlet characters of the idele group of an imaginary quadratic field.

A second important class of Hecke characters are defined by abelian varieties of CM type. Let A/F be an abelian variety of CM type (K, Φ) with good reduction at $\mathfrak{p}$, and let $\pi_{\mathfrak{p}}$ be the Frobenius endomorphism of the special fibre of the local Néron model $\widetilde{A_{\mathfrak{p}}}$. Since $\pi_{\mathfrak{p}}$ is in the image of the natural embedding $K \hookrightarrow \mathrm{End}^0_{\overline{F}_{\mathfrak{p}}}(\widetilde{A_{\mathfrak{p}}})$ we have found a map from the set of primes of F at which A has good reduction to K. In Section 2.3 we shall extend this map to a homomorphism χ_A from $\mathfrak{I}_F$ to K called the *Grössencharacter* of A. This is an isogeny invariant of A, and we will see that A is a k-variety (in the sense of Definition 1.2.3), if and only if χ_A is fixed by every element of $\mathrm{Gal}(F/k)$. The relationship between Dirichlet characters and Grössencharacters is as follows: if L/F is a quadratic extension associated with the Dirichlet character ϕ_L and B is the twist of A with respect to L, then the Grössencharacter χ_B of B satisfies

$$\chi_B = \phi_L \cdot \chi_A.$$

Theorem 2.3.9 describes when a Hecke character of $\mathfrak{I}_F$ occurs as the Grössencharacter of an abelian variety of given CM type (K, Φ). If k is a proper subfield of F and there exists a Hecke character χ of $\mathfrak{I}_k$ such that

$$\chi_A = \chi \circ \mathrm{N}_{F/k},$$

then we say that A is of k-type 1. The results of Sections 2.2 and 2.3 will be applied in Section 4.1 to obtain a full description of the elliptic curves of K-type 1 defined over the Hilbert class field of an imaginary quadratic field K.

2.1. Hecke Characters

Let F be an algebraic number field and let S_0 be the set of infinite places of F. Let S be the union of S_0 and a finite set of primes of F and let I_S be the group of fractional ideals coprime to S.

Definition 2.1.1. *Let T be a set of places of F. We define $\mathfrak{U}_T$ be the set of ideles $\boldsymbol{\alpha}$ of $\mathfrak{J}_F$ such that $\alpha_{\mathfrak{p}} = 1$ for all $\mathfrak{p}$ in T and $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0$ for all $\mathfrak{p}$ not in T.*

If $S = S_0$ then $\mathfrak{U}_S = U_F$, the subgroup of $\mathfrak{J}_F$ introduced in Definition 1.1.11.

Definition 2.1.2. *A* Hecke character *of $\mathfrak{J}_F$ with* exceptional set *S is a continuous homomorphism $\chi : \mathfrak{J}_F \to \mathbb{C}^*$ such that the kernel of χ contains $F^*\mathfrak{U}_S$.*

If $|\chi(\boldsymbol{\alpha})| = 1$ for all $\boldsymbol{\alpha}$ in $\mathfrak{J}_F$, then χ is an *ordinary character* of $\mathfrak{J}_F$.

Definition 2.1.3. *Let χ be a Hecke character of $\mathfrak{J}_F$ with exceptional set S. Then the* Hecke L-series *of χ with respect to S is defined as*

$$L_F^S(\chi, s) := \prod_{\mathfrak{p} \notin S} \left(1 - \frac{\chi(\mathfrak{p})}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^s}\right)^{-1}. \tag{2.1}$$

Definition 2.1.4. *Let $\mathfrak{a} = \prod \mathfrak{p}^{a_{\mathfrak{p}}}$ be an ideal of I_F, and for every prime $\mathfrak{p}$ of F let $\pi_{\mathfrak{p}}$ be an element of F such that $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$. Let $\boldsymbol{\alpha}(\mathfrak{a})$ be the idele with components given by*

$$\boldsymbol{\alpha}(\mathfrak{a})_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \in S_0, \\ \pi_{\mathfrak{p}}^{a_{\mathfrak{p}}} & \text{otherwise.} \end{cases} \tag{2.2}$$

Given a Hecke character χ of $\mathfrak{J}_F$ with exceptional set S, it is customary, and frequently convenient for calculations, to regard χ as a homomorphism $I_S \to \mathbb{C}^*$ by setting

$$\chi(\mathfrak{a}) := \chi(\boldsymbol{\alpha}(\mathfrak{a})) \text{ for all } \mathfrak{a} \in I_S. \tag{2.3}$$

The definition is independent of the choice of $\pi_{\mathfrak{p}}$ in (2.2), since any two choices determine the same class in $\mathfrak{J}_F/\mathfrak{U}_S$.

Definition 2.1.5. *For any idele $\boldsymbol{\alpha}$, let $\iota_{\mathfrak{p}}(\boldsymbol{\alpha})$ be the idele with $\mathfrak{p}$-component $\alpha_{\mathfrak{p}}$ which is 1 everywhere else. Let $\chi_{\mathfrak{p}}(\boldsymbol{\alpha}) := \chi(\iota_{\mathfrak{p}}(\boldsymbol{\alpha}))$. We call $\chi_{\mathfrak{p}}$ a* local component *of χ. We say that $\chi_{\mathfrak{p}}$ is a* finite *or* infinite component *of χ according to whether $\mathfrak{p}$ is a finite or infinite place of F.*

Each $\chi_{\mathfrak{p}}$ is a Hecke character of $\mathfrak{J}_F$, and

$$\chi(\boldsymbol{\alpha}) = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(\boldsymbol{\alpha}).$$

Proposition 2.1.6. *Let χ be a Hecke character of $\mathfrak{I}_F$. For every prime $\mathfrak{p}$ of F, there exists a minimal non-negative integer $n_\mathfrak{p}$ such that $\chi_\mathfrak{p}(1+\mathfrak{p}^{n_\mathfrak{p}}) = 1$. Moreover, $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$.*

Proof. Let N be a neighbourhood of 1 in $\mathbb{C}^*$ which contains no subgroup of $\chi(\mathfrak{I}_F)$ except $\{1\}$. Since χ is continuous, there exists a neighbourhood N' of 1 in $\mathfrak{I}_F$ such that $\chi(N') \subset N$, and for such a neighbourhood there exists a finite set T of primes of $\mathfrak{I}_F$, and integers $\{t_\mathfrak{p} : \mathfrak{p} \in T\}$ such that

$$v_\mathfrak{p}(\alpha_\mathfrak{p} - 1) > t_\mathfrak{p} \text{ for } \mathfrak{p} \in T \text{ and } v_\mathfrak{p}(\alpha_\mathfrak{p}) = 0 \text{ for } \mathfrak{p} \notin T$$

for all α in N'. Choosing N' to have both T and each $t_\mathfrak{p}$ as small as possible, we set

$$n_\mathfrak{p} = \begin{cases} t_\mathfrak{p} & \text{if } \mathfrak{p} \in T, \\ 0 & \text{otherwise.} \end{cases}$$

□

The smallest possible exceptional set for which χ is defined is $S_m := S_0 \cup T$, with T as in the proof of Proposition 2.1.6. This allows us to make a canonical choice amongst the Hecke L-series associated with χ and we define

$$L_F(\chi, s) := L_F^{S_m}(\chi, s). \tag{2.4}$$

Definition 2.1.7. *The* conductor *of χ is the ideal*

$$\mathfrak{f}_\chi = \prod_{\mathfrak{p}\, \textit{finite}} \mathfrak{p}^{n_\mathfrak{p}},$$

where for each prime $\mathfrak{p}$ the exponent $n_\mathfrak{p}$ is the integer defined in Proposition 2.1.6. We say that χ is ramified *at $\mathfrak{p}$ if $\mathfrak{p}$ divides $\mathfrak{f}_\chi$.*

If $\chi_\mathfrak{p}$ has finite order for all $\mathfrak{p}$ in S_0 then we say that χ has *discrete infinite components*. By the continuity of $\chi_\mathfrak{p}$ this means that if $\mathfrak{p}$ is complex then $\chi_\mathfrak{p} = 1$ and if $\mathfrak{p}$ is real then $\chi_\mathfrak{p}$ is either the identity character or $\mathrm{sgn}_\mathfrak{p}$ where

$$\mathrm{sgn}_\mathfrak{p}(\boldsymbol{\alpha}) = \mathrm{sgn}(\alpha_\mathfrak{p}) \text{ for all } \boldsymbol{\alpha} \in \mathfrak{I}_F. \tag{2.5}$$

Remark 2.1.8. If $\chi_\mathfrak{p}$ has finite order then $\chi_\mathfrak{p}$ is ordinary, but the converse need not hold. As a counterexample, suppose that $\mathfrak{p}$ is a complex place of F and consider the character

$$\chi_\mathfrak{p}(\boldsymbol{\alpha}) = \frac{\alpha_\mathfrak{p}}{(\alpha_\mathfrak{p}\overline{\alpha}_\mathfrak{p})^{1/2}}.$$

2.1.1. Dirichlet Characters and Field Extensions. There is an important subclass of ordinary Hecke characters of $\mathfrak{I}_F$ which correspond to abelian extensions of L/F by class field theory. We call such characters *Dirichlet characters* and describe the correspondence below.

Definition 2.1.9. *Let $\mathcal{O}$ be an order of F and let $\mathfrak{m}$ be an ideal of $\mathcal{O}$. The* support *of $\mathfrak{m}$, denoted $\operatorname{supp}\mathfrak{m}$, is the set of primes of $\mathcal{O}$ dividing $\mathfrak{m}$.*

Definition 2.1.10. *Let $\mathfrak{m}$ be an integral ideal of F and let x and y be field elements of F. We say that x is* congruent to y modulo $\mathfrak{m}$, *symbolically that $x \equiv y \bmod \mathfrak{m}$, if*

$$v_{\mathfrak{p}}(x-y) \geq v_{\mathfrak{p}}(\mathfrak{m}) \textit{ for all prime ideals } \mathfrak{p} \textit{ of } F.$$

Lemma 2.1.11. *Let χ be a Hecke character of $\mathfrak{I}_F$. For any principal ideal $\mathfrak{b} = (b)$ such that b is congruent to 1 modulo $\mathfrak{f}_\chi$,*

$$\chi(\mathfrak{b}) = \prod_{\mathfrak{p}\in S_0} \chi_{\mathfrak{p}}(b^{-1}).$$

Proof. The idele $\boldsymbol{\beta} := \boldsymbol{\alpha}(\mathfrak{b})$ has $\mathfrak{p}$-component 1 for all $\mathfrak{p}$ in S and is b everywhere else. Multiplying by the principal idele b^{-1} we have

$$\chi(\mathfrak{b}) = \prod_{\mathfrak{p}\in S} \chi_{\mathfrak{p}}(b^{-1}),$$

but our choice of b ensures that $\chi_{\mathfrak{p}}(b) = 1$ for all finite $\mathfrak{p}$ in S. □

We say that an element x of F is *totally positive* if for every real infinite place $\mathfrak{p}$ of F the natural embedding of F into $F_{\mathfrak{p}} \cong \mathbb{R}$ maps x to a positive number.

Definition 2.1.12. *A* modulus *is a formal product of finite and real infinite places of F: $\mathfrak{m} := \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ where each $n_{\mathfrak{p}}$ is a non-negative integer which is 0 for almost all $\mathfrak{p}$ and if $\mathfrak{p}$ is a real infinite place of F then $n_{\mathfrak{p}} \leq 1$. If $\mathfrak{a}$ is an integral ideal of F we denote by $\mathfrak{a}_0$ the modulus defined by*

$$\mathfrak{a}_0 := \mathfrak{a} \cdot \prod_{\mathfrak{p}\in S_0^+} \mathfrak{p},$$

where S_0^+ denotes the subset of real infinite places of S_0.

Let $S = S_0 \cup \operatorname{supp}\mathfrak{m}$, define $P_{\mathfrak{m}}$ to be the group of principal ideals of I_S and $P_{\mathfrak{m},1}$ to be the subgroup of $P_{\mathfrak{m}}$ generated by principal ideals of the form $\mathfrak{b} = (b)$ where $b \equiv 1 \bmod \mathfrak{m}$. We define $P^+_{\mathfrak{m},1}$ to be the subgroup of $P_{\mathfrak{m},1}$ with totally positive generators. The *ray class group of conductor* $\mathfrak{m}_0$ is the quotient $I_F/P^+_{\mathfrak{m},1}$.

Proposition 2.1.13. *Let χ be an ordinary character of $\mathfrak{I}_F$ with discrete infinite components, and let $\mathfrak{m}$ be an integral ideal divisible by $\mathfrak{f}_\chi$. Then χ is a linear character of the ray class group of F with conductor $\mathfrak{m}_0$. Conversely, if η is a linear character of the ray class group of F with conductor $\mathfrak{m}_0$, then it arises from a character χ with discrete infinite components and exceptional set $S_0 \cup \operatorname{supp} \mathfrak{m}$.*

Proof. The first part of the proposition says that if χ is an ordinary character of $\mathfrak{I}_F$ with discrete infinite components then $\chi(\mathfrak{b}) = 1$ for all principal ideals $\mathfrak{b} = (b)$ of F such that b is totally positive and $b \equiv 1 \bmod \mathfrak{m}$. By Lemma 2.1.11,

$$\chi(\mathfrak{b}) = \prod_{\mathfrak{p} \in S_0} \chi_\mathfrak{p}(b^{-1}).$$

and since χ has discrete infinite components and (b^{-1}) is totally positive, the result follows directly.

Let $S = S_0 \cup \operatorname{supp} \mathfrak{m}$ and let η be a character of I_S which is 1 on $P^+_{\mathfrak{m},1}$. We wish to show that there exists an ordinary character χ of $\mathfrak{I}_F$ with exceptional set S such that for all ideals $\mathfrak{a}$ in I_S,

$$\chi(\boldsymbol{\alpha}(\mathfrak{a})) = \eta(\mathfrak{a}), \tag{2.6}$$

where $\boldsymbol{\alpha}(\mathfrak{a})$ is the idele defined in (2.2).

Let $\eta_\mathfrak{m}$ be the restriction of η to $P_\mathfrak{m}$. We know that $\eta_\mathfrak{m}((a))$ is 1 whenever a is totally positive, and it follows that there must be a subset T of S_0 such that

$$\eta_\mathfrak{m} = \prod_{\mathfrak{p} \in T} \operatorname{sgn}_\mathfrak{p}.$$

We also denote by $\eta_\mathfrak{m}$ the map $F^* \to \{\pm 1\}$ sending x to $\prod_{\mathfrak{p} \in T} \operatorname{sgn}_\mathfrak{p}(x)$.

Let η_1 denote the restriction of η to $P_{\mathfrak{m},1}$ and $\eta' := \eta_1 \eta_\mathfrak{m}^{-1}$. Let $\chi_\mathfrak{p}(\boldsymbol{\alpha}) := 1$ for $\mathfrak{p}$ in $S_0 \setminus T$ and for $\mathfrak{p}$ in T let

$$\chi_\mathfrak{p}(\boldsymbol{\alpha}) := \operatorname{sgn}_\mathfrak{p}(\alpha_\mathfrak{p}^{-1}) \tag{2.7}$$

for $\alpha_\mathfrak{p}$ in F^*; this has a unique continuous extension to $F^*_\mathfrak{p}$. For primes $\mathfrak{p}$ outside S, let $a_\mathfrak{p} := v_\mathfrak{p}(\alpha_\mathfrak{p})$ and define

$$\chi_\mathfrak{p}(\boldsymbol{\alpha}) := \eta(\mathfrak{p}^{a_\mathfrak{p}}), \tag{2.8}$$

for all $\boldsymbol{\alpha}$ in $\mathfrak{I}_F$.

For primes $\mathfrak{p}$ in $S \setminus S_0$, we first find an element x of F^* such that $v_\mathfrak{p}(x\alpha_\mathfrak{p}) = 0$ for all $\mathfrak{p}$ in $S \setminus S_0$. By the Chinese Remainder Theorem, there exists an element y of F^* such that $y \equiv x\alpha_\mathfrak{p} \bmod \mathfrak{m}$ for all $\mathfrak{p}$ in $S \setminus S_0$, and we set

$$\prod_{\mathfrak{p} \in S \setminus S_0} \chi_\mathfrak{p}(\boldsymbol{\alpha}) := \eta'(y). \tag{2.9}$$

Equation (2.8) shows that χ satisfies (2.6), and also ensures that $\ker\chi$ contains $\mathfrak{U}_S$. Combining Equations (2.7), (2.8) and (2.9) we see that $|\chi(\boldsymbol{\alpha})| = 1$ for all $\boldsymbol{\alpha}$ in $\mathfrak{I}_F$, and that $\chi(F^*) = 1$, so it only remains to check that χ is continuous in the idele topology. Now, by construction $\ker\chi$ contains the set of ideles $\boldsymbol{\alpha}$ such that

a) $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0$ for all $\mathfrak{p}$ not in S,
b) $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}} - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ for all $\mathfrak{p}$ in $S \setminus S_0$, and
c) $\mathrm{sgn}_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) > 0$ for all $\mathfrak{p}$ in S_0^+.

This is an open set in the idele topology, so $\ker\chi$ is open and χ is continuous. □

Definition 2.1.14. *Let* $\mathfrak{m}$ *be an ideal of* F*. An ordinary character* χ *of* $\mathfrak{I}_F$ *with discrete infinite components and exceptional set contained in* $S_0 \cup \operatorname{supp}\mathfrak{m}$ *is called a* Dirichlet character of modulus $\mathfrak{m}$.

Let $\mathfrak{m}$ be an integral ideal and G be a group of Dirichlet characters of modulus $\mathfrak{m}$. Let

$$M := \bigcap_{\chi\in G} \ker(\chi) \text{ and } N := M/F^*.$$

Then N is an open subgroup of $C_F := \mathfrak{I}_F/F^*$ and hence by the Existence Theorem of global class field theory, there exists a unique abelian extension L/F such that $\mathrm{N}_{L/F}(C_L) = N$. We call L/F the extension associated with G.

Given a finite abelian extension L/F we define the group of Dirichlet characters of $\mathfrak{I}_F$ corresponding to L/F to be those which correspond via the Artin mapping to characters of $\mathrm{Gal}(L/F)$. In particular, if L/F is quadratic then we shall say that χ is the Dirichlet character corresponding to L/F if χ generates the group of Dirichlet characters of $\mathfrak{I}_F$ corresponding to L/F.

Definition 2.1.15. *Let* L/F *be a finite abelian extension associated with a group of Dirichlet characters* G *of modulus* $\mathfrak{m}$*. The* conductor *of* L/F *is the ideal* $\mathfrak{f}_L := \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{a_{\mathfrak{p}}}$ *where for each* $\mathfrak{p}$ *in* $\operatorname{supp}\mathfrak{m}$,

$$a_{\mathfrak{p}} := \max\{v_{\mathfrak{p}}(\mathfrak{f}_\chi) : \chi \in G\}.$$

Let k be an algebraic number field contained in F. Then if χ_k is a character of $\mathfrak{I}_k$ with exceptional set S_k, composition with the norm mapping defines a character $\chi := \chi_k \circ \mathrm{N}_{F/k}$ of $\mathfrak{I}_F$ with exceptional set S containing every prime of F which divides an element of S_k. Note that even if S_k is a minimal exceptional set for χ_k, if F/k is ramified at some prime in S_k then S need not be a minimal exceptional set for χ.

Lemma 2.1.16. *Let* F/k *be an abelian extension and suppose that* χ_k *is a Dirichlet character of* $\mathfrak{I}_k$*; set* $\chi := \chi_k \circ \mathrm{N}_{F/k}$ *and let* M *and* L *be the* *corresponding extensions of k and F respectively. Then $L = FM$ and L/k is an abelian extension.*

Proof. This is a simple application of the properties of the Artin map for towers of number fields, see for example p. 172 of Tate [**61**]. □

Definition 2.1.17. *Let k be a number field. The* Dedekind zeta-function *of k is defined as*

$$\begin{aligned}\zeta_k(s) &:= \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})^s}\right)^{-1} \\ &= L_k(1, s),\end{aligned}$$

where $L_k(1, s)$ is as in (2.4) *with $\chi = 1$.*

Theorem 2.1.18 (Heilbronn [**23**] Theorem 6)**.** *Let F/k be a finite abelian extension. Let G be the group of Dirichlet characters associated with F/k. Then*

$$\zeta_F(s) = \prod_{\chi \in G} L_k(\chi, s).$$

We shall revisit Hecke L-series in Section 4.2.

2.1.2. Local Components and Field Extensions. For a place $\mathfrak{p}$ of an algebraic number field F, let $U_{\mathfrak{p}}$ be the unit group of the maximal order of $F_{\mathfrak{p}}$ if $\mathfrak{p}$ is finite and the multiplicative group of $F_{\mathfrak{p}}$ otherwise. We say that an element x of F is a *local unit* (at $\mathfrak{p}$) if x belongs to $U_{\mathfrak{p}}$ and that x is a *global unit* if x is a local unit for all places $\mathfrak{p}$ of F.

Let

$$\mathfrak{U}_F := \prod_{\mathfrak{p} \in F} U_{\mathfrak{p}} = U_F \prod_{\mathfrak{p} \in S_0} U_{\mathfrak{p}} = U_F F_\infty^*.$$

We define a *character* χ of $\mathfrak{U}_F$ to be a product

$$\chi := \prod_{\mathfrak{p}} \chi_{\mathfrak{p}},$$

where each $\chi_{\mathfrak{p}}$ is a homomorphism from $U_{\mathfrak{p}}$ to the unit circle of $\mathbb{C}$ and $\chi_{\mathfrak{p}} = 1$ for almost all places $\mathfrak{p}$ of F.

Definition 2.1.19. *Let χ be an ordinary Hecke character of $\mathfrak{I}_F$ and let*

$$\chi'_{\mathfrak{p}} = \chi_{\mathfrak{p}}|_{U_{\mathfrak{p}}}.$$

We call $\chi'_{\mathfrak{p}}$ a restricted local component *of χ.*

Let χ be a Dirichlet character of modulus $\mathfrak{m}$ and order ℓ^n for some prime ℓ. Let $c_1, \dots, c_m$ be a set of elements of $\mathfrak{I}_F$ which generate the ℓ-class group of F and set $C := \langle c_1, \dots, c_m \rangle$. We define χ_1 to be the restriction of χ to C. Let h be the homomorphism from $C \times \mathfrak{U}_F$ to $\mathfrak{I}_F / F^*$ defined by multiplication of ideles.

Lemma 2.1.20 (Halter-Koch [**20**] pp. 2–3)**.** *With notation as in the preceding paragraph, χ is uniquely determined by χ_1 and the restricted local components $\chi'_{\mathfrak{p}}$. Conversely suppose that ϕ is a character of $\mathfrak{U}_F$ of order ℓ^m with discrete infinite components and that ϕ_1 is a character of C of order ℓ^m. Then there exists a unique Dirichlet character χ of $\mathfrak{I}_F$ of order ℓ^m such that $\chi|_C = \phi_1$ and $\chi|_{\mathfrak{U}_F} = \phi$ if*

$$\phi_1(\alpha)\phi(\beta) = 1$$

whenever (α, β) is an element of $\ker h$.

As a special case we note the following:

Lemma 2.1.21. *Let ϕ be a character of U_F of order ℓ^n, and let H be the Hilbert class field of F. If ϕ is 1 on the group of global units of F then $\phi \circ \mathrm{N}_{H/F}$ extends to a Dirichlet character of $\mathfrak{I}_H$ of order ℓ^n.*

We now collect some results on the structure of the unit group of a local field of finite characteristic. Further details and proofs may be found in Chapters IV and V of Serre [**49**]. Let k_w be a local field with finite residue field $\overline{k}_w$ of characteristic $p > 0$ and unit group U_w. Recall from Section 1.3.1 the definition of the ramification groups $U_w^{(i)}$.

Proposition 2.1.22. *Let F_v/k_w be a cyclic extension of degree n.*

a) *The quotient $U_v/U_v^{(1)}$ is isomorphic to $\overline{F}_v^*$,*
b) *The unit group of k_w contains $\mathrm{N}_{F_v/k_w}(U_v)$,*
c) *If F_v/k_w is unramified, then $\mathrm{N}_{F_v/k_w}(U_v) = U_w$ and $\mathrm{N}_{F_v/k_w}(\overline{F}_v^*) = \overline{k}_w^*$,*
d) *If F_v/k_w is totally ramified then $\overline{F}_v = \overline{k}_w$ and*

$$U_w/\mathrm{N}_{F_v/k_w}(U_v) \cong C_n.$$

Let ℓ be a rational prime and let F_v/k_w be a cyclic extension of degree ℓ which is totally ramified. Let σ be a generator of $\mathrm{Gal}(F_v/k_w)$, let x be an element of F_v such that $v(x) = 1$ and set $i_v := v(\sigma(x) - x)$. By Definition 1.3.1, i_v is the smallest integer i such that $G_i := G_i(F_v/k_w) = 1$.

Proposition 2.1.23. *In the situation above, $i_v \geq 1$, with equality if and only if $\ell \neq p$.*

Lemma 2.1.24. *Let F_v be a totally ramified quadratic extension of k_w and let φ be the function with the property that $G_i = G^{\varphi(i)}$ as defined in* (1.12). *Then $\varphi(i_v) = i_v$.*

Proof. This is a simple application of Lemma 3 of Serre [**49**] IV.3. □

By Proposition 1.3.3, it follows that i_v is the exponent of the conductor of F_v/k_w.

Corollary 2.1.25. *If $i_v = 1$, then the character associated with F_v/k_w is a character of $\overline{k}_w^*$ composed with the residue class field mapping $x \mapsto \bar{x}$.*

For example, suppose that $k_w = \mathbb{Q}_p$ for some rational prime p and let F_v be a quadratic extension of $\mathbb{Q}_p$. If $\mathfrak{p}$ is odd then by Corollary 2.1.25 the character associated with $F_v/\mathbb{Q}_p$ corresponds to a quadratic character of $\mathbb{F}_p^*$.

If $p = 2$ then we must have $i_w > 1$. The following lemma shows that we have $i_w \leq 3$.

Lemma 2.1.26 (Serre [**49**] Lemma XIV.3)**.** *If an element m of $\mathbb{Z}_2$ is congruent to 1 mod 8 then m is a square.*

Example 2.1.27. Let $k_w = \mathbb{Q}_p$ as above. If p is odd then there is a unique non-trivial quadratic character $\eta_p : U_w \to \pm 1$ given by

$$\eta_p(x) := \left(\frac{\overline{x}}{p}\right) = \left(\frac{p^*}{\overline{x}}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the quadratic residue symbol on $\overline{k}_w^* = \mathbb{F}_p^*$.

If $p = 2$ then by Lemma 2.1.26, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \langle -1, 2, 5\rangle$ and $U_w/U_w^2 = \langle -1, 5\rangle$. The non-trivial quadratic characters of U_w are $\eta_s := \left(\frac{s}{\overline{x}}\right)$ for s in $\{-8, -4, 8\}$. These characters satisfy the condition that $\eta_n(x) = 1$ if and only if x is a norm in the extension $\mathbb{Q}_2(\sqrt{n})/\mathbb{Q}_2$ and are given explicitly by the equations:

$$\begin{aligned}\eta_{-4}(x) &:= (-1)^{(\overline{x}-1)/2},\\ \eta_8(x) &:= (-1)^{(\overline{x}^2-1)/8},\\ \eta_{-8}(x) &:= (-1)^{(\overline{x}^2-1)/8+(\overline{x}-1)/2}.\end{aligned}$$

2.2. Quadratic Characters of Quadratic Fields

Imaginary quadratic fields $K/\mathbb{Q}$ play a special role in this work as the CM fields of elliptic curves. In this section we investigate the quadratic Hecke characters of $\mathfrak{I}_K$ in terms of their restricted local components to establish results which will be used repeatedly in each of the subsequent chapters. As a preliminary we look in Section 2.2.1 at the Hecke characters of $\mathbb{Q}$ associated with quadratic extensions $K/\mathbb{Q}$, which should give an insight into the relationship between the Dirichlet characters of modulus $\mathfrak{m}$

of a number field $\mathfrak{I}_F$ and the classical notion of a Dirichlet character of modulus m as a character of $(\mathbb{Z}/m\mathbb{Z})^*$. In Section 2.2.2 we recall classical results of genus theory on the quadratic characters of the class group $Cl(\mathcal{O})$ of orders $\mathcal{O}$ of K and in Section 2.2.3 we describe the characters of the local unit groups $U_\mathfrak{p}$.

Throughout this section, K denotes a quadratic extension of $\mathbb{Q}$.

2.2.1. Quadratic Fields. Let $K/\mathbb{Q}$ be a quadratic field. The *discriminant* D_K of K is the discriminant of the maximal order $\mathcal{O}_K$ of K.

Definition 2.2.1. *An integer s is a* prime discriminant *if s is divisible by precisely one rational prime, and s is the discriminant of* $\mathbb{Q}(\sqrt{s})$.

Proposition 2.2.2. *Let $K/\mathbb{Q}$ be a quadratic field with discriminant D_K divisible by t distinct primes $s_1, \ldots, s_t$. Then there is a unique decomposition of D_K into a product of prime discriminants*

$$D_K = s_1^* \cdots s_t^*,$$

where for odd primes

$$s_i^* := \begin{cases} -s_i & \text{if } s_i \equiv 3 \bmod 4, \\ s_i & \text{if } s_i \equiv 1 \bmod 4, \end{cases}$$

and the prime discriminant 2^* is the unique element s of $\{-8, -4, 8\}$ such that $D_K/s \equiv 1 \bmod 4$. The restriction of the Dirichlet character η associated with $K/\mathbb{Q}$ to $\mathfrak{U}_\mathbb{Q}$ is given by

$$\eta = \eta_\infty \cdot \prod_{i=1}^{t} \eta_{s_i^*} \tag{2.10}$$

where $\eta_\infty = 1$ if $D_K > 0$ and sgn_∞ *otherwise, and we define $\eta_{-p} := \eta_p$ for odd primes p.*

Proof. The unique factorization of D_K into a product of prime discriminants is a simple proof by induction. Since $\mathbb{Q}$ has class number 1, η is determined by its restricted local components, which for finite places of $\mathbb{Q}$ are as determined in Example 2.1.27. Finally, since η is an idele class character it must be 1 on $\mathbb{Q}^*$, and in particular, must be even. This determines the infinite component of η as claimed. □

2.2.2. The Genus Field. Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order of K of discriminant D. Let $t := t_D$ be the number of rational primes dividing D. In this section we shall determine which quadratic extensions of K are contained in the ring class field of $\mathcal{O}$. For more details see Cox [**6**] or Hecke [**22**].

Definition 2.2.3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals of $\mathcal{O}$, coprime to D. We say that $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same* genus *if*

$$|\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})| = \mathrm{N}_{K/\mathbb{Q}}(x) \cdot |\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b})| \mod D$$

for some x in K.

Let $\mathfrak{G}_D$ denote the set of genera of $\mathcal{O}$. We can make $\mathfrak{G}_D$ into a group by defining the product of elements $\mathfrak{g}_1, \mathfrak{g}_2$ of $\mathfrak{G}_D$ to be the genus of the ideal $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ where $\mathfrak{a}_1$ belongs to $\mathfrak{g}_1$ and $\mathfrak{a}_2$ to $\mathfrak{g}_2$. The genus containing the principal ideals of $\mathcal{O}$ is called the *principal genus*: it is the identity element of $\mathfrak{G}_D$.

Definition 2.2.4. *Let a be an integer coprime to D. We say that a genus $\mathfrak{g}$* represents *a if $a = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ for some ideal $\mathfrak{a}$ in $\mathfrak{g}$.*

If ideals $\mathfrak{a}, \mathfrak{b}$ belong to the same class of $I_{\mathcal{O}}$, then they belong to the same genus, hence the group of genera is a quotient group of the ideal class group of $\mathcal{O}$. By Artin reciprocity then, it defines a subfield F_g of the ring class field of $\mathcal{O}$. We call F_g the *genus field* of $\mathcal{O}$.

Remark 2.2.5. In a more general context, the genus field of a number field F is defined to be the maximal subfield k of F such that $k/\mathbb{Q}$ is abelian. With this convention the field F_g defined above is the genus field of $H_{\mathcal{O}}$.

Definition 2.2.6. *Let D and $\mathcal{O}$ be as above and let S be the set of odd primes dividing D. If D is divisible by 4, set $d := -D/4$. We define*

$$X_D := \begin{cases} \{\eta_p : p \in S\} & D \text{ odd, or } d \equiv 3, 7 \bmod 8, \\ \{\eta_p : p \in S \cup \{-4\}\} & d \equiv 1, 4, 5 \bmod 8, \\ \{\eta_p : p \in S \cup \{8\}\} & d \equiv 2 \bmod 8, \\ \{\eta_p : p \in S \cup \{-8\}\} & d \equiv 6 \bmod 8, \\ \{\eta_p : p \in S \cup \{-4, 8\}\} & d \equiv 0 \bmod 8, \end{cases}$$

and set $\mu := |X_D|$.

Lemma 2.2.7 (Cox [6] Lemma 3.17)**.** *An element a of $(\mathbb{Z}/D\mathbb{Z})^*$ belongs to the kernel of η for all η in X_D if and only if it is represented by the principal genus.*

Lemma 2.2.8 (Cox [6] Theorem 2.16)**.** *Let $\chi_D := \prod_{\eta \in X_D} \eta$. Then a is represented by a genus of $\mathfrak{G}_D$ if and only if $\chi_D(a) = 1$.*

Corollary 2.2.9. *The group of genera of $\mathcal{O}$ is isomorphic to $C_2^{\times \mu - 1}$, with μ as in Definition 2.2.6. Moreover the group of characters associated with $F_g/\mathbb{Q}$ is generated by the set Y_D of even quadratic characters whose non-trivial finite components are in X_D.*

Therefore if L is a quadratic extension of K contained in F_g, the character of $\mathfrak{I}_K$ associated with L/K is of the form

$$\phi_L = \phi \circ \mathrm{N}_{K/\mathbb{Q}},$$

for some ϕ in Y_D.

2.2.3. Quadratic Characters of Local Unit Groups. Let K be a quadratic field with discriminant D_K, let p be a rational prime and $\mathfrak{p}$ a prime of K dividing p, and set $s := 2^*$ if $p = 2$ and $s := p$ otherwise. Let κ_s be the character of $U_\mathfrak{p}$ defined by

$$\kappa_s := \eta_s \circ N_{K/\mathbb{Q}}. \tag{2.11}$$

If p is odd let $\lambda_\mathfrak{p}$ be defined by

$$\lambda_\mathfrak{p}(x) := \left(\frac{\overline{x}}{p}\right), \tag{2.12}$$

where $\bar{x}$ denotes the image of x in the residue field $\overline{K}_\mathfrak{p}$.

Corollary 2.2.10. *Let p be an odd prime and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ dividing p. There is a unique non-trivial real quadratic character on $U_\mathfrak{p}$ which is equal to $\lambda_\mathfrak{p}$ if p divides D_K and to κ_p otherwise.*

This is an immediate consequence of Lemma 2.1.22. If p is inert in $\mathcal{O}_K$ then $\kappa_p = \lambda_\mathfrak{p}$ is the only non-trivial quadratic character on $U_\mathfrak{p}$. If p splits, then it lies under two conjugate primes, $\mathfrak{p}$ and $\mathfrak{p}^\rho$, the local unit group $U_\mathfrak{p} \cong \mathbb{Z}_p^*$ has exactly one (non-trivial) quadratic character $\lambda_\mathfrak{p}$, and by c)

$$\lambda_\mathfrak{p}\lambda_\mathfrak{p}^\rho = \kappa_p. \tag{2.13}$$

If p divides D_K then we set $\lambda_p := \lambda_\mathfrak{p}$.

When $p = 2$, the situation is a little more complicated, because there exist local characters with conductor exponent greater than one. In this case Proposition 2.1.22 tells us that

Corollary 2.2.11. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ dividing 2. There exists some s in $\{-8, -4, 8\}$ such that $\kappa_s(U_\mathfrak{p}) = 1$ if and only if 2 divides D_K.*

Lemma 2.2.12. *Suppose that 2 splits in K, and let $\mathfrak{p}$ be a prime of K dividing 2. Then $U_\mathfrak{p}$ is isomorphic to $\mathbb{Z}_2^*$, and the non-trivial quadratic characters of $U_\mathfrak{p}$, denoted by $\lambda_{-8}, \lambda_{-4}, \lambda_8$, satisfy*

$$\lambda_a\lambda_a^\rho = \kappa_a$$

for a in $\{-8, -4, 8\}$.

This follows in precisely the same way as the case p odd.

Lemma 2.2.13. *Suppose that 2 does not split in K, and let $\mathfrak{p}$ be the prime of K dividing 2. Then*

$$U := U_{\mathfrak{p}}/U_{\mathfrak{p}}^2 \cong (\mathbb{Z}/2\mathbb{Z})^3. \tag{2.14}$$

Proof. By Proposition II.6 of Lang [**25**],

$$|U_{\mathfrak{p}}/U_{\mathfrak{p}}^2| = 2^{[K_{\mathfrak{p}}:\mathbb{Q}_2]+1} = 2^3.$$

□

Lemma 2.2.14. *Suppose that 2 is inert in K. Then the character group of $U_{\mathfrak{p}}$ is generated by $\{\kappa_8, \nu, \nu^\rho\}$ where*

$$\nu\nu^\rho = \kappa_{-4}.$$

Proof. Since 2 is inert in K, there exists x in K with $\bar{x}^2 + \bar{x} + 1 = 0$, and U is generated by $\{-1, 1+2x, 1+4x\}$. Let ν be the character of U with kernel generated by $\{1+2x, 1+4x\}$. Then as $x^\rho = x^2$, the kernel of ν^ρ is generated by $\{1+2x^2, 1+4x^2\}$ and $\nu\nu^\rho = \kappa_{-4}$. □

Let $s(K) := 2^*$ where 2^* is as defined in Proposition 2.2.2.

Lemma 2.2.15. *If 2 ramifies in K then the group of quadratic characters of $U_{\mathfrak{p}}$ is generated by $\{\nu, \nu^\rho, \lambda_s\}$ where $s := s(K)$,*

$$\nu\nu^\rho = \begin{cases} \kappa_8 & \textit{if } D_K/4 \equiv 3 \bmod 4, \\ \kappa_{-4} & \textit{if } D_K/4 \equiv 2 \bmod 4, \end{cases}$$

and λ_s is a real character which is odd if $s = -8$ and even otherwise.

Proof. Let U be as in (2.14) and let $m \in K$ be the square root of $D_K/4$. We have two cases to consider:

a) $D_K/4$ is odd.

Consider the set S of elements of $U_{\mathfrak{p}}$ of the form $x = a + bm$, with a, b in $\mathbb{Z}/8\mathbb{Z}$ such that a, b are not both even. Squares in S are of the form $c + 2dm$, with c, d odd. (In this context we consider 0 to be an even number.) Therefore $|S/S^2| = 8 = |U|$, hence

$$U = \langle m, 3-2m, 5\rangle.$$

Let ν, λ_{-4} be the characters of U with kernels $\langle m, 3-2m\rangle$ and $\langle 3-2m, 5\rangle$ respectively.

Then $\lambda_{-4}^\rho = \lambda_{-4}$, $\nu\nu^\rho = \kappa_8$ and $\nu, \nu^\rho, \lambda_{-4}$ generate the character group of U.

b) $D_K/4$ is even.

