THE CHOWLA-SELBERG FORMULA FOR CM FIELDS AND THE COLMEZ CONJECTURE

A Dissertation

by

ADRIAN ALBERTO BARQUERO-SANCHEZ

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Riad Masri
Committee Members,	Matthew Papanikolas
	Matthew P. Young
	Lan Zhou
Head of Department,	Emil Straube

August 2016

Major Subject: Mathematics

ABSTRACT

In this thesis we start by giving a quick review of the classical Chowla-Selberg formula. We then recall a conjecture of Colmez which relates the Faltings height of an abelian variety with complex multiplication by the ring of integers of a CM field E to logarithmic derivatives of certain Artin L–functions at $s = 0$. It turns out that in the case in which the abelian variety is a CM elliptic curve, the conjecture of Colmez can be seen as a geometric reformulation of the classical Chowla-Selberg formula.

Then we will focus our attention on establishing a generalization of the classical Chowla-Selberg formula for abelian CM fields. This is an identity which relates values of a Hilbert modular function at CM points to values of Euler's gamma function Γ and an analogous function Γ_2 at rational numbers.

Finally, we will study the above mentioned conjecture of Colmez. We will prove that if F is any fixed totally real number field of degree $[F : \mathbb{Q}] \geq 3$, then there are infinitely many CM extensions E/F such that $E/\mathbb{Q}$ is *non-abelian* and the Colmez conjecture is true for E. Moreover, these CM extensions are explicitly constructed to be ramified at "arbitrary" prescribed sets of prime ideals of F. We also prove that the Colmez conjecture is true for a generic class of non-abelian CM fields called Weyl CM fields, and use this to develop an arithmetic statistics approach to the Colmez conjecture based on counting CM fields of fixed degree and bounded discriminant. We illustrate these results by evaluating the Faltings height of the Jacobian of a genus 2 hyperelliptic curve with complex multiplication by a non-abelian quartic CM field in terms of the Barnes double Gamma function at algebraic arguments. This can be seen as an explicit non-abelian Chowla-Selberg formula.

DEDICATION

Este trabajo es dedicado a mi madre, Rita Sánchez Vargas, a quien le debo todo en la vida. Gracias mamita, sin tu apoyo incondicional, esto no habría sido posible.

ACKNOWLEDGEMENTS

I would first and foremost like to thank my advisor, Riad Masri, not only for the guidance and the support that he provided me during the time that we have been working together, but more importantly because of the friendship that has stemmed out of our mathematical work. Thank you very much for everything Riad! I am very happy to be able to consider you as one of my best friends.

Secondly, I would like to thank all of the professors from the number theory group at Texas A&M, particularly Matt Papanikolas and Matt Young, from whom I've learned a lot. I am indebted to Matt Papanikolas for his masterful lessons in Algebraic Number Theory and Elliptic Curves. Also, I would like to thank professor Alexei Poltoratski, whose wonderful year long Complex Analysis sequence in the 2011-2012 academic year has left a deep and lasting love in me for the beauty that this subject possesses.

I would also like to thank and acknowledge the University of Costa Rica for the partial support provided during the preparation of this work.

I would like to thank my best friends, who have always been there for me throughout the years. In particular, I would like to thank Bryan Yocks, Yersinio Jiménez, Mariela Morales, Leanne Jacobs, Rebecca Milam and Mackenzie Aguillard.

I (re)discovered my love for mathematics when I was an undergraduate student at the University of Costa Rica. I received an excellent education there, which has definitely been intrumental for me getting to this point. I would like to thank professors Jorge Guier, William Ugalde, Eduardo Piza, Héctor Figueroa, Pedro Méndez, Joseph Várilly, Michael Josephy, Edwin Castro, Mark Villarino, John Bradley, Lizeth Sancho, Edgardo Arita, Julio Céspedes, Evelio Hernández and also professor Léster Izaguirre for suggesting me to take the first course for math majors when my engeneering math classes had run out.

I would also like to thank a wonderful group of friends that I've made while a student at Texas A&M. In particular, Edwin Xiao, Esteban Jiménez, Camilo Bastidas, Raquel Granados, Xavier

Jaime and Luis de Jesús. I have really enjoyed watching and playing soccer with you guys!

Finally, none of this would have been possible without the uncondicional support of my beloved family, my dad Dennis Barquero, my mom Rita Sánchez, my two little brothers Francisco and Daniel and all of my aunts, uncles, cousins, etc.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE Page

1. INTRODUCTION

The Chowla-Selberg formula [CS49, CS67] is a remarkable identity which relates values of the Dedekind eta function at CM points to values of Euler's gamma function Γ at rational numbers. This formula arises in connection with many topics in number theory, including elliptic curves, L–functions, modular forms, and transcendence. For a very nice discussion, see Zagier [Zag08, Section 6.3]. In the second chapter of this thesis we will establish a Chowla-Selberg formula for abelian CM fields. This is an identity which relates values of a Hilbert modular function at CM points to values of Γ and an analogous function Γ_2 at rational numbers. The function Γ_2 was studied extensively by Deninger [Den84] in his work on the Chowla-Selberg formula for real quadratic fields. We note that there has recently been a great amount of interest in formulas for CM values of Hilbert modular functions. Some examples occur in the work of Bruinier-Yang [BY06, BY07, BY11] and Bruinier-Kudla-Yang [BKY12], which is related to Borcherds products and the seminal work of Gross-Zagier [GZ85] on factorization of differences of singular moduli.

1.1 The Chowla-Selberg formula

We begin by reviewing the classical Chowla-Selberg formula (see e.g. [Wei76, Chapter IX]). Let $\Delta = f^2 d$ be a fundamental discriminant where $f > 0$ and d is square-free. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant Δ, $\mathcal{O}_K$ be the ring of integers, CL(K) be the ideal class group, h_d be the class number, $w_d = \#\mathcal{O}_K^\times$ be the number of units (for $d < 0$), ε_d be the fundamental unit (for $d > 0$), and $\chi_d(\cdot) = \left(\frac{\Delta}{\cdot}\right)$ be the Kronecker symbol associated to K. Assume now that $d < 0$. Given an ideal class $C \in$ CL(K), one may choose a primitive integral ideal $\mathfrak{a} \in C^{-1}$ such that

$$\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}\left(\frac{-b+\sqrt{\Delta}}{2}\right), \quad a, b \in \mathbb{Z}$$

where $a = N_{K/\mathbb{Q}}(\mathfrak{a})$ is the norm of $\mathfrak{a}$ and b satisfies $b^2 \equiv \Delta \mod 4a$. Then

$$\tau_{\mathfrak{a}} = \frac{-b+\sqrt{\Delta}}{2a}$$

is a CM point in the complex upper half-plane $\mathbb{H}$ which corresponds to the inverse class $[\mathfrak{a}] = C^{-1}$.

The Chowla-Selberg formula is obtained by comparing two different expressions for the Dedekind zeta function $\zeta_K(s)$. One has the classical identity

$$\zeta_K(s) = \frac{2}{w_d}\zeta(2s)\left(\frac{2}{\sqrt{|\Delta|}}\right)^s \sum_{[\mathfrak{a}]\in \mathrm{CL}(K)} E(\tau_{\mathfrak{a}}, s),$$

where

$$E(z,s) := \sum_{M\in\Gamma_\infty\backslash \mathrm{SL}_2(\mathbb{Z})} \mathrm{Im}(Mz)^s, \quad z\in\mathbb{H}, \quad \mathrm{Re}(s)>1$$

is the non-holomorphic Eisenstein series for $\mathrm{SL}_2(\mathbb{Z})$. On the other hand, one has the well-known factorization

$$\zeta_K(s) = \zeta(s)L(\chi_d, s),$$

where $L(\chi_d, s)$ is the Dirichlet L-function associated to χ_d. Comparing these expressions and making the shift $s\mapsto (s+1)/2$ yields

$$\sum_{[\mathfrak{a}]\in \mathrm{CL}(K)} E\left(\tau_{\mathfrak{a}}, \frac{s+1}{2}\right) = \frac{w_d}{2}\left(\frac{\sqrt{|\Delta|}}{2}\right)^{\frac{s+1}{2}} \frac{\zeta(\frac{s+1}{2})}{\zeta(s+1)} L\left(\chi_d, \frac{s+1}{2}\right). \tag{1.1}$$

Now, one has the "renormalized" Kronecker limit formula

$$E\left(z, \frac{s+1}{2}\right) = 1 + \log(G(z))(s+1) + O((s+1)^2), \tag{1.2}$$

where

$$G(z) := \sqrt{\mathrm{Im}(z)}|\eta(z)|^2$$

and

$$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \quad q := e^{2\pi i z}, \quad z\in\mathbb{H}$$

is the Dedekind eta function, a weight 1/2 cusp form for $\mathrm{SL}_2(\mathbb{Z})$. Substitute (1.2) into the left hand side of (1.1), calculate the Taylor expansion of the right hand side of (1.1) at $s=-1$, differentiate both sides of the resulting identity with respect to s, and evaluate at $s=-1$ to get

$$\sum_{[\mathfrak{a}]\in \mathrm{CL}(K)} \log(G(\tau_{\mathfrak{a}})) = \frac{w_d}{2}L(\chi_d, 0)\left\{\log\left(\frac{\sqrt{|\Delta|}}{2}\right) - \frac{\zeta'(0)}{\zeta(0)} + \frac{L'(\chi_d,0)}{L(\chi_d,0)}\right\}. \tag{1.3}$$

Recall the evaluation

$$-\frac{\zeta'(0)}{\zeta(0)} = -\log(2\pi), \tag{1.4}$$

and the class number formula

$$L(\chi_d, 0) = \frac{2h_d}{w_d}. \tag{1.5}$$

To evaluate $L'(\chi_d, 0)$, one uses the decomposition

$$L(\chi_d, s) = |\Delta|^{-s} \sum_{k=1}^{|\Delta|} \chi_d(k) \zeta\left(s, \frac{k}{|\Delta|}\right), \tag{1.6}$$

where

$$\zeta(s, w) := \sum_{n=0}^{\infty} \frac{1}{(n+w)^s}, \quad \text{Re}(w) > 0, \quad \text{Re}(s) > 1$$

is the Hurwitz zeta function. Lerch [Ler87] showed that

$$\zeta(s, x) = \frac{1}{2} - x + \log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right) s + O(s^2), \quad x > 0 \tag{1.7}$$

where

$$\Gamma(s) := \int_0^{\infty} t^{s-1} e^{-t} dt$$

is Euler's gamma function. Substitute (1.7) into (1.6), then differentiate to get

$$L'(\chi_d, 0) = -\log(|\Delta|) L(\chi_d, 0) + \sum_{k=1}^{|\Delta|} \chi_d(k) \log\left\{\Gamma\left(\frac{k}{|\Delta|}\right)\right\}. \tag{1.8}$$

Finally, substitute (1.4), (1.5) and (1.8) into (1.3), then exponentiate to obtain the Chowla-Selberg formula

$$\prod_{[\mathfrak{a}] \in \text{CL}(K)} G(\tau_{\mathfrak{a}}) = \left(\frac{1}{4\pi\sqrt{|\Delta|}}\right)^{\frac{h_d}{2}} \prod_{k=1}^{|\Delta|} \Gamma\left(\frac{k}{|\Delta|}\right)^{\frac{w_d \chi_d(k)}{4}}. \tag{1.9}$$

1.2 The Colmez conjecture

In order to state the Colmez conjecture, we start by recalling the definition of the Faltings height of a CM abelian variety. Let F be a totally real number field of degree n. Let E/F be a CM extension of F and Φ be a CM type for E. Let X_Φ be an abelian variety defined over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_E$ and CM type Φ. We call X_Φ a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Let $K \subseteq \overline{\mathbb{Q}}$ be a number field over which X_Φ has everywhere good reduction, and choose a Néron differential $\omega \in H^0(X_\Phi, \Omega^n_{X_\Phi})$. Then the *Faltings height* of X_Φ is defined by

$$h_{\mathrm{Fal}}(X_\Phi) := -\frac{1}{2[K:\mathbb{Q}]} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log \left| \int_{X_\Phi^\sigma(\mathbb{C})} \omega \wedge \overline{\omega^\sigma} \right|.$$

The Faltings height does not depend on the choice of K or ω.

Now, let E^s denote the Galois closure of E. We define a function $A_{E,\Phi} : \mathrm{Gal}(E^s/\mathbb{Q}) \longrightarrow \mathbb{Z}$ by

$$A_{E,\Phi}(\sigma) := |\Phi \cap \sigma\Phi|,$$

where $\sigma\Phi := \{\sigma \circ \tau \mid \tau \in \Phi\}$. We also define a function $A^0_{E,\Phi} : \mathrm{Gal}(E^s/\mathbb{Q}) \longrightarrow \mathbb{Q}$ by

$$A^0_{E,\Phi}(\sigma) := \frac{1}{|\,\mathrm{Gal}(E^s/\mathbb{Q})|} \sum_{\tau \in \mathrm{Gal}(E^s/\mathbb{Q})} A_{E,\Phi}(\tau\sigma\tau^{-1}).$$

Let $\mathrm{Irr}(\mathrm{Gal}(E^s/\mathbb{Q}))$ be the set of irreducible Artin characters of the Galois group $\mathrm{Gal}(E^s/\mathbb{Q})$. It can be shown that the function $A^0_{E,\Phi}$ is a class function on the group $\mathrm{Gal}(E^s/\mathbb{Q})$. The set of class functions $f : \mathrm{Gal}(E^s/\mathbb{Q}) \longrightarrow \mathbb{C}$ is a finite dimensional inner product vector space, with inner product given by

$$\langle f_1, f_2 \rangle := \frac{1}{|\,\mathrm{Gal}(E^s/\mathbb{Q})|} \sum_{g \in \mathrm{Gal}(E^s/\mathbb{Q})} f_1(g)\overline{f_2(g)}.$$

It is known that the set of irreducible Artin characters $\mathrm{Irr}(\mathrm{Gal}(E^s/\mathbb{Q}))$ forms an orthonormal basis for this inner product space. Hence by basic linear algebra we know that the function $A^0_{E,\Phi}$ can be expressed as

$$A_{E,\Phi}^0 = \sum_{\chi \in \mathrm{Irr}(\mathrm{Gal}(E^s/\mathbb{Q}))} \langle A_{E,\Phi}, \chi \rangle \chi.$$

With all these preliminaries, we can finally state the Colmez conjecture as follows.

Conjecture 1.2.1 (Colmez)**.** *The Faltings height of X_Φ is given by*

$$h_{\mathrm{Fal}}(X_\Phi) = - \sum_{\chi \in \mathrm{Irr}(\mathrm{Gal}(E^s/\mathbb{Q}))} \langle A_{E,\Phi}, \chi \rangle \left(\frac{L'(\chi, 0)}{L(\chi, 0)} + \frac{1}{2} \log \left(\mathfrak{f}_\chi \right) \right),$$

where $L(\chi, s)$ is the Artin L–function associated to the character χ and $\mathfrak{f}_\chi$ is the corresponding analytic Artin conductor of χ.

In the introduction to chapter 3 we will see how the Colmez conjecture can be seen as a geometric reformulation of the classical Chowla-Selberg formula in the case in which the CM abelian variety is a CM elliptic curve.

Recently there has been increased interest in the Colmez conjecture because of the important role that it played in Tsimerman's proof [Tsi15] of the André-Oort conjecture for the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g.

In chapter 3, we will study the Colmez conjecture for non-abelian CM fields.

2. THE CHOWLA-SELBERG FORMULA FOR ABELIAN CM FIELDS*

2.1 Introduction

To establish a Chowla-Selberg formula for abelian CM fields, we will follow the basic structure of the argument described in Chapter 1.

The following facts concerning Hilbert modular varieties and CM points are explained in detail in Sections 2.3 and 2.4.

Let $F/\mathbb{Q}$ be a totally real field of degree n. Let $\mathcal{O}_F$ be the ring of integers, $\mathcal{O}_F^\times$ be the group of units, d_F be the absolute value of the discriminant, and $\zeta_F(s)$ be the Dedekind zeta function. Let $z = (z_1, \ldots, z_n) \in \mathbb{H}^n$. The Hilbert modular group $\mathrm{SL}_2(\mathcal{O}_F)$ acts componentwise on $\mathbb{H}^n$ by linear fractional transformations.

Let E be a CM extension of F and $\Phi = \{\sigma_1, \ldots, \sigma_n\}$ be a CM type for E. Let h_E be the class number of E, and assume that F has narrow class number 1. Given an ideal class $C \in \mathrm{CL}(E)$, let $z_{\mathfrak{a}}$ be a CM point corresponding to the inverse class $[\mathfrak{a}] = C^{-1}$. To ease notation, we identify the CM point $z_{\mathfrak{a}}$ with its image $\Phi(z_{\mathfrak{a}}) \in \mathbb{H}^n$ under the CM type Φ. Let

$$\mathcal{CM}(E, \Phi, \mathcal{O}_F) := \{z_{\mathfrak{a}} : \ [\mathfrak{a}] \in \mathrm{CL}(E)\}$$

be a set of CM points of type (E, Φ). This is a CM zero-cycle on the Hilbert modular variety $\mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^n$.

We will establish the following analog of (1.3),

$$\sum_{[\mathfrak{a}]\in \mathrm{CL}(E)} \log\left(H(z_{\mathfrak{a}})\right) = \frac{h_E}{2}\left\{\log\left(\frac{\sqrt{d_E}}{2^n d_F}\right) - \frac{1}{n}\frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)} + \frac{L'(\chi_{E/F}, 0)}{L(\chi_{E/F}, 0)}\right\}, \qquad (2.1)$$

where $H : \mathbb{H}^n \to \mathbb{R}^+$ is a $\mathrm{SL}_2(\mathcal{O}_F)$-invariant function analogous to $G(z)$ which arises from a renormalized Kronecker limit formula for the non-holomorphic Hilbert modular Eisenstein series (see Section 2.3, and in particular, equation (2.10)), and $L(\chi_{E/F}, s)$ is the L–function of the

---

*Sections of this chapter are reprinted with permission from Adrian Barquero-Sanchez and Riad Masri (2016), *The Chowla-Selberg formula for abelian CM fields and Faltings heights*. Compositio Mathematica, **152**, pp 445–476 doi:10.1112/S0010437X15007629. Published online: 24 September 2015.

quadratic character $\chi_{E/F}$ associated by class field theory to the CM extension E/F.

Assume now that E is *abelian* over $\mathbb{Q}$. Then $F \subset E \subset \mathbb{Q}(\zeta_N)$ for some primitive N-th root of unity $\zeta_N := e^{2\pi i/N}$. Let H_E (resp. H_F) be the subgroup of $G_N := \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ which fixes E (resp. F). Using the isomorphism $G_N \cong (\mathbb{Z}/N\mathbb{Z})^\times$, one defines the group of Dirichlet characters associated to E (resp. F) by

$$X_E := \{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} : \ \chi_{|_{H_E}} \equiv 1\}$$

(resp. X_F). Clearly, we have $H_E \leq H_F$ and $X_F \leq X_E$.

Given a Dirichlet character $\chi \in X_E$, let $L(\chi, s)$ denote the L–function of the primitive Dirichlet character of conductor c_χ which induces χ. The Gauss sum of $\chi \in X_E$ is defined by

$$\tau(\chi) := \sum_{k=1}^{c_\chi} \chi(k)\zeta_{c_\chi}^k, \quad \zeta_{c_\chi} := e^{2\pi i/c_\chi}.$$

We will establish the identity

$$\frac{L'(\chi_{E/F}, s)}{L(\chi_{E/F}, s)} = \sum_{\chi \in X_E \setminus X_F} \frac{L'(\chi, s)}{L(\chi, s)},$$

hence to evaluate the logarithmic derivative of $L(\chi_{E/F}, s)$ at $s = 0$, we must evaluate $L'(\chi, 0)$ for $\chi \in X_E \setminus X_F$. We can express $L'(\chi, 0)$ in terms of values of $\log(\Gamma(s))$ at rational numbers as in (1.8).

On the other hand, we will reduce the evaluation of the logarithmic derivative of $\zeta_F^{(n-1)}(s)$ at $s = 0$ to the evaluation of $L'(\chi, 1)$ for nontrivial $\chi \in X_F$. Because each $\chi \in X_F$ is even, $L'(\chi, 1)$ cannot be expressed in terms of values of $\log(\Gamma(s))$ at rational numbers (this is due to the sign of the functional equation for $L(\chi, s)$ when χ is even). However, Deninger [Den84] showed how to evaluate $L'(\chi, 1)$ in terms of values of the function

$$R(w) := \partial_s^2 \zeta(0, w), \quad \mathrm{Re}(w) > 0$$

at rational numbers. The function $R(w)$ is analogous to $\log(\Gamma(s)/\sqrt{2\pi})$, as we now explain.

Consider the Taylor expansion

$$\zeta(s, x) = \frac{1}{2} - x + \log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right) s + R(x)s^2 + O(s^3), \quad x > 0.$$

By the Bohr-Mollerup theorem, $\log(\Gamma(x)/\sqrt{2\pi})$ is the unique function $f : \mathbb{R}^+ \to \mathbb{R}$ such that

$$f(x+1) - f(x) = \log(x),$$

$f(1) = \zeta'(0) = -\log(\sqrt{2\pi})$, and $f(x)$ is convex on $\mathbb{R}^+$. Using properties of the Hurwitz zeta function, one can show that $\partial_s \zeta(0, x)$ also satisfies these three conditions, hence by uniqueness, one recovers Lerch's identity

$$\partial_s \zeta(0, x) = \log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right).$$

Note that using the limit

$$\Gamma(x) = \lim_{n\to\infty} \frac{n! n^x}{x(x+1)\cdots(x+n)}, \quad x > 0$$

one has

$$\log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right) = \lim_{n\to\infty}\left(\zeta'(0) + x\log(n) - \log(x) - \sum_{k=1}^{n-1}(\log(x+k) - \log(k))\right). \tag{2.2}$$

Deninger [Den84, Theorem 2.2] proved a similar result for the functions $\partial_s^\alpha \zeta(0, x), \alpha \in \mathbb{Z}^+$, by modeling the proof of Lerch's identity just described. In particular, for $\alpha = 2$ he proved that $R(x)$ is the unique function $R : \mathbb{R}^+ \to \mathbb{R}$ such that

$$R(x+1) - R(x) = \log^2(x),$$

$R(1) = -\zeta''(0)$, and $R(x)$ is convex on (e, ∞). He also proved the following analog of (2.2),

$$R(x) = \lim_{n\to\infty}\left(-\zeta''(0) + x\log^2(n) - \log^2(x) - \sum_{k=1}^{n-1}\left(\log^2(x+k) - \log^2(k)\right)\right).$$

Define the function

$$\Gamma_2(w) := \exp(R(w)), \quad \text{Re}(w) > 0$$

which is analogous to $\Gamma(s)/\sqrt{2\pi}$. Note that $\Gamma_2(w)$ does not extend to a meromorphic function on $\mathbb{C}$ (see e.g. [Den84, Remark (2.4)]).

We can now state our Chowla-Selberg formula for abelian CM fields.

Theorem 2.1.1. *Let $F/\mathbb{Q}$ be a totally real field of degree n with narrow class number 1. Let E/F*

be a CM extension with $E/\mathbb{Q}$ abelian. Let Φ be a CM type for E and

$$\mathcal{CM}(E,\Phi,\mathcal{O}_F) = \{z_{\mathfrak{a}} :\ [\mathfrak{a}] \in \mathrm{CL}(E)\}$$

be a set of CM points of type (E,Φ). Then

$$\prod_{[\mathfrak{a}]\in\mathrm{CL}(E)} H(z_{\mathfrak{a}}) = c_1(E,F,n) \prod_{\chi\in X_E\setminus X_F} \prod_{k=1}^{c_\chi} \Gamma\left(\frac{k}{c_\chi}\right)^{\frac{h_E\chi(k)}{2L(\chi,0)}} \prod_{\substack{\chi\in X_F\\ \chi\neq 1}} \prod_{k=1}^{c_\chi} \Gamma_2\left(\frac{k}{c_\chi}\right)^{\frac{h_E\tau(\chi)\overline{\chi}(k)}{2c_\chi L(\chi,1)}},$$

where

$$c_1(E,F,n) := \left(\frac{d_F}{2^{n+1}\pi\sqrt{d_E}}\right)^{\frac{h_E}{2}}.$$

Remark 2.1.2. Given a triple (E,F,Φ) satisfying the hypotheses of Theorem 2.1.1, one can obtain explicit examples by determining the group of characters X_E (resp. X_F) and a set of CM points $\mathcal{CM}(E,\Phi,\mathcal{O}_F)$ of type (E,Φ) (see Section 2.2).

Remark 2.1.3. The narrow class number 1 assumption in Theorem 2.1.1 could be removed by working adelically. We have worked in the classical language to emphasize parallels with the original Chowla-Selberg formula.

When $E/\mathbb{Q}$ is a multiquadratic extension (equivalently, Gal$(E/\mathbb{Q})$ is an elementary abelian 2-group), one can explicitly determine the group of characters X_E (resp. X_F), leading to the following result.

Theorem 2.1.4. *Let $d_1,\dots,d_{\ell+1}$ be squarefree, pairwise relatively prime integers with $d_i > 0$ for $i = 1,\dots,\ell$ and $d_{\ell+1} < 0$ where $\ell = 1$ or 2. Assume that $F = \mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_\ell})$ has narrow class number 1 and let $E = F(\sqrt{d_{\ell+1}})$. Let χ_α (resp. χ_β) be the Kronecker symbol associated to the quadratic field $\mathbb{Q}(\sqrt{\alpha})$ (resp. $\mathbb{Q}(\sqrt{\beta})$), where $\alpha = d_1^{e_1}\cdots d_\ell^{e_\ell} d_{\ell+1}$ (resp. $\beta = d_1^{e_1}\cdots d_\ell^{e_\ell}$) for $\mathbf{e} = (e_1,\dots,e_\ell) \in \{0,1\}^\ell$. Then*

$$\prod_{[\mathfrak{a}]\in\mathrm{CL}(E)} H(z_{\mathfrak{a}}) = c_1(E,F,2^\ell) \prod_{\substack{\mathbf{e}\in\{0,1\}^\ell\\ \alpha=d_1^{e_1}\cdots d_\ell^{e_\ell}d_{\ell+1}}} \prod_{k=1}^{c_\alpha} \Gamma\left(\frac{k}{c_\alpha}\right)^{\frac{h_E\chi_\alpha(k)w_\alpha}{4h_\alpha}} \prod_{\substack{\mathbf{e}\in\{0,1\}^\ell\\ \beta=d_1^{e_1}\cdots d_\ell^{e_\ell}\neq 1}} \prod_{k=1}^{c_\beta} \Gamma_2\left(\frac{k}{c_\beta}\right)^{\frac{h_E\chi_\beta(k)}{4h_\beta\log(\varepsilon_\beta)}}.$$

Remark 2.1.5. The restriction to $\ell = 1$ or 2 in Theorem 2.1.4 is made for the following reasons. By Fröhlich [Fro83, Theorem 5.6], if F is a totally real abelian field in which at least 5 rational primes ramify, then the class number of F is even. If $\ell \geq 5$, then at least 5 rational primes ramify in $F = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$, hence F cannot have narrow class number 1 (since the class number divides the narrow class number). It is well-known that there exist real quadratic fields of narrow class number 1, and these must be of the form $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{p})$ for a prime $p \equiv 1 \pmod 4$ (see e.g. [CH88, Corollary 12.5]). This leaves the possibilities $\ell = 2, 3$ or 4. One can compute many examples of real biquadratic fields with narrow class number 1. We wrote a program in SAGE which calculates the narrow class numbers of the real biquadratic fields $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ for p and q primes with $2 \leq p < q \leq n$. For example, if $n = 30$ there are 6 real biquadratic fields in this list with narrow class number 1, corresponding to the pairs (p, q) given by $\{(2,5), (2,13), (2,29), (5,13), (5,17), (17,29)\}$. On the other hand, for $\ell = 3$ or 4 the class number of $F = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$ can be 1 (see e.g. [Mou09]), but we were unable to find any examples with narrow class number 1.

For CM biquadratic fields of class number 1, we have the following result.

Theorem 2.1.6. *Let $p = 2$ or $p \equiv 1 \pmod 4$ be a prime such that $F = \mathbb{Q}(\sqrt{p})$ has narrow class number 1. Let $d < 0$ be a squarefree integer relatively prime to p such that $E = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ has class number 1. Let Δ_p, Δ_d and Δ_{pd} be the discriminants of the quadratic fields $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{pd})$, resp., and assume that Δ_p and Δ_d are relatively prime. Then*

$$H(z_{\mathcal{O}_E}) = \frac{1}{2\sqrt{2\pi|\Delta_d|}} \prod_{k=1}^{|\Delta_d|} \Gamma\left(\frac{k}{|\Delta_d|}\right)^{\frac{\chi_d(k)w_d}{4h_d}} \prod_{k=1}^{|\Delta_{pd}|} \Gamma\left(\frac{k}{|\Delta_{pd}|}\right)^{\frac{\chi_{pd}(k)w_{pd}}{4h_{pd}}} \prod_{k=1}^{\Delta_p} \Gamma_2\left(\frac{k}{\Delta_p}\right)^{\frac{\chi_p(k)}{4\log(\varepsilon_p)}},$$

where

$$z_{\mathcal{O}_E} = \begin{cases} (\sqrt{d}, \sqrt{d}), & d \equiv 2, 3 \pmod 4 \\ \left(\frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\right), & d \equiv 1 \pmod 4 \end{cases}$$

is a CM point of type (E, Φ) for $\Phi = \{\sigma_1 = \mathrm{id},\ \sigma_2 : \sqrt{p} \mapsto -\sqrt{p}, \sqrt{d} \mapsto \sqrt{d}\}$.

2.1.1 Connection to some existing work

We conclude the introduction by discussing the connection between our results and some existing work. A version of the Chowla-Selberg formula for CM fields was given by Moreno [Mor83] over 30 years ago. The foundation for such a generalization was laid by Asai [Asa70] in the late 1960's, who established a Kronecker limit formula for Eisenstein series associated to any number field of class number 1. Following Weil's [Wei76, Chapter IX] beautiful exposition of the classical Chowla-Selberg formula (which involves a renormalized Kronecker limit formula for Eisenstein series over $\mathbb{Q}$), Moreno obtained an expression relating values of a Hilbert modular function at special points on a Hilbert-Blumenthal variety to the logarithmic derivative of $L(\chi_{E/F}, s)$ at $s = 0$. Moreno then used Shintani's [Shi77a, Shi76] remarkable work on special values of L–functions to express $L'(\chi_{E/F}, 0)$ in terms of certain Barnes-type multiple gamma functions (formulas of this type resulting from Shintani's work can be viewed as "higher" analogs of Lerch's identity). Putting things together, he obtained a version of the Chowla-Selberg formula for CM fields (see [Mor83, Main Theorem, p. 242]). The starting point of the work done in this chapter was that it should be possible to give a much more explicit version of the Chowla-Selberg formula for abelian CM fields. The initial structure of the proof is similar to that of Moreno's, namely to arrive at a version of the identity (2.1), though there are important differences. For example, we identify the CM zero-cycles along which we evaluate the Hilbert modular Eisenstein series, which allows us to give explicit examples of our formula (see Section 2.2).

2.2 Examples

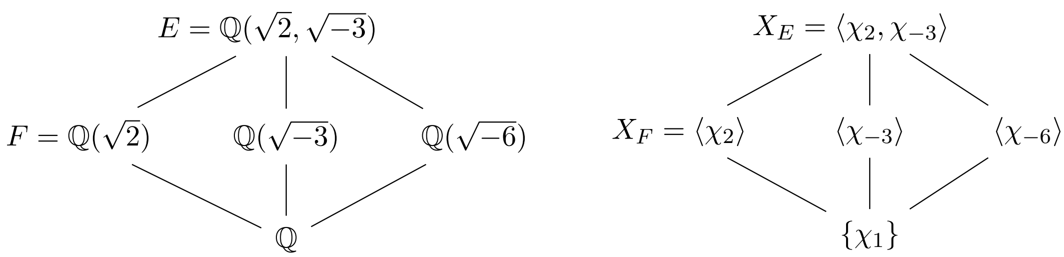
In this section we give some explicit examples of the Chowla-Selberg formula for abelian CM fields. Recall that the function $H : \mathbb{H}^n \to \mathbb{R}^+$ appearing in these examples is a $\mathrm{SL}_2(\mathcal{O}_F)$-invariant function analogous to $G(z) := \sqrt{\mathrm{Im}(z)}|\eta(z)|^2$ which arises from a renormalized Kronecker limit formula for the non-holomorphic Hilbert modular Eisenstein series. See (2.10) for the definition of $H(z)$. For background and notation regarding CM points, see Section 2.4.

Example 2.2.1 (Theorem 2.1.6, $d_1 = 2$ and $d_2 = -3$)**.** Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and $F = \mathbb{Q}(\sqrt{2})$. Then E has class number 1 and F has narrow class number 1. Moreover, $\Delta_2 = 8, \Delta_{-3} = -3$ and $\Delta_{-6} = -24$, so that Δ_2 and Δ_{-3} are relatively prime. The hypotheses of Theorem 2.1.6 are satisfied, so it remains to determine the quantities in the identity stated in Theorem 2.1.6.

Since $-3 \equiv 1 \mod 4$, the CM point of type (E, Φ) corresponding to the class $[\mathcal{O}_E]$ is given by

$$z_{\mathcal{O}_E} = \left(\frac{1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\right).$$

The groups of characters associated to E and F are $X_E = \{\chi_1, \chi_{-3}, \chi_2, \chi_{-6}\}$ and $X_F = \{\chi_1, \chi_2\}$, resp., hence $X_E \setminus X_F = \{\chi_{-3}, \chi_{-6}\}$. We have the following correspondence between subfields and associated character groups:



The characters $\chi_2 = \left(\frac{8}{\cdot}\right)$, $\chi_{-6} = \left(\frac{-24}{\cdot}\right)$ and $\chi_{-3} = \left(\frac{-3}{\cdot}\right)$ have conductors 8, 24 and 3, resp. (note the character χ_2 generates X_F and the characters χ_{-3} and χ_2 generate X_E).

