Contemporary Mathematics
Volume **701**, 2018
http://dx.doi.org/10.1090/conm/701/14149

Arithmetic twists and Abelian extensions

V. Kumar Murty

To the memory of my friend, Fumiyuki Momose

Abstract. Hilbert's twelfth problem asks for the explicit construction of abelian extensions of general number fields. This is still an open problem even for a real quadratic field. In some cases, Shimura succeeded in the 1970s to construct some abelian extensions of real quadratic fields using points of finite order on abelian varieties associated to modular forms of weight 2 with real Nebentypus. Using results of Momose and Ribet, we shall generalize Shimura's construction to forms with non-real Nebentypus.

Contents

1. Introduction

It is an elementary fact that the field $\mathbb{Q}(\zeta_n)$ obtained by adjoining an n-th root of unity is Galois over $\mathbb{Q}$ with group $(\mathbb{Z}/n)^\times$. We may think of this extension as the one generated by the coordinates of points of order dividing n on the multiplicative group $\mathbb{G}_m$. The classical theorem of Kronecker and Weber asserts that any abelian extension of the rational number field $\mathbb{Q}$ is contained in a cyclotomic extension. It is also known that the abelian extensions of an imaginary quadratic field K are contained in the extensions generated by points of finite order on an elliptic curve

2010 *Mathematics Subject Classification.* Primary 11F11, 11F80; Secondary 11R11, 11R29, 14K15.

Key words and phrases. Abelian extensions, real quadratic field, modular forms, arithmetic twists, Galois representations.

Research partially supported by a Discovery grant from NSERC..

with multiplication by (an order in) K. Kronecker's Jugendtraum, or Hilbert's twelfth problem, ask for such constructions for any number field K. This is still an open problem. In particular, even the case of real quadratic fields is not understood.

In some cases, Shimura succeeded in the 1970s to construct ([**22**], Chapter 7 and [**23**]) some abelian extensions of real quadratic fields using points of finite order on abelian varieties associated to modular forms of weight 2. We shall generalize Shimura's construction to forms with non-real Nebentypus.

The results of this paper essentially formed Chapter 3 of my thesis [**10**] which was written in 1982, and this work was directly influenced by the paper of Momose [**12**]. I am grateful to him for patiently explaining his work to me, and for listening to my ideas as they were evolving. I remember spending many pleasant hours of conversation with Momose discussing mathematics.

Since my work (which has not been published until now), several other authors have considered Shimura's construction and generalized it in various ways. In particular, there are some results of Hida [**7**], Brown and Ghate [**1**] and Darmon and Green [**4**]. We give a brief description of this work and its relation to our work in the final section.

2. Abelian varieties of type (T')

Let K be a number field. We consider an Abelian variety $A_{/K}$ defined over K. If M is any extension of K, we denote by $\mathrm{End}_M(A)$ the algebra of M-rational endomorphisms of A. Write $G_K = \mathrm{Gal}(\overline{K}/K)$. If E is a subfield of $\mathrm{End}_K(A) \otimes \mathbb{Q}$ there is a natural action

$$\rho_\ell : G_K \longrightarrow \mathrm{Aut}_{E\otimes\mathbb{Q}_\ell} V_\ell(A)$$

Moreover, writing

$$E \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} E_\lambda,$$

we have a K-rational decomposition

$$V_\ell(A) = \prod_{\lambda|\ell} V_\lambda$$

and the action of G_K on V_λ is denoted ρ_λ.

We say that $A_{/K}$ is of type (T') if there is a subfield E of $\mathrm{End}_K(A) \otimes \mathbb{Q}$ such that for all primes ℓ, the triple (K, A, E) satisfies

- $(T1')$ $V_\ell(A)$ is a free $E \otimes \mathbb{Q}_\ell$ module of rank 2.
- $(T2')$ for each prime λ of E dividing ℓ, the λ-adic representation ρ_λ does not have an abelian semi-simplification, and this remains true even if ρ_λ is restricted to an open subgroup of G_K.
- $(T3')$ $\det_{E\otimes\mathbb{Q}_\ell} \rho_\ell = \epsilon\chi_\ell$ where ϵ is a finite order E-valued character independent of ℓ.

Let Π_ℓ denote the set of primes of K which either divide ℓ or at which A has bad reduction. Then, for $v \notin \Pi_\ell$, set

$$a_{v,\ell} = \mathrm{Tr}_{E\otimes\mathbb{Q}_\ell} \rho_\ell(\mathrm{Frob}_v).$$

Then $a_{v,\ell}$ is an element of E and is in fact independent of ℓ (so can be designated a_v). The subfield of E generated by these traces will be denoted P and we call it the trace subfield.

3. The arithmetic twisting group

Let K be a number field and A an Abelian variety defined over K. The construction described below is modelled on the work of Momose [**11**] and Ribet [**18**], [**19**] who worked with the Abelian varieties associated to quotients of the Jacobian of a modular curve.

Suppose we are given a subfield E of $\mathrm{End}_K(A)\otimes\mathbb{Q}$ such that the triple (K, A, E) is of type (T'). Let ℓ denote a fixed rational prime and denote by Π_ℓ the set of primes of K which divide ℓ or at which A has bad reduction.

The decomposition

$$E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \;=\; \prod \overline{\mathbb{Q}}_\ell$$

induces a corresponding decomposition

$$\overline{V_\ell} \;=\; V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \;=\; \prod V_\sigma$$

indexed by the various embeddings $\sigma : E \hookrightarrow \overline{\mathbb{Q}}_\ell$. By a result of Ribet ([**16**], Lemma 4.4.4), the hypothesis $(T2')$ implies that the V_σ are simple $\overline{\mathbb{Q}}_\ell[H]$ modules for any open subgroup H of G_K.

Throughout this section, we view E as a subfield of $\overline{\mathbb{Q}}_\ell$ and we shall write $1 : E \hookrightarrow \overline{\mathbb{Q}}_\ell$ for this distinguished embedding.