In this case S consists of elements $x = a + bm$ as above, where a must always be odd, and x is a square if b is even. Hence

$$U = \langle 1+m, -1, 5\rangle,$$

and the character group of U is generated by μ_8 and μ_{-8}, the characters with kernels $\langle 1+m, -1\rangle, \langle 1+m, 5\rangle$ respectively, and their conjugates.

If $D_K/8 \equiv 3 \bmod 4$, then $\lambda_{-8} := \mu_{-8} = \mu_{-8}^{\rho}$ and $\mu_8\mu_8^{\rho} = \kappa_{-4}$. If $D_K/8 \equiv 1 \bmod 4$, then $\lambda_8 := \mu_8 = \mu_8^{\rho}$ and $\mu_{-8}\mu_{-8}^{\rho} = \kappa_{-4}$.

□

Corollary 2.2.16. *Suppose that 2 ramifies in $K/\mathbb{Q}$ and let $\mathfrak{p}$ be the prime of $\mathcal{O}_K$ dividing 2. Then the conductors of the real quadratic characters of $U_{\mathfrak{p}}$ are given by*

$D_K \bmod 8$	$\mathfrak{f}_\kappa$	$\mathfrak{f}_\lambda$
4	$\mathfrak{p}^4$	$\mathfrak{p}^2$
0	$\mathfrak{p}^2$	$\mathfrak{p}^5$

where $\lambda := \lambda_{s(K)}$ and $\kappa := \kappa_m$ where $m = 8$ if $s(K) = -4$ and $m = -4$ otherwise.

We summarize the properties of the characters λ_p for p dividing D_K below:

Proposition 2.2.17. *Let p be an odd prime dividing D_K. Then λ_p is a real quadratic character which is odd if and only if $p \equiv 3 \bmod 4$. Suppose that D_K is even and let $s := s(K)$. Then λ_s is a real quadratic character which is odd if $s = -8$ and even otherwise.*

In order to treat characters λ_s in a unified way, we set $\lambda_{p^*} := \lambda_p$ for any prime p dividing D_K. We define

$$G_K := \langle \lambda_{p^*} : p | D_K \rangle. \tag{2.15}$$

Let G_K^+ and G_K^- be respectively the subsets of even and odd characters in G_K.

Corollary 2.2.18. *Suppose that D_K is a negative discriminant divisible by t distinct primes, $p_1, \ldots, p_t$. Then $|G_K^+|$ is 2^{t-1} if D_K is divisible either by 8 or by some prime $p \equiv 3 \bmod 4$ and 2^t otherwise.*

Proof. If D_K is divisible neither by 8 nor by any prime $p \equiv 3 \bmod 4$ then λ_{p^*} is even for every p dividing D_K, and clearly these characters generate a group of order 2^t. Otherwise, suppose that $\lambda_{p_i^*}$ is odd for $1 \le i \le u$ and even for $u+1 \le i \le t$. The characters $\lambda_1\lambda_i$ with $2 \le i \le u$ generate a group G_1 of order 2^{u-1} and

$$G_K^+ := \langle G_1, \lambda_j : j > u \rangle,$$

hence G_K^+ has order 2^{t-1} as claimed. □

It follows that G_K^- is either empty or of order 2^{t-1}.

2.3. Grössencharacters

Let (K, Φ) be a CM type with reflex (K', Φ') as in Definition 1.2.13 and let F be a finite extension of K'. We will retain this notation for the remainder of this chapter.

Definition 2.3.1. *Let $f_\Phi := \det \Phi' \circ \mathrm{N}_{F/K'}$, and denote by the same symbol its continuous extension to a homomorphism $\mathfrak{I}_F \to \mathfrak{I}_K$. For any place $\mathfrak{p}$ of F, let $f_{\Phi,\mathfrak{p}} : \mathfrak{I}_F \to K_\mathfrak{p}$ be the map defined by*

$$f_{\Phi,\mathfrak{p}}(\boldsymbol{\alpha}) = \beta_\mathfrak{p}, \textit{ where } \boldsymbol{\beta} = f_\Phi(\boldsymbol{\alpha}).$$

It follows from the definition of f_Φ that

$$f_\Phi(\boldsymbol{\alpha}) f_\Phi(\boldsymbol{\alpha})^\rho = \mathrm{N}_{F/\mathbb{Q}}(\boldsymbol{\alpha}). \tag{2.16}$$

where ρ denotes complex conjugation on K.

Suppose that (A, θ) is an abelian variety of CM type (K, Φ) defined over F, with good reduction at the place $\mathfrak{p}$ of F. Let $\widetilde{A_\mathfrak{p}}$ be the special fibre of the Néron model of A at $\mathfrak{p}$, let $k = \overline{F}_\mathfrak{p}$, and let $\pi_\mathfrak{p}$ be the Frobenius endomorphism of $\widetilde{A_\mathfrak{p}}$ over k.

By the universal property of the Néron model (or by Lemma 1.1.16 if $g = 1$), the reduction of θ at $\mathfrak{p}$ defines an injection

$$\theta_\mathfrak{p} : K \hookrightarrow \mathrm{End}_k^0(\widetilde{A_\mathfrak{p}}).$$

Now $\pi_\mathfrak{p}$ commutes with every k-endomorphism of $\widetilde{A_\mathfrak{p}}$, so, by Proposition 1.3.22, (or by Proposition 1.1.22 for $g = 1$), it is in the image of $\theta_\mathfrak{p}$ and since $\theta_\mathfrak{p}$ is injective, there exists a unique element $x_\mathfrak{p}$ of K satisfying

$$\pi_\mathfrak{p} = \theta_\mathfrak{p}(x_\mathfrak{p}). \tag{2.17}$$

Let S be the set of places of F which are infinite or at which A has bad reduction. Let $\mathfrak{I}_{F,S}$ be the ideles of F which have $\mathfrak{p}$-component 1 for all $\mathfrak{p}$ in S. Then (A, θ) defines a map ϕ_A from $\mathfrak{I}_{F,S}$ to K^* by

$$\phi_A(\boldsymbol{\alpha}) := \prod_{\mathfrak{p} \notin S} x_\mathfrak{p}^{n_\mathfrak{p}} \tag{2.18}$$

where $n_\mathfrak{p} = v_\mathfrak{p}(\alpha_\mathfrak{p})$.

Theorem 2.3.2 (Serre-Tate [**51**] Theorem 10)**.** *There is a unique continuous homomorphism $\phi_A : \mathfrak{I}_F \to K^*$ which extends the map of* (2.18) *on $\mathfrak{I}_{F,S}$ and agrees with f_Φ on F^*.*

Remark 2.3.3. If A is an elliptic curve, then $K' = K$ and for all x in F,

$$f_\Phi(x) = \mathrm{N}_{F/K}(x).$$

Let $\mathfrak{p}$ be any infinite place of K. Then since K is a CM field, $K_{\mathfrak{p}}$ is isomorphic to $\mathbb{C}$. We define

$$\chi_{A,\mathfrak{p}} := \phi_A \cdot f_{\phi,\mathfrak{p}}^{-1}. \tag{2.19}$$

Fixing a choice of infinite place $\mathfrak{p}$, we let $f_\infty := f_{\phi,\mathfrak{p}}$.

Definition 2.3.4. *The* Grössencharacter *of A is the Hecke character of $\mathfrak{I}_F$ defined by*

$$\chi_A := \phi_A f_\infty^{-1}.$$

We note that the infinite components of χ_A are determined by the CM type of A.

Lemma 2.3.5. *Let A and B be abelian varieties of CM type (K, Φ) and let $\chi := \chi_A \chi_B^{-1}$. Then χ is a Dirichlet character.*

Proof. Since the infinite components of χ_A and χ_B are equal, χ is a Hecke character with discrete infinite components and exceptional set contained in the union T of the exceptional sets of χ_A and χ_B. It remains to show that $\chi(\boldsymbol{\alpha})$ lies on the unit circle of $\mathbb{C}^*$ for all ideles $\boldsymbol{\alpha}$ of F. But this is clear for any idele $\boldsymbol{\alpha}$ in $\mathfrak{I}_{F,T}$ since

$$\chi_A(\boldsymbol{\alpha}) = \prod_{\mathfrak{p} \notin T} x_{\mathfrak{p}}^{n_{\mathfrak{p}}},\ \chi_B(\boldsymbol{\alpha}) = \prod_{\mathfrak{p} \notin T} y_{\mathfrak{p}}^{n_{\mathfrak{p}}},$$

and $x_{\mathfrak{p}}/y_{\mathfrak{p}}$ is a unit for each $\mathfrak{p}$. The general result follows by the continuity of χ_A and χ_B. □

Proposition 2.3.6. *If (A, θ) and (A', θ') are abelian varieties of CM type (K, Φ) defined over F then $\chi_A = \chi_{A'}$ if and only if A and A' are isogenous over F. Moreover, the minimal extension L/F over which A and A' become isogenous is the one associated with the Hecke character $\phi_L = \chi_{A'}\chi_A^{-1}$.*

Proof. See Lemma 19.12 of Shimura [**54**], or for the case of elliptic curves Gross [**16**] pp. 25–26. □

Proposition 2.3.7. *With other notation as above, suppose that $F/\mathbb{Q}$ is normal and let σ be an element of* $\mathrm{Gal}(F/\mathbb{Q})$*. The variety (A^σ, θ') is of CM type (K, Φ') where $\theta'(x) = \theta(x)^\sigma$ and $\Phi'(x) = \Phi(x)^\sigma$ for x in K and*

$$\chi_{A^\sigma} = (\chi_A)^\sigma.$$

Proof. See Shimura [**54**] Lemma 20.6. □

Corollary 2.3.8. *Let A and F be as in Proposition 2.3.6 and suppose that k is a normal subfield of F. Then A is a k-variety (in the sense of Definition 1.2.3), if and only if $\chi_{A^\sigma} = (\chi_A)^\sigma$ for all σ in* $\mathrm{Gal}(F/k)$.

Proof. In Definition 1.2.3 we defined A to be a k-variety if it is F-isogenous to A^σ for all σ in $\mathrm{Gal}(F/k)$. Clearly this property is isogeny invariant, hence by Proposition 2.3.6, A is a k-variety if and only if $\chi_A = \chi_{A^\sigma}$ for all σ in $\mathrm{Gal}(F/k)$ and Proposition 2.3.7 shows that this is true if and only if

$$(\chi_A)^\sigma = \chi_A \text{ for all } \sigma \in \mathrm{Gal}(F/k).$$

□

Earlier in this chapter we saw that any ordinary Hecke character of $\mathfrak{I}_F$ with discrete infinite components corresponds to an abelian extension L/F. The next theorem gives conditions for a Hecke character of $\mathfrak{I}_F$ to be the Grössencharacter of an abelian variety of a given CM type.

Theorem 2.3.9 (Shimura [**55**] Theorem 6)**.** *Let (K, Φ) be a CM type with reflex (K', Φ') and let F be a finite extension of K'. Let ψ be a Hecke character of $\mathfrak{I}_F$ with values in K^* and with trivial infinite components, satisfying*

$$\psi(\boldsymbol{\alpha})\psi(\boldsymbol{\alpha})^\rho = \mathrm{N}_{F/\mathbb{Q}}(\boldsymbol{\alpha}). \tag{2.20}$$

Then if there exists a lattice Λ in K such that

$$\psi(\boldsymbol{\alpha}) f_\Phi(\boldsymbol{\alpha})\Lambda = \Lambda, \tag{2.21}$$

for all $\boldsymbol{\alpha}$ in $\mathfrak{I}_F$, then there exists an abelian variety A defined over F such that there is an exact sequence

$$0 \to \Lambda \to \mathbb{C}^g \to A \to 0,$$

and $\chi_A = \psi \cdot f_\infty^{-1}$.

Example 2.3.10. Let $K/\mathbb{Q}$ be an imaginary quadratic field with discriminant D_K divisible by some prime p congruent to 3 modulo 4, and let H be the Hilbert class field of K. Then λ_p extends to an ordinary Hecke character ψ of $\mathfrak{I}_K$ such that $\psi_\infty(\boldsymbol{\alpha}) = \alpha_\infty^{-1}$ and if $\mathfrak{a} = (a)$ is a principal ideal coprime to D_K then $\psi(\boldsymbol{\alpha}(\mathfrak{a})) = \lambda_p(a) \cdot a$ and

$$\chi := \psi \circ \mathrm{N}_{H/K}$$

is a Hecke character of $\mathfrak{I}_H$ satisfying the conditions of Theorem 2.3.9 for any lattice of K.

The above example introduces a class of Grössencharacters in which we will be especially interested. If A is defined over k with Grössencharacter ϕ and F is any extension of k, then the Grössencharacter of A over F is given by

$$\chi_A = \phi \circ \mathrm{N}_{F/k}, \tag{2.22}$$

however as we saw in Example 2.3.10 it is not necessary for A to be defined over k for an equation of the form (2.22) to exist.

Definition 2.3.11 (Shimura's Condition)**.** *Let A, F, K and χ_A be as in Theorem 2.3.9 and let k be a subfield of F containing K' such that A is a k-variety. Then we say that A is of k-type 1 if there exists a Hecke character χ_k of $\mathfrak{I}_k$ such that*

$$\chi_A = \chi_k \circ \mathrm{N}_{F/k},$$

and of k-type 2 otherwise.

If $k = K'$ then we may say that A is type 1 (resp. 2) instead of k-type 1 (resp. 2).

Theorem 2.3.12 (Shimura [**56**] Theorem 7.44)**.** *If A, F and k are as above then A is of k-type 1 if and only if $F(A_{tors})$ is an abelian extension of k.*

Corollary 2.3.13. *Suppose that A/F and A'/F are as in Proposition 2.3.6, that they are non-isogenous over F and that A is of k-type 1, where k is a subfield of F containing K' such that $\mathrm{Gal}(F/k)$ is abelian. Let L be the minimal extension of F contained in F^{alg} over which A and A' become isogenous. Then L/k is abelian if and only if if A' is of k-type 1.*

Proof. The extension L/F corresponds to the Hecke character $\phi_L = \chi_{A'}\chi_A^{-1}$ and if A and A' are k-type 1 then there exist Hecke characters χ and χ' of $\mathfrak{I}_k$ such that $\chi_A = \chi \circ \mathrm{N}_{F/k}$ and $\chi_{A'} = \chi' \circ \mathrm{N}_{F/k}$, hence $\phi_L = \chi'\chi^{-1} \circ \mathrm{N}_{F/k}$ and L/k is abelian by Lemma 2.1.16.

Conversely, suppose that L/k is abelian. Then by Theorem 2.3.12, $L(A_{tors}) = L(A'_{tors})$ is an abelian extension of k, and since $F(A'_{tors}) \subseteq L(A_{tors})$, we see that A' is of k-type 1. □

Corollary 2.3.14. *With notation as above, let L be a quadratic extension of F. Then L/k is abelian if and only if*

$$\phi_L = \phi_0 \circ \mathrm{N}_{F/k}$$

for some character ϕ_0 of $\mathfrak{I}_k$.

2.3.1. Grössencharacters and ℓ-adic Representations.

Let A be an abelian variety of CM type (K, Φ) defined over a number field F. We continue to assume that F is a finite extension of the reflex field K' of K. In Section 1.3.3 we defined the ℓ-adic representation

$$\rho_\ell : \mathrm{Gal}(F^{alg}/F) \to \mathrm{Aut}(T_\ell(A)).$$

for any rational prime ℓ. By class field theory, we can consider ρ_ℓ as a homomorphism from $\mathfrak{I}_F$ to K_ℓ^* with kernel containing F^*.

Definition 2.3.15. *For any rational prime ℓ, let*

$$f_\ell(\boldsymbol{\alpha}) := f_{\Phi,\mathfrak{q}}(\boldsymbol{\alpha}),$$

where $\mathfrak{q}$ is a prime of $\mathcal{O}_K$ dividing ℓ and $f_{\Phi,\mathfrak{q}}$ is as in Definition 2.3.1.

Proposition 2.3.16. *For any rational prime ℓ,*

$$\rho_\ell = \phi_A f_\ell^{-1},$$

where ϕ_A is the homomorphism from $\mathfrak{I}_F$ to K^* of Theorem 2.3.2.

Proof. By definition, $\phi_A = f_\ell$ on F^*. Let $\mathfrak{p}$ be a prime at which A has good reduction and let p be the characteristic of $F_\mathfrak{p}$. If $p \neq \ell$ then Proposition 1.3.14 tells us that $\rho_\ell(U_\mathfrak{p}) = 1$, and if $v_\mathfrak{p}(\alpha_\mathfrak{p}) = 1$ then $\rho_{\ell,\mathfrak{p}}(\boldsymbol{\alpha}) = x_\mathfrak{p}$, where $x_\mathfrak{p}$ is as defined in (2.17). Let $S_\ell = S \cup \{\mathfrak{p} : \mathfrak{p}|\ell\}$ where S is the union of S_0 and the set of primes of F at which A has bad reduction. We have established the claim on $F^*\mathfrak{I}_{F,S_\ell}$, which is a dense subgroup of $\mathfrak{I}_F$, hence the result holds for all of $\mathfrak{I}_F$ since both sides of the equation are continuous. □

Comparing the action of ρ_ℓ and ϕ_A on $U_\mathfrak{p}$, we see that A has bad reduction at $\mathfrak{p}$ if and only if $\mathfrak{p}$ divides the conductor of χ_A.

Corollary 2.3.17 (Serre-Tate [**51**] Theorem 12)**.** *Let A/F be an abelian variety of CM type (K, Φ) with Grössencharacter $\chi := \chi_A$ and suppose that F contains the reflex field K'. The conductor $\mathfrak{f}_A$ of A is related to the conductor $\mathfrak{f}_\chi$ of χ by*

$$\mathfrak{f}_A = \mathfrak{f}_\chi^{2g}.$$

Proof. Let $\mathfrak{p}$ be a prime at which χ_A is ramified. By Definition 2.1.7, the exponent of $\mathfrak{f}_A$ at $\mathfrak{p}$ is $2g \cdot m_\mathfrak{p}$, where $m_\mathfrak{p}$ is the smallest integer i such that $G^i(F_\mathfrak{P}^{alg}/F_\mathfrak{p})) \subset \ker \rho_\ell$. By Proposition 1.3.3, Proposition 2.3.16 and the definition of χ_A, we see that $m_\mathfrak{p}$ is the smallest non-negative integer such that $\chi_{A,\mathfrak{p}}(1 + \mathfrak{p}^i) = 1$, and the result follows by Definition 2.1.7. □

Theorem 2.3.18 (Shimura [**56**] Theorem 7.42)**.** *Let A/F be an abelian variety of CM type (K, Φ). The L-series of A, defined in Definition 1.3.18, is equal to*

$$L(A/F, s) = \prod_{\mathfrak{p} \in S_0} L_F(\chi_{A,\mathfrak{p}}, s) \cdot L_F(\overline{\chi}_{A,\mathfrak{p}}, s),$$

where $\chi_{A,\mathfrak{p}}$ is as defined in (2.19).

If A is an elliptic curve with CM then comparing (2.1) and (1.19) shows that the claim of the theorem is that if A has good reduction at $\mathfrak{p}$ then

$$\chi_A(\mathfrak{p}) + \overline{\chi_A(\mathfrak{p})} = a_\mathfrak{p}, \text{ and } \chi_A(\mathfrak{p}) \cdot \overline{\chi_A(\mathfrak{p})} = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}).$$

The second equality follows directly from the definition of the Grössencharacter, (c.f. Theorem 2.3.9). Silverman [**59**] gives a proof of both on pp. 174–175.

CHAPTER 3

Counting Admissible Extensions

Suppose that A is an abelian variety of CM type (K, Φ) with reflex field k and let F be a field of definition for A containing k. Suppose further that A is of k-type 1, and that A is F-isogenous to A^σ for all σ in $\mathrm{Gal}(F/k_0)$ for some subfield k_0 of k, that is, A is a k_0-variety.

Let L/F be a quadratic extension and let B be the twist of A by L. We saw in Chapter 2 that

a) B is of k-type 1 if and only if L/k is abelian,
b) B is a k_0-variety if and only if L/k_0 is normal, and
c) the set of primes of F at which B has bad reduction is contained in the union of the set of primes at which A has bad reduction and those at which L/F is ramified.

When calculating the endomorphism algebras of Weil restrictions in Chapter 5, we shall want more detailed information about $\mathrm{Gal}(L/k)$. For example, suppose that A is simple and of k-type 1, that L/k is normal and let W_A and W_B be the Weil restrictions of A and B from F to k. We shall see in Proposition 5.2.18 that $\mathrm{End}_k^0(W_A)$ and $\mathrm{End}_k^0(W_B)$ are isomorphic if and only if $\mathrm{Gal}(L/k) \cong C_2 \times \mathrm{Gal}(F/k)$.

These considerations motivate the subject matter of this chapter, in which we investigate extensions L/k which occur in towers

$$L/F/k$$

with the properties that F/k is abelian, L/F is quadratic and L/k is normal. We shall call such extensions *admissible* and denote the set of admissible extensions contained in a fixed algebraic closure of k by $\mathcal{G}_{F/k}$. The subset of admissible extensions which are abelian over k is denoted $\mathcal{A}_{F/k}$. If L, F and k are all normal over $\mathbb{Q}$, then we say that L is *strictly admissible*. Multiplication of Dirichlet characters gives a natural group structure to the set of quadratic extensions of F, and we shall see in Section 3.1 that the subset $\mathcal{G}^s_{F/k}$ of strictly admissible extensions is a subgroup of $\mathcal{G}_{F/k}$. In Section 3.2 we recall, following Massy [**27**] and Fröhlich [**11**], some of the cohomological theory of central extensions of an abelian group by ± 1. We obtain an upper bound for the dimension $d_{F/k}$ of $\mathcal{G}_{F/k}/\mathcal{A}_{F/k}$ as an $\mathbb{F}_2$-vector space, and under the additional assumption that $\mathrm{Gal}(F/k) \cong C_2^{\times n}$, investigate the

Galois groups which may occur as $\mathrm{Gal}(L/k)$ when L is an admissible extension. Retaining this assumption, the last part of this section looks in more detail at the relationship between the Galois groups $\mathrm{Gal}(L/k), \mathrm{Gal}(L'/k)$ and $\mathrm{Gal}(L \circ L'/k)$ where $\circ$ denotes the composition relation on $\mathcal{G}_{F/k}$.

In the final section we apply the preceding theory to the case where k is an imaginary quadratic field and F is the Hilbert class field of k. Nakamura [**34**] has proved that in this case $d_{F/k} = \binom{n}{2}$ where n is the 2-rank of the class group of k, which is the upper bound found in the preceding section. The groups occurring as $\mathrm{Gal}(L/k)$ for L in $\mathcal{G}_{F/k}$ are therefore largely determined by those of L in $\mathcal{A}_{F/k}$, to which our attention turns.

3.1. Admissible Extensions

In this chapter we fix an algebraic closure $\mathbb{Q}^{alg}$ of $\mathbb{Q}$ and consider any algebraic number field F as a subfield of $\mathbb{Q}^{alg}$.

Definition 3.1.1. *An algebra over a field F is called* étale *if it is isomorphic to a product of finite separable field extensions of F, each contained in $\mathbb{Q}^{alg}$.*

Definition 3.1.2. *Let F be an algebraic number field. We define $\mathcal{G}_F$ to be the set of étale F-algebras of dimension 2.*

Suppose that $L \cong F \times F$. We shall define the discriminant $D_{L/F}$ of L/F to be the trivial ideal of $\mathcal{O}_F$, and the character ϕ_L of the F-algebra L/F to be the character sending every element of $\mathfrak{I}_F$ to 1. If L/F is a quadratic extension of number fields then ϕ_L is the Dirichlet character of $\mathfrak{I}_F$ corresponding to the extension L/F as in Chapter 2, and $D_{L/F}$ is the relative discriminant in the usual sense.

Definition 3.1.3. *Let L and L' be elements of $\mathcal{G}_F$ associated with Dirichlet characters ϕ and ϕ' of $\mathfrak{I}_F$. We define $L'' = L \circ L'$ to be the element of $\mathcal{G}_F$ with character $\phi'' = \phi \cdot \phi'$.*

With notation as in the definition, if ϕ is equal to neither ϕ' nor 1, then the composite field $L'L$ is an extension of F with Galois group isomorphic to $C_2 \times C_2$ and corresponding to the group of Dirichlet characters $\langle \phi, \phi' \rangle$. The field L'' is the unique quadratic extension of F contained in $L'L$ which is equal to neither L nor L'. It follows that if a and b are elements of F such that $L = F(\sqrt{a})$ and $L' = F(\sqrt{b})$ and $L'' = L \circ L'$ then $L'' = F(\sqrt{ab})$.

Let G be a finite group and p a rational prime and let G_p be the maximal abelian quotient group of G with order a power of p. The *p-rank* of G is the number of non-trivial cyclic factors of G_p. We extend this definition to positive powers of primes by defining the *p^j-rank* of G to be the p-rank of $G_{p^{j-1}} := \{\sigma^{p^{j-1}} : \sigma \in G_p\}$. When G is abelian, this corresponds to the number of factors of order divisible by p^j which occur in a decomposition of G into a direct product of cyclic groups.

Definition 3.1.4. *Let F/k be a normal extension of number fields, let p be a rational prime and let $m = p^j$ for some integer $j \geq 1$. We define $r_m(F/k)$ to be the m-rank of* $\mathrm{Gal}(F/k)$.

Lemma 3.1.5. *Let M be a normal extension of F and let*

$$\mathcal{G}_{F,M} = \{L \in \mathcal{G}_F : L \subset M\} \cup \{F \times F\}.$$

Then $\mathcal{G}_{F,M}$ is a subgroup of $\mathcal{G}_F$. In particular, if M is a finite extension of F, let A be the largest subextension of M which is abelian over F and set $m := r_2(A/F)$. Then $\mathcal{G}_{F,M}$ is isomorphic to $C_2^{\times m}$.

Proof. Without loss of generality, we may assume that M/F is abelian, hence the characters of $\mathrm{Gal}(M/F)$ form a group isomorphic to $\mathrm{Gal}(M/F)$, and the result is a consequence of the properties of profinite groups. □

For any normal subfield k of F, let

$$\begin{aligned}\mathcal{G}_{F/k} &:= \{L \in \mathcal{G}_F : L/k \text{ is normal}\} \cup \{F \times F\},\\ \mathcal{A}_{F/k} &:= \{L \in \mathcal{G}_{F/k} : L/k \text{ is abelian}\} \cup \{F \times F\}.\end{aligned}$$

Applying Lemma 3.1.5 with M a normal closure of k shows that $\mathcal{G}_{F/k}$ is a group, and it follows that $\mathcal{A}_{F/k}$ is too. Let

$$\mathcal{C}_{F/k} := \{L \in \mathcal{G}_{F/k} : \mathrm{Gal}(L/k) \cong C_2 \times \mathrm{Gal}(F/k)\} \cup \{F \times F\}. \quad (3.1)$$

It is also a corollary of Lemma 3.1.5 that $\mathcal{C}_{F/k}$ is a subgroup of $\mathcal{G}_{F/k}$.

We say that L and L' are *k-equivalent* if $L' = L \circ L''$ for some extension L'' in $\mathcal{C}_{F/k}$, that is if they lie in the same $\mathcal{C}_{F/k}$-coset of $\mathcal{G}_{F/k}$. This defines an equivalence relation on $\mathcal{G}_{F/k}$.

Definition 3.1.6. *Suppose that F and k are normal over $\mathbb{Q}$ and* $\mathrm{Gal}(F/k)$ *is abelian. Let $\mathcal{G}^s_{F/k}$ be the subgroup of $\mathcal{G}_{F/k}$ containing extensions of F/k which are normal over $\mathbb{Q}$. If L belongs to $\mathcal{G}^s_{F/k}$ then we say that L is a* strictly admissible extension *of F.*

Let

$$\begin{aligned}\mathcal{A}^s_{F/k} &:= \mathcal{A}_{F/k} \cap \mathcal{G}^s_{F/k} \text{ and} && (3.2)\\ \mathcal{C}^s_{F/k} &:= \mathcal{C}_{F/k} \cap \mathcal{G}^s_{F/k}. && (3.3)\end{aligned}$$

Remark 3.1.7. There is a natural isomorphism $\mathcal{G}_{F/\mathbb{Q}} \cong \mathcal{G}^s_{F/k}$, which defines an injection $\mathcal{A}_{F/\mathbb{Q}} \hookrightarrow \mathcal{A}^s_{F/k}$.

The group $\mathcal{C}^s_{F/k}$ is clearly a subgroup of $\mathcal{A}^s_{F/k}$ and we define

$$c_4(F/k) := \log_2 |\mathcal{A}^s_{F/k}/\mathcal{C}^s_{F/k}|. \quad (3.4)$$

In Proposition 3.3.5 we shall see that if $F/\mathbb{Q}$ is abelian then every $\mathbb{Q}$-equivalence class of $\mathcal{G}_{F/\mathbb{Q}}$ has a representative which is unramified outside primes ramifying in $F/\mathbb{Q}$.

Since $C_{2a} \cong C_2 \times C_a$ for any odd integer a, we see that $c_4(F/k) \leq r_2(F/k)$. Suppose that σ is an element of $\mathrm{Gal}(F/k)$ of order 2. Kummer theory yields a well-known criterion for deciding whether there exists an extension L/F in $\mathcal{G}_F$ cyclic over $F^{\langle\sigma\rangle}$:

Theorem 3.1.8 (Albert's Theorem). *There exists a quadratic extension L/F such that $L/F^{\langle\sigma\rangle}$ is cyclic, if and only if $-1 \in \mathrm{N}_{F/F^{\langle\sigma\rangle}}(F)$.*

Proof. See Gras [**15**] p. 58. □

We shall say that F/k *satisfies Albert's condition* if the condition of the theorem is satisfied for all elements σ of $\mathrm{Gal}(F/k)$ of order 2. This is a necessary but not a sufficient condition for $c_4(F/k)$ to be maximal. For example, if $k_0 = \mathbb{Q}$, $k = \mathbb{Q}(\sqrt{d})$ and F is the Hilbert class field of k then for $d = -84$ and -651, the extension F/k satisfies Albert's condition, but $c_4(F/k) = 1$, as in both cases there exists an element σ of $\mathrm{Gal}(F/k)$ such that for all L in $\mathcal{G}_{F/F^{\langle\sigma\rangle}}$ if $L/\mathbb{Q}$ is normal then $\mathrm{Gal}(L/F^{\langle\sigma\rangle})$ is noncyclic. There may also exist L in $\mathcal{G}_{F/k}$ satisfying the condition, but no L in $\mathcal{A}_{F/k}$. For example, let $k = \mathbb{Q}$ and $F = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$. Then there exist quadratic extensions L/F which are cyclic over $\mathbb{Q}(\sqrt{-7})$ and normal over $\mathbb{Q}$, but none which are abelian over $\mathbb{Q}$.

3.2. The Cohomology of Quadratic Extensions

This section develops theory which will be applied in Section 3.3 and the next two chapters. We proceed in three stages. In Section 3.2.1 we recall some standard results from the cohomology of group extensions. In Section 3.2.2 we apply the theory of polycyclic groups to determine the possible group structure of $\mathrm{Gal}(L/k)$ where $L \in \mathcal{G}_{F/k}$ and $\mathrm{Gal}(F/k) \cong C_2^{\times n}$, while in Section 3.2.3 we investigate the frequency with which these groups occur in $\mathcal{G}_{F/k}$ by analysing the group structure of $\mathrm{Gal}(L \circ L'/k)$ where L and L' are elements of $\mathcal{G}_{F/k}$ and $\mathrm{Gal}(L/k)$ and $\mathrm{Gal}(L'/k)$ are known.

3.2.1. Cohomology. Let F/k be an abelian extension of number fields. Any extension L in $\mathcal{G}_{F/k}$ satisfies an exact sequence

$$1 \to \pm 1 \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(F/k) \to 1, \tag{3.5}$$

and so determines a class ϵ_L in $H^2(F/k, \pm 1) := H^2(\mathrm{Gal}(F/k), \pm 1)$ which is trivial if and only if L is in $\mathcal{C}_{F/k}$, as this is precisely when the sequence splits. Indeed, we shall see in Theorem 3.2.3 that if $L'' = L \circ L'$ then

$$\epsilon_{L''} = \epsilon_L \epsilon_{L'},$$

so we can consider $\mathcal{G}_{F/k}/\mathcal{C}_{F/k}$ as a subgroup of $H^2(F/k, \pm 1)$ under the embedding $L \mapsto \epsilon_L$. Any admissible extension L in $\mathcal{G}_{F/k}$ defines a central extension of $\mathrm{Gal}(F/k)$ which means that $\mathrm{Gal}(L/F)$ is contained in the centre of $\mathrm{Gal}(L/k)$.

Let G be a finite abelian group, let ϵ be a class of $H^2(G, \pm 1)$ and let a be a 2-cocycle representing ϵ. We define ϵ_* to be the bilinear alternating form given by

$$\epsilon_*(\sigma, \tau) := a(\sigma, \tau) a(\tau, \sigma)^{-1} \text{ for all } \sigma, \tau \in G. \tag{3.6}$$

and set

$$\epsilon^*(\sigma) := \prod_{i=0}^{s-1} a(\sigma, \sigma^i), \tag{3.7}$$

where s is the order of σ in G.

The next two lemmas are proved in Section 2 of Fröhlich [**11**].

Lemma 3.2.1. *Suppose that $L/F/k$ are as in* (3.5) *and let ϵ_L be the class of $H^2(F/k, \pm 1)$ determined by* $\mathrm{Gal}(L/k)$*. For any σ, τ in* $\mathrm{Gal}(F/k)$*, let $\tilde{\sigma}, \tilde{\tau}$ be elements of* $\mathrm{Gal}(L/k)$ *which map to σ and τ respectively in the exact sequence* (3.5)*. Identifying $\{\pm 1\}$ with a subgroup of* $\mathrm{Gal}(L/k)$ *as in* (3.5)*, and denoting the commutator $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1}$ by $[\tilde{\sigma}, \tilde{\tau}]$,*

a) $\tilde{\sigma}^s = \epsilon^*(\sigma)$ *and*
b) $[\tilde{\sigma}, \tilde{\tau}] = \epsilon_*(\sigma, \tau)$.

Lemma 3.2.2. *If G is an abelian 2-group then any class ϵ of $H^2(G, \pm 1)$ is uniquely defined by the pair ϵ_*, ϵ^*.*

Theorem 3.2.3 (Fröhlich [**11**] Theorem 2)**.** *Suppose that F/k is an abelian extension of number fields and that L is an element of $\mathcal{G}_{F/k}$. Let ϕ be the quadratic character of $\mathfrak{I}_F$ and ϵ the class of $H^2(F/k, \pm 1)$ associated with L. Let σ be an element of* $\mathrm{Gal}(F/k)$ *of order $s > 1$ and let $\boldsymbol{\alpha}$ be an idele of $F^{\langle\sigma\rangle}$ such that $(F/F^{\langle\sigma\rangle}; \boldsymbol{\alpha}) = \sigma$. Then for any τ in* $\mathrm{Gal}(F/k)$ *there exist ideles $\boldsymbol{\beta}_\sigma$ and $\boldsymbol{\gamma}_{\sigma,\tau}$ of F satisfying*

$$\mathrm{N}_{F/F^{\langle\sigma\rangle}}(\boldsymbol{\beta}_\sigma) = \boldsymbol{\alpha}^s, \tag{3.8}$$

$$\mathrm{N}_{F/F^{\langle\sigma\rangle}}(\boldsymbol{\gamma}_{\sigma,\tau}) = a\boldsymbol{\alpha}^{\tau-1} \textit{ for some } a \in (F^{\langle\sigma\rangle})^*, \tag{3.9}$$

and for any such ideles,

$$\epsilon^*(\sigma) = \phi(\boldsymbol{\beta}_\sigma), \textit{ and } \epsilon_*(\sigma, \tau) = \phi(\boldsymbol{\gamma}_{\sigma,\tau}).$$

Proof. Let $\mathfrak{p}$ be a prime ideal of k which does not ramify in F/k such that $(F/k;\mathfrak{p}) = \sigma$, and let $\mathfrak{P}$ be a prime of $F^{\langle\sigma\rangle}$ dividing $\mathfrak{p}$. Then $(F/F^{\langle\sigma\rangle};\mathfrak{P}) = \sigma$ and we can choose $\boldsymbol{\alpha}$ to be an idele such that $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) = 1$ and $v_{\mathfrak{Q}}(\alpha_{\mathfrak{Q}}) = 0$ at every other prime $\mathfrak{Q}$ of $F^{\langle\sigma\rangle}$. We can take $\boldsymbol{\beta}_\sigma$ to be the lift of $\boldsymbol{\alpha}$ to $\mathfrak{J}_F$, that is the idele with $\mathfrak{q}$-component α_q whenever $\mathfrak{q}$ divides q. Now

$$(F/F^{\langle\sigma\rangle};\boldsymbol{\alpha}^\tau \cdot \boldsymbol{\alpha}^{-1}) = 1,$$

so $\boldsymbol{\alpha}^{\tau-1}$ is in the kernel of the Artin map, hence there exist a and $\boldsymbol{\gamma}_{\sigma,\tau}$ satisfying (3.9).

By Lemma 3.2.1

$$\epsilon_*(\sigma,\tau) = [\tilde{\sigma},\tilde{\tau}] \text{ and } \epsilon^*(\sigma) = \tilde{\sigma}^s,$$

hence by Equations (3.8) and (3.9) and the properties of the Artin symbol it follows that

$$(L/F;\boldsymbol{\beta}_\sigma) = (L/F^{\langle\sigma\rangle};\boldsymbol{\alpha}^s) = \tilde{\sigma}^s,$$

and

$$(L/F;\boldsymbol{\gamma}_{\sigma,\tau}) \;\; = \;\; (L/F^{\langle\sigma\rangle};\boldsymbol{\alpha}^\tau \cdot \boldsymbol{\alpha}^{-1} \cdot a) = [\tilde{\sigma},\tilde{\tau}].$$

□

For any abelian group G the subgroup S of $H^2(G,\pm1)$ corresponding to abelian extensions of G is isomorphic to $\mathrm{Ext}^1_{\mathbb{Z}}(G,\pm1)$ (see Massy [**27**] p. 510), and we shall denote S by $\mathrm{Ext}(G,\pm1)$ accordingly. A class ϵ belongs to $\mathrm{Ext}(G,\pm1)$ if and only if $\epsilon_* = 1$.

Let $\widetilde{G}$ be an extension of G by ±1 and let ϵ be the class of $H^2(G,\pm1)$ corresponding to $\widetilde{G}$. Since $\epsilon_*(\sigma^2,\tau) = 1$ for all σ,τ in G, by Lemma 3.2.1 the image of G^2 under the natural embedding $G \hookrightarrow \widetilde{G}$ is always contained in the centre of $\widetilde{G}$, hence

$$|H^2(G/G^2,\pm1)/\mathrm{Ext}(G/G^2,\pm1)| = |H^2(G,\pm1)/\mathrm{Ext}(G,\pm1)|.$$

With this as justification we shall assume for the remainder of this section that G is isomorphic to the elementary abelian 2-group of order 2^n, which we denote by $C_2^{\times n}$.