The following tables list the values of these characters. In particular, Table 2.1 lists the values of $\chi_2 = \left(\frac{8}{\cdot}\right)$, Table 2.2 lists the values of $\chi_{-6} = \left(\frac{-24}{\cdot}\right)$, and Table 2.3 lists the values of $\chi_{-3} = \left(\frac{-3}{\cdot}\right)$.

Values of $\chi_2 = \left(\frac{8}{\cdot}\right)$				
k	1	3	5	7
$\chi_2(k)$	1	-1	-1	1

Table 2.1: Character values $\chi_2(k)$.

Values of $\chi_{-6} = \left(\frac{-24}{\cdot}\right)$								
k	1	5	7	11	13	17	19	23
$\chi_{-6}(k)$	1	1	1	1	-1	-1	-1	-1

Table 2.2: Character values $\chi_{-6}(k)$.

Values of $\chi_{-3} = \left(\frac{-3}{\cdot}\right)$		
k	1	2
$\chi_{-3}(k)$	1	-1

Table 2.3: Character values $\chi_{-3}(k)$.

The fundamental unit of F is $\varepsilon_2 = 1 + \sqrt{2}$, and we have $h_{-3} = 1, h_{-6} = 2, w_{-3} = 6$ and $w_{-6} = 2$.

Substituting these quantities in Theorem 2.1.6 yields

$$H(z_{\mathcal{O}_E}) = \frac{1}{2\sqrt{6}\pi} \prod_{k=1}^{3} \Gamma\left(\frac{k}{3}\right)^{\frac{3\chi_{-3}(k)}{2}} \prod_{k=1}^{24} \Gamma\left(\frac{k}{24}\right)^{\frac{\chi_{-6}(k)}{4}} \prod_{k=1}^{8} \Gamma_2\left(\frac{k}{8}\right)^{\frac{\chi_2(k)}{4\log(1+\sqrt{2})}}.$$

After expanding each product on the right hand side, we get

$$H\left(\frac{1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\right) = \frac{1}{2\sqrt{6}\pi} \left(\frac{\Gamma\left(\frac{1}{3}\right)}{\Gamma\left(\frac{2}{3}\right)}\right)^{3/2} \left(\frac{\Gamma\left(\frac{1}{24}\right)\Gamma\left(\frac{5}{24}\right)\Gamma\left(\frac{7}{24}\right)\Gamma\left(\frac{11}{24}\right)}{\Gamma\left(\frac{13}{24}\right)\Gamma\left(\frac{17}{24}\right)\Gamma\left(\frac{19}{24}\right)\Gamma\left(\frac{23}{24}\right)}\right)^{1/4}$$

$$\times \left(\frac{\Gamma_2\left(\frac{1}{8}\right)\Gamma_2\left(\frac{7}{8}\right)}{\Gamma_2\left(\frac{3}{8}\right)\Gamma_2\left(\frac{5}{8}\right)}\right)^{\frac{1}{4\log(1+\sqrt{2})}}.$$

Example 2.2.2 (Theorem 2.1.4, $d_1 = 2$ and $d_2 = -5$)**.** Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{-5})$ and $F = \mathbb{Q}(\sqrt{2})$. Then E has class number 2 and F has narrow class number 1. Moreover, $d_1 = 2$ and $d_2 = -5$

are squarefree and relatively prime. The hypotheses of Theorem 2.1.4 are satisfied, so it remains to determine the quantities in the identity stated in Theorem 2.1.4.

The four embeddings of E are determined by

$$\begin{aligned} \sigma_1 &: \sqrt{2} \longmapsto \sqrt{2}, \quad && \sqrt{-5} \longmapsto \sqrt{-5} \\ \sigma_2 &: \sqrt{2} \longmapsto -\sqrt{2}, && \sqrt{-5} \longmapsto \sqrt{-5} \\ \sigma_3 &: \sqrt{2} \longmapsto \sqrt{2}, && \sqrt{-5} \longmapsto -\sqrt{-5} \\ \sigma_4 &: \sqrt{2} \longmapsto -\sqrt{2}, && \sqrt{-5} \longmapsto -\sqrt{-5}. \end{aligned}$$

Fix the choice of CM type $\Phi = \{\sigma_1, \sigma_2\}$. The class group of E is given by $\mathrm{CL}(E) = \{[\mathcal{O}_E], [\mathfrak{a}]\}$ where

$$[\mathcal{O}_E] = [\mathcal{O}_F(10 - \sqrt{2}) + \mathcal{O}_F(\sqrt{-5} + 18\sqrt{2} - 1)],$$

$$[\mathfrak{a}] = [\mathcal{O}_F 2 + \mathcal{O}_F(\sqrt{-5} - \sqrt{2} + 1)].$$

Then

$$z_{\mathcal{O}_E} = \frac{\sqrt{-5} + 18\sqrt{2} - 1}{10 - \sqrt{2}} \qquad \text{and} \qquad z_{\mathfrak{a}} = \frac{\sqrt{-5} - \sqrt{2} - 1}{2}$$

are CM points of type (E, Φ) corresponding to the classes $[\mathcal{O}_F]$ and $[\mathfrak{a}]$ resp., since

$$\Phi(z_{\mathcal{O}_E}) = \left(\frac{\sqrt{-5} + 18\sqrt{2} - 1}{10 - \sqrt{2}}, \frac{\sqrt{-5} - 18\sqrt{2} - 1}{10 + \sqrt{2}} \right) \in E^\times \cap \mathbb{H}^2$$

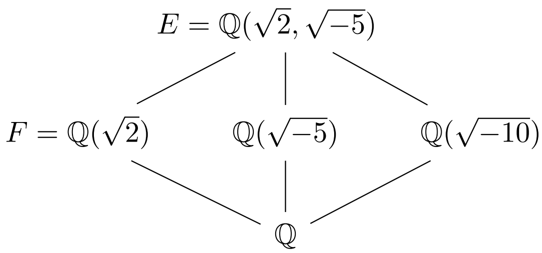
and

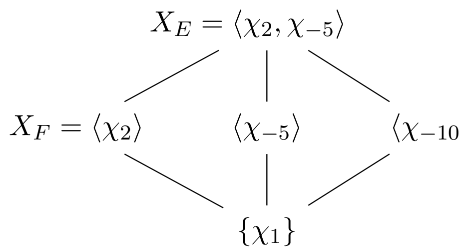
$$\Phi(z_{\mathfrak{a}}) = \left(\frac{\sqrt{-5} - \sqrt{2} - 1}{2}, \frac{\sqrt{-5} + \sqrt{2} - 1}{2} \right) \in E^\times \cap \mathbb{H}^2.$$

The absolute values of the discriminants of E and F are $d_E = 6400$ and $d_F = 8$, resp., hence the constant

$$c_1(E, F, 2) = \frac{8}{2^3 \pi \sqrt{6400}} = \frac{1}{80\pi}.$$

The groups of characters associated to E and F are $X_E = \{\chi_1, \chi_2, \chi_{-5}, \chi_{-10}\}$ and $X_F = \{\chi_1, \chi_2\}$, resp., hence $X_E \setminus X_F = \{\chi_{-5}, \chi_{-10}\}$. We have the following correspondence between subfields and associated character groups:





The characters $\chi_2 = \left(\frac{8}{\cdot}\right)$, $\chi_{-5} = \left(\frac{-20}{\cdot}\right)$ and $\chi_{-10} = \left(\frac{-40}{\cdot}\right)$ have conductors 8, 20 and 40, resp. (note the character χ_2 generates X_F and the characters χ_2 and χ_{-5} generate X_E). The following tables give the values of these characters. In particular, Table 2.4 gives the values of $\chi_2 = \left(\frac{8}{\cdot}\right)$, Table 2.5 gives the values of $\chi_{-5} = \left(\frac{-20}{\cdot}\right)$, and Table 2.6 gives the values of $\chi_{-10} = \left(\frac{-40}{\cdot}\right)$.

Values of $\chi_2 = \left(\frac{8}{\cdot}\right)$				
k	1	3	5	7
$\chi_2(k)$	1	-1	-1	1

Table 2.4: Values of $\chi_2 = \left(\frac{8}{\cdot}\right)$.

Values of $\chi_{-5} = \left(\frac{-20}{\cdot}\right)$								
k	1	3	7	9	11	13	17	19
$\chi_{-5}(k)$	1	1	1	1	-1	-1	-1	-1

Table 2.5: Values of $\chi_{-5} = \left(\frac{-20}{\cdot}\right)$.

Values of $\chi_{-10} = \left(\frac{-40}{\cdot}\right)$																
k	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
$\chi_{-10}(k)$	1	-1	1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1

Table 2.6: Values of $\chi_{-10} = \left(\frac{-40}{\cdot}\right)$.

The fundamental unit of F is $\varepsilon_2 = 1 + \sqrt{2}$, and we have $h_2 = 1$, $h_{-5} = 2$, $h_{-10} = 2$, $w_2 = 2$, $w_{-5} = 2$ and $w_{-10} = 2$.

Substituting the preceding quantities in Theorem 2.1.4 yields

$$H(z_{\mathcal{O}_E})H(z_{\mathfrak{a}}) = \frac{1}{80\pi}\prod_{k=1}^{20}\Gamma\left(\frac{k}{20}\right)^{\frac{\chi_{-5}(k)}{2}}\prod_{k=1}^{40}\Gamma\left(\frac{k}{40}\right)^{\frac{\chi_{-10}(k)}{2}}\prod_{k=1}^{8}\Gamma_2\left(\frac{k}{8}\right)^{\frac{\chi_2(k)}{2\log(1+\sqrt{2})}}.$$

After expanding each product on the right hand side, we get

$$H\left(\frac{\sqrt{-5}+18\sqrt{2}-1}{10-\sqrt{2}}, \frac{\sqrt{-5}-18\sqrt{2}-1}{10+\sqrt{2}}\right) H\left(\frac{\sqrt{-5}-\sqrt{2}-1}{2}, \frac{\sqrt{-5}+\sqrt{2}-1}{2}\right)$$

$$= \frac{1}{80\pi}\left(\frac{\Gamma(\frac{1}{20})\Gamma(\frac{3}{20})\Gamma(\frac{7}{20})\Gamma(\frac{9}{20})}{\Gamma(\frac{11}{20})\Gamma(\frac{13}{20})\Gamma(\frac{17}{20})\Gamma(\frac{19}{20})}\right)^{\frac{1}{2}}\left(\frac{\Gamma(\frac{1}{40})\Gamma(\frac{7}{40})\Gamma(\frac{9}{40})\Gamma(\frac{11}{40})\Gamma(\frac{13}{40})\Gamma(\frac{19}{40})\Gamma(\frac{23}{40})\Gamma(\frac{37}{40})}{\Gamma(\frac{3}{40})\Gamma(\frac{17}{40})\Gamma(\frac{21}{40})\Gamma(\frac{27}{40})\Gamma(\frac{29}{40})\Gamma(\frac{31}{40})\Gamma(\frac{33}{40})\Gamma(\frac{39}{40})}\right)^{\frac{1}{2}}$$

$$\times\left(\frac{\Gamma_2(\frac{1}{8})\Gamma_2(\frac{7}{8})}{\Gamma_2(\frac{3}{8})\Gamma_2(\frac{5}{8})}\right)^{\frac{1}{2\log(1+\sqrt{2})}}.$$

Example 2.2.3 (Theorem 2.1.1, $E=\mathbb{Q}(\zeta_5)$ and $F=\mathbb{Q}(\sqrt{5})$)**.** Let $E=\mathbb{Q}(\zeta_5)$ and $F=\mathbb{Q}(\sqrt{5})$. Then E is a CM extension of the real quadratic field F with $E/\mathbb{Q}$ abelian (a cyclic quartic extension). Moreover, E has class number 1 and F has narrow class number 1. The hypotheses of Theorem 2.1.1 are satisfied, so it remains to determine the quantities in the identity stated in Theorem 2.1.1.

The four embeddings of E are determined by $\sigma_i(\zeta_5)=\zeta_5^i$ for $i=1,\dots,4$. Fix the choice of CM type $\Phi=\{\sigma_1,\sigma_2\}$ for E. We have $\mathcal{O}_E=\mathcal{O}_F+\mathcal{O}_F\zeta_5$, thus $z_{\mathcal{O}_E}=\zeta_5$ is a CM point of type (E,Φ) since $\Phi(z_{\mathcal{O}_E})=(\zeta_5,\zeta_5^2)\in E^\times\cap\mathbb{H}^2$.

The absolute values of the discriminants are $d_E=125$ and $d_F=5$, resp., hence the constant

$$c_1(E,F,2)=\left(\frac{1}{8\pi\sqrt{5}}\right)^{1/2}.$$

Since $E=\mathbb{Q}(\zeta_5)$ is cyclotomic, we have $X_E=\widehat{(\mathbb{Z}/5\mathbb{Z})^\times}$. The group of Dirichlet characters modulo 5 is given by the characters listed in Table 2.7.

Dirichlet characters modulo 5				
	1	2	3	4
χ_1	1	1	1	1
χ	1	i	$-i$	-1
$\chi^2 = \chi_5 = \left(\frac{5}{\cdot}\right)$	1	-1	-1	1
$\chi^3 = \overline{\chi}$	1	$-i$	i	-1

Table 2.7: The Dirichlet characters modulo 5.

We have the following correspondence between subfields and associated character groups:

$$\begin{array}{ccc} E = \mathbb{Q}(\zeta_5) & & X_E = \langle \chi \rangle \\ | & & | \\ F = \mathbb{Q}(\sqrt{5}) & & X_F = \langle \chi_5 \rangle \\ | & & | \\ \mathbb{Q} & & \{\chi_1\} \end{array}$$

It follows that $X_F = \{\chi_1, \chi^2\} = \{\chi_1, \chi_5\}$ and $X_E \setminus X_F = \{\chi, \chi^3\} = \{\chi, \overline{\chi}\}$.

The L–values corresponding to the characters $\chi, \overline{\chi}$ are given in terms of generalized Bernoulli numbers by

$$L(\chi, 0) = -B_1(\chi) = \frac{3}{5} + \frac{1}{5}i \quad \text{and} \quad L(\overline{\chi}, 0) = -B_1(\overline{\chi}) = \frac{3}{5} - \frac{1}{5}i.$$

Moreover, by the class number formula we have

$$L(\chi_5, 1) = \frac{2\log(\frac{1+\sqrt{5}}{2})}{\sqrt{5}},$$

the Gauss sum is evaluated as $\tau(\chi_5) = \sqrt{5}$, and the fundamental unit of F is $\varepsilon_5 = \frac{1+\sqrt{5}}{2}$.

Substituting the preceding quantities in Theorem 2.1.1 yields

$$H(z_{\mathcal{O}_E}) = \left(\frac{1}{8\pi\sqrt{5}}\right)^{1/2} \prod_{k=1}^{5} \Gamma\left(\frac{k}{5}\right)^{\frac{\chi(k)}{2\left(\frac{3}{5}+\frac{1}{5}i\right)}} \prod_{k=1}^{5} \Gamma\left(\frac{k}{5}\right)^{\frac{\overline{\chi}(k)}{2\left(\frac{3}{5}-\frac{1}{5}i\right)}} \prod_{k=1}^{5} \Gamma_2\left(\frac{k}{5}\right)^{\frac{\chi_5(k)}{4\log\left(\frac{1+\sqrt{5}}{2}\right)}}.$$

After expanding each product on the right hand side, we get

$$H(\zeta_5, \zeta_5^2) = \left(\frac{1}{8\pi\sqrt{5}}\right)^{1/2} \left(\frac{\Gamma\left(\frac{1}{5}\right)}{\Gamma\left(\frac{4}{5}\right)}\right)^{3/2} \left(\frac{\Gamma\left(\frac{2}{5}\right)}{\Gamma\left(\frac{3}{5}\right)}\right)^{1/2} \left(\frac{\Gamma_2\left(\frac{1}{5}\right)\Gamma_2\left(\frac{4}{5}\right)}{\Gamma_2\left(\frac{2}{5}\right)\Gamma_2\left(\frac{3}{5}\right)}\right)^{\frac{1}{4\log\left(\frac{1+\sqrt{5}}{2}\right)}}.$$

2.3 Hilbert modular Eisenstein series

In this section we establish a renormalized Kronecker limit formula for the non-holo-morphic Hilbert modular Eisenstein series. Moreno stated such a formula in [Mor83, Section 3.1], and gave a very brief explanation as to how it is derived from a Fourier expansion of Asai [Asa70] for the Eisenstein series. Here we give a similar formula using a slightly different form of the Fourier expansion (the Fourier expansion we use for the Hilbert modular Eisenstein series goes back to Hecke).

Let F be a totally real number field of degree n over $\mathbb{Q}$ with embeddings $\tau_1, \ldots, \tau_n$. Let

$$z = x + iy = (z_1, \ldots, z_n) \in \mathbb{H}^n$$

where $\mathbb{H}$ denotes the complex upper half-plane. Let $\mathcal{O}_F$ be the ring of integers of F and $\mathrm{SL}_2(\mathcal{O}_F)$ be the Hilbert modular group. Then $\mathrm{SL}_2(\mathcal{O}_F)$ acts componentwise on $\mathbb{H}^n$ by linear fractional transformations,

$$Mz = (\tau_1(M)z_1, \ldots, \tau_n(M)z_n), \quad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F)$$

where

$$\tau_j(M) = \begin{pmatrix} \tau_j(\alpha) & \tau_j(\beta) \\ \tau_j(\gamma) & \tau_j(\delta) \end{pmatrix}.$$

Let

$$N(y(z)) := \prod_{j=1}^{n} \mathrm{Im}(z_j) = \prod_{j=1}^{n} y_j$$

denote the product of the imaginary parts of the components of $z \in \mathbb{H}^n$. Define the non-holomorphic Hilbert modular Eisenstein series

$$E(z,s) := \sum_{M \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathcal{O}_F)} N(y(Mz))^s, \quad z \in \mathbb{H}^n, \quad \mathrm{Re}(s) > 1$$

where

$$\Gamma_\infty = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F) \right\}.$$

Furthermore, let

$$N(a+bz) := \prod_{j=1}^{n} (\sigma_j(a) + \sigma_j(b) z_j)$$

for $(a,b) \in \mathcal{O}_F \times \mathcal{O}_F$ and define the Epstein zeta function

$$Z(z,s) := \sideset{}{'}\sum_{(a,b) \in \mathcal{O}_F \times \mathcal{O}_F / \mathcal{O}_F^\times} \frac{N(y(z))^s}{|N(a+bz)|^{2s}}, \quad z \in \mathbb{H}^n, \quad \mathrm{Re}(s) > 1$$

where the sum is over a complete set of nonzero, nonassociated representatives of $\mathcal{O}_F \times \mathcal{O}_F$ (recall that (a,b) and (a',b') are said to be *associated* if there exists a unit $\epsilon \in \mathcal{O}_F^\times$ such that $(a,b) = (\epsilon a', \epsilon b')$). One has the identity

$$Z(z,s) = \zeta_F(2s) E(z,s), \tag{2.3}$$

where $\zeta_F(s)$ is the Dedekind zeta function of F.

Define the completed Eisenstein series

$$E^*(z,s) := \zeta_F^*(2s) E(z,s) \tag{2.4}$$

where

$$\zeta_F^*(s) := d_F^{s/2} \pi^{-ns/2} \Gamma(s/2)^n \zeta_F(s),$$

is the completed Dedekind zeta function of F.

From [vdG88, Proposition 6.9], equation (2.4), and the shift $s \mapsto (s+1)/2$, we obtain the renormalized Fourier expansion

$$\begin{aligned} E\left(z, \frac{s+1}{2}\right) &= N(y)^{\frac{s+1}{2}} + \frac{\zeta_F^*(s)}{\zeta_F^*(s+1)} N(y)^{\frac{1-s}{2}} \\ &+ \frac{2^n N(y)^{1/2}}{\zeta_F^*(s+1)} \sum_{\substack{\mu \in \partial_F^{-1}/\mathcal{O}_F^\times \\ \mu \neq 0}} N_{F/\mathbb{Q}}((\mu)\partial_F)^{\frac{s}{2}} \sigma_{-s}((\mu)\partial_F) \prod_{j=1}^{n} K_{\frac{s}{2}}(2\pi |\mu^{(j)}| y_j) e^{2\pi i \,\mathrm{Tr}(\mu x)}, \end{aligned} \tag{2.5}$$

where ∂_F is the different of F,

$$\sigma_\nu(\mathfrak{a}) := \sum_{\mathfrak{b}|\mathfrak{a}} N_{F/\mathbb{Q}}(\mathfrak{b})^\nu$$

is the divisor function,

$$\mathrm{Tr}(\mu x) := \sum_{j=1}^{n} \mu^{(j)} x_j, \quad \mu^{(j)} := \tau_j(\mu)$$

is the trace and

$$K_s(t) := \int_0^\infty e^{-t\cosh x} \cosh(sx) dx$$

is the K-Bessel function of order s.

Let $A(s)$, $B(s)$ and $C(s)$ denote the first, second, and third terms on the right hand side of (2.5), respectively. We compute the first two terms in the Taylor expansion of $E\left(z, \frac{s+1}{2}\right)$ at $s = -1$ by doing this for each of the functions $A(s)$, $B(s)$ and $C(s)$, in turn.

First, observe that

$$A(s) = 1 + \log N(y)^{1/2}(s+1) + O((s+1)^2).$$

Second, we calculate the Taylor expansion

$$B(s) = B(-1) + B'(-1)(s+1) + O(s+1)^2.$$

Since

$$\frac{1}{\zeta_F^*(s)} = d_F^{-s/2}\left(\frac{\pi^{s/2}}{\Gamma(s/2)}\right)^n \frac{1}{\zeta_F(s)}$$

and $\zeta_F(s)$ has a simple pole at $s = 1$, the function $1/\zeta_F^*(s)$ has a simple zero at $s = 1$. Using the functional equation $\zeta_F^*(s) = \zeta_F^*(1-s)$, it follows that

($*$) $1/\zeta_F^*(s)$ has a simple zero at $s = 0$.

Now, by ($*$) we have

$$B(-1) = \frac{\zeta_F^*(-1)}{\zeta_F^*(0)} N(y) = 0.$$

Moreover, an application of the product and quotient rules along with two applications of $(*)$ yields

$$B'(s) = -N(y)^{\frac{1-s}{2}} \zeta_F^*(s) \left(\frac{\frac{d}{ds}\zeta_F^*(s+1)}{\zeta_F^*(s+1)^2} \right) + O(s+1),$$

so that

$$B'(-1) = -N(y)\zeta_F^*(-1)\frac{(\zeta_F^*)'(0)}{\zeta_F^*(0)^2}.$$

A calculation using the Laurent expansion

$$\zeta_F^*(s+1) = \frac{r_F}{s+1} + O(s+1)$$

yields

$$-\frac{\frac{d}{ds}\zeta_F^*(s+1)}{\zeta_F^*(s+1)^2} = \frac{r_F + O(s+1)^2}{\{r_F + O(s+1)\}^2}, \tag{2.6}$$

where r_F is the residue of $\zeta_F^*(s+1)$ at $s = -1$. Hence

$$B'(-1) = \frac{N(y)\zeta_F^*(-1)}{r_F}.$$

Third, we calculate the Taylor expansion

$$C(s) = C(-1) + C'(-1)(s+1) + O(s+1)^2.$$

For convenience, we write

$$C(s) = 2^n N(y)^{1/2} \sum_{\substack{\mu \in \partial_F^{-1}/\mathcal{O}_F^\times \\ \mu \neq 0}} D_\mu(s) e^{2\pi i \operatorname{Tr}(\mu x)},$$

where

$$D_\mu(s) := \frac{N_{F/\mathbb{Q}}((\mu)\partial_F)^{\frac{s}{2}}}{\zeta_F^*(s+1)} \sigma_{-s}((\mu)\partial_F) \prod_{j=1}^n K_{\frac{s}{2}}(2\pi|\mu^{(j)}|y_j).$$

By $(*)$ we have $D_\mu(-1) = 0$, thus $C(-1) = 0$.

To compute $C'(-1)$, it suffices to compute $D'_\mu(-1)$. Using the product rule, two applications of $(*)$, and (2.6) we obtain

$$D'_\mu(-1) = \frac{N_{F/\mathbb{Q}}((\mu)\partial_F)^{-\frac{1}{2}}}{r_F} \sigma_1((\mu)\partial_F) \prod_{j=1}^n K_{-\frac{1}{2}}(2\pi|\mu^{(j)}|y_j).$$

A calculation using the identities $K_{-s}(t) = K_s(t)$ and $K_{\frac{1}{2}}(t) = \sqrt{\frac{\pi}{2}} e^{-t} t^{-\frac{1}{2}}$ for $t > 0$ gives

$$D'_\mu(-1) = \frac{N_{F/\mathbb{Q}}((\mu)\partial_F)^{-\frac{1}{2}}}{r_F} \sigma_1((\mu)\partial_F) \prod_{j=1}^{n} \sqrt{\frac{\pi}{2}} e^{-2\pi|\mu^{(j)}|y_j} (2\pi|\mu^{(j)}|y_j)^{-\frac{1}{2}}. \tag{2.7}$$

Note also that

$$\left\{ \prod_{j=1}^{n} \sqrt{\frac{\pi}{2}} e^{-2\pi|\mu^{(j)}|y_j} (2\pi|\mu^{(j)}|y_j)^{-\frac{1}{2}} \right\} e^{2\pi i \mathrm{Tr}(\mu x)} = 2^{-n} |N_{F/\mathbb{Q}}(\mu)|^{-\frac{1}{2}} N(y)^{-\frac{1}{2}} e^{2\pi i T(\mu, z)}, \tag{2.8}$$

where

$$T(\mu, z) := \mathrm{Tr}(\mu x) + i \sum_{j=1}^{n} |\mu^{(j)}| y_j.$$

Then using (2.7) and (2.8), we get

$$C'(-1) = \sum_{\substack{\mu \in \partial_F^{-1}/\mathcal{O}_F^\times \\ \mu \neq 0}} \frac{N_{F/\mathbb{Q}}((\mu)\partial_F)^{-\frac{1}{2}}}{r_F} \sigma_1((\mu)\partial_F) |N_{F/\mathbb{Q}}(\mu)|^{-\frac{1}{2}} e^{2\pi i T(\mu, z)}.$$

Finally, by combining the Taylor expansions for $A(s), B(s)$ and $C(s)$, we obtain the following result.

Proposition 2.3.1. *We have*

$$E\left(z, \frac{s+1}{2}\right) = 1 + \log\left(H(z)\right)(s+1) + O((s+1)^2), \tag{2.9}$$

where

$$H(z) := \sqrt{N(y)} \phi(z) \tag{2.10}$$

and

$$\log(\phi(z)) := \frac{\zeta_F^*(-1) N(y)}{r_F} + \sum_{\substack{\mu \in \partial_F^{-1}/\mathcal{O}_F^\times \\ \mu \neq 0}} \frac{N_{F/\mathbb{Q}}((\mu)\partial_F)^{-\frac{1}{2}}}{r_F} \sigma_1((\mu)\partial_F) |N_{F/\mathbb{Q}}(\mu)|^{-\frac{1}{2}} e^{2\pi i T(\mu, z)}.$$

Remark 2.3.2. Using (2.9) and the automorphy of $E(z, s)$, we have $H(Mz) = H(z)$ for all $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F)$. Then a straightforward calculation yields the transformation formula

$$\phi(Mz) = |N(\gamma z + \delta)| \, \phi(z).$$

2.4 CM zero-cycles on Hilbert modular varieties

In this section we summarize some facts we will need regarding CM zero-cycles on Hilbert modular varieties. For more details, see [BY06, Section 3]. Let F be a totally real number field of degree n over $\mathbb{Q}$ with embeddings $\tau_1, \ldots, \tau_n$, and assume that F has *narrow class number one*. The quotient $X(\mathcal{O}_F) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^n$ is the (open) Hilbert modular variety associated to $\mathcal{O}_F$. The variety $X(\mathcal{O}_F)$ parametrizes isomorphism classes of principally polarized abelian varieties (A, i) with real multiplication $i : \mathcal{O}_F \hookrightarrow \mathrm{End}(A)$.

Let E be a CM extension of F and $\Phi = (\sigma_1, \ldots, \sigma_n)$ be a CM type for E. A point $z = (A, i) \in X(\mathcal{O}_F)$ is a *CM point* of type (E, Φ) if one of the following equivalent conditions holds:

(1) As a point $z \in \mathbb{H}^n$, there is a point $\tau \in E$ such that

$$\Phi(\tau) = (\sigma_1(\tau), \ldots, \sigma_n(\tau)) = z$$

and

$$\Lambda_\tau = \mathcal{O}_F + \mathcal{O}_F\tau$$

is a fractional ideal of E.

(2) There exists a pair (A, i') that is a CM abelian variety of type (E, Φ) with complex multiplication $i' : \mathcal{O}_E \hookrightarrow \mathrm{End}(A)$ such that $i = i'|_{\mathcal{O}_F}$.

By [BY06, Lemma 3.2] and the narrow class number one assumption, there is a bijection between the ideal class group $\mathrm{CL}(E)$ and the CM points of type (E, Φ) defined as follows: given an ideal class $C \in \mathrm{CL}(E)$, there exists a fractional ideal $\mathfrak{a} \in C^{-1}$ and $\alpha, \beta \in E^\times$ such that

$$\mathfrak{a} = \mathcal{O}_F\alpha + \mathcal{O}_F\beta \tag{2.11}$$

and

$$z = \frac{\beta}{\alpha} \in E^\times \cap \mathbb{H}^n = \{z \in E^\times : \Phi(z) \in \mathbb{H}^n\}.$$

Then z represents a CM point in $X(\mathcal{O}_F)$ in the sense that $\mathbb{C}^n/\Lambda_z$ is a principally polarized abelian variety of type (E, Φ) with complex multiplication by $\mathcal{O}_E$. Conversely, every principally polarized abelian variety of type (E, Φ) with complex multiplication by $\mathcal{O}_E$ arises from a decomposition as in (2.11) for some $\mathfrak{a}$ in a unique fractional ideal class in $\mathrm{CL}(E)$. We denote the CM zero-cycle consisting of the set of CM points of type (E, Φ) by $\mathcal{CM}(E, \Phi, \mathcal{O}_F)$ and identify it with the set

$$\{z_{\mathfrak{a}} \in E^\times \cap \mathbb{H}^n : [\mathfrak{a}] \in \mathrm{CL}(E)\}$$

under the bijection just described. The reader should keep in mind that the latter set depends on Φ.

2.5 Periods of Eisenstein series

In this section we evaluate the non-holomorphic Hilbert modular Eisenstein series along a CM zero-cycle on the Hilbert modular variety $X(\mathcal{O}_F)$. Let F be a totally real number field of degree n over $\mathbb{Q}$ with narrow class number 1. Let E be a CM extension of F, and fix a CM type Φ for E. By the results of Section 3, given an ideal class $C \in \mathrm{CL}(E)$, there exists a fractional ideal $\mathfrak{a} \in C^{-1}$ such that

$$\mathfrak{a} = \mathcal{O}_F\alpha + \mathcal{O}_F\beta, \quad \alpha, \beta \in E^\times \tag{2.12}$$

where $z_{\mathfrak{a}} = \beta/\alpha \in E^\times \cap \mathbb{H}^n$ is a CM point of type (E, Φ).

By [Mas10, Proposition 4.1], we have the identity

$$\zeta_E(s, C) = \left(\frac{2^n d_F}{\sqrt{d_E}}\right)^s \frac{1}{[\mathcal{O}_E^\times : \mathcal{O}_F^\times]} \zeta_F(2s) E(z_{\mathfrak{a}}, s),$$

where we have identified $z_{\mathfrak{a}}$ with its image $\Phi(z_{\mathfrak{a}}) \in \mathbb{H}^n$. Make the shift $s \mapsto (s+1)/2$ in this identity and sum over ideal classes $C \in \mathrm{CL}(E)$ to obtain

$$\sum_{[\mathfrak{a}] \in \mathrm{CL}(E)} E\left(z_{\mathfrak{a}}, \frac{s+1}{2}\right) = [\mathcal{O}_E^\times : \mathcal{O}_F^\times] \left(\frac{\sqrt{d_E}}{2^n d_F}\right)^{\frac{s+1}{2}} \frac{\zeta_E(\frac{s+1}{2})}{\zeta_F(s+1)}.$$

By class field theory, we have the factorization

$$\zeta_E(s) = \zeta_F(s) L(\chi_{E/F}, s), \tag{2.13}$$

where $L(\chi_{E/F}, s)$ is the L–function of the quadratic character $\chi_{E/F}$ associated to the extension E/F. Using the Taylor expansion (2.9), the factorization (2.13), and the Taylor expansion

$$\frac{\zeta_F\left(\frac{s+1}{2}\right)}{\zeta_F(s+1)} = \frac{1}{2^{n-1}} \left\{1 - \frac{1}{2n} \frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)}(s+1) + O((s+1)^2)\right\},$$

we obtain

$$\sum_{[\mathfrak{a}]\in \mathrm{CL}(E)} \left\{1+\log\left(H(z_{\mathfrak{a}})\right)(s+1)+O(s+1)^2\right\} = \frac{[\mathcal{O}_E^\times : \mathcal{O}_F^\times] L(\chi_{E/F},0)}{2^n} \tag{2.14}$$

$$\times \left\{ 2+\log\left(\frac{\sqrt{d_E}}{2^n d_F}\right)(s+1) - \frac{1}{n}\frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)}(s+1) + \frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)}(s+1) + O((s+1)^2)\right\}.$$

Let $s=-1$ in (2.14) to recover the class number formula

$$L(\chi_{E/F},0) = \frac{2^{n-1}h_E}{[\mathcal{O}_E^\times : \mathcal{O}_F^\times]}.$$

Then differentiate (2.14) with respect to s and evaluate at $s=-1$ to get

$$\sum_{[\mathfrak{a}]\in \mathrm{CL}(E)} \log\left(H(z_{\mathfrak{a}})\right) = \frac{h_E}{2}\left\{\log\left(\frac{\sqrt{d_E}}{2^n d_F}\right) - \frac{1}{n}\frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)} + \frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)}\right\}. \tag{2.15}$$

2.6 Evaluation of the logarithmic derivative

In this section we evaluate the logarithmic derivative of $L(\chi_{E/F},s)$ at $s=0$ in terms of values of the gamma function Γ at rational numbers. Let $\mathbb{Q}\subseteq F\subseteq E$ be abelian number fields. By the Kronecker-Weber theorem, there is a cyclotomic field $\mathbb{Q}(\zeta_N)$ such that $F\subseteq E\subseteq \mathbb{Q}(\zeta_N)$ where $\zeta_N := e^{2\pi i/N}$ is a primitive N-th root of unity. Let $G_N := \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, which we identify with the group $(\mathbb{Z}/N\mathbb{Z})^\times$ via the isomorphism

$$s_N : G_N \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$$

$$\sigma \longmapsto [s_N(\sigma)]_N,$$

where $\sigma(\zeta_N)=\zeta_N^{s_N(\sigma)}$ for some integer $s_N(\sigma)$ modulo N. Let H_F and H_E be the subgroups of G_N which fix F and E, resp. Since G_N is abelian, H_F and H_E are normal, and by Galois theory we have $\mathrm{Gal}(F/\mathbb{Q})\cong G_N/H_F$ and $\mathrm{Gal}(E/\mathbb{Q})\cong G_N/H_E$. We also note that $H_E\le H_F\le G_N$, since the Galois correspondence is inclusion reversing.