LEMMA 3.1. *We have* $\mathbb{Q}(\epsilon) \;\subseteq\; P$.

PROOF. Let $\sigma : \overline{\mathbb{Q}}_\ell \;\longrightarrow\; \overline{\mathbb{Q}}_\ell$ be an automorphism of $\overline{\mathbb{Q}}_\ell$ which leaves P fixed. Let $\sigma 1$ denote the composition of σ and 1. We consider the representation spaces V_1 and $V_{\sigma 1}$ of G_K. For $v \notin \Pi_\ell$, they have equal traces. Hence, by the Chebotarev density theorem, they have equal traces. As they are simple $\overline{\mathbb{Q}}_\ell[G_K]$-modules (in particular, semisimple), it follows that they are isomorphic. Thus, their determinants are equal, so $\epsilon^\sigma \chi_\ell \;=\; \epsilon\chi_\ell$. The result follows. □

We now describe the construction of the twisting group of A. Consider the set Γ of embeddings

$$\gamma : P \;\hookrightarrow\; \overline{\mathbb{Q}}_\ell$$

for which there exists a character

$$\chi_\gamma : G_K \;\longrightarrow\; \overline{\mathbb{Q}}_\ell^\times$$

such that for almost all v (that is, for all but finitely many v), we have

$$a_v^\gamma \;=\; a_v \chi_\gamma(\mathrm{Frob}_v). \tag{1}$$

LEMMA 3.2. *The character* χ_γ *is of finite order and* $\mathbb{Q}(\chi_\gamma) \;\subseteq\; \mathbb{Q}(\epsilon)$.

PROOF. Choose an extension of γ to an embedding $E \;\hookrightarrow\; \overline{\mathbb{Q}}_\ell$ and denote it again by γ. The relation (1) implies that as $\overline{\mathbb{Q}}_\ell[G_K]$-modules, we have

$$V_\gamma \;\simeq\; V_1 \;\otimes\; \chi_\gamma.$$

In particular, the determinants are equal and so we have

$$\epsilon^\gamma \;=\; \epsilon\chi_\gamma^2. \tag{2}$$

Since ϵ is of finite order, so is χ_γ. Furthermore, χ_γ must be of the form $\epsilon^i\omega_\gamma$ where i is an integer and ω_γ is a character satisfying $\omega_\gamma^2 = 1$. This shows that $\mathbb{Q}(\chi_\gamma) \;\subseteq\; \mathbb{Q}(\epsilon)$. □

The following lemma is modelled on Ribet ([**17**], p. 40).

LEMMA 3.3. *If $\gamma \in \Gamma$, there is a unique character χ_γ satisfying* (1).

PROOF. If χ_γ is not unique, then there is a non-trivial character χ of G_K taking values in P such that

$$a_v \;=\; a_v\chi(\mathrm{Frob}_v)$$

for almost all v. This implies that there is an automorphism M of the vector space V_1 such that for all $g \in G_K$, we have

$$M^{-1}\rho_{1,\ell}(g)M \;=\; \chi(g)\rho_{1,\ell}(g).$$

It follows that M is not a scalar and that it lies in $\mathrm{End}_{\overline{\mathbb{Q}}_\ell[H]}V_1$ where $H = \mathrm{Ker}\ \chi$. This contradicts the simplicity of the $\overline{\mathbb{Q}}_\ell[H]$-module V_1. □

PROPOSITION 3.4. *Γ is a finite Abelian group. It consists of the automorphisms γ of P for which there exists a character χ_γ such that*

$$a_v^\gamma \;=\; a_v\chi_\gamma(\mathrm{Frob}_v)$$

for almost all v.

PROOF. The second statement is implied by Lemma 3.1 and Lemma 3.2. It is clearly a finite group and it remains only to check that it is abelian. If $\gamma_1, \gamma_2 \in \Gamma$, we see that for almost all v, we have

$$\gamma_1\gamma_2(a_v) \;=\; a_v(\chi_{\gamma_1}\chi_{\gamma_2}^{\gamma_1})(\mathrm{Frob}_v).$$

It follows from Lemma 3.3 that

$$\chi_{\gamma_1\gamma_2} \;=\; \chi_{\gamma_1}\chi_{\gamma_2}^{\gamma_1}$$

and similarly that

$$\chi_{\gamma_2\gamma_1} \;=\; \chi_{\gamma_2}\chi_{\gamma_1}^{\gamma_2}.$$

Again by Lemma 3.3, we have

$$\gamma_1\gamma_2 \;=\; \gamma_2\gamma_1$$

if and only if

$$\chi_{\gamma_1\gamma_2} \;=\; \chi_{\gamma_2\gamma_1}.$$

For $i = 1, 2$, write

$$\chi_{\gamma_i} \;=\; \epsilon^{m_i}\omega_i$$

where ω_i is a character such that $\omega_i^2 = 1$ and m_i is an integer such that

$$\epsilon^{\gamma_i - 1} \;=\; \chi_{\gamma_i}^2 \;=\; \epsilon^{2m_i},$$

the first equality following from (2). Thus,

$$\chi_{\gamma_1\gamma_2}\chi_{\gamma_2\gamma_1}^{-1} \;=\; \epsilon^{[m_2(\gamma_1-1)-m_1(\gamma_2-1)]} \;=\; 1.$$

□

Now, let M be a finite extension of K and set

$$\Gamma_M \;=\; \{\gamma \in \Gamma,\ \ker\ \chi_\gamma \;\supseteq\; \mathrm{Gal}(\overline{K}/M)\}.$$

4. A general construction

We describe an abstract method of constructing abelian extensions. Let p be an odd prime and $\mathbb{F}$ a finite field of characteristic p. Let X be a 2-dimensional $\mathbb{F}$ vector space and let G be an abstract group. Suppose we are given a normal subgroup H of G such that G/H is finite and cyclic. Moreover, suppose that the following condition holds.