We now switch briefly from a multiplicative to an additive notion of composition to investigate the structure of $H^2(G,\mathbb{F}_2)$ as a vector space over $\mathbb{F}_2$. The group $G \cong C_2^{\times n}$ is isomorphic to the additive group of an $\mathbb{F}_2$-vector space of dimension n and we shall write

$$\dim_{\mathbb{F}_2} G = n.$$

In this context ϵ^* is the quadratic form satisfying

$$\epsilon^*(\sigma) := a(\sigma,\sigma) + a(\sigma,1) \;\text{ for all } \sigma \in G, \tag{3.10}$$

where a is a cocycle representing ϵ as in (3.7).

Lemma 3.2.4 (Massy [**27**] Lemma 1(i))**.** *For all elements σ, τ of G,*

$$\epsilon^*(\sigma\tau) = \epsilon^*(\sigma) + \epsilon^*(\tau) + \epsilon_*(\sigma, \tau).$$

Proposition 3.2.5. *Let $Q(G)$ be the $\mathbb{F}_2$-vector space of quadratic forms on G, and let $\mathrm{Alt}(G, \mathbb{F}_2)$ denote the subspace of alternating quadratic forms. The map*

$$f : H^2(G, \mathbb{F}_2) \to Q(G),\ \epsilon \mapsto \epsilon^*,$$

is an isomorphism of vector spaces, and the restriction of f to $\mathrm{Ext}(G, \mathbb{F}_2)$ induces an isomorphism between $\mathrm{Ext}(G, \mathbb{F}_2)$ and $\mathrm{Hom}(G, \mathbb{F}_2)$.

Proof. See Equations (1.9) and (1.10) of Massy [**27**]. □

By Lemma 3.2.4, ϵ^* is a homomorphism if and only if $\epsilon_* = 0$.

Corollary 3.2.6. *Let $n = \dim_{\mathbb{F}_2} G$. The sequence*

$$0 \to \mathrm{Ext}(G, \mathbb{F}_2) \to H^2(G, \mathbb{F}_2) \to \mathrm{Alt}(G, \mathbb{F}_2) \to 0.$$

is exact and

$$\begin{aligned} \dim_{\mathbb{F}_2} H^2(G, \mathbb{F}_2) &= \binom{n+1}{2}, \\ \dim_{\mathbb{F}_2} \mathrm{Ext}(G, \mathbb{F}_2) &= n, \\ \dim_{\mathbb{F}_2} \mathrm{Alt}(G, \mathbb{F}_2) &= \binom{n}{2}. \end{aligned}$$

Corollary 3.2.7. *Suppose that $r_2(F/k) = n$. Then*

$$\mathcal{G}^s_{F/k}/\mathcal{A}^s_{F/k} \cong C_2^{\times m} \textit{ for some } m \leq \binom{n}{2}. \tag{3.11}$$

Proof. By Corollary 3.2.6

$$\dim_{\mathbb{F}_2} \mathcal{G}_{F/k}/\mathcal{A}_{F/k} \leq \binom{n}{2},$$

so it remains to show that $\dim_{\mathbb{F}_2} \mathcal{G}^s_{F/k}/\mathcal{A}^s_{F/k} \leq \dim_{\mathbb{F}_2} \mathcal{G}_{F/k}/\mathcal{A}_{F/k}$. This follows from the observation that

$$\dim_{\mathbb{F}_2} \mathcal{G}_{F/k}/\mathcal{C}_{F/k} \cdot \mathcal{G}^s_{F/k} \geq \dim_{\mathbb{F}_2} \mathcal{A}_{F/k}/\mathcal{C}_{F/k} \cdot \mathcal{A}^s_{F/k}.$$

□

We shall see in (3.16) that this upper bound is attained if k is an imaginary quadratic field and F is the Hilbert class field of k.

We now return to multiplicative notation for cohomology classes. The following lemma is fundamental in determining the structure of $\mathrm{Gal}(L/k)$ for extensions L in $\mathcal{G}_{F/k}$. We denote the class of $H^2(F/k, \pm 1)$ associated with L by ϵ_L, and we shall write ϵ_{L*} for $(\epsilon_L)_*$. For any group G we let $Z(G)$ denote the centre of G.

Lemma 3.2.8. *Let $L/F/k$ be as above, and let $G := \mathrm{Gal}(F/k)$ and $\widetilde{G} := \mathrm{Gal}(L/k)$. Then*

$$\widetilde{G}/Z(\widetilde{G}) \cong C_2^{\times 2m}, \text{ with } 0 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor, \tag{3.12}$$

there are elements $\sigma_1, \ldots, \sigma_{2m}$ of G satisfying

$$\begin{aligned} \epsilon_{L*}(\sigma_{2i}, \sigma_{2i-1}) &= -1,\ 1 \leq i \leq m, \\ \epsilon_{L*}(\sigma_i, \sigma_j) &= 1 \text{ for all } j \notin \{i+1, i-1\}, \end{aligned}$$

and $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{2m}$ is a basis for $\widetilde{G}/Z(\widetilde{G})$.

Proof. Since ϵ_{L*} is bilinear, $\epsilon_{L*}(\sigma^2, \tau) = 1$ for all σ, τ in G, so G^2 is contained in $Z(\widetilde{G})$, hence we must have $\widetilde{G}/Z(\widetilde{G}) \cong C_2^{\times b}$ for some integer $b \geq 0$.

To see that b must be even, suppose that $\epsilon_{L*}(\sigma_1, \sigma_2) = -1$ and that $\epsilon_{L*}(\sigma_3, \tau) = -1$ for some τ in G. By the bilinearity of ϵ_{L*}, if $\sigma_3 \neq \sigma_1\sigma_2$ then $\tilde{\sigma_3}$ must commute with $\tilde{\sigma_1}$ and $\tilde{\sigma_2}$, and the result follows. □

Definition 3.2.9. *Let m be a non-negative integer. We define*

$$\mathcal{G}_{F/k}^{(m)} := \{L \in \mathcal{G}_{F/k} : \mathrm{Gal}(L/k)/Z(\mathrm{Gal}(L/k)) \cong C_2^{\times 2m}\}.$$

For $m > 0$, $\mathcal{G}_{F/k}^{(m)}$ is not a subgroup of $\mathcal{G}_{F/k}$, but by Theorem 3.2.3, it is closed under the action of $\circ$ with $\mathcal{A}_{F/k} = \mathcal{G}_{F/k}^{(0)}$. We shall often find it useful to consider $\mathcal{G}_{F/k}^{(m)}$ as a collection of $\mathcal{A}_{F/k}$-cosets.

Lemma 3.2.10. *Suppose that L_1 and L_2 are in $\mathcal{G}_{F/k}^{(1)}$ and for $i = 1, 2$ define $G_i := \mathrm{Gal}(L_i/k)$, $Z_i := Z(G_i)$ and $S_i := \mathrm{Gal}(L^{Z_i}/k)$. Let $S := S_1 \cap S_2$ and $L := L_1 \circ L_2$. Then $|S_1| = |S_2| = 4$ and*

a) *if $|S| = 4$ then $L \in \mathcal{A}_{F/k}$,*

b) *if $|S| = 2$ then $L \in \mathcal{G}_{F/k}^{(1)}$,*

c) *if $|S| = 0$ then $L \in \mathcal{G}_{F/k}^{(2)}$.*

Proof. Cases a) and c) are simple consequences of the properties of ϵ_*. In case b), let G_0 be the subgroup of $\mathrm{Gal}(F/k)$ generated by S_1S_2. This is a non-cyclic group of order 8, hence by Lemma 3.2.8 must contain an element of order 2 which maps into the centre of $\mathrm{Gal}(L/k)$. □

The following special case will be particularly useful. Setting $G := \mathrm{Gal}(F/k)$, let $\sigma_1, \ldots, \sigma_n$ be a basis for G/G^2 and let $F_{i,j} = F^{\langle \sigma_i, \sigma_j \rangle}$. Suppose that L_1 and L_2 are as in the lemma above, with $L_1/F_{i,j}$ and $L_2/F_{j,\ell}$ non-abelian. Then $\epsilon_*(\sigma_i\sigma_\ell, \tau) = 1$ for all τ in $\mathrm{Gal}(L/k)$.

As a generalization of Lemma 3.2.10 we obtain:

Proposition 3.2.11. *Suppose that $L_i \in \mathcal{G}_{F/k}^{(r_i)}$ and let $Z_i := Z(\mathrm{Gal}(L_i/k))$ and $S_i := \mathrm{Gal}(L^{Z_i}/k)$ for $i = 1, 2$. Let $S := S_1 \cap S_2$, $T := S_1S_2$ and $L := L_1 \circ L_2$. Then L belongs to $\mathcal{G}_{F/k}^{(r)}$ where*

$$r := \frac{\log_2 |T| - \log_2 |S|}{2}.$$

3.2.2. Admissible Groups. Suppose that F/k is an extension of number fields with Galois group isomorphic to $C_2^{\times n}$ and let L be an element of $\mathcal{G}_{F/k}$. In this section we will determine the groups which may occur as $G := \mathrm{Gal}(L/k)$, that is which satisfy Lemma 3.2.8. We will make use of the theory of polycyclic groups, which we introduce briefly below. For more details see Sims [**60**] Chapter 9. For proofs of Lemma 3.2.18, Proposition 3.2.19 and Theorem 3.2.21, see Appendix A.

Definition 3.2.12. *Let G be a group. A series of subgroups*

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m \trianglerighteq G_{m+1} = 1$$

is a polycyclic series *for G if*

a) *G_{i+1} is a normal subgroup of G_i, and*
b) *the quotient G_i/G_{i+1} is cyclic*

for $1 \leq i \leq m$.

Definition 3.2.13. *If G has a polycyclic series we say that G is a* polycyclic group.

It is well known that all finitely generated nilpotent groups are polycyclic. We shall only consider polycyclic groups of finite order, (i.e. soluble groups).

Let G be a polycyclic group with polycyclic series

$$G = G_1 \geq G_2 \geq \cdots \geq G_m \geq G_{m+1} = 1,$$

and suppose that the quotient G_i/G_{i+1} has order r_i for $1 \leq i \leq m$. For each i between 1 and m let σ_i denote an element of G whose image in G_i/G_{i+1} has order r_i. Then $\sigma_1, \ldots, \sigma_m$ is a *polycyclic generating sequence* for G. We may assume that σ_i never belongs to G_{i+1}.

Definition 3.2.14. *A* collected word *with respect to $\sigma_1, \ldots, \sigma_m$ is a word of the form*

$$\sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_m^{a_m},$$

where $0 \leq a_i < r_i$ for $1 \leq i \leq m$.

Lemma 3.2.15. *Every element g of G has a unique expression as a collected word with respect to $\sigma_1, \ldots, \sigma_m$.*

Proof. See Sims [**60**] Section 9.4. □

It is a (potentially confusing) convention of polycyclic presentations of groups that if a commutator relation is not given for a pair of generators σ_i, σ_j, it is assumed that they commute. For any group G, let $\Sigma_i(G)$ denote the number of elements of G of order i. The identity element of G will be denoted by 1.

Definition 3.2.16. *Let n be an even integer.*

a) *We define $\mathfrak{D}_n$ to be the polycyclic group generated by $\sigma_1, \ldots, \sigma_{n+1}$ where*

$$[\sigma_{2a-1}, \sigma_{2a}] = \sigma_{n+1}, \qquad \textit{for } 1 \le a \le n/2, \tag{3.13}$$

and $\sigma_i^2 = 1$ for $1 \le i \le n+1$.

b) *Let $\mathfrak{Q}_n$ be the polycyclic group generated by $\sigma_1, \ldots, \sigma_{n+1}$ where* (3.13) *holds and $\sigma_1^2 = \sigma_2^2 = \sigma_{n+1}$ and $\sigma_i^2 = 1$ for $3 \le i \le n+1$.*

c) *Let $\mathfrak{B}_{n+1}$ be the polycyclic group generated by $\sigma_1, \ldots \sigma_{n+2}$ where*

$$\sigma_{2a-1}\sigma_{2a}\sigma_{2a-1}^{-1} = \sigma_{2a}\sigma_{n+2}, \qquad \textit{for } 1 \le a \le n/2,$$

$$\sigma_1^2 = \ldots = \sigma_n^2 = \sigma_{n+2}^2 = 1 \textit{ and } \sigma_{n+1}^4 = 1.$$

Remark 3.2.17. The groups $\mathfrak{D}_2$ and $\mathfrak{Q}_2$ are respectively the dihedral and quaternion groups of order 8. To visualise $\mathfrak{B}_{n+1}$ it may be helpful to notice that the generators $\sigma_1, \ldots, \sigma_n, \sigma_{n+2}$ satisfy the defining relations of a generating set for a subgroup S isomorphic to $\mathfrak{D}_n$ and if s is in S then $s\sigma_{n+1}$ has order 2 if s has order 4, and order 4 otherwise. The standard description of $\mathfrak{B}_{n+1}$, which we use in Appendix A, is as the central product of either $\mathfrak{D}_n$ or $\mathfrak{Q}_n$ with C_4.

Lemma 3.2.18. *Let n be an even integer. The groups G defined in Definition 3.2.16 have the properties described in the following table:*

G	$\#G$	$\Sigma_4(G)$	$Z(G)$
$\mathfrak{D}_n$	2^{n+1}	$2^n - 2^{n/2}$	C_2
$\mathfrak{Q}_n$	2^{n+1}	$2^n + 2^{n/2}$	C_2
$\mathfrak{B}_{n+1}$	2^{n+2}	2^{n+1}	C_4

Proposition 3.2.19. *Let $n \ge 2$ be an even integer. If G is a group of order 2^{n+1} with a minimal generating set of size n and centre of order 2, which satisfies the conditions of Lemma 3.2.8 then G is isomorphic to either $\mathfrak{D}_n$ or $\mathfrak{Q}_n$. If G is a group of order 2^{n+2} with a minimal generating set of size $n+1$ and centre of order 4, then G must be isomorphic to either $\mathfrak{B}_{n+1}$, $C_2 \times \mathfrak{D}_n$ or $C_2 \times \mathfrak{Q}_n$.*

Definition 3.2.20. *Let m and n be integers with $n \ge 2$, $0 \le m < n$ and $n - m$ even. If n is even and $m = 0$ then define $T_{n,m} := \{\mathfrak{D}_n, \mathfrak{Q}_n\}$, otherwise*

$$T_{n,m} := \{\mathfrak{D}_{n,m}, \mathfrak{B}_{n,m}, \mathfrak{Q}_{n,m}\},$$

where

$$\begin{aligned}\mathfrak{D}_{n,m} &:= C_2^{\times m} \times \mathfrak{D}_{n-m},\\ \mathfrak{Q}_{n,m} &:= C_2^{\times m} \times \mathfrak{Q}_{n-m} \textit{ and}\\ \mathfrak{B}_{n,m} &:= C_2^{\times m-1} \times \mathfrak{B}_{n+1-m}.\end{aligned}$$

Theorem 3.2.21. *Let m and n be as in Definition 3.2.20. If $\widetilde{G}$ is a group satisfying Lemma 3.2.8 of order 2^{n+1} with n generators and centres of order 2^{m+1}, then $\widetilde{G}$ is isomorphic to a group in $T_{n,m}$.*

Corollary 3.2.22. *Let L be an element of $\mathcal{G}_{F/k}$. Then $\mathrm{Gal}(L/k)$ is uniquely determined by its centre and the number of elements of order 4.*

Thus we now have a full list of the groups which may occur as $\mathrm{Gal}(L/k)$ for L in $\mathcal{G}^s_{F/k}$.

3.2.3. Cyclicity Vectors and $\mathrm{Gal}(L \circ L'/k)$. We shall say that an extension L/k is of *type G* if $\mathrm{Gal}(L/k)$ is isomorphic to G. Given extensions L/k and L'/k of types G and G', we would like to determine the type of $L \circ L'$. In particular, we shall examine extensions of the form $A \circ L$ where A is an abelian extension of k. One of our most useful tools for this task will be addition of *cyclicity vectors* which we introduce below.

Let $\sigma_0, \dots \sigma_{2^n-1}$ be an ordering of the elements of $G := \mathrm{Gal}(F/k)$ such that σ_0 is the identity element, and $\sigma_1, \dots \sigma_n$ is a polycyclic generating sequence for G. Let $J := \{j_1, \dots, j_m\}$ be a subset of $\{1, \dots, 2^{n-1}\}$. We define F_J to be the maximal subfield of F fixed by $\langle \sigma_j : j \in J \rangle$. We say that σ_j *divides* g if σ_j appears in the unique representation of g as a collected word with respect to the basis $\{\sigma_1, \dots, \sigma_n\}$.

Definition 3.2.23. *Let L be an element of $\mathcal{G}_{F/k}$. Fixing an ordering of* $\mathrm{Gal}(F/k)$ *as above, we define the* cyclicity vector s_L *to be the element of $\mathbb{F}_2^{2^n-1}$ which has ith component $s_L^{(i)} = 1$ if and only if* $\mathrm{Gal}(L/F_i) \cong C_4$. *In addition, we define*

$$s_L(\sigma_i) := s_L^{(i)}.$$

Lemma 3.2.24 (Vaughan [**63**]). *Suppose that L and L' are elements of $\mathcal{G}_{F/k}$ and let $L'' = L \circ L'$. Then*

$$s_{L''} = s_L + s_{L'}. \tag{3.14}$$

Definition 3.2.25. *For any element s of $\mathbb{F}_2^\ell$, we define the* length *of s to be ℓ and the* weight *of s, $w(s)$ to be the number of non-zero entries of s.*

Example 3.2.26. We construct examples of cyclicity vectors for admissible extensions of all possible types when $n - m = 2$.

a) If L is of type $C_2^{\times n+1}$ then s_L is the all-zero vector.

b) If L is of type $C_2^{\times n-1} \times C_4$ then s_L is a finite sum of vectors $s_j := (s_j(g))$, with $1 \leq j \leq n$ where $s_j(g) = 1$ if and only if σ_j divides g.
c) If L is of type $\mathfrak{D}_{n,n-2}$, the extension L/F_1 is cyclic and $L/F^{\langle\sigma_1\sigma_2\rangle} \cong C_2 \times C_2$ then $s_L(g) = 1$ if and only if σ_1 divides g and σ_2 does not divide g.
d) If L is of type $\mathfrak{Q}_{n,n-2}$ and L/F_1 and L/F_2 are cyclic then $s_L(g) = 1$ if and only if at least one of σ_1 and σ_2 divides g.
e) If L is of type $\mathfrak{B}_{n,n-2}$ and L/F_1 and $L/F^{\langle\sigma_2\sigma_3\rangle}$ are both cyclic then $s_L(g) = 1$ if and only if
    - σ_1 divides g and neither σ_2 nor σ_3 divides g or
    - $\sigma_2\sigma_3$ divides g and σ_1 does not divide g.

Retaining the notation developed above, suppose that $F/\mathbb{Q}$ is normal, F/k is of type $C_2^{\times n}$ and $\dim_{\mathbb{F}_2} \mathcal{G}_{F/k}/\mathcal{A}_{F/k} = \binom{n}{2}$. We shall now investigate the frequency with which each group in $T_{n,m}$ may occur as $\mathrm{Gal}(L/k)$ for L in $\mathcal{G}_{F/k}$.

Lemma 3.2.27. *Suppose that $n \geq 3$. Let A be an element of $\mathcal{A}_{F/k}$ such that $\mathrm{Gal}(A/k) \cong C_2^{\times n-1} \times C_4$ and $\mathrm{Gal}(A/F_{i,j}) \cong C_2^{\times 3}$, and let L be an element of $\mathcal{G}^{(1)}_{F/k}$ with $\mathrm{Gal}(L/k)$ isomorphic to $C_2^{\times n-2} \times \mathrm{Gal}(L/F_{i,j})$. Then $\mathrm{Gal}(A \circ L/k)$ is isomorphic to $\mathfrak{B}_{n,n-2}$.*

Proof. Let A and L be as in the statement of the lemma. We must have $\mathrm{Gal}(L/k)$ isomorphic to either $\mathfrak{D}_{n,n-2}$ or $\mathfrak{Q}_{n,n-2}$, and we will have proved the assertion if we can show that $w(s_{A\circ L}) = 2^{n-1}$.

If we suppose that $\mathrm{Gal}(L/k) \cong \mathfrak{D}_{n,n-2}$, then we may order our basis so that $s_L(g) = 1$ if and only if σ_1 divides g and σ_2 does not, and that $s_A(g) = 1$ if and only if σ_3 divides g.

Suppose that σ_3 divides g. This occurs 2^{n-1} times. Of these σ_1 will divide g 2^{n-2} times and $\sigma_1\sigma_2$ will divide g 2^{n-3} times, so there are 2^{n-3} distinct g for which $s_L(g) = s_A(g) = 1$, hence

$$\begin{aligned} w(s_{A\circ L}) &= w(s_A) + w(s_L) - 2 \cdot 2^{n-3} \\ &= 2^{n-1} + (2^{n-1} - 2^{n-2}) - 2^{n-2} \\ &= 2^{n-1} = w(s_A) \end{aligned}$$

as claimed. Similarly, if $\mathrm{Gal}(L/k) \cong \mathfrak{Q}_{n,n-2}$, then we order our basis so that $s_L(g) = 1$ if and only if σ_1 or σ_2 (or both) divide g. In this case there are $2^{n-2} + 2^{n-2} - 2^{n-3} = 2^{n-2} + 2^{n-3}$ distinct elements of G for which $s_L(g) = s_A(G) = 1$, hence

$$\begin{aligned} w(s_{A\circ L}) &= w(s_A) + w(s_L) - 2 \cdot (2^{n-2} + 2^{n-3}) \\ &= 2^{n-1} + (2^{n-1} + 2^{n-2}) - (2^{n-1} + 2^{n-2}) \\ &= 2^{n-1} = w(s_A). \end{aligned}$$

□

Lemma 3.2.28. *Suppose that $n \geq 3$. Let L be an element of $\mathcal{G}^{(1)}_{F/k}$ with $\mathrm{Gal}(L/F_{i,j,\ell}) \cong \mathfrak{B}_3$ and $\mathrm{Gal}(L/F_{i,j}) \cong \mathfrak{D}_2$, and let A be an element of $\mathcal{A}_{F/k}$. For i in $\{1, \dots, n\}$, let v_i denote the element of $\mathbb{F}_2^{2^n-1}$ which has jth component 1 if and only if σ_i divides σ_j. If*

$$s_A = v_\ell + v \text{ for some } v \in \langle v_i, v_j \rangle,$$

then $A \circ L$ is not of type $\mathfrak{B}_{n,n-2}$.

Proof. It follows directly from the construction of $\mathfrak{B}_n$ in Remark 3.2.17 that if $s_L + v_\ell$ is the cyclicity vector of an extension $L'/F/k$ that extension is of type $\mathfrak{D}_{n,n-2}$, and is dihedral of order 8 over $F_{i,j}$. □

Definition 3.2.29. *Let L be an element of $\mathcal{G}^s_{F/k}$, and let S be a set of representatives of the equivalence classes of $\mathcal{A}_{F/k}/\mathcal{C}_{F/k}$. For any group $\mathfrak{G}$ we define*

$$N(\mathfrak{G}, L) := |\{A \in S : \mathrm{Gal}((A \circ L)/k) \cong \mathfrak{G}\}|.$$

Proposition 3.2.30. *If $|S| = n$ then for any L in $\mathcal{G}^{(1)}_{F/k}$,*

$$N(\mathfrak{D}_{n,n-2}, L) = 3,\ N(\mathfrak{Q}_{n,n-2}, L) = 1 \text{ and } N(\mathfrak{B}_{n,n-2}, L) = 2^n - 4.$$

Proof. Suppose that $\mathrm{Gal}(L/k) \cong \mathfrak{D}_{n,n-2}$ or $\mathfrak{Q}_{n,n-2}$ and that $\mathrm{Gal}(L/F_{i,j})$ is non-abelian. By Lemma 3.2.27, there are at least as many $\mathfrak{B}_{n,n-2}$ extensions in $S \circ L$ as there are fields A in S with $\mathrm{Gal}(A/F_{i,j}) \cong C_2^{\times 3}$ and $\mathrm{Gal}(A/k) \cong C_4 \times C_2^{\times n-1}$. Since $|S| = n$ there are $2^n - 4$ such A and the result follows at once. On the other hand if $\mathrm{Gal}(L/k) \cong \mathfrak{B}_{n,n-2}$ then we saw in Lemma 3.2.28 that there exists an abelian extension A in $\mathcal{A}^s_{F/k}$ such that $A \circ L$ is of type $\mathfrak{D}_{n,n-2}$, and the result follows by the argument above. □

We now relax the condition on n and m, and extend the definition of $T_{n,m}$ to the case where $n = m$, by setting $T_{n,n} := \{C_4 \times C_2^{\times n-1}\}$. Recall that $n - m$ is always an even non-negative integer and that if L belongs to $\mathcal{G}_{F/k}$ and $\mathrm{Gal}(L/k)$ is in $T_{n,m}$ then L is in $\mathcal{G}^{(r)}_{F/k}$, where $r := (n - m)/2$.

The next result is a generalization of Lemma 3.2.27.

Lemma 3.2.31. *Suppose that L is an element of $\mathcal{G}_{F/k}$ of type $\mathfrak{D}_{n,m}$ and let G_L be a subgroup of $\mathrm{Gal}(F/k)$ such that L/F^{G_L} is of type $\mathfrak{D}_n$. If there exists a field A in $\mathcal{A}_{F/k}$ such that $\mathrm{Gal}(A/F^{G_L})$ contains no elements of order 4 then $A \circ L$ is of type $\mathfrak{B}_{n,m}$.*

Proof. We retain the notation of Lemma 3.2.27. Again we wish to prove that $w(s_{A \circ L}) = w(s_A)$. Let $r := (n - m)/2$. We have $s_L(g) = s_A(g)$ for g

in $\mathrm{Gal}(F/k)$ when $\sigma_1\sigma_2$ divides g and $\sigma_3 \dots \sigma_{r+2}$ does not. This will occur $2^{n-2} - 2^{n-(r+2)}$ times, and so

$$w(s_{A\circ L}) = 2^{n-1} + 2^{n-1} - 2^{n-r-1} - 2(2^{n-2} - 2^{n-r-2}) = w(s_A).$$

□

A similar statement holds if L/k is of type $\mathfrak{Q}_{n,m}$. Therefore if $\mathrm{Gal}(L/k)$ is in $T_{n,m}$, and $c_4(F/k) = n$ then $N(\mathfrak{B}_{n,m}, L) \geq 2^n - 2^{n-m}$.

On the other hand, since $\mathfrak{B}_{n,m}$ may be constructed via a dihedral group of type $\mathfrak{D}_{n-1,m-1}$, it follows analogously to the proof of Lemma 3.2.28 that if L is of type $\mathfrak{B}_{n,m}$ then there will be either 0 or 2^{n-m} extensions of type $\mathfrak{D}_{n,m}$ or type $\mathfrak{Q}_{n,m}$ in $S \circ L$, the former if $|S| = n$.

Proposition 3.2.32. *Suppose that $|S| = n$. Let L be an element of $\mathcal{G}_{F/k}$ of type $\mathfrak{D}_{n,m}$ (resp. $\mathfrak{Q}_{n,m}$) and let $r := (n-m)/2$. Then*

$N(\mathfrak{B}_{n,m}, L)$	$N(\mathfrak{D}_{n,m}, L)$	$N(\mathfrak{Q}_{n,m}, L)$
$2^n - 2^{2r}$	$2^{2r-1} + 2^{r-1}$	$2^{2r-1} - 2^{r-1}$

Proof. Let L be as in the statement of the lemma and let K be an extension of k contained in F such that $\mathrm{Gal}(L/K)$ is isomorphic to $\mathfrak{D}_{n-m,0}$ or $\mathfrak{Q}_{n-m,0}$. Let $\mathcal{A}$ be the subgroup of S generated by the elements which are cyclic over $F^{\langle\sigma\rangle}$ for some σ in $\mathrm{Gal}(F/K)$. If A is in S then by Lemma 3.2.31, A belongs to $\mathcal{A}$ if and only if $A \circ L$ is not of type $\mathfrak{B}_{n,m}$. Therefore

$$f_D + f_Q = |\mathcal{A}| = 2^{n-m}, \tag{3.15}$$

where $f_D = N(\mathfrak{D}_{n,m}, L)$ and $f_Q = N(\mathfrak{Q}_{n,m}, L)$. Now consider the cyclicity vectors $s_{A\circ L} = s_A + s_L$. Let w_D and w_Q be the weights of the cyclicity vectors of extensions of type $\mathfrak{D}_{n,m}$ and type $\mathfrak{Q}_{n,m}$ respectively. Because we are applying the same translation to s_A for all A in $\mathcal{A}$, we see that

$$2^{n-m} w_A = f_D w_D + f_Q w_Q,$$

and substituting the values of w_A, w_D and w_Q and combining with (3.15) gives us the result. □

3.3. Admissible Extensions and Quadratic Twists

Having developed some general theory for towers of extensions $L/F/k$ with L/F quadratic, F/k abelian and L/k normal, we shall now apply it to towers where $k/\mathbb{Q}$ is an imaginary quadratic field and F is a field of definition for an elliptic curve with CM by an order of k.

Let K be an imaginary quadratic field, let H be the Hilbert class field of K and suppose that D_K is divisible by $n+1$ distinct primes. Let F_g be the genus field of K, and recall that F_g is the maximal subfield of H which

FIGURE 1

$$\begin{tikzcd}
 & L \arrow[d, dash] & \\
 & H \arrow[dl, dash] \arrow[ddr, dash] & \\
H^{G_2} \arrow[ddr, dash] & & \\
 & & F_g \arrow[dl, dash] \\
 & K \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\mathrm{Gal}(F_g/K) \cong C_2^{\times n}$$

$$G_2 := \{g \in \mathrm{Gal}(H/K) : g^2 = 1\}$$

$$\mathrm{Gal}(H/H^{G_2}) \cong C_2^{\times n}$$

is abelian over $\mathbb{Q}$. The first major result of this section is the theorem of Nakamura [**34**] that

$$\dim_{\mathbb{F}_2} \mathcal{G}^s_{H/K}/\mathcal{A}^s_{H/K} = \binom{n}{2}. \tag{3.16}$$

Next we shall investigate the structure of $\mathcal{A}^s_{H/K}$. The second main result of this section is Proposition 3.3.23 where we prove that for all imaginary quadratic fields K with discriminants D_K divisible by at least 2 distinct rational primes,

$$n - r_4(H/K) - 1 \leq c_4(H/K) \leq n - r_4(H/K).$$

Applying results of Gerth [**12**] on the 4-rank of the class group of imaginary quadratic fields we shall see that for all $n \geq 1$ there are an infinite number of imaginary quadratic fields K with $c_4(H/K) = n$.

Let $n := r_2(H/K)$ and let

$$D_K = p_1^* \dots p_{n+1}^* \tag{3.17}$$

be a decomposition of D_K into a product of prime discriminants as in Proposition 2.2.2, with the convention that if 2 divides D_K then $p_{n+1} = 2$. By a *dihedral extension*, we shall mean an extension with Galois group isomorphic to the dihedral group of order 8, which we denoted $\mathfrak{D}_2$ in Section 3.2.2.

Proposition 3.3.1 (Nakamura [**34**]). *For any integers i, j such that $1 \leq i < j \leq n$ there exists a dihedral extension L/K containing $K(\sqrt{p_i^*}, \sqrt{p_j^*})$ such that $L/\mathbb{Q}$ is normal.*

Equation (3.16) is an immediate corollary to this proposition, which we shall prove, following Nakamura [**34**] as a consequence of Lemmas 3.3.3, 3.3.2 and 3.3.6 below. We begin by recalling some background on dihedral extensions.

Let k be a number field and let F/k be an extension with

$$\mathrm{Gal}(F/k) = \langle\sigma,\tau\rangle \cong C_2 \times C_2.$$

An extension $L \in \mathcal{G}_{F/k}$ is a dihedral extension of k if and only if it is cyclic over precisely one of $F^{\langle\sigma\rangle}$, $F^{\langle\tau\rangle}$, and $F^{\langle\sigma\tau\rangle}$, hence the cohomology class of the extension $L/F/k$ is determined by knowledge of this subfield.

Let d_1 and d_2 be elements of k and let $\mathfrak{p}$ be a prime of k. We denote the quadratic Hilbert symbol by $\left(\frac{d_1,d_2}{\mathfrak{p}}\right)$ and recall that

$$\left(\frac{d_1,d_2}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } d_1 \text{ is a norm in } k_{\mathfrak{p}}(\sqrt{d_2})/k_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

and that $\left(\frac{d_1,d_2}{\mathfrak{p}}\right) = \left(\frac{d_2,d_1}{\mathfrak{p}}\right)$. For more properties of the Hilbert symbol, see for example Neukirch [**35**] Section V.3. We shall make frequent use of the fact that the conic

$$x^2 - d_1y^2 - d_2z^2 = 0,$$

has k-rational points if and only if

$$\left(\frac{d_1,d_2}{\mathfrak{p}}\right) = 1$$

for all primes $\mathfrak{p}$ of k ramifying in $k(\sqrt{d_1},\sqrt{d_2})$, and that if this is the case and $P = (x : y : z)$ is such a point, the field $F := k(\sqrt{x+y\sqrt{d_1}},\sqrt{d_2})$ is a dihedral extension of k which is cyclic of degree 4 over $k(\sqrt{d_1d_2})$. If d_1 and d_2 are rational integers then we may choose P so that the extension F/k is unramified outside primes dividing $2d_1d_2$ and if d_1 and d_2 are discriminants, then we may choose P to ensure that F/k is unramified outside d_1d_2, (see Rédei and Reichardt [**38**]). We summarize the last part of this discussion as Lemma 3.3.2 for ease of reference.

Lemma 3.3.2. *Let k be either $\mathbb{Q}$ or K. If there exist discriminants d_1 and d_2 dividing D_K such that*

$$\left(\frac{d_1,d_2}{\mathfrak{p}}\right) = 1,$$

for all primes $\mathfrak{p}$ of k dividing d_1d_2 then there exists a dihedral extension F/k containing $k(\sqrt{d_1},\sqrt{d_2})$, cyclic over $k(\sqrt{d_1d_2})$ and unramified outside d_1d_2.

We call such a pair (d_1, d_2) a *partial decomposition* of D_K. If F is as in Lemma 3.3.2 then the compositum FH is either equal to, or a quadratic extension of, H. In this section we shall mostly consider the case where d_1 and d_2 are both prime discriminants and in Section 3.3.2 the case where $d_1d_2 = D_K$.

Lemma 3.3.3. *For any odd primes p_i and p_j dividing D_K there exist discriminants d_1, d_2 dividing $p_i p_j$ and satisfying the conditions of Lemma 3.3.2 with k equal to K.*

Proof. See Nakamura [**34**] p. 639. □

Example 3.3.4. If $p_i \equiv p_j \equiv 3 \bmod 4$ we may always take $k = \mathbb{Q}$ in Lemma 3.3.2, since in this case $\left(\frac{-p_i}{p_j}\right) = -\left(\frac{-p_j}{p_i}\right)$.

Proposition 3.3.5. *Let F be an algebraic number field such that $F/\mathbb{Q}$ is normal and $G := \mathrm{Gal}(F/\mathbb{Q})$ is an abelian 2-group, let D_F be the discriminant of $F/\mathbb{Q}$ and let ϵ be a class in $H^2(G, \pm 1)$. If there exists an extension L in $\mathcal{G}_{F/\mathbb{Q}}$ of type ϵ, then there exists an extension L' of type ϵ unramified outside primes dividing D_F.*

Proof. This is Corollary 1 to Theorem 5 of Fröhlich [**11**]. □

Lemma 3.3.6 (Nakamura [**34**] Lemma 1)**.** *Let F/K be a dihedral extension containing $K(\sqrt{p_i^*}, \sqrt{p_j^*})$. Then there exists a Dirichlet character κ of K such that if L_κ is the extension of H corresponding to the character $\kappa \circ \mathrm{N}_{H/K}$ and $L := F \circ L_\kappa$, then $L/\mathbb{Q}$ is normal.*

Since L_κ is K-trivial, L/K is dihedral and Proposition 3.3.1 is proved. As $k := K(\sqrt{p_i^*}, \sqrt{p_j^*})$ is abelian over $\mathbb{Q}$, by Proposition 3.3.5 there is an extension L' in the same class in $H^2(k/\mathbb{Q}, \pm 1)$ such that L' is unramified outside primes dividing D_K. Since these extensions $L'H$ form a basis for $\mathcal{G}^s_{H/K}$ over $\mathcal{A}^s_{H/K}$ we have shown:

Corollary 3.3.7. *Every class in $\mathcal{G}^s_{H/K}$ contains a representative unramified outside D_K.*

Corollary 3.3.8. *The map from $\mathcal{G}^s_{H/K}$ to $\mathrm{Alt}(H/K, \pm 1)$ sending L to ϵ_{L*} is surjective.*

3.3.1. Admissible Extensions of Ring Class Fields.

Let K be an imaginary quadratic field with $D_K < -4$, let $\mathcal{O}$ be a proper suborder of $\mathcal{O}_K$ and set $F := H_{\mathcal{O}}$, the ring class field of $\mathcal{O}$.

Let S be the set of odd primes dividing $D := D_{\mathcal{O}}$, the discriminant of $\mathcal{O}$, and let T be the subset of $\{-8, -4, 8\}$ such that

$$X_D = \{\eta_p : p \in S \cup T\},$$

where X_D is as defined in Definition 2.2.6. Let f be the positive integer such that $D = f^2 D_K$ and set $\mu := |X_D|$.

Lemma 3.3.9. *Let p be an odd prime. Then for some s in $\{-8, -4, 8\}$ there exists a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{p^*}, \sqrt{s})$ unramified outside $2p$.*

Proof. Clearly this depends only on the congruence class $m \equiv p \bmod 8$. By quadratic reciprocity we may take:

m	1	3	5	7
s	any	-8	-4	8

□

Proposition 3.3.10. *Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order of K and let S, T and μ be as above. Then setting $F := H_{\mathcal{O}}$, we have*

$$\dim_{\mathbb{F}_2} \mathcal{G}_{F/K}/\mathcal{A}_{F/K} = \binom{\mu - 1}{2}. \tag{3.18}$$

Proof. Let S_f be the set of odd prime divisors of f and set

$$N := D_K \prod_{p \in S_f} p^*.$$

Since the proof of Proposition 3.3.1 nowhere relies upon the fact that K is imaginary quadratic, it follows that for any pair of odd primes p_i, p_j dividing N that there is a dihedral extension of $\mathbb{Q}(\sqrt{N})$ which is normal over $\mathbb{Q}$ and contains $\mathbb{Q}(\sqrt{p_i^*}, \sqrt{p_j^*})$. We need to check when these extensions are dihedral over $K(\sqrt{N})$. If p_i and p_j both divide D_K then by Lemma 3.3.3 there exists such an extension over K so we may assume that p_i does not divide D_K. But then the extension becomes $C_2 \times C_2$ over $K(\sqrt{N})$ only if $N = p_i^* D_K$ or $N = p_i p_j D_K$.