Let G be a finite abelian group and $\widehat{G}$ be its character group. Given a subgroup $H\le G$, we have $\widehat{G/H}\cong H^\perp$ where

$$H^\perp := \{\chi\in\widehat{G} \mid \chi|_H\equiv 1\}.$$

Additionally, if $H' \leq H \leq G$ then $H^\perp \leq H'^\perp$.

Given an abelian field $K \subseteq \mathbb{Q}(\zeta_N)$, the group of characters associated to K is defined by

$$X_K := H_K^\perp = \{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} \mid \chi|_{H_K} \equiv 1\}.$$

By our preceding observations, we have $\widehat{G_N/H_E} \cong X_E$ and $\widehat{G_N/H_F} \cong X_F$, and since $H_E \leq H_F \leq G_N$, we have $X_F \leq X_E$.

We now evaluate the logarithmic derivative of $L(\chi_{E/F}, s)$ at $s = 0$. The Dedekind zeta function $\zeta_K(s)$ of an abelian field $K \subset \mathbb{Q}(\zeta_N)$ factors as

$$\zeta_K(s) = \prod_{\chi \in X_K} L(\chi, s),$$

where $L(\chi, s)$ is understood to be the Dirichlet L–function associated to the primitive Dirichlet character of conductor c_χ which induces $\chi \in X_K$ (see [Coh07, Theorem 10.5.25]). Therefore by (2.13), we have

$$\frac{L'(\chi_{E/F}, s)}{L(\chi_{E/F}, s)} = \frac{d}{ds}\left(\log \frac{\zeta_E(s)}{\zeta_F(s)}\right) = \sum_{\chi \in X_E \setminus X_F} \frac{L'(\chi, s)}{L(\chi, s)}, \tag{2.16}$$

where

$$X_E \setminus X_F = \{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} \mid \chi|_{H_E} \equiv 1 \quad \text{and} \quad \chi|_{H_F \setminus H_E} \not\equiv 1\}$$

is the set of characters in $\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ that are trivial on H_E but not trivial on H_F.

Now, we have

$$L(\chi, s) = c_\chi^{-s} \sum_{k=1}^{c_\chi} \chi(k) \zeta\left(s, \frac{k}{c_\chi}\right), \tag{2.17}$$

where

$$\zeta(s, w) := \sum_{n=0}^{\infty} \frac{1}{(n+w)^s}, \quad \text{Re}(w) > 0, \quad \text{Re}(s) > 1$$

is the Hurwitz zeta function. Differentiating (2.17) yields

$$L'(\chi, s) = -\log(c_\chi) L(\chi, s) + c_\chi^{-s} \sum_{k=1}^{c_\chi} \chi(k) \zeta'\left(s, \frac{k}{c_\chi}\right).$$

The Taylor expansion of the Hurwitz zeta function at $s = 0$ is given by

$$\zeta(s,x) = \zeta(0,x) + \zeta'(0,x)s + O(s^2), \quad x > 0$$

where $\zeta(0,x) = \frac{1}{2} - x$ and Lerch's identity [Ler87] gives

$$\zeta'(0,x) = \log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right). \tag{2.18}$$

Using (2.18), we find that

$$L'(\chi,0) = -\log(c_\chi)L(\chi,0) + \sum_{k=1}^{c_\chi} \chi(k)\log\left(\frac{\Gamma\left(\frac{k}{c_\chi}\right)}{\sqrt{2\pi}}\right).$$

Recall that if χ is even, then $L(\chi,0) = 0$, while if χ is odd, then $L(\chi,0) \neq 0$. If we assume that E is a CM extension of F, then all of the characters $\chi \in X_E \setminus X_F$ are odd (see Lemma 2.6.2). Hence using the orthogonality relations for group characters, we get

$$\frac{L'(\chi,0)}{L(\chi,0)} = -\log(c_\chi) + \frac{1}{L(\chi,0)}\sum_{k=1}^{c_\chi} \chi(k)\log\Gamma\left(\frac{k}{c_\chi}\right). \tag{2.19}$$

Finally, substituting (2.19) into (2.16) yields

$$\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} = -\sum_{\chi\in X_E\setminus X_F} \log(c_\chi) + \sum_{\chi\in X_E\setminus X_F}\sum_{k=1}^{c_\chi} \frac{\chi(k)}{L(\chi,0)}\log\Gamma\left(\frac{k}{c_\chi}\right). \tag{2.20}$$

Remark 2.6.1. Since the primitive Dirichlet character χ of conductor c_χ which induces a Dirichlet character $\chi \in X_K$ is also a Dirichlet character modulo N, we have the following analog of (2.17),

$$L(\chi,s) = N^{-s}\sum_{k=1}^{N} \chi(k)\zeta\left(s, \frac{k}{N}\right). \tag{2.21}$$

Then by repeating the preceding calculation with (2.21) instead of (2.17), we get

$$\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} = -\log(N)[F:\mathbb{Q}] + \sum_{\chi\in X_E\setminus X_F}\sum_{k=1}^{N} \frac{\chi(k)}{L(\chi,0)}\log\Gamma\left(\frac{k}{N}\right), \tag{2.22}$$

where we used $\#(X_E \setminus X_F) = [F:\mathbb{Q}]$.

It remains to prove the following

Lemma 2.6.2. *If E/F is a CM extension, then all of the characters $\chi \in X_E \setminus X_F$ are odd.*

Proof. Let E/F be a CM extension. Then the nontrivial automorphism $\sigma_c \in \mathrm{Gal}(E/F)$ is complex conjugation, which when viewed as an element of $G_N \cong (\mathbb{Z}/N\mathbb{Z})^\times$ corresponds to the residue class $[-1]_N \in (\mathbb{Z}/N\mathbb{Z})^\times$. Clearly, $[-1]_N \in H_F$ but $[-1]_N \notin H_E$, and by Galois theory we have $H_F = \langle H_E \cup \{[-1]_N\}\rangle$. Let $\chi \in X_E \setminus X_F$. Then χ is trivial on H_E but nontrivial on H_F, so we must have $\chi([-1]_N) = -1$, which implies that χ is odd.

□

2.7 Taylor coefficients of Dedekind zeta functions

In this section we evaluate the logarithmic derivative of $\zeta_F^{(n-1)}(s)$ at $s = 0$ and prove Theorem 2.1.1. The evaluation we obtain is analogous to (2.20), the difference being that $\log(\Gamma(x))$ is replaced by Deninger's R-function $R(x)$. Let F be a totally real field of degree n over $\mathbb{Q}$. Write the Laurent expansion of $\zeta_F(s)$ at $s = 1$ as

$$\zeta_F(s) = \frac{A_{-1}}{s-1} + A_0 + O(s-1).$$

Lemma 2.7.1. *We have the Taylor expansion*

$$\zeta_F(s) = -\frac{\sqrt{d_F}A_{-1}}{2^n}s^{n-1} + \frac{\sqrt{d_F}}{2^n}(A_0 + A_{-1}\log(d_F) - nA_{-1}\{\gamma + \log(2\pi)\})s^n + O(s^{n+1}),$$

where γ is Euler's constant.

Proof. From the functional equation $\zeta_F^*(s) = \zeta_F^*(1-s)$, we have

$$\zeta_F(s) = d_F^{\frac{1}{2}-s}\left(\frac{\Gamma_\mathbb{R}(1-s)}{\Gamma_\mathbb{R}(s)}\right)^n \zeta_F(1-s),$$

where $\Gamma_\mathbb{R}(s) := \pi^{-s/2}\Gamma(s/2)$. Then the lemma follows by multiplying the Taylor expansions

$$d_F^{\frac{1}{2}-s} = \sqrt{d_F} - \sqrt{d_F}\log(d_F)s + O(s^2),$$

$$\left(\frac{\Gamma_\mathbb{R}(1-s)}{\Gamma_\mathbb{R}(s)}\right)^n = \left(\frac{s}{2} + \frac{1}{2}\left(\gamma + \log(2\pi)\right)s^2 + O(s^3)\right)^n$$
$$= \frac{s^n}{2^n} + \frac{n}{2^n}(\gamma + \log(2\pi))s^{n+1} + O(s^{n+2}),$$

and

$$\zeta_F(1-s) = -\frac{A_{-1}}{s} + A_0 + O(s).$$

□

From Lemma 2.7.1, we have

$$\frac{\zeta_F^{(n-1)}(0)}{(n-1)!} = -\frac{\sqrt{d_F}A_{-1}}{2^n}$$

and

$$\frac{\zeta_F^{(n)}(0)}{n!} = \frac{\sqrt{d_F}}{2^n}\left(A_0 + A_{-1}\log(d_F) - nA_{-1}\{\gamma + \log(2\pi)\}\right),$$

which gives

$$\frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)} = -n\left(\frac{A_0}{A_{-1}} + \log(d_F) - n\gamma - n\log(2\pi)\right). \tag{2.23}$$

Assume now that F is abelian. Then we have the factorization

$$\zeta_F(s) = \zeta(s)\prod_{\substack{\chi\in X_F\\ \chi\neq 1}} L(\chi, s).$$

Substituting the Laurent expansions

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(s-1)$$

and

$$L(\chi, s) = L(\chi, 1) + L'(\chi, 1)(s-1) + O((s-1)^2)$$

into this factorization yields

$$\zeta_F(s) = \left(\frac{1}{s-1} + \gamma + O(s-1)\right)\prod_{\substack{\chi\in X_F\\ \chi\neq 1}}\left(L(\chi, 1) + L'(\chi, 1)(s-1) + O((s-1)^2)\right).$$

Then expanding the right hand side and comparing coefficients yields

$$A_{-1} = \prod_{\substack{\chi\in X_F\\ \chi\neq 1}} L(\chi, 1)$$

and

$$A_0 = \gamma \prod_{\substack{\chi \in X_F \\ \chi \neq 1}} L(\chi, 1) + \left(\prod_{\substack{\chi \in X_F \\ \chi \neq 1}} L(\chi, 1) \right) \sum_{\substack{\chi \in X_F \\ \chi \neq 1}} \frac{L'(\chi, 1)}{L(\chi, 1)} = \gamma A_{-1} + A_{-1} \sum_{\substack{\chi \in X_F \\ \chi \neq 1}} \frac{L'(\chi, 1)}{L(\chi, 1)}.$$

It follows that

$$\frac{A_0}{A_{-1}} = \gamma + \sum_{\substack{\chi \in X_F \\ \chi \neq 1}} \frac{L'(\chi, 1)}{L(\chi, 1)}. \tag{2.24}$$

Each of the characters $\chi \in X_F$ is even, since $[-1]_N \in H_F$ and

$$X_F = \{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} \mid \chi|_{H_F} \equiv 1\}.$$

Therefore, we must evaluate $L'(\chi, 1)$ for χ an even, primitive Dirichlet character. This problem was solved by Deninger [Den84] in the following way. Let χ be an even, primitive Dirichlet character of conductor c_χ. Then the functional equation for the Dirichlet L–function is

$$L(\chi, 1-s) = \frac{2c_\chi^{s-1}\Gamma(s)}{(2\pi)^s} \cos\left(\frac{\pi s}{2}\right) \tau(\chi) L(\overline{\chi}, s),$$

where

$$\tau(\chi) := \sum_{k=1}^{c_\chi} \chi(k) \zeta_{c_\chi}^k, \quad \zeta_{c_\chi} := e^{2\pi i / c_\chi}$$

is the Gauss sum of χ. A calculation with the functional equation yields

$$L'(\chi, 1) = \frac{2\tau(\chi)}{c_\chi} \left(\left(\gamma - \log\left(\frac{c_\chi}{2\pi}\right) \right) L'(\overline{\chi}, 0) - \frac{1}{2} L''(\overline{\chi}, 0) \right).$$

Because

$$L(\chi, s) = c_\chi^{-s} \sum_{k=1}^{c_\chi} \chi(k) \zeta\left(s, \frac{k}{c_\chi}\right),$$

to evaluate $L'(\overline{\chi}, 0)$ and $L''(\overline{\chi}, 0)$, it suffices to evaluate the coefficients in the Taylor expansion

$$\zeta(s, x) = \zeta(0, x) + \zeta'(0, x)s + \zeta''(0, x)s^2 + O(s^3), \quad x > 0.$$

Recall the logarithmic form of the Bohr-Mollerup theorem.

Theorem 2.7.2 (Bohr-Mollerup). *Let $f : \mathbb{R}^+ \to \mathbb{R}$ be a function such that*

$$f(x+1) - f(x) = \log(x),$$

$f(1) = 0$*, and* $f(x)$ *is convex on* $\mathbb{R}^+$*. Then* $f(x) = \log(\Gamma(x))$*.*

Deninger [Den84, Theorem 2.2] proved the following result.

Theorem 2.7.3 (Deninger). *The function*

$$f_\alpha(x) := (-1)^{\alpha+1}\left(\partial_s^\alpha \zeta(0,x) - \zeta^{(\alpha)}(0)\right), \quad x > 0, \quad \alpha = 0, 1, 2, \ldots$$

is the unique function such that

(1) $f_\alpha(x+1) - f_\alpha(x) = \log^\alpha(x)$

(2) $f_\alpha(1) = 0$

(3) $f_\alpha(x)$ *is convex on* $(\exp(\alpha - 1), \infty)$.

Let $\alpha = 1$ in Theorem 2.7.3. Then $f_1(x)$ is convex on $(1, \infty)$ (hence convex on $\mathbb{R}^+$ by virtue of (1)), so by the Bohr-Mollerup theorem, $f_1(x) = \log(\Gamma(x))$, or equivalently

$$\zeta'(0,x) = \log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right),$$

where we used $\zeta'(0) = -\frac{1}{2}\log(2\pi)$. This gives a conceptual proof of Lerch's identity (2.18) (a beautiful account of this approach to Lerch's identity is given by Weil [Wei76, Chapter VII]). Moreover, using the limit

$$\Gamma(x) = \lim_{n\to\infty} \frac{n!n^x}{x(x+1)\cdots(x+n)}, \quad x > 0$$

one has

$$\log\left(\frac{\Gamma(x)}{\sqrt{2\pi}}\right) = \lim_{n\to\infty}\left(\zeta'(0) + x\log(n) - \log(x) - \sum_{k=1}^{n-1}(\log(x+k) - \log(k))\right).$$

Next, let $\alpha = 2$ in Theorem 2.7.3 and define $R(x) := -\zeta''(0,x)$. Then $R(x)$ is the unique function such that

$(1')$ $R(x+1) - R(x) = \log^2(x), \quad x > 0$

(2′) $R(1) = -\zeta''(0)$

(3′) $R(x)$ is convex on (e, ∞).

Moreover, by [Den84, Lemma 2.1, eqn. (2.1.2)] one has

$$R(x) = \lim_{n\to\infty} \left(-\zeta''(0) + x\log^2(n) - \log^2(x) - \sum_{k=1}^{n-1} \left(\log^2(x+k) - \log^2(k)\right) \right). \tag{2.25}$$

These facts show that $R(x)$ is analogous to $\log(\Gamma(x)/\sqrt{2\pi})$ (see [Den84, Section 2] for more details concerning this analogy).

Remark 2.7.4. Alternatively, one could *define* $R(x)$ by the limit (2.25), then verify directly that $R(x)$ satisfies conditions (1′)–(3′). Then by uniqueness, one has the identity $R(x) = -\zeta''(0, x)$. This is analogous to the conceptual proof of Lerch's identity just described.

Using the preceding facts, Deninger [Den84, Section 3] established the formula

$$L'(\chi, 1) = (\gamma + \log(2\pi))L(\chi, 1) + \frac{\tau(\chi)}{c_\chi} \sum_{k=1}^{c_\chi} \overline{\chi}(k) R\left(\frac{k}{c_\chi}\right). \tag{2.26}$$

Substituting (2.26) into (2.24) yields

$$\frac{A_0}{A_{-1}} = \gamma + \sum_{\substack{\chi \in X_F \\ \chi \neq 1}} \left\{ (\gamma + \log(2\pi)) + \frac{\tau(\chi)}{c_\chi} \sum_{k=1}^{c_\chi} \frac{\overline{\chi}(k)}{L(\chi, 1)} R\left(\frac{k}{c_\chi}\right) \right\}. \tag{2.27}$$

Since $X_F \cong \widehat{G_N/H_F} \cong G_N/H_F \cong \mathrm{Gal}(F/\mathbb{Q})$, we have $\#X_F = [F : \mathbb{Q}] = n$. Then substituting (2.27) into (2.23) and simplifying yields the formula

$$\frac{\zeta_F^{(n)}(0)}{\zeta_F^{(n-1)}(0)} = -n \left(-\log(2\pi) + \log(d_F) + \sum_{\substack{\chi \in X_F \\ \chi \neq 1}} \frac{\tau(\chi)}{c_\chi} \sum_{k=1}^{c_\chi} \frac{\overline{\chi}(k)}{L(\chi, 1)} R\left(\frac{k}{c_\chi}\right) \right). \tag{2.28}$$

Proof of Theorem 2.1.1. By combining equations (2.15), (2.20) and (2.28), we obtain Theorem 2.1.1 after a short calculation with the conductor-discriminant formula

$$d_L = \prod_{\chi \in X_L} c_\chi, \tag{2.29}$$

where d_L denotes the absolute value of the discriminant of a number field L. □

2.8 The group of characters of a multiquadratic extension

In this section we determine the group of characters associated to a multiquadratic extension. Let $d_1, \ldots, d_t$ be squarefree, pairwise relatively prime integers and define the multiquadratic extension $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$. The absolute value of the discriminant of the quadratic subfield $\mathbb{Q}(\sqrt{d_i})$ is given by

$$D_i = \begin{cases} |d_i| & \text{if } \ d_i \equiv 1 \pmod 4 \\ 4|d_i| & \text{if } \ d_i \equiv 2, 3 \pmod 4. \end{cases}$$

One has $\mathbb{Q}(\sqrt{d_i}) \subseteq \mathbb{Q}(\zeta_{D_i})$, so by taking compositums we obtain

$$K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t}) \subseteq \mathbb{Q}(\zeta_{D_1}, \ldots, \zeta_{D_t}) \subseteq \mathbb{Q}(\zeta_{D_1 \cdots D_t}) = \mathbb{Q}(\zeta_D)$$

where $D := D_1 \cdots D_t$.

Recall that the group of characters associated to K is given by

$$X_K = \{\chi \in \widehat{(\mathbb{Z}/D\mathbb{Z})}^\times \mid \chi|_{H_K} \equiv 1\},$$

where H_K is the subgroup of $G_D := \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ which fixes K. Let $m = d_1^{e_1} \cdots d_t^{e_t}$ for $(0, \ldots, 0) \neq (e_1, \ldots, e_t) \in \{0, 1\}^t$, and define the quadratic subfield

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{d_1^{e_1} \cdots d_t^{e_t}}) \subset K.$$

Let χ_1 be the trivial character of $(\mathbb{Z}/D\mathbb{Z})^\times$, and χ'_m be the Dirichlet character of $(\mathbb{Z}/D\mathbb{Z})^\times$ induced by the Kronecker symbol χ_m associated to the quadratic field $\mathbb{Q}(\sqrt{m})$.

Proposition 2.8.1. *The group of characters associated to K is given by*

$$X_K = \{\chi_1\} \cup \left\{\chi'_m : \ m = d_1^{e_1} \cdots d_t^{e_t} \quad \text{for} \quad (0, \ldots, 0) \neq (e_1, \ldots, e_t) \in \{0, 1\}^t\right\}.$$

Proof. For notational convenience, let $G_m := \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$, and let $H_m := H_{\mathbb{Q}(\sqrt{m})}$ be the subgroup of G_D which fixes $\mathbb{Q}(\sqrt{m})$. Define the integers

$$M = M_m := \begin{cases} |m| & \text{if } m \equiv 1 \pmod 4 \\ 4|m| & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

Clearly, the primitive Dirichlet characters $\chi_m : (\mathbb{Z}/M\mathbb{Z})^\times \to \{\pm 1\}$ induce $2^\ell - 1$ Dirichlet characters $\chi'_m : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ by composing with the projections $\pi : (\mathbb{Z}/D\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$. Thus to show $\chi'_m \in X_K$, it suffices to show $\chi'_m|_{H_K} \equiv 1$. In fact, because $H_K \le H_m$, it suffices to show $\chi'_m|_{H_m} \equiv 1$. We have the diagram

$$\begin{array}{ccc}
H_K \le H_m \le G_D & \xrightarrow{s_D} & (\mathbb{Z}/D\mathbb{Z})^\times \\
\downarrow \textbf{res} & & \downarrow \pi \\
G_M & \xrightarrow{s_M} & (\mathbb{Z}/M\mathbb{Z})^\times \\
\downarrow \textbf{res} & & \downarrow \chi_m \\
G_m & \xrightarrow{\simeq} & \{\pm 1\}
\end{array} \quad \text{(with } \chi'_m : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}\text{)}$$

where **res** is the restriction map, and s_D and s_M are the canonical isomorphisms. We will prove that

$$\chi'_m([s_D(\sigma)]_D) = \frac{\sigma(\sqrt{m})}{\sqrt{m}} \quad \text{for all} \quad \sigma \in G_D. \tag{2.30}$$

Then (2.30) implies that $\chi'_m|_{H_m} \equiv 1$, since

$$\frac{\sigma(\sqrt{m})}{\sqrt{m}} = 1 \quad \text{for all} \quad \sigma \in H_m.$$

That is, an automorphism $\sigma \in H_m$ restricts to the identity in G_m. Because the following diagram commutes (see [KKS11, Proposition 5.14])

$$\begin{array}{ccc}
G_M & \xrightarrow{s_M} & (\mathbb{Z}/M\mathbb{Z})^\times \\
\downarrow \textbf{res} & & \downarrow \chi_m \\
G_m & \xrightarrow{\simeq} & \{\pm 1\}
\end{array}$$

we have

$$\chi_m([s_M(\sigma)]_M) = \frac{\sigma(\sqrt{m})}{\sqrt{m}} \quad \text{for} \quad \sigma \in G_M.$$

Thus to prove (2.30), it suffices to show that

$$\chi'_m([s_D(\sigma)]_D) = \chi_m([s_M(\textbf{res}(\sigma))]_M) \quad \text{for} \quad \sigma \in G_D.$$

Let $\sigma \in G_D$. Then since $\chi'_m = \chi_m \circ \pi$, we have $\chi'_m([s_D(\sigma)]_D) = \chi_m(\pi([s_D(\sigma)]_D)) = \chi_m([s_D(\sigma)]_M)$. Thus it suffices to show $[s_D(\sigma)]_M = [s_M(\textbf{res}(\sigma))]_M$, or equivalently, $s_D(\sigma) \equiv$

$s_M(\mathbf{res}(\sigma)) \pmod M$. Since $M|D$, there is an integer k such that $\zeta_M = \zeta_D^k$. Thus $\sigma(\zeta_M) = \sigma(\zeta_D^k) = \sigma(\zeta_D)^k = \zeta_D^{ks_D(\sigma)} = \zeta_M^{s_D(\sigma)}$. On the other hand, $\sigma(\zeta_M) = \mathbf{res}(\sigma)(\zeta_M) = \zeta_M^{s_M(\mathbf{res}(\sigma))}$, thus $s_D(\sigma) \equiv s_M(\mathbf{res}(\sigma)) \pmod M$. □

2.9 Proof of Theorem 2.1.4

In this section we will prove Theorem 2.1.4. We first recall the setup in the theorem. Let $d_1, \dots, d_{\ell+1}$ be squarefree, pairwise relatively prime integers with $d_i > 0$ for $i = 1, \dots, \ell$ and $d_{\ell+1} < 0$, where $\ell = 1$ or 2. Assume that $F = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_\ell})$ has narrow class number 1, and let $E = F(\sqrt{d_{\ell+1}})$. Let χ_α (resp. χ_β) be the Kronecker symbol associated to the quadratic field $\mathbb{Q}(\sqrt{\alpha})$ (resp. $\mathbb{Q}(\sqrt{\beta})$), where $\alpha = d_1^{e_1} \cdots d_\ell^{e_\ell} d_{\ell+1}$ (resp. $\beta = d_1^{e_1} \cdots d_\ell^{e_\ell}$) for $(e_1, \dots, e_\ell) \in \{0,1\}^\ell$. Now, the field F is totally real of degree $n = 2^\ell$ over $\mathbb{Q}$, and E is a CM extension of F. We have $F \subset E \subset \mathbb{Q}(\zeta_D)$ where $D = D_1 \cdots D_{\ell+1}$ (see Section 2.8 for the notation). Then by Proposition 2.8.1,

$$X_F = \{\chi_1\} \cup \left\{\chi'_\beta \in \widehat{(\mathbb{Z}/D\mathbb{Z})^\times} :\ \beta = d_1^{e_1} \cdots d_\ell^{e_\ell},\ (0, \dots, 0) \neq (e_1, \dots, e_\ell) \in \{0,1\}^\ell\right\} \quad \text{and}$$

$$X_E = \{\chi_1\} \cup \left\{\chi'_\alpha \in \widehat{(\mathbb{Z}/D\mathbb{Z})^\times} :\ \alpha = d_1^{e_1} \cdots d_{\ell+1}^{e_{\ell+1}},\ (0, \dots, 0) \neq (e_1, \dots, e_{\ell+1}) \in \{0,1\}^{\ell+1}\right\}.$$

It follows that

$$X_E \setminus X_F = \left\{\chi'_\alpha \in \widehat{(\mathbb{Z}/D\mathbb{Z})^\times} \mid \alpha = d_1^{e_1} \cdots d_\ell^{e_\ell} d_{\ell+1}, \quad (e_1, \dots, e_\ell) \in \{0,1\}^\ell\right\}.$$

Using the class number formulas

$$L(\chi_\alpha, 0) = \frac{2h_\alpha}{w_\alpha} \quad \text{and} \quad L(\chi_\beta, 1) = \frac{2h_\beta \log \varepsilon_\beta}{\sqrt{c_\beta}},$$

along with the evaluation $\tau(\chi_\beta) = \sqrt{c_\beta}$, we deduce Theorem 2.1.4 from Theorem 2.1.1. □

2.10 Proof of Theorem 2.1.6

In this section we prove Theorem 2.1.6, which amounts to using the assumptions in Theorem 2.1.6 to give an explicit version of the formula appearing in Theorem 2.1.4 for a particular choice of CM point $z_{\mathcal{O}_E}$. We first recall the setup in the theorem. Let $p = 2$ or $p \equiv 1 \mod 4$ be a prime such that $F = \mathbb{Q}(\sqrt{p})$ has narrow class number 1. Let $d < 0$ be a squarefree integer relatively prime to p such that $E = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ has class number 1. Let Δ_p, Δ_d and Δ_{pd} be the discriminants of $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{pd})$, resp., and assume that Δ_p and Δ_d are relatively prime. The four embeddings of E are given by

$$\begin{aligned}
\mathrm{id}: &\quad \sqrt{p} \longmapsto \sqrt{p}, \quad \sqrt{d} \longmapsto \sqrt{d} \\
\sigma: &\quad \sqrt{p} \longmapsto -\sqrt{p}, \quad \sqrt{d} \longmapsto \sqrt{d} \\
\tau: &\quad \sqrt{p} \longmapsto \sqrt{p}, \quad \sqrt{d} \longmapsto -\sqrt{d} \\
\sigma\tau: &\quad \sqrt{p} \longmapsto -\sqrt{p}, \quad \sqrt{d} \longmapsto -\sqrt{d}.
\end{aligned}$$

These embeddings occur in the complex conjugate pairs $\{\mathrm{id}, \tau\}$ and $\{\sigma, \sigma\tau\}$. Fix the choice of CM type $\Phi = \{\mathrm{id}, \sigma\}$. We now determine a CM point of type (E, Φ) associated to the ideal class $[\mathcal{O}_E]$. Define θ_p and θ_d by

$$\theta_p := \begin{cases} \dfrac{1+\sqrt{p}}{2} & \text{if } p \equiv 1 \pmod 4 \\ \sqrt{2} & \text{if } p = 2 \end{cases} \quad \text{and} \quad \theta_d := \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4). \end{cases}$$

The integer rings $\mathcal{O}_F = \mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ have integral bases $\{1, \theta_p\}$ and $\{1, \theta_d\}$, resp. Since Δ_p and Δ_d are relatively prime, and $E = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ is the compositum of $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{d})$, it follows that $\mathcal{O}_E$ has the integral basis $\{1, \theta_p, \theta_d, \theta_p\theta_d\}$ and $d_E = \Delta_p^2\Delta_d^2$ (see [Lan94, Chapter 3, Theorem 17]). Recall from Section 2.4 that to determine a CM point $z_{\mathcal{O}_E}$ of type (E, Φ) associated to the ideal class $[\mathcal{O}_E]$, we need a decomposition $\mathcal{O}_E = \mathcal{O}_F\alpha + \mathcal{O}_F\beta$ for some $\alpha, \beta \in \mathcal{O}_E$ with $\beta/\alpha \in E^\times \cap \mathbb{H}^2 = \{z \in E^\times : \Phi(z) \in \mathbb{H}^2\}$. We have

$$\mathcal{O}_E = \mathbb{Z} + \theta_p\mathbb{Z} + \theta_d\mathbb{Z} + \theta_p\theta_d\mathbb{Z} = (\mathbb{Z} + \theta_p\mathbb{Z}) + (\mathbb{Z} + \theta_p\mathbb{Z})\theta_d = \mathcal{O}_F + \mathcal{O}_F\theta_d.$$

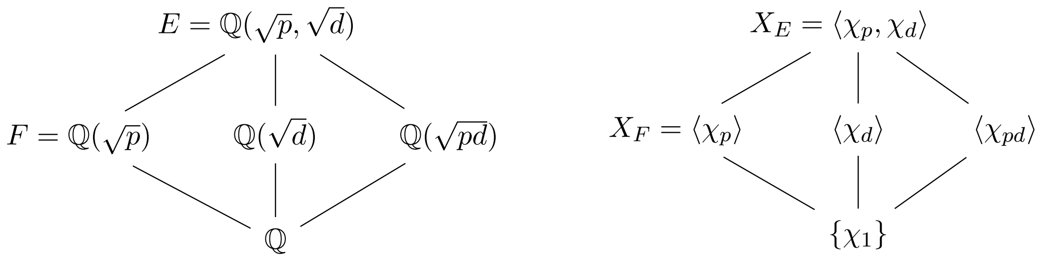
Letting $\alpha = 1$ and $\beta = \theta_d$, we get a CM point $z_{\mathcal{O}_E} = \beta/\alpha = \theta_d$, since $\Phi(\theta_d) = (\mathrm{id}(\theta_d), \sigma(\theta_d)) = (\theta_d, \theta_d) \in \mathbb{H}^2$. Then with our convention of identifying a CM point with its image under the CM type Φ, we have

$$z_{\mathcal{O}_E} = \Phi(\theta_d) = \begin{cases} (\sqrt{d}, \sqrt{d}), & d \equiv 2, 3 \pmod 4) \\ \left(\frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\right), & d \equiv 1 \pmod 4). \end{cases}$$

To determine the constant $c_1(E, F, 2)$, recall that $d_E = \Delta_p^2 \Delta_d^2$, $d_F = \Delta_p$ and $h_E = 1$, thus

$$c_1(E, F, 2) = \left(\frac{\Delta_p}{8\pi\sqrt{\Delta_p^2 \Delta_d^2}} \right)^{\frac{1}{2}} = \frac{1}{2\sqrt{2\pi|\Delta_d|}}.$$

The groups of characters associated to the fields F and E are $X_F = \{\chi_1, \chi_p\}$ and $X_E = \{\chi_1, \chi_p, \chi_d, \chi_{pd}\}$, resp., so that $X_E \setminus X_F = \{\chi_d, \chi_{pd}\}$. The character $\chi_p = \left(\frac{\Delta_p}{\cdot}\right)$ has conductor Δ_p, the character $\chi_d = \left(\frac{\Delta_d}{\cdot}\right)$ has conductor $|\Delta_d|$, and the character $\chi_{pd} = \left(\frac{\Delta_{pd}}{\cdot}\right)$ has conductor $|\Delta_{pd}|$. The characters χ_p and χ_d generate X_E. The following diagrams show the correspondence between subfields and associated groups of characters:



Since $F = \mathbb{Q}(\sqrt{p})$ has narrow class number 1, we have $h_p = 1$. Then recalling that ε_p denotes the fundamental unit in F, the result follows by substituting the quantities determined in this section into the identity in Theorem 2.1.4. □

3. THE COLMEZ CONJECTURE FOR NON-ABELIAN CM FIELDS*

3.1 Introduction

3.1.1 The Chowla-Selberg formula and the Colmez conjecture

One of the central objects of study in number theory is the *Dedekind eta function*, which is the weight $1/2$ modular form for $SL_2(\mathbb{Z})$ defined by the infinite product

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad q := e^{2\pi i z}.$$

As was already discussed in the introduction in Chapter 1, a remarkable formula of Chowla and Selberg [CS67] relates values of $\eta(z)$ at CM points to values of the Euler Gamma function $\Gamma(s)$ at rational numbers. Here we briefly recall this formula again in order to set the discussion in the proper context. Let E be an imaginary quadratic field of discriminant $-D < 0$. Let $h(-D)$ be the class number, $w(-D)$ be the number of units, and χ_{-D} be the Kronecker symbol. Using Kronecker's first limit formula, one can prove the identity

$$\sum_{C} \log\left(\sqrt{\operatorname{Im}(\tau_C)}|\eta(\tau_C)|^2\right) = \frac{h(-D)}{2}\left(\log\left(\frac{\sqrt{D}}{2}\right) - \frac{1}{2}\log(2\pi) + \frac{L'(\chi_{-D},0)}{L(\chi_{-D},0)}\right), \tag{3.1}$$

where the sum is over a complete set of CM points τ_C of discriminant $-D$ on $SL_2(\mathbb{Z})\backslash\mathbb{H}$. There are $h(-D)$ such points, corresponding to the ideal classes C of E. On the other hand, a classical identity of Lerch [Ler87] evaluates the logarithmic derivative of the Dirichlet L–function $L(\chi_{-D}, s)$ at $s = 0$ in terms of values of $\Gamma(s)$ at rational numbers,

$$\frac{L'(\chi_{-D},0)}{L(\chi_{-D},0)} = -\log(D) + \frac{w(-D)}{2h(-D)} \sum_{k=1}^{D} \chi_{-D}(k) \log\left(\Gamma\left(\frac{k}{D}\right)\right). \tag{3.2}$$

Substituting Lerch's identity (3.2) into (3.1) then yields the *Chowla-Selberg formula*

$$\prod_{C} \sqrt{\operatorname{Im}(\tau_C)}|\eta(\tau_C)|^2 = \left(\frac{1}{4\pi\sqrt{D}}\right)^{\frac{h(-D)}{2}} \prod_{k=1}^{D} \Gamma\left(\frac{k}{D}\right)^{\frac{w(-D)\chi_{-D}(k)}{4}}. \tag{3.3}$$

There is a beautiful geometric reformulation of the Chowla-Selberg formula (3.3) as an identity

*Sections of this chapter are reprinted with permission from Adrian Barquero-Sanchez and Riad Masri (2016), *On the Colmez conjecture for non-abelian CM fields*. `arXiv:1604.01057 [math.NT]`.

which relates the Faltings height of a CM elliptic curve to the logarithmic derivative of $L(\chi_{-D}, s)$ at $s = 0$. In order to describe this, we first recall the definition of the (stable) Faltings height of a CM abelian variety. Let F be a totally real number field of degree n. Let E/F be a CM extension of F and Φ be a CM type for E. Let X_Φ be an abelian variety defined over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_E$ and CM type Φ. We call X_Φ a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Let $K \subseteq \overline{\mathbb{Q}}$ be a number field over which X_Φ has everywhere good reduction, and choose a Néron differential $\omega \in H^0(X_\Phi, \Omega^n_{X_\Phi})$. Then the *Faltings height* of X_Φ is defined by

$$h_{\text{Fal}}(X_\Phi) := -\frac{1}{2[K:\mathbb{Q}]} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log \left| \int_{X_\Phi^\sigma(\mathbb{C})} \omega \wedge \overline{\omega^\sigma} \right|.$$

The Faltings height does not depend on the choice of K or ω.