HYPOTHESIS 4.1. *We have a representation*

$$\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{F}}(X) \simeq \mathrm{GL}_2(\mathbb{F})$$

such that $\mathrm{Tr}\ \rho(g) = 0$ *whenever* gH *generates* G/H.

LEMMA 4.2. *With the above hypothesis,* $[G : H]$ *is even.*

PROOF. We shall say that $g \in G$ is *special* if gH is a generator of G/H. For special g, we see by Hypothesis 4.1 that

$$\mathrm{Tr}\ \rho(g) = 0.$$

Hence,

$$\rho(g^2) = -\det \rho(g).$$

But if $[G : H]$ is odd, then g^2 is also special. Again, by Hypothesis 4.1, this would imply that

$$\mathrm{Tr}\ \rho(g^2) = 0$$

which is a contradiction. □

Let J denote the unique subgroup of G which contains H and is of index 2 in G, its existence and uniqueness being assured by Lemma 4.2 and the cyclicity of G/H.

LEMMA 4.3. *We have* $\rho(J)$ *is abelian, and contained in a Borel subgroup of* $\mathrm{GL}_2(\mathbb{F})$.

PROOF. We observe that for any special $g \in G$, the subgroup J is generated by H and g^2. We claim that for any element $g' \in G \setminus J$, we have $\mathrm{Tr}\ \rho(g') = 0$. Indeed, write $g' = gx$, for some special g and some $x \in J$. Since we can write $x = g^{2a}h$ for some $h \in H$ and some integer $a \geq 0$, we find that

$$\mathrm{Tr}\ \rho(g') = \mathrm{Tr}\ \rho((g^2)^a gh) = (-\det \rho(g))^a\ \mathrm{Tr}\ \rho(gh) = 0.$$

Now consider the representation

$$\overline{\rho} : G \longrightarrow \mathrm{Aut}_{\overline{\mathbb{F}}}(\overline{X}) \simeq \mathrm{GL}_2(\overline{\mathbb{F}})$$

where $\overline{\mathbb{F}}$ denotes an algebraic closure of $\mathbb{F}$ and $\overline{X} = X \otimes_{\mathbb{F}} \overline{\mathbb{F}}$. Consider the $\overline{\mathbb{F}}$ algebra $R = \overline{\mathbb{F}}[\overline{\rho}(J)]$. Fix a special g. By the observation of the previous paragraph, we have

$$\mathrm{Tr}\ R\rho(g) = 0. \tag{3}$$

Moreover,

$$\rho(g^2) \text{ is a scalar.} \tag{4}$$

These conditions imply that R is commutative. Indeed, by (4), there is a basis of X such that $\rho(g)$ has the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$$

for some $\alpha \in \overline{\mathbb{F}}$. If

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\overline{\mathbb{F}})$$

is a general element of R, then (3) implies that $a = d$. Then, there are several possibilities:

(a) R consists of scalars ($\dim R = 1$)
(b) for all $x \in R$, we have $c = 0$ but $\dim R > 1$:

$$R \subseteq \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a, b \in \overline{\mathbb{F}} \right\}$$

(c) for all $x \in R$, we have $b = 0$ but $\dim R > 1$:

$$R \subseteq \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix}, a, c \in \overline{\mathbb{F}} \right\}$$

(d) there exists an $x \in R$ for which $b \neq 0$ and $c \neq 0$. In this case $\dim R > 1$ and

$$R \subseteq \left\{ \begin{pmatrix} a & c\nu \\ c & a \end{pmatrix}, a, c \in \overline{\mathbb{F}} \right\}$$

for some element $\nu \in \overline{\mathbb{F}}^{\times}$.

In the last three cases, $\dim R = 2$. In all cases, R is commutative and $\rho(J)$ is contained in a Borel subgroup. □

Next, we give a criterion for $\rho(J)$ to be contained in a Cartan subgroup (case (a) or (d) above). Let ω denote the non-trivial character of G/J. We shall also think of it as a character of G.

PROPOSITION 4.4. *Suppose that there does not exist an $\overline{\mathbb{F}}^{\times}$ valued character η of G such that $\det \rho = \omega\eta^2$. Then $\rho(J)$ is contained in a Cartan subgroup C of $\mathrm{Aut}_{\mathbb{F}}(X)$. Furthermore, $\rho(G)$ is contained in the normalizer of C but not in C itself.*

PROOF. This is modelled on (Momose [**12**], Lemma 1.2). By Lemma 4.3, we know that there is a line $\overline{V}$ left stable by $\overline{\rho}(J)$. Suppose that

$$\overline{\rho}(G)\overline{V} \ = \ \overline{V}.$$

Then, the semisimplification of $\overline{\rho}$ is given by two characters ν and η such that

$$\nu\eta \ = \ \det \ \overline{\rho}$$

$$(\nu + \eta)(g) \ = \ 0 \text{ if } g \in G \setminus J.$$

From the second relation, it follows that

$$\nu/\eta \ = \ \omega.$$

Then, the first relation implies that

$$\omega\eta^2 \ = \ \det \ \rho$$

contrary to hypothesis. Thus,

$$\overline{\rho}(G)\overline{V} \ \neq \ \overline{V}.$$

It follows that for any $g \in G \setminus J$, we have a non-trivial decomposition

$$\overline{X} \ = \ \overline{V} \ \oplus \ \overline{\rho}(g)\overline{V}.$$

If we choose another element $g' \in G \setminus J$, then

$$\overline{\rho}(g')\overline{V} \;=\; \overline{\rho}(g)\overline{V}.$$

It follows that $\overline{\rho}(J)$ is contained in the Cartan subgroup

$$C \;=\; \mathrm{Aut}_{\overline{F}}(\overline{V}) \;\times\; \mathrm{Aut}_{\overline{F}}(\overline{\rho}(g)\overline{V}).$$

Since any $g' \in G \setminus J$ interchanges $\overline{V}$ and $\overline{\rho}(g)\overline{V}$, it follows that $\overline{\rho}(G)$ is contained in the normalizer of C but not in C itself. This proves the result. □

Throughout the rest of this section, we shall assume that the hypothesis of Proposition 4.4 holds. Thus, we get two characters

$$\phi_1, \phi_2 : J \;\longrightarrow\; \overline{\mathbb{F}}^{\times}$$

and an $\overline{\mathbb{F}}$ basis of $\overline{X}$ such that ρ restricted to J has the form

$$\begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix}.$$

Moreover, for any $\delta \in G \setminus J$, we have $\rho(\delta)$ has the form

$$\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$$

for some $x, y \in \overline{\mathbb{F}}^{\times}$. Now let us fix one $\delta \in G \setminus J$.