If D_K and f are both odd, or if $|T| = 1$ then we are done. If not then by Lemma 3.3.9, for every odd prime p_i dividing $D_{\mathcal{O}}$ there exists some $s \in T$ such that there is a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{p_i^*}, \sqrt{s})$ which yields the result. □

Corollary 3.3.11. *With F and K defined as above the map from $\mathcal{G}^s_{F/K}$ to $\mathrm{Alt}(F/K, \pm 1)$ sending L to ϵ_{L*} is surjective.*

3.3.2. Abelian Extensions of K. Let K be a quadratic field, either real or imaginary. If K is real then we let H be the Hilbert class field of K in the 'strict' sense: that is H is the maximal abelian extension of K unramified outside the infinite places of K. The class group $Cl(K)$ of K is taken to be the class group of K corresponding to H. In either case if D_K is divisible by t distinct primes, the 2-rank of H/K is equal to $n := t - 1$ and the genus field of K is

$$F_g := \mathbb{Q}(\sqrt{p_1^*}, \dots \sqrt{p_t^*}), \text{ where } D_K = \prod_{i=1}^{t} p_i^*.$$

Definition 3.3.12. *Let G_K be the group of quadratic characters defined in* (2.15) *and define Γ_K to be the group of quadratic characters φ of $\mathfrak{I}_K$ such that*

a) *if $\mathfrak{p}$ is finite then either $\varphi_{\mathfrak{p}} = 1$ or $\varphi_{\mathfrak{p}} \in G_K$ and*
b) *$\varphi \circ \mathrm{N}_{H/K}$ is a Dirichlet character of $\mathfrak{I}_H$.*

The definition of G_K ensures that every element of Γ_K is ramified only at primes dividing D_K, and if K is real, possibly at infinite places of K. Let M be the compositum of the fields L in $\mathcal{A}^s_{H/K}$ which have Dirichlet characters of the form $\varphi \circ \mathrm{N}_{H/K}$ with $\varphi \in \Gamma_K$. Define $\mathcal{A} := \mathcal{A}_{F_g/\mathbb{Q},M}$ to be the group of quadratic extensions of F_g contained in M and $\mathcal{C} := \mathcal{C}_{F_g/K,M}$ to be the subgroup of fields L in $\mathcal{A}$ with the property that $\mathrm{Gal}(L/K) \cong C_2^{\times n+1}$.

The main advantage of working with extensions of F_g rather than H is that $F_g/\mathbb{Q}$ is abelian.

Lemma 3.3.13. *Let F_0 and k be abelian extensions of $\mathbb{Q}$ such that $F_0 \cap k = \mathbb{Q}$, and let $F := F_0 k$. Let H be the subgroup of $H^2(F/k, \pm 1)$ corresponding to quadratic extensions L/F such that $L := L_0 k$ where L_0 is a quadratic extension of F_0 which is normal over $\mathbb{Q}$. Then the map from H to $H^2(F_0/\mathbb{Q} \pm 1)$ sending*

$$\epsilon_L \mapsto \epsilon_{L_0}$$

is injective.

Proof. Let F, F_0 and k be as above and suppose that $L = L_0 k$ and $L' = L'_0 k$ are elements of $\mathcal{G}_{F/k}$ which represent different classes in $H^2(F/k, \pm 1)$. Then the Dirichlet characters of $\mathfrak{I}_F$ corresponding to the extensions L/F and L'/F are

$$\phi_L := \phi \circ \mathrm{N}_{F/F_0} \text{ and } \phi_{L'} := \phi' \circ \mathrm{N}_{F/F_0}$$

where ϕ and ϕ' are the quadratic Dirichlet characters of $\mathfrak{I}_{F_0}$ corresponding to L_0/F_0 and L'_0/F_0 respectively. Now if L_0 and L'_0 represent the same class in $H^2(F_0/\mathbb{Q}, \pm 1)$ then there exists a quadratic Dirichlet character η of $\mathfrak{I}_{\mathbb{Q}}$ such that $\phi'\phi^{-1} = \eta \circ \mathrm{N}_{F_0/\mathbb{Q}}$. But then

$$\begin{aligned} \phi_{L'} &= ((\eta \circ \mathrm{N}_{F_0/\mathbb{Q}})\phi) \circ \mathrm{N}_{F/F_0} \\ &= (\eta \circ \mathrm{N}_{F/\mathbb{Q}}) \cdot \phi_L, \end{aligned}$$

which implies that L and L' represent the same class in $H^2(F/k, \pm 1)$ which is a contradiction. □

Proposition 3.3.14 (Fröhlich [**11**] Corollary 1 to Theorem 11)**.** *Let F be as in Proposition 3.3.5 and suppose either that D_F is odd or else that F contains $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Let p be a prime dividing D_F, let L be an element of $\mathcal{G}_{F/\mathbb{Q}}$ of type ϵ and suppose that every prime dividing p is unramified in* *the extension L/F. Then p is unramified in L'/F for all extensions L' of type ϵ.*

Corollary 3.3.15. *The natural map from $\mathcal{A}$ to $H^2(F_g/\mathbb{Q}, \pm 1)$ sending L to ϵ_L is injective.*

Proof. Suppose that D_K is odd and that there exist L_1, L_2 in $\mathcal{A}$ such that $\epsilon_{L_1} = \epsilon_{L_2}$. By Proposition 3.3.14 the extension $L := L_1 \circ L_2$ must be unramified, since if L_1 and L_2 are ramified at all the same primes dividing D_K they must differ by some character of $Cl(K)$. But then L is contained in H and $L/\mathbb{Q}$ is abelian, hence L is contained in F_g and $L_1 = L_2$.

If D_K is even let k be a quadratic field such that $F := F_g k$ satisfies the condition of Proposition 3.3.14. Our choice of Γ_K means that there are no two elements L_1, L_2 of $\mathcal{A}$ such that $L_1 \circ L_2 = F$ hence the map from $\mathcal{A}$ to $H^2(F/\mathbb{Q}, \pm 1)$ defined by $L \mapsto \epsilon_{Lk}$ is injective. Moreover the map $\mathcal{A} \to H^2(F/k, \pm 1)$ is injective and by Lemma 3.3.13 $H^2(F/k, \pm 1)$ injects into $H^2(F_g/\mathbb{Q}, \pm 1)$. □

Lemma 3.3.16. *If K is imaginary, or if K is real and D_K is divisible by some prime $p \equiv 3 \bmod 4$ then every element of $\mathcal{C}$ except the identity is of type $\mathfrak{D}_2 \times C_2^{\times n-1}$.*

Proof. if D_K is negative or divisible by some prime $p \equiv 3 \bmod 4$, it cannot be the sum of two squares in $\mathbb{Q}$, therefore there are no extensions F of $\mathbb{Q}$ of type $C_2 \times C_4$ containing K such that $F/K \cong C_2^{\times 2}$. It follows that every element L of $\mathcal{C}$ is non-abelian over $\mathbb{Q}$.

Since L/K is abelian, the Galois group of $L/\mathbb{Q}$ must be isomorphic to one of $\mathfrak{D}_2 \times C_2^{\times n-1}$, $\mathfrak{Q}_2 \times C_2^{\times n-1}$ and $\mathfrak{B}_3 \times C_2^{\times n-2}$. In the latter two cases, $\mathrm{Gal}(L/K)$ would be isomorphic to $C_4 \times C_2^{\times n-1}$ which is a contradiction. □

We have reduced the problem of determining $c_4(H/K)$ when K is imaginary to one of counting dihedral extensions L of $\mathbb{Q}$ such that $L \cap F_g$ is a biquadratic field containing K and L/K is not cyclic.

Definition 3.3.17. *We say that a pair of integers (d_1, d_2) is a* decomposition *of D_K if d_1 and d_2 are discriminants such that $d_1 > 0$, $d_1 d_2 = D_K$ and*

$$\left(\frac{d_i}{p}\right) = 1, \text{ for all primes } p \text{ dividing } d_j,\ i, j \in \{1, 2\}, i \neq j. \qquad (3.19)$$

The requirement that d_1 and d_2 are discriminants such that $d_1 d_2 = D_K$ ensures that each d_i may be written as a product of prime discriminants

$$d_i = \prod_{j \in J_i} p_j^* \text{ where } D_K = \prod_{J_1 \cup J_2} p_j^*.$$

Two decompositions (a_1, a_2) and (b_1, b_2) are *independent* if there exists no integer m such that $b_1 \equiv a_1 m$ and $b_2 \equiv a_2 m$ modulo squares in $\mathbb{Z}$, and *dependent* otherwise.

Let (a_1, a_2) and (b_1, b_2) be distinct decompositions of D_K and for $i = 1, 2$ let d_i be the product of all the prime discriminants p^* dividing D_K such that p^* divides a_1 or b_i but not both. By construction d_1 and d_2 are discriminants with the property that $d_1 d_2 = D_K$. If a prime p dividing d_2 is coprime to $a_1 b_1$ then

$$\left(\frac{d_1}{p}\right) = \left(\frac{a_1 b_2}{p}\right) = 1,$$

and if p divides both a_1 and b_1, then

$$\left(\frac{a_1/p^*}{p}\right)\left(\frac{a_2}{p}\right) = \left(\frac{b_1/p^*}{p}\right)\left(\frac{b_2}{p}\right), \text{ so } \left(\frac{a_1/p^*}{p}\right) = \left(\frac{b_1/p^*}{p}\right),$$

and (3.19) holds for $i = 1$. The situation is just the same for primes dividing d_1, so (d_1, d_2) is a decomposition of D_K.

We call (d_1, d_2) the *product* of (a_1, a_2) and (b_1, b_2). Since any decomposition of D_K is uniquely defined by its first element, the product of (a_1, a_2) and (b_1, b_2) is equal to the product of (b_1, b_2) and (a_1, a_2). We have shown:

Proposition 3.3.18. *Suppose that D_K has r independent decompositions with $r \geq 1$. The set of decompositions of D_K generates a group with identity element $(1, D_K)$ congruent to $C_2^{\times r}$.*

Proposition 3.3.19. *The number of independent decompositions of D_K is equal to $r_4(H/K)$, the 4-rank of the class group of K.*

Proof. We outline the proof given in Rédei and Reichardt [**38**].
Suppose that there exists a cyclic extension F/K of degree 4 contained in H. Because H/K is unramified, $\mathrm{Gal}(H/\mathbb{Q})$ is the semidirect product of $\mathrm{Gal}(H/K)$ and $\mathrm{Gal}(K/\mathbb{Q})$ so the extension $F/\mathbb{Q}$ is dihedral. Let k be the biquadratic extension of $\mathbb{Q}$ contained in H. We may write $k = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ for some discriminants d_1, d_2 such that $D_K = d_1 d_2$. We claim that (d_1, d_2) satisfies (3.19): this is equivalent to the claim that for any prime $\mathfrak{p}$ of F dividing d_1 (resp. d_2), the field $\mathbb{Q}(\sqrt{d_2})$ (resp. $\mathbb{Q}(\sqrt{d_1})$) is contained in the decomposition field of $\mathfrak{p}$.

Conversely let (d_1, d_2) be a decomposition of D_K. By (3.19), we have

$$\left(\frac{d_1, d_2}{p}\right) = 1 \text{ for all primes } p \text{ dividing } D_K,$$

hence the conic $x^2 - d_1 y^2 - d_2 z^2 = 0$ has rational points $(x : y : z)$ with $y \neq 0$, any of which which define a dihedral extension $F/\mathbb{Q}$ containing

$k := \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and cyclic over K by

$$F := k(x + y\sqrt{d_1}).$$

It is shown on p. 72 of Rédei and Reichardt [**38**] that we may choose a point $(x : y : z)$ so that F/K is unramified and hence F is contained in H.

□

Lemma 3.3.20. *Let $\mathcal{A}$ be as defined on p. 58 and suppose that there exists a non-trivial discriminant d dividing D_K such that*

$$\left(\frac{D_K, d}{p}\right) = 1 \textit{ for all primes } p | D_K.$$

Then there exists an extension L in $\mathcal{A}$ such that L/K is of type $C_2^{\times n+1}$.

Proof. Suppose that such a discriminant d exists, and let $a := D_K/d$. There exists a dihedral extension $F/\mathbb{Q}$ unramified outside D_K containing $K(\sqrt{d})$ and cyclic of degree 4 over $\mathbb{Q}(\sqrt{a})$. Now $\mathrm{Gal}(F/K) \cong C_2^{\times 2}$, hence $\mathrm{Gal}(FF_g/K) \cong C_2^{\times n+1}$. Therefore FF_g is $\mathbb{Q}$-equivalent to some non-trivial extension L in $\mathcal{A}_{F_g/K}$. □

Corollary 3.3.21. *Suppose that $D_K = -4d$ for some odd integer d. Then there exists an extension L in $\mathcal{A}$ such that L/K is of type $C_2^{\times n+1}$.*

Proof. This follows immediately from Lemma 3.3.20 and the properties of the Hilbert symbol since

$$\begin{aligned} \left(\frac{D_K, d}{p}\right) &= \left(\frac{-4d, d}{p}\right) = \left(\frac{-d, d}{p}\right)\left(\frac{4, d}{p}\right) \\ &= \left(\frac{4, d}{p}\right) = \left(\frac{2, d}{p}\right)\left(\frac{2, d}{p}\right) = 1. \end{aligned}$$

□

Lemma 3.3.22 (Rédei [**39**] p. 56)**.** *Let S be the set of positive, squarefree integers d dividing D_K, such that the conic*

$$dx^2 - d'y^2 - z^2 = 0, \textit{ where } d' := D_K/d \tag{3.20}$$

has a rational solution. Let $r := r_4(H/K)$ be the 4-rank of $\mathrm{Gal}(H/K)$*. Then*

$$2^r = \frac{|S|}{2}.$$

Proposition 3.3.23. *Let K be an imaginary quadratic number field with discriminant D_K divisible by at least 2 distinct rational primes. If $D_K \equiv 4 \bmod 8$ and D_K is divisible by some prime $p \equiv 3 \bmod 4$ then*

$$n - r_4(H/K) - 1 \leq c_4(H/K) \leq n - \max\{1, r_4(H/K)\},$$

and otherwise

$$c_4(H/K) = n - r_4(H/K).$$

Proof. Let S be as in Lemma 3.3.22 and let d be an element of S. Let $\mathcal{C}$ be the group of extensions defined on p. 58. Multiplying both sides of (3.20) by $-d$ we have

$$-d^2x^2 + D_Ky^2 + dz^2 = 0,$$

hence (3.20) has a rational solution if and only if

$$D_Kx^2 + dy^2 - z^2 = 0 \tag{3.21}$$

does, and this holds if and only if $\left(\frac{D_K,d}{p}\right) = 1$ for all primes dividing D_K. Therefore if $\sqrt{d}$ is contained in H, Equation (3.21) corresponds to an element of $\mathcal{C}$, which is non-trivial if $d \neq 1$.

Suppose that D_K is odd. Then by the above discussion there is a bijection between $\mathcal{C}$ and the elements d of S such that $d \equiv 1 \bmod 4$ which is true for exactly $|S|/2$ different d because if $P = \prod p_i^*$ satisfies (3.20) then $|P|$ and $|D_K/P|$ will both belong to S and precisely one of these is congruent to 1 modulo 4.

Suppose that D_K is divisible by 8 and let $s = 2^*$ be the integer defined in (3.17). By the above argument we see that an odd element of S corresponds to an element of $\mathcal{C}$ if and only if it is congruent to $1 \bmod 4$. Suppose that d is an even element of S. Then if $s = 8$ ($s = -8$), d corresponds to an element of $\mathcal{C}$ if and only if $d/2 \equiv 1 \bmod 4$ ($d/2 \equiv 3 \bmod 4$) respectively, hence for any d in S precisely one of d and $|D_K/d|$ satisfy our condition.

Suppose that D_K is precisely divisible by 4. Then $\sqrt{-1}$ is in H so every odd element of S will correspond to an element of $\mathcal{C}$. By the multiplicity of the Hilbert symbol, either half or all of the elements of S must be odd, and the requirement $c_4 \leq n-1$ if D_K is divisible by some prime p congruent to $3 \bmod 4$ follows from Corollary 3.3.21 and the fact that by Corollary 2.2.18 there are 2^n quadratic Dirichlet characters of $\mathfrak{I}_K$ unramified outside D_K.

Finally, if D_K is divisible by n distinct primes p_i congruent to 1 mod 4 then by Corollary 1.7(C) of Vaughan [**63**] there exists a $C_2 \times C_4$ extension of $\mathbb{Q}$ containing $K(\sqrt{p_i})$ which is $C_2^{\times 2}$ over $\mathbb{Q}(\sqrt{p_i})$, so we must have $c_4(H/K) = n - r_4(H/K)$. □

Remark 3.3.24. If $D_K > 0$ then we cannot obtain such a bound in general, because with notation as in the proof of Proposition 3.3.23, if P satisfies (3.20) then either both or neither of $|P|$ and $|D_K/P|$ may be congruent to 1 modulo 4. However, for any given D_K this does give us a criterion for the existence of extensions in $\mathcal{C}$.

Example 3.3.25. Let K be an imaginary quadratic field with discriminant $D_K = -4d$ where d is odd and divisible by some prime congruent to 3 modulo 4. If $r_4(H/K) = 0$ then Proposition 3.3.23 tells us that $c_4(H/K) = n-1$. If $r_4(H/K) > 0$ then there are two possibilities, both of which occur:

D_K	$\mathrm{Gal}(H/K)$	$c_4(H/K)$
$-1045 = -4 \cdot 5 \cdot 11 \cdot 19$	$C_2^{\times 2} \times C_4$	1
$-1140 = -4 \cdot 3 \cdot 5 \cdot 19$	$C_2^{\times 2} \times C_4$	2

The characters λ in G_K^+ such that $\lambda \circ \mathrm{N}_{H/K}$ is the Dirichlet character of an extension L/H in $\mathcal{C}_{H/K}^s$ are:

D_K	λ
-1045	$\langle \lambda_{-4}\lambda_5,\ \lambda_{11}\lambda_{19} \rangle$
-1140	$\langle \lambda_{-4}\lambda_5\lambda_{11}\lambda_{19} \rangle$

The relationship between $r_4(H/K)$ and $c_4(H/K)$ has an interesting expression in terms of the rank of the Rédei matrix of K, which we describe briefly below. For more details and proofs, see Rédei [**39**].

Definition 3.3.26. *For* $1 \leq i, j \leq t$ *let*

$$a_{i,i} := \left(\frac{D_K/p_i^*}{p_i}\right) \text{ and}$$
$$a_{i,j} := \left(\frac{p_j^*}{p_i}\right),\ i \neq j.$$

and let $M_K := (m_{i,j})$ *be the matrix in* $\mathbb{M}_t(\mathbb{F}_2)$ *with entries satisfying*

$$a_{i,j} = (-1)^{m_{i,j}}.$$

We call M_K *the* Rédei matrix *of* K.

Quadratic reciprocity ensures that every row and column of M_K sums to zero (in $\mathbb{F}_2$). If d is a positive discriminant dividing D_K such that (3.20) has a rational solution then the sum of the row vectors

$$\sum_{i:p_i|d} (m_{i,j})_{1\leq j\leq t} = \vec{0}, \tag{3.22}$$

where $\vec{0}$ is the all-zero vector in $\mathbb{F}_2^t$, and conversely if d is a discriminant satisfying (3.22) then (3.20) has a rational solution. Moreover, if there exists a subset J of $\{1, \ldots, t\}$ such that the sum of the column vectors

$$\sum_{j\in J} (m_{i,j})_{1\leq i\leq t} = \vec{0}$$

then setting

$$d_1 = \prod_{j\in J} p_j^*,\ d_2 = D_K/d_1,$$

we see that (d_1, d_2) is a decomposition of D_K as defined in Definition 3.3.17, and conversely that every decomposition of D_K has this property. It follows that the rank of M_K is $t - 1 - r_4(H/K)$.

Gerth [**12**] described the distribution of $r_4(H/K)$ by counting the number of matrices in $\mathbb{M}_t(\mathbb{F}_2)$ which occur as Rédei matrices of quadratic fields, and estimating the number of fields K with D_K below a given bound which correspond to each matrix.

Definition 3.3.27. *Suppose that K is an imaginary quadratic field. Let t be the number of prime divisors of D_K and let $d_K = D_K$ if D is odd and $D_K/4$ otherwise. We define*

$$\begin{aligned} A_{t;B} &:= \{K : d_K \geq B\}, \\ A_{t,r;B} &:= \{K : K \in A_{t;B} \text{ and } r_4(K) = r\}, \\ a_{t,r} &:= \lim_{B\to\infty} \frac{|A_{t,r;B}|}{|A_{t;B}|}, \\ a_{\infty,r} &:= \lim_{t\to\infty} a_{t,r}. \end{aligned}$$

Let $\eta_k(s) := \prod_{j=1}^{k}(1 - s^{-j})$.

Theorem 3.3.28 (Gerth [**12**])**.** *The limits $a_{t,r}$ exist and in particular*

$$a_{\infty,r} = 2^{-r^2}\eta_\infty(2)\eta_r(2)^{-2}.$$

The sequence $\{a_{t,0}\}_{n\geq 1}$ is a monotonic sequence with limit $a_{\infty,0} > 0.288$, and for any $t > 0$,

$$a_{t,0} + a_{t,1} + a_{t,2} > 0.99.$$

If K is real quadratic, then with the corresponding definitions replacing a (resp. A) with b (resp. B) Gerth found similar results including that

$$\begin{aligned} &b_{\infty,r} = 2^{-r(r+1)}\eta_\infty(2)\eta_r(2)^{-1}\eta_{r+1}(2)^{-1}, \\ &b_{\infty,0} > 0.577 \end{aligned}$$

and for any $t > 0$

$$b_{t,0} + b_{t,1} + b_{t,2} > 0.997.$$

In [**9**] Fouvry and Klüners proved that the density of negative and positive fundamental discriminants D_K such that $r_4(H/K) = r$ are equal to $a_{\infty,r}$ and $b_{\infty,r}$ respectively.

CHAPTER 4

$\mathbb{Q}$-Curves with Complex Multiplication

In this chapter we apply the theory developed in the preceding chapters to CM elliptic curves with endomorphism algebra K, in particular to K and $\mathbb{Q}$-curves. In the first section we describe the Grössencharacters of K-curves of type 1 in terms of the quadratic characters of U_K defined in Section 2.2.3. Since every $\mathbb{Q}$-curve $E/H_{\mathcal{O}}$ is the quadratic twist of a $\mathbb{Q}$-curve of type 1 by a strictly admissible extension of $H_{\mathcal{O}}$, we may then apply the results of Section 3.3 to obtain a set Γ of $\mathbb{Q}$-curves with good reduction outside D_K and the property that if $A/H_{\mathcal{O}}$ is a $\mathbb{Q}$-curve then there exists an elliptic curve E in Γ such that $\chi_E\chi_A^{-1} = \kappa \circ \mathrm{N}_{H/\mathbb{Q}}$ for some quadratic Dirichlet character κ of $\mathfrak{I}_{\mathbb{Q}}$.

In Section 4.2 we outline some of the properties of the L-series attached to a Hecke character χ, with particular attention to the case where χ is the Grössencharacter of an elliptic curve E. The conjecture of Birch and Swinnerton-Dyer connects the Mordell-Weil rank of an elliptic curve E with the value of the L-series of E at $s = 1$. For a certain class of K-curves of type 1, which we introduce in Section 4.2.1, this conjecture is known to be true. Such curves are termed *canonical*.

Having described the Grössencharacters of some special classes of elliptic curves, it is natural to ask whether we can also find explicit models for them. The relationship between Grössencharacter and model has been studied by several people, notably Weil [**64**], Gross [**16, 17**], Rumely [**46, 47**] and Rubin and Silverberg [**45**] who have recently found models for canonical elliptic curves. In theory, one can always find a model for a curve with a given Grössencharacter by brute force: take any curve with CM by the desired order and twist until the L-series agree. In Section 4.3.1 we describe an interesting shortcut. Suppose that E/F is a CM elliptic curve which has at least one 3-torsion point $P = (x(P), y(P))$ with $x(P)$ defined over F. We shall see that the quadratic twist of E by $y(P)^2$ is a K-curve of type 1 with good reduction at all primes of F coprime to 3.

In Section 4.4 we prove that there exists a CM elliptic curve with good reduction everywhere over H if and only if the discriminant D_K of K is divisible by at least two primes congruent to 3 mod 4, and that in this case there exists a $\mathbb{Q}$-curve with this property.

4.1. $\mathbb{Q}$-Curves

Let $K/\mathbb{Q}$ be an imaginary quadratic field with discriminant D_K and let $\mathcal{O}$ be an order of K. We saw in Proposition 1.1.15 that the subgroup

$$N_{\mathcal{O}} := \mathrm{N}_{H_{\mathcal{O}}/K}(\mathfrak{I}_{H_{\mathcal{O}}}/H_{\mathcal{O}}^*)$$

of $\mathfrak{I}_K/K^*$ is $U_{\mathcal{O}}K_\infty^*K^*$.

Proposition 4.1.1 (Shimura [**55**] Proposition 8)**.** *If φ is a Hecke character of $\mathfrak{I}_K$ then $\varphi \circ \mathrm{N}_{H_{\mathcal{O}}/K}$ is the Grössencharacter of an elliptic curve $E/H_{\mathcal{O}}$ with CM by $\mathcal{O}$ if and only if*

a) $\varphi(u)^2 = 1$ *for all $u \in U_{\mathcal{O}}$ and*
b) $\varphi(y) = y^{-1}$ *for all $y \in K_\infty^*$,*

and the restriction of φ to $U_{\mathcal{O}}$ determines χ_E up to choice of infinite prime of $H_{\mathcal{O}}$.

From now on we suppose that a choice of infinite prime has been made. Note that this choice is equivalent to the choice of infinite prime defining f_∞ in Definition 2.3.4.

Let E be a K-curve of type 1, let $\chi_E := \varphi \circ \mathrm{N}_{H_{\mathcal{O}}/K}$ and let λ be the restriction of φ to $U_{\mathcal{O}}$. By Proposition 4.1.1, λ is an odd quadratic character of $U_{\mathcal{O}}$. Conversely, suppose that λ is an odd quadratic character of $U_{\mathcal{O}}$. We can extend λ to a homomorphism φ_λ from $N_{\mathcal{O}}$ to $\mathbb{C}^*$ by setting

$$\varphi_\lambda(K^*) = 1 \text{ and } \varphi_\lambda(x) = x^{-1} \text{ for all } x \in K_\infty^*.$$

Proposition 4.1.2. *We can extend φ_λ to a Hecke character φ of $\mathfrak{I}_K$, and $\chi := \varphi \circ \mathrm{N}_{H_{\mathcal{O}}/K}$ is the Grössencharacter of a K-curve of type 1 with CM by $\mathcal{O}$.*

Proof. This is a special case of Theorem 11 of Shimura [**55**]. □

By Proposition 4.1.1 the extension of φ_λ is unique up to choice of infinite prime of $H_{\mathcal{O}}$. For any idele $\boldsymbol{\alpha} = \boldsymbol{\alpha}(\mathfrak{a})$ where $\mathfrak{a} = (a)$ is a principal ideal coprime to $\mathfrak{f}_\lambda$,

$$\varphi(\boldsymbol{\alpha}) = \lambda(a)a. \tag{4.1}$$

Proposition 4.1.3 (Shimura [**55**] Proposition 9)**.** *The following are equivalent:*

a) $\chi_E(\boldsymbol{\alpha}^\rho) = \chi_E(\boldsymbol{\alpha})^\rho$ *for all $\boldsymbol{\alpha}$ in $\mathfrak{I}_{H_{\mathcal{O}}}$,*
b) $\varphi(\boldsymbol{\alpha}^\rho) = \varphi(\boldsymbol{\alpha})^\rho$ *for all $\boldsymbol{\alpha}$ in $N_{\mathcal{O}}$,*
c) $\lambda(\boldsymbol{\alpha}^\rho) = \lambda(\boldsymbol{\alpha})^\rho$ *for all $\boldsymbol{\alpha}$ in $U_{\mathcal{O}}$.*

Note that condition a) is precisely the condition for a K-curve of type 1 to be a $\mathbb{Q}$-curve. Condition c) is a necessary but not a sufficient condition for φ to be real on all of $\mathfrak{I}_K$. A description of when the latter occurs will be given in Proposition 4.2.11. In particular, condition c) ensures that if $\mathfrak{a}$ and $\boldsymbol{\alpha}$ are as in (4.1) then $\lambda(\boldsymbol{\alpha}^\rho) = \lambda(\boldsymbol{\alpha})^\rho$, but if $\mathfrak{a}$ is not principal then this need not hold. We shall see several examples of this in Section 5.3.

Let p be an odd rational prime dividing D_K and let $\mathfrak{p}$ be the prime of K dividing p. In Section 2.2.3, we defined a real quadratic character λ_p of U_K by

$$\lambda_p(x) := \left(\frac{\bar{x}}{p}\right) \tag{4.2}$$

where $\bar{x}$ denotes the image of x in $\overline{K}_\mathfrak{p}$. By Lemma 2.2.15 and Proposition 2.2.17, λ_p is odd if and only if $p \equiv 3 \bmod 4$ and there exists a real, odd character λ_{-8} of U_K ramified only over 2, if and only if $D_K = -8d$ for some integer $d \equiv 1 \bmod 4$.

Definition 4.1.4. *Let E and E' be elliptic curves defined over F with CM by an order $\mathcal{O}$ of K, and let k be a subfield of F. We say that E and E' are* k-equivalent *if there exists a Dirichlet character η of $\mathfrak{I}_k$ such that*

$$\chi_{E'}\chi_E^{-1} = \eta \circ \mathrm{N}_{F/k}.$$

As in Section 2.2.3 we let G_K be the group of quadratic characters of U_K generated by the characters λ_s where s runs through the set of integers appearing in a decomposition of D_K into a product of prime discriminants (see Proposition 2.2.2), and let G_K^- be the subset of odd characters in G_K. We recall that if s is either an odd prime or a prime discriminant divisible by 2 then

$$\kappa_s := \eta_s \circ \mathrm{N}_{K/\mathbb{Q}}.$$

We shall say that K is *exceptional* if D_K is divisible neither by 8 nor by any prime $p \equiv 3 \bmod 4$. By Corollary 2.2.18 if D_K is divisible by t distinct primes then

$$|G_K^-| = \begin{cases} 0 & \text{if } K \text{ is exceptional, and} \\ 2^{t-1} & \text{otherwise.} \end{cases}$$

Definition 4.1.5. *Let $\Gamma_1(K)$ denote the set of Hecke characters χ of $\mathfrak{I}_H$ such that χ is a Grössencharacter of a K-curve of type 1 with CM by $\mathcal{O}_K$ and*

$$\chi = \varphi \circ \mathrm{N}_{H/K}, \textit{ and } \varphi|_{U_K} = \lambda,$$

for some element λ of G_K^-.

Proposition 4.1.6. *Every $\mathbb{Q}$-curve E/H of type 1 with CM by $\mathcal{O}_K$ is $\mathbb{Q}$-equivalent to an elliptic curve with CM by $\mathcal{O}_K$ and Grössencharacter in $\Gamma_1(K)$. Conversely, if E/H and E'/H are elliptic curves with CM by $\mathcal{O}_K$ and Grössencharacters in $\Gamma_1(K)$ then E is $\mathbb{Q}$-equivalent to E' if and only if χ and χ' correspond to the same element of G_K^-.*

Proof. Let E be a $\mathbb{Q}$-curve of type 1, let μ be the real, odd quadratic character of U_K which determines χ_E and let $N := \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_\mu)$. Define T_0 to be the set of primes dividing N which are coprime to D_K and T_1 to be the set of primes dividing both N and D_K. Then $\mu = \mu_0\mu_1$ where

$$\mu_0 = \prod_{\mathfrak{p}\in T_0} \mu_{\mathfrak{p}} \text{ and } \mu_1 = \prod_{\mathfrak{p}\in T_1} \mu_{\mathfrak{p}}.$$

By Corollary 2.2.10 and Lemmas 2.2.12 and 2.2.14, μ_0 is a real even character of the form $\nu \circ \mathrm{N}_{K/\mathbb{Q}}$ for some quadratic character ν of $\mathfrak{I}_{\mathbb{Q}}$. But then μ_1 is a real odd quadratic character of U_K. Moreover, by Corollary 2.2.10 if every prime in T_1 divides an odd rational prime then $\mu_1 = \prod_{\mathfrak{p}\in T_1} \lambda_{\mathfrak{p}}$ and hence determines some element χ of $\Gamma_1(K)$.

If T_1 contains a prime $\mathfrak{p}$ of K dividing 2 then either $\mu_{\mathfrak{p}} = \lambda_{\mathfrak{p}}$ or $\mu_{\mathfrak{p}} = \kappa_s \cdot \lambda_{\mathfrak{p}}$ where $s \in \{-8, -4, 8\}$ is as determined in Lemma 2.2.15. Therefore either μ_1 or $\kappa_s^{-1}\mu_1$ determine some element χ of $\Gamma_1(K)$ and χ and χ_E are $\mathbb{Q}$-equivalent.

To prove the converse, notice that $\chi_{E'}\chi_E^{-1} = \phi \circ \mathrm{N}_{H/K}$ where ϕ is a Dirichlet character of $\mathfrak{I}_K$ and $\phi|_{U_K}$ is an element of G_K^+. Now by construction, (see Section 2.2.3), no λ_s with s dividing D_K has the form $\eta_s \circ \mathrm{N}_{K/\mathbb{Q}}$ where κ is a character of $U_{\mathbb{Q}}$, hence if E and E' are $\mathbb{Q}$-equivalent then ϕ must be the trivial character on $\mathfrak{I}_K$. □

We saw in the proof of the last proposition that $\Gamma_1(K)$ corresponds to either all or half of the set of Grössencharacters of $\mathbb{Q}$-curves of type 1 with good reduction outside primes dividing D_K according to whether D_K is odd or even.

We next consider $\mathbb{Q}$-curves of type 2. With our usual assumption that $D_K < -4$, if E/H is a $\mathbb{Q}$-curve of type 2 then there exists a quadratic extension L/H such that $L/\mathbb{Q}$ is normal and E^L is a $\mathbb{Q}$-curve of type 1. This allows us to use results from Chapter 3 to classify $\mathbb{Q}$-equivalence classes of $\mathbb{Q}$-curves of type 2 in a similar manner to those of type 1. Let $\mathcal{L} := \{L_1, \ldots, L_m\}$ be a minimal set of elements of $\mathcal{G}^s_{H/K}$ such that

$$\mathcal{G}^s_{H/K} = \langle \mathcal{A}^s_{H/K}, \mathcal{L}\rangle.$$

Recall that $m = \binom{n}{2}$ by (3.16) and that by Lemma 3.3.3 and Corollary 3.3.7 we may suppose for $1 \le i \le m$ that $L_i = F_iH$ where F_i/K is a dihedral extension of order 8, unramified outside D_K.

Definition 4.1.7. *Let $\mathcal{L}$ and m be as above and for $1 \le i \le m$ let ϕ_i be the Dirichlet character associated with the extension L_i/H. For any non-empty subset J of $1, \ldots, m$ let $\phi_J := \prod_{j\in J} \phi_j$. We define $\Gamma_2(K)$ to be the set of Hecke characters of the form $\phi_J\chi_1$ with $\chi_1 \in \Gamma_1$.*

Proposition 4.1.8. *Every $\mathbb{Q}$-curve E/H of type 2 with CM by $\mathcal{O}_K$ is $\mathbb{Q}$-equivalent to an elliptic curve with Grössencharacter $\chi_E = \phi_L \chi_1$ where χ_1 is in $\Gamma_1(K)$ and ϕ_L is the Dirichlet character of a quadratic extension L/H which is normal over $\mathbb{Q}$ and unramified outside primes dividing D_K.*

Proof. Let χ_1 be any element of Γ_1 and let $\phi := \chi_E \chi_1^{-1}$. Both χ and χ_E are fixed by $\mathrm{Gal}(H/\mathbb{Q})$ so by Lemma 2.3.5, ϕ is the Dirichlet character associated with a quadratic extension of L'/H which is normal over $\mathbb{Q}$. By Corollary 3.3.7, there exists a field L/H unramified outside primes dividing D_K such that $\phi = (\nu \circ \mathrm{N}_{H/\mathbb{Q}})\phi_L$ for some Dirichlet character ν of $\mathfrak{I}_{\mathbb{Q}}$. Therefore χ_E is $\mathbb{Q}$-equivalent to $\phi_L \chi_1$ as claimed. □

Corollary 4.1.9. *Every $\mathbb{Q}$-curve E/H of type 2 is $\mathbb{Q}$-equivalent to an elliptic curve with Grössencharacter in Γ_2.*

Remark 4.1.10. The content of Propositions 4.1.6 and 4.1.8 is essentially that of Theorem 2 of Nakamura [**34**].

4.1.1. $\mathbb{Q}$-Curves with CM by Non-Maximal Orders.

We now consider $\mathbb{Q}$-curves with CM by a non-maximal order $\mathcal{O}$ of K. Let f be the conductor of $\mathcal{O}$, $D_{\mathcal{O}} := f^2 D_K$ its discriminant and $H_{\mathcal{O}}$ its ring class field.

Proposition 4.1.11. *Let E be a $\mathbb{Q}$-curve with complex multiplication by $\mathcal{O}$ defined over $H_{\mathcal{O}}$. Then there exists an elliptic curve E_m with CM by $\mathcal{O}_K$ such that E and E_m are isogenous over $H_{\mathcal{O}}$. Moreover, if E is a $\mathbb{Q}$-curve of type 1 over $H_{\mathcal{O}}$ then E_m is a K-curve of type 1 over H.*

Proof. Suppose that $E/H_{\mathcal{O}}$ is a $\mathbb{Q}$-curve of type 1, so that $\chi_E = \varphi \circ \mathrm{N}_{H_{\mathcal{O}}/K}$ for some Hecke character φ of $\mathfrak{I}_K$. Then by Proposition 4.1.1, φ is determined up to choice of infinite place of $H_{\mathcal{O}}$ by a real odd quadratic character of $U_{\mathcal{O}}$. But since H is contained in $H_{\mathcal{O}}$, $U_{\mathcal{O}}$ is contained in U_K and $\varphi \circ \mathrm{N}_{H/K}$ is the Grössencharacter of a K-curve with CM by $\mathcal{O}_K$ over H.

If $E/H_{\mathcal{O}}$ is type 2, then it is the quadratic twist of a type 1 curve E_0 by some quadratic extension $L/H_{\mathcal{O}}$. If A/H is the curve with complex multiplication by $\mathcal{O}_K$ which becomes isogenous to E_0 over $H_{\mathcal{O}}$ then clearly $E_m := A^L_{H_{\mathcal{O}}}$ is isogenous to E over $H_{\mathcal{O}}$ and since it has CM by $\mathcal{O}_K$ it has a model defined over H. □

Remark 4.1.12. By Proposition 4.1.3, E_m will be a $\mathbb{Q}$-curve if and only if φ is real on $N_{\mathcal{O}_K}$. This will not be true, for example, if E has bad reduction at any odd prime p which divides f but is coprime to D_K.

Corollary 4.1.13. *Suppose that E and E' are $\mathbb{Q}$-curves with CM by $\mathcal{O}$ defined over $H_{\mathcal{O}}$ and that E and E' are not isogenous over $H_{\mathcal{O}}$. Let L be the quadratic extension of $H_{\mathcal{O}}$ such that E and E' are L-isogenous. Then L is an absolutely normal field and there exists a quadratic extension L_m/H*

such that $L = L_m H_{\mathcal{O}}$. Moreover if E and E' are of type 1, then L/K and L_m/K are abelian.