Now, if $E = \mathbb{Q}(\sqrt{-D})$ is an imaginary quadratic field and X_Φ is a CM elliptic curve of type $(\mathcal{O}_E, \Phi)$, then one can prove that (see e.g. [Gro80, Sil86])

$$h_{\text{Fal}}(X_\Phi) = -\log\left(2\sqrt[4]{2\pi^3}\right) - \frac{1}{h(-D)} \sum_C \log\left(\sqrt{\text{Im}(\tau_C)}|\eta(\tau_C)|^2\right).$$

Combining this identity with (3.1) allows one to express the Chowla-Selberg formula in the equivalent form

$$h_{\text{Fal}}(X_\Phi) = -\frac{1}{2}\frac{L'(\chi_{-D}, 0)}{L(\chi_{-D}, 0)} - \frac{1}{4}\log(D) - \frac{1}{2}\log(2\pi). \tag{3.4}$$

Colmez [Col93] gave a vast conjectural generalization of the identity (3.4) which relates the Faltings height of *any* CM abelian variety X_Φ of type $(\mathcal{O}_E, \Phi)$ to logarithmic derivatives at $s = 0$ of certain Artin L–functions constructed from the CM pair (E, Φ). See Section 3.3 for the precise statement of the Colmez conjecture.

3.1.2 Previous work on the Colmez conjecture

There have been many remarkable works on the Colmez conjecture.

Colmez [Col93] proved his conjecture when $E/\mathbb{Q}$ is abelian, up to addition of a rational multiple of $\log(2)$ which was recently shown to equal zero by Obus [Obu13].

Yang [Yan10a, Yan10b, Yan13] proved the Colmez conjecture for a large class of non-biquadratic CM fields of degree $[E:\mathbb{Q}] = 4$, thus establishing the only known cases of the Colmez conjecture when $E/\mathbb{Q}$ is *non-abelian*.

In his paper, Colmez [Col93] also stated an *averaged* version of his conjecture, where the Faltings heights are averaged over the different CM types for the given CM field E. See Section 3.4 for the statement of the average Colmez conjecture. Very recently, Andreatta-Goren-Howard-Madapusi Pera [AGHM15] and Yuan-Zhang [YZ15] independently proved the average Colmez conjecture. Interest in the average Colmez conjecture is motivated in part by work of Tsimerman [Tsi15], who used it to prove the André-Oort conjecture for the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g. The average Colmez conjecture will also play a crucial role in the proofs of the results in this chapter (see e.g. Section 3.1.6).

3.1.3 Statement of the main results

As discussed, the only known cases of the Colmez conjecture for non-abelian CM fields are due to Yang for a large class of CM fields of degree 4. In our first main result, we will prove that if F is any fixed totally real number field of degree $n \geq 3$, then there are infinitely many CM extensions E/F such that $E/\mathbb{Q}$ is *non-abelian* and the Colmez conjecture is true for E.

More precisely, let p be a prime number which splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. We will prove that if we fix an "arbitrary" finite set $\mathcal{R}$ of prime ideals of F, then we can explicitly construct infinitely many CM extensions E/F which are ramified only at the primes in the prescribed set $\mathcal{R} \cup \{\mathfrak{p}\}$ and at exactly one more prime ideal of F (which is different for each of the extensions E/F) such that $E/\mathbb{Q}$ is non-Galois and the Colmez conjecture is true for E. Similarly, we can prescribe finite sets $\mathcal{U}_1$ (resp. $\mathcal{U}_2$) of prime ideals of F that will be split (resp. remain inert) in the extensions E/F.

Theorem A. *Let F be a totally real number field of degree $n \geq 3$. Let $p \in \mathbb{Z}$ be a prime number which splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let d_{F^s} be the discriminant of F^s and $\mathcal{R}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Let $\mathcal{U}_1$ and $\mathcal{U}_2$ be finite sets of prime ideals of F not dividing $2pd_{F^s}$ such that $\mathcal{R}$, $\mathcal{U}_1$ and $\mathcal{U}_2$ are pairwise disjoint. Then there is a set $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ of prime ideals of F which is disjoint from $\mathcal{R} \cup \mathcal{U}_1 \cup \mathcal{U}_2 \cup \{\mathfrak{p}\}$ such that the following statements are true.*

(i) *$\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ has positive natural density.*[†]

(ii) *For each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$, there is an element $\Delta_{\mathfrak{q}} \in \mathcal{O}_F$ with prime factorization*

$$\Delta_{\mathfrak{q}}\mathcal{O}_F = \mathfrak{p}\mathfrak{q} \prod_{\mathfrak{r} \in \mathcal{R}} \mathfrak{r}.$$

(iii) *The field $E_{\mathfrak{q}} := F(\sqrt{\Delta_{\mathfrak{q}}})$ is a CM extension of F which is non-Galois over $\mathbb{Q}$ and is ramified only at the prime ideals of F dividing $\Delta_{\mathfrak{q}}$. Moreover, each prime ideal in $\mathcal{U}_1$ splits in $E_{\mathfrak{q}}$ and each prime ideal in $\mathcal{U}_2$ remains inert in $E_{\mathfrak{q}}$.*

(iv) *The Colmez conjecture is true for $E_{\mathfrak{q}}$.*

Remark 3.1.1. We emphasize that Theorem A is *effective* in the sense that we give an algorithm to construct the set $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ and the associated CM fields $E_{\mathfrak{q}}$ for $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$. See Section 3.7, and in particular, Section 3.7.4, Algorithm 1.

Remark 3.1.2. The set of prime numbers $p \in \mathbb{Z}$ which split in the Galois closure F^s has natural density $1/[F^s : \mathbb{Q}]$.

In our second main result, we will prove that the Colmez conjecture is true for a generic class of non-abelian CM fields called Weyl CM fields (see e.g. [CO12]). As remarked by Oort [Oor12, p. 5], "most CM fields are Weyl CM fields". There are (at least) two different ways in which "most" can be understood. In the context of Oort's remark, "most" refers to density results for isogeny classes of abelian varieties over finite fields. In Section 3.1.5 we will give an alternative point of view based on counting CM fields of fixed degree and bounded discriminant, and use this to develop a probabilistic approach to the Colmez conjecture.

To define the notion of a Weyl CM field, let $E = \mathbb{Q}(\alpha)$ be a CM field of degree $2g$. Let $m_\alpha(X)$ be the minimal polynomial of α and denote its roots by $\alpha_1 = \alpha, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g}$. Let $a_{2\ell-1} := \alpha_\ell$ and $a_{2\ell} := \overline{\alpha_\ell}$ for $\ell = 1, \ldots, g$. Then $E^s = \mathbb{Q}(a_1, \ldots, a_{2g})$ is the Galois closure of E. Let S_{2g}

[†] The *natural density* of a set $\mathcal{S}$ of prime ideals of a number field L is defined by

$$d(\mathcal{S}) := \lim_{X \to \infty} \frac{\#\{\mathfrak{q} \in \mathcal{S} \mid N_{L/\mathbb{Q}}(\mathfrak{q}) \leq X\}}{\#\{\mathfrak{q} \subset \mathcal{O}_L \mid \mathfrak{q} \text{ is a prime ideal with } N_{L/\mathbb{Q}}(\mathfrak{q}) \leq X\}},$$

provided the limit exists.

be the symmetric group on the letters $\{a_1, \ldots, a_{2g}\}$ and W_{2g} be the subgroup of S_{2g} consisting of permutations which map any pair of the form $\{a_{2j-1}, a_{2j}\}$ to a pair $\{a_{2k-1}, a_{2k}\}$. The group W_{2g} is called the *Weyl group*. The Weyl group has order $\#W_{2g} = 2^g g!$ and fits in the exact sequence

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^g \longrightarrow W_{2g} \longrightarrow S_g \longrightarrow 1.$$

Now, it can be shown that the Galois group $\mathrm{Gal}(E^s/\mathbb{Q})$ is isomorphic to a subgroup of W_{2g}. If E is a CM field such that $\mathrm{Gal}(E^s/\mathbb{Q}) \cong W_{2g}$, then E is called a *Weyl CM field*. Thus, for a CM field to be Weyl is analogous to the classical fact that the splitting field of a generic polynomial in $\mathbb{Q}[X]$ of degree g has Galois group isomorphic to S_g (see e.g. [Gal73]).

Theorem B. *If E is a Weyl CM field, then the Colmez conjecture is true for E.*

Remark 3.1.3. If E is a CM field with $[E : \mathbb{Q}] = 4$, the only possibilities for $\mathrm{Gal}(E^s/\mathbb{Q})$ are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or D_4. Therefore, since $D_4 \cong W_4$, every non-abelian quartic CM field E is Weyl. It then follows from Theorem B and the work of Colmez [Col93] and Obus [Obu13] that the Colmez conjecture is true for *every* quartic CM field.

Remark 3.1.4. We emphasize that if $g \geq 2$ and E is a Weyl CM field of degree $2g$, then $E/\mathbb{Q}$ is non-Galois since $\#\mathrm{Gal}(E^s/\mathbb{Q}) = 2^g g! > 2g = [E : \mathbb{Q}]$. In particular, any Weyl CM field of degree $2g \geq 4$ is non-abelian.

Remark 3.1.5. In Section 3.7 (see e.g. Remark 3.7.12), we will prove that the CM fields $E_{\mathfrak{q}}$ which appear in Theorem A are Weyl CM fields if and only if $[F^s : \mathbb{Q}] = n!$. In particular, if $[F^s : \mathbb{Q}] < n!$, then the fields $E_{\mathfrak{q}}$ are not Weyl CM fields, so that Theorems A and B can be viewed as complementary to one another.

3.1.4 Explicit non-abelian Chowla-Selberg formulas

One important feature of the precise form of the Colmez conjecture for the CM fields appearing in Theorems A and B is that it allows us to give explicit evaluations of Faltings heights of CM abelian varieties.

Recall that for imaginary quadratic fields, the Colmez conjecture is a geometric reformulation of the Chowla-Selberg formula which evaluates the Faltings height of a CM elliptic curve in terms of values of $\Gamma(s)$ at rational numbers. More precisely, if $E = \mathbb{Q}(\sqrt{-D})$ and X_Φ is a CM elliptic curve of type $(\mathcal{O}_E, \Phi)$, then substituting (3.2) into (3.4) yields

$$h_{\mathrm{Fal}}(X_\Phi) = -\frac{w(-D)}{4h(-D)} \sum_{k=1}^{D} \chi_{-D}(k) \log\left(\Gamma\left(\frac{k}{D}\right)\right) + \frac{1}{4}\log(D) - \frac{1}{2}\log(2\pi). \tag{3.5}$$

Now, if E is a CM field as in Theorem A or Theorem B, and X_Φ is a CM abelian variety of type $(\mathcal{O}_E, \Phi)$, then the Colmez conjecture takes the form (see Proposition 3.5.1)

$$h_{\mathrm{Fal}}(X_\Phi) = -\frac{1}{2}\frac{L'(\chi_{E/F}, 0)}{L(\chi_{E/F}, 0)} - \frac{1}{4}\log\left(\frac{|d_E|}{d_F}\right) - \frac{n}{2}\log(2\pi), \tag{3.6}$$

where $L(\chi_{E/F}, s)$ is the (incomplete) L–function of the Hecke character $\chi_{E/F}$ associated to the quadratic extension E/F and d_E (resp. d_F) is the discriminant of E (resp. F). In fact, we will develop a probabilistic framework which predicts that the Colmez conjecture takes this form "most" of the time (see Section 3.1.5). One reason for interest in this form of the Colmez conjecture is the appearance of the L–function $L(\chi_{E/F}, s)$, which allows us to give explicit "non-abelian Chowla-Selberg formulas" analogous to (3.5) which evaluate the Faltings heights of CM abelian varieties in terms of values of the Barnes multiple Gamma function at algebraic numbers in F. We will study this problem extensively in the forthcoming papers [BS-M16a, BS-M16b]. Here we give an example of such an evaluation for the Faltings height of the Jacobian of a genus 2 hyperelliptic curve with complex multiplication by a non-abelian quartic CM field.

Example 3.1.6. Let $E = \mathbb{Q}(\sqrt{-5-2\sqrt{2}})$. Then E is a non-abelian quartic CM field of discriminant $d_E = 1088$ with real quadratic subfield $F = \mathbb{Q}(\sqrt{2})$ of discriminant $d_F = 8$. Moreover, by Remark 3.1.3 the CM field E is Weyl, hence the Colmez conjecture is true for E.

Now, by [BS15, Theorem 1.1 and Table 2b] with the choice $[D, A, B] = [8, 10, 17]$, the Jacobian J_C of the genus 2 hyperelliptic curve C over $\mathbb{Q}(\sqrt{17})$ given by the equation

$$y^2 = x^6 + (3+\sqrt{17})x^5 + \left(\frac{25+3\sqrt{17}}{2}\right)x^4 + (3+5\sqrt{17})x^3 + \left(\frac{73-9\sqrt{17}}{2}\right)x^2 + (-24+8\sqrt{17})x + 10 - 2\sqrt{17} \tag{3.7}$$

is a CM abelian surface defined over $\overline{\mathbb{Q}}$ with complex multiplication by the ring of integers $\mathcal{O}_E$ of

E. The hyperelliptic curve C is shown in Figure 3.1.

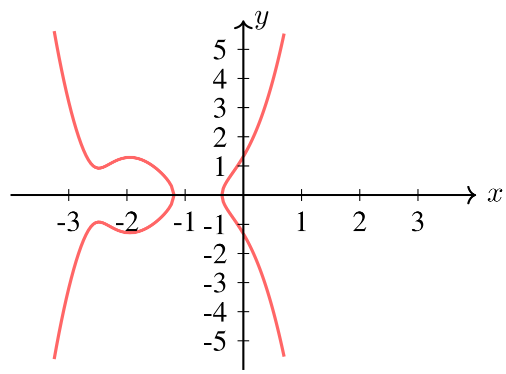


Figure 3.1: The hyperelliptic curve C.

Since the Colmez conjecture is true for E, it follows from (3.6) that

$$h_{\mathrm{Fal}}(J_C) = -\frac{1}{2}\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} - \frac{1}{4}\log(136) - \log(2\pi). \tag{3.8}$$

Hence, to complete the evaluation of $h_{\mathrm{Fal}}(J_C)$, we need a two-dimensional analog of Lerch's identity for the logarithmic derivative of $L(\chi_{E/F}, s)$ at $s = 0$. For this we require the Barnes double Gamma function (see e.g. [Bar01, Shi77b]).

Let $\omega = (\omega_1, \omega_2) \in \mathbb{R}_+^2$ and $z \in \mathbb{C}$. Then the *Barnes double Gamma function* is defined by

$$\Gamma_2(z, \omega) := F(z, \omega)^{-1},$$

where

$$F(z,\omega) := z \exp\left(\gamma_{22}(\omega) z + \frac{z^2}{2}\gamma_{21}(\omega)\right) \times \prod_{(m,n)} \left(1 + \frac{z}{m\omega_1 + n\omega_2}\right) \exp\left(-\frac{z}{m\omega_1 + n\omega_2} + \frac{z^2}{2(m\omega_1 + n\omega_2)^2}\right),$$

the product being over all pairs of integers $(m, n) \in \mathbb{Z}_{\geq 0}^2$ with $(m, n) \neq (0, 0)$. The function $F(z, \omega)$ is entire, and the constants $\gamma_{22}(\omega), \gamma_{21}(\omega)$ are explicit "higher" analogs of Euler's constant γ.

Given an element $\alpha \in F$, let $\langle \alpha \rangle = \alpha \mathcal{O}_F$ and α^σ be the image of α under an automorphism $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. We also let α' denote the image of α under the nontrivial automorphism in $\mathrm{Gal}(F/\mathbb{Q})$.

Let $\mathfrak{D}_{E/F}$ be the relative discriminant, h_E be the class number of E, and $\varepsilon > 1$ be the generator of the group $\mathcal{O}_F^{\times,+}$ of totally positive units of F. Let $B_2(t) = t^2 - t + 1/6$ be the second Bernoulli polynomial.

In [BS-M16a], we use work of Shintani [Shi77b] to establish the following two dimensional analog of Lerch's identity (3.2),

$$\begin{aligned}\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} &= -\log(N_{F/\mathbb{Q}}(\mathfrak{D}_{E/F})) \\ &+ \frac{[\mathcal{O}_E^\times : \mathcal{O}_F^\times]}{2h_E} \sum_{z \in \mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})} \chi_{E/F}\left(\mathfrak{D}_{E/F}\langle z \rangle\right) \log\left(\prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \Gamma_2\big(z^\sigma, (1, \varepsilon^\sigma)\big)\right) \\ &+ \frac{\varepsilon - \varepsilon'}{2} \log(\varepsilon') \frac{[\mathcal{O}_E^\times : \mathcal{O}_F^\times]}{2h_E} \sum_{\substack{z \in \mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1}) \\ z = x + y\varepsilon}} \chi_{E/F}\left(\mathfrak{D}_{E/F}\langle z \rangle\right) B_2(x),\end{aligned} \tag{3.9}$$

where $\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})$ is a finite subset of $\mathfrak{D}_{E/F}^{-1}$ consisting of the elements $z = x + y\varepsilon \in \mathfrak{D}_{E/F}^{-1}$ such that

- $x, y \in \mathbb{Q}$,
- $0 < x \leq 1,\ 0 \leq y < 1$, and
- $\mathfrak{D}_{E/F}\langle z \rangle$ is coprime to $\mathfrak{D}_{E/F}$.

Here we have $\mathfrak{D}_{E/F} = \langle -5 - 2\sqrt{2} \rangle$ and $\varepsilon = 3 + 2\sqrt{2}$. We wrote a program in `SageMath` to compute the Shintani set $\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})$. This set can be visualized geometrically in $\mathbb{R}_+^2$ via the embedding $\alpha \longmapsto (\alpha, \alpha')$ as a finite subset of the Shintani cone

$$C(\varepsilon) := \left\{ t_1(1,1) + t_2\left(\varepsilon, \varepsilon'\right) \;\middle|\; t_1 > 0,\ t_2 \geq 0 \right\} \subset \mathbb{R}_+^2$$

generated by the vectors $(1,1)$ and $(\varepsilon, \varepsilon')$, as shown in Figure 3.2.[‡]

[‡]The shaded parallelogram in Figure 3.2 is the subset of the Shintani cone $\mathcal{C}(\varepsilon)$ determined by the inequalities $0 < t_1 \leq 1$ and $0 \leq t_2 < 1$, which correspond to the inequalities appearing in the definition of $\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})$.

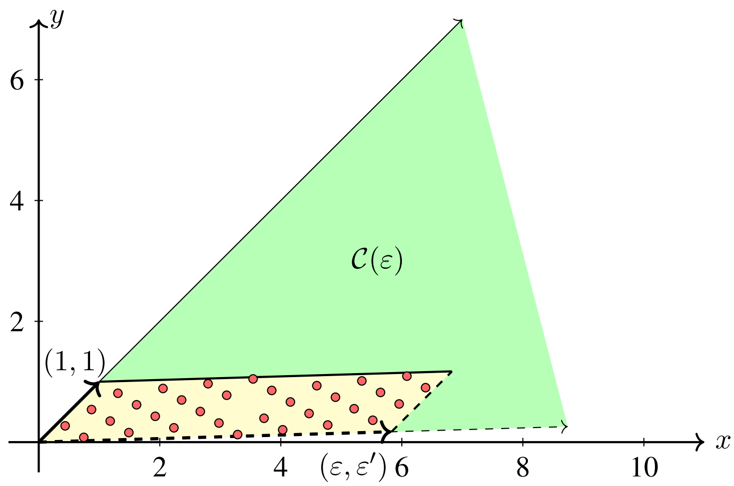


Figure 3.2: The embedding of $\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})$ into $C(\varepsilon)$.

In order to give a uniform description of the points in $\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1})$, it is convenient to express them in terms of a $\mathbb{Z}$-basis for $\mathfrak{D}_{E/F}^{-1}$. In particular, for the $\mathbb{Z}$-basis given by

$$\mathfrak{D}_{E/F}^{-1} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \left(\frac{6+\sqrt{2}}{17} \right),$$

we find that

$$\mathcal{R}(\varepsilon, \mathfrak{D}_{E/F}^{-1}) = \left\{ z_{m,n} := -m + (4m+n-1) \left(\tfrac{6+\sqrt{2}}{17} \right) \;\middle|\; 0 \le m \le 8,\ n \in S(m) \right\},$$

where

$$S(m) := \begin{cases} \{2,3,4\} & \text{if } m = 0 \\ \{1,2,3,4\} & \text{if } m = 1,2,3 \\ \{1,3\} & \text{if } m = 4 \\ \{0,1,2,3\} & \text{if } m = 5,6,7 \\ \{0,1,2\} & \text{if } m = 8. \end{cases}$$

We also wrote a program in SageMath to compute the character values

$$c_{m,n} := \chi_{E/F}(\mathfrak{D}_{E/F}\langle z_{m,n}\rangle) \in \{\pm 1\},$$

which are given in Table 3.1.

Values of $c_{m,n}$									
$n \backslash m$	0	1	2	3	4	5	6	7	8
0						-1	1	1	1
1		-1	-1	1	-1	1	1	1	-1
2	-1	1	-1	-1		-1	-1	1	-1
3	-1	1	1	1	-1	1	-1	-1	
4	1	1	1	-1					

Table 3.1: The character values $c_{m,n} := \chi_{E/F}(\mathfrak{D}_{E/F}\langle z_{m,n}\rangle)$.

Since $[\mathcal{O}_E^\times : \mathcal{O}_F^\times] = 1$ and $h_E = 1$, the preceding calculations yield the following explicit version of (3.9),

$$\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} = -\log(17) + \frac{1}{2}\sum_{\substack{0\le m\le 8\\ n\in S(m)}} c_{m,n}\log\left(\prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}\Gamma_2\big(z_{m,n}^{\sigma},(1,\varepsilon^{\sigma})\big)\right) - \frac{4\sqrt{2}}{17}\log(\varepsilon). \tag{3.10}$$

Finally, by combining (3.8) and (3.10) we get an explicit evaluation of $h_{\mathrm{Fal}}(J_C)$ which is summarized in the following theorem.

Theorem 3.1.7. *Let C be the genus 2 hyperelliptic curve over $\mathbb{Q}(\sqrt{17})$ defined by (3.7). The Jacobian J_C is a CM abelian surface defined over $\overline{\mathbb{Q}}$ with complex multiplication by the ring of integers $\mathcal{O}_E$ of the non-abelian quartic CM field $E = \mathbb{Q}(\sqrt{-5-2\sqrt{2}})$ with real quadratic subfield $F = \mathbb{Q}(\sqrt{2})$. The Faltings height of J_C is given by*

$$h_{\mathrm{Fal}}(J_C) = -\frac{1}{4} \sum_{\substack{0 \le m \le 8 \\ n \in S(m)}} c_{m,n} \log \left(\prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \Gamma_2\big(z_{m,n}^{\sigma}, (1, \varepsilon^{\sigma})\big) \right)$$
$$+ \frac{2\sqrt{2}}{17} \log(\varepsilon) + \frac{1}{4} \log\left(\frac{17}{8}\right) - \log(2\pi),$$

where $z_{m,n} = -m + (4m+n-1)(\frac{6+\sqrt{2}}{17})$, $\varepsilon = 3 + 2\sqrt{2}$, and the numbers $c_{m,n} \in \{\pm 1\}$ are given in Table 3.1.

3.1.5 An arithmetic statistics approach to the Colmez conjecture

In this section we develop an approach to the Colmez conjecture based on the study of certain problems of arithmetic distribution.

3.1.5.1 The density of Weyl CM fields when ordered by discriminant

A natural way to count number fields $K/\mathbb{Q}$ which satisfy some property is to order them by the absolute value of their discriminant d_K. Here we are interested in the problem of counting number fields (and in particular CM fields) with a given Galois group. This problem has a long history and has been studied extensively by many authors in recent years. See for example the excellent survey articles [CDO06, Woo16].

We start by introducing some notation. If $K/\mathbb{Q}$ is a number field, we denote its isomorphism class by $[K/\mathbb{Q}]$. For a permutation group G on n letters, we define the counting function

$$N_n(G, X) := \#\{[K/\mathbb{Q}] \mid [K : \mathbb{Q}] = n,\ \mathrm{Gal}(K^s/\mathbb{Q}) \cong G \text{ and } |d_K| \le X\},$$

which counts the number of isomorphism classes of number fields $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = n$ such that the Galois group of the Galois closure K^s is $\mathrm{Gal}(K^s/\mathbb{Q}) \cong G$ and such that $|d_K| \le X$.

Similarly, in order to count isomorphism classes of number fields with a specific signature

(r_1, r_2), where $n = r_1 + 2r_2$, we define the counting function

$$N_{r_1,r_2}(G, X) := \#\{[K/\mathbb{Q}] \in N_n(G, X) \mid \text{signature}(K) = (r_1, r_2)\}.$$

Now, for CM fields we define the counting functions

$$\mathrm{CM}_n(X) := \#\{[E/\mathbb{Q}] \mid E \text{ is a CM field, } [E : \mathbb{Q}] = n \text{ and } |d_E| \leq X\}$$

and

$$\mathrm{CM}_n(G, X) := \#\{[E/\mathbb{Q}] \in \mathrm{CM}_n(X) \mid \mathrm{Gal}(E^s/\mathbb{Q}) \cong G\}.$$

We want to study the density of Weyl CM fields of fixed degree $2n$ when ordered by discriminant, i.e., we want to study the limit

$$\rho_{\text{Weyl}}(2n) := \lim_{X\to\infty} \frac{\mathrm{CM}_{2n}(W_{2n}, X)}{\mathrm{CM}_{2n}(X)},$$

provided the limit exists. Conjectures of Malle [Mal02, Mal04] and various refinements (see e.g. [Bha07, Woo16]) concerning asymptotics for the counting functions $N_n(G, X)$ and $N_{r_1,r_2}(G, X)$ suggest that this limit exists and is positive. This is of great interest, for if $\rho_{\text{Weyl}}(2n) > 0$ then Theorem B implies that the Colmez conjecture is true for a positive proportion of CM fields of fixed degree $2n$ when ordered by discriminant.

When $n = 1$, a CM field of degree 2 is just an imaginary quadratic field. In this case the Weyl group $W_2 \cong \mathbb{Z}/2\mathbb{Z}$, so trivially every quadratic CM field is Weyl and hence

$$\rho_{\text{Weyl}}(2) = \lim_{X\to\infty} \frac{\mathrm{CM}_2(W_2, X)}{\mathrm{CM}_2(X)} = 1.$$

When $n = 2$, the situation is already much more complicated. The following table can be extracted from [Coh03, p. 376], and strongly suggests that $\rho_{\text{Weyl}}(4)$ exists and equals 1.

X	$\mathrm{CM}_4(W_4, X)$	$\mathrm{CM}_4(X)$	$\frac{\mathrm{CM}_4(W_4,X)}{\mathrm{CM}_4(X)}$
10^4	27	72	37.5%
10^5	395	613	64.4%
10^6	4512	5384	83.8%
10^7	47708	51220	93.1%
10^8	486531	500189	97.3%
10^9	4904276	4956208	98.9%
10^{10}	49190647	49384381	99.6%
10^{12}	4926673909	4929271179	99.9%

Table 3.2: Density of quartic Weyl CM fields.

In fact, we will appeal to the works of Baily [Bai80], Mäki [Mäk85], and Cohen, Diaz y Diaz and Olivier [CDO02, CDO05, CDO06] to deduce the following result, which confirms the computational observations from Table 3.2.

Theorem 3.1.8. *The density of quartic Weyl CM fields is*

$$\rho_{\mathrm{Weyl}}(4) = \lim_{X \to \infty} \frac{\mathrm{CM}_4(W_4, X)}{\mathrm{CM}_4(X)} = 1.$$

Remark 3.1.9. It follows from Theorem B and Theorem 3.1.8 that the Colmez conjecture is true for 100% of quartic CM fields. On the other hand, we have already observed in Remark 3.1.3 that the Colmez conjecture is true for *every* quartic CM field. Nonetheless, Theorem 3.1.8 supports our belief that the probabilistic approach described here can be used to prove (at least in low degree) that the Colmez conjecture is true for a positive proportion of CM fields of fixed degree. We are currently investigating this problem for sextic CM fields.

3.1.5.2 Abelian varieties over finite fields and density results

We now explain how to use density results for isogeny classes of abelian varieties over finite fields to prove probabilistic results about the Colmez conjecture.

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements. Let α_A be a root of the characteristic polynomial f_A of the Frobenius endomorphism π_A of an abelian variety $A/\mathbb{F}_q$ of dimension g. It is known that if $A/\mathbb{F}_q$ and $B/\mathbb{F}_q$ are isogenous abelian varieties, then $f_A = f_B$.

Let $\mathcal{A}_g(q)$ be the set of isogeny classes of abelian varieties $A/\mathbb{F}_q$ of dimension g. Let $K_{f_A} = \mathbb{Q}(\alpha_A)^s$ be the splitting field of f_A and $\mathrm{Gal}(K_{f_A}/\mathbb{Q})$ be the Galois group. Kowalski [Kow06] proved that the proportion of isogeny classes $[A] \in \mathcal{A}_g(p^n)$ which satisfy $\mathrm{Gal}(K_{f_A}/\mathbb{Q}) \cong W_{2g}$ approaches 1 as $n \to \infty$. We will show that if $\mathrm{Gal}(K_{f_A}/\mathbb{Q}) \cong W_{2g}$ and $g \geq 2$, then $\mathbb{Q}(\alpha_A)$ is a non-Galois Weyl CM field of degree $2g \geq 4$. By combining these results with Theorem B, we will establish the following probabilistic result.

Theorem 3.1.10. *Suppose that $g \geq 2$. Then*

$$\lim_{n\to\infty} \frac{\#\{[A] \in \mathcal{A}_g(p^n) \mid \mathbb{Q}(\alpha_A) \textit{ is a non-Galois CM field satisfying the Colmez conjecture}\}}{\#\mathcal{A}_g(p^n)} = 1.$$

On the other hand, let $\mathcal{A}_g^s(q)$ be the set of isogeny classes of *simple* abelian varieties $A/\mathbb{F}_q$ of dimension g. We will use work of Greaves-Odoni [GO88] and Honda-Tate (see e.g. [Tat71]) to prove that given a CM field E of degree $2g$ and an integer $n \geq 2$, there is a set of prime numbers $p \in \mathbb{Z}$ with positive natural density such that $E \cong \mathbb{Q}(\pi_A)$ for some simple abelian variety $A/\mathbb{F}_{p^n}$ of dimension g. It seems likely that a modification of the methods in [Kow06] can be used to prove that the proportion of isogeny classes $[A] \in \mathcal{A}_g^s(p^n)$ which satisfy $\mathrm{Gal}(K_{f_A}/\mathbb{Q}) \cong W_{2g}$ approaches 1 as $n \to \infty$. As in Corollary 3.1.10, it would follow that if $g \geq 2$, then

$$\lim_{n\to\infty} \frac{\#\{[A] \in \mathcal{A}_g^s(p^n) \mid \mathbb{Q}(\pi_A) \text{ is a non-Galois CM field satisfying the Colmez conjecture}\}}{\#\mathcal{A}_g^s(p^n)} = 1.$$

3.1.6 Outline of the proofs of the main results

We now briefly outline the proofs of Theorems A and B.