COROLLARY 4.5. *For any $j \in J$, we have*

$$\phi_1(j)\phi_1(\delta^{-1}j\delta) \;=\; \phi_2(j)\phi_2(\delta^{-1}j\delta) \;=\; \det\ \rho(j).$$

PROOF. We have

$$\det \rho(j) \;=\; \det\ \overline{\rho}(j)$$

and

$$\begin{pmatrix} \phi_1(\delta^{-1}j\delta) & 0 \\ 0 & \phi_2(\delta^{-1}j\delta) \end{pmatrix} \;=\; \overline{\rho}(\delta^{-1}j\delta) \;=\; \overline{\rho}(\delta)^{-1}\overline{\rho}(j)\overline{\rho}(\delta) \;=\; \begin{pmatrix} \phi_2(j) & 0 \\ 0 & \phi_1(j) \end{pmatrix}.$$

Thus,

$$\det\ \rho(j) \;=\; \phi_1(j)\phi_2(j) \;=\; \phi_1(j)\phi_1(\delta^{-1}j\delta) \;=\; \phi_2(j)\phi_2(\delta^{-1}j\delta).$$

□

Let G' (resp. J') denote the commutator subgroup of G (resp. J). We view ϕ_1 and ϕ_2 as characters of the quotient J/J'. Consider the composite homomorphisms

$$\Phi_i : G \;\longrightarrow\; G/G' \;\longrightarrow J/J' \;\longrightarrow \overline{\mathbb{F}}^{\times}$$

for $i = 1, 2$. Here, the rightmost map is ϕ_i and the middle map is the transfer homomorphism Ver (see Serre [**20**], p. 120) which in our case can be made quite explicit:

$$\mathrm{Ver}(g \bmod G') \;=\; \begin{cases} g^2 \bmod J' & \text{if } g \notin J \\ g\delta g\delta^{-1} \bmod J' & \text{if } g \in J. \end{cases}$$

COROLLARY 4.6. *For any $g \in G$, we have*

$$\Phi_1(g) \;=\; \Phi_2(g) \;=\; \omega(g) \det\ \rho(g).$$

PROOF. If $g \notin J$, then

$$\mathrm{Tr}\rho(g) \;=\; 0.$$

Thus,

$$\rho(g^2) \;=\; -\det\rho(g).$$

If $g \in J$, we have by Corollary 4.5,

$$\phi_i(\mathrm{Ver}(g \bmod G')) \;=\; \det\;\rho(g)$$

for $i = 1, 2$. This proves the result. □

COROLLARY 4.7. *$\rho(G)$ is non-abelian.*

PROOF. Since conjugation by $\rho(\delta)$ interchanges the eigenspaces of C, we see that $\rho(G)$ is abelian if and only if $\phi_1 = \phi_2$. Suppose $\rho(G)$ is abelian. Then ϕ_1 can be extended to a character ϕ (say) of G, This character satisfies

$$\Phi_1 \;=\; \Phi_2 \;=\; \phi^2.$$

Thus, by Corollary 4.6, we have

$$\det\rho \;=\; \omega\phi^2.$$

This contradicts the hypothesis of Proposition 4.4. □

PROPOSITION 4.8. *Let M denote the quadratic field corresponding to ω. The splitting field of $\rho_{\mathrm{Gal}(\overline{K}/M)}$ is an abelian extension of M which is at most tamely ramified at p.*

PROOF. We have already seen that the splitting field is abelian as $\rho(\mathrm{Gal}(\overline{K}/M))$ is contained in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F})$. Such a subgroup has order $(q-1)^2$ or q^2-1 depending on whether it is split or not, where q is the cardinality of $\mathbb{F}$. In particular, the order of $\rho(\mathrm{Gal}(\overline{K}/M))$ is prime to p. □

REMARK 4.9. In section 6 we shall find examples of representations ρ satisfying the hypotheses in this section, as follows. We consider a triple (K, A, E) of type (T')which has a non-trivial twist γ and we associate an ideal S_γ of E. Then, the representation ρ is obtained by studying the Galois action on the S_γ-division points. In the next section, we abstractly define and develop the properties of S_γ.

5. The ideal $S_n(E/F)$

Let E/F be a cyclic Galois extension of (local or global) fields. Let γ be a generator of $\mathrm{Gal}(E/F)$, and let ζ be a root of unity in E such that $\mathrm{Norm}_{E/F}\zeta = 1$. (Note that ζ may or may not be in F). Let $\mathfrak{b}(\gamma, \zeta)$ be the ideal of E generated by the set

$$\mathfrak{b}_0(\gamma, \zeta) \;=\; \{x \in \mathcal{O}_E :\; x^\gamma \;=\; \zeta x\}.$$

Our assumption on ζ implies that this set contains non-zero elements.

DEFINITION 5.1. *$S(\gamma, \zeta)$ is the radical of $\mathfrak{b}(\gamma, \zeta)$.*

REMARK 5.2. Whenever we write $S(\gamma, \zeta)$ or $\mathfrak{b}(\gamma, \zeta)$, with some root of unity ζ, we shall be tacitly assuming that $\mathrm{Norm}_{E/F}\zeta = 1$.

REMARK 5.3. In the case that E is a CM-field, γ is complex conjugation and $\zeta = -1$, this ideal was considered by Shimura [**22**], [**23**] and it is this case that is the motivation for this work.