Proof. Recall that the Hecke character ϕ_L associated with the extension $L/H_{\mathcal{O}}$ satisfies

$$\phi_L = \chi_{E'}\chi_E^{-1}.$$

Since E and E' are $\mathbb{Q}$-curves, χ_E and $\chi_{E'}$ are fixed by $\mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q})$, so $L/\mathbb{Q}$ is normal. The existence of L_m follows from Proposition 4.1.11. If E and E' are of type 1 then there exist Hecke characters φ and φ' of $\mathfrak{I}_K$ such that $\chi_E = \varphi \circ \mathrm{N}_{H_{\mathcal{O}}/K}$ and $\chi_{E'} = \varphi' \circ \mathrm{N}_{H_{\mathcal{O}}/K}$. Therefore L/K is abelian, and since $L = L_m H_{\mathcal{O}}$ it follows that L_m/K is also abelian. □

Proposition 4.1.14. *Let $\mathcal{O}$ be an order of K with discriminant D and let μ be the integer defined in Definition 2.2.6. Then if D is divisible by 8 or by some prime $p \equiv 3 \bmod 4$ there are $2^{\mu-1}$ distinct $\mathbb{Q}$-equivalence classes of $\mathbb{Q}$-curves of type 1 with CM by $\mathcal{O}$ defined over $H_{\mathcal{O}}$ and none otherwise.*

Proof. The only possibility which is not in direct analogy with the case when $\mathcal{O}$ is maximal is if $D_{\mathcal{O}}$ is divisible by 32. Suppose that this is so and let $\mathfrak{p}$ be the prime of $\mathcal{O}$ dividing 2. If D_K is even set $s := 2^*$ and let ν be the character defined in Lemma 2.2.15. Since $H_{\mathcal{O}}$ contains $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$ the character κ_s is trivial on $U_{\mathfrak{p}}$ for all s in $\{-8, -4, 8\}$, so the restriction of ν to $U_{\mathfrak{p}}$ is real, and the character group of $U_{\mathfrak{p}}$ is generated by ν and λ_s, precisely one of which is odd.

If D_K is odd then we achieve the same result by considering first the suborder $\mathcal{O}'$ of $\mathcal{O}_K$ of conductor $f/4$ and then treating $\mathcal{O}$ as a suborder of $\mathcal{O}'$ in the same manner as above. □

Extending our previous definition, we say that $\mathcal{O}$ is *exceptional* if $D_{\mathcal{O}}$ is divisible neither by 8 nor by any prime congruent to 3 mod 4.

Lemma 4.1.15 (Nakamura [**34**] Proposition 5)**.** *If $\mathcal{O}$ is exceptional, then there are no $\mathbb{Q}$-curves defined over $H_{\mathcal{O}}$ with CM by $\mathcal{O}$.*

Proof. By Proposition 4.1.14 there are no such curves of K-type 1. Suppose there exists a $\mathbb{Q}$-curve $E/H_{\mathcal{O}}$ of K-type 2 with Grössencharacter χ. Let E_0 be a K-curve of type 1 with Grössencharacter χ_0. Set $\phi := \chi_0\chi^{-1}$ and let L be the quadratic extension of $H_{\mathcal{O}}$ associated with ϕ. By Corollary 3.3.11 there exists an extension $L'/H_{\mathcal{O}}$ such that $L'/\mathbb{Q}$ is normal and $\epsilon_{L*} = \epsilon_{L'*}$ so the field $L'' := L \circ L'$ is an abelian extension of K. But then the curve $E_1 := E_0^{L''}$ is a $\mathbb{Q}$-curve of K-type 1 which is a contradiction. □

Example 4.1.16. Suppose that K is exceptional, and let ϕ_K be a real, even character of $\mathfrak{I}_K$. Then there exists a type 1 curve E defined over H with CM by $\mathcal{O}_K$ such that

$$\chi_E = \nu \cdot \phi_K \circ \mathrm{N}_{H/K},$$

where ν is the character defined in Lemma 2.2.15, and E and E^ρ become isogenous over the extension of H corresponding to the character $\kappa_8 \circ \mathrm{N}_{H/K}$. This is the ring class field of K of conductor 2.

4.2. The L-series and the Functional Equation

In this section we outline some of the properties of the L-series of Hecke characters. Proofs and details of the material covered may be found in Chapter 7 of Weil [**66**] and the same chapter of Lang [**25**].

Throughout this section we let χ be a Hecke character of $\mathfrak{I}_F$ with minimal exceptional set S. We recall from Definition 2.1.3 that the Hecke L-series of χ is defined as

$$L_F(\chi, s) := \prod_{\mathfrak{p} \notin S} \left(1 - \frac{\chi(\mathfrak{p})}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})^s}\right)^{-1}. \tag{4.3}$$

If χ is a Dirichlet character then $L_F(\chi, s)$ converges for $\Re(s) > 1$.

Theorem 4.2.1 (Hecke [**21**]). *The Hecke L-series of χ has an analytic continuation to the whole complex plane.*

The first proof of this theorem in idelic language was given in Tate's thesis, reprinted in [**62**].

Definition 4.2.2. *Let $\mathfrak{p}$ be a place of F. For any x in $F_\mathfrak{p}$ we define*

$$\begin{aligned} |x|_\mathfrak{p} &:= N_\mathfrak{p}^{-v(x)} && \textit{if } \mathfrak{p} \textit{ is finite,} \\ |x|_\mathfrak{p} &:= |x|, && \textit{if } F_\mathfrak{p} = \mathbb{R}, \\ |x|_\mathfrak{p} &:= |x|^2, && \textit{if } F_\mathfrak{p} = \mathbb{C}, \end{aligned}$$

where if $\mathfrak{p}$ is finite v is the additive valuation on $F_\mathfrak{p}$ and $N_\mathfrak{p}$ is the cardinality of the residue class field $\overline{F}_\mathfrak{p}$.

Definition 4.2.3. *The* idele volume $\|\boldsymbol{\alpha}\|_F$ *of an idele $\boldsymbol{\alpha}$ of F is*

$$\|\boldsymbol{\alpha}\|_F := \prod_\mathfrak{p} |\alpha_\mathfrak{p}|_\mathfrak{p}.$$

Definition 4.2.4. *For any complex number t we define ω_t to be the Hecke character of $\mathfrak{I}_F$ given by*

$$\omega_t(\boldsymbol{\alpha}) := \|\boldsymbol{\alpha}\|_F^t. \tag{4.4}$$

Let χ be a Hecke character of $\mathfrak{I}_F$. We define χ_{un} to be the ordinary Hecke character with conductor $\mathfrak{f}_\chi$ given by

$$\chi_{un}(\boldsymbol{\alpha}) := \frac{\chi(\boldsymbol{\alpha})}{|\chi(\boldsymbol{\alpha})|} \text{for all } \boldsymbol{\alpha} \in \mathfrak{I}_F.$$

Lemma 4.2.5 (Weil [**66**] p. 118)**.** *For any Hecke character χ of $\mathfrak{I}_F$ there exists a unique element t of $\mathbb{C}$ such that*

$$\chi = \chi_{un}\omega_t.$$

Lemma 4.2.6 (Lang [**25**] p. 94)**.** *Let ψ be an ordinary Hecke character of $\mathfrak{I}_F$ and let $\mathfrak{p}$ be an infinite place of F. For any idele $\boldsymbol{\alpha}$ in $\mathfrak{I}_F$ the local component of ψ is given by*

$$\psi_{\mathfrak{p}}(\boldsymbol{\alpha}) := \alpha_{\mathfrak{p}}^{a}|\alpha_{\mathfrak{p}}|^{ib-a}$$

for some integer a and real number b.

If ψ has discrete infinite components then if $\mathfrak{p}$ is complex then $a = b = 0$ and if $\mathfrak{p}$ is real then $b = 0$ and a is either 0 or 1.

With definitions as in Lemma 4.2.6, set $n_{\mathfrak{p}} := 1$ if $\mathfrak{p}$ is real and $n_{\mathfrak{p}} := 2$ otherwise, and define

$$u(\psi, \mathfrak{p}, s) := \frac{n_{\mathfrak{p}}s + ib + |a|}{2}. \tag{4.5}$$

For any Hecke character χ of $\mathfrak{I}_F$ we define

$$d_{\chi} := \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_{\chi}) \cdot |D_{F/\mathbb{Q}}|. \tag{4.6}$$

Let ψ be an ordinary Hecke character. Setting $u := u(\psi, \mathfrak{p}, s)$, r_1 to be the number of real places in S_0 and $n := [F : \mathbb{Q}]$ we define

$$\Lambda(\psi, s) := (2^{r_1}(2\pi)^{-n}d_{\psi})^{s/2}\left(\prod_{\mathfrak{p}\in S_0}\Gamma(u)\right)L_F(\chi, s), \tag{4.7}$$

where

$$\Gamma(s) = \int_0^{\infty} e^{-u}u^{s-1}du.$$

Proposition 4.2.7 (Weil [**66**] pp. 133–134)**.** *For any Hecke character χ of $\mathfrak{I}_F$,*

$$L_F(\chi, s) = L_F(\chi_{un}, s + t).$$

Proposition 4.2.8. *If ψ is an ordinary Hecke character of $\mathfrak{I}_F$ then $\Lambda(\psi, s)$ satisfies a functional equation*

$$\Lambda(\psi, s) = W(\psi)\Lambda(\overline{\psi}, 1 - s). \tag{4.8}$$

where $W(\psi)$ is a complex number of absolute value 1.

Proof. For proof, and the definition of $W(\psi)$, see Lang [**25**] p. 114. □

For general Hecke characters one may obtain a functional equation of a similar form by applying Proposition 4.2.7. In the following example we let K be an imaginary quadratic field, take χ to be a Hecke character of $\mathfrak{I}_K$ such that $\chi_E := \chi \circ \mathrm{N}_{H/K}$ is the Grössencharacter of an elliptic curve, and derive the functional equation of $L(\chi, s)$ in the form commonly found in the literature.

Example 4.2.9. Let K be an imaginary quadratic field with Hilbert class field H and suppose that E/H is a CM elliptic curve such that

$$\chi_E := \chi \circ \mathrm{N}_{H/K}.$$

By Proposition 4.1.1, if $\mathfrak{p} = (a)$ is a principal prime ideal coprime to the conductor of E then $\chi(\boldsymbol{\alpha}(\mathfrak{p})) = \pm a$, and if $x \in K_\infty^*$ then $\chi(x) = x^{-1}$. Now, with the natural embedding of K in $\mathbb{C}$

$$\omega_1(\boldsymbol{\alpha}(\mathfrak{p})) = \mathrm{N}_{K/\mathbb{Q}}(a)^{-1} = |a|^{-2} = |\chi(\boldsymbol{\alpha}(\mathfrak{p}))|^{-2}$$

and similarly, letting ∞ denote the infinite place of K,

$$\omega_1(x) = |x_\infty|^2.$$

Therefore $\chi = \chi_{un}\omega_{-1/2}$. The infinite component of χ_{un} maps an idele $\boldsymbol{\alpha}$ to $\alpha_\infty/|\alpha_\infty|$ so $u(\chi_{un}, \infty, s) = s + 1/2$ and by (4.7),

$$\Lambda(\chi_{un}, s) = (2\pi)^{-s} d_\chi^{s/2} \Gamma(s + 1/2) L_H(\chi_{un}, s).$$

It follows from Proposition 4.2.7 that $L_H(\chi_{un}, s - 1/2) = L_H(\chi, s)$ and $L_H(\chi_{un}, 3/2 - s) = L_H(\chi, 2 - s)$, hence if we define

$$\Lambda(\chi, s) := (2\pi)^{-s} d_\chi^{s/2} \Gamma(s) L_H(\chi, s),$$

and set $W(\chi) := W(\chi_{un})$ then $\Lambda(\chi, s)$ satisfies the functional equation

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 2 - s).$$

For the elliptic curve E in the above example, it is clear that $L(E/H, s)$ satisfies a functional equation with symmetry between s and $2 - s$. Indeed, applying Theorem 2.3.18 we find:

Proposition 4.2.10. *Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order of K and let F be a field containing $H_\mathcal{O}$. For an elliptic curve E/F with CM by $\mathcal{O}$ and Grössencharacter $\chi := \chi_E$ let $n := [F : \mathbb{Q}]$ and define*

$$\Lambda(E/F, s) := ((2\pi)^{-n} d_\chi)^s \Gamma(s)^n L(E/F, s).$$

Then

$$\Lambda(E/F, s) = \Lambda(E/F, 2 - s).$$

For the case where F does not contain K, see Silverman [**59**] p. 176.

It is conjectured that the L-series of any abelian variety has similar properties of analytic continuation and functional equation.

4.2.1. Canonical Hecke Characters. Let k be a CM field with maximal real subfield k_0, and let ρ be a generator of $\mathrm{Gal}(k/k_0)$. Recall that a Hecke character χ of k is *real* if $\chi(\boldsymbol{\alpha})^\rho = \chi(\boldsymbol{\alpha}^\rho)$ for all ideles $\boldsymbol{\alpha}$ of k. In Section 4.1 we constructed Hecke characters χ of $\mathfrak{I}_K$ by extension of real quadratic characters λ of U_K. In this section, following Rohrlich [**41**], we investigate when χ itself is real.

Let E/F be an elliptic curve and let r_M be the Mordell-Weil rank of E/F. Birch and Swinnerton-Dyer famously conjectured that $L(E/F, s)$ has a zero of order r_M at $s = 1$. It has been proved (see Rubin [**44**]), that if E is a K-curve of type 1 with CM and F is an abelian extension of K then if $E(F)$ is infinite $L(E/F, 1) = 0$.

If E/H is a $\mathbb{Q}$-curve of type 1 with CM by $\mathcal{O}_K$ and Grössencharacter $\chi_E := \chi \circ \mathrm{N}_{H/K}$ such that χ is real then by Lemma 6.2 of Miller and Yang [**28**] the order of the zero at $s = 1$ agrees with the conjecture of Birch and Swinnerton-Dyer. The functional equation of $\Lambda(\chi, s)$ has a particularly simple form in this case as $W(\chi)$ is ± 1, and it is known that the Mordell-Weil rank of E is 0 if $W(\chi) = 1$ and $2h_K$ if $W(\chi) = -1$. If χ is unramified outside primes dividing D_K then Proposition 4.2.14 describes when each of these cases occurs.

Proposition 4.2.11 (Rohrlich [**41**] Proposition 1)**.** *Let k be a CM field with maximal real subfield k_0. Let χ be a Hecke character of k and let κ be the character associated with the extension k/k_0. Then χ is real if and only if the restriction of χ_{un} to the idele group of k_0 is equal to κ.*

If in addition χ is unramified outside primes dividing D_{k/k_0} then χ is termed a *canonical* character. An elliptic curve E is *canonical* if $\chi_E = \chi \circ \mathrm{N}_{H_K/K}$ for some canonical character χ of $\mathfrak{I}_K$. We note that the condition on the discriminant means that it is sufficient to consider curves with CM by the maximal order.

Proposition 4.2.12 (Rohrlich [**41**] Propositions 3, 4, 5)**.** *Let K be an imaginary quadratic field, and let n_K denote the number of ordinary canonical characters of $\mathfrak{I}_K$. Then*

$$n_K = \begin{cases} 0 & \text{if } D_K \equiv 4 \bmod 8, \\ 1 & \text{if } D_K \text{ is odd,} \\ 2 & \text{if } D_K \equiv 0 \bmod 8. \end{cases}$$

Proof. For any odd prime p, the character λ_p is the unique extension of η_p from $\mathfrak{I}_{\mathbb{Q}}$ to $\mathfrak{I}_K$, which gives us the result if D_K is odd. There is no continuous extension of η_{-4} to $\mathfrak{I}_K$, since λ_{-4} is even, and κ_{-8} is trivial on $\mathfrak{I}_{\mathbb{Q}}$. Finally, there are two extensions of η_s to $\mathfrak{I}_K$ for s in $\{\pm 8\}$ since λ_{-8} and $\kappa_8\lambda_{-8}$ extend η_{-8} and λ_8 and $\kappa_{-4}\lambda_8$ extend η_8. □

Remark 4.2.13. Propositions 3–5 of Rohrlich [**41**] prove an equivalent result to Proposition 4.2.12 for a considerably more general class of CM fields. Suppose that k is a CM field of degree $2g$ over $\mathbb{Q}$ with maximal real subfield k_0 such that all units of k are real, and if an ideal $\mathfrak{a}$ of k_0 is principal in k then it is principal in k_0. Then if k/k_0 is unramified over 2, $n_k = 1$ and otherwise n_k is either 0, 2^g or 2^{g+1} depending upon the local structure of k/k_0.

We say that a $\mathbb{Q}$-curve E/H is *canonical* if its Grössencharacter has the form $\chi_E := \chi \circ \mathrm{N}_{H/K}$ where χ is a canonical Hecke character of $\mathfrak{I}_K$.

If D_K is divisible by 8, then any two elliptic curves corresponding to distinct canonical Hecke characters on $\mathfrak{I}_K$ are $\mathbb{Q}$-equivalent, so there is one canonical elliptic curve with Grössencharacter in $\Gamma_1(K)$ if D_K is odd or divisible by 8 and otherwise there are none.

Proposition 4.2.14 (Montgomery and Rohrlich [**30**]). *Suppose that K is an imaginary quadratic field with discriminant D_K which is odd or divisible by 8, let χ be a canonical character of $\mathfrak{I}_K$ and let λ be the restriction of χ_{un} to U_K. Then*

$$W(\chi) = \begin{cases} \left(\frac{2}{-D_K}\right) & \textit{if } D_K \textit{ is odd}, \\ \lambda(1+\sqrt{d_K}) & \textit{if } D_K = 4d_K,\ d_K \in \mathbb{Z}. \end{cases}$$

Example 4.2.15. This example is due to Gross [**16**]. Let $D_K = -p$ where $p \equiv 3 \bmod 4$ is an odd prime, and let E/H be the elliptic curve with Grössencharacter $\chi \circ \mathrm{N}_{H/K}$ where χ is determined by λ_p. Then χ is real and $W(\chi) = 1$ if and only if $p \equiv 7$ mod 8.

Example 4.2.16. We look at the Mordell-Weil groups of the $\mathbb{Q}$-curves over H_K with Grössencharacters in $\Gamma_1(K)$ for $D_K = -15$ and -35. The canonical character χ of $\mathfrak{I}_K$ has $W(\chi) = 1$ in the first case and -1 in the second.

D_K	λ	$E(H)$
-15	λ_3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
	$\lambda_3\lambda_5$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-35	λ_7	0
	$\lambda_5\lambda_7$	$\mathbb{Z}^4$

There are two primes $\mathfrak{p}$, $\mathfrak{p}^\rho$ dividing 3 in $K := \mathbb{Q}(\sqrt{-35})$ and the Mordell-Weil group of the K-curve corresponding to $\lambda_{\mathfrak{p}}$ is $\mathbb{Z}/3\mathbb{Z}$.

Remark 4.2.17. The Hecke character χ is the Grössencharacter of an abelian variety A/K of dimension h_K. We shall see in Chapter 5 that A is the Weil restriction from H to K of E, with E defined as above, and shall also see that $\mathrm{End}^0_{\mathbb{Q}}(A)$ is real.

4.3. Models of $\mathbb{Q}$-Curves

In Chapter 2 we saw that knowledge of the Grössencharacter of an abelian variety of CM type tells us a great deal about the arithmetic properties of the variety, hence, given a variety A of CM type it is natural to attempt to determine its Grössencharacter. Conversely, given a CM type (K, Φ) with reflex (K', Φ') and a Hecke character χ satisfying Theorem 2.3.9 for some lattice Λ of K and finite extension F/K', one may wish to find an explicit description of an abelian variety A/F with Grössencharacter χ.

The first question has been studied by Weil [**64**] for families of elliptic curves with models of the form

$$y^2 = ax^n + b,\ 3 \leq n \leq 4 \text{ and } a, b \in \mathbb{Z},$$

and more generally by Rumely [**47, 46**] for abelian varieties with complex multiplication belonging to families of abelian varieties parametrized by arithmetic theta-functions. To give a flavour of these results we describe an example of a special case corresponding to a family of elliptic curves, known as *Hesse curves*, drawn from Rumely [**47**] pp. 394–395. Let $\mathfrak{H}$ be the complex upper half-plane, and let $K := \mathbb{Q}(\tau)$ for some CM point τ in $\mathfrak{H}$. Let $j := j(\tau)$ be the j-invariant of a curve with complex multiplication by $\mathcal{O}_K$ and let $\mu := \mu(\tau)$ satisfy

$$j = \frac{27\mu^3(\mu^3+2)^3}{(\mu^3-1)^3}.$$

The elliptic curve E with model given by

$$x^3 + y^3 + 1 = 3\mu xy$$

is defined over $F := K(\mu)$ and has CM by $\mathcal{O}_K$. We can express any element a of K uniquely in the form $a = a_1 + a_2\tau$ with a_1 and $a_2 \in \mathbb{Q}$. In particular, suppose that $\tau^2 = t_1 + t_2\tau$. We define f_τ to be the embedding $K \hookrightarrow \mathbb{M}_2(\mathbb{Q})$ given by

$$f_\tau(a) = \left(\begin{array}{cc} a_1 + a_2t_2 & a_2t_1 \\ a_2 & a_1 \end{array} \right).$$

This embedding has the property that

$$f_\tau(a)\begin{pmatrix}\tau\\1\end{pmatrix} = \begin{pmatrix}a\tau\\a\end{pmatrix}.$$

We denote by the same symbol the extension of f_τ to an embedding of $\mathfrak{I}_K$ into $G_A := \mathrm{GL}_2(\mathfrak{A})_+$ where $\mathfrak{A}$ is the adele group of $\mathbb{Q}$ and the subscript indicates that the infinite part of any matrix in G_A has positive determinant. Let $\mathrm{GL}_2(\mathbb{R})_+$ be the subgroup of matrices in $\mathrm{GL}_2(\mathbb{R})$ with positive determinant and define

$$G := \mathrm{GL}_2(\mathbb{R})_+ \times \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

For an element g of G let g_p denote the component of g in $\mathrm{GL}_2(\mathbb{Z}_p)$, and define

$$G_E := \{g \in G : g_3 \equiv \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 3\}.$$

In this case, Theorem 2 of Rumely [**47**] tells us that

a) $F := K(\mu)$ is the class field of K corresponding to $K^* f_\tau^{-1}(G_E)$.
b) For any $\boldsymbol{\alpha}$ in $\mathfrak{I}_F$ there is a unique decomposition $\mathrm{N}_{F/K}(\boldsymbol{\alpha}) = a_\alpha \boldsymbol{\beta}$ with a_α in K^* and $\boldsymbol{\beta}$ in $f_\tau^{-1}(G_E)$.
c) The Grössencharacter of E is defined by

$$\chi_E(\boldsymbol{\alpha}) = \beta_\infty^{-1}.$$

Example 4.3.1 (Rumely [**47**] Example 3(d))**.** Let $\tau = (4+\sqrt{-2})/3$. Then $D_K = -8$, $j = 8000$ and $\mu = (-2+\sqrt{-2})/3$ so that

$$E : x^3 + y^3 + 1 = (-2+\sqrt{-2})xy$$

is defined over $K = H_K$. The conductor of χ_E is $\mathfrak{p} = (1+\sqrt{-2})$, one of the two primes of K dividing 3. We shall see another description of χ_E in Section 4.3.1.

The curves constructed in this way are clearly K-curves, but for the families described in detail by Rumely, it is rare that the models in question are defined over $K(j)$.

If $\gamma_2(\tau)$ and $\gamma_3(\tau)$ are the modular functions, known as *Weber functions*, satisfying

$$\begin{aligned} \gamma_2^3(\tau) &= j(\tau), \\ \gamma_3^2(\tau) &= j(\tau) - 1728, \end{aligned}$$

and m is an element of $\mathbb{C}^*$ then the curves

$$\mathcal{E}(\tau, m) : y^2 = x^3 - m^2 \frac{\gamma_2(\tau)}{48} x + m^3 \frac{\gamma_3(\tau)}{864} \tag{4.9}$$

have j-invariant $j(\tau)$ and Grössencharacters which may be determined in a manner similar to those of the Hesse curves (see Theorem 1 of Rumely [**46**] and Section 5 of Rubin and Silverberg [**45**]). The following lemma helps to determine for which m the curves $E(\tau, m)$ will be defined over $K(j(\tau))$.

Lemma 4.3.2 (Rubin-Silverberg [**45**] Lemma 3.4)**.** *Let $\mathcal{O}$ be the order of K associated with the j-invariant $j(\tau)$. Then*

a) *If $D_{\mathcal{O}}$ is odd then $\gamma_3(\tau)$ and $\gamma_2(\tau)\sqrt{D_{\mathcal{O}}}$ are defined over $K(j(\tau))$.*
b) *If $D_{\mathcal{O}} \equiv 4, 8 \bmod 16$ then $i\gamma_3(\tau)$ and $\gamma_2(\tau)\sqrt{-D_{\mathcal{O}}/4}$ are defined over $K(j(\tau))$.*

For the fields $K = \mathbb{Q}(\sqrt{-p})$ where there is only one $\mathbb{Q}$-equivalence class of $\mathbb{Q}$-curves, Gross has given a systematic answer to the problem of finding minimal models for $\mathbb{Q}$-curves in each $\mathbb{Q}$-equivalence class over H.

Proposition 4.3.3 (Gross [**16**] Chapter 5 and [**17**])**.** *Let $p \equiv 3 \bmod 4$ be a prime and let $K = \mathbb{Q}(\sqrt{-p})$. Let j be the j-invariant of a curve with CM by $\mathcal{O}_K$ and define*

$$f_2(x) = x^3 - j, f_3(x) = -px^2 + (1728 - j).$$

Then f_2 has a unique zero, a_2 in H, and f_3 splits in H, with zeroes $\pm a_3$, where we choose the sign of a_3 by requiring that $a_3 \cdot \left(\frac{2}{p}\right) > 0$. The elliptic curve

$$A(p) : y^2 = x^3 + \frac{a_2 p}{48}x - \frac{a_3 p^2}{864}, \tag{4.10}$$

has j-invariant j, discriminant $\Delta = -p^3$ over $\mathbb{Q}(j)$, and is a $\mathbb{Q}$-curve. The Grössencharacter of $A(p)$ over H_K has conductor p.

Rubin and Silverberg [**45**] Section 7, have generalized Gross' construction to find a model over $\mathbb{Q}(j_E)$ for canonical $\mathbb{Q}$-curves. When D_K is odd one has, setting $m := \sqrt{D_K}\gamma_2^4$ in (4.9)

$$\mathcal{E} : y^2 = x^3 - \frac{D_K j_E^3}{48}x + \frac{D_K\sqrt{D_K}\gamma_3 j_E^4}{864}, \tag{4.11}$$

where $\gamma_3^2 = j_E - 1728$. When $D_K \equiv 0 \mod 8$ then setting $d_K := -D_K/4$ and $m := \pm\sqrt{d_K}\gamma_2^4$, the two canonical curves have models

$$\mathcal{E} : y^2 = x^3 - \frac{d_K j_E^3}{48}x \pm \frac{d_K\sqrt{d_K}\gamma_3 j_E^4}{864}. \tag{4.12}$$

For general orders $\mathcal{O}$ we may attempt to find a curve with a given Grössencharacter χ computationally by taking a standard model of a curve $E/H_{\mathcal{O}}$ with j-invariant j_E, for example

$$y^2 = x^3 - \frac{27 j_E x}{j_E - 1728}x + \frac{54 j_E}{j_E - 1728}, \tag{4.13}$$

(the default Weierstrass model in Magma for $D_{\mathcal{O}} < -4$), calculating its conductor, and finding $m \in H_{\mathcal{O}}$ such that

$$\mathfrak{f}_{E^m} = \mathfrak{f}_{\chi}^2,$$

and, if there exist unramified quadratic extensions of $H_{\mathcal{O}}$, verify by evaluating L-series coefficients of χ and the possible curves E' until a unique match is found. The main disadvantage of this method is that it involves calculating the conductor of an elliptic curve which is computationally expensive, because it involves finding a $\mathfrak{p}$-minimal model for every prime dividing the discriminant of E (see Remark 4.3.10). Finding m also becomes more difficult when the conductor of E_0 is not principal. If 3 is either split or ramified in $\mathcal{O}$, then there is an alternative method based on the 3-torsion points of E which we describe below.

4.3.1. Three-Torsion Points. Let $\mathcal{O}$ be an order of an imaginary quadratic field K with ring class field $H_{\mathcal{O}}$, and let E be an elliptic curve with CM by $\mathcal{O}$. The 3-division polynomial f_3 of E has degree 4, is irreducible over $H_{\mathcal{O}}$ if and only if 3 is inert in $\mathcal{O}$ and has either one or two roots in $H_{\mathcal{O}}$ depending on whether 3 ramifies or splits in $\mathcal{O}$. If $D_{\mathcal{O}}$ is divisible by 3 then f_3 has a root in $\mathbb{Q}(j_E)$.

Proposition 4.3.4. *Suppose that 3 either ramifies or splits in $\mathcal{O}$, let $P = (x(P), y(P))$ be an element of $E[3]$ with $x(P)$ in $H_{\mathcal{O}}$ and let $L = H_{\mathcal{O}}(y(P))$. Then E^L is an elliptic curve with bad reduction only at primes of H dividing 3.*

Proof. As usual, we are assuming $D_K \neq -3, -4$. Let S be the set of primes of $H_{\mathcal{O}}$, coprime to 3, at which E has bad reduction, and let $\mathfrak{p}$ be an element of S. The image of the inertia group $G(\mathfrak{p})$ under the 3-adic representation is $\{\pm 1\}$ by Theorem 6(b) of Serre-Tate [**51**], and hence becomes trivial over a quadratic extension of $H_{\mathcal{O}}$. Now the action of $G(\mathfrak{p})$ on P becomes trivial over L, so by Proposition 1.3.14, E^L has good reduction at $\mathfrak{p}$, for all $\mathfrak{p}$ in S. □

Lemma 4.3.5. *Suppose that 3 either ramifies or splits in $\mathcal{O}$. Let E and E_0 be CM curves defined over $H_{\mathcal{O}}$, such that $j_E = j_{E_0}$ and let P_0 be a point of $E_0[3]$ with x-coordinate $x(P_0)$ in $H_{\mathcal{O}}$, and let $L_0 = H(y(P_0))$. Then there exists a point P of $E[3]$ such that*

$$E_0^{L_0} \simeq E^L,$$

where $L = H_{\mathcal{O}}(y(P))$.

Proof. Let k be the quadratic extension of $H_{\mathcal{O}}$ over which E and E_0 become isogenous, and let P be the 3-torsion point of E with the property that $E^{y(P)^2}$ is k-isogenous to $E_0^{L_0}$. By the definition of the quadratic twist,

$$L = H_{\mathcal{O}}(y(P)) = k \circ H_{\mathcal{O}}(y(P_0)) = k \circ L_0$$

so the isogeny is defined over $H_{\mathcal{O}}$. □

Remark 4.3.6. Let L and L' be quadratic extensions of F with Dirichlet characters ϕ and ϕ' respectively. Recall that in Definition 3.1.3 we defined $L'' := L \circ L''$ to be the quadratic extension of F corresponding to the character $\phi\phi'$ of $\mathfrak{I}_F$.

Proposition 4.3.7. *Let E and L be as in Proposition 4.3.4. Then E^L is a K-curve of type 1.*

Proof. Suppose that E is a K-curve of type 1. Then L/K is abelian by Theorem 2.3.12, hence by Corollary 2.3.13, E^L is also of type 1. Since there exists a K-curve E_0 of type 1 over $H_{\mathcal{O}}$ for any imaginary quadratic field K, the result follows from Lemma 4.3.5 for any curve E/H with CM by $\mathcal{O}$. □

If $\mathcal{O} = \mathcal{O}_K$ and D_K is divisible by 3, then the curve E^L is the $\mathbb{Q}$-curve determined by the character λ_3 defined in Proposition 2.2.17. If 3 splits into primes $\mathfrak{p}, \mathfrak{p}^\rho$ of K then the twists of E by the 3-torsion points P_1, P_2 with $x(P_i)$ in H correspond to the K-curves determined by the quadratic characters $\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^\rho$ defined in (2.12). These curves become isogenous over $H(\sqrt{-3})$.

Example 4.3.8. Let $K = \mathbb{Q}(\sqrt{-8})$. We saw in Example 4.3.1 that the elliptic curve E/K with model $x^3 + y^3 + 1 = (-2 + \sqrt{-2})xy$ has Grössencharacter χ_E with conductor $\mathfrak{p} = (1 + \sqrt{2})$, one of the primes of K dividing 3. Since $K = H_K$ has class number 1, χ_E must correspond to $\lambda_{\mathfrak{p}}$. Taking a random curve over K with CM by $\mathcal{O}_K$ and twisting by a 3-division point in the sense of Proposition 4.3.4, we find a Weierstrass model

$$y^2 = x^3 + 1/8748(50\sqrt{-2} + 115)x + 1/2125764(-665\sqrt{-2} + 1022)$$

We could also obtain a Weierstrass model by entering the Hesse curve directly, which gives us another way to verify that the two models define the same curve.

Example 4.3.9. Let K be the quadratic field with discriminant $D_K := -84 = -4 \cdot 3 \cdot 7$ and let j_E be the j-invariant of an elliptic curve with CM by $\mathcal{O}_K$. The maximal real subfield $\mathbb{Q}(j_E)$ of H_K is $F := \mathbb{Q}(\sqrt{3}, \sqrt{7})$. The curve E/F with this j-invariant and Weierstrass model defined in (4.13) has conductor ramified over primes dividing 2, 3, 7, 47, 53, 59 and 83. Since D_K is divisible by 3 there exists a single point $P \in E[3]$ such that $x(P)$ is defined over F. Twisting E by $y(P)^2$ yields:

$$\begin{aligned} y^2 = x^3 &+ a_1(3281187890779919 j_E^3 - 1048930450552515895094810937 6 j_E^2 \\ &- 187460611742123760723480011930296 32 j_E \\ &+ 108743922263266511181455628494202 4704)x \\ &+ a_2(26666036511099989741 j_E^3 - 85246010356905994966259679102528 j_E^2 \\ &- 1523482252017814063032482241675368 57088 j_E \\ &+ 883755974107050551118785311313276 6724096) \end{aligned}$$

where

$$a_1 := 1/93034391040943585943719960903 68, \text{ and}$$
$$a_2 := 1/372137564163774343774879843614 72.$$

Remark 4.3.10. To quantify our claim about the relative efficiency of this method, we timed the calculation in Magma of the conductor of the default curve E with j-invariant j_E over either $\mathbb{Q}(j_E)$ or $K(j_E)$, and then twisted by a 3-torsion point. The results were as follows:

$D_{\mathcal{O}}$	$Cl(\mathcal{O})$	Twist	Conductor
$-15 = -3 \cdot 5$	C_2	0.000	0.040
$-195 = -3 \cdot 5 \cdot 13$	$C_2^{\times 2}$	0.040	0.340
$-660 = -2^2 \cdot 3 \cdot 5 \cdot 11$	$C_2^{\times 3}$	0.480	8.550
$-231 = -3 \cdot 7 \cdot 11$	$C_2 \times C_6$	0.900	17.270
$-495 = -3^2 \cdot 5 \cdot 11$	$C_2 \times C_8$	3.140	61.090
$-440 = -2^3 \cdot 5 \cdot 11$	$C_2 \times C_6$	6.400	131.150

In the first four cases E is a curve defined over $\mathbb{Q}(j_E)$. In the final example, where 3 splits in $\mathcal{O}_K$, the 3-division polynomial does not have a root over $\mathbb{Q}(j_E)$, hence E is defined over $K(j_E)$, a field of degree 24.

4.4. $\mathbb{Q}$-Curves with Good Reduction Everywhere

Let K be an imaginary quadratic field with discriminant D_K and Hilbert class field H. If $D_K < -4$ it is known (see Theorem 9 of Serre-Tate [**51**]), that any elliptic curve E/F with CM by an order of K attains good reduction everywhere over a quadratic extension of F. We would like to know when there exists an elliptic curve E/H with CM by $\mathcal{O}_K$ which has good reduction at every prime of H. In this section we determine a necessary and sufficient condition for the existence of a CM elliptic curve with good reduction everywhere over H. The main result is Proposition 4.4.13 which extends results of Rohrlich [**42**]. Throughout this section we assume $D_K < -4$.

Lemma 4.4.1. *Let $p \equiv 3 \bmod 4$ be a rational prime dividing D_K and let k be a quadratic field contained in H. Then there exists an even quadratic character ϕ of $\mathfrak{I}_k$ ramified only over primes of k dividing p if and only if k is real and p divides D_k.*

Proof. If p ramifies in k then λ_p defines an odd character of $\mathfrak{I}_k$ which does not become trivial on $\mathrm{N}_{H/k}(\mathfrak{I}_H)$, and it follows that such an L exists if and only if k is real.

If p is inert in k then the only extension of k ramified only over p is $k(\sqrt{-p})$ which is contained in H since p divides D_K.

Finally if p splits in k let $\mathfrak{q}$ and $\mathfrak{q}^\sigma$ be the primes of k dividing p and let L and L_σ be the quadratic extensions of k defined by $\lambda_{\mathfrak{q}}$, $\lambda_{\mathfrak{q}}^\sigma$ (with the appropriate infinite components). Let $F = k(\sqrt{-p})$. Then $LF = L_\sigma F$ and LF/F is unramified, hence so is LH/H. □

Proposition 4.4.2. *Let p be a prime dividing D_K and suppose that p is congruent to 3 modulo 4. There exists a field L in $\mathcal{G}^s_{H/K}$ such that L/H is ramified precisely at the primes of H dividing p if and only if D_K is divisible by at least two rational primes congruent to 3 modulo 4.*

Proof. By Proposition 3.3.1 and (3.16) every field L in $\mathcal{G}^s_{H/K}$ which is unramified outside D_K may be written in the form

$$L = L_0 \circ L_1 \circ \cdots \circ L_m,$$

for some $m \leq \binom{n}{2}$ where L_0/K is abelian and for each $i \geq 1$ there exist odd prime discriminants s^*, t^* dividing D_K and a dihedral extension F_i/K containing $K(\sqrt{s^*}, \sqrt{t^*})$ such that $L_i = F_iH$. Let ϕ_i be the character associated with the extension $F_i/K(\sqrt{s^*}, \sqrt{t^*})$. By construction, for some d in $\{t^*, s^*, t^*s^*\}$ there exists a quadratic Dirichlet character ϕ of $K(\sqrt{d})$ such that

$$\phi_i := \phi \circ \mathrm{N}_{F_i/K(\sqrt{d})}$$

and L_i/H is ramified over p if and only if ϕ is. As we saw in Chapter 3 that any dihedral extension of this form is $\mathbb{Q}$-equivalent to one unramified outside st, we need only consider the cases where $s^* = -p$.

First, suppose that $t \equiv p \equiv 3 \bmod 4$. If $\left(\frac{-p}{t}\right) = 1$ then we may suppose that F_i is a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{-p}, \sqrt{-t})$ and cyclic over $\mathbb{Q}(\sqrt{-t})$. Let $k := \mathbb{Q}(\sqrt{pt})$. Then since the class number of k is odd, there is a quadratic extension F/k ramified only at p and ∞_i for each of the infinite places ∞_1, ∞_2 of k. The extension $F(\sqrt{-t})$ is normal over $\mathbb{Q}$ and clearly belongs to the class of F_i. If $\left(\frac{-p}{t}\right) = -1$ then we obtain an extension F/k ramified over t, but by Proposition 2.2.17 there exists a quadratic extension A/H abelian over K ramified over pt and the extension $A \circ FH$ is ramified only over p. (See the proof of Proposition 4.4.3 for why this is so.)