Let E be a CM field of degree $2n$ and $\Phi(E)$ be the set of CM types for E. Let $\mathbb{Q}^{\mathcal{CM}}$ be the compositum of all CM fields. Then the Galois group $G^{\mathcal{CM}} := \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/\mathbb{Q})$ acts on $\Phi(E)$ by composition. By a careful study of the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ and a theorem of Colmez [Col93, Théoreme 0.3] which relates the Faltings height of a CM abelian variety X_Φ of type $(\mathcal{O}_E, \Phi)$ to the "height" of a certain locally constant function on $G^{\mathcal{CM}}$ constructed from the CM pair (E, Φ), we will prove that the Faltings height of X_Φ depends only on the $G^{\mathcal{CM}}$-orbit of Φ. Given this result, we will prove that if the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ is transitive, then an averaged version of the Colmez conjecture proved recently by Andreatta-Goren-Howard-Madapusi Pera [AGHM15] and Yuan-Zhang [YZ15] implies the Colmez conjecture for E.

Now, let Φ be a CM type and E_Φ be the associated reflex field. The reflex degree satisfies $[E_\Phi : \mathbb{Q}] \leq 2^n$. We will prove that the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ is transitive if and only if $[E_\Phi : \mathbb{Q}] = 2^n$. In particular, by the results discussed in the previous paragraph, if $[E_\Phi : \mathbb{Q}] = 2^n$ then the Colmez conjecture is true for E. This leads to the problem of constructing CM fields with reflex fields of maximal degree.

Roughly speaking, Theorems A and B comprise two different ways of constructing infinite families of CM fields with reflex fields of maximal degree. Our approach to Theorem A is as follows. Let F be a fixed totally real number field of degree $n \geq 3$. Based on an idea of Shimura [Shi70], in Section 3.7 we explicitly construct infinite families of CM extensions E/F such that $E/\mathbb{Q}$ is non-Galois and the reflex fields E_Φ have maximal degree. This construction is quite elaborate, and consists of two main parts. First, in Proposition 3.7.1 we explicitly construct infinite families of CM extensions E/F with "arbitrary" prescribed ramification. Second, in Theorem 3.7.6 we prove that if E/F is a CM extension satisfying a certain mild ramification condition, then the reflex fields E_Φ have maximal degree, and moreover, if $n \geq 3$ then $E/\mathbb{Q}$ is non-Galois. By combining these two results, we will obtain Theorem A. For the convenience of the reader, we have summarized this construction in Section 3.7.4, Algorithm 1. On the other hand, to prove Theorem B, we will show that the reflex fields of a Weyl CM field have maximal degree.

3.2 CM types and their equivalence

In this section we prove some important facts that we will need regarding CM types and their equivalence.

Let $\mathbb{Q}^{\mathcal{CM}}$ be the compositum of all CM fields. Then $\mathbb{Q}^{\mathcal{CM}}/\mathbb{Q}$ is a Galois extension of infinite degree, and the Galois group $G^{\mathcal{CM}} := \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/\mathbb{Q})$ is a profinite group with the Krull topology. Recall that the open sets of $G^{\mathcal{CM}}$ with the Krull topology are the empty set $\varnothing$ and the arbitrary unions

$$\bigcup_{i\in I} \sigma_i \operatorname{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_i),$$

where for every $i \in I$ we have $\sigma_i \in G^{\mathcal{CM}}$ and $\mathbb{Q} \subseteq E_i \subseteq \mathbb{Q}^{\mathcal{CM}}$ with $[E_i : \mathbb{Q}] < \infty$ and $E_i/\mathbb{Q}$ a Galois extension. The group $G^{\mathcal{CM}}$ is Hausdorff, compact, and totally disconnected (see e.g. [Mor96, Chapter IV]). A function $f : G^{\mathcal{CM}} \to \overline{\mathbb{Q}}$ is *locally constant* if for each $g \in G^{\mathcal{CM}}$, there is a neighborhood N_g of g such that f is constant on N_g.

Let $c \in G^{\mathcal{CM}}$ denote complex conjugation.

Definition 3.2.1. Let E be a CM field of degree $2n$. A *CM type* for E is a set Φ_E consisting of embeddings $E \hookrightarrow \overline{\mathbb{Q}}$ such that $\operatorname{Hom}(E, \overline{\mathbb{Q}}) = \Phi_E \bigcup c\Phi_E$. We denote the set of all CM types for E by $\Phi(E)$. The Galois group $G^{\mathcal{CM}}$ acts on $\Phi(E)$ as follows. For $\Phi_E := \{\sigma_1, \ldots, \sigma_n\} \in \Phi(E)$ and $\tau \in G^{\mathcal{CM}}$ let

$$\tau \cdot \Phi_E = \tau\Phi_E := \{\tau\sigma_1, \ldots, \tau\sigma_n\} \in \Phi(E).$$

Two CM types $\Phi_E, \Phi_E' \in \Phi(E)$ are said to be *equivalent* if they lie in the same orbit under the action of $G^{\mathcal{CM}}$, i.e., if there is an element $\tau \in G^{\mathcal{CM}}$ such that $\Phi_E = \tau \cdot \Phi_E'$.

We also have the following alternative definition.

Definition 3.2.2. A *CM type* is a locally constant function $\Phi : G^{\mathcal{CM}} \longrightarrow \overline{\mathbb{Q}}$ such that $\Phi(g) \in \{0, 1\}$ and $\Phi(g) + \Phi(cg) = 1$ for every $g \in G^{\mathcal{CM}}$. We let

$$\mathcal{CM} := \{\Phi : G^{\mathcal{CM}} \longrightarrow \overline{\mathbb{Q}} \mid \Phi \text{ is a CM type}\}$$

be the set of all CM types. The Galois group $G^{\mathcal{CM}}$ acts on $\mathcal{CM}$ as follows. For $\Phi \in \mathcal{CM}$ and $\tau \in G^{\mathcal{CM}}$, let $\tau \cdot \Phi \in \mathcal{CM}$ be the CM type defined by

$$(\tau \cdot \Phi)(g) := \Phi(\tau^{-1}g) \quad \text{for every } g \in G^{\mathcal{CM}}.$$

Two CM types $\Phi, \Phi' \in \mathcal{CM}$ are said to be *equivalent* if they lie in the same orbit under the action of $G^{\mathcal{CM}}$, i.e., if there is an element $\tau \in G^{\mathcal{CM}}$ such that $\Phi(g) = \Phi'(\tau^{-1}g)$ for every $g \in G^{\mathcal{CM}}$.

The following proposition gives a dictionary relating the two notions of a CM type and their equivalence.

Proposition 3.2.3. *The following statements are true.*

(i) Let E be a CM field and $\Phi_E \in \Phi(E)$. Define the function $\Phi : G^{\mathcal{CM}} \longrightarrow \overline{\mathbb{Q}}$ by

$$\Phi(g) := \chi_{\Phi_E}(g|_E), \quad g \in G^{\mathcal{CM}}$$

where χ_{Φ_E} denotes the characteristic function of the set Φ_E and $g|_E$ is the restriction of g to E. Then $\Phi \in \mathcal{CM}$. Moreover, if $\Phi'_E \in \Phi(E)$ is equivalent to Φ_E and $\tau \in G^{\mathcal{CM}}$ is such that $\Phi_E = \tau \cdot \Phi'_E$, then Φ' is equivalent to Φ with $\Phi = \tau \cdot \Phi'$.

(ii) Let $\Phi \in \mathcal{CM}$. Then there exists a Galois CM field E such that for every $g \in G^{\mathcal{CM}}$ and every $h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$, we have $\Phi(gh) = \Phi(g)$. Moreover, if $[g] := g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$ and we define

$$\Phi_E := \{\sigma \in \mathrm{Hom}(E, \overline{\mathbb{Q}}) \mid \textit{there exists } g \in G^{\mathcal{CM}} \textit{ with } \sigma = g|_E \textit{ and } \Phi([g]) = \{1\}\},$$

then $\Phi_E \in \Phi(E)$. Finally, if $\Phi' \in \mathcal{CM}$ is equivalent to Φ and $\tau \in G^{\mathcal{CM}}$ is such that $\Phi = \tau \cdot \Phi'$, then for every $g \in G^{\mathcal{CM}}$ and every $h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$, we have $\Phi'(gh) = \Phi'(g)$, and Φ'_E is equivalent to Φ_E with $\Phi_E = \tau \cdot \Phi'_E$.

For clarity we divide the proof of Proposition 3.2.3 into the following two subsections.

3.2.1 Proof of Proposition 3.2.3 (i)

Let E be a CM field and $\Phi_E \in \Phi(E)$ be a CM type for E. Define the function $\Phi : G^{\mathcal{CM}} \longrightarrow \{0, 1\}$ by

$$\Phi(g) := \chi_{\Phi_E}(g|_E), \quad g \in G^{\mathcal{CM}}$$

where χ_{Φ_E} is the characteristic function of the set Φ_E and $g|_E \in \mathrm{Hom}(E, \overline{\mathbb{Q}})$ is the restriction of g to E. We now prove that $\Phi \in \mathcal{CM}$.

Let $g \in G^{\mathcal{CM}}$. Since $\mathrm{Hom}(E, \overline{\mathbb{Q}}) = \Phi_E \dot{\bigcup} c\Phi_E$, we either have $g|_E \in \Phi_E$ or $g|_E \in c\Phi_E$, or equivalently, $g|_E \in \Phi_E$ or $(cg)|_E \in \Phi_E$. This proves that $\Phi(g) + \Phi(cg) = 1$. It remains to prove that Φ is locally constant. Let E^s be the Galois closure of E. Then E^s is also a CM field (see e.g.

[Shi94, Proposition 5.12]), and it follows that $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E^s)$ is an open set containing g. Now, observe that for any $h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E^s)$, we have $h|_E = \mathrm{id}_E$, so that $(gh)|_E = g|_E$. Therefore

$$\Phi(gh) = \chi_{\Phi_E}((gh)|_E) = \chi_{\Phi_E}(g|_E) = \Phi(g),$$

which implies that Φ is constant on $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E^s)$. It follows that Φ is locally constant, and hence $\Phi \in \mathcal{CM}$.

Now, suppose that Φ_E and $\Phi_E^{'}$ are equivalent CM types for E. Let $\tau \in G^{\mathcal{CM}}$ be such $\Phi_E = \tau\Phi_E^{'}$. Then for an arbitrary element $g \in G^{\mathcal{CM}}$, the corresponding CM types $\Phi, \Phi^{'} \in \mathcal{CM}$ satisfy

$$\Phi(g) = \chi_{\Phi_E}(g|_E) = \chi_{\tau\Phi_E^{'}}(g|_E) = \chi_{\Phi_E^{'}}((\tau^{-1}g)|_E) = \Phi^{'}(\tau^{-1}g).$$

Therefore, Φ is equivalent to Φ' with $\Phi = \tau \cdot \Phi'$. This completes the proof of Proposition 3.2.3 (i). □

3.2.2 Proof of Proposition 3.2.3 (ii)

The first assertion of Proposition 3.2.3 (ii) is proved in the following lemma.

Lemma 3.2.4. *Let $\Phi \in \mathcal{CM}$ be a CM type. Then there exists a Galois CM field E such that for every $g \in G^{\mathcal{CM}}$ and every $h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$ we have $\Phi(gh) = \Phi(g)$.*

Proof. Let $g \in G^{\mathcal{CM}}$. Since Φ is locally constant, there exists an open set U_g containing g such that Φ is constant on U_g. Now, by definition of the Krull topology we have

$$U_g = \bigcup_{i \in I} g_i\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_i),$$

where for every $i \in I$ we have $g_i \in G^{\mathcal{CM}}$ and $\mathbb{Q} \subseteq E_i \subseteq \mathbb{Q}^{\mathcal{CM}}$ with $[E_i : \mathbb{Q}] < \infty$ and $E_i/\mathbb{Q}$ a Galois extension. Since $g \in U_g$, we have $g \in g_{i_0}\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{i_0})$ for some $i_0 \in I$. It follows that $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{i_0}) \subseteq g_{i_0}\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{i_0})$. Let E_g be any Galois CM field containing E_{i_0}. Then

$$g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_g) \subseteq g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{i_0}) \subseteq g_{i_0}\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{i_0}) \subseteq U_g.$$

From the preceding facts, we conclude that

$$\{g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_g) \mid g \in G^{\mathcal{CM}}\}$$

is an open cover of $G^{\mathcal{CM}}$ such that Φ is constant on each of the sets $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_g)$.

Now, since $G^{\mathcal{CM}}$ is compact, there exists a finite subcover

$$\{g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})\}_{j=1}^{r}$$

for some elements $g_j \in G^{\mathcal{CM}}$. Let $E := E_{g_1} \cdots E_{g_r}$ be the compositum of the Galois CM fields E_{g_j}. Then E is a Galois CM field (see e.g. [Shi94, Proposition 5.12]). To complete the proof, we will show that Φ is constant on $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$ for every $g \in G^{\mathcal{CM}}$.

Since Φ is constant on each $g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$, it suffices to show that there exists an integer $j \in \{1, \ldots, r\}$ such that $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E) \subset g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$. Since

$$\{g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})\}_{j=1}^{r}$$

covers $G^{\mathcal{CM}}$, there exists an integer $j \in \{1, \ldots, r\}$ such that $g \in g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$. This implies that $g = g_j h_j$ for some $h_j \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$. Let $\sigma \in g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$. Then $\sigma = gh$ for some $h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$, hence $\sigma = g_j h_j h$. Moreover, since $\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E) \subset \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_i})$, we have $h_j h \in \mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$. It follows that $\sigma \in g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$, and so $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E) \subset g_j\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E_{g_j})$, as desired. □

We now prove the second assertion of Proposition 3.2.3 (ii). Let $\Phi \in \mathcal{CM}$ be a CM type. By Lemma 3.2.4, there exists a Galois CM field E such that Φ is constant on $g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$ for every $g \in G^{\mathcal{CM}}$. For notational convenience, we define $[g] := g\,\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$. Since $E/\mathbb{Q}$ is Galois, we have $\mathrm{Hom}(E, \overline{\mathbb{Q}}) = \mathrm{Gal}(E/\mathbb{Q})$, and

$$\frac{G^{\mathcal{CM}}}{\mathrm{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)} \cong \mathrm{Hom}(E, \overline{\mathbb{Q}}). \tag{3.11}$$

Define the set

$$\Phi_E := \{\sigma \in \mathrm{Hom}(E, \overline{\mathbb{Q}}) \mid \text{there exists } g \in G^{\mathcal{CM}} \text{ with } \sigma = g|_E \text{ and } \Phi([g]) = \{1\}\}.$$

We now show that $\Phi_E \in \Phi(E)$.

By (3.11), given an element $\sigma \in \operatorname{Hom}(E, \overline{\mathbb{Q}})$, there is a unique coset

$$[g] \in G^{\mathcal{CM}} / \operatorname{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$$

such that $\sigma = g|_E$. Since Φ is constant on each coset $[g]$, it follows that either $\Phi([g]) = \{0\}$ or $\Phi([g]) = \{1\}$. Suppose that $\sigma \notin \Phi_E$. Then $\Phi([g]) = \{0\}$, so that $\Phi([cg]) = \{1\}$. Moreover, we have $c\sigma = (cg)|_E$, and thus $c\sigma \in \Phi_E$, or equivalently, $\sigma \in c\Phi_E$. A short calculation shows that $\Phi_E \cap c\Phi_E = \varnothing$. Hence $\operatorname{Hom}(E, \overline{\mathbb{Q}}) = \Phi_E \biguplus c\Phi_E$, and we conclude that $\Phi_E \in \Phi(E)$.

Finally, we prove the third assertion of Proposition 3.2.3 (ii). Suppose that $\Phi^{'} \in \mathcal{CM}$ is equivalent to Φ. Let $\tau \in G^{\mathcal{CM}}$ be such that $\Phi = \tau \cdot \Phi'$, i.e. $\Phi(g) = \Phi^{'}(\tau^{-1}g)$ for every $g \in G^{\mathcal{CM}}$. Since Φ is constant on $\tau g \operatorname{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$, it follows that for every $g \in G^{\mathcal{CM}}$ and every $h \in \operatorname{Gal}(\mathbb{Q}^{\mathcal{CM}}/E)$, we have

$$\Phi^{'}(gh) = \Phi(\tau gh) = \Phi(\tau g) = \Phi^{'}(g).$$

Let

$$\Phi^{'}_E := \{\sigma' \in \operatorname{Hom}(E, \overline{\mathbb{Q}}) \mid \text{there exists } g' \in G^{\mathcal{CM}} \text{ with } \sigma = g'|_E \text{ and } \Phi^{'}([g']) = \{1\}\}.$$

We will prove that $\Phi_E = \tau\Phi^{'}_E$. We need only prove the containment $\Phi_E \subseteq \tau\Phi^{'}_E$, since the reverse containment can be proved mutatis mutandis. Let $\sigma \in \Phi_E$ and let $g \in G^{\mathcal{CM}}$ be such that $\sigma = g|_E$ and $\Phi(g) = 1$. Then this implies that $\Phi^{'}(\tau^{-1}g) = 1$. Finally, let $\sigma' := (\tau^{-1}g)|_E$. Then $\sigma' \in \Phi^{'}_E$, and moreover $\sigma = \tau\sigma'$, so that $\sigma \in \tau\Phi^{'}_E$. Hence $\Phi_E \subseteq \tau\Phi^{'}_E$. This completes the proof of Proposition 2.3 (ii). □

Important Remark. *In light of Proposition 3.2.3, from here forward we will use the two different notions of CM type and equivalence of CM types interchangeably, leaving it to the reader to distinguish which notion is being used from the context.*

3.3 Faltings heights and the Colmez conjecture

In this section we review the statement of the Colmez conjecture, following closely the discussion in [Col98] and [Yan10b].

We begin by recalling the definition of the Faltings height of a CM abelian variety. Let F be a totally real number field of degree n. Let E/F be a CM extension of F and $\Phi \in \Phi(E)$ be a CM type for E. Let X_Φ be an abelian variety defined over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_E$ and CM type Φ. We call X_Φ a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Let $K \subseteq \overline{\mathbb{Q}}$ be a number field over which X_Φ has everywhere good reduction and choose a Néron differential $\omega \in H^0(X_\Phi, \Omega^n_{X_\Phi})$. Then the *Faltings height* of X_Φ is defined by

$$h_{\mathrm{Fal}}(X_\Phi) := -\frac{1}{2[K:\mathbb{Q}]} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log \left| \int_{X^\sigma_\Phi(\mathbb{C})} \omega \wedge \overline{\omega^\sigma} \right|.$$

The Faltings height does not depend on the choice of K or ω. Moreover, Colmez [Col93] proved that if X_Φ and Y_Φ are CM abelian varieties of type $(\mathcal{O}_E, \Phi)$, then $h_{\mathrm{Fal}}(X_\Phi) = h_{\mathrm{Fal}}(Y_\Phi)$, i.e., the Faltings height depends on the CM type Φ, but does not depend on the choice of CM abelian variety X_Φ.

Let $H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ be the Hecke algebra of Schwartz functions on the Galois group $G^{\mathcal{CM}}$ which take values in $\overline{\mathbb{Q}}$ (see e.g. [Win89]). This is the $\overline{\mathbb{Q}}$-algebra of locally constant, compactly supported functions $f : G^{\mathcal{CM}} \longrightarrow \overline{\mathbb{Q}}$ with multiplication of functions $f_1, f_2 \in H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ given by the convolution

$$(f_1 * f_2)(g) := \int_{G^{\mathcal{CM}}} f_1(h) f_2(h^{-1}g)\, d\mu(h).$$

Here μ is the left-invariant Haar measure on $G^{\mathcal{CM}}$, normalized so that

$$\mathrm{Vol}(G^{\mathcal{CM}}) = \int_{G^{\mathcal{CM}}} d\mu(g) = 1.$$

The Hecke algebra $H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ is an associative algebra with no identity element. For a function $f \in H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$, the *reflex function* $f^\vee \in H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ is defined by $f^\vee(g) := \overline{f(g^{-1})}$. We define a Hermitian inner product on $H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ by

$$\langle f_1, f_2 \rangle := \int_{G^{\mathcal{CM}}} f_1(h) \overline{f_2(h)}\, d\mu(h).$$

Let $H^0(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ be the $\overline{\mathbb{Q}}$-subalgebra of $H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ of class functions, i.e., the $\overline{\mathbb{Q}}$-subalgebra of functions $f \in H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ satisfying $f(hgh^{-1}) = f(g)$ for all $h, g \in G^{\mathcal{CM}}$. It is known that an orthonormal basis for $H^0(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ is given by the set

$$\{\chi_\pi \mid \pi \text{ an irreducible representation of } G^{\mathcal{CM}}\}$$

of Artin characters χ_π associated to the irreducible representations π of $G^{\mathcal{CM}}$.

There is a projection map

$$H(G^{\mathcal{CM}}, \overline{\mathbb{Q}}) \longrightarrow H^0(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$$

$$f \longmapsto f^0$$

defined by

$$f^0(g) := \int_{G^{\mathcal{CM}}} f(hgh^{-1})\, d\mu(h).$$

As a map of $\overline{\mathbb{Q}}$-vector spaces, it corresponds to the orthogonal projection of $H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ onto $H^0(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$. In particular, one has

$$f^0 = \sum_{\chi_\pi} \langle f, \chi_\pi \rangle \chi_\pi.$$

Define the functions

$$Z(f^0, s) := \sum_{\chi_\pi} \langle f, \chi_\pi \rangle \frac{L'(\chi_\pi, s)}{L(\chi_\pi, s)} \quad \text{and} \quad \mu_{\mathrm{Art}}(f^0) := \sum_{\chi_\pi} \langle f, \chi_\pi \rangle \log(\mathfrak{f}_{\chi_\pi}),$$

where $L(\chi_\pi, s)$ is the (incomplete) Artin L–function of χ_π and $\mathfrak{f}_{\chi_\pi}$ is the analytic Artin conductor of χ_π.

If $\Phi \in \mathcal{CM}$ is a CM type, we define the function $A_\Phi \in H(G^{\mathcal{CM}}, \overline{\mathbb{Q}})$ by

$$A_\Phi := \Phi * \Phi^\vee.$$

Colmez [Col93] made the following conjecture.

Conjecture 3.3.1 (Colmez [Col93])**.** *Let E be a CM field, Φ be a CM type for E, and X_Φ be a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Let $A_{E,\Phi} := [E:\mathbb{Q}]A_\Phi$. Then*

$$h_{\mathrm{Fal}}(X_\Phi) = -Z(A^0_{E,\Phi}, 0) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi}).$$

Colmez [Col93] proved Conjecture 3.3.1 when $E/\mathbb{Q}$ is abelian, up to addition of a rational multiple of $\log(2)$ which was recently shown to equal zero by Obus [Obu13]. Yang [Yan10a, Yan10b, Yan13] proved Conjecture 3.3.1 for a large class of non-biquadratic quartic CM fields, thus establishing the only known cases of the Colmez conjecture when $E/\mathbb{Q}$ is *non-abelian*.

3.4 The average Colmez conjecture

Let F be a totally real number field of degree n. Let E/F be a CM extension of F and $\Phi(E)$ be the set of CM types for E. There are 2^n CM types $\Phi \in \Phi(E)$. By averaging both sides of Conjecture 3.3.1 over $\Phi(E)$, one gets the conjectural identity

$$\frac{1}{2^n}\sum_{\Phi\in\Phi(E)} h_{\mathrm{Fal}}(X_\Phi) = \frac{1}{2^n}\sum_{\Phi\in\Phi(E)} (-Z(A^0_{E,\Phi},0) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi})). \tag{3.12}$$

The average on the right hand side of (3.12) can be simplified. Namely, by [AGHM15, Proposition 8.4.1] we have

$$\frac{1}{2^n}\sum_{\Phi\in\Phi(E)} \left(-Z(A^0_{E,\Phi},0) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi})\right) = -\frac{1}{2}\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} - \frac{1}{4}\log\left(\frac{|d_E|}{d_F}\right) - \frac{n}{2}\log(2\pi), \tag{3.13}$$

where $L(\chi_{E/F},s)$ is the (incomplete) L–function of the Hecke character $\chi_{E/F}$ associated to the quadratic extension E/F and d_E (resp. d_F) is the discriminant of E (resp. F).

These identities yield the following averaged version of the Colmez conjecture.

Conjecture 3.4.1 (The Average Colmez Conjecture)**.** *Let F be a totally real number field of degree n. Let E/F be a CM extension of F, and for each CM type $\Phi \in \Phi(E)$, let X_Φ be a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Then*

$$\frac{1}{2^n}\sum_{\Phi\in\Phi(E)} h_{\mathrm{Fal}}(X_\Phi) = -\frac{1}{2}\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} - \frac{1}{4}\log\left(\frac{|d_E|}{d_F}\right) - \frac{n}{2}\log(2\pi). \tag{3.14}$$

Conjecture 3.4.1 was recently proved independently by Andreatta, Goren, Howard, Madapusi Pera [AGHM15] and Yuan-Zhang [YZ15].

Theorem 3.4.2 ([AGHM15], [YZ15])**.** *Conjecture 3.4.1 is true.*

3.5 The action of $G^{\mathcal{CM}}$ on $\Phi(E)$ and the Colmez conjecture

In this section we prove the following result.

Proposition 3.5.1. *Let F be a totally real number field of degree n. Let E/F be a CM extension of F and $\Phi(E)$ be the set of CM types for E. If the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ is transitive, then*

Conjecture 3.3.1 is true. In particular, if $\Phi \in \Phi(E)$ and X_Φ is a CM abelian variety of type $(\mathcal{O}_E, \Phi)$, then

$$h_{\mathrm{Fal}}(X_\Phi) = -\frac{1}{2}\frac{L'(\chi_{E/F},0)}{L(\chi_{E/F},0)} - \frac{1}{4}\log\left(\frac{|d_E|}{d_F}\right) - \frac{n}{2}\log(2\pi). \tag{3.15}$$

We will need the following two crucial lemmas.

Lemma 3.5.2. *If $\Phi_1, \Phi_2 \in \mathcal{CM}$ are equivalent CM types, then $A^0_{\Phi_1} = A^0_{\Phi_2}$.*

Proof. Since the CM types Φ_1 and Φ_2 are equivalent, there is an element $\tau^{-1} \in G^{\mathcal{CM}}$ such that $\Phi_1(g) = \Phi_2(\tau g)$ for every $g \in G^{\mathcal{CM}}$. Then we have

$$\begin{aligned}
A^0_{\Phi_1}(g) &= \int_{G^{\mathcal{CM}}} A_{\Phi_1}(hgh^{-1})\, d\mu(h) \\
&= \int_{G^{\mathcal{CM}}}\int_{G^{\mathcal{CM}}} \Phi_1(t)\Phi_1^\vee(t^{-1}hgh^{-1})\, d\mu(t)d\mu(h) \\
&= \int_{G^{\mathcal{CM}}}\int_{G^{\mathcal{CM}}} \Phi_1(t)\Phi_1(hg^{-1}h^{-1}t)\, d\mu(h)d\mu(t) \\
&= \int_{G^{\mathcal{CM}}}\int_{G^{\mathcal{CM}}} \Phi_2(\tau t)\Phi_2(\tau hg^{-1}h^{-1}t)\, d\mu(h)d\mu(t) \\
&= \int_{G^{\mathcal{CM}}} \Phi_2(\tau t)\left(\int_{G^{\mathcal{CM}}} \Phi_2(\tau hg^{-1}h^{-1}\tau^{-1}\tau t)\, d\mu(h)\right) d\mu(t).
\end{aligned} \tag{3.16}$$

Now, define the function $f_{g,\tau,t}(h) := \Phi_2(hg^{-1}h^{-1}\tau t)$. Then the inner integral in (3.16) can be written as

$$\begin{aligned}
\int_{G^{\mathcal{CM}}} \Phi_2(\tau hg^{-1}h^{-1}\tau^{-1}\tau t)\, d\mu(h) &= \int_{G^{\mathcal{CM}}} f_{g,\tau,t}(\tau h)\, d\mu(h) \\
&= \int_{G^{\mathcal{CM}}} f_{g,\tau,t}(h)\, d\mu(h) \\
&= \int_{G^{\mathcal{CM}}} \Phi_2(hg^{-1}h^{-1}\tau t)\, d\mu(h),
\end{aligned} \tag{3.17}$$

where in the second equality we used the left-invariance of the Haar measure. We substitute the identity (3.17) for the inner integral in (3.16) and continue the calculation to get

$$\begin{aligned}
A^0_{\Phi_1}(g) &= \int_{G^{\mathcal{CM}}} \Phi_2(\tau t) \left(\int_{G^{\mathcal{CM}}} \Phi_2(hg^{-1}h^{-1}\tau t)\, d\mu(h) \right) d\mu(t) \\
&= \int_{G^{\mathcal{CM}}} \left(\int_{G^{\mathcal{CM}}} \Phi_2(\tau t)\Phi_2(hg^{-1}h^{-1}\tau t)\, d\mu(t) \right) d\mu(h) \\
&= \int_{G^{\mathcal{CM}}} \left(\int_{G^{\mathcal{CM}}} \Phi_2(t)\Phi_2(hg^{-1}h^{-1}t)\, d\mu(t) \right) d\mu(h) \\
&= \int_{G^{\mathcal{CM}}} \left(\int_{G^{\mathcal{CM}}} \Phi_2(t)\Phi_2^{\vee}(t^{-1}hgh^{-1})\, d\mu(t) \right) d\mu(h) \\
&= \int_{G^{\mathcal{CM}}} A_{\Phi_2}(hgh^{-1})\, d\mu(h) \\
&= A^0_{\Phi_2}(g),
\end{aligned}$$

where in the third equality we again used the left-invariance of the Haar measure. □

Lemma 3.5.3. *Let E be a CM field, let Φ_1 and Φ_2 be CM types for E, and let X_{Φ_1} and X_{Φ_2} be CM abelian varieties of types $(\mathcal{O}_E, \Phi_1)$ and $(\mathcal{O}_E, \Phi_2)$, respectively. If Φ_1 and Φ_2 are equivalent, then*

$$h_{\mathrm{Fal}}(X_{\Phi_1}) = h_{\mathrm{Fal}}(X_{\Phi_2}).$$

Proof. Let X_Φ be a CM abelian variety of type $(\mathcal{O}_E, \Phi)$. Then by Colmez [Col93, Théore-me 0.3], there is a unique $\mathbb{Q}$-linear height function ht : $H^0(G^{\mathcal{CM}}, \overline{\mathbb{Q}}) \to \mathbb{R}$ such that

$$h_{\mathrm{Fal}}(X_\Phi) = -\mathrm{ht}(A^0_{E,\Phi}) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi}). \tag{3.18}$$

Since Φ_1 and Φ_2 are equivalent, by Lemma 3.5.2 we have $A^0_{\Phi_1} = A^0_{\Phi_2}$, so that

$$A^0_{E,\Phi_1} = [E:\mathbb{Q}]A^0_{\Phi_1} = [E:\mathbb{Q}]A^0_{\Phi_2} = A^0_{E,\Phi_2}.$$

It follows from (3.18) that $h_{\mathrm{Fal}}(X_{\Phi_1}) = h_{\mathrm{Fal}}(X_{\Phi_2})$. □

Proof of Proposition 3.5.1. Fix a CM type $\Phi_0 \in \Phi(E)$, and let X_{Φ_0} be a CM abelian variety of type $(\mathcal{O}_E, \Phi_0)$. Since the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ is transitive, we have

$$\begin{aligned} h_{\mathrm{Fal}}(X_{\Phi_0}) &= \frac{1}{2^n} \sum_{\Phi \in \Phi(E)} h_{\mathrm{Fal}}(X_\Phi) \\ &= \frac{1}{2^n} \sum_{\Phi \in \Phi(E)} (-Z(A^0_{E,\Phi}, 0) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi})) \\ &= -Z(A^0_{E,\Phi_0}, 0) - \frac{1}{2}\mu_{\mathrm{Art}}(A^0_{E,\Phi_0}), \end{aligned} \tag{3.19}$$

where the first equality follows from Lemma 3.5.3, the second equality is the identity (3.12) (which is equivalent to Theorem 3.4.2), and the third equality follows from Lemma 3.5.2. Since Φ_0 was arbitrary, this proves Conjecture 3.3.1. The identity (3.15) for the Faltings height then follows from (3.19) and (3.13). □

3.6 The action of $G^{\mathcal{CM}}$ on $\Phi(E)$ and the reflex degree

In this section we relate the action of $G^{\mathcal{CM}}$ on $\Phi(E)$ to the degree of the reflex field of a CM pair (E, Φ).

Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. The following result can be found in [Mil06, Proposition 1.16] and [Shi98, Proposition 28], for example.

Proposition 3.6.1. *Let E be a CM field and Φ be a CM type for E. Then the following conditions on a subfield E_Φ of $\overline{\mathbb{Q}}$ are equivalent.*

(i) We have

$$\{\sigma \in G_{\mathbb{Q}} \mid \sigma \textit{ fixes } E_\Phi\} = \{\sigma \in G_{\mathbb{Q}} \mid \sigma\Phi = \Phi\},$$

that is, $\mathrm{Gal}(\overline{\mathbb{Q}}/E_\Phi) = \mathrm{Stab}_{G_{\mathbb{Q}}}(\Phi)$.

(ii) $E_\Phi = \mathbb{Q}\left(\{\mathrm{Tr}_\Phi(a) \mid a \in E\}\right)$, *where* $\mathrm{Tr}_\Phi(a) := \sum_{\phi \in \Phi} \phi(a)$ *is the type trace of* $a \in E$.

Definition 3.6.2. The field E_Φ satisfying the equivalent conditions in Proposition 3.6.1 is called the *reflex field* of the CM pair (E, Φ).

Let E^s denote the Galois closure of E.