We begin by developing some of the elementary properties of this ideal.

PROPOSITION 5.4. (1) *If ζ and η are two primitive n-th roots of unity, then*

$$S(\gamma,\zeta) \;=\; S(\gamma,\eta).$$

(2) *If $\tau \in \mathrm{Aut}(E/\mathbb{Q})$, then*

$$S(\gamma,\zeta)^{\tau} \;=\; S(\tau^{-1}\gamma\tau,\zeta^{\tau}).$$

PROOF. We can write $\eta = \zeta^i$ for some positive integer i satisfying $(i,n) = 1$. Then, we clearly have

$$\mathfrak{b}_0(\gamma,\zeta)^i \;\subseteq\; \mathfrak{b}_0(\gamma,\eta).$$

By symmetry, for some j, we have

$$\mathfrak{b}_0(\gamma,\eta)^j \;\subseteq\; \mathfrak{b}_0(\gamma,\zeta).$$

Thus, the radicals of $\mathfrak{b}(\gamma,\zeta)$ and $\mathfrak{b}(\gamma,\eta)$ are equal, proving the first assertion. If $x \in \mathfrak{b}_0(\gamma,\zeta)$, then

$$(x^{\tau})^{\tau^{-1}\gamma\tau} \;=\; x^{\gamma\tau} \;=\; \zeta^{\tau}x^{\tau}$$

and so

$$x^{\tau} \;\in\; \mathfrak{b}_0(\tau^{-1}\gamma\tau,\zeta^{\tau}).$$

Conversely, if $x \in \mathfrak{b}_0(\tau^{-1}\gamma\tau,\zeta^{\tau})$, then

$$(x^{\tau^{-1}})^{\gamma} \;=\; (x^{\tau^{-1}\gamma\tau})^{\tau^{-1}} \;=\; (\zeta^{\tau}x)^{\tau^{-1}} \;=\; \zeta x^{\tau^{-1}}.$$

Thus, $x^{\tau^{-1}} \;\in\; \mathfrak{b}_0(\gamma,\zeta)$. This shows that

$$\mathfrak{b}_0(\gamma,\zeta)^{\tau} \;=\; \mathfrak{b}_0(\tau^{-1}\gamma\tau,\zeta^{\tau}).$$

It follows that the corresponding equality also holds for $\mathfrak{b}$ and its radical S, proving the second assertion. □

PROPOSITION 5.5. *Let m be the order of γ, and r a positive integer with $(r,m) = 1$. Let ζ be a primitive n-th root of 1 in E. Then*

$$S(\gamma^r,\zeta) \;=\; S(\gamma,\zeta).$$

PROOF. Let i be the unique integer satisfying $0 \le i < n$ with $\zeta^{\gamma} = \zeta^i$. Let

$$j = 1 + i + i^2 + \cdots + i^{r-1}.$$

If for an $x \in \mathcal{O}_E$, we have

$$x^{\gamma} = \zeta x,$$

then

$$x^{\gamma^r} \;=\; \zeta^j x.$$

Thus

$$S(\gamma,\zeta) \;\subseteq\; S(\gamma^r,\zeta^j).$$

We claim that $(j,n) = 1$. If this were so, then

$$S(\gamma^r,\zeta^j) \;=\; S(\gamma^r,\zeta)$$

by Proposition 5.4. Thus

$$S(\gamma,\zeta) \;\subseteq\; S(\gamma^r,\zeta).$$

And then, by symmetry, it follows that equality holds. To complete the proof, it only remains to check that $(j,n) = 1$. For this, we note that

$$i^r - 1 = j(i-1)$$

and

$$(i^m - 1, i^r - 1) \;=\; i^{(m,r)} - 1 \;=\; i - 1.$$

But

$$1 + i + i^2 + \cdots + i^{m-1} \;\equiv\; 0 \pmod{n}$$

since $\gamma^m = 1$. Thus, (n, j) divides $((i^m - 1)/(i - 1), j) = 1$. □

DEFINITION 5.6. *We write $S_n(E/F)$ for $S(\gamma, \zeta)$ where γ is* any *generator of* $\mathrm{Gal}(E/F)$ *and ζ is* any *primitive n-th root of unity such that $Norm_{E/F}(\zeta) = 1$.*

By Propositions 5.4 and 5.5 this is well-defined.

In the next few results, we relate $S_n(E/F)$ to the different of E/F.

PROPOSITION 5.7. *Let $\alpha \in \mathcal{O}_E$ be such that $\alpha^\gamma \;=\; \zeta\alpha$. Then*

$$S_n(E/F) \;=\; \sqrt{S_n(F(\alpha)/F)}\mathcal{O}_E.$$

PROOF. If $\beta \in \mathcal{O}_E$ and $\beta^\gamma \;=\; \zeta\beta$, then $\beta\alpha^{-1} \in F$. Thus,

$$\mathfrak{b}_0(\gamma, \zeta) \;\subseteq\; F(\alpha)$$

and $\mathfrak{b}(\gamma, \zeta)$ is the lifting to E of the ideal in $F(\alpha)$ generated by $\mathfrak{b}_0(\gamma, \zeta)$. □

REMARK 5.8. The field $F(\alpha)$ above depends only on n and the extension E/F, but not on the choice of γ, ζ or the choice of α in $\mathfrak{b}_0(\gamma, \zeta)$. We shall denote this field E' for short, when no ambiguity can arise. In general, it is a proper subfield of E. For example, let $E \;=\; \mathbb{Q}(\zeta_5)$ and $F = \mathbb{Q}$, where ζ_5 is a primitive 5-th root of unity. Then $\mathrm{Gal}(E/F)$ is generated by the automorphism which maps ζ_5 to ζ_5^2. Now, $\sqrt{5} \in E$ and $(\sqrt{5})^\gamma \;=\; -\sqrt{5}$. Hence, $E' \;=\; \mathbb{Q}(\sqrt{5})$. In this case,

$$S_2(E/F) = \sqrt{S_2(\mathbb{Q}(\sqrt{5})/\mathbb{Q})}\mathcal{O}_E \;=\; \sqrt{\sqrt{5}\mathcal{O}_E} \;=\; (1 - \zeta_5)\mathcal{O}_E.$$