Now suppose that p is the only prime divisor of D_K congruent to $3 \bmod 4$. If either

$$\left(\frac{t}{p}\right) = 1 \text{ or } \left(\frac{-p}{t}\right) = 1$$

then there exists a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{t}, \sqrt{-p})$. But by Lemma 4.4.1, if $k = \mathbb{Q}(\sqrt{d})$ with d in $\{-p, -pt, t\}$ there are no even quadratic characters of $\mathfrak{I}_k$ ramified only at infinite primes and primes dividing p. Otherwise, p is inert in $\mathbb{Q}(\sqrt{t})$ hence also in $K(\sqrt{t})/K$ and we may take $d = t$. Any quadratic character of $K(\sqrt{t})$ ramified over p is lifted from K, and we are done. □

Proposition 4.4.3. *There exists a $\mathbb{Q}$-curve E/H with good reduction at every prime of H if and only if D_K is divisible by at least two primes $p, q \equiv 3 \bmod 4$.*

Proof. Suppose that D_K is divisible by some prime $p \equiv 3 \bmod 4$ and let E_0 be the $\mathbb{Q}$-curve of type 1 corresponding to the character λ_p. There is a $\mathbb{Q}$-curve E/H with good reduction everywhere if and only if there exists an absolutely normal quadratic extension L/H such that $E = E_0^L$. Clearly L/H is ramified only over p, so we have proved the 'only if' part of the proposition for this case in Proposition 4.4.2.

If we can construct a quadratic extension L/H with character ϕ such that for any prime $\mathfrak{P}$ of H,

$$\phi_{\mathfrak{P}} = \begin{cases} \lambda_p \circ \mathrm{N}_{H/K} & \text{if } \mathfrak{P}|p, \\ 1 & \text{otherwise,} \end{cases}$$

then $E = E_0^L$ will have good reduction everywhere over H.

Let $k = \mathbb{Q}(\sqrt{pq})$. The class number of k is odd, hence any even quadratic character on U_k defines a Dirichlet character of $\mathfrak{I}_k$.

Let ∞ denote one of the real infinite places of k, and $\mathfrak{p}$ the prime of k dividing p and consider the character ϕ' of $\mathfrak{I}_k$ with non-trivial local components $\phi'_{\mathfrak{p}} = \lambda_{\mathfrak{p}}$ and $\phi'_\infty = \mathrm{sgn}_\infty$.

We shall demonstrate that $L = L'H$ and $\phi = \phi' \circ \mathrm{N}_{H/k}$ have the required properties.

First, we note that since H is a CM field, it has no real infinite places and hence the infinite components of ϕ are trivial. Let $\mathfrak{q}$ be the prime of K dividing p, and recall that $\lambda_{\mathfrak{q}}$ and $\lambda_{\mathfrak{p}}$ are trivial on $U_{\mathfrak{q}}^{(1)}$ and $U_{\mathfrak{p}}^{(1)}$ respectively.

Now since H/K and H/k are unramified over p, by Serre [**49**] Chapter V, Proposition 2(i), the norm maps

$$\begin{aligned} N_k : U_{\mathfrak{P}}^{(0)}/U_{\mathfrak{P}}^{(1)} &\rightarrow U_{\mathfrak{p}}^{(0)}/U_{\mathfrak{p}}^{(1)}, \\ N_K : U_{\mathfrak{P}}^{(0)}/U_{\mathfrak{P}}^{(1)} &\rightarrow U_{\mathfrak{q}}^{(0)}/U_{\mathfrak{q}}^{(1)}, \end{aligned}$$

correspond to the norm on the residue field extensions $\overline{H}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}}$ and $\overline{H}_{\mathfrak{P}}/\overline{K}_{\mathfrak{q}}$ respectively. But $\overline{k}_{\mathfrak{p}} = \overline{K}_{\mathfrak{q}} = \mathbb{F}_p$ so the result follows.

If K is exceptional, then there are no $\mathbb{Q}$-curves defined over H so the claim is trivially true. The only remaining case is that $D = -8d$, where every prime dividing d is congruent to 1 modulo 4. Let E_0 be the $\mathbb{Q}$-curve of type 1 determined by λ_{-8}. Since 2 is unramified in every real subfield of H, the result follows in the same manner as for λ_p. □

Remark 4.4.4. The construction of the Grössencharacter of an elliptic curve E/H with good reduction everywhere is equivalent to that of Rohrlich [**42**], though we take a different approach.

Example 4.4.5. Suppose that 3 and 7 ramify in K, let $k = \mathbb{Q}(\sqrt{21})$ and let $\mathfrak{p}$ be the prime of k dividing 3. Then $\mathfrak{p}$ is a principal ideal generated by

$$x = \frac{\sqrt{21}+3}{2},$$

and the extension $L' = k(\sqrt{x})$ has conductor with finite part $\mathfrak{p}$ and normal closure $k(\sqrt{x}, \sqrt{-3})$.

If D_K is divisible by at least two primes congruent to 3 mod 4, then the number n_G of $\mathbb{Q}$-curves E/H with good reduction everywhere is equal to the order of the subgroup of $\mathcal{G}^s_{H/K}$ generated by unramified extensions of K. Conversely, Proposition 4.4.3 provides a lower bound on the 2-rank of the class group of H. Suppose that $p_1, \dots, p_u$ are distinct prime divisors of D_K such that p_i^* is either $-p_i$ or -8. The pairs p_i, p_{i+1} and p_j, p_{j+1} with $j > i+1$ define distinct $\mathbb{Q}$-curves with good reduction everywhere, hence as a first estimate, $n_G \geq \lfloor \frac{u}{2} \rfloor$. If we start from a fixed curve E, then we can find another estimate as in the corollary below.

Corollary 4.4.6. *Let $n+1$ be the number of distinct prime divisors of D_K and let u be the number of primes p dividing D_K such that $p^* < 0$ and $p^* \neq -4$ and suppose that $u \geq 2$. Then*

$$n_G \geq \begin{cases} 2^{u-3} & \textit{if } n+1 = u, \\ 2^{u-2} & \textit{otherwise.} \end{cases}$$

Proof. We note that if u is even then $n+1 > u$ so there is no immediate contradiction when $u = 2$. Let p and E_0 be as in the proof of Proposition 4.4.3, and let S be the set of prime divisors q of D_K such that $q^* \in \{-q, -8\}$ and $q \neq p$. Now by Proposition 4.4.3 for any $q \in S$ we can construct a dihedral extension $L := L_q$ of K containing $K(\sqrt{-p}, \sqrt{-q})$ such that E_0^L has good reduction everywhere over H, and clearly for any two primes $q, q' \in S$ the extension $L_q \circ L_{q'}$ is unramified over H. By Lemma 3.2.10, $L_q \circ L_{q'}$ belongs to $\mathcal{G}^{(1)}_{F/k}$, and it follows from Proposition 3.3.1 and (3.16) that the group $G_L := \langle L_q : q \in S \rangle$ has $u-2$ independent generators if $u = n+1$ and $u-1$ otherwise. Now precisely half of the elements of G_L are unramified extensions of H, and the other half are of the form $L = L_q \circ L'$ with $q \in S$ and L'/H unramified, and for any such L the elliptic curve

$$E = E_0^L = (E_0^{L_q})^{L'}$$

clearly has good reduction everywhere. □

Proposition 4.4.7. *If D_K is non-exceptional and $p \equiv 3 \bmod 4$ is a rational prime which is unramified in $K/\mathbb{Q}$, there is a $\mathbb{Q}$-curve with CM by $\mathcal{O}_K$ which has good reduction everywhere over $H(\sqrt{-p})$.*

Proof. Let $F = H(\sqrt{-p})$ and $k = \mathbb{Q}(\sqrt{sp})$, where s is a positive integer such that $-s$ appears in the factorization of D_K into prime discriminants. The result then follows precisely as in Proposition 4.4.3 with E_0 the type 1 curve ramified only over s and F in place of H. □

Example 4.4.8. Let $D_K = -8$. Then $h_K = 1$ and there is a single equivalence class of $\mathbb{Q}$-curves of type 1 defined over $H = K$. By the previous proposition, there exist $\mathbb{Q}$-curves with good reduction everywhere over $K(\sqrt{-p})$ for all primes $p \equiv 3 \bmod 4$. In particular, if $p = 3$ we obtain the curve $\mathcal{E}$ investigated by Setzer [**52**] and Schoof [**48**]. This curve has good reduction over $k = \mathbb{Q}(\sqrt{6})$.

Using the theory of Weil restrictions developed in Chapter 5 we obtain the following corollary to Proposition 4.4.3

Corollary 4.4.9. *If D_K is divisible by distinct primes $p, q \equiv 3 \bmod 4$, and k is a subfield of H such that H/k is unramified, then there exist abelian varieties defined over k with good reduction everywhere.*

Proof. Let A be the Weil restriction from H to k of an elliptic curve E with good reduction everywhere over H. As we shall see in Proposition 5.2.2,

$$\mathfrak{f}_{A/k} = \mathrm{N}_{H/k}(\mathfrak{f}_{E/H}) \cdot D_{H/k}^2,$$

hence $\mathfrak{f}_{A/k} = 1$ so A/k has good reduction everywhere. □

Lemma 4.4.10. *Let K be an imaginary quadratic field and let H be the Hilbert class field of K. Let k be a subfield of H and suppose that there exists a k-curve E defined over H. Then if there exists an elliptic curve E_0/H with good reduction everywhere then there exists a k-curve defined over H with good reduction everywhere.*

Proof. Set $\chi := \chi_E$, $\chi_0 := \chi_{E_0}$ and let L/H be the quadratic extension corresponding to the Dirichlet character $\phi := \chi\chi_0^{-1}$. Then $\mathfrak{f}_\phi = \mathfrak{f}_\chi$ and the restriction of ϕ to U_H must be fixed by $\mathrm{Gal}(H/k)$. Recalling that ϕ must have trivial infinite components, we must have

$$\phi = \varphi \cdot \chi|_{U_H}$$

where φ is a character of $Cl(H)$ (see Section 2.1.2). Now if the class group of H is trivial then L/k is normal, hence E_0 is a k-curve. But if not then since φ is a quadratic Dirichlet character, $\varphi \cdot \chi_0$ is the Grössencharacter of a k-curve with good reduction everywhere over H. □

The question still remains as to whether there exists a CM elliptic curve with good reduction everywhere over H if K is exceptional.

Lemma 4.4.11. *Let $p \equiv 3 \bmod 4$ be a rational prime which splits into primes $\mathfrak{p}, \mathfrak{p}^\rho$ in K and let E be the K-curve determined by $\lambda_\mathfrak{p}$. Let k be a real quadratic field contained in H in which p splits. Then there does not exist an quadratic extension L/k such that the twist of E by LH has good reduction everywhere over H.*

Proof. The analogy with the ramified case breaks down because, whereas if p is ramified in k and K it is unramified in the extension Kk/k, if p splits in k and K then it also splits in the extension Kk/k. In consequence, the conductors of LH/H and E/H will differ. □

The curve E will obtain good reduction everywhere over $L := H(\sqrt{-p})$ since $\lambda_\mathfrak{p}$ is trivial on $\mathrm{N}_{L/K}(\mathfrak{I}_L)$.

Proposition 4.4.12. *If K is exceptional then there are no elliptic curves with good reduction everywhere over H.*

Proof. Comparing Lemma 4.4.11 and the proof of Proposition 4.4.3 we see that there are no K-curves with good reduction everywhere defined over H. But by Lemma 4.4.10 this means that there are no elliptic curves with CM by $\mathcal{O}_K$ with good reduction everywhere over H. □

Proposition 4.4.13. *Let K be an imaginary quadratic field and let $F := \mathbb{Q}(j_E)$ where j_E is the j-invariant of an elliptic curve with CM by $\mathcal{O}_K$. The following are equivalent:*

a) *D_K is divisible by at least two primes congruent to $3 \bmod 4$.*
b) *The extension H_K/F is unramified at every finite place of F.*
c) *There exists an elliptic curve E/F with CM by $\mathcal{O}_K$ over H and with good reduction everywhere over F.*
d) *There exists a $\mathbb{Q}$-curve with CM by $\mathcal{O}_K$ having good reduction everywhere over H.*
e) *There exists an elliptic curve E/H with CM by $\mathcal{O}_K$ and good reduction everywhere over H.*

Proof. The equivalence of a), b), c) is proved by Rohrlich in [**42**], and the equivalence of a) and d) is the content of Proposition 4.4.3. The equivalence of d) and e) is a consequence of Lemma 4.4.10 and Proposition 4.4.12. □

CHAPTER 5

Weil Restrictions and Endomorphism Algebras

Let F/k be a normal field extension, and let X be an abelian variety defined over F. Recall that X *descends to* k if there exists an abelian variety Y defined over k such that X and $Y_F := Y \times_k F$ are isomorphic. We shall see that the product variety

$$\prod_{\sigma \in \mathrm{Gal}(F/k)} X^\sigma$$

always descends to k, and shall investigate the properties of the k-variety W with $W_F \cong \prod X^\sigma$, known as the *Weil restriction* of X from F to k.

In the first section we develop the properties of the Weil restriction for a more general class of objects, and return to look in detail at abelian varieties in Section 5.2. If the abelian variety A is defined over k, then A is a factor of W. The remaining factors of W are related to the non-trivial idempotents of $\mathrm{End}_k^0(W)$ as described in Section 5.2.2, which follows Kani and Rosen [**24**] and Yu [**69, 70**].

By Lemma 5.2.5

$$[\mathrm{End}_k^0(W) : \mathrm{End}_F^0(A)] = |\langle \sigma \in G : A \simeq A^\sigma \rangle|,$$

so that if A is of CM type then W is also of CM type over k only if A is a k-variety. We shall see in Theorem 5.2.16 that if A is a k-variety of type 1 then W/k is a product of simple non-isogenous abelian varieties of CM type. If A and B are k-equivalent k-varieties of CM type then their Weil restrictions have isomorphic endomorphism algebras; if moreover $\mathrm{Aut}(A) = \pm 1$ and A is of k-type 1 then the converse is also true, (see Proposition 5.2.18).

In Section 5.3, which largely follows the papers [**33, 34**] of Nakamura, we investigate the endomorphism algebra of the Weil restriction of a CM elliptic curve, with particular emphasis on the $\mathbb{Q}$-curve case, and describe its computation, giving a number of examples in Section 5.4. In Section 5.5 we consider abelian varieties of dimension 2. Let K be an imaginary quadratic field and let k be a biquadratic CM field containing K. Section 5.5.1 investigates the existence of $\mathbb{Q}$-curves E/H and subfields F of H such that E/H has CM by K and the Weil restriction of E from H to F has CM by k over F. In Section 5.5.2 we let k be a quartic CM field such that $\mathrm{Gal}(k/\mathbb{Q})$

is cyclic and let k_0 be the maximal real subfield of k. If A is an abelian variety with CM by k then A is defined over the Hilbert class field of k, and the theory of k_0-varieties with CM by k is very similar to that of $\mathbb{Q}$-curves. We illustrate this by describing the Grössencharacters and calculating the endomorphism algebras of the Weil restrictions to k_0 of a family of k_0-varieties where k has class number 4.

5.1. Weil Restriction in General

Let k be a field, F a finite extension of k and k^{alg} an algebraic closure of k containing F and suppose that $\{\sigma_1, \dots, \sigma_n\}$ is the set of distinct isomorphisms of F into k^{alg}. Let X be a variety defined over F, let W be a variety defined over k and suppose that ϕ is a map from $W_F := W \times_k F$ to X. Then for any $1 \leq i \leq n$ we can define a map $\phi^{\sigma_i} : W_F \to X^{\sigma_i}$ and hence a map $\Phi := (\phi^{\sigma_1}, \dots, \phi^{\sigma_n})$,

$$\Phi : W_F \to \prod_{i=1}^{n} X^{\sigma_i}. \tag{5.1}$$

Definition 5.1.1. *If a map $\phi : W_F \to X$ exists such that the map Φ of* (5.1) *is an isomorphism, then we call W the* Weil restriction *of X from F to k; symbolically we write $W := \mathfrak{W}_{F/k}(X)$.*

In some references, the Weil restriction of X is referred to as 'the variety obtained from X by restriction of scalars (or restriction of the field of definition) from F to k'.

Definition 5.1.2. *Let F/k be a field extension. Given a morphism of k-varieties $\lambda : X \to Y$ we denote by λ_F the natural extension of λ to a morphism $X_F \to Y_F$.*

Proposition 5.1.3 (Universal Mapping Property)**.** *Let F, k, X, W, ϕ and Φ be as above and suppose that Φ is an isomorphism. Then if Y is a variety defined over k, for any map $\lambda : Y_F \to X$ there is a unique morphism ζ from Y to W defined over k such that $\lambda = \phi \circ \zeta_F$.*

Proof. The map $(\lambda^{\sigma_1}, \dots, \lambda^{\sigma_n}) : Y_F \to \prod X^{\sigma_i}$ is fixed by every element of $\{\sigma_1, \dots, \sigma_n\}$ and hence is defined over k, so we can take

$$\zeta = (\phi^{\sigma_1}, \dots, \phi^{\sigma_n})^{-1} \circ (\lambda^{\sigma_1}, \dots, \lambda^{\sigma_n}).$$

□

Corollary 5.1.4. *If $\mathfrak{W}_{F/k}(X)$ exists, it is unique up to isomorphism.*

FIGURE 1. Universal Mapping Property

$$\begin{tikzcd}
W_F \arrow[r, "\phi"] & X \\
& Y_F \arrow[u, "\lambda"'] \arrow[ul, dashed, "\zeta_F"]
\end{tikzcd}$$

Proposition 5.1.5 (Weil [**67**] Proposition 1.3.1)**.** *Let F/k be a finite separable extension of fields and let X_1 and X_2 be varieties defined over F with well-defined Weil restrictions to k. Let Y be a subvariety of $X_1 \times X_2$. Then*

$$\mathfrak{W}_{F/k}(X_1 \times X_2) = \mathfrak{W}_{F/k}(X_1) \times \mathfrak{W}_{F/k}(X_2), \tag{5.2}$$

and $\mathfrak{W}_{F/k}(Y)$ is defined.

Let $\mathbb{A}_F^m$ and $\mathbb{P}_F^m$ denote respectively affine and projective space of dimension m over F.

Lemma 5.1.6 (Weil [**67**] p. 6)**.** *Let F/k be as in Proposition 5.1.5. If X is isomorphic to either $\mathbb{A}_F^m$ or $\mathbb{P}_F^m$ for $m \geq 1$ then $\mathfrak{W}_{F/k}(X)$ is well defined.*

Example 5.1.7. If F/k is a normal extension of degree n and $X \cong \mathbb{A}_F^1$ (the affine line over F) then $\mathfrak{W}_{F/k}(X) \cong \mathbb{A}_k^n$.

Combining Proposition 5.1.5 and Lemma 5.1.6, we see that

Proposition 5.1.8. *If X is a variety which is embeddable in affine or projective space over F then $\mathfrak{W}_{F/k}(X)$ is well defined.*

Proposition 5.1.9. *Let F/k be a finite separable extension and let X be a variety defined over F. If X is embeddable in affine (projective) space over F then $\mathfrak{W}_{F/k}(X)$ is embeddable in affine (projective) space over k.*

Proof. By Theorem 7 of Weil [**65**], if F is a finite separable extension of k and Y is a variety defined over F which descends to k, then if Y is embeddable in affine (projective) space over F, the descended variety is embeddable in affine (projective) space over k.

Now since X is embeddable in affine (projective) space, so is $\prod_i X^{\sigma_i}$ where the σ_i are defined as in (5.1), and the result follows immediately. □

Let F/k be a separable algebraic extension, and let $\mathcal{S}$ be the set of distinct isomorphisms of F into k^{alg}. Let $L \subset k^{alg}$ be an extension of k. Then if τ is an automorphism of k^{alg}/L, we can define a right-action of τ on $\mathcal{S}$ by

$$t^{\sigma\tau} := (t^{\sigma})^{\tau}, \text{ where } \sigma \in \mathcal{S}, \text{ and } t \in F. \tag{5.3}$$

We define an equivalence relation $\sim$ on $\mathcal{S}$ by setting $\sigma_i \sim \sigma_j$ if $\sigma_i = \sigma_j \tau$ and let $\{s_i\}$ be a set of representatives of equivalence classes of $\mathcal{S}$ with s_1 the identity on F.

Let $L_i := F^{s_i} \cdot L$, $X_i := X^{s_i}$, $W := \mathfrak{W}_{F \cdot L/L}(X)$ and $W_i := \mathfrak{W}_{L_i/L}(X_i)$. Now we have

$$\begin{aligned} W \times_L F \cdot L &\cong \prod_\tau \Big(\prod_i X^{s_i} \Big)^\tau \\ &\cong \prod_i W_i \times_L F \cdot L, \end{aligned}$$

hence

$$W \cong \prod W_i. \tag{5.4}$$

By definition there is an isomorphism $W_i(L) \cong X(L_i)$ and hence

$$W(L) \cong \prod X(L_i). \tag{5.5}$$

Remark 5.1.10 (Semidirect products)**.** Let G be a group and suppose that N and H are subgroups of G with the properties that $G = NH$, $N \cap H = 1$ and N is a normal subgroup of G. Then G is the *semidirect product* of N by H and we write $G = N \rtimes H$. For example, if G is the dihedral group of order 8 then $G \cong C_2 \rtimes C_4$.

Lemma 5.1.11. *Suppose that $L/F/k$ is an absolutely normal tower of number fields and X is a variety over L such that $\mathfrak{W}_{L/k}(X)$ is well defined. If* $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(L/F) \rtimes \mathrm{Gal}(F/k)$*, then*

$$\mathfrak{W}_{L/k}(X) = \mathfrak{W}_{F/k}(\mathfrak{W}_{L/F}(X)).$$

Proof. Let $G := \mathrm{Gal}(L/k)$, $N := \mathrm{Gal}(L/F)$ and $H := \mathrm{Gal}(F/k)$. Tensoring by L and expanding the right hand side we have

$$\begin{aligned} \mathfrak{W}_{F/k}(\mathfrak{W}_{L/F}(X)) \times_k L &\cong \prod_{\tau \in H} \big(\mathfrak{W}_{L/F}(X) \times_F L \big)^\tau \\ &\cong \prod_{\tau \in H} \Big(\prod_{\sigma \in N} X^\sigma \Big)^\tau. \end{aligned}$$

Since every element g of G has a unique expression $g = \sigma\tau$ with $\tau \in H$ and $\sigma \in N$ we are done. □

We have shown that Weil restriction is well defined for a far larger class of objects than we need, but far smaller than that for which it is usually defined. A more general definition, based upon Milne [**29**] is given below. For a higher level of abstraction, see for example Bosch et al [**5**].

Theorem 5.1.12. *Let $T \to S$ be a finite, faithfully flat morphism of schemes, and suppose that X is a quasi-projective T-scheme. Then there exists a unique S-scheme W such that for any S-scheme Y,*

$$\operatorname{Hom}(W, Y) \cong X(Y \times_S T). \tag{5.6}$$

We shall write Y_T to denote $Y \times_S T$.

If $T = \operatorname{Spec}(F)$ and $S = \operatorname{Spec}(k)$ where F/k is a finite separable extension of fields and X is a variety defined over F, the S-scheme W satisfying (5.6) is the variety defined in (5.1.1) so in the general case of Theorem 5.1.12 it is unambiguous to call the S-scheme W the *Weil restriction* $\mathfrak{W}_{T/S}(X)$. In this case the content of part a) of the following proposition is precisely that of Proposition 5.1.3.

Proposition 5.1.13. *Suppose T, S, X and W are as in* (5.1.12). *Then*

a) *(Universal Mapping Property) There is a T-morphism*

$$\phi : W_T \to X$$

such that if ϕ' is a T-morphism $\phi' : Y_T \to X$, then there exists a unique S-morphism $\rho : Y \to W$ such that $\phi' = \phi \cdot \rho_T$.

b) *If X is a group scheme, then ϕ is a morphism of group schemes.*

c) *If X is smooth over T then W is smooth over S.*

By b), we see that the Weil restriction of an abelian variety is always a group scheme. If F/k is separable, then (5.1) shows that $\mathfrak{W}_{F/k}(A)$ is an abelian variety, since it is isomorphic to an abelian variety over F. If F/k is a purely inseparable field extension and A is an abelian variety defined over F then $\mathfrak{W}_{F/k}(A)$ is not an abelian variety (see Milne [**29**] p. 178 for more details).

When X is a variety with an affine model over F and F/k is normal, we can find an explicit affine model for $\mathfrak{W}_{F/k}(X)$ by considering F as a k-algebra and grouping to find k-rational terms as in the example below.

Example 5.1.14 (Frey [**10**])**.** Let k be a finite field of characteristic $p \equiv 1 \bmod 3$ with $|k| \not\equiv 1 \bmod 9$, and let F/k be a cyclic extension of degree 3. Let $\operatorname{Gal}(F/k) = \langle \tau \rangle$ and let $\{1, u, u^2\}$ be a basis for F as an k-algebra with the property that $u^3 = v$ is in k and $u^9 = 1$. Then given an elliptic curve E/F with affine patch

$$\mathcal{E} : y^2 = x^3 + ax + b, \tag{5.7}$$

we set

$$\begin{aligned} x &:= x_0 + ux_1 + u^2x_2, \\ y &:= y_0 + uy_1 + u^2y_2. \end{aligned}$$

If $\mathcal{E}$ is defined over k then we have, after expanding and grouping powers of u, a system of defining equations

$$\begin{aligned} 2y_0y_1 + vy_2^2 &= 3vx_1^2x_2 + 3x_0^2x_1 + 3vx_0x_2^2 + ax_1, \\ 2y_0y_2 + y_1^2 &= 3vx_1x_2^2 + 3x_0^2x_2 + 3x_0x_1^2 + ax_2, \\ 2vy_1y_2 + y_0^2 &= x_0^3 + vx_1^3 + v^2x_2^3 + 6vx_0x_1x_2 + ax_0 + b, \end{aligned}$$

for an open affine subvariety of $W := \mathfrak{W}_{F/k}(E)$. The map sending (x, y) to (x_0, y_0) embeds E in W as the closed subvariety of W defined by

$$x_1 = x_2 = y_1 = y_2 = 0.$$

In fact, $W \simeq E \times A$ where A/k is the irreducible abelian subvariety of W determined by the condition that if $P = (x, y)$ is a point of $E(L)$ then $(x_0, x_1, x_2, y_0, y_1, y_2)$ is a point of $A(k)$ if and only if

$$P + P^\tau + P^{\tau^2} = 0$$

with respect to the group law on $E(L)$ (see Frey [**10**]). If E is not defined over k then setting

$$\begin{aligned} a &:= a_0 + ua_1 + u^2a_2, \\ b &:= b_0 + ub_1 + u^2b_2 \end{aligned}$$

we have a model for an open affine subvariety of W given by

$$\begin{aligned} 2y_0y_1 + vy_2^2 &= 3vx_1^2x_2 + 3x_0^2x_1 + 3vx_0x_2^2 + a_0x_1 + va_2x_2 + a_1x_0 + b_1, \\ 2y_0y_2 + y_1^2 &= 3vx_1x_2^2 + 3x_0^2x_2 + 3vx_0x_1^2 + a_0x_2 + a_1x_1 + a_2x_0 + b_2, \\ 2vy_1y_2 + y_0^2 &= x_0^3 + vx_1^3 + v^2x_2^3 + 6vx_0x_1x_2 + a_0x_0 + va_1x_2 + va_2x_1 + b_0. \end{aligned}$$

Since the extension F/k is separable, W is an abelian variety which is irreducible over k.

5.2. Weil Restrictions of Abelian Varieties

We now consider the properties of Weil restrictions of abelian varieties, and in particular CM elliptic curves, defined over number fields.

Let F/k be a Galois extension of number fields with discriminant $D_{F/k}$, let A/F be an abelian variety of dimension g, let $W := \mathfrak{W}_{F/k}(A)$, and let L be a Galois extension of k containing F. For any finite prime $\mathfrak{p}$, we let p be the characteristic of $\overline{F}_\mathfrak{p}$. Since $W(k) \cong A(F)$, the map $\phi : W_F \to A$ induces an isomorphism

$$W(L) \cong \mathbb{Z}[\mathrm{Gal}(L/k)] \otimes_{\mathbb{Z}[\mathrm{Gal}(L/F)]} A(L), \tag{5.8}$$

it follows that

$$T_\ell(W) \cong \mathbb{Z}_\ell[G_k] \otimes_{\mathbb{Z}[G_F]} T_\ell(A), \text{ and } V_\ell(W) \cong \mathbb{Q}_\ell[G_k] \otimes_{\mathbb{Q}[G_F]} T_\ell(A),$$

where we write G_k and G_F for $\mathrm{Gal}(k^{alg}/k)$ and $\mathrm{Gal}(F^{alg}/F)$. Therefore the ℓ-adic representation $\rho_\ell(W) : G_k \to \mathrm{Aut}(V_\ell(W))$ is induced from $\rho_\ell(A)$ via the inclusion $G_F \hookrightarrow G_k$.

Proposition 5.2.1. *The Néron model commutes with Weil restriction, that is, for any primes* $\mathfrak{p}$ *of* k *and* $\mathfrak{P}$ *of* F *with* $\mathfrak{P}$ *dividing* $\mathfrak{p}$,

$$\mathfrak{W}_{F_{\mathfrak{P}}/k_{\mathfrak{p}}}(N(A,\mathfrak{P})) = N(\mathfrak{W}_{F/k}(A),\mathfrak{p}).$$

Proof. This is a consequence of the Universal Mapping Properties of the Weil restriction as defined in Proposition 5.1.13 and of the Néron model as in Definition 1.3.7. □

Proposition 5.2.2 (Milne [**29**] Proposition 1)**.** *Let F/k be an extension of number fields, with discriminant $D_{F/k}$, let A be an abelian variety of dimension g defined over F, and let W be the Weil restriction of A from F to k. Then the conductor of W/k is*

$$\mathfrak{f}_W = \mathrm{N}_{F/k}(\mathfrak{f}_A) \cdot D_{F/k}^{2g}.$$

Remark 5.2.3. As a corollary we see that there are no abelian varieties over $\mathbb{Q}$ with good reduction everywhere which arise from Weil restriction to $\mathbb{Q}$, simply because there are no unramified extensions of $\mathbb{Q}$. Fontaine [**8**], and independently Abrashkin, proved that there are no abelian varieties over $\mathbb{Q}$ with good reduction everywhere.

For example, let K be an imaginary quadratic field with discriminant D_K and class number h, and let H be the Hilbert class field of K. The discriminant of H/K is 1, but the discriminant of $H/\mathbb{Q}$ is D_K^h. By Proposition 4.4.3, if D_K is divisible by at least two primes congruent to $3 \bmod 4$ there exists a $\mathbb{Q}$-curve E/H with CM by K good reduction everywhere, and the proposition above shows that $W = \mathfrak{W}_{H/K}(E)$ is an abelian variety with good reduction everywhere over K, but that $\mathfrak{W}_{H/\mathbb{Q}}(E)$ has bad reduction at every prime dividing the discriminant of K. See also Example 5.2.15.

Proposition 5.2.4 (Milne [**29**] Proposition 3)**.** *Let F/k be a normal extension of number fields, let A be an abelian variety defined over F and let W be the Weil restriction of A to k. Then the L-series of A/F, defined in* (1.19)*, is equal to the L-series of W/k.*

5.2.1. Endomorphisms of $\mathfrak{W}_{F/k}(A)$.

Let F/k be a finite normal extension of number fields, let A/F be an abelian variety, and set $W := \mathfrak{W}_{F/k}(A)$ and $G := \mathrm{Gal}(F/k)$. By definition,

$$W_F \cong \prod_{\sigma\in G} A^\sigma,$$

and hence

$$\mathrm{End}_F(W) \cong \prod_{(\sigma,\tau)\in G\times G} \mathrm{Hom}_F(A^\sigma, A^\tau). \tag{5.9}$$

Lemma 5.2.5. *Let* $\Phi = (\phi^{\sigma_1}, \ldots, \phi^{\sigma_{|G|}})$ *be the isomorphism defined in* (5.1). *Then* $\mathrm{End}_k(W) \cong \sum_{\sigma\in G} \mathrm{Hom}_F(A^\sigma, A)\phi^\sigma$.

Proof. Suppose that there is an F-isogeny

$$\iota_\sigma : A^\sigma \longrightarrow A.$$

Then the composite map $\lambda := \iota_\sigma \circ \phi^\sigma$ is a morphism $W_F \to A$ and by Proposition 5.1.3 there exists a unique k-morphism $\zeta : W \to W$ such that $\phi \circ \zeta_F = \lambda$. Hence there is a subring R of $\mathrm{End}_k(W)$ such that

$$R \cong \sum_{\sigma\in G} \mathrm{Hom}_F(A^\sigma, A)\phi^\sigma.$$

Let $\alpha = (\alpha_{\sigma,\tau})$ be an element of $\mathrm{End}_F(W)$. Then for any τ in G,

$$\phi^\tau(\alpha(W)) = \sum_\sigma \alpha_{\sigma,\tau} A^\sigma.$$

Now $\phi^\tau(\alpha(W)) = \phi^\tau(\alpha^\omega(W))$ if and only if

$$\sum_\sigma \alpha_{\sigma,\tau} A^\sigma = \sum_\sigma \alpha_{\sigma,\omega^{-1}\tau} A^\sigma,$$

and hence we see that we need $\alpha_{\tau\sigma,\tau} = \alpha_{\sigma,1}$ for all $\sigma, \tau \in G$. □

This is true regardless of whether A is a k-variety over F. In particular we see that

$$[\mathrm{End}_k^0(W) : \mathrm{End}_F^0(A)] = |\langle \sigma \in G : A \simeq A^\sigma \rangle|, \tag{5.10}$$

and so $[\mathrm{End}_k^0(W) : \mathrm{End}_F^0(A)] = [F : k]$ if and only if A is a k-variety.

5.2.2. Factors of Abelian Varieties. In this section we investigate the special case of Weil restriction from F to k of an abelian variety which is defined over k.

Let A/k be an abelian variety with endomorphism algebra S. Recall that an element ϵ of S is an *idempotent* if $\epsilon = \epsilon^2$. If A is simple, then the only idempotents of S are 1 and 0 and hence

Lemma 5.2.6. *Any factor of* A *is* k*-isogenous to* ϵA *for some idempotent* ϵ *in* S.

By Poincaré's Complete Reducibility Theorem (see Theorem 1.2.5), there exist k-simple pairwise non-isogenous abelian varieties A_i and integers n_i such that A is isogenous over k to the product

$$A_1^{n_1} \times \cdots \times A_r^{n_r}, \tag{5.11}$$

and hence that

$$\mathrm{End}_k^0(A) \cong \mathbb{M}_{n_1}(S_1) \oplus \cdots \oplus \mathbb{M}_{n_r}(S_r),$$

where $S_i := \mathrm{End}_k^0(A_i)$ is a division algebra. For each i there exists an irreducible S-module V_i which is faithful over $\mathbb{M}_{n_i}(S_i)$. Let $\rho_i : S \to \mathrm{End}_{\mathbb{Q}}(V_i)$ be the representation induced by V_i and χ_i the character associated with ρ_i.

Theorem 5.2.7 (Kani and Rosen [**24**] Theorem 1)**.** *Let ϵ be an idempotent of* $\mathrm{End}_F^0(A)$*. Then*

$$\epsilon A \simeq A_1^{m_1} \times \cdots \times A_r^{m_r}, \textit{ where } m_i := \frac{\chi_i(\epsilon)}{\dim_{\mathbb{Q}} S_i}, \ i \in 1, \ldots, r.$$

With A, F and k as above, suppose that F/k is normal with Galois group G. Let $W := \mathfrak{W}_{F/k}(A)$ and let $\phi : W \to A$ be the map defined in Definition 5.1.1. We write R_F for $\mathrm{End}_F(A)$ and define $R_F\langle G\rangle$ to be the twisted group ring with multiplication given by $s\sigma \circ t\tau = st^{\sigma^{-1}}\sigma\tau$.

By Proposition 5.1.3, for any s in R_F and σ in G there exists a unique element $\tilde{s}$ of $\mathrm{End}_k(W)$ such that $\phi\tilde{s} = s\phi$ and a unique element ψ_σ of R_F such that $\phi\psi_\sigma = \phi^{\sigma^{-1}}$. Let $\Psi : R_F\langle G\rangle \to \mathrm{End}_k(W)$ be the map sending

$$\sum_{\sigma \in G} s_\sigma \sigma \mapsto \sum_{\sigma \in G} \tilde{s}_\sigma \psi_\sigma.$$

Let $\Psi_{\mathbb{Q}}$ be the natural extension of Ψ mapping $R_F\langle G\rangle \otimes \mathbb{Q}$ to $\mathrm{End}_k^0(W)$.

Lemma 5.2.8. *Ψ is a ring homomorphism, and $\Psi_{\mathbb{Q}}$ is an isomorphism.*

Proof. See Lemmas 2.2 and 2.3 of Yu [**70**]. □

Where it is unambiguous, we will also write Ψ for $\Psi_{\mathbb{Q}}$.

Theorem 5.2.9 (Yu [**69**] Theorem 2)**.** *Let H be a subgroup of G. Then $\left(\sum_{\sigma \in H} \psi_\sigma\right) \mathfrak{W}_{F/k}(A)$ and $\mathfrak{W}_{F^H/k}(A)$ are isogenous over F.*

From now on, we suppose that $\mathrm{End}_k^0(A) = \mathrm{End}_F^0(A)$ is commutative. This means that $s^\sigma = s$ for all s in R_F and σ in G, and since $\Psi_{\mathbb{Q}}$ is an isomorphism, $\mathrm{End}_k^0(W)$ is commutative if and only if G is an abelian group.

We know that there exist simple abelian varieties $B_1, \ldots, B_r$ defined over k such that

$$W \simeq B_1^{n_1} \times \cdots \times B_r^{n_r},$$

and hence that

$$\mathrm{End}_k^0(W) \cong \mathbb{M}_{n_1}(T_1) \oplus \cdots \oplus \mathbb{M}_{n_r}(T_r)$$

where $T_i = \mathrm{End}_k^0(B_i)$. Let $\{\rho_i\}$ and $\{\chi_i\}$ be defined as in the discussion above Theorem 5.2.7, with W taking the place of A.

Theorem 5.2.10 (Yu [**70**] Theorem A)**.** *Let A be an abelian variety defined over a number field k. Let F be a Galois extension of k and suppose that $\mathrm{End}_k^0(A) = \mathrm{End}_F^0(A) = S$ is a field. Suppose that there are r distinct irreducible characters $\chi_1, \dots, \chi_r$ of $G := \mathrm{Gal}(F/k)$ over S, corresponding to representations $\rho_1, \dots, \rho_r$. Then the abelian varieties*

$$B_i := \Psi\left(\frac{1}{|G|}\sum_{\sigma\in G}\rho_i(\sigma^{-1})^T\sigma\right)W^{\chi_i(1)},$$

are simple and pairwise non-k-isogenous and $W = \prod_i B_i^{n_i}$ where

$$n_i = \frac{\chi_i(1)|G|}{\sum_{\sigma\in G}\chi_i(\sigma^{-1})\chi_i(\sigma)}.$$

If G is *abelian* then all the ρ_i are one-dimensional, $\chi_i(1) = 1$ and we have

$$B_i := \Psi\left(\frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma\right)W,$$

and $n_i = 1$.