Proposition 3.6.3. *Let E be a CM field of degree $2n$ and Φ be a CM type for E. Then*

$$[E_\Phi : \mathbb{Q}] = \#(\mathrm{Gal}(E^s/\mathbb{Q}) \cdot \Phi).$$

In particular, $[E_\Phi : \mathbb{Q}] \leq 2^n$.

Proof. By Proposition 3.6.1 (ii) we have $E_\Phi \subseteq E^s$, hence one can replace $\overline{\mathbb{Q}}$ with E^s and $G_\mathbb{Q}$ with $\mathrm{Gal}(E^s/\mathbb{Q})$ in Proposition 3.6.1 (i) to conclude that

$$\mathrm{Gal}(E^s/E_\Phi) = \mathrm{Stab}_{\mathrm{Gal}(E^s/\mathbb{Q})}(\Phi). \tag{3.20}$$

Then using the fundamental theorem of Galois theory, identity (3.20), and the orbit-stabilizer theorem, we have

$$\begin{aligned}[E_\Phi : \mathbb{Q}] &= [\mathrm{Gal}(E^s/\mathbb{Q}) : \mathrm{Gal}(E^s/E_\Phi)] = [\mathrm{Gal}(E^s/\mathbb{Q}) : \mathrm{Stab}_{\mathrm{Gal}(E^s/\mathbb{Q})}(\Phi)] \\ &= \#(\mathrm{Gal}(E^s/\mathbb{Q}) \cdot \Phi).\end{aligned}$$

Finally, since $\mathrm{Gal}(E^s/\mathbb{Q}) \cdot \Phi \subseteq \Phi(E)$ and $\#\Phi(E) = 2^n$, it follows that $[E_\Phi : \mathbb{Q}] \leq 2^n$. ☐

Corollary 3.6.4. *The action of $G^{\mathcal{CM}}$ on $\Phi(E)$ is transitive if and only if $[E_\Phi : \mathbb{Q}] = 2^n$ for some CM type $\Phi \in \Phi(E)$.*

Proof. Since E^s is a CM field, we have

$$\mathrm{Gal}(E^s/\mathbb{Q}) \cdot \Phi = G^{\mathcal{CM}} \cdot \Phi.$$

The result now follows from Proposition 3.6.3 and the fact that $\#\Phi(E) = 2^n$. ☐

3.7 CM fields with reflex fields of maximal degree

Let F be a totally real number field of degree n. In the paragraph following [Shi70, (1.10.1)], Shimura briefly sketched the construction of a CM extension E/F with reflex fields of maximal degree. Based on this idea, we undertake an extensive study of the problem of constructing CM fields with reflex fields of maximal degree and explicitly construct infinite families of CM extensions E/F with this property. When $n \geq 3$ these CM fields E are non-Galois over $\mathbb{Q}$.

We begin with the following facts and notation which will be needed for the results in this section.

3.7.1 Multiplicative congruences, ray class groups, and higher unit groups

Let K be a number field. For a prime ideal $\mathfrak{P}$ of K, let $v_{\mathfrak{P}} : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the discrete valuation defined by $v_{\mathfrak{P}}(x) := \mathrm{ord}_{\mathfrak{P}}(x)$. Also, let $K_{\mathfrak{P}}$ be the completion of K with respect to the $\mathfrak{P}$-adic absolute value $|\cdot|_{\mathfrak{P}}$ induced by the valuation $v_{\mathfrak{P}}$. We denote the ring of $\mathfrak{P}$-adic integers by $\mathcal{O}_{\mathfrak{P}}$. The unique maximal ideal of $\mathcal{O}_{\mathfrak{P}}$ is $\widehat{\mathfrak{P}} := \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$.

Let $U := \mathcal{O}_{\mathfrak{P}}^{\times}$ be the group of units of $\mathcal{O}_{\mathfrak{P}}$. For any $n \geq 1$, there is a subgroup of U defined by

$$U^{(n)} := 1 + \mathfrak{P}^n \mathcal{O}_{\mathfrak{P}},$$

called the *n-th higher unit group*. The higher unit groups form a decreasing filtration

$$U \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots \supseteq U^{(n)} \supseteq \cdots .$$

For elements $\alpha, \beta \in K^{\times}$, we define the multiplicative congruence by

$$\alpha \overset{\times}{\equiv} \beta \pmod{\mathfrak{P}^n} \iff \alpha \in \beta(1 + \mathfrak{P}^n \mathcal{O}_{\mathfrak{P}}).$$

Thus we see that equivalently

$$\alpha \overset{\times}{\equiv} \beta \pmod{\mathfrak{P}^n} \iff \frac{\alpha}{\beta} \in U^{(n)} \iff v_{\mathfrak{P}}\left(\frac{\alpha}{\beta} - 1\right) \geq n.$$

Let $\mathfrak{m}_0$ be an integral ideal of K and $\mathfrak{m}_\infty$ be the formal product of all the real infinite primes corresponding to the embeddings in $\mathrm{Hom}(K, \mathbb{R})$. Define the modulus $\mathfrak{m} := \mathfrak{m}_0 \mathfrak{m}_\infty$. Then we extend the multiplicative congruence by setting

$$\alpha \overset{\times}{\equiv} \beta \pmod{\mathfrak{m}} \iff \begin{cases} \alpha \overset{\times}{\equiv} \beta \pmod{\mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{m}_0)}} & \text{for all } \mathfrak{P} | \mathfrak{m}_0, \text{ and} \\ \dfrac{\sigma(\alpha)}{\sigma(\beta)} > 0 & \text{for all } \sigma \in \mathrm{Hom}(K, \mathbb{R}). \end{cases}$$

The multiplicative congruence is indeed multiplicative, i.e., if

$$\alpha_1 \overset{\times}{\equiv} \beta_1 \pmod{\mathfrak{m}} \quad \text{and} \quad \alpha_2 \overset{\times}{\equiv} \beta_2 \pmod{\mathfrak{m}},$$

then

$$\alpha_1\alpha_2 \overset{\times}{\equiv} \beta_1\beta_2 \pmod{\mathfrak{m}}.$$

Let $\mathcal{I}_K(\mathfrak{m}_0)$ be the group of all fractional ideals of K that are relatively prime to $\mathfrak{m}_0$. Let

$$K_{\mathfrak{m},1} := \{x \in K^\times \mid x\mathcal{O}_K \text{ is relatively prime to } \mathfrak{m}_0 \text{ and } x \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}\}$$

be the ray modulo $\mathfrak{m}$ and $\mathcal{P}_K(\mathfrak{m})$ be the subgroup of $\mathcal{I}_K(\mathfrak{m}_0)$ of principal fractional ideals $x\mathcal{O}_K$ generated by elements $x \in K_{\mathfrak{m},1}$. Then the *ray class group* of K modulo $\mathfrak{m}$ is the quotient group

$$\mathcal{R}_K(\mathfrak{m}) := \mathcal{I}_K(\mathfrak{m}_0)/\mathcal{P}_K(\mathfrak{m}).$$

A coset in the ray class group is called a *ray class* modulo $\mathfrak{m}$.

3.7.2 Constructing CM extensions with prescribed ramification

In the following proposition we explicitly construct infinite families of CM extensions with "arbitrary" prescribed ramification. This is a variation on [Shi67, Lemma 1.5], adapted to the particular setting we will consider.

Proposition 3.7.1. *Let F be a totally real number field. Let $p \in \mathbb{Z}$ be a prime number and $m \geq 1$ be a positive integer. Let $\mathfrak{p}$ be a prime ideal of F lying above p. Let $\mathcal{R}$ be a finite set of prime ideals of F not dividing pm. Let $\mathcal{U}_1$ and $\mathcal{U}_2$ be finite sets of prime ideals of F not dividing $2pm$ such that $\mathcal{R}, \mathcal{U}_1$ and $\mathcal{U}_2$ are pairwise disjoint. Then there is a set $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ of prime ideals of F which is disjoint from $\mathcal{R} \cup \mathcal{U}_1 \cup \mathcal{U}_2 \cup \{\mathfrak{p}\}$ such that the following statements are true.*

(i) $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ has positive natural density.

(ii) Each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$ is relatively prime to pm.

(iii) For each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$, there is an element $\Delta_\mathfrak{q} \in \mathcal{O}_F$ with prime factorization

$$\Delta_\mathfrak{q}\mathcal{O}_F = \mathfrak{p}\mathfrak{q}\prod_{\mathfrak{r}\in\mathcal{R}} \mathfrak{r}.$$

(iv) The field $E_\mathfrak{q} := F(\sqrt{\Delta_\mathfrak{q}})$ is a CM extension of F which is ramified only at the prime ideals of F dividing $\Delta_\mathfrak{q}$. Moreover, each prime ideal in $\mathcal{U}_1$ splits in $E_\mathfrak{q}$ and each prime ideal in $\mathcal{U}_2$

is inert in $E_{\mathfrak{q}}$.

Remark 3.7.2. Note that if $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$, then the associated CM extensions $E_{\mathfrak{q}_1}/F$ and $E_{\mathfrak{q}_2}/F$ are distinct since they are ramified only at the primes in the sets $\mathcal{R} \cup \{\mathfrak{p}, \mathfrak{q}_1\}$ and $\mathcal{R} \cup \{\mathfrak{p}, \mathfrak{q}_2\}$, respectively.

In order to prove Proposition 3.7.1 we will need the following two lemmas.

Lemma 3.7.3. *Let* $\mathcal{S}$ *be a set of prime ideals of* F *and suppose that* $e \in \mathbb{Z}$ *satisfies*

$$e \geq 2\max\{v_{\mathfrak{P}}(2) \mid \mathfrak{P} \in \mathcal{S}\} + 1.$$

Then for any prime ideal $\mathfrak{P} \in \mathcal{S}$*, if* $\alpha \in F^\times$ *and* $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$ *then* $F_{\mathfrak{P}}(\sqrt{\alpha}) = F_{\mathfrak{P}}$.

Proof. Let $\mathfrak{P} \in \mathcal{S}$. Observe that $F_{\mathfrak{P}}(\sqrt{\alpha}) = F_{\mathfrak{P}}$ if and only if α is a perfect square in $F_{\mathfrak{P}}$. Let $\mathcal{O}_{\mathfrak{P}}$ be the ring of integers of $F_{\mathfrak{P}}$ and $U^{(n)} := 1 + \mathfrak{P}^n\mathcal{O}_{\mathfrak{P}}$ be the n-th higher unit group. Let $v_{\mathfrak{P}} : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the discrete valuation given by $v_{\mathfrak{P}}(x) := \mathrm{ord}_{\mathfrak{P}}(x)$. By [Wei98, Proposition 3-1-6, p. 79], if $m, i \in \mathbb{Z}$ are integers with $m \geq 1$ and $i \geq v_{\mathfrak{P}}(m) + 1$, then the map $\phi_m : U^{(i)} \longrightarrow U^{(i+v_{\mathfrak{P}}(m))}$ given by $\phi_m(x) := x^m$ is an isomorphism. In particular, when $m = 2$ the surjectivity of the map ϕ_2 implies that every element of $U^{(i+v_{\mathfrak{P}}(2))}$ is a perfect square.

Now, let $i := \max\{v_{\mathfrak{P}}(2) \mid \mathfrak{P} \in \mathcal{S}\} + 1$. Then because $i \geq v_{\mathfrak{P}}(2) + 1$, every element of $U^{(i+v_{\mathfrak{P}}(2))}$ is a perfect square. On the other hand, if $e \in \mathbb{Z}$ satisfies

$$e \geq 2\max\{v_{\mathfrak{P}}(2) \mid \mathfrak{P} \in \mathcal{S}\} + 1,$$

then $e \geq i + v_{\mathfrak{P}}(2)$. Since the higher unit groups form a decreasing filtration, it follows that

$$U^{(e)} \subseteq U^{(i+v_{\mathfrak{P}}(2))}.$$

In particular, every element of $U^{(e)}$ is a perfect square. Finally, since $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$ implies that $\alpha \in U^{(e)}$, the proof is complete. □

Lemma 3.7.4. *For each prime ideal* $\mathfrak{P}$ *of* F*, there exists an element* $\alpha_{\mathfrak{P}} \in \mathcal{O}_F$ *such that* $F_{\mathfrak{P}}(\sqrt{\alpha_{\mathfrak{P}}})$ *is an unramified quadratic extension of* $F_{\mathfrak{P}}$.

Proof. Up to isomorphism, there is a unique unramified quadratic extension of $F_{\mathfrak{P}}$, and moreover, it can be obtained by adjoining to $F_{\mathfrak{P}}$ a lifting of a primitive element for the unique quadratic extension of the finite field

$$\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$$

(see e.g. [Chi09, Theorem 1.2.2, p. 14] or [KKS11, Proposition 6.54]). Thus, let

$$\widehat{f}(x) := x^2 + \widehat{a_1}x + \widehat{a_0} \in \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}[x]$$

be an irreducible quadratic polynomial. It is known that the homomorphism

$$\phi : \mathcal{O}_F \longrightarrow \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$$

$$\alpha \longmapsto \alpha + \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$$

has kernel $\mathfrak{P}$ and is surjective (see e.g. [Neu99, Propositions II.4.3 and II.2.4] or [FT93, Theorem 11(c)]). Thus every coset of $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$ has a representative in $\mathcal{O}_F$. Let $a_0, a_1 \in \mathcal{O}_F$ be such that $\widehat{a_0} = a_0 + \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$ and $\widehat{a_1} = a_1 + \mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. Then define the polynomial

$$f(x) := x^2 + a_1x + a_0 \in \mathcal{O}_F[x] \subset F_{\mathfrak{P}}[x].$$

It follows that $f(x)$ is irreducible in $F_{\mathfrak{P}}[x]$, and moreover by the quadratic formula its roots have the form

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}.$$

Hence by taking $\alpha_{\mathfrak{P}} := a_1^2 - 4a_0 \in \mathcal{O}_F$, we see that $F_{\mathfrak{P}}(\sqrt{\alpha_{\mathfrak{P}}})$ is an unramified quadratic extension of $F_{\mathfrak{P}}$. $\square$

Proof of Proposition 3.7.1. Define the following disjoint sets of prime ideals of F.

$$\mathcal{T}_1 := (\mathcal{U}_1 \cup \{\mathfrak{P} \subset \mathcal{O}_F \mid \mathfrak{P} \text{ divides } pm\}) \smallsetminus \{\mathfrak{p}\},$$

$$\mathcal{T}_2 := (\mathcal{U}_2 \cup \{\mathfrak{P} \subset \mathcal{O}_F \mid \mathfrak{P} \text{ divides } 2\}) \smallsetminus (\mathcal{T}_1 \cup \mathcal{R} \cup \{\mathfrak{p}\}).$$

Now, fix an integer $e \in \mathbb{Z}$ satisfying

$$e \geq 2\max\{v_{\mathfrak{P}}(2) \mid \mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2\} + 1.$$

Then by Lemma 3.7.3, for any prime ideal $\mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2$, if $\alpha \in F^\times$ and $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$ then $F_{\mathfrak{P}}(\sqrt{\alpha}) = F_{\mathfrak{P}}$. Also, as in Lemma 3.7.4, for each prime ideal $\mathfrak{P} \in \mathcal{T}_2$, let $\alpha_{\mathfrak{P}} \in \mathcal{O}_F$ be such that $F_{\mathfrak{P}}(\sqrt{\alpha_{\mathfrak{P}}})$ is an unramified quadratic extension of $F_{\mathfrak{P}}$.

Let $\mathfrak{m}_\infty$ be the formal product of all the real infinite primes corresponding to the embeddings in $\mathrm{Hom}(F, \mathbb{R})$. By an application of the Approximation Theorem (see e.g. [Jan96, pp. 137-139]), there exists an element $a \in F^\times$ satisfying the following congruences.

(1) $a \overset{\times}{\equiv} -1 \pmod{\mathfrak{m}_\infty}$.

(2) $a \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$ for every $\mathfrak{P} \in \mathcal{T}_1$.

(3) $a \overset{\times}{\equiv} \alpha_{\mathfrak{P}} \pmod{\mathfrak{P}^e}$ for every $\mathfrak{P} \in \mathcal{T}_2$.

Define the integral ideal

$$\mathfrak{m}_0 := \prod_{\mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2} \mathfrak{P}^e$$

and the modulus $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$. Let $\mathcal{R}_F(\mathfrak{m})$ be the ray class group modulo $\mathfrak{m}$. Observe that the fractional ideal

$$\mathfrak{n} := a\mathfrak{p}^{-1} \prod_{\mathfrak{r} \in \mathcal{R}} \mathfrak{r}^{-1} \tag{3.21}$$

is relatively prime to $\mathfrak{m}_0$. Then we can define the set of prime ideals

$$\mathcal{S}(\mathfrak{n}) := \{\mathfrak{q} \subset \mathcal{O}_F \mid \mathfrak{q} \text{ is a prime ideal and } [\mathfrak{q}] = [\mathfrak{n}] \text{ in } \mathcal{R}_F(\mathfrak{m})\}.$$

Also, define the set of prime ideals

$$\mathcal{S}_{\mathcal{R},\mathfrak{p}} := \mathcal{S}(\mathfrak{n}) \smallsetminus (\mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{R} \cup \{\mathfrak{p}\}).$$

To prove Proposition 3.7.1 (i), it is known that the set $\mathcal{S}(\mathfrak{n})$ has natural density

$$d(\mathcal{S}(\mathfrak{n})) := \lim_{X \to \infty} \frac{\#\{\mathfrak{q} \in \mathcal{S}(\mathfrak{n}) \mid N_{F/\mathbb{Q}}(\mathfrak{q}) \leq X\}}{\#\{\mathfrak{q} \subset \mathcal{O}_F \mid \mathfrak{q} \text{ is a prime ideal with } N_{F/\mathbb{Q}}(\mathfrak{q}) \leq X\}} = \frac{1}{\#\mathcal{R}_F(\mathfrak{m})}.$$

Since the set $\mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{R} \cup \{\mathfrak{p}\}$ is finite, we also have

$$d(\mathcal{S}_{\mathcal{R},\mathfrak{p}}) = \frac{1}{\#\mathcal{R}_F(\mathfrak{m})}.$$

To prove Proposition 3.7.1 (ii), note that if $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$ then $\mathfrak{q} \notin \mathcal{T}_1 \cup \{\mathfrak{p}\}$, hence $\mathfrak{q}$ is relatively prime to pm.

To prove Proposition 3.7.1 (iii), let $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$. Since $[\mathfrak{q}] = [\mathfrak{n}]$ in $\mathcal{R}_F(\mathfrak{m})$, there exists an element $b_\mathfrak{q} \in F^\times$ such that

(4) $b_\mathfrak{q} \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$ and $\mathfrak{q} = b_\mathfrak{q}\mathfrak{n}$.

By (3.21) and (4) we have

$$\mathfrak{q} = ab_\mathfrak{q}\mathfrak{p}^{-1} \prod_{\mathfrak{r}\in\mathcal{R}} \mathfrak{r}^{-1}.$$

Define $\Delta_\mathfrak{q} := ab_\mathfrak{q}$. Then

$$\Delta_\mathfrak{q}\mathcal{O}_F = ab_\mathfrak{q}\mathcal{O}_F = \mathfrak{p}\mathfrak{q} \prod_{\mathfrak{r}\in\mathcal{R}} \mathfrak{r}. \tag{3.22}$$

Note that this also proves that $\Delta_\mathfrak{q} \in \mathcal{O}_F$.

Finally, define the field $E_\mathfrak{q} := F(\sqrt{\Delta_\mathfrak{q}})$. Then Proposition 3.7.1 (iv) is a consequence of the following lemma.

Lemma 3.7.5. *Let $a \in F^\times$ be an element satisfying $(1)-(3)$ and $b_\mathfrak{q} \in F^\times$ be an element satisfying (4). Let $\Delta_\mathfrak{q} := ab_\mathfrak{q} \in \mathcal{O}_F$. Then the field $E_\mathfrak{q} := F(\sqrt{\Delta_\mathfrak{q}})$ is a CM extension of F which satisfies the following properties.*

(i) $E_\mathfrak{q}$ is ramified only at the prime ideals of F dividing $\Delta_\mathfrak{q}$.

(ii) Each prime ideal in $\mathcal{U}_1$ splits in $E_\mathfrak{q}$ and each prime ideal in $\mathcal{U}_2$ is inert in $E_\mathfrak{q}$.

Proof. Since the prime ideals $\mathfrak{p}, \mathfrak{q}$ and $\mathfrak{r} \in \mathcal{R}$ are all distinct, the identity (3.22) shows that $\Delta_\mathfrak{q}$ is not a perfect square in F. Also, by (1) and (4) we have $\Delta_\mathfrak{q} = ab_\mathfrak{q} \overset{\times}{\equiv} -1 \pmod{\mathfrak{m}_\infty}$, or equivalently $\Delta_\mathfrak{q} \ll 0$. These facts imply that $E_\mathfrak{q}$ is a totally imaginary quadratic extension of F, hence a CM field.

Now, since $\Delta_{\mathfrak{q}} \in \mathcal{O}_F$ we have $\sqrt{\Delta_{\mathfrak{q}}} \in \mathcal{O}_{E_{\mathfrak{q}}}$. Then by (3.22) we have

$$\mathfrak{p}\mathcal{O}_{E_{\mathfrak{q}}}\mathfrak{q}\mathcal{O}_{E_{\mathfrak{q}}}\prod_{\mathfrak{r}\in\mathcal{R}}\mathfrak{r}\mathcal{O}_{E_{\mathfrak{q}}} = \Delta_{\mathfrak{q}}\mathcal{O}_{E_{\mathfrak{q}}} = \left(\sqrt{\Delta_{\mathfrak{q}}}\mathcal{O}_{E_{\mathfrak{q}}}\right)^2.$$

This implies that each of the prime ideals of F dividing $\Delta_{\mathfrak{q}}$ is ramified in $E_{\mathfrak{q}}$. Thus, to prove (i), it remains to show that if $\mathfrak{P}$ is a prime ideal of F not dividing $\Delta_{\mathfrak{q}}$, then $\mathfrak{P}$ is unramified in $E_{\mathfrak{q}}$.

It is known that if K is a number field and α is a root of the polynomial

$$f(x) := x^2 - \beta \in \mathcal{O}_K[x],$$

then any nonzero prime ideal $\mathfrak{P}$ of K such that $\mathfrak{P}$ does not divide 2β is unramified in $L := K(\alpha)$ (see e.g. [KKS11, Example 6.40, p. 59]). Therefore if $\mathfrak{P}$ is a prime ideal of F such that $\mathfrak{P}$ does not divide $2\Delta_{\mathfrak{q}}$, then $\mathfrak{P}$ is unramified in $E_{\mathfrak{q}}$. Thus it suffices to prove that if $\mathfrak{P}$ is a prime ideal of F such that $\mathfrak{P}$ divides 2 and $\mathfrak{P}$ does not divide $\Delta_{\mathfrak{q}}$, then $\mathfrak{P}$ is unramified in $E_{\mathfrak{q}}$.

By (3.22) we know that the prime ideals of F that divide $\Delta_{\mathfrak{q}}$ are the primes in the set $\mathcal{R}\cup\{\mathfrak{p},\mathfrak{q}\}$. Therefore from the definitions of $\mathcal{T}_1$ and $\mathcal{T}_2$ we see that the set of prime ideals $\mathfrak{P}$ of F such that $\mathfrak{P}$ divides 2 and $\mathfrak{P} \notin \mathcal{R} \cup \{\mathfrak{p},\mathfrak{q}\}$ is a subset of $\mathcal{T}_1 \cup \mathcal{T}_2$. Hence, in the remainder of the proof we will show that the prime ideals in $\mathcal{T}_1 \cup \mathcal{T}_2$ are unramified in $E_{\mathfrak{q}}$. In fact, we will show that the prime ideals in $\mathcal{T}_1$ split in $E_{\mathfrak{q}}$ and the prime ideals in $\mathcal{T}_2$ remain inert in $E_{\mathfrak{q}}$. Since $\mathcal{U}_1 \subset \mathcal{T}_1$ and $\mathcal{U}_2 \subset \mathcal{T}_2$, this will also complete the proof of (ii).

Thus let $\mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2$ and let $\mathfrak{Q}$ be a prime ideal of $E_{\mathfrak{q}}$ lying above $\mathfrak{P}$. Also, let $\widehat{\mathfrak{P}}$ and $\widehat{\mathfrak{Q}}$ denote the unique prime ideals in the completions $F_{\mathfrak{P}}$ and $E_{\mathfrak{q},\mathfrak{Q}}$, respectively. It is known that the ramification indices are the same, i.e., we have

$$e(\mathfrak{Q}|\mathfrak{P}) = e(\widehat{\mathfrak{Q}}|\widehat{\mathfrak{P}}).$$

We will show that $e(\mathfrak{Q}|\mathfrak{P}) = e(\widehat{\mathfrak{Q}}|\widehat{\mathfrak{P}}) = 1$.

The minimal polynomial of the primitive element $\sqrt{\Delta_{\mathfrak{q}}}$ of $E_{\mathfrak{q}}$ over F is

$$m_{\Delta_{\mathfrak{q}}}(x) := x^2 - \Delta_{\mathfrak{q}} \in \mathcal{O}_F[x].$$

It is known that the primes of $E_{\mathfrak{q}}$ lying above $\mathfrak{P}$ are in one to one correspondence with the irreducible factors of $m_{\Delta_{\mathfrak{q}}}(x)$ when considered as a polynomial in $F_{\mathfrak{P}}[x]$ and moreover, if $\mathfrak{Q}$ corresponds to an irreducible factor $m_i(x)$, then the completion of $E_{\mathfrak{q}}$ at $\mathfrak{Q}$ satisfies

$$E_{\mathfrak{q},\mathfrak{Q}} \cong \frac{F_{\mathfrak{P}}[x]}{\langle m_i(x) \rangle}$$

(see for example [Jan96, Theorem II.6.1, p. 115]).

We have two cases to consider.

Case 1: $\mathfrak{P} \in \mathcal{T}_1$. In this case the congruences (2) and (4) satisfied by a and $b_{\mathfrak{q}}$ imply that $\Delta_{\mathfrak{q}} = ab_{\mathfrak{q}} \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$. Hence by Lemma 3.7.3 we conclude that $F_{\mathfrak{P}}(\sqrt{\Delta_{\mathfrak{q}}}) = F_{\mathfrak{P}}$. This implies that there is an element $c \in F_{\mathfrak{P}}$ such that $\Delta_{\mathfrak{q}} = c^2$. Therefore the polynomial $m_{\Delta_{\mathfrak{q}}}(x)$ factors as

$$m_{\Delta_{\mathfrak{q}}}(x) = x^2 - c^2 = (x-c)(x+c)$$

in $F_{\mathfrak{P}}[x]$. Since the prime ideals of $E_{\mathfrak{q}}$ lying over $\mathfrak{P}$ are in one to one correspondence with the irreducible factors $x-c$ and $x+c$, and since $E_{\mathfrak{q}}/F$ is a quadratic extension, we see that $\mathfrak{P}$ splits in $E_{\mathfrak{q}}$, so that $e(\mathfrak{Q}|\mathfrak{P}) = 1$.

Case 2: $\mathfrak{P} \in \mathcal{T}_2$. In this case the congruences (3) and (4) satisfied by a and $b_{\mathfrak{q}}$ imply that $\Delta_{\mathfrak{q}} = ab_{\mathfrak{q}} \overset{\times}{\equiv} \alpha_{\mathfrak{P}} \pmod{\mathfrak{P}^e}$, or equivalently,

$$\frac{\Delta_{\mathfrak{q}}}{\alpha_{\mathfrak{P}}} \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}.$$

Hence by Lemma 3.7.3, we have $\Delta_{\mathfrak{q}} = c^2\alpha_{\mathfrak{P}}$ for some $c \in F_{\mathfrak{P}}^{\times}$, which implies that

$$F_{\mathfrak{P}}(\sqrt{\Delta_{\mathfrak{q}}}) = F_{\mathfrak{P}}(\sqrt{\alpha_{\mathfrak{P}}}).$$

On the other hand, by Lemma 3.7.4 we have that $F_{\mathfrak{P}}(\sqrt{\alpha_{\mathfrak{P}}})$ is an unramified quadratic extension of $F_{\mathfrak{P}}$. It follows that $m_{\Delta_{\mathfrak{q}}}(x)$ is irreducible in $F_{\mathfrak{P}}[x]$. Thus $\mathfrak{Q}$ is the only prime ideal of $E_{\mathfrak{q}}$ lying above $\mathfrak{P}$ and it corresponds to $m_{\Delta_{\mathfrak{q}}}(x) = x^2 - \Delta_{\mathfrak{q}}$. Therefore we have

$$E_{\mathfrak{q},\mathfrak{Q}} \cong \frac{F_{\mathfrak{P}}[x]}{\langle m_{\Delta_{\mathfrak{q}}}(x) \rangle} \cong F_{\mathfrak{P}}(\sqrt{\Delta_{\mathfrak{q}}}).$$

This implies that $E_{\mathfrak{q},\mathfrak{Q}}$ is an unramified quadratic extension of $F_{\mathfrak{P}}$, hence $e(\widehat{\mathfrak{Q}}|\widehat{\mathfrak{P}}) = 1$. Therefore $e(\mathfrak{Q}|\mathfrak{P}) = 1$, and in particular $\mathfrak{P}$ remains inert in $E_{\mathfrak{q}}$. □

This completes the proof of Proposition 3.7.1. □

3.7.3 *Constructing non-abelian CM fields with reflex fields of maximal degree*

In the following theorem we prove that if E/F is a CM extension satisfying a certain mild ramification condition, then the reflex fields E_Φ have maximal degree, and moreover, if $n \geq 3$ then $E/\mathbb{Q}$ is non-Galois.

Theorem 3.7.6. *Let F be a totally real number field of degree n. Let $p \in \mathbb{Z}$ be a prime number that splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let d_{F^s} be the discriminant of F^s and $\mathcal{L}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Then if E/F is a CM extension which is ramified only at the prime ideals of F in the set $\mathcal{L} \cup \{\mathfrak{p}\}$, the reflex degree $[E_\Phi : \mathbb{Q}] = 2^n$ for every CM type $\Phi \in \Phi(E)$. Moreover, if $n \geq 3$ then $E/\mathbb{Q}$ is non-Galois (hence non-abelian).*

We will prove Theorem 3.7.6 using a sequence of five lemmas which are now proved in succession.

Lemma 3.7.7. *Let F be a totally real number field of degree n. Let E/F be a CM extension and $\Phi = \{\sigma_1, \ldots, \sigma_n\} \in \Phi(E)$ be a CM type for E. Let E_Φ be the reflex field of the CM pair (E, Φ). Then*

$$E_\Phi F^s = E^{\sigma_1} \cdots E^{\sigma_n} = E^s.$$

Proof. We first prove that

$$E^{\sigma_1} \cdots E^{\sigma_n} \subseteq E_\Phi F^s.$$

It suffices to show that $\sigma_j(c) \in E_\Phi F^s$ for all $c \in E$ and $j = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for F. By Proposition 3.6.1 (ii), the reflex field of the CM pair (E, Φ) is given by

$$E_\Phi = \mathbb{Q}\left(\{\mathrm{Tr}_\Phi(a) \mid a \in E\}\right),$$

where $\mathrm{Tr}_\Phi(a) = \sum_{j=1}^{n} \sigma_j(a)$. Then for all $c \in E$ and $i = 1, \ldots, n$, we have

$$\mathrm{Tr}_\Phi(c\alpha_i) = \sum_{j=1}^{n} \sigma_j(c\alpha_i) = \sum_{j=1}^{n} \sigma_j(\alpha_i)\sigma_j(c) \in E_\Phi.$$

In particular, there are elements $\beta_i \in E_\Phi$ such that

$$\sum_{j=1}^{n} \sigma_j(\alpha_i)\sigma_j(c) = \beta_i$$

for $i = 1, \ldots, n$. This yields the linear system

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} \sigma_1(c) \\ \sigma_2(c) \\ \vdots \\ \sigma_n(c) \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}.$$

The matrix $[\sigma_j(\alpha_i)] \in M^{n\times n}(F^s)$, and it is invertible since $\det[\sigma_j(\alpha_i)]^2 = d_F \neq 0$. It follows from Cramer's rule that

$$\sigma_j(c) = \frac{\det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{j-1}(\alpha_1) & \beta_1 & \sigma_{j+1}(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{j-1}(\alpha_n) & \beta_n & \sigma_{j+1}(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}}{\det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}} \tag{3.23}$$

for $j = 1, \ldots, n$. Since $\sigma_j(\alpha_i) \in F^s$ and $\beta_i \in E_\Phi$ for $i, j = 1, \ldots, n$, the denominator in (3.23) is in F^s and the numerator is in $E_\Phi F^s$. Therefore, $\sigma_j(c) \in E_\Phi F^s$ for all $c \in E$ and $j = 1, \ldots, n$, which implies that

$$E^{\sigma_1} \cdots E^{\sigma_n} \subseteq E_\Phi F^s.$$

On the other hand, since the compositum of all the conjugate fields of a number field is equal to its Galois closure, and since complex conjugation is an automorphism of E that commutes with every embedding (see [Shi94, Proposition 5.11]), we have $E^{\sigma_1} \cdots E^{\sigma_n} = E^s$. Therefore, since $E_\Phi F^s \subseteq E^s$, we conclude that

$$E_\Phi F^s = E^{\sigma_1} \cdots E^{\sigma_n} = E^s.$$

□

Lemma 3.7.8. *Let F be a totally real number field of degree n. Let $p \in \mathbb{Z}$ be a prime number that splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let E/F be a CM extension and $\Phi = \{\sigma_1, \dots, \sigma_n\} \in \Phi(E)$ be a CM type for E. Then the ideals $\mathfrak{p}^{\sigma_1}\mathcal{O}_{F^s}, \dots, \mathfrak{p}^{\sigma_n}\mathcal{O}_{F^s}$ are pairwise relatively prime.*

Proof. Suppose that $\mathfrak{P}$ is a prime of F^s lying above $\mathfrak{p}$. Thus $\mathfrak{P}$ also lies above $p \in \mathbb{Z}$. Since $F^s/\mathbb{Q}$ is Galois, we have

$$p\mathcal{O}_{F^s} = \prod_{\sigma \in \mathrm{Gal}(F^s/\mathbb{Q})} \sigma(\mathfrak{P}). \tag{3.24}$$

Moreover, since p splits in F^s, then $\sigma(\mathfrak{P}) \neq \tau(\mathfrak{P})$ for any $\sigma, \tau \in \mathrm{Gal}(F^s/\mathbb{Q})$ with $\sigma \neq \tau$.