DEFINITION 5.9. (1) *If T is a number field and R is a finite extension of T, we denote by $\mathfrak{d}(R/T)$ the different of R/T. It is an ideal of $\mathcal{O}_R$.*

(2) *If I is an ideal of T and r is an integer, $I^{\text{prime to } r}$ denotes the ideal $\prod \mathfrak{p}^{v_\mathfrak{p}}$ where the product is over prime divisors of I which do not divide $r\mathcal{O}_E$ and $v_\mathfrak{p}$ is the exact exponent of $\mathfrak{p}$ in I. We shall also write I^{odd} when $r = 2$.*

(3) *If r is a positive integer, ζ_r denotes a primitive r-th root of unity.*

(4) *The degree $[E : F]$ will be denoted by m.*

PROPOSITION 5.10. *We have*

$$S_n(E/F) \;\supseteq\; \sqrt{\mathfrak{d}(E'/F)}\mathcal{O}_E.$$

PROOF. By Proposition 5.7, we may assume that $E \neq E'$. Let $\mathfrak{p}$ be a prime of E and suppose that $\mathfrak{p} \nmid \mathfrak{d}(E/F)$. We want to show that $\mathfrak{p} \nmid S_n(E/F)$. For this, it is enough to produce an element $y \in \mathcal{O}_E$ such that $y^\gamma \;=\; \zeta_n y$ and $y \notin \mathfrak{p}$. Since the inertia group at $\mathfrak{p}$ is trivial, the ring homomorphisms

$$\chi_i : \mathcal{O}_E \;\longrightarrow^{\gamma^i}\; \mathcal{O}_E \;\longrightarrow\; \mathcal{O}_E/\mathfrak{p}$$

are distinct. Suppose we are given $a_0, a_1, \cdots, a_{m-1} \in \mathcal{O}_E$, not all zero modulo $\mathfrak{p}$. By mimicing the proof of independence of characters, we can show that there is an $x \in \mathcal{O}_E$ such that

$$(a_0\chi_0 \;+\; a_1\chi_1 \;+\; \cdots \;+\; a_{m-1}\chi_{m-1})(x) \not\equiv\; 0 \pmod{\mathfrak{p}}.$$

In particular, there is an integer $x \in E$ such that

$$y \;=\; \sum_{j=0}^{m-1} \zeta_n^{-(1+\gamma+\gamma^2\,+\,\cdots\,+\,\gamma^{j-1})}\gamma^j x \;\not\equiv\; 0 \pmod{\mathfrak{p}}.$$

Here, the exponent of ζ_n is interpreted as 1 for $j = 0$. Now,

$$y^\gamma \;=\; \zeta_n y$$

as is readily verified. □

PROPOSITION 5.11. *We have*

$$S_n(E/F)^{\text{prime to } n} \;=\; \sqrt{\mathfrak{d}(E'/F)^{\text{prime to } n}}\mathcal{O}_E.$$

PROOF. By Proposition 5.10, it is enough to prove that

$$S_n(E/F)^{\text{prime to } n} \;\subseteq\; \sqrt{\mathfrak{d}(E'/F)^{\text{prime to } n}}\mathcal{O}_E.$$

By Proposition 5.7, we may suppose that $E = E'$. Choose an element

$$\alpha \in \mathfrak{b}_0(\gamma, \zeta_n).$$

Then α is an integral generator of E/F. Thus,

$$(\alpha - \alpha^\gamma)\cdots(\alpha - \alpha^{\gamma^{m-1}}) \;\in \mathfrak{d}(E/F).$$

This expression simplifies to

$$\alpha^{m-1}(1-\zeta_n)(1-\zeta_n^{1+\gamma})\cdots(1-\zeta_n^{1+\gamma+\gamma^2+\cdots+\gamma^{m-2}}) \;\in\; \mathfrak{d}(E//F).$$

Thus,

$$\alpha \in \sqrt{\mathfrak{d}(E/F)^{\text{prime to } n}}\mathcal{O}_E.$$

□

PROPOSITION 5.12. *We have*

$$S_n(E/F) \;\subseteq\; \sqrt{\mathfrak{d}(E'/F(\zeta_n))^{\text{prime to } m}}\mathcal{O}_E.$$

PROOF. let $e = [E' : F]$. Suppose we show that

$$S_n(E'/F) \;\subseteq\; \sqrt{\mathfrak{d}(E'/F(\zeta_n))^{\text{prime to } e}}\mathcal{O}_E.$$

Then, since e divides $m = [E : F]$, we get the stated result. Write

$$d = [F(\zeta_n) : F].$$

Then $\mathrm{Gal}(E'/F(\zeta_n))$ is generated by $\tau = \gamma^d$. In particular, for any

$$\alpha \in \mathfrak{b}_0(\gamma, \zeta_n),$$

we have

$$\alpha^\tau \;=\; \zeta_n^{1+\gamma+\cdots\,+\,\gamma^{d-1}}\alpha$$

and let us write the right hand side as $\eta\alpha$. It is easily checked that η is a primitive f-th root of unity, where $f = e/d$. Since α is an integral generator of $E'/F(\zeta_n)$, we have

$$(\alpha - \alpha^\tau)\cdots(\alpha - \alpha^{\tau^{f-1}}) \;\in \mathfrak{d}(E'/F(\zeta_n)).$$

But this element is equal to

$$\alpha^{f-1}(1-\eta)(1-\eta^{1+\tau})\cdots(1-\eta^{1+\tau+\tau^2+\cdots+\tau^{f-2}}).$$

Hence,

$$\alpha \in \sqrt{\mathfrak{d}(E'/F(\zeta_n))^{\text{prime to } e}}\mathcal{O}_E.$$

proving the result. □

REMARK 5.13. Without a further restriction, it is *not* true that

$$S_n(E/F) \subseteq \sqrt{\mathfrak{d}(E'/F)^{\text{prime to } m}}\mathcal{O}_E.$$

For example, take $E = \mathbb{Q}(\zeta_3)$, $F = \mathbb{Q}$ *and* γ *to be complex conjugation. Then* $S_3(E/F) = 1$ *since*

$$\zeta_3^\gamma = \zeta_3^2 = \zeta_3\zeta_3.$$

But

$$\mathfrak{d}(E/F)^{\text{prime to } 2} = \sqrt{-3}\mathcal{O}_E.$$

Next, we give some necessary conditions for $S_n(E/F)$ to be non-trivial.