Corollary 5.2.11. *If A, F, k and W satisfy the conditions of Theorem 5.2.10 then A is isogenous to a simple factor of W:*

$$A \simeq \Psi\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma\right)W.$$

In particular, if F/k is a quadratic extension and A^F is the twist of A by F, then

$$W \simeq A \times A^F.$$

Proposition 5.2.12. *Let E be a $\mathbb{Q}$-curve with CM by an order $\mathcal{O}$ of K, and let $F := \mathbb{Q}(j_E)$ and $H := K(j_E)$. Then E descends to F and $\mathfrak{W}_{H/K}(E)$ descends to $\mathbb{Q}$.*

Proof. The first statement is a special case of Gross [**16**] Theorem 10.1.3. For the second, let $W := \mathfrak{W}_{H/K}(E)$ and $B := \mathfrak{W}_{F/\mathbb{Q}}(E)$. Then $B_H \cong W_H$, so by the uniqueness of Weil restriction, $B_K \cong W$. □

Theorem 5.2.13 (Milne [**29**] Theorem 3)**.** *Suppose that $[F : k] = n$ and $\mathrm{End}_F^0(A)$ contains a commutative subalgebra S such that*

$$[S : S \cap \mathrm{End}_k^0(A)] = n.$$

Then if $T := S \cap \mathrm{End}_k^0(A)$ is a field, $\mathfrak{W}_{F/k}(A)$ is isogenous to A^n.

Example 5.2.14. Let E be an elliptic curve with CM by an order $\mathcal{O}$ of K, and let $F := K(j_E)$ and $k := \mathbb{Q}(j_E)$. Then $\mathrm{End}_F^0(E) = K$ and $\mathrm{End}_k^0(E) = \mathbb{Q}$ and so by Theorem 5.2.13, $\mathfrak{W}_{F/k}(E) \simeq E^2$.

Example 5.2.15. Let E, F and K be as in the previous example and let $W := \mathfrak{W}_{F/K}(E)$. By Proposition 5.2.12, W descends to $\mathbb{Q}$ so by Theorem 5.2.13,

$$\mathfrak{W}_{K/\mathbb{Q}}(W) \simeq W^2,$$

hence by Proposition 5.2.2, D_K divides $\mathfrak{f}_{W/\mathbb{Q}}$.

5.2.3. Abelian Varieties of CM Type. Let A be a simple abelian variety of CM type (K, Φ) with reflex (K', Φ'), let F be a field of definition for A containing K' and let χ_A be the Grössencharacter of A/F. Let k be a subfield of F such that F/k is abelian and suppose that A is a k-variety. We are interested in when the Weil restriction $W := \mathfrak{W}_{F/k}(A)$ is also a simple variety of CM type, and more generally in the structure of the endomorphism algebra $\mathrm{End}_k^0(W)$.

Let $G := \mathrm{Gal}(F/k)$, and for each element σ of G, let ι_σ be an F-isogeny $A^\sigma \to A$, and let u_σ be the k-endomorphism of W associated to $\iota_\sigma \circ \phi^\sigma$ by the Universal Mapping Property. By Lemma 5.2.5,

$$\mathrm{End}_k^0(W) \cong \sum_{\sigma \in G} K \cdot u_\sigma, \tag{5.12}$$

so to understand the structure of $\mathrm{End}_k^0(W)$ we need to know when u_σ and u_τ commute. If A descends to k then by Theorem 5.2.10 and Theorem 5.2.13 W is isogenous to a product of simple abelian varieties B_i and whether the B_i are pairwise non-isogenous depends upon whether or not $\mathrm{End}_k^0(A) = \mathrm{End}_F^0(A)$. By Proposition 1.2.24, the B_i will be pairwise non-isogenous if k contains the reflex field K'. If A is a k-variety of type 1 then we have a similar result.

Theorem 5.2.16. *Let A be a simple abelian variety of CM type (K, Φ) with reflex field K'. Let k be a field containing K' and suppose that F is a finite abelian extension of k such that F is a field of definition for A. Let W be the Weil restriction $\mathfrak{W}_{F/k}(A)$. Then the following are equivalent:*

a) *A is a k-variety of type 1,*
b) *$F(A_{tors})/k$ is abelian,*
c) *The ℓ-adic representation $\rho_\ell(W)$ is abelian for all ℓ,*
d) *There exist CM fields T_i containing K such that*

$$\sum [T_i : K] = [F : k] \textit{ and } \mathrm{End}_k^0(W) \cong \prod T_i.$$

Proof. Let $G_k := \mathrm{Gal}(k^{alg}/k)$ and $\rho_\ell := \rho_\ell(W)$. The equivalence between parts a) and b) is given by Theorem 2.3.12. The equivalence of b) and c) follows from the definitions as by (5.8) b) holds if and only if $F(W_{tors})/k$ is abelian and

$$\mathrm{Gal}(F(W_{tors})/k) = \lim_{n \to \infty} \mathrm{Gal}(F(W[n])/k),$$

and

$$\prod_{\ell} \rho_\ell(G_k) \cong \varprojlim_{n} \mathrm{Gal}(F(W[n])/k).$$

It remains to prove the equivalence of d) with a), b) and c). If d) holds then W is the product of simple pairwise non-isogenous abelian varieties B_i of CM type and that ρ_ℓ is abelian is a consequence of the fact that each $\rho_\ell(B_i)$ is abelian, hence d) implies c). To show that c) implies d), let $n := [F : k]$, $K_\ell := K \otimes \mathbb{Q}_\ell$ and $k_\ell := k \otimes \mathbb{Q}_\ell$ and consider subalgebras of $\mathrm{End}_{k_\ell}(V_\ell(W)) \cong \mathbb{M}_n(K_\ell)$. Define R to be the image of $\rho_\ell(K[G_k])$ in $\mathrm{End}_{k_\ell}(V_\ell(W))$.

Considering the action of the quotient group $\mathrm{Gal}(F/k)$ on $V_\ell(W)$, we see that R has dimension n over K_ℓ. By c) R is commutative, hence R must be its own commutator in $\mathrm{End}_{k_\ell}(V_\ell(W))$. Now $\mathrm{End}_k(W) \otimes K_\ell$ is also a K_ℓ-algebra of rank n by (5.10) and by Lemma 5.2.5 commutes with R so

$$\mathrm{End}_k(W) \otimes K_\ell \cong R.$$

Now R is a commutative semisimple algebra of dimension n which implies d). □

Remark 5.2.17. In Théorème 4.1 of [**13**], Goldstein and Schappacher prove this theorem for elliptic curves with $k = K = K'$ and F a finite abelian extension of K containing the Hilbert class field of K. Nakamura [**33**] noted that one could take k to be any intermediate field $K \subseteq k \subseteq F$.

In the special case that A descends to k, Theorem 5.2.16 shows that the simple factors B_i of W, which we knew from Theorem 5.2.10 to be pairwise non-isogenous, are of CM type.

Let F and k be as in Theorem 5.2.16, let A be a k-variety and let $W := \mathfrak{W}_{F/k}(A)$. Let p be a rational prime which is unramified in $F/\mathbb{Q}$ and at which A has good reduction, suppose that $\mathfrak{p}$ is a degree 1 prime of k dividing p, and let $\sigma := (F/k; \mathfrak{p})$. Let $\mathfrak{P}$ be a prime of F dividing $\mathfrak{p}$. As in Section 2.4 we may choose ι_σ to be the isogeny whose reduction modulo $\mathfrak{P}$ is the pth power Frobenius, and hence by (2.17) and (2.18),

$$\chi_A(\mathfrak{P}) = u_\sigma^n.$$

where n is the order of σ. If A is a k-variety of type 1, it follows that

$$\chi_A(\mathfrak{P}) = \chi(\mathfrak{p})^n \text{ where } \chi_A = \chi \circ \mathrm{N}_{F/k},$$

hence $u_\sigma = \zeta_n \chi(\mathfrak{p})$ for some nth root of unity ζ_n which is independent of $\mathfrak{p}$.

Suppose that there exists a k-variety B of type 1 and a quadratic extension of L/F and that $A = B^L$. Let ϵ be the class of L/F in $H^2(F/k, \pm 1)$.

Since $\chi_B = \phi_L \chi_A$, with notation as in Theorem 3.2.3 we have

$$u_\sigma^n = \phi_L(\mathfrak{P})\chi_A(\mathfrak{P}) = \epsilon^*(\sigma)\chi_A(\mathfrak{P}) \tag{5.13}$$

and

$$\begin{aligned} u_\sigma u_\tau &= \phi_L(\gamma_{\sigma,\tau}) u_\tau u_\sigma \\ &= \epsilon_*(\sigma,\tau) u_\tau u_\sigma. \end{aligned} \tag{5.14}$$

Supposing that k is a CM field, let $k_0 := k^{\langle\rho\rangle}$ be the maximal real subfield of k, and suppose that F/k_0 is normal and that A is a k_0-variety. Then by Proposition 10 of Shimura [**55**], W descends to k_0 and

$$\mathrm{End}^0_{k_0}(W) \cong \sum_{\sigma \in G} (u_\sigma + u_{\sigma\rho}) k_0.$$

If $A = A^\rho$ then $u_\sigma^\rho = u_{\sigma\rho}$ hence, if A is a k-variety of type 1 then

$$\chi(\mathfrak{p}^\rho) = \chi(\mathfrak{p})^\rho. \tag{5.15}$$

and $\mathrm{End}^0_{k_0}(W)$ is real. By Proposition 4.2.11, Equation (5.15) holds for all primes $\mathfrak{p}$ of k coprime to $\mathfrak{f}_\chi$ if and only if χ is a canonical Hecke character of $\mathfrak{I}_k$.

Proposition 5.2.18. *Let A/F and B/F be abelian varieties of CM type (K, Φ) which are k-varieties. Then if A and B are k-equivalent,*

$$\mathrm{End}^0_k(\mathfrak{W}_{F/k}(A)) \cong \mathrm{End}^0_k(\mathfrak{W}_{F/k}(B))$$

and if $\mathrm{Aut}(A) = \{\pm 1\}$ and A and B are of k-type 1 then the converse holds.

Proof. Suppose that A and B are k-equivalent. Then $B = A^L$ for some quadratic extension L/F which represents the trivial class in $H^2(F/k, \pm 1)$ and the claim follows from (5.13) and (5.14) since $\epsilon_* = \epsilon^* = 1$.

If $\mathrm{Aut}(A) = \{\pm 1\}$ then B is the twist of A by some quadratic extension L/F and if A and B are both of k-type 1 then L/k is abelian, hence $\epsilon_* = 1$. Now if $\mathrm{End}^0_k(\mathfrak{W}_{F/k}(A)) \cong \mathrm{End}^0_k(\mathfrak{W}_{F/k}(B))$ then we must have $\epsilon^*(\sigma) = 1$ for every element σ of G such that the order of σ is a power of two, which implies that ϵ is trivial. □

Remark 5.2.19. In dimension 1 this result is due to Nakamura [**34**].

5.3. Endomorphisms of Weil Restrictions of $\mathbb{Q}$- and K-Curves

Let K be an imaginary quadratic field and let E/F be an elliptic curve with CM by an order $\mathcal{O}$ of K. Let k be a number field containing K and suppose that F is a finite abelian extension of k which contains the ring class field of $\mathcal{O}$. By Theorem 5.2.16 if E is a k-curve of type 1 then $W := \mathfrak{W}_{F/k}(E)$ is a product of simple non-k-isogenous abelian varieties of CM type and hence $\mathrm{End}_k^0(W)$ is commutative. If $\mathcal{O} = \mathcal{O}_K$ and F is the Hilbert class field of K then there is a stronger result.

Proposition 5.3.1 (Nakamura [**33**] Theorem 2)**.** *Let K be an imaginary quadratic field and let H be the Hilbert class field of K. If E/H is a k-curve of type 1 with CM by $\mathcal{O}_K$ then $W := \mathfrak{W}_{H/k}(E)$ is a simple abelian variety of CM type.*

Proof. By Theorem 5.2.16 it is enough to show that $\mathrm{End}_k^0(W)$ is a field of degree $2[H : k]$. Let C be the subgroup of $Cl(K)$ corresponding to $\mathrm{Gal}(H/k)$ via the Artin mapping. For any prime p dividing $|C|$ we let C_p be the Sylow-p-subgroup of C. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be a set of independent generators of C_p coprime to $D_K \cdot \mathrm{N}_{H/\mathbb{Q}}(\mathfrak{f}_E)$, let $\sigma_i := (H/k; \mathfrak{p}_i)$ and let $u_i := u_{\sigma_i}$ be as in (5.12). Setting r to be the integer such that $|C_p| = p^r$, and

$$T_p := \prod_{i=1}^{m} K(u_i),$$

the claim of the theorem is that $[T_p : K] = p^r$ for each p dividing h.

Let K_p denote the extension of K obtained by adjoining the group of p^rth roots of unity. Now T_pK_p/K_p is a Kummer extension of degree p^r, and if p is odd we have the desired result because the embedding of $K^*/(K^*)p^r$ into $K_p^*/(K_p^*)^{p^r}$ is injective. The case when $p = 2$ is similar, see Nakamura [**33**] for details. □

Let $\mathcal{O}$ be any order of K, let $f_{\mathcal{O}}$ be the conductor of $\mathcal{O}$ and let $E/H_{\mathcal{O}}$ be a $\mathbb{Q}$-curve with CM by $\mathcal{O}$. By Proposition 4.1.11 there exists an elliptic curve E_m with CM by $\mathcal{O}_K$ such that E and E_m are isogenous over $H_{\mathcal{O}}$, and E descends to a K-curve over H.

For a normal subfield k of $H_{\mathcal{O}}$, let $W(k) := \mathfrak{W}_{H_{\mathcal{O}}/k}(E)$. By Proposition 4.1.11 and the Universal Mapping Property, $W(k)$ and $\mathfrak{W}_{H_{\mathcal{O}}/k}(E_m)$ are isogenous, and hence have isomorphic endomorphism algebras.

If k contains H then $\mathrm{Gal}(F/k)$ is abelian and applying Theorem 5.2.10 to E_m we see that $W(k)$ is a product of simple non-isogenous varieties of CM type, and in particular, that it has a factor isogenous to E_m.

Suppose that k is contained in H. By Lemma 5.1.11, if there exists a subfield F of $H_{\mathcal{O}}$ containing H such that

$$\mathrm{Gal}(H_{\mathcal{O}}/k) \cong \mathrm{Gal}(H_{\mathcal{O}}/F) \times \mathrm{Gal}(F/k),$$

then

$$W(k) \simeq \mathfrak{W}_{F/k}(\mathfrak{W}_{H_{\mathcal{O}}/F}(E)) \simeq \mathfrak{W}_{F/k}(\mathfrak{W}_{H_{\mathcal{O}}/F}(E_m))$$

and $W(k)$ contains a factor isogenous to $\mathfrak{W}_{F/k}(E_m)$. Suppose no such field F exists. By Corollary 2.2.9, this means that $f_{\mathcal{O}}$ must be divisible only primes dividing $2D_K$, and that $D_{\mathcal{O}}$ must not be divisible by 32 since otherwise the genus field of $H_{\mathcal{O}}$ is not contained in H. But then, if p^2 divides $D_{\mathcal{O}}$, where p is some odd prime dividing D_K then $H_{\mathcal{O}}$ contains a cyclic extension of H of order p, and there is a similar case if D_K is odd and $D_{\mathcal{O}}$ is even. The only possibility remaining is

$$D_K = -4d, \text{ and } D_{\mathcal{O}} = -16d \text{ with } d \equiv 1 \bmod 4. \tag{5.16}$$

In Example 5.4.3 we shall see that in this case $\mathrm{End}^0_K(W(K))$ is sometimes but not always a field.

Theorem 5.3.2 (Nakamura [**33**] Theorem 3)**.** *Let E be a K-curve defined over H with CM by $\mathcal{O}_K$. Let $W := \mathfrak{W}_{H/K}(E)$ and set $n := r_2(H/K)$ and $h := h_K$. Then there are two possibilities*

a) $\mathrm{End}^0_K(W)$ *is a field of degree h over K.*
b) *The centre of* $\mathrm{End}^0_K(W)$ *is a field Z_K of degree $h/2^{2m}$ over K for some m with $1 \leq m \leq \lfloor \frac{n}{2} \rfloor$, and* $\mathrm{End}^0_K(W) \cong \mathbb{M}_{2^{m-1}}(R_0)$*, where R_0 is a quaternion algebra over Z_K.*

Proof. If E is of type 1, then this is a restatement of Proposition 5.3.1. If E is of type 2 then by (5.14) and Lemma 3.2.8,

$$\mathrm{End}^0_K(W) \cong R_1 \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R_m,$$

where each R_i is a quaternion algebra over Z_K. Therefore $\mathrm{End}^0_K(W)$ is isomorphic to $\mathbb{M}_{2^{m-1}}(R_0)$ for some quaternion algebra R_0 over Z_K. The algebra R_0 is the quaternion algebra which ramifies at each prime $\mathfrak{p}$ of Z_K which is ramified in an odd number of the R_i.

□

Remark 5.3.3. If R_0 is a *split* quaternion algebra over Z_K then $\mathrm{End}^0_K(W) \cong \mathbb{M}_{2^m}(Z_K)$. In particular if $m = 1$ then W/K is simple only if R_0 is a ramified quaternion algebra.

Theorem 5.3.4 (Nakamura [**34**] Theorem 3)**.** *Let E be a $\mathbb{Q}$-curve defined over H with CM by $\mathcal{O}_K$. Let $W := \mathfrak{W}_{H/K}(E)$, as before and let $Z_{\mathbb{Q}}$ be the centre of* $\mathrm{End}^0_{\mathbb{Q}}(W)$*. Then the possibilities for* $\mathrm{End}^0_{\mathbb{Q}}(W)$ *and $Z_{\mathbb{Q}}$ are precisely those of Theorem 5.3.2 with K replaced by $\mathbb{Q}$.*

If E is a $\mathbb{Q}$-curve of type 2 and $\mathrm{End}^0_{\mathbb{Q}}(W)$ is a matrix algebra over a ramified quaternion algebra $R_{\mathbb{Q}}$, then the natural question is whether or not the quaternion algebra $R_K := R_{\mathbb{Q}} \otimes_{\mathbb{Z}} K$ is split.

As $R_{\mathbb{Q}}$ may only be ramified at $2, \infty$ and rational primes dividing D_K, it follows that R_K will be ramified only if there are at least two primes of Z_K dividing 2, however this is not a sufficient condition.

In [**33**] Nakamura shows that if $D_K = -pqr$ for some rational primes $p \equiv 3 \bmod 4$ and $q, r \equiv 1 \bmod 4$ and $r_4(H/K) = 0$ then there exists a

$\mathbb{Q}$-curve E such that R_K is ramified if and only if 2 splits in K and

$$\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = -1.$$

The quadratic fields with discriminants -255 and -455, which have class numbers 12 and 20 respectively, are examples satisfying these conditions.

Example 5.3.5. Suppose that K is the quadratic field with discriminant $-231 = -3 \cdot 7 \cdot 11$. Then $h_K = 12$, $\mathrm{Gal}(F_g/K) \cong C_2^{\times 2}$ and

$$G_K^- := \{\lambda_3,\ \lambda_7,\ \lambda_{11},\ \lambda_3\lambda_7\lambda_{11}\}.$$

By Propositions 4.1.1 and 4.1.3 the $\mathbb{Q}$-curves E_λ of type 1 with good reduction outside D_K will have characters of the form $\varphi \circ \mathrm{N}_{H/K}$ where φ is a Hecke character of $\mathfrak{I}_K$ such that the restriction of φ to U_K is equal to an element λ in G_K^-. Taking $(-3, 21)$ as a partial decomposition of D_K as in Lemma 3.3.2, we obtain a dihedral extension of L/K containing F_g, and twisting by this extension gives us $\mathbb{Q}$-curves of type 2.

Let $F_Z := \mathbb{Q}(x)$ where $x^3 - 12x + 5 = 0$. The endomorphism fields $\mathrm{End}^0_{\mathbb{Q}}(\mathfrak{W}_{H/K}(E_\lambda))$ are

$$F_Z(\sqrt{-11}, \sqrt{7}),\ F_Z(\sqrt{-3}, \sqrt{11}),\ F_Z(\sqrt{3}, \sqrt{-7}),\ F_Z(\sqrt{77}, \sqrt{33}).$$

If $E := E_\lambda^L$ for some $\lambda \in G_K^-$ then in three cases $R_{\mathbb{Q}}$ is a split quaternion algebra over F_Z and in the fourth it is ramified at $(2, \infty)$. Since 2 splits in K, this algebra remains ramified over $F_Z K$.

5.4. Computing Endomorphism Algebras

5.4.1. Curves of Type 1. Let K be an imaginary quadratic field, let E/H be a $\mathbb{Q}$-curve of type 1 with complex multiplication by $\mathcal{O}_K$ and let $W := \mathfrak{W}_{F/K}(E)$ where F/K is a finite abelian extension containing H. Suppose that $\chi_E := \chi \circ \mathrm{N}_{H/K}$. In order to calculate $\mathrm{End}^0_{\mathbb{Q}}(W)$ we need to find minimal polynomials for

$$\chi(\mathfrak{p}) + \chi(\mathfrak{p}^\rho)$$

for $\mathfrak{p}$ in S where $\{(F/K; \mathfrak{p}) : \mathfrak{p} \in S\}$ generates $\mathrm{Gal}(F/K)$ and each prime in S is coprime to D_K. Suppose that $(F/K; \mathfrak{p})$ has order n. Then $\mathfrak{p}^n$, $(\mathfrak{p}^\rho)^n$ and $\mathfrak{p}\mathfrak{p}^\rho$ are principal, and expanding $(\chi(\mathfrak{p}) + \chi(\mathfrak{p}^\rho))^n$ and rearranging, we obtain a polynomial $f_{n,\chi}$ of degree n with coefficients in $\mathbb{Q}$. For clarity of notation we write $\bar{\mathfrak{p}}$ for $\mathfrak{p}^\rho$ in this section.

Example 5.4.1. Suppose $n = 2$. Then

$$(\chi(\mathfrak{p}) + \chi(\bar{\mathfrak{p}}))^2 = \chi(\mathfrak{p}^2) + \chi(\bar{\mathfrak{p}}^2) + 2\chi(\mathfrak{p}\bar{\mathfrak{p}}),$$

hence

$$f_{2,\chi}(X) := X^2 - (\chi(\mathfrak{p}^2) + \chi(\bar{\mathfrak{p}}^2) + 2\chi(\mathfrak{p}\bar{\mathfrak{p}})). \tag{5.17}$$

If $n = 4$ then

$$\begin{aligned}(\chi(\mathfrak{p}) + \chi(\bar{\mathfrak{p}}))^4 &= \chi(\mathfrak{p}^4) + \chi(\bar{\mathfrak{p}}^4) + 4\chi(\mathfrak{p}\bar{\mathfrak{p}})(\chi(\mathfrak{p})^2 + \chi(\bar{\mathfrak{p}})^2) + 6\chi(\mathfrak{p}\bar{\mathfrak{p}})^2 \\ &= \chi(\mathfrak{p}^4) + \chi(\bar{\mathfrak{p}}^4) + 4\chi(\mathfrak{p}\bar{\mathfrak{p}})(\chi(\mathfrak{p}) + \chi(\bar{\mathfrak{p}})^2 - 2\chi(\mathfrak{p}\bar{\mathfrak{p}})^2,\end{aligned}$$

hence

$$f_{4,\chi}(X) := X^4 - 4\chi(\mathfrak{p}\bar{\mathfrak{p}})X^2 + 2\chi(\mathfrak{p}\bar{\mathfrak{p}})^2 - \chi(\mathfrak{p}^4) - \chi(\bar{\mathfrak{p}}^4). \tag{5.18}$$

Similarly

$$f_{3,\chi}(X) = X^3 - 3\chi(\mathfrak{p}\bar{\mathfrak{p}})X - \chi(\mathfrak{p}^3) - \chi(\bar{\mathfrak{p}}^3), \tag{5.19}$$

and in general we observe that every power of X with non-zero coefficients in $f_{n,\chi}$ has the same parity as n. If $\mathrm{Gal}(F/K)$ contains elements of order greater than 2 then $\mathrm{End}^0_{\mathbb{Q}}(W)$ will not usually be normal.

Example 5.4.2. Let K be the quadratic field with discriminant $D_K = -759 = -3 \cdot 11 \cdot 23$ and Hilbert class field H. The class group of K is isomorphic to $C_2 \times C_3 \times C_4$ and is generated by primes $\mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_4$ lying over 389, 31 and 29 which have orders 2, 3 and 4 respectively.

There are four $\mathbb{Q}$-equivalence classes of $\mathbb{Q}$-curves with CM by $\mathcal{O}_K$ defined over H corresponding as in Example 5.3.5 to the odd quadratic characters:

$$\lambda_3,\ \lambda_{11},\ \lambda_{23},\ \lambda_3\lambda_{11}\lambda_{23}$$

of $\mathfrak{I}_K$. The character

$$\lambda_{11}\lambda_{23} \circ \mathrm{N}_{H/K}$$

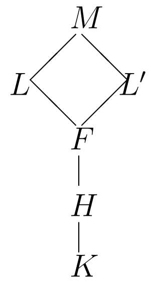
corresponds to an extension of $L/H/K$ of type $C_2^{\times 2} \times C_{12}$ and the characters $\lambda_3\lambda_{23} \circ \mathrm{N}_{H/K}$ and $\lambda_3\lambda_{11} \circ \mathrm{N}_{H/K}$ to extensions of type $C_4 \times C_{12}$, hence the curves corresponding to λ_3 and λ_{11} are K-equivalent to those corresponding to $\lambda_3\lambda_{11}\lambda_{23}$ and λ_{23} respectively.

Evaluating the polynomials $f_{j,\chi}(x)$ at $\mathfrak{p}_j$ for $j \in \{2, 3, 4\}$ we find (after removing square factors for $j = 2$),

λ	$f_{2,\chi}$	$f_{3,\chi}$	$f_{4,\chi}$
λ_3	$x^2 + 23$	$x^3 - 93x + 208$	$x^4 + 116x^2 + 2352$
λ_{11}	$x^2 - 23$	$x^3 - 93x - 208$	$x^4 + 116x^2 + 1012$
λ_{23}	$x^2 + 33$	$x^3 - 93x - 208$	$x^4 - 116x^2 + 1012$
$\lambda_3\lambda_{11}\lambda_{23}$	$x^2 - 33$	$x^3 - 93x + 208$	$x^4 - 116x^2 + 2352$

Let $F_{j,\chi}$ denote the extension of $\mathbb{Q}$ with defining polynomial $f_{j,\chi}(x)$. The fields $F_{3,\chi}$ are isomorphic for all χ. The fields $F_{4,\chi}$ are non-normal with quadratic subfields with discriminants 253, 12, 12 and 253 respectively. When $\lambda = \lambda_3\lambda_{11}\lambda_{23}$ all the fields $F_{j,\chi}$ are real.

FIGURE 2. Example 5.4.3



$\mathrm{Gal}(M/K) \cong C_2^{\times 2} \times C_8$

$\mathrm{Gal}(L/K) \cong C_2 \times C_8$

$\mathrm{Gal}(F/K) \cong C_2 \times C_4$

$\mathrm{Gal}(H/K) \cong C_2 \times C_2$

Example 5.4.3. Let $K = \mathbb{Q}(\sqrt{-21})$ and let H be the Hilbert class field of K so that $D_K = -84$ and $\mathrm{Gal}(H/K) \cong C_2 \times C_2$. Let F be the ring class field of conductor 2. The extension F/H is quadratic and $\mathrm{Gal}(F/K) \cong C_2 \times C_4$. The ring class field M of conductor 8 has Galois group isomorphic to $C_2^{\times 2} \times C_8$ over K. Let L be one of the subfields of M such that $\mathrm{Gal}(L/K) \cong C_2 \times C_8$ (see Figure 2).

The $\mathbb{Q}$-curves E of type 1 with complex multiplication by $\mathcal{O}_K$ and Grössencharacters in $\Gamma_1(K)$ correspond to the quadratic characters:

$$\lambda_3,\ \lambda_{-4}\lambda_3,\ \lambda_7,\ \lambda_{-4}\lambda_7$$

of $\mathfrak{I}_K$. By Proposition 4.1.6 every $\mathbb{Q}$-curve of type 1 with CM by $\mathcal{O}_K$ is $\mathbb{Q}$-equivalent to such a curve. Since $\lambda_{-4}\lambda_3\lambda_7$ is a Dirichlet character of $\mathfrak{I}_K$ there are two K-equivalence classes of $\mathbb{Q}$-curves. Setting $W_0 := \mathfrak{W}_{H/K}(E)$ where E runs through a set of representatives of $\Gamma_1(K)$ we find:

λ	$\mathrm{End}^0_{\mathbb{Q}}(W_0)$	$\mathrm{End}^0_K(W_0)$
λ_3	$\mathbb{Q}(\sqrt{-2}, \sqrt{-14})$	$K(\sqrt{-2}, \sqrt{-14})$
$\lambda_{-4}\lambda_3$	$\mathbb{Q}(\sqrt{-42}, \sqrt{-6})$	$K(\sqrt{-42}, \sqrt{-6})$
λ_7	$\mathbb{Q}(\sqrt{2}, \sqrt{-6})$	$K(\sqrt{-42}, \sqrt{-6})$
$\lambda_{-4}\lambda_7$	$\mathbb{Q}(\sqrt{42}, \sqrt{-14})$	$K(\sqrt{-2}, \sqrt{-14})$

Since there are no canonical Hecke characters of $\mathfrak{I}_K$, none of these fields is real.

The extension of F/H has Dirichlet character $\lambda_{-4} \circ \mathrm{N}_{H/K}$, so the four isogeny classes of $\mathbb{Q}$-curves over H combine into two over F. On the other hand two classes of K-curves, corresponding to the characters ν and $\nu\lambda_3\lambda_7$, become $\mathbb{Q}$-curves over F. These curves are isogenous to elliptic curves with CM by $\mathcal{O}$ where $\mathcal{O}$ is the order of K with discriminant $D_{\mathcal{O}} := 4D_K$. Up to $\mathbb{Q}$-equivalence these are the only $\mathbb{Q}$-curves with CM by $\mathcal{O}_K$ defined over

F. Setting $W_1 := \mathfrak{W}_{F/K}(E)$ we find:

λ	$\mathrm{End}^0_{\mathbb{Q}}(W_1)$	$\mathrm{End}^0_K(W_1)$
λ_3	$\mathbb{Q}(\sqrt{-42}, \sqrt{-2}, \sqrt{7})$	$H(\sqrt{2})$
λ_7	$\mathbb{Q}(\sqrt{-42}, \sqrt{2}, \sqrt{-6})$	$H(\sqrt{2})$
ν	$K(\sqrt{-3}, \sqrt{-4})$	$H \times H$
$\nu\lambda_3\lambda_7$	$\mathbb{Q}(\sqrt{7}, \sqrt{21}) \times \mathbb{Q}(\sqrt{7}, \sqrt{21})$	$H \times H$

There are two subfields L, L' of M which have Galois group $C_2 \times C_8$ over K. Neither of these are normal over $\mathbb{Q}$. Setting $W_2 := \mathfrak{W}_{L/K}(E)$:

λ	$\mathrm{End}^0_{\mathbb{Q}}(W_2)$	$\mathrm{End}^0_K(W_2)$
λ_3	$H(\sqrt{2})$	$H(\sqrt{2}) \times H(\sqrt{2})$
λ_7	$\mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{2}) \times \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{2})$	$H(\sqrt{2}) \times H(\sqrt{2})$
ν	$H(\sqrt{2})$	$H(\sqrt{2}) \times H(\sqrt{2})$
$\nu\lambda_3\lambda_7$	$\mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{2}) \times \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{2})$	$H(\sqrt{2}) \times H(\sqrt{2})$

5.4.2. Type 2 Curves. Let K be a non-exceptional imaginary quadratic field with discriminant D_K divisible by at least three distinct primes. Let F be an abelian extension of K containing H and let E_0/F and E/F be $\mathbb{Q}$-curves of types 1 and 2 respectively. Let L be the quadratic extension of F such that $E = E_0^L$.

Then, setting $\chi_{E_0} := \chi_0 \circ \mathrm{N}_{F/K}$,

$$\chi_E = \phi_L \cdot \chi_{E_0} = \phi_L \cdot \chi_0 \circ \mathrm{N}_{F/K}.$$

Let S be a subset of $G := \mathrm{Gal}(F/K)$ such that each element σ of S has the properties that the sequence

$$1 \to \mathrm{Gal}(F/F^{\langle\sigma\rangle}) \to G \to \mathrm{Gal}(F^{\langle\sigma\rangle}/K) \to 1$$

splits and that the order of σ is either odd or a power of 2. Since G is abelian, we can further require that S is a generating subset of G.

Since $L/F^{\langle\sigma\rangle}$ is abelian E is of $F^{\langle\sigma\rangle}$-type 1, hence $\chi_E = \chi_\sigma \circ \mathrm{N}_{F/F^\sigma}$ for some Hecke character χ_σ of $\mathfrak{I}_{F^{\langle\sigma\rangle}}$. Moreover there exists a Dirichlet character ϕ_σ of $\mathfrak{I}_{F^{\langle\sigma\rangle}}$ such that $\phi_L = \phi_\sigma \circ \mathrm{N}_{F/F^{\langle\sigma\rangle}}$ hence

$$\chi_\sigma = \phi_\sigma \cdot \chi_0 \circ \mathrm{N}_{F/F^{\langle\sigma\rangle}}. \tag{5.20}$$

Let $\mathfrak{P}$ be a prime of $F^{\langle\sigma\rangle}$ coprime to D_K such that $(F/F^{\langle\sigma\rangle}; \mathfrak{P}) = \sigma$. Let $\mathfrak{Q}$ be a prime of F dividing $\mathfrak{P}$ and let $\mathfrak{p}$ be a prime of K lying under $\mathfrak{P}$.

$$\begin{tikzcd}
F \arrow[d, no head] & \mathfrak{Q} \\
F^{\langle\sigma\rangle} \arrow[d, no head] & \mathfrak{P} \\
K & \mathfrak{p}
\end{tikzcd}$$

Then

$$\chi_E(\mathfrak{Q}) = \chi_\sigma(\mathfrak{P}^n) = \phi_\sigma(\mathfrak{P}^n)\chi_0(\mathfrak{p}^n), \tag{5.21}$$

where n is the order of σ and

$$\chi_\sigma(\mathfrak{P}\overline{\mathfrak{P}}) = \phi_\sigma(\mathfrak{P}\overline{\mathfrak{P}}) \cdot \chi_0(\mathfrak{p}\overline{\mathfrak{p}}), \tag{5.22}$$

so if we can evaluate $\phi_\sigma(\mathfrak{P}^n)$ and $\phi_\sigma(\mathfrak{P}\overline{\mathfrak{P}})$, we can construct a minimal polynomial for $u_\sigma + u_{\sigma\rho}$ as in the previous section. Now $\mathrm{End}^0_{\mathbb{Q}}(W)$ is generated by the elements

$$\{t_\sigma := u_\sigma + u_{\sigma\rho} : \sigma \in S\}$$

and

$$\begin{aligned} t_\sigma t_\tau &= \epsilon_{L*}(\sigma,\tau) t_\tau t_\sigma \\ &= \phi_L(\boldsymbol{\gamma}_{\sigma,\tau}) t_\tau t_\sigma. \end{aligned}$$

Therefore, using the techniques developed in Chapter 3 we can construct endomorphism algebras corresponding to each $\mathbb{Q}$-equivalence class of $\mathbb{Q}$-curves over H.

Example 5.4.4. Let $D_K = -660 = -4\cdot 3\cdot 5\cdot 11$ so that $\mathrm{Gal}(H/K) \cong C_2^{\times 3}$. Let F be the dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{-3}, \sqrt{-11})$ unramified outside 33, and let $L = FH$. By construction the centre of $\mathrm{Gal}(L/K)$ will contain the automorphism σ of H sending $\sqrt{5}$ to $-\sqrt{5}$. Now $\sigma = (H/K; \mathfrak{p})$ where $\mathfrak{p}$ is a prime of K lying over 53, and the remainder of the class group is generated by primes lying over 59 and 83. There are eight $\mathbb{Q}$-equivalence classes of $\mathbb{Q}$-curves of type 1 over H. Since $D_K \equiv 4 \bmod 8$ and $r_4(H/K) = 0$ it follows from Proposition 3.3.23 that $c_4(H/K) = 2$, so there are four K-equivalence classes of $\mathbb{Q}$-curves. Evaluating elements of G_K^+ on generators of $Cl(K)$ we find that

$$\lambda_{-4}\lambda_3\lambda_5\lambda_{11}$$

is a Dirichlet character of $\mathfrak{I}_K$. Let $E := E_\lambda^L$ where E_λ runs through a set of representatives of $\Gamma_1(K)$. The Weil restrictions $\mathfrak{W}_{H/K}(E)$ form two categories depending on whether $Z_{\mathbb{Q}}$ is $\mathbb{Q}(\sqrt{-33})$ or $\mathbb{Q}(\sqrt{33})$:

	k	ramified primes
$a.$	$\mathbb{Q}(\sqrt{33})$	$\mathfrak{p}_2, \mathfrak{p}_2'$
$b.$	$\mathbb{Q}(\sqrt{-33})$	split

where λ is one of

$$\lambda_3,\ \lambda_{-4}\lambda_3,\ \lambda_5\lambda_{11},\ \lambda_{-4}\lambda_5\lambda_{11}$$

in the former case and

$$\lambda_3\lambda_5,\ \lambda_{-4}\lambda_3\lambda_5,\ \lambda_{11},\ \lambda_{-4}\lambda_{11}$$

in the latter.

In Definition 3.2.9 we defined $\mathcal{G}_{H/K}^{(m)}$ to be the subset of fields L in $\mathcal{G}_{H/K}$ such that

$$|\mathrm{Gal}(L/K)/Z(\mathrm{Gal}(L/K))| = 2^m,\ m \geq 0.$$

In the examples above we have considered only twists of type 1 curves by $L \in \mathcal{G}_{H/K}^{(1)}$, but in theory at least it is possible to use the same methods for arbitrary m. We can express any field L in $\mathcal{G}_{H/K}^{(m)}$ as a product of the form

$$L := L_1 \circ \cdots \circ L_m,$$

where L_i belongs to $\mathcal{G}_{H/K}^{(1)}$ for $1 \leq i \leq m$. This decomposition determines a set of mutually disjoint pairs σ_i, τ_i such that $\epsilon_{i*}(\sigma_i, \tau_i) = -1$. By Theorem 3.2.3, $\epsilon_{L*} = \prod_i \epsilon_{i*}$, so the commutator relations of the endomorphism algebra may be derived from those of the L_i in a manner corresponding to the previous example.

The computational difficulties are therefore chiefly those of working with large fields since if $\mathcal{G}_{H/K}^{(2)}$ is non-empty then K must have class number at least 16, and any field L in $\mathcal{G}_{H/K}$ will have absolute degree at least 64.