Now, let $G_i := \mathrm{Gal}(F^s/F^{\sigma_i})$ for $i = 1, \dots, n$. For each $i = 1, \dots, n$ we have that $\mathfrak{p}^{\sigma_i}$ is a prime ideal of F^{σ_i} lying above p. Hence $\mathfrak{p}^{\sigma_i}$ also splits in F^s. Let $\widetilde{\sigma_i} \in \mathrm{Gal}(F^s/\mathbb{Q})$ be an extension of the embedding $\sigma_i|_F : F \hookrightarrow F^s$, i.e. $\widetilde{\sigma_i}|_F = \sigma_i|_F$. It follows that $\widetilde{\sigma_i}(\mathfrak{P})$ lies above $\mathfrak{p}^{\sigma_i}$, and since the extension F^s/F^{σ_i} is Galois, we have

$$\mathfrak{p}^{\sigma_i}\mathcal{O}_{F^s} = \prod_{\sigma \in G_i} \sigma(\widetilde{\sigma_i}(\mathfrak{P})) = \prod_{\tau \in G_i\widetilde{\sigma_i}} \tau(\mathfrak{P}).$$

Since $G_i\widetilde{\sigma_i} \subseteq \mathrm{Gal}(F^s/\mathbb{Q})$ for $i = 1, \dots, n$ and $\sigma(\mathfrak{P}) \neq \tau(\mathfrak{P})$ for any $\sigma, \tau \in \mathrm{Gal}(F^s/\mathbb{Q})$ with $\sigma \neq \tau$, it suffices to prove that $G_i\widetilde{\sigma_i} \cap G_j\widetilde{\sigma_j} = \varnothing$ for $i \neq j$.

Suppose by contradiction that there exists an element $\sigma \in G_i\widetilde{\sigma_i} \cap G_j\widetilde{\sigma_j}$ for $i \neq j$. Then there are elements $\tau_i \in G_i$ and $\tau_j \in G_j$ such that $\sigma = \tau_i\widetilde{\sigma_i}$ and $\sigma = \tau_j\widetilde{\sigma_j}$. Since $\{\sigma_1, \dots, \sigma_n\}$ is a CM type for E, then $\mathrm{Hom}(F, \overline{\mathbb{Q}}) = \{\sigma_1|_F, \dots, \sigma_n|_F\}$ and therefore the embeddings $\sigma_i|_F$ and $\sigma_j|_F$ are different. Hence there is an element $x \in F$ such that $\sigma_i(x) \neq \sigma_j(x)$. Since $\sigma_i(x) \in F^{\sigma_i}$ and $\tau_i|_{F^{\sigma_i}} = \mathrm{id}_{F^{\sigma_i}}$, it follows that

$$\sigma_i(x) = \widetilde{\sigma_i}(x) = \tau_i(\widetilde{\sigma_i}(x)) = \tau_j(\widetilde{\sigma_j}(x)) = \widetilde{\sigma_j}(x) = \sigma_j(x),$$

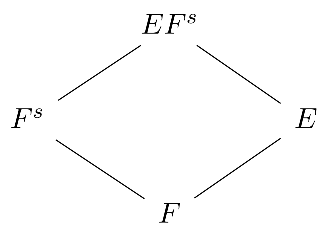
which is a contradiction. Thus for $i \neq j$, we have $G_i\widetilde{\sigma_i} \cap G_j\widetilde{\sigma_j} = \varnothing$, which shows that the ideals $\mathfrak{p}^{\sigma_i}\mathcal{O}_F^s$ and $\mathfrak{p}^{\sigma_i}\mathcal{O}_F^s$ are relatively prime. □

For an extension of number fields L/K, let $\mathfrak{D}(L/K)$ be the relative different, which is an integral ideal of L.

Lemma 3.7.9. *Let F be a totally real number field. Let $p \in \mathbb{Z}$ be a prime number that splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let $\mathcal{L}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Let E/F be a CM extension which is ramified only at the prime ideals of F in the set $\mathcal{L} \cup \{\mathfrak{p}\}$. Then*

$$\mathfrak{D}(EF^s/F^s) = \mathfrak{D}(E/F)\mathcal{O}_{EF^s}.$$

Proof. We have the following towers of fields.



Since the relative different is multiplicative in towers, we have the identity

$$\mathfrak{D}(EF^s/F^s)\mathfrak{D}(F^s/F) = \mathfrak{D}(EF^s/E)\mathfrak{D}(E/F). \tag{3.25}$$

We will prove that $\mathfrak{D}(EF^s/F^s)$ and $\mathfrak{D}(EF^s/E)$ are relatively prime, and that $\mathfrak{D}(F^s/F)$ and $\mathfrak{D}(E/F)$ are relatively prime as ideals in $\mathcal{O}_{EF^s}$. Then (3.25) would imply that

$$\mathfrak{D}(EF^s/F^s) = \mathfrak{D}(E/F)\mathcal{O}_{EF^s}. \tag{3.26}$$

First, we prove that $\mathfrak{D}(F^s/F)$ and $\mathfrak{D}(E/F)$ are relatively prime as ideals in $\mathcal{O}_{EF^s}$. To see this, suppose by contradiction that there is a prime ideal $\mathfrak{P}_{EF^s}$ of $\mathcal{O}_{EF^s}$ such that

$$\mathfrak{P}_{EF^s}|\mathfrak{D}(F^s/F)\mathcal{O}_{EF^s} \quad \text{and} \quad \mathfrak{P}_{EF^s}|\mathfrak{D}(E/F)\mathcal{O}_{EF^s}.$$

Define the prime ideals $\mathfrak{P}_F := \mathfrak{P}_{EF^s} \cap \mathcal{O}_F$, $\mathfrak{P}_{F^s} := \mathfrak{P}_{EF^s} \cap \mathcal{O}_{F^s}$ and $\mathfrak{P}_E := \mathfrak{P}_{EF^s} \cap \mathcal{O}_E$. Then $\mathfrak{P}_{F^s}$ is a prime in F^s that divides $\mathfrak{D}(F^s/F)$ and hence $\mathfrak{P}_F = \mathfrak{P}_{F^s} \cap \mathcal{O}_F$ ramifies in the extension F^s/F. Similarly, $\mathfrak{P}_E$ is a prime ideal of E that divides $\mathfrak{D}(E/F)$ and hence $\mathfrak{P}_F = \mathfrak{P}_E \cap \mathcal{O}_F$ ramifies in the extension E/F.

Now, since the only primes of F that ramify in E are the primes in the set $\mathcal{L} \cup \{\mathfrak{p}\}$, it follows that $\mathfrak{P}_F = \mathfrak{p}$ or $\mathfrak{P}_F = \mathfrak{l}$ for some $\mathfrak{l} \in \mathcal{L}$. We will see now that each of these two possibilities leads to a contradiction. If $\mathfrak{P}_F = \mathfrak{p}$, then $\mathfrak{p}$ would be ramified in F^s. But this would contradict the fact that p splits in F^s, since $\mathfrak{p}$ lies above p. On the other hand, if $\mathfrak{P}_F = \mathfrak{l}$ for some $\mathfrak{l} \in \mathcal{L}$, then $\mathfrak{l}$ would be ramified in F^s. Hence the rational prime ℓ such that $\ell\mathbb{Z} = \mathfrak{l} \cap \mathbb{Z}$ would be ramified in F^s, which implies that ℓ divides d_{F^s} and hence that $\mathfrak{l}$ divides d_{F^s}. However, this is a contradiction since we assumed that the prime ideals in the set $\mathcal{L}$ do not divide pd_{F^s}. Thus $\mathfrak{D}(F^s/F)$ and $\mathfrak{D}(E/F)$ are relatively prime as ideals in $\mathcal{O}_{EF^s}$, as claimed.

Next, we prove that $\mathfrak{D}(EF^s/F^s)$ and $\mathfrak{D}(EF^s/E)$ are relatively prime. By [Rib01, Section 13.2, **U**. (1), p. 253], we have that $\mathfrak{D}(EF^s/F^s)$ divides $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$ and $\mathfrak{D}(EF^s/E)$ divides $\mathfrak{D}(F^s/F)\mathcal{O}_{EF^s}$. Since we proved that the ideals $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$ and $\mathfrak{D}(F^s/F)\mathcal{O}_{EF^s}$ are relatively prime, it follows that $\mathfrak{D}(EF^s/F^s)$ and $\mathfrak{D}(EF^s/E)$ are relatively prime. This completes the proof of the lemma.

□

For an extension of number fields L/K, let $\mathfrak{d}(L/K)$ be the relative discriminant, which is an integral ideal of K.

Lemma 3.7.10. *Let F be a totally real number field of degree n. Let $p \in \mathbb{Z}$ be a prime number that splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let $\mathcal{L}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Let E/F be a CM extension which is ramified only at the prime ideals of F in the set $\mathcal{L} \cup \{\mathfrak{p}\}$. Let $\Phi = \{\sigma_1, \dots, \sigma_n\} \in \Phi(E)$ be a CM type for E. Then the relative discriminant $\mathfrak{d}(E^{\sigma_i}F^s/F^s)$ is divisible by $\mathfrak{p}^{\sigma_i}\mathcal{O}_{F^s}$, but relatively prime to $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ for $j \neq i$.*

Proof. We first prove the following claim.

Claim. *The relative different $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$ is divisible by the primes of EF^s lying above the primes in the set $\mathcal{L} \cup \{\mathfrak{p}\}$, and by no other primes of EF^s.*

Proof of the Claim. Since the primes in the set $\mathcal{L} \cup \{\mathfrak{p}\}$ are the only primes of F which ramify in E, we have

$$\mathfrak{d}(E/F) = \mathfrak{p}^{a_\mathfrak{p}} \prod_{\mathfrak{l} \in \mathcal{L}} \mathfrak{l}^{a_\mathfrak{l}}$$

for some positive integers $a_\mathfrak{p}$ and $a_\mathfrak{l}$ for $\mathfrak{l} \in \mathcal{L}$. Moreover, since E/F is quadratic, there is a prime ideal $\mathfrak{P}$ of E such that $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}^2$ and a set of prime ideals $\{\mathfrak{P}_\mathfrak{l} \mid \mathfrak{l} \in \mathcal{L}\}$ of E such that $\mathfrak{l}\mathcal{O}_E = \mathfrak{P}_\mathfrak{l}^2$ for each $\mathfrak{l} \in \mathcal{L}$. Therefore, the relative different factors as

$$\mathfrak{D}(E/F) = \mathfrak{P}^{u_\mathfrak{P}} \prod_{\mathfrak{l}\in\mathcal{L}} \mathfrak{P}_\mathfrak{l}^{u_\mathfrak{l}}$$

for some positive integers $u_\mathfrak{P}$ and $u_\mathfrak{l}$ for $\mathfrak{l} \in \mathcal{L}$. By extending the relative different to EF^s, we see that $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$ is divisible by the primes of EF^s lying above the primes in the set $\{\mathfrak{P}\} \cup \{\mathfrak{P}_\mathfrak{l} \mid \mathfrak{l} \in \mathcal{L}\}$, and by no other primes of EF^s. It follows that $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$ is divisible by the primes of EF^s lying above the primes in the set $\mathcal{L} \cup \{\mathfrak{p}\}$, and by no other primes of EF^s. This completes the proof of the claim. □

Now, since p splits in F^s, then $\mathfrak{p}$ splits in F^s. Hence

$$\mathfrak{p}\mathcal{O}_{F^s} = \mathfrak{p}_1 \cdots \mathfrak{p}_g, \tag{3.27}$$

where $g = [F^s : F]$ and the $\mathfrak{p}_k$ are distinct prime ideals of F^s. For $k = 1, \ldots, g$, we have

$$\mathfrak{p}_k\mathcal{O}_{EF^s} = \prod_{t=1}^{a_k} \mathfrak{P}_{k,t}^{b_{k,t}}$$

for distinct prime ideals $\mathfrak{P}_{k,t}$ of EF^s and some positive integers a_k and $b_{k,t}$. Thus

$$\mathfrak{p}\mathcal{O}_{EF^s} = \prod_{k=1}^{g}\prod_{t=1}^{a_k} \mathfrak{P}_{k,t}^{b_{k,t}}.$$

The prime ideals $\mathfrak{P}_{k,t}$ are the primes of EF^s lying above $\mathfrak{p}$. Hence by the Claim, we see that $\mathfrak{P}_{k,t}$ divides $\mathfrak{D}(E/F)\mathcal{O}_{EF^s}$. However, by Lemma 3.7.9,

$$\mathfrak{D}(EF^s/F^s) = \mathfrak{D}(E/F)\mathcal{O}_{EF^s}, \tag{3.28}$$

hence $\mathfrak{P}_{k,t}$ divides $\mathfrak{D}(EF^s/F^s)$. It follows that $\mathfrak{p}_k = \mathfrak{P}_{k,t} \cap \mathcal{O}_{F^s}$ divides $\mathfrak{d}(EF^s/F^s)$ for $k = 1, \ldots, g$.

Similarly, for a prime ideal $\mathfrak{l} \in \mathcal{L}$, starting with the factorization

$$\mathfrak{l}\mathcal{O}_{F^s} = \mathfrak{P}_{\mathfrak{l},1}^{r(\mathfrak{l},1)} \cdots \mathfrak{P}_{\mathfrak{l},g_\mathfrak{l}}^{r(\mathfrak{l},g_\mathfrak{l})}$$

for distinct prime ideals $\mathfrak{P}_{\mathfrak{l},k}$ of F^s and some positive integers $r(\mathfrak{l}, k)$ for $k = 1, \ldots, g_\mathfrak{l}$, an analogous argument shows that $\mathfrak{P}_{\mathfrak{l},k}$ divides $\mathfrak{d}(EF^s/F^s)$ for $k = 1, \ldots, g_\mathfrak{l}$.

By the Claim and the identity (3.28), the primes of EF^s lying above the primes in the set

$$\{\mathfrak{p}_k \mid k = 1, \ldots, g\} \cup \bigcup_{\mathfrak{l} \in \mathcal{L}} \{\mathfrak{P}_{\mathfrak{l},k} \mid k = 1, \ldots, g_{\mathfrak{l}}\}$$

are the only primes of EF^s which divide $\mathfrak{D}(EF^s/F^s)$. Hence, the relative discriminant factors as

$$\mathfrak{d}(EF^s/F^s) = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_g^{c_g} \prod_{\mathfrak{l} \in \mathcal{L}} \prod_{k=1}^{g_{\mathfrak{l}}} \mathfrak{P}_{\mathfrak{l},k}^{d(\mathfrak{l},k)} \tag{3.29}$$

for some positive integers $c_1, \ldots, c_g$ and $d(\mathfrak{l}, k)$ for $\mathfrak{l} \in \mathcal{L}$ and $k = 1, \ldots, g_{\mathfrak{l}}$.

Now, for each embedding $\sigma_i \in \Phi$, let $\widetilde{\sigma_i}$ be an extension of σ_i to EF^s. Then since $F^s/\mathbb{Q}$ is Galois, we have $\widetilde{\sigma_i}(F^s) = F^s$, and therefore conjugating by $\widetilde{\sigma_i}$ in equation (3.29) yields

$$\mathfrak{d}(E^{\sigma_i}F^s/F^s) = \widetilde{\sigma_i}(\mathfrak{p}_1)^{c_1} \cdots \widetilde{\sigma_i}(\mathfrak{p}_g)^{c_g} \prod_{\mathfrak{l} \in \mathcal{L}} \prod_{k=1}^{g_{\mathfrak{l}}} \widetilde{\sigma_i}\left(\mathfrak{P}_{\mathfrak{l},k}\right)^{d(\mathfrak{l},k)}. \tag{3.30}$$

It follows from (3.27) and (3.30) that

$$\mathfrak{p}^{\sigma_i}\mathcal{O}_{F^s} = \widetilde{\sigma_i}(\mathfrak{p}_1) \cdots \widetilde{\sigma_i}(\mathfrak{p}_g) \tag{3.31}$$

divides $\mathfrak{d}(E^{\sigma_i}F^s/F^s)$. This proves the first part of the lemma.

It remains to prove that $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ is relatively prime to $\mathfrak{d}(E^{\sigma_i}F^s/F^s)$ for $j \neq i$. By Lemma 3.7.8, the ideal $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ is relatively prime to $\mathfrak{p}^{\sigma_i}\mathcal{O}_{F^s}$ for $j \neq i$, and hence relatively prime to $\widetilde{\sigma_i}(\mathfrak{p}_1)^{c_1} \cdots \widetilde{\sigma_i}(\mathfrak{p}_g)^{c_g}$ by equation (3.31). Thus, by (3.30) it suffices to prove that $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ is relatively prime to $\widetilde{\sigma_i}\left(\mathfrak{P}_{\mathfrak{l},k}\right)$ for each $\mathfrak{l} \in \mathcal{L}$ and $k = 1, \ldots, g_{\mathfrak{l}}$. To see this, recall that the prime ideal $\mathfrak{l}$ does not divide pd_{F^s}, hence $\mathfrak{l}$ lies above a rational prime $\ell \in \mathbb{Z}$ with $\ell \neq p$. Since $\widetilde{\sigma_i}\left(\mathfrak{P}_{\mathfrak{l},k}\right)$ lies above ℓ, and each of the prime factors of $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ lies above p, it follows that $\mathfrak{p}^{\sigma_j}\mathcal{O}_{F^s}$ must be relatively prime to $\widetilde{\sigma_i}\left(\mathfrak{P}_{\mathfrak{l},k}\right)$. This proves the second part of the lemma. □

Lemma 3.7.11. *Let F be a totally real number field of degree n. Let $p \in \mathbb{Z}$ be a prime number that splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let $\mathcal{L}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Let E/F be a CM extension which is ramified only at the prime ideals of F in the set $\mathcal{L} \cup \{\mathfrak{p}\}$. Let $\Phi = \{\sigma_1, \ldots, \sigma_n\} \in \Phi(E)$ be a CM type for E and E_Φ be the reflex field of the CM pair (E, Φ). Then $[E_\Phi F^s : F^s] = 2^n$ and $[E^s : \mathbb{Q}] = 2^n[F^s : \mathbb{Q}]$.*

Proof. By Lemma 3.7.7 we have $E_\Phi F^s = E^{\sigma_1} \cdots E^{\sigma_n} F^s = E^s$. Hence, to prove that $[E_\Phi F^s :$

$F^s] = 2^n$, we will show that in the tower of extensions

$$F^s \subseteq E^{\sigma_1}F^s \subseteq E^{\sigma_1}E^{\sigma_2}F^s \subseteq \cdots \subseteq E^{\sigma_1}\cdots E^{\sigma_n}F^s,$$

each successive extension

$$\begin{array}{c} E^{\sigma_1}\cdots E^{\sigma_{i-1}}E^{\sigma_i}F^s \\ \Big| \\ E^{\sigma_1}\cdots E^{\sigma_{i-1}}F^s \end{array}$$

is quadratic. First, observe that there is an element $\Delta \in \mathcal{O}_F$ with $\Delta \ll 0$ and $E = F(\sqrt{\Delta})$. Therefore $E^{\sigma_i}F^s = F^s(\sqrt{\sigma_i(\Delta)})$, and hence for each $i = 1, \ldots, n$ we have

$$E^{\sigma_1}\cdots E^{\sigma_i}F^s = F^s(\sqrt{\sigma_1(\Delta)}, \ldots, \sqrt{\sigma_i(\Delta)}).$$

This implies that

$$[E^{\sigma_1}\cdots E^{\sigma_{i-1}}E^{\sigma_i}F^s : E^{\sigma_1}\cdots E^{\sigma_{i-1}}F^s] \leq 2.$$

Now, for each $i = 1, \ldots, n$, let $\mathfrak{p}_i$ be a prime ideal of F^s dividing the ideal $\mathfrak{p}^{\sigma_i}\mathcal{O}_{F^s}$. Then for $i \neq j$, Lemma 3.7.8 implies that $\mathfrak{p}_i \neq \mathfrak{p}_j$, and moreover, by Lemma 3.7.10, the relative discriminant $\mathfrak{d}(E^{\sigma_i}F^s/F^s)$ is divisible by $\mathfrak{p}_i$, but not by $\mathfrak{p}_j$. This implies that $\mathfrak{p}_i$ is ramified in $E^{\sigma_i}F^s$, but $\mathfrak{p}_j$ is unramified in $E^{\sigma_i}F^s$.

By the preceding paragraph, for each $i = 1, \ldots, n$, the prime ideal $\mathfrak{p}_i$ is unramified in the extensions $E^{\sigma_1}F^s, \ldots, E^{\sigma_{i-1}}F^s$. Now, it is known that if a prime ideal of a number field M is unramified in the extensions K/M and L/M, then it is unramified in their compositum KL/M (see e.g [Koc00, Proposition 4.9.2]). Therefore, it follows that $\mathfrak{p}_i$ is unramified in the compositum $E^{\sigma_1}\cdots E^{\sigma_{i-1}}F^s$. On the other hand, since $\mathfrak{p}_i$ is ramified in $E^{\sigma_i}F^s/F^s$, it is ramified in $E^{\sigma_1}\cdots E^{\sigma_{i-1}}E^{\sigma_i}F^s/F^s$.

Let $\mathfrak{P}$ be a ramified prime ideal of $E^{\sigma_1}\cdots E^{\sigma_{i-1}}E^{\sigma_i}F^s$ lying above $\mathfrak{p}_i$. Then $\mathfrak{Q} := \mathfrak{P} \cap \mathcal{O}_{E^{\sigma_1}\cdots E^{\sigma_{i-1}}F^s}$ is an unramified prime ideal of $E^{\sigma_1}\cdots E^{\sigma_{i-1}}F^s$ lying above $\mathfrak{p}_i$. In terms of ramification indices, we have $e(\mathfrak{P}|\mathfrak{p}_i) \geq 2$ and $e(\mathfrak{Q}|\mathfrak{p}_i) = 1$. Then by multiplicativity of the ramification index, we have

$$e(\mathfrak{P}|\mathfrak{p}_i) = e(\mathfrak{P}|\mathfrak{Q})e(\mathfrak{Q}|\mathfrak{p}_i) = e(\mathfrak{P}|\mathfrak{Q}).$$

Hence

$$[E^{\sigma_1} \cdots E^{\sigma_{i-1}} E^{\sigma_i} F^s : E^{\sigma_1} \cdots E^{\sigma_{i-1}} F^s] \geq e(\mathfrak{P}|\mathfrak{Q}) = e(\mathfrak{P}|\mathfrak{p}_i) \geq 2.$$

We conclude that

$$[E^{\sigma_1} \cdots E^{\sigma_{i-1}} E^{\sigma_i} F^s : E^{\sigma_1} \cdots E^{\sigma_{i-1}} F^s] = 2.$$

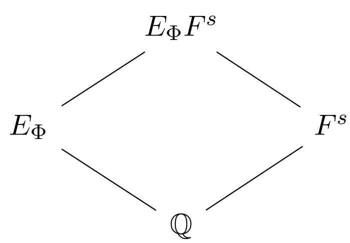
This completes the proof that $[E_\Phi F^s : F^s] = 2^n$.

Finally, since $E^s = E_\Phi F^s$ and $[E_\Phi F^s : F^s] = 2^n$, it follows that

$$[E^s : \mathbb{Q}] = [E^s : F^s][F^s : \mathbb{Q}] = 2^n [F^s : \mathbb{Q}].$$

□

Proof of Theorem 3.7.6. We have the following towers of fields.



Therefore,

$$[E_\Phi F^s : E_\Phi][E_\Phi : \mathbb{Q}] = [E_\Phi F^s : F^s][F^s : \mathbb{Q}],$$

hence by Lemma 3.7.11 we have

$$[E_\Phi : \mathbb{Q}] = 2^n \frac{[F^s : \mathbb{Q}]}{[E_\Phi F^s : E_\Phi]}.$$

Now, it is known that if K/M is a finite Galois extension and L/M is an arbitrary extension, then $[KL : L]$ divides $[K : M]$ (see e.g. [Lan02, Corollary VI.1.13]). Since $F^s/\mathbb{Q}$ is Galois, we have that $[E_\Phi F^s : E_\Phi]$ divides $[F^s : \mathbb{Q}]$. This implies that $[E_\Phi : \mathbb{Q}] \geq 2^n$. On the other hand, by Proposition 3.6.3, we also know that $[E_\Phi : \mathbb{Q}] \leq 2^n$, thus we conclude that $[E_\Phi : \mathbb{Q}] = 2^n$, as desired.

Finally, since $\mathbb{Q} \subseteq E_\Phi \subseteq E^s$, it follows that $[E_\Phi : \mathbb{Q}] = 2^n$ divides $[E^s : \mathbb{Q}]$. Then if $n \geq 3$

we have $[E^s : \mathbb{Q}] \geq 2^n > 2n = [E : \mathbb{Q}]$, which proves that the field extension $E/\mathbb{Q}$ is non-Galois, therefore non-abelian. □

Remark 3.7.12. Let E/F be a CM extension as in Lemma 3.7.11. Then since $[E^s : \mathbb{Q}] = 2^n[F^s : \mathbb{Q}]$, the CM field E is a Weyl CM field if and only if $[F^s : \mathbb{Q}] = n!$.

3.7.4 Algorithm for constructing CM fields with reflex fields of maximal degree

By combining (the proof of) Proposition 3.7.1 with the choice $m = d_{F^s}$ and Theorem 3.7.6 with the choice $\mathcal{L} = \mathcal{R} \cup \{\mathfrak{q}\}$, we obtain the following algorithm for constructing infinite families of CM extensions which are non-Galois over $\mathbb{Q}$ and have reflex fields of maximal degree.

Algorithm 1 CM fields with reflex fields of maximal degree

1: **Input**: A tuple $(F, p, \mathfrak{p}, \mathcal{R}, \mathcal{U}_1, \mathcal{U}_2)$ consisting of a totally real number field F of degree n, a rational prime $p \in \mathbb{Z}$ that splits in F^s, a prime ideal $\mathfrak{p}$ of F lying above p, a finite set $\mathcal{R}$ of prime ideals of F not dividing pd_{F^s}, and finite sets $\mathcal{U}_1$ and $\mathcal{U}_2$ of prime ideals of F not dividing $2pd_{F^s}$ such that $\mathcal{R}, \mathcal{U}_1$ and $\mathcal{U}_2$ are pairwise disjoint.

2: **Output**: A pair $(\mathfrak{q}, \Delta_\mathfrak{q})$ where $\mathfrak{q}$ is a prime ideal of F not dividing pd_{F^s}, and $\Delta_\mathfrak{q}$ is an element of $\mathcal{O}_F$ with prime factorization

$$\Delta_\mathfrak{q}\mathcal{O}_F = \mathfrak{p}\mathfrak{q}\prod_{\mathfrak{r}\in\mathcal{R}}\mathfrak{r}.$$

The field $E_\mathfrak{q} := F(\sqrt{\Delta_\mathfrak{q}})$ is a CM extension of F ramified only at the prime ideals of F dividing $\Delta_\mathfrak{q}$ with reflex fields of maximal degree 2^n. Moreover, each prime ideal in $\mathcal{U}_1$ splits in $E_\mathfrak{q}$ and each prime ideal in $\mathcal{U}_2$ remains inert in $E_\mathfrak{q}$. If $n \geq 3$ then $E_\mathfrak{q}/\mathbb{Q}$ is non-Galois.

3: Set $\mathcal{T}_1 := (\mathcal{U}_1 \cup \{\mathfrak{P} \subset \mathcal{O}_F \mid \mathfrak{P} \text{ divides } pd_{F^s}\}) \setminus \{\mathfrak{p}\}$.

4: Set $\mathcal{T}_2 := (\mathcal{U}_2 \cup \{\mathfrak{P} \subset \mathcal{O}_F \mid \mathfrak{P} \text{ divides } 2\}) \setminus (\mathcal{T}_1 \cup \mathcal{R} \cup \{\mathfrak{p}\})$.

5: Choose an integer $e \in \mathbb{Z}$ satisfying $e \geq 2\max\{v_\mathfrak{P}(2) \mid \mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2\} + 1$.

6: Set $\mathfrak{m}_\infty$ to be the formal product of all the embeddings in $\mathrm{Hom}(F, \mathbb{R})$.

7: Set

$$\mathfrak{m}_0 := \prod_{\mathfrak{P}\in\mathcal{T}_1\cup\mathcal{T}_2}\mathfrak{P}^e$$

and $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$.

8: For each $\mathfrak{P} \in \mathcal{T}_2$ find an element $\alpha_\mathfrak{P} \in \mathcal{O}_F$ such that $F_\mathfrak{P}(\sqrt{\alpha_\mathfrak{P}})$ is an unramified quadratic extension of $F_\mathfrak{P}$.

9: Find an element $a \in F^\times$ satisfying the following congruences.

(i) $a \overset{\times}{\equiv} -1 \pmod{\mathfrak{m}_\infty}$.

(ii) $a \overset{\times}{\equiv} 1 \pmod{\mathfrak{P}^e}$ for every $\mathfrak{P} \in \mathcal{T}_1$.

(iii) $a \overset{\times}{\equiv} \alpha_\mathfrak{P} \pmod{\mathfrak{P}^e}$ for every $\mathfrak{P} \in \mathcal{T}_2$.

10: Set

$$\mathfrak{n} := a\mathfrak{p}^{-1} \prod_{\mathfrak{r} \in \mathcal{R}} \mathfrak{r}^{-1}.$$

11: Choose a prime ideal $\mathfrak{q} \subset \mathcal{O}_F$ lying in the ray class of $\mathfrak{n}$ modulo $\mathfrak{m}$ such that $\mathfrak{q} \notin \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{R} \cup \{\mathfrak{p}\}$.

12: Find an element $b_{\mathfrak{q}} \in F^{\times}$ such that $b_{\mathfrak{q}} \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$ and $\mathfrak{q} = b_{\mathfrak{q}}\mathfrak{n}$.

13: Set $\Delta_{\mathfrak{q}} := ab_{\mathfrak{q}}$.

14: **Return**: $(\mathfrak{q}, \Delta_{\mathfrak{q}})$.

Remark 3.7.13. For steps 5 and 8 in the algorithm, see Lemmas 3.7.3 and 3.7.4, respectively.

Remark 3.7.14. The congruences in steps 9 and 11 of the algorithm are chosen to force the given prime ideal $\mathfrak{P} \in \mathcal{T}_1 \cup \mathcal{T}_2$ to be unramified in the extension $E_{\mathfrak{q}}$. In fact, as was shown in the proof of Lemma 3.7.5, the congruence 9 (ii) forces $\mathfrak{P}$ to split in $E_{\mathfrak{q}}$, while the congruence 9 (iii) forces $\mathfrak{P}$ to remain inert in $E_{\mathfrak{q}}$.

Remark 3.7.15. Recall from the proof of Proposition 3.7.1 that

$$\mathcal{S}_{\mathcal{R},\mathfrak{p}} := \mathcal{S}(\mathfrak{n}) \smallsetminus (\mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{R} \cup \{\mathfrak{p}\}),$$

where

$$\mathcal{S}(\mathfrak{n}) := \{\mathfrak{q} \subset \mathcal{O}_F \mid \mathfrak{q} \text{ is a prime ideal and } [\mathfrak{q}] = [\mathfrak{n}] \text{ in } \mathcal{R}_F(\mathfrak{m})\}.$$

Also, as was shown in the proof of Proposition 3.7.1, the set $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ has natural density $d(\mathcal{S}_{\mathcal{R},\mathfrak{p}}) = 1/\#\mathcal{R}_F(\mathfrak{m})$.

3.8 Proof of Theorem A

Let F be a totally real number field of degree $n \geq 3$. Let $p \in \mathbb{Z}$ be a prime number which splits in the Galois closure F^s and let $\mathfrak{p}$ be a prime ideal of F lying above p. Let $\mathcal{R}$ be a finite set of prime ideals of F not dividing pd_{F^s}. Let $\mathcal{U}_1$ and $\mathcal{U}_2$ be finite sets of prime ideals of F not dividing $2pd_{F^s}$ such that $\mathcal{R}, \mathcal{U}_1$ and $\mathcal{U}_2$ are pairwise disjoint. Then by Proposition 3.7.1 with the choice $m = d_{F^s}$, there is a set $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ of prime ideals of F which is disjoint from $\mathcal{R} \cup \mathcal{U}_1 \cup \mathcal{U}_2 \cup \{\mathfrak{p}\}$ such that the following statements are true.

(i) $\mathcal{S}_{\mathcal{R},\mathfrak{p}}$ has positive natural density.

(ii) Each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$ is relatively prime to pd_{F^s}.

(iii) For each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$, there is an element $\Delta_{\mathfrak{q}} \in \mathcal{O}_F$ with prime factorization

$$\Delta_{\mathfrak{q}}\mathcal{O}_F = \mathfrak{p}\mathfrak{q}\prod_{\mathfrak{r}\in\mathcal{R}} \mathfrak{r}.$$

(iv) The field $E_{\mathfrak{q}} := F(\sqrt{\Delta_{\mathfrak{q}}})$ is a CM extension of F which is ramified only at the prime ideals of F dividing $\Delta_{\mathfrak{q}}$. Moreover, each prime ideal in $\mathcal{U}_1$ splits in $E_{\mathfrak{q}}$ and each prime ideal in $\mathcal{U}_2$ is inert in $E_{\mathfrak{q}}$.

It follows from Theorem 3.7.6 with the choice $\mathcal{L} = \mathcal{R} \cup \{\mathfrak{q}\}$ that for each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$, the degree of the reflex field $E_{\mathfrak{q},\Phi}$ is $[E_{\mathfrak{q},\Phi} : \mathbb{Q}] = 2^n$ for every CM type $\Phi \in \Phi(E_{\mathfrak{q}})$, and moreover, since $n \geq 3$ then $E_{\mathfrak{q}}/\mathbb{Q}$ is non-Galois.