PROPOSITION 5.14. *Let* i *be an integer such that* $0 < i < n$ *and* $\zeta^\gamma = \zeta^i$. *Let* $d = (i-1, n)$. *If* $(d, n/d) = 1$, *then*

$$S_n(E/F) = S_d(E/F).$$

In particular, if $d = 1$, $S_n(E/F) = 1$.

PROOF. Write $n = dn_0$. Then

$$\mathfrak{b}_0(\gamma, \zeta_n)^{n_0} \subseteq \mathfrak{b}_0(\gamma, \zeta_d),$$

and so

$$S_n(E/F) \subseteq S_d(E/F).$$

Similarly,

$$\mathfrak{b}_0(\gamma, \zeta_d)\mathfrak{b}_0(\gamma, \zeta_{n_0}) \subseteq \mathfrak{b}_0(\gamma, \zeta_{n/(n_0,d)}),$$

and so

$$S_d(E/F)S_{n_0}(E/F) \subseteq S_{n/(n_0,d)}(E/F) = S_n(E/F).$$

Now let $i - 1 = da$. Then

$$\zeta_n^\gamma = \zeta_n^{da}\zeta_n = \zeta_{n_0}^a\zeta_n.$$

Since $(a, n_0) = 1$, we have

$$\zeta_n \in S(\gamma, \zeta_{n_0}^a) = S(\gamma, \zeta_{n_0}) = S_{n_0}(E/F).$$

Hence, $S_{n_0}(E/F) = 1$ and the result follows. □

COROLLARY 5.15. *If* $(m, n) = 1$, *then* $S_n(E/F) = 1$.

PROOF. Let i be as in Proposition 5.14. Then

$$1 + i + \cdots + i^{m-1} \equiv 0 \pmod{n}.$$

But also

$$1 + i + \cdots + i^{m-1} \equiv m \pmod{(i-1)}.$$

Thus, $(i-1, n)$ divides (m, n). Now the result follows from Proposition 5.14. □

Finally, we determine the ideal $S_n(E/F)$ when $m = 2$.

PROPOSITION 5.16. *Suppose that* γ *has order* 2 *(that is,* $m = 2$*). Then, we have the following:*

(1) *If* n *is odd,* $S_n(E/F) = 1$.
(2) *If* $n = 2n_0$ *with* n_0 *odd, then* $S_n(E/F) = S_2(E/F)$.

(3) *If* $4|n$ *and* n *is not a power of* 2*, then* $S_n(E/F) = S_2(E/F) = 1$.
(4) *If* n *is a power of* 2 *but* $n \neq 2$*, then* $S_2(E/F) = 1$ *and* $S_n(E/F)$ *divides* $(1 - \zeta_n)$.

PROOF. Let i be as above, that is $\zeta_n^\gamma = \zeta_n^i$. Since $\gamma^2 = 1$, we have

$$\zeta^{1+i} = 1.$$

If $i = 1$, then $n = 2$ and there is nothing to prove. So assume from now on that $i \equiv -1 \pmod{n}$ and $i \neq 1$. For the first assertion, we have $(m, n) = (2, n) = 1$ and so by Corollary 5.15, $S_n(E/F) = 1$. For the second assertion, we have $(i-1, n) = 2$. Then by Proposition 5.14, we have

$$S_n(E/F) = S_2(E/F).$$

For any even n, we see that

$$\mathfrak{b}(\gamma, \zeta_n)^{n/2} \ \subseteq \ \mathfrak{b}(\gamma, -1).$$

Thus,

$$S_n(E/F) \ \subseteq S_2(E/F).$$

On the other hand, $S_{n/2}(E/F) = 1$ since $\zeta_n \in \mathfrak{b}_0(\gamma, \zeta_{n/2}^{-1})$ from the relation

$$\zeta_n^\gamma \ = \ \zeta_n^{-2}\zeta_n \ = \ \zeta_{n/2}^{-1}\zeta_n.$$

Thus, if $4|n$, we find that $S_2(E/F) = 1$. In particular, this proves part of the third and part of the fourth assertions. To complete the proof, write $n_0 = n/4$ and consider

$$y \ = \ \zeta_n^{n_0 - 1}(1 - \zeta_n).$$

Then

$$y^\gamma \ = \ (\zeta_n^{n_0-1})^i \ - \ \zeta_n^{n_0 i} \ = \ \zeta_n^{1-n_0} \ - \ \zeta_n^{-n_0} \ = \ -\zeta_n^{n_0+1} + \zeta_n^{n_0} \ = \ \zeta_n y.$$

Thus,

$$y \in \mathfrak{b}(\gamma, \zeta_n)$$

and

$$(1 - \zeta_n) \in S_n(E/F).$$

If n is a power of 2 but not equal to 2, then $1 - \zeta_n$ is a unit. This completes the proof of the third assertion and also proves the fourth assertion. □

COROLLARY 5.17. *Suppose that* γ *has order* 2*. Then*

$$S_n(E/F) = 1 \text{ unless } n = 2q \text{ with } q = 1 \text{ or a prime power.}$$

If q *is odd, then*

$$S_n(E/F) \ = \ S_2(E/F)$$

and

$$S_2(E/F)^{\text{odd}} \ = \ \mathfrak{d}(E/F)^{\text{odd}}$$

where $\mathfrak{d}(E/F)$ *is the different of* E/F*. Moreover, this different divides* $(1 - \zeta_q)\mathcal{O}_E$.