Remark 5.4.5. For the general case of Weil restrictions of abelian varieties it may not always be possible to break the twist down in this way, since it is not always true that $\mathcal{G}_{F/k}^{(1)}$ contains a basis for $\mathcal{G}_{F/k}^s/\mathcal{A}_{F/k}^s$. See Massy [**27**] p. 525 for an example.

5.5. Abelian Surfaces and Weil Restrictions

5.5.1. Abelian Surfaces as Weil Restrictions: Biquadratic CM fields.

Let F be a quartic CM field such that $\mathrm{Gal}(F/\mathbb{Q}) \cong C_2^{\times 2}$. The reflex field K of any CM type (F, Ψ) is an imaginary quadratic subfield of F, and consequently if A/k is an abelian variety of type (F, Ψ), then A splits into a product $E_1 \times E_2$ of elliptic curves with CM by K over some quadratic extension k'/k. We are interested in the cases where

$$A \cong \mathfrak{W}_{k'/k}(E)$$

for some elliptic curve E.

Suppose that E is an elliptic curve with CM by K. Let H be the Hilbert class field of K, and let σ be an element of $\mathrm{Gal}(H/K)$ of order 2. If $W = \mathfrak{W}_{H/H^{\langle\sigma\rangle}}(E)$, then W_H is isomorphic to $E \times E^\sigma$ and $\mathrm{End}^0_K(W)$ is isomorphic to $K(u_\sigma)$ if E is H-isogenous to E^σ and to K otherwise.

Let F/k be a finite Galois extension of number fields. As in Section 3.1 we say that F/k *satisfies Albert's condition* if -1 belongs to the norm group $\mathrm{N}_{F/M}(M^*)$ for every quadratic subfield M of F containing k. Recall that by Theorem 3.1.8, F/M satisfies Albert's condition if and only if there exists a quadratic extension L/F cyclic over M and that by (3.4), there exists a quadratic extension L/F cyclic over M and normal over $\mathbb{Q}$ if and only if $c_4(F/M) = 1$.

Proposition 5.5.1. *Let D_1 and D_2 be negative discriminants such that if $4|D_2$ then $(D_2/4)|D_1$ and if $D_2 \not\equiv 4 \bmod 8$ then $D_2|D_1$. Let K_1 and K_2 be the quadratic fields with discriminants D_1 and D_2 respectively, let H be the Hilbert class field of K_1 and set $F := K_1K_2$.*

Then if H/K_1 satisfies Albert's condition there exists an elliptic curve E with CM by K_1 and an element σ of $\mathrm{Gal}(H/K_1)$ such that $\mathfrak{W}_{H/H^{\langle\sigma\rangle}}(E)$ is an abelian variety of type (F, Ψ), where Ψ is induced from K_1. Moreover if $c_4(H/H^{\langle\sigma\rangle}) = 1$, and K_1 is non-exceptional (resp. exceptional) then there exists a $\mathbb{Q}$-curve (resp. K_1-curve) of type 1 with this property.

Proof. Suppose that K is an imaginary quadratic field such that H/K satisfies Albert's condition and let E/H be a K-curve of type 1 with CM by $\mathcal{O}_K$. For any σ in $\mathrm{Gal}(H/K)$ of order 2, the Weil restriction $W_\sigma := \mathfrak{W}_{H/H^{\langle\sigma\rangle}}(E)$ has endomorphism algebra isomorphic to $K(\sqrt{d_\sigma})$ for some integer d_σ dividing D_K. If D_σ is the discriminant of $\mathbb{Q}(\sqrt{d_\sigma})$, then D_K and D_σ satisfy the conditions of the proposition on D_1 and D_2. Let σ run through a set of independent generators of $\mathrm{Gal}(H/K)[2]$. Since each field $K(\sqrt{D_\sigma})$ is contained in $\mathrm{End}_K(\mathfrak{W}_{H/K}(E))$, which is a field, they must all be distinct. Since Hecke characters are homomorphisms, $K(\sqrt{D_{\sigma\tau}}) = K(\sqrt{D_\sigma D_\tau})$ and hence half the possible values of D_2 are realized as D_σ for some $\sigma \in \mathrm{Gal}(H/K)$. Now suppose that there exists some quadratic extension L/H such that L/H^σ is cyclic. Then by (5.21) the endomorphism algebra of $\mathfrak{W}_{H/H^{\langle\sigma\rangle}}(E^L)$ is isomorphic to $K(\sqrt{-d_\sigma})$.

Suppose that $c_4(H/H^{\langle\sigma\rangle}) = 1$. We can then choose L to be a normal extension of $\mathbb{Q}$ which means that E^L is a K-curve. If K is non-exceptional, then we can choose E to be a $\mathbb{Q}$-curve, in which case E^L is a $\mathbb{Q}$-curve. □

Example 5.5.2. Suppose that $D_1 = -195$ and $D_2 = -39$, so that $F = \mathbb{Q}(\sqrt{-195}, \sqrt{-39})$. Let $K := K_1$ and $H := H_K$. The class number of $\mathcal{O}_K$ is 4 and the elements of $\mathrm{Gal}(H/K)$ of order 2 are

$$\sigma_i := (H/K; \mathfrak{p}_i),\ i = 1, 2, 3$$

where $\mathfrak{p}_1, \mathfrak{p}_2$ and $\mathfrak{p}_3$ are primes of K dividing $p_1 := 7, p_2 := 11$ and $p_3 := 17$ respectively. Suppose that E is the $\mathbb{Q}$-curve of type 1 with CM by $\mathcal{O}_K$ with Grössencharacter corresponding to $\lambda_3\lambda_5\lambda_{13}$ and let $M = H^{\langle\sigma_2\rangle}$. Then

$$\mathbb{Q}(u_{\sigma_2} + u_{\sigma_2\rho}) = \mathbb{Q}(\sqrt{5}),$$

and hence

$$\mathrm{End}^0_M(\mathfrak{W}_{H/M}(E)) = K(\sqrt{5}) = F.$$

As $c_4(H/K)$ is maximal, we can deal with the other negative discriminants D_2 dividing D_1 or $4D_1$ in a similar manner to find $\mathbb{Q}$-curves E_λ and fields $M := H^{\langle\sigma_i\rangle}$ such that

$$\mathrm{End}^0_M(\mathfrak{W}_{H/M}(E_\lambda)) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$$

as indicated by the table below:

D_2	p_i	λ
-39	11	$\lambda_3\lambda_{13},\ \lambda_3\lambda_5\lambda_{13}$
-15	7	$\lambda_3,\ \lambda_3\lambda_5\lambda_{13}$
-3	17	$\lambda_3\lambda_5,\ \lambda_3\lambda_5\lambda_{13}$
-260	17	$\lambda_3,\ \lambda_3\lambda_{13}$
-52	7	$\lambda_3\lambda_5, \lambda_3\lambda_{13}$
-20	11	$\lambda_3,\ \lambda_3\lambda_5$

Next we consider an example where c_4 is non-maximal.

Example 5.5.3. Let $D_1 = -651 = -3 \cdot 7 \cdot 31$ and let H be the Hilbert class field of K_1. The class group of K_1 is isomorphic to $C_2 \times C_4$ and since D_1 is odd $c_4(H/K_1) = 2 - r_4(H/K_1) = 1$ by Proposition 3.3.23. The elements of order 2 in $\mathrm{Gal}(H/K_1)$ correspond to primes of K_1 dividing 13, 61 and 67. Looking at the quadratic extensions of H abelian over K_1 we find representatives for all possible values of D_2 except $D_2 = -868$. Let $\mathfrak{p}$ be a prime of K_1 dividing 61, and let M be the decomposition field of $\mathfrak{p}$ in H. Every strictly admissible extension of H abelian over K_1 has Galois group isomorphic to $C_2 \times C_2$ over M so we want to find a C_4 extension of M containing H. Let H_{651} be the ray class field of conductor $651 \cdot \mathcal{O}_M$. There are several C_4 subextensions of H_{651} containing H, hence there exists an elliptic curve E/H with good reduction outside D_1 such that $\mathfrak{W}_{H/M}(E)$ has CM by $\mathbb{Q}(\sqrt{-651}, \sqrt{-868})$.

We can choose E to be a K_1-curve, if we are willing to relax the condition on bad reduction. Let $\mathfrak{p}$ and $\mathfrak{p}^\rho$ be the primes of K dividing 29, and let L be the quadratic extension of H corresponding to the Dirichlet character

$$\phi := \lambda_{\mathfrak{p}} \circ \mathrm{N}_{H/K}.$$

The extension L/M is cyclic of degree four and becomes normal over the ring class field of K of conductor 29, which has Galois group isomorphic to $C_2 \times C_4 \times C_{28}$ over K.

Let $S := \{3, 7, 31, 651\}$. In the following table $p \in \{13, 61, 67\}$ is the rational prime determining M as in the previous example and k is the smallest field such that E is a k-curve of type 1. The integers f are such that we may choose E to be unramified outside primes dividing f subject to the conditions that E is a k-curve of type 1 and that

$$\mathrm{End}^0_M(\mathfrak{W}_{H/M}(E_\lambda)) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}).$$

D_2	p	f	k
-3	61	$d \in S$	$\mathbb{Q}$
-7	67	7	$\mathbb{Q}$
-31	13	7	$\mathbb{Q}$
-84	13	$3, 31$	$\mathbb{Q}$
-372	67	$3, 31$	$\mathbb{Q}$
-868	61	651	M
-868	61	$d \cdot \mathfrak{p},\ d \in S$	K_1

If $h_K = 2$, and E is a K-curve defined over H then the Weil restriction $\mathfrak{W}_{H/K}(E)$ will have CM by a biquadratic field containing K. The following result of Yang [**68**] shows that there is a partial converse:

Proposition 5.5.4 (Yang [**68**] Corollary 3.6)**.** *When D_K is coprime to 6, every CM abelian variety of dimension h_K defined over K is isogenous to the Weil restriction of some CM elliptic curve defined over H.*

5.5.2. Weil Restrictions of Abelian Surfaces: Cyclic Quartic CM Fields. Let k be a quartic CM field such that $\mathrm{Gal}(k/\mathbb{Q}) \cong C_4$. The reflex of any CM type (k, Ψ) is (k, Ψ^{-1}) hence any abelian variety A with CM by an order of k is absolutely simple. Further, the field of moduli of A is contained in the Hilbert class field H of k, so A is defined over H.

Let k_0 be the maximal real subfield of k and let ∞_1 denote the infinite place of k corresponding to the inclusion of k in $\mathbb{C}$. Let σ be a generator of $\mathrm{Gal}(k/\mathbb{Q})$, let ι be a fixed embedding of k into $\mathbb{C}$, and let Ψ be $\{\iota, \iota_\sigma\}$ where we define $\iota_\sigma(x) := \iota(x^\sigma)$ for any element x of k. Note that then $\Psi^{-1} = \{\iota, \iota_{\sigma^3}\}$.

If $f := f_{\Psi,\infty_1}$ is the map from $\mathfrak{I}_H$ to $\mathbb{C}$ introduced in Definition 2.3.1 then for any idele $\boldsymbol{\alpha}$ of $\mathfrak{I}_H$

$$f(\boldsymbol{\alpha}) = \mathrm{N}_{H/k}(\alpha_{\infty_1})^{1+\sigma^3}.$$

Let λ be a quadratic character of U_k such that

$$\lambda(u)u^{1+\sigma^3} = 1 \tag{5.23}$$

for every unit u of $\mathcal{O}_k$. We now have a situation very similar to that of Proposition 4.1.1.

Proposition 5.5.5. *Let* (k, Ψ) *and* ∞_1 *be as above and let* λ *be a quadratic character of* U_k *satisfying* (5.23)*. Then there exists a Hecke character* φ *of* $\mathfrak{I}_k$ *such that*

a) *if* $\boldsymbol{\alpha} \in U_k$ *then* $\varphi_{un}(\boldsymbol{\alpha}) = \lambda(\boldsymbol{\alpha})$*,*

b) *if* $\boldsymbol{\alpha} \in K_\infty^*$ *then* $\varphi(\boldsymbol{\alpha}) = \alpha_{\infty_1}^{1+\sigma^3}$*,*

and $\chi := \varphi \circ \mathrm{N}_{H/K}$ *is the Grössencharacter of an abelian variety* A/H *of type* (k, Ψ)*.*

Proof. See Theorem 11 and Example 1 of p. 525 of Shimura [**55**]. □

An abelian variety A of CM type (k, Ψ) will have automorphism group $\{\pm 1\}$ except if $k = \mathbb{Q}(\mu_5)$ where μ_5 is a fifth root of unity, so excluding this case we are in much the same position as considering quadratic twists of elliptic curves with CM by K where $D_K < -4$. If k_0 has class number 1 then, as discussed in Section 4.2.1, whether or not there exists a canonical Hecke character of $\mathfrak{I}_k$, depends upon the structure of the local unit group $U_\mathfrak{p}$ at primes $\mathfrak{p}$ of k dividing 2. In particular, if D_k is odd then there is a unique quadratic character λ of U_k such that if φ is a canonical character of $\mathfrak{I}_k$ the restriction of φ_{un} to U_k is equal to λ. If D_k is even then there are 0, 4 or 8 such characters of U_k. We refer to Rohrlich [**41**] for the precise conditions and Murabayashi [**32**] for examples of the determination of the quadratic characters of $U_\mathfrak{p}$.

We shall avoid this complexity by requiring that the discriminant D_k of $k/\mathbb{Q}$ be odd. We would also like to ensure that there exist k_0-varieties of type 2, hence we look for quartic CM fields with class groups isomorphic to $C_2^{\times 2}$, the smallest group for which this will occur.

From the lists in Park-Kwon [**36**] we see that there are 13 cyclic quartic CM fields k with class number 4 which have maximal real subfields k_0 with class number 1. Of these, all have class group isomorphic to $C_2^{\times 2}$ and 5 have discriminants divisible by three rational primes and hence their Hilbert class fields are abelian over $\mathbb{Q}$. In the remaining cases one of the two prime divisors of D_k splits in $k_0/\mathbb{Q}$, so any towers of admissible extensions of k of the kind studied in Chapter 3 must take k_0 rather than $\mathbb{Q}$ as their base.

Example 5.5.6. Let $k := \mathbb{Q}(\sqrt{-255 + 60\sqrt{17}})$. The maximal real subfield k_0 of k is $\mathbb{Q}(\sqrt{17})$, the discriminant of k is $D_k := 3^2 \cdot 5^2 \cdot 17^3$, the Hilbert class field is $H := k(\sqrt{5}, \sqrt{-3})$, and the group of units of $\mathcal{O}_k$ is generated by $\{-1, u\}$ with $u = 4 + \sqrt{17}$. Now since every rational prime dividing D_k is odd, and either inert or ramified in k_0, the quadratic characters of U_k unramified outside D_k are simply the quadratic residue characters defined by

$$\lambda_p(x) := \left(\frac{\bar{x}}{p}\right)$$

where $\bar{x}$ is the image of x in $\overline{k}_{\mathfrak{p}}$ and $\mathfrak{p}$ is the unique prime of k dividing p.

Since $u^{1+\sigma^3} = -1$, the conditions for a quadratic character λ to satisfy (5.23) are that $\lambda(-1) = 1$ and $\lambda(u) = -1$. For $\lambda \circ \mathrm{N}_{H/k}$ to be a Dirichlet character of $\mathfrak{I}_H$ however, we need $\lambda(-1) = \lambda(u) = 1$.

Evaluating the characters λ_p we find

p	$\lambda_p(-1)$	$\lambda_p(u)$
3	1	-1
5	1	1
17	1	1

hence there are Dirichlet characters of $\mathfrak{I}_H$ of the form $\lambda \circ \mathrm{N}_{H/k}$ with λ in $\{\lambda_5,\ \lambda_{17},\ \lambda_5\lambda_{17}\}$, and each of the corresponding extensions L/H is normal over $\mathbb{Q}$ and $C_2 \times C_4$ over k, so $c_4(H/k) = 2$. There is a dihedral extension of $\mathbb{Q}$ defined by the partial decomposition $(-15, 85)$ so we have $\dim_{\mathbb{F}_2} \mathcal{G}^s_{H/k}/\mathcal{A}^s_{H/k} = 1$.

For this choice of k, the primes congruent to 1 and $3 \bmod 4$ behave in a manner reminiscent of their roles in an imaginary quadratic field, with u taking the place of -1. The following example shows that this is not a general rule.

Example 5.5.7. Let $k := \mathbb{Q}(\sqrt{-105 + 42\sqrt{5}})$. The discriminant of $k/\mathbb{Q}$ is $D_k := 3^2 \cdot 5^3 \cdot 7^2$ and the Hilbert class field of k is $H := k(\sqrt{-3}, \sqrt{-7})$, and again $H/\mathbb{Q}$ is abelian. The unit group of $\mathcal{O}_k$ is generated by -1 and u where

$$u := \frac{-1 + \sqrt{5}}{2}$$

and

p	$\lambda_p(-1)$	$\lambda_p(u)$
3	1	-1
5	1	-1
7	1	-1

hence the k-equivalence classes of $\mathcal{A}_{H/k}$ are represented by the extensions corresponding to the Dirichlet characters $\lambda \circ \mathrm{N}_{H/k}$ with

$$\lambda \in \{\lambda_3\lambda_5,\ \lambda_3\lambda_7,\ \lambda_5\lambda_7\}.$$

Each of these characters defines an extension of k with Galois group $C_2 \times C_4$, so $c_4(H/k) = 2$.

Returning to our first example, $k := \mathbb{Q}(\sqrt{-255 + 60\sqrt{17}})$, and to the main subject of this chapter we will now investigate the endomorphism algebras of the Weil restrictions of abelian varieties A/H with CM by k and Grössencharacters fixed by $\mathrm{Gal}(H/k_0)$. The situation is almost entirely analogous to that when A has dimension 1 and we follow the same procedure as in Section 5.4.

The class group of k is generated by primes $\mathfrak{p}_1$, $\mathfrak{p}_2$ dividing 43 and 47 respectively. Choosing generators a_i and b_i of $\mathfrak{p}_i^2$ and $\mathfrak{p}_i\mathfrak{p}_i^\rho$ we find:

$$\begin{aligned} a_1 + a_1^\rho &= -6\sqrt{17} - 23, \quad b_1 = 3\sqrt{17} + 14 \\ a_2 + a_2^\rho &= -2\sqrt{17} - 1, \quad\ \ b_2 = \sqrt{17} + 8. \end{aligned}$$

Let A_λ be the abelian variety of CM type (k, Ψ) with Grössencharacter determined as in Proposition 5.5.5 by the quadratic character λ and let $W_\lambda := \mathfrak{W}_{H/k_0}(A_\lambda)$. Setting $\sigma_i := (H/k; \mathfrak{p}_i)$, and letting u_σ be as in (5.12),

$$\mathrm{End}^0_{k_0}(W_\lambda) = k_0(u_{\sigma_1} + u_{\sigma_1\rho}, u_{\sigma_2} + u_{\sigma_2\rho})$$

and

$$(u_{\sigma_i} + u_{\sigma_i\rho})^2 = \lambda(\mathfrak{p}_i^2)a_i + 2\lambda(\mathfrak{p}_i\mathfrak{p}_i^\rho)b_i.$$

Evaluating characters we find:

λ	$\mathrm{End}^0_{k_0}(W_\lambda)$
λ_3	$k_0(\sqrt{5}, \sqrt{-15})$
$\lambda_3\lambda_5$	$k_0(\sqrt{-5}, \sqrt{15})$
$\lambda_3\lambda_{17}$	$k_0(\sqrt{-5}, \sqrt{-15})$
$\lambda_3\lambda_5\lambda_{17}$	$k_0(\sqrt{5}, \sqrt{15})$

Remark 5.5.8. It may be seen from the table above that we have $\lambda(\mathfrak{p}_i^2) = \lambda(\mathfrak{p}_i\mathfrak{p}_i^\rho)$ for each λ; this is a consequence of the fact that each of the extensions in $\mathcal{A}_{H/k}$ is also abelian over $\mathbb{Q}$. In dimension 1, this occurs for example when $D_K = -195$.

We conclude by calculating the endomorphism algebra of the Weil restriction of a k_0-variety of k-type 2.

Let L be the compositum HL_0 where L_0 is a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{-15}, \sqrt{85})$ and cyclic over $\mathbb{Q}(\sqrt{-51})$. Let A/H be a canonical variety of k-type 1 and let W be the Weil restriction of A^L from H to k_0.

Let F_i be the decomposition field of $\mathfrak{p}_i$ in H and let $\mathfrak{P}_i$ and be primes of F_i dividing $\mathfrak{p}_i$. We denote the Hecke character of L/F_i by ϕ_i. Now $\phi_1(\mathfrak{P}_1^2) = 1$ and $\phi_1(\mathfrak{P}_1\mathfrak{P}_1^\rho) = -1$ hence,

$$(u_{\sigma_1} + u_{\sigma_1\rho})^2 = a_1 - 2b_1 = -12\sqrt{17} - 51.$$

The extension L/F_2 is cyclic hence $\phi_2(\mathfrak{P}_2^2) = -1$ and since $\phi_2(\mathfrak{P}_2\mathfrak{P}_2^\rho) = 1$ we have

$$(u_{\sigma_2} + u_{\sigma_2\rho})^2 = -a_2 + 2b_2 = 4\sqrt{17} + 17.$$

The algebra of k_0-rational endomorphisms $\mathrm{End}_{k_0}^0(W)$ is the quaternion algebra generated by $u_{\sigma_1} + u_{\sigma_1\rho}$ and $u_{\sigma_2} + u_{\sigma_2\rho}$ over k_0, ramifies at the primes of k_0 dividing 3 and 17 and splits over k.

Calculating the remaining endomorphism algebras in a similar way one finds that they are all ramified over k_0 and split over k.

APPENDIX A

The purpose of this appendix is to describe the groups occuring as $\mathrm{Gal}(L/k)$ when $L/F/k$ is a normal tower of fields such that $\mathrm{Gal}(F/k) \cong C_2^{\times n}$ and L/F is quadratic, and in particular to prove Lemma 3.2.18, Proposition 3.2.19 and Theorem 3.2.21. For convenience we shall repeat some of the definitions and results found in Chapter 3. Restated lemmas and theorems have references to their original statement given in brackets.

For any group G we recall that we denote the centre of G by $Z(G)$ and the number of elements of G having order n by $\Sigma_n(G)$.

Lemma A.1 (Lemma 3.2.8)**.** *With F and k as above, let L be a quadratic extension of F which is normal over k and set $G := \mathrm{Gal}(F/k)$ and $\widetilde{G} := \mathrm{Gal}(L/k)$. Then*

$$\widetilde{G}/Z(\widetilde{G}) \cong C_2^{\times 2m}, \text{ with } 0 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor, \tag{A.1}$$

there are elements $\sigma_1, \ldots, \sigma_{2m}$ of G satisfying

$$\begin{aligned} \epsilon_{L*}(\sigma_{2i}, \sigma_{2i-1}) &= -1,\ 1 \leq i \leq m, \\ \epsilon_{L*}(\sigma_i, \sigma_j) &= 1 \text{ for all } j \notin \{i+1, i-1\}, \end{aligned}$$

and $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{2m}$ is a basis for $\widetilde{G}/Z(\widetilde{G})$.

Definition A.2. *Let G be a group, and let H and M be subgroups of G such that $G = HM$ and $H \cap M \subset Z(G)$. We say that G is the* central product *of H and M if every element of M commutes with every element of H.*

We denote the central product of groups H and M by HM. The direct product of H and M is denoted $H \times M$ as in Chapter 3. Let D and Q denote respectively the dihedral and quaternion groups of order 8. In all central products of the form GD or GQ, the intersection $G \cap D$ (resp. $G \cap Q$) is to be taken as $Z(D)$ (resp. $Z(Q)$).

Definition A.3. *A p-group G is* extra-special *if it has centre of order p and*

$$G/Z(G) \cong C_p^{\times n}$$

for some integer $n \geq 1$.

Theorem A.4 (Gorenstein [**14**] Theorem 5.5.2)**.** *An extra-special 2-group is the central product of $r \geq 1$ nonabelian subgroups of order 8. Moreover $D^k Q^{r-k}$ is isomorphic to DQ^{r-1} and to Q^r if k is even, and the groups DQ^{r-1} and Q^r are not isomorphic.*

Lemma A.5. *The central product of C_4 and D is isomorphic to the central product of C_4 and Q.*

Proof. The groups $C_4 Q$ and $C_4 D$ each have order 16, centre C_4 and the property that $G/Z(G) \cong C_2^{\times 2}$. Checking the list of groups in Magma's Small Groups Database, which contains every 2-group of order at most 2^6, we find that up to isomorphism there is exactly one group with these properties. □

Definition A.6. *Let n be an even integer. We define*

a) *$\mathfrak{Q}_n$ to be the central product $Q^{n/2}$,*
b) *$\mathfrak{D}_n$ to be the central product DQ^r where $r = \frac{n-2}{2}$ and*
c) *$\mathfrak{B}_{n+1}$ to be the central product of C_4 with $\mathfrak{D}_n$.*

The group $\mathfrak{D}_n$ has a polycyclic presentation as the group generated by $\sigma_1, \ldots, \sigma_{n+1}$ where

$$\sigma_{2a-1}\sigma_{2a}\sigma_{2a-1}^{-1} = \sigma_{2a}\sigma_{n+1}, \qquad \text{for } 1 \leq a \leq n/2, \tag{A.2}$$

and $\sigma_i^2 = 1$ for $1 \leq i \leq n+1$.

Similarly $\mathfrak{Q}_n$ is isomorphic to the group generated by $\sigma_0, \ldots, \sigma_n$ where (A.2) holds and $\sigma_1^2 = \sigma_2^2 = \sigma_{n+1}$ and $\sigma_i^2 = 1$ for $3 \leq i \leq n+1$. The group $\mathfrak{B}_{n+1}$ is isomorphic to the group generated by $\sigma_1, \ldots, \sigma_{n+2}$ where

$$\sigma_{2a-1}\sigma_{2a}\sigma_{2a-1}^{-1} = \sigma_{2a}\sigma_{n+2}, \qquad \text{for } 1 \leq a \leq n/2, \tag{A.3}$$

$\sigma_1^2 = \ldots = \sigma_n^2 = 1$ and $\sigma_{n+1}^4 = 1$.

Lemma A.7. *Let $\widetilde{G}$ be a group satisfying the conditions of Lemma 3.2.8. Then $\widetilde{G}$ is either abelian or the central product of an abelian group A with an extra-special group E where*

$$A \cong \begin{cases} C_4 \times C_2^{\times a} & \textit{if } Z(G) \textit{ contains an element of order 4,} \\ C_2^{\times a+2} & \textit{otherwise.} \end{cases}$$

Proof. With notation as in Lemma A.1, it is clear that

$$\widetilde{G} \cong Z(\widetilde{G})\langle \tilde{\sigma}_1, \cdots, \tilde{\sigma}_{2m} \rangle.$$

Now each pair $\sigma_{2i-1}, \sigma_{2i}$ with $i \leq m$ generates an extra-special group E_i of order 8 and E_i commutes with E_j for all $i \neq j$. □

Lemma A.8 (Lemma 3.2.18)**.** *Let n be an even integer. The groups G defined in Definition 3.2.16 have the properties described in the following table:*

G	$\#G$	$\Sigma_4(G)$	$Z(G)$
$\mathfrak{D}_n$	2^{n+1}	$2^n - 2^{n/2}$	C_2
$\mathfrak{Q}_n$	2^{n+1}	$2^n + 2^{n/2}$	C_2
$\mathfrak{B}_{n+1}$	2^{n+2}	2^{n+1}	C_4

Proof. The structure of $Z(G)$ is immediate from the definition and the number of elements of G from the standard fact that if $G = HM$ then

$$|G| = \frac{|H||M|}{|H \cap M|},$$

(see eg. Alperin and Bell [**1**] Proposition 1.12). For proof of the values of $\Sigma_4(G)$ if G is isomorphic to $\mathfrak{D}_n$ or $\mathfrak{Q}_n$ see Gorenstein [**14**] p. 206. It remains to show that the number of elements of order 4 of $\mathfrak{B}_{n+1}$ is 2^n. If we write

$$\mathfrak{B}_{n+1} = \langle \sigma_1, \sigma_2, \ldots, \sigma_{n+2} \rangle,$$

then with our standard ordering of generators

$$\mathfrak{D}_n \cong \langle \sigma_1, \sigma_2, \ldots, \sigma_n, \sigma_{n+2} \rangle.$$

Now if g has order 2 in $\mathfrak{D}_n$, or if $g = 1$ then $g\sigma_{n+1}$ has order 4 in $\mathfrak{B}_{n+1}$. On the other hand if g has order 4 in $\mathfrak{D}_n$ then g has order 4 in $\mathfrak{B}_n$ and $g\sigma_{n+1}$ has order 2. Therefore

$$\epsilon_4(\mathfrak{B}_{n+1}) = \epsilon_4(\mathfrak{D}_n) + \epsilon_2(\mathfrak{D}_n) + 1 = |\mathfrak{D}_n|.$$

□

Definition A0.9. *Let m and n be integers with $n \geq 2$, $0 \leq m < n$ and $n-m$ even. If n is even and $m = 0$ then define $T_{n,m} := \{\mathfrak{D}_n, \mathfrak{Q}_n\}$, otherwise*

$$T_{n,m} = \{\mathfrak{D}_{n,m}, \mathfrak{B}_{n,m}, \mathfrak{Q}_{n,m}\},$$

where

$$\begin{aligned} \mathfrak{D}_{n,m} &:= C_2^{\times m} \times \mathfrak{D}_{n-m}, \\ \mathfrak{Q}_{n,m} &:= C_2^{\times m} \times \mathfrak{Q}_{n-m} \text{ and} \\ \mathfrak{B}_{n,m} &:= C_2^{\times m-1} \times \mathfrak{B}_{n+1-m}. \end{aligned}$$

Theorem A.9 (Theorem 3.2.21)**.** *Let m and n be as in Definition A0.9. If $\widetilde{G}$ is a group satisfying Lemma 3.2.8 of order 2^{n+1} with n generators and centres of order 2^{m+1}, then $\widetilde{G}$ is isomorphic to a group in $T_{n,m}$.*

Proof. If $\widetilde{G}$ is a non-abelian group satisfying Lemma 3.2.8 it follows from Lemma A.7, Theorem A.4 and Lemma A.5 that $\widetilde{G}$ is isomorphic to the central product of $C_2^{\times m}$ with one of $\mathfrak{D}_r$, $\mathfrak{Q}_r$ or $\mathfrak{B}_r$, and the orders and centres of such groups follow from Lemma A.8. □

Remark A0.10. The claims of Proposition 3.2.19 are a subset of those of Theorem 3.2.21.

References

[1] J. Alperin and R. Bell, *Groups and Representations*, Graduate Texts in Mathematics 162, Springer-Verlag, 1995.

[2] E. Artin and J. Tate, *Class Field Theory*, W.A. Benjamin, 1967.

[3] M. Artin, Néron Models, in *Arithmetic Geometry*, (ed. G. Cornell and J. Silverman) Springer-Verlag, 1986 213–230.

[4] C. Birkenhake and H. Lange, *Complex Abelian Varieties* (second edition), Springer-Verlag, 2004.

[5] S. Bosch, W. Lütkebohmert, M. Reynaud, *Néron Models*, Springer-Verlag, 1990.

[6] D. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley & Sons, 1989.

[7] M. Deuring, Die Zetafunktion einer algebraischen Kurve von Geschlechte eins I, *Nachr. Akad. Wiss. Göttingen* (1953) 85–94.

[8] J.-M. Fontaine, Il n'y a pas de variété abélienne sur Z, *Invent. Math.* **81** (1985) 515–538.

[9] É. Fouvry and J. Klüners. On the 4-rank of the class groups of quadratic number fields, *Invent. Math.* **167** (2007) 455–513.

[10] G. Frey, How to disguise an elliptic curve, slides of talk given at the Second Workshop on Elliptic Curve Cryptography (ECC '98), `www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`.

[11] A. Fröhlich, The Rational Characterization of Certain Sets of Relatively Abelian Extensions, *Philos. Trans. Roy. Soc. Lond., Ser. A* **251** (1959) 385–425.

[12] F. Gerth III, The 4-class ranks of quadratic fields, *Invent. Math.* **77** (1984) 489–515.

[13] C. Goldstein and N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, *J. Reine Angew. Math.* **327** (1981) 184–218.

[14] D. Gorenstein, *Finite Groups* (second edition), Chelsea, 1980.

[15] G. Gras, *Class Field Theory*, Springer Monographs in Mathematics, Springer, 2003.

[16] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Mathematics 776, Springer-Verlag, 1980.

[17] B. Gross, Minimal models for elliptic curves with complex multiplication, *Comp. Math.* **45** (1982) 155–164.

[18] A. Grothendieck, Modèles de Néron et monodromie, Exposé IX of S.G.A. 7, in *Groupes de Monodromie en Géometrie Algébrique*, Springer Lecture Notes in Mathematics 288, Springer-Verlag 1972.

[19] F. Hajir and F. Rodriguez Villegas, On the Tate-Shaferevich Group of Certain Elliptic Curves, *Math. Res. Lett.* **5** (1998) 637–655.

[20] F. Halter-Koch, Construction of continuous idele class characters in quadratic number fields and imbedding problems for dihedral and quaternion fields, *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, **17** (1975-1976), exp. 14, 1–13.

[21] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (zweite Mitteilung), *Math. Z.* **6** (1920) 11–51.

[22] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Mathematics 77, Springer-Verlag, 1981.

[23] H. Heilbronn, Zeta-Functions and L-Functions, in *Algebraic Number Theory*, (ed. J. Cassels and A. Fröhlich), Academic Press, 1967, 204–230.

[24] E. Kani and M. Rosen, Idempotent relations and factors of Jacobians, *Math. Ann.* **284** (1989) 307–327.

[25] S. Lang, *Algebraic Numbers*, Addison-Wesley, 1964.

[26] S. Lang, *Complex Multiplication*, Springer-Verlag, 1983.

[27] R. Massy, Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p, *J. Alg.* **109** (1987) 508–535.

[28] S. Miller and T. Yang, Non-vanishing of the central derivative of canonical Hecke L-functions, *Math. Res. Lett.* **7** no. 3 (2000) 263–277.

[29] J. Milne, On the Arithmetic of Abelian Varieties, *Invent. Math.* **17** (1972) 177–190.

[30] H. Montgomery and D. Rohrlich, On the L-functions of canonical Hecke characters of imaginary quadratic fields II, *Duke Math. J.* **29** (1982) 937–942.

[31] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970.

[32] N. Murabayashi, Determination of simple CM abelian surfaces defined over $\mathbb{Q}$, *Math. Ann.* **342** (2008) 657–671.

[33] T. Nakamura, On abelian varieties associated with elliptic curves with complex multiplication, *Acta Arith.* **XCVII.4** (2001) 379–385.

[34] T. Nakamura, A classification of $\mathbb{Q}$-curves with complex multiplication, *J. Math. Soc. Japan* **56** no.2, (2004) 636–648.

[35] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag 1992.

[36] Y. Park and S. Kwon, Determination of all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number $\leq$ 20, *Acta Arith.* **LXXXIII.3** (1998) 211–223.

[37] J. Quer, $\mathbb{Q}$-curves and abelian varieties of GL_2-type, *Proc. Lond. Math. Soc.* (3) **81** (2000) 285–317.

[38] L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten eines beliebigen quadratischen Zahlkörpers, *J. Reine Angew. Math.* **170** (1934) 69–74.

[39] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. Reine Angew. Math.* **171** (1934) 55–60.

[40] D. Rohrlich, The non-vanishing of certain Hecke L-functions at the center of the critical strip, *Duke Math. J.* **47** no. 1, (1980) 223–232.

[41] D. Rohrlich, Root Numbers of Hecke L-Functions of CM Fields, *Am. J. Math.* **104** no. 3, (1982), 517–543.

[42] D. Rohrlich, Elliptic curves with good reduction everywhere, *J. Lond. Math. Soc.* (2) **25** no. 2, (1982) 216–222.

[43] M. Rosenlicht, Some Basic Theorems on Algebraic Groups, *Am. J. Math.* **78** no. 2, (1956) 401–403.

[44] K. Rubin, Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **64** (1981) 455–470.

[45] K. Rubin and A. Silverberg, Point counting on reductions of CM elliptic curves, *J. Number Theory* (2009), doi:10.1016/j.jnt.2009.01.020.

[46] R. Rumely, A Formula for the Grössencharacter of a Parametrized Elliptic Curve, *J. Number Theory* **17** (1983) 389–402.

[47] R. Rumely, On the Grössencharacter of an abelian variety in a parametrized family, *Trans. Am. Math. Soc.* **276** (1983) 213–233.

[48] R. Schoof, Abelian varieties over $\mathbb{Q}(\sqrt{6})$ with good reduction everywhere, in *Class Field Theory—Its Centenary and Prospect*, ed. K. Miyake, Advanced Studies in Pure Mathematics 30, Math. Soc. Japan, 2001, 287–306.

[49] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, 1979.

[50] J.-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, **11** no. 2, (1969-70) 1–15.

[51] J.-P. Serre and J. Tate, Good Reduction of Abelian Varieties, *Ann. Math.* **88** (1968) 492–517.

[52] B.Setzer, Elliptic curves over complex quadratic fields, *Pacific J. Math.* **74** (1978) 235–250.

[53] S. Shatz, Group Schemes, Formal Groups and p-Divisible Groups, in *Arithmetic Geometry*, (ed. G. Cornell and J. Silverman) Springer-Verlag, 1986, 29–78.

[54] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.

[55] G. Shimura, On the zeta function of an abelian variety with complex multiplication, *Ann. Math.* **94** (1971) 504–533.

[56] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

[57] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan, no. 6, 1961.

[58] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, 1986.

[59] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994.

[60] C. Sims, *Computation with Finitely Presented Groups*, Cambridge University Press, 1994.

[61] J. Tate, Global Class Field Theory, in *Algebraic Number Theory*, (ed. J. Cassels and A. Fröhlich), Academic Press, 1967, 162–203.

[62] J. Tate, Fourier Analysis in Number Fields and Hecke's Zeta-Functions, in *Algebraic Number Theory*, (ed. J. Cassels and A. Fröhlich), Academic Press, 1967, 305–347.

[63] T. Vaughan, Constructing quaternionic fields, *Glasgow Math. J.* **34** (1992) 43–54.

[64] A. Weil, Jacobi Sums as "Grossencharaktere", *Trans. Am. Math. Soc.* **73** no. 3, (1952) 487–495.

[65] A. Weil, The Field of Definition of a Variety, *Am. J. Math.*, **78** no. 3, (1956) 509–524.

[66] A. Weil, *Basic Number Theory* (third edition), Springer-Verlag, 1974.

[67] A. Weil, *Adeles and Algebraic Groups*, Progress in Mathematics 23, Birkhäuser, 1982.

[68] T. Yang, On CM abelian varieties over imaginary quadratic fields, *Math. Ann.* **329** (2004) 87–117.

[69] H. Yu, Idempotent relations and the conjecture of Birch and Swinnerton-Dyer, *Math. Ann.* **327** (2003) 67–78.

[70] H. Yu, Representations and factors of the restriction of scalars, *J. Number Theory* **109** (2004) 266-277.

List of Symbols