Now, by Proposition 3.5.1 and Corollary 3.6.4, if E is a CM field and there exists a CM type $\Phi \in \Phi(E)$ such that the degree of the reflex field E_Φ is $[E_\Phi : \mathbb{Q}] = 2^n$, then Conjecture 3.3.1 is true for E. It then follows from the previous paragraph that for each prime ideal $\mathfrak{q} \in \mathcal{S}_{\mathcal{R},\mathfrak{p}}$, Conjecture 3.3.1 is true for $E_{\mathfrak{q}}$. □

3.9 Weyl CM fields and the proof of Theorem B

Let $E = \mathbb{Q}(\alpha)$ be a CM field of degree $2g$. Let $m_\alpha(X)$ be the minimal polynomial of α and denote its roots by $\alpha_1 = \alpha, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g}$. Let

$$a_{2\ell-1} := \alpha_\ell \qquad \text{and} \qquad a_{2\ell} := \overline{\alpha_\ell} \tag{3.32}$$

for $\ell = 1, \ldots, g$. Then $E^s = \mathbb{Q}(a_1, \ldots, a_{2g})$ is the Galois closure of E. Let S_{2g} be the symmetric group on the elements $\{a_1, \ldots, a_{2g}\}$ and W_{2g} be the subgroup of S_{2g} consisting of permutations which map any pair of the form $\{a_{2j-1}, a_{2j}\}$ to a pair $\{a_{2k-1}, a_{2k}\}$. The group W_{2g} is called the

Weyl group. It can be shown that $\#W_{2g} = 2^g g!$ and that W_{2g} fits in the exact sequence

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^g \longrightarrow W_{2g} \longrightarrow S_g \longrightarrow 1.$$

Proposition 3.9.1. *The Galois group* $\mathrm{Gal}(E^s/\mathbb{Q})$ *is isomorphic to a subgroup of* W_{2g}.

Proof. There is an injective group homomorphism $\phi : \mathrm{Gal}(E^s/\mathbb{Q}) \longrightarrow S_{2g}$ given by restriction $\sigma \longmapsto \sigma|_{\{a_1,\ldots,a_{2g}\}}$. Hence $\mathrm{Gal}(E^s/\mathbb{Q}) \cong \phi(\mathrm{Gal}(E^s/\mathbb{Q})) < S_{2g}$, so it suffices to prove that $\phi(\mathrm{Gal}(E^s/\mathbb{Q})) \subseteq W_{2g}$, or equivalently, that given $\sigma \in \mathrm{Gal}(E^s/\mathbb{Q})$ and a pair $\{a_{2j-1}, a_{2j}\}$, we have $\sigma(\{a_{2j-1}, a_{2j}\}) = \{a_{2k-1}, a_{2k}\}$. Since σ permutes the elements $\{a_1, \ldots, a_{2g}\}$, we have $\sigma(a_{2j-1}) = a_{2k-1}$ or $\sigma(a_{2j-1}) = a_{2k}$ for some k. Now, since E is a CM field, given any $b \in E$, we have $\overline{\sigma(b)} = \sigma(\overline{b})$ for all $\sigma \in \mathrm{Gal}(E^s/\mathbb{Q})$. Moreover, from (3.32), we have $\overline{a_{2\ell-1}} = a_{2\ell}$ and $\overline{a_{2\ell}} = a_{2\ell-1}$. Combining these facts yields

$$\sigma(a_{2j}) = \sigma(\overline{a_{2j-1}}) = \overline{a_{2k-1}} = a_{2k} \quad \text{or} \quad \sigma(a_{2j}) = \sigma(\overline{a_{2j-1}}) = \overline{a_{2k}} = a_{2k-1}.$$

This completes the proof. □

Definition 3.9.2. If E is a CM field such that $\mathrm{Gal}(E^s/\mathbb{Q}) \cong W_{2g}$, then E is called a *Weyl CM field*.

Observe that if $g \geq 2$ and E is a Weyl CM field of degree $2g$, then $E/\mathbb{Q}$ is non-Galois since $\#\mathrm{Gal}(E^s/\mathbb{Q}) = 2^g g! > 2g = [E : \mathbb{Q}]$. In particular, any Weyl CM field of degree $2g \geq 4$ is non-abelian.

Proof of Theorem B. Let E be a Weyl CM field. Then by Proposition 3.5.1 and Corollary 3.6.4, it suffices to prove that there exists a CM type Φ for E such that the reflex field E_Φ has degree $[E_\Phi : \mathbb{Q}] = 2^g$. For $i = 1, \ldots, g$ let $\tau_i : E \hookrightarrow \mathbb{C}$ be the embedding defined by $\tau_i(\alpha_1) = \alpha_i$, where $\alpha_1 = \alpha$. Then $\mathrm{Hom}(E, \mathbb{C}) = \{\tau_1, \overline{\tau_1}, \ldots, \tau_g, \overline{\tau_g}\}$. Note that $\tau_i(a_1) = a_{2i-1}$ for $i = 1, \ldots, g$. Fix the choice of CM type $\Phi = \{\tau_1, \ldots, \tau_g\}$. We will prove that $[E_\Phi : \mathbb{Q}] = 2^g$.

Since E is a Weyl CM field, we have $\mathrm{Gal}(E^s/\mathbb{Q}) \cong W_{2g}$, and thus $\#\mathrm{Gal}(E^s/\mathbb{Q}) = 2^g g!$. Moreover, the calculations in the proof of Lemma 3.6.3 yield

$$[E_\Phi : \mathbb{Q}] = \frac{\#\,\mathrm{Gal}(E^s/\mathbb{Q})}{\#\,\mathrm{Stab}_{\mathrm{Gal}(E^s/\mathbb{Q})}(\Phi)} = \frac{2^g g!}{\#\,\mathrm{Stab}_{\mathrm{Gal}(E^s/\mathbb{Q})}(\Phi)}.$$

Hence it suffices to prove that $\# \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi) = g!$.

Let S_{2g}^{odd} be the symmetric group on the odd-indexed elements $\{a_1, a_3, \ldots, a_{2g-1}\}$. Then

$$\begin{aligned}
\sigma \in \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi) &\iff \sigma\Phi = \Phi \\
&\iff \text{for all } i, \text{ there exists a } j \text{ such that } \sigma\tau_i(a_1) = \tau_j(a_1) \\
&\iff \text{for all } i, \text{ there exists a } j \text{ such that } \sigma(a_{2i-1}) = a_{2j-1} \\
&\iff \sigma|_{\{a_1,a_3,\ldots,a_{2g-1}\}} \in S_{2g}^{\text{odd}}.
\end{aligned}$$

Thus we have a map $\widetilde{\phi} : \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi) \longrightarrow S_{2g}^{\text{odd}}$ given by restriction

$$\sigma \longmapsto \sigma|_{\{a_1,a_3,\ldots,a_{2g-1}\}}.$$

We will prove that $\widetilde{\phi}$ is bijective.

Surjectivity: Let $\pi \in S_{2g}^{\text{odd}}$. Then for all i, there exists a j such that $\pi(a_{2i-1}) = a_{2j-1}$. There is a unique lift $\widetilde{\pi}$ of π to W_{2g} given by $\widetilde{\pi}(a_{2i-1}) = a_{2j-1}$ and $\widetilde{\pi}(a_{2i}) = a_{2j}$. Since E is a Weyl CM field, we have an isomorphism $\operatorname{Gal}(E^s/\mathbb{Q}) \cong \phi(\operatorname{Gal}(E^s/\mathbb{Q})) = W_{2g}$, where ϕ is the restriction map $\sigma \longmapsto \sigma|_{\{a_1,\ldots,a_{2g}\}}$ in the proof of Proposition 3.9.1. Hence there exists a unique element $\sigma \in \operatorname{Gal}(E^s/\mathbb{Q})$ such that $\phi(\sigma) = \widetilde{\pi}$. Observe that

$$\sigma|_{\{a_1,a_3,\ldots,a_{2g-1}\}} = \widetilde{\pi}|_{\{a_1,a_3,\ldots,a_{2g-1}\}} = \pi \in S_{2g}^{\text{odd}}.$$

It follows that $\sigma \in \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi)$ with $\widetilde{\phi}(\sigma) = \pi$. This proves that $\widetilde{\phi}$ is surjective.

Injectivity: Let $\sigma_1, \sigma_2 \in \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi)$ with $\widetilde{\phi}(\sigma_1) = \widetilde{\phi}(\sigma_2)$. Then

$$\sigma_1|_{\{a_1,a_3,\ldots,a_{2g-1}\}} = \sigma_2|_{\{a_1,a_3,\ldots,a_{2g-1}\}},$$

i.e., $\sigma_1(a_{2i-1}) = \sigma_2(a_{2i-1})$ for $i = 1, \ldots, g$. On the other hand, arguing as in the proof of Proposition 3.9.1, we have

$$\sigma_1(a_{2i}) = \sigma_1(\overline{a_{2i-1}}) = \overline{\sigma_1(a_{2i-1})} = \overline{\sigma_2(a_{2i-1})} = \sigma_2(\overline{a_{2i-1}}) = \sigma_2(a_{2i})$$

for $i = 1, \ldots, g$. Thus, $\sigma_1 = \sigma_2$. This proves that $\widetilde{\phi}$ is injective.

Since $\widetilde{\phi}$ is bijective, we have $\# \operatorname{Stab}_{\operatorname{Gal}(E^s/\mathbb{Q})}(\Phi) = \# S_{2g}^{\text{odd}} = g!$. This completes the proof.

□

3.10 Proof of Theorem 3.1.8

As mentioned in Remark 3.1.3, if E is a quartic CM field then the only possible Galois groups of its Galois closure are $C_4 := \mathbb{Z}/4\mathbb{Z}$, $V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and D_4. Moreover, the Weyl group $W_4 \cong D_4$. It is known that if a quartic number field K has Galois group $\mathrm{Gal}(K^s/\mathbb{Q}) \cong C_4$ or V_4, then K contains a unique real quadratic subfield. Hence for the signature $(0, 2)$ (which corresponds to the quartic totally complex case) we have

$$\mathrm{CM}_4(C_4, X) = N_{0,2}(C_4, X) \quad \text{and} \quad \mathrm{CM}_4(V_4, X) = N_{0,2}(V_4, X). \tag{3.33}$$

When $\mathrm{Gal}(K^s/\mathbb{Q}) \cong D_4$, then K can either contain a real quadratic subfield or an imaginary quadratic subfield. Thus in that case one can define a refined counting function $N^+_{0,2}(D_4, X)$ which counts only isomorphism classes of quartic number fields $K/\mathbb{Q}$ with signature $(0, 2)$ containing a real quadratic subfield, and such that $\mathrm{Gal}(K^s/\mathbb{Q}) \cong D_4$ and $|d_K| \leq X$ (see [CDO02]). With this notation we then have

$$\mathrm{CM}_4(W_4, X) = \mathrm{CM}_4(D_4, X) = N^+_{0,2}(D_4, X). \tag{3.34}$$

By Cohen, Diaz y Diaz and Olivier [CDO05, Corollary 4.5 (2), p. 501] (which refines earlier work of Baily [Bai80] and Mäki [Mäk85]) we have

$$N_{0,2}(C_4, X) = c(C_4)X^{\frac{1}{2}} + O(X^{\frac{1}{3}+\varepsilon}), \tag{3.35}$$

for some explicit positive constant $c(C_4)$ and any $\varepsilon > 0$. Similarly, in [CDO06, p. 582] we find the asymptotic formula

$$N_{0,2}(V_4, X) = c(V_4)X^{\frac{1}{2}} \log^2 X + O(X^{\frac{1}{2}} \log X), \tag{3.36}$$

for some explicit positive constant $c(V_4)$. Finally, in [CDO02, Proposition 6.2, p. 88] we find the asymptotic formula

$$N^+_{0,2}(D_4, X) = c(D_4)^+ X + O(X^{\frac{3}{4}+\varepsilon}), \tag{3.37}$$

where again $c(D_4)^+$ is an explicit positive constant.

Since

$$\mathrm{CM}_4(X) = \mathrm{CM}_4(D_4, X) + \mathrm{CM}_4(C_4, X) + \mathrm{CM}_4(V_4, X),$$

it follows from equations (3.33)–(3.37) that

$$\mathrm{CM}_4(X) = c(D_4)^{+}X + O(X^{\frac{3}{4}+\varepsilon}).$$

Finally, since this is the same asymptotic formula satisfied by the counting function $\mathrm{CM}_4(W_4, X)$, we conclude that the density of quartic Weyl CM fields is

$$\rho_{\text{Weyl}}(4) = \lim_{X\to\infty} \frac{\mathrm{CM}_4(W_4, X)}{\mathrm{CM}_4(X)} = 1.$$

□

3.11 Abelian varieties over finite fields, Weil q-numbers, and density results

We first review some facts concerning Weil q-numbers and abelian varieties over finite fields.

3.11.1 Weil q-numbers and abelian varieties over $\mathbb{F}_q$

Let $q = p^n$ where p is a prime number and n is a positive integer. A *Weil q-number* is an algebraic integer π such that for every embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have $|\sigma(\pi)| = q^{1/2}$. Let $W(q)$ denote the set of Weil q-numbers. Two Weil q-numbers π_1 and π_2 are *conjugate* if there exists an isomorphism $\mathbb{Q}(\pi_1) \to \mathbb{Q}(\pi_2)$ which maps π_1 to π_2. In this case, we write $\pi_1 \sim \pi_2$.

We have the following facts about Weil q-numbers (see e.g. [GO88, p. 1 and Corollary 2.1]).

Lemma 3.11.1. *Let $q = p^n$ and $\pi \in W(q)$.*

(i) If $\sigma(\pi) \in \mathbb{R}$ for some embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, then $\mathbb{Q}(\pi) = \mathbb{Q}$ if n is even and $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$ if n is odd.

(ii) If $\sigma(\pi) \in \mathbb{C} \setminus \mathbb{R}$ for all embeddings $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, then $\mathbb{Q}(\pi)$ is a CM field with maximal totally real subfield $\mathbb{Q}(\pi + q/\pi)$.

Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$ elements. Let $A/\mathbb{F}_q$ be an abelian variety of dimension g defined over $\mathbb{F}_q$ and let $\pi_A \in \mathrm{End}(A)$ be the Frobenius endomorphism of A. Let f_A be the characteristic polynomial of A, which is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$. Let $\mathbb{Q}[\pi_A]$ be the $\mathbb{Q}$-subalgebra of End$(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ generated by π_A. It is known that $\mathbb{Q}[\pi_A]$ is a field if and only if $A/\mathbb{F}_q$ is simple.

Weil proved that the roots of f_A are Weil q-numbers. Moreover, if $A/\mathbb{F}_q$ is simple, then the image of π_A under any homomorphism $\phi : \mathbb{Q}[\pi_A] \to \mathbb{C}$ is a Weil q-number. Any such homomorphism ϕ maps π_A to a root α_A of f_A. From here forward, we identify π_A with $\phi(\pi_A)$ for some choice of ϕ. This choice does not matter, since we will only consider Weil q-numbers up to conjugacy.

If $A/\mathbb{F}_q$ and $B/\mathbb{F}_q$ are isogenous simple abelian varieties, then $f_A = f_B$. In particular, $\pi_A \sim \pi_B$. This gives a well-defined map $A \mapsto \pi_A$ between the set of isogeny classes of simple abelian varieties $A/\mathbb{F}_q$ and Weil q-numbers up to conjugacy. A celebrated theorem of Honda and Tate (see e.g. [Tat71]) asserts that this map is a bijection.

3.11.2 Density results and the proof of Theorem 3.1.10

Let $A/\mathbb{F}_q$ be an abelian variety and α_A be a root of f_A. Let $K_{f_A} = \mathbb{Q}(\alpha_A)^s$ be the splitting field of f_A and $G_{f_A} = \text{Gal}(K_{f_A}/\mathbb{Q})$. Define the sets

$$\mathcal{A}_g(q) := \{\text{isogeny classes of abelian varieties } A/\mathbb{F}_q \text{ with } \dim(A) = g\},$$

$$\mathcal{B}_g(q) := \{\text{isogeny classes of abelian varieties } A/\mathbb{F}_q \text{ with } \dim(A) = g \text{ and } G_{f_A} \cong W_{2g}\}.$$

Kowalski [Kow06, Proposition 8] proved the following density result.

Theorem 3.11.2. *With notation as above, one has*

$$\lim_{n\to\infty} \frac{\#\mathcal{B}_g(p^n)}{\#\mathcal{A}_g(p^n)} = 1.$$

On the other hand, we have the following result.

Proposition 3.11.3. *Let $A/\mathbb{F}_q$ be an abelian variety of dimension $g \geq 2$. If $G_{f_A} \cong W_{2g}$, then $\mathbb{Q}(\alpha_A)$ is a non-Galois Weyl CM field of degree $2g$.*

Proof. Let $m := [\mathbb{Q}(\alpha_A) : \mathbb{Q}]$. Since α_A is a root of f_A and $f_A \in \mathbb{Z}[x]$ is monic of degree $2g$, then α_A is an algebraic integer of degree m where $m|2g$. Suppose by contradiction that $m < 2g$.

Since m is a proper divisor of $2g$, we have $m \leq g$. Hence the Galois closure $K_{f_A} = \mathbb{Q}(\alpha_A)^s$ has degree $[K_{f_A} : \mathbb{Q}] \leq m! \leq g!$. However, $\#W_{2g} = 2^g g!$, which contradicts the assumption that $G_{f_A} \cong W_{2g}$. Thus $m = 2g \geq 4$, hence it follows from Lemma 3.11.1 that $\mathbb{Q}(\alpha_A)$ is a CM field. Finally, since $2g \geq 4$, we conclude that $\mathbb{Q}(\alpha_A)$ is a non-Galois Weyl CM field of degree $2g$. □

Proof of Theorem 3.1.10. By Theorem 3.11.2 and Proposition 3.11.3, if $g \geq 2$ then the proportion of isogeny classes $[A] \in A_g(p^n)$ for which $\mathbb{Q}(\alpha_A)$ is a non-Galois Weyl CM field approaches 1 as $n \to \infty$. Theorem 3.1.10 now follows from Theorem B. □

We next show that any CM field E is isomorphic to a CM field of the form $\mathbb{Q}(\pi_A)$ for a simple abelian variety $A/\mathbb{F}_q$.

The following result is a consequence of [GO88, Theorems 1 and 2 (i)].

Theorem 3.11.4. *Let E be a CM field. Then for each integer $n \geq 2$, there exists a prime number $p = p(E, n)$ such that $E = \mathbb{Q}(\pi_p)$ for some Weil p^n-number $\pi_p \in W(p^n)$.*

Greaves and Odoni used the Chebotarev density theorem to deduce the following corollary.

Corollary 3.11.5. *There exists an integer $a(E, n) \geq 1$ such that*

$$\#\{p = p(E,n) :\ 2 \leq p \leq X,\ E = \mathbb{Q}(\pi_p),\ \pi_p \in W(p^n)\} =$$

$$\frac{a(E,n)}{[H(E^s) : \mathbb{Q}]}\mathrm{Li}(X) + O_{E,n}\left(X \exp\left(-c(E,n)\sqrt{\log(X)}\right)\right)$$

as $X \to \infty$, where $H(E^s)$ denotes the Hilbert class field of E^s, $\mathrm{Li}(X) := \int_2^X dt/\log(t)$, and $c(E, n) > 0$.

We have the following corollary.

Corollary 3.11.6. *Let E be a CM field. Then for each integer $n \geq 2$, there is a set of prime numbers $p = p(E, n)$ with positive natural density such that $E \cong \mathbb{Q}(\pi_A)$ for some simple abelian variety $A/\mathbb{F}_{p^n}$.*

Proof. Let E be a CM field. Then by Corollary 3.11.5, for each integer $n \geq 2$ there is a set of prime numbers $p = p(E, n)$ with positive natural density such that $E = \mathbb{Q}(\pi_p)$ for some $\pi_p \in W(p^n)$.

On the other hand, by the Honda-Tate theorem, for each such prime number p, there exists a simple abelian variety $A/\mathbb{F}_{p^n}$ such that $\pi_A \sim \pi_p$. Therefore, $\mathbb{Q}(\pi_A) \cong \mathbb{Q}(\pi_p) = E$. $\square$

Given Corollary 3.11.6, it is natural to ask whether a density result analogous to Theorem 3.11.2 holds for simple abelian varieties. Define the sets

$$\mathcal{A}_g^s(q) := \{\text{isogeny classes of simple abelian varieties } A/\mathbb{F}_q \text{ with } \dim(A) = g\},$$

$$\mathcal{B}_g^s(q) := \{[A/\mathbb{F}_q] \in \mathcal{A}_g^s(q) \mid G_{f_A} \cong W_{2g}\}.$$

It seems likely that a modification of the methods in [Kow06] can be used to prove that

$$\lim_{n\to\infty} \frac{\#\mathcal{B}_g^s(p^n)}{\#\mathcal{A}_g^s(p^n)} = 1.$$

If true, then arguing as in the proof of Theorem 3.1.10, it would follow that if $g \geq 2$, then the proportion of isogeny classes $[A] \in \mathcal{A}_g^s(p^n)$ for which $\mathbb{Q}(\pi_A)$ is a CM field that satisfies the Colmez conjecture approaches 1 as $n \to \infty$.

4. CONCLUSIONS

The two main topics treated in this thesis were the establishment of a Chowla-Selberg formula for abelian CM-fields, which was done in chapter 2, and the proof of infinitely many new cases of the Colmez conjecture for non-abelian CM fields, which was done in chapter 3.

Both topics still merit further investigation, and in what follows we briefly indicate how we attempt to study this in future joint work with Riad Masri.

In the case of the Chowla-Selberg formula, the non-abelian case still remains to be studied in detail. We plan to prove non-abelian Chowla-Selberg formulas by using the non-abelian cases of the Colmez conjecture that we proved, in combination with a very detailed study and refinement of Shintani's work on the evaluation of L-functions.

On the other hand, as was indicated in the introduction of chapter 3, we plan to attack the Colmez conjecture in low degree for non-abelian CM fields by using methods from arithmetic statistics to study the density of Weyl CM fields of a fixed degree, when ordered by the absolute value of their discriminant.

REFERENCES

[And82] G. W. Anderson, *Logarithmic derivatives of Dirichlet L-functions and the periods of abelian varieties.* Compositio Math. **45** (1982), 315–332.

[ABP04] G. W. Anderson, D. W. Brownawell, and M. A. Papanikolas, *Determination of the algebraic relations among special Γ-values in positive characteristic.* Ann. of Math. **160** (2004), 237–313.

[AGHM15] F. Andreatta, E. Z. Goren, B. Howard and K. Madapusi Pera, *Faltings heights of abelian varieties with complex multiplication.* `arXiv:1508.00178 [math.NT]` (2015).

[Asa70] T. Asai, *On a certain function analogous to* $\log|\eta(z)|$. Nagoya Math. J. **40** (1970), 193–211.

[Bai80] A. M. Baily, *On the density of discriminants of quartic fields.* J. Reine Angew. Math. **315** (1980), 190–210.

[Bar01] E. W. Barnes, *The theory of the double Gamma function*. Phil. Trans. R. Soc. Lond. A **196** (1901), 265–387.

[BS-M16a] A. Barquero-Sanchez and R. Masri, *Faltings heights of CM abelian surfaces and the non-abelian Chowla-Selberg formula*, preprint (2016).

[BS-M16b] A. Barquero-Sanchez and R. Masri, *Faltings heights of CM abelian threefolds and the non-abelian Chowla-Selberg formula*, in preparation (2016).

[Bha07] M. Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants.* Int. Math. Res. Not. IMRN 2007, no. 17, Art. ID rnm052, 20 pp.

[BMM-B90] Jean-Benoît Bost, Jean-François Mestre, and Laurent Moret-Bailly, *Sur le calcul explicite des ”classes de Chern” des surfaces arithmétiques de genre 2.* (French) [On the explicit calculation of the ”Chern classes” of arithmetic surfaces of genus 2] Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). Astérisque No. 183 (1990), 69–105.

[BS15] F. Bouyer and M. Streng, *Examples of CM curves of genus two defined over the reflex field.* LMS J. Comput. Math. **18** (2015), no. 1, 507–538.

[BKY12] J. H. Bruinier, S. S. Kudla, and T. H. Yang, *Special values of Green functions at big CM points.* Int. Math. Res. Not. IMRN 2012, no. 9, 1917–1967.

[BY06] J. H. Bruinier and T. H. Yang, *CM-values of Hilbert modular functions*. Invent. Math. **163** (2006), 229–288.

[BY07] J. H. Bruinier and T. H. Yang, *Twisted Borcherds products on Hilbert modular surfaces and their CM values.* Amer. J. Math. **129** (2007), 807–841.

[BY11] J. H. Bruinier and T. H. Yang, *CM values of automorphic Green functions on orthogonal groups over totally real fields.* Arithmetic geometry and automorphic forms, 1–54, Adv. Lect. Math. (ALM), 19, Int. Press, Somerville, MA, 2011.

[CO12] C. Chai and F. Oort, *Abelian varieties isogenous to a Jacobian.* Ann. of Math. (2) **176** (2012), no. 1, 589–635.

[Chi09] N. Childress, *Class field theory.* Universitext. Springer, New York, 2009.

[CS49] S. Chowla and A. Selberg, *On Epstein's zeta function. I.* Proc. Nat. Acad. Sci. U. S. A. **35** (1949). 371–374.

[CS67] S. Chowla and A. Selberg, *On Epstein's zeta-function.* J. Reine Angew. Math. **227** (1967), 86–110.

[Coh03] H. Cohen, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$ *with signatures.* Ann. Inst. Fourier (Grenoble) **53** (2003), no. 2, 339–377.

[Coh07] H. Cohen, *Number theory. Vol. II. Analytic and modern tools.* Graduate Texts in Mathematics, **240**. Springer, New York, 2007. xxiv+596 pp.

[CDO02] H. Cohen, F. Diaz y Diaz and M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$. Compositio Math. **133** (2002), no. 1, 65–93.

[CDO05] H. Cohen, F. Diaz y Diaz and M. Olivier, *Counting cyclic quartic extensions of a number field.* J. Théor. Nombres Bordeaux **17** (2005), no. 2, 475–510.

[CDO06] H. Cohen, F. Diaz y Diaz and M. Olivier, *Counting discriminants of number fields.* J. Théor. Nombres Bordeaux **18** (2006), no. 3, 573–593.

[Col93] P. Colmez, *Périodes des variétés abéliennes à multiplication complexe*. Ann. of Math. **138** (1993), 625–683.

[Col98] P. Colmez, *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe. (French) [On the Faltings height of abelian varieties with complex multiplication]* Compositio Math. **111** (1998), no. 3, 359–368.

[CH88] P. E. Conner and J. Hurrelbrink, *Class number parity.* Series in Pure Mathematics, 8. World Scientific Publishing Co., Singapore, 1988. xii+234 pp.

[Del79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales. With an appendix by N. Koblitz and A. Ogus.* Proc. Sympos. Pure Math., XXXIII, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 313–346, Amer. Math. Soc., Providence, R.I., 1979.

[Den84] C. Deninger, *On the analogue of the formula of Chowla and Selberg for real quadratic fields.* J. Reine Angew. Math. **351** (1984), 171–191.

[Fro83] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields.* Contemporary Mathematics, **24**. American Mathematical Society, Providence, RI, 1983. viii+86 pp.

[FT93] A. Fröhlich and M. J. Taylor, *Algebraic number theory.* Cambridge Studies in Advanced Mathematics, **27**. Cambridge University Press, Cambridge, 1993.

[Gal73] P. X. Gallagher, *The large sieve and probabilistic Galois theory.* Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 91–101. Amer. Math. Soc., Providence, R.I., 1973.

[GO88] A. Greaves and R. W. K. Odoni, *Weil-numbers and CM-fields. I.* J. Reine Angew. Math. 391 (1988), 198–212.

[Gro80] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication. With an appendix by B. Mazur.* Lecture Notes in Mathematics, **776**. Springer, Berlin, 1980.

[GZ85] B. H. Gross and D. B. Zagier, *On singular moduli.* J. Reine Angew. Math. **355** (1985), 191–220.

[Jan96] G. J. Janusz, *Algebraic number fields.* Second edition. Graduate Studies in Mathematics, **7**. American Mathematical Society, Providence, RI, 1996.

[KKS11] K. Kato, N. Kurokawa, T. Saito, *Number theory. 2. Introduction to class field theory.* Translated from the 1998 Japanese original by Masato Kuwata and Katsumi Nomizu. Translations of Mathematical Monographs, **240**. Iwanami Series in Modern Mathematics. American Mathematical Society, Providence, RI, 2011.

[Koc00] H. Koch, *Number theory. Algebraic numbers and functions.* Translated from the 1997 German original by David Kramer. Graduate Studies in Mathematics, **24**. American Mathematical Society, Providence, RI, 2000.

[Kow06] E. Kowalski, *Weil numbers generated by other Weil numbers and torsion fields of abelian varieties.* J. London Math. Soc. (2) **74** (2006), no. 2, 273–288.

[Lan94] S. Lang, *Algebraic number theory.* Second edition. Graduate Texts in Mathematics, **110**. Springer-Verlag, New York, 1994. xiv+357 pp.

[Lan02] S. Lang, *Algebra.* Revised third edition. Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002.

[Ler87] M. Lerch, *Sur quelques formules relatives au nombre des classes.* Bull. d. sci. math. (2) **21** (1897), 302–303.

[Mäk85] S. Mäki, *On the density of abelian number fields*. Thesis, Helsinki, 1985.

[Mal02] G. Malle, *On the distribution of Galois groups.* J. Number Theory **92** (2002), 315–329.

[Mal04] G. Malle, *On the distribution of Galois groups. II.* Experiment. Math. **13** (2004), 129–135.

[Mas10] R. Masri, *CM cycles and nonvanishing of class group L–functions.* Math. Res. Lett. **17** (2010), 749–760.

[Mil06] J. S. Milne, *Complex Multiplication*. Course notes, version 0, April 7 (2006).

`http://www.jmilne.org/math/CourseNotes/CM.pdf`

[Mor96] P. Morandi, *Field and Galois theory.* Graduate Texts in Mathematics, **167**. Springer-Verlag, New York, 1996.

[Mor83] C. J. Moreno, *The Chowla-Selberg formula.* J. Number Theory **17** (1983), 226–245.

[Mou09] A. Mouhib, *On the parity of the class number of multiquadratic number fields.* J. Number Theory **129** (2009), 1205–1211.

[Neu99] J. Neukirch, *Algebraic number theory.* Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **322**. Springer-Verlag, Berlin, 1999.

[Obu13] A. Obus, *On Colmez's product formula for periods of CM-abelian varieties*. Math. Ann. **356** (2013), 401–418.

[Oor12] F. Oort, *CM Jacobians*. Notes from a talk at the conference "Galois covers and deformations", Bordeaux, June 25–29, 2012. `http://www.staff.science.uu.nl/∼oort0109/Bord2-VI-12.pdf`

[Rib01] P. Ribenboim, *Classical theory of algebraic numbers.* Universitext. Springer-Verlag, New York, 2001.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves.* Ann. of Math. (2) **85** (1967), 58–159.

[Shi70] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains.* Ann. of Math. (2) **91** (1970), 144–222.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Reprint of the 1971 original. Publications of the Mathematical Society of Japan, **11**. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[Shi98] G. Shimura, *Abelian varieties with complex multiplication and modular functions.* Princeton Mathematical Series, **46**. Princeton University Press, Princeton, NJ, 1998.

[Shi76] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **23** (1976), 393–417.

[Shi77a] T. Shintani, *On values at s=1 of certain L functions of totally real algebraic number fields.* Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), pp. 201–212. Japan Soc. Promotion Sci., Tokyo, 1977.

[Shi77b] , T. Shintani, *On a Kronecker limit formula for real quadratic fields.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 167–199.

[Sie65] C. L. Siegel, *Lectures on advanced analytic number theory*. Notes by S. Raghavan. Tata Institute of Fundamental Research Lectures on Mathematics, No. 23 Tata Institute of Fundamental Research, Bombay 1965 iii+331+iii pp.

[Sil86] J. H. Silverman, *Heights and elliptic curves.* Arithmetic geometry (Storrs, Conn., 1984), 253–265, Springer, New York, 1986.

[Tat71] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). (French) [Isogeny classes of abelian varieties over finite fields (after T. Honda)]* Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Exp. No. 352, 95–110, Lecture Notes in Math., **175**, Springer, Berlin, 1971.

[Tsi15] J. Tsimerman, *A proof of the André-Oort conjecture for* $\mathcal{A}_g$. `arXiv:1506.01466 [math.NT]` (2015).

[vdG88] G. van der Geer, *Hilbert modular surfaces.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 16. Springer-Verlag, Berlin, 1988. x+291 pp.

[Wei76] A. Weil, *Elliptic functions according to Eisenstein and Kronecker.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 88. Springer-Verlag, Berlin-New York, 1976.

[Wei98] E. Weiss, *Algebraic number theory.* Reprint of the 1963 original. Dover Publications, Inc., Mineola, NY, 1998.

[Win89] K. Wingberg, *Representations of locally profinite groups.* Representation theory and number theory in connection with the local Langlands conjecture (Augsburg, 1985), 117–125, Contemp. Math., **86**, Amer. Math. Soc., Providence, RI, 1989.

[Woo16] M. Wood, *Asymptotics for number fields and class groups*. Women in Numbers 3: Research Directions in Number Theory, to appear.

[Yan10a] T. H. Yang, *An arithmetic intersection formula on Hilbert modular surfaces.* Amer. J. Math. **132** (2010), 1275–1309.

[Yan10b] T. H. Yang, *The Chowla-Selberg formula and the Colmez conjecture.* Canad. J. Math. **62** (2010), 456–472.

[Yan13] T. H. Yang, *Arithmetic intersection on a Hilbert modular surface and the Faltings height.* Asian J. Math. **17** (2013), 335–381.

[Yos99] H. Yoshida, *On absolute CM-periods.* Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 221–278, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, 1999.

[YZ15] S. Yuan and S. Zhang, *On the Averaged Colmez Conjecture.* `arXiv:1507.06903 [math.NT]` (2015).

[Zag08] D. Zagier, *Elliptic modular forms and their applications.* The 1-2-3 of modular forms, 1–103, Universitext, Springer, Berlin, 2008.