6. Applications to Abelian varieties

We now use the results of the first three sections to construct abelian extensions of number fields. We preserve the notation of section 3. Thus (K, A, E) is a triple of type (T'). We suppose that $\Gamma(A) \neq \{1\}$. We have the following associated notation:

- Π : the set of places of K where A has bad reduction
- P: the trace field
- γ: a non-trivial element of $\Gamma(A)$
- R: the subfield of P fixed by γ
- χ: the twisting character corresponding to γ.

The following elementary lemma is crucial in what follows.

LEMMA 6.1. *If the order n of χ is odd, then $S_n(P/R) = \{1\}$.*

PROOF. If n is odd, then χ^2 also has order n. Let v be a prime of K, not dividing the conductor of χ or ϵ, such that $\chi^2(\mathrm{Frob}_v)$ is a primitive n-th root of unity. Then, from the relation

$$\epsilon^\gamma = \epsilon\chi^2,$$

we deduce that

$$\epsilon(\mathrm{Frob}_v) \in S(\gamma, \chi^2(\mathrm{Frob}_v)).$$

□

Now we introduce the rest of our notation and assumptions:

- n: the order of χ; we assume n is even, say $n = 2q$
- S: the ideal $(S_n(P/R)\mathcal{O}_E)^{\mathrm{odd}}$ which we assume is not the unit ideal
- $\mathfrak{p}$: a prime divisor of S
- $\mathbb{F}$: the residue field $\mathcal{O}_E/\mathfrak{p}$ of $\mathfrak{p}$
- p: the characteristic of $\mathbb{F}$; it is necessarily odd
- $\mathcal{L}$: an $\mathcal{O}_\mathfrak{p}[G_K]$-stable lattice in $V_\mathfrak{p}(A) = V_p(A) \otimes_{E\otimes\mathbb{Q}_p} E_\mathfrak{p}$, such lattices exist (see below).
- X: the two dimensional $\mathbb{F}$ vector space $\mathcal{L}/\mathfrak{p}\mathcal{L}$
- ω: the character χ^q
- M: the fixed field of $\ker \omega$
- M_ϵ: the fixed field of $\ker \epsilon$
- $\tilde{\omega}$, $\tilde{\epsilon}$, $\tilde{\chi_p}$: the reduction of the appropriate character modulo $\mathfrak{p}$.

REMARK 6.2. *As G_K is compact and $\rho_\mathfrak{p}$ is continuous, there always exist $\mathcal{O}_\mathfrak{p}[G_K]$ stable lattices.*

REMARK 6.3. *The fact that X is two dimensional over $\mathbb{F}$ follows from $(T1')$.*

Since E acts K-rationally on A, the action of G_K on X is $\mathbb{F}$-linear. Thus, we get a representation

$$\rho : G_K \longrightarrow \mathrm{Aut}_\mathbb{F}(X).$$

LEMMA 6.4. *Let $K(X)$ be the fixed field of $\ker \rho$. Then $M \subseteq K(X)$ and $K(X)/M$ is an abelian extension.*

PROOF. If we let $G = G_K$, $H = \ker \chi$, and ρ as above, then it is clear that H is normal and G/H is finite and cyclic. Moreover, the Hypothesis 4.1 is satisfied. Indeed, let $g \in G$ be such that gH generates G/H. There are infinitely many

primes v of K so that $g = \mathrm{Frob}_v$. For such v, we see that $\chi(\mathrm{Frob}_v)$ is a primitive n-th root of unity. The relation

$$a_v^\gamma \;=\; a_v \chi(\mathrm{Frob}_v)$$

implies that

$$a_v \;\equiv\; 0 \bmod \mathfrak{p}.$$

Thus, $\mathrm{Tr}\ \rho(g) = 0$. It follows from Lemma 4.3 that $\rho(J)$ is abelian, where $J = \ker(\omega)$. Furthermore, if $g \in G \backslash J$ then $\mathrm{Tr}\ \rho(g) = 0$. If $g \in \ker \rho$, then $\mathrm{Tr}\ \rho(g) = 2 \neq 0$ as p is odd. Therefore,

$$\ker\ \rho \;\subseteq\; J$$

and the Lemma follows. □

THEOREM 6.5. *The extension $K(X)/M$ is unramified outside of the primes of M which divide p or an element of Π. Suppose that at least one of the following holds:*

(i) *K has a real place ∞ and ω and ϵ agree on the inertia group at that place*
(ii) *K has a place $\mathfrak{q}$ over p of odd local degree $[K_\mathfrak{q} : \mathbb{Q}_p]$ such that ω and ϵ agree on an inertia group over $\mathfrak{q}$.*

Then,

(1) *$\mathrm{Gal}(K(X)/M)$ is contained in a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F})$.*
(2) *$K(X)/K$ is Galois and non-abelian. Its group is contained in the normalizer of C.*
(3) *If* (i) *above holds, then in fact ω and ϵ are unramified at the place ∞.*
(4) *If* (ii) *above holds, then $\omega(-1) = \epsilon(-1) = 1$ where -1 denotes an element of order 2 in any inertia group over $\mathfrak{q}$.*

PROOF. The $\mathfrak{p}$-adic representation of G_K on $V_\mathfrak{p}(A)$ is unramified outside of the primes of K which divide p or lie in Π. The first assertion follows from this.

Suppose there exists a character

$$\eta : G_K \;\longrightarrow\; \overline{\mathbb{F}}^\times$$

such that

$$\tilde{\omega}\eta^2 \;=\; \tilde{\epsilon}\tilde{\chi}_p. \tag{5}$$

It remains to show that either of the assumptions (i) or (ii) contradict this. Then (1) and (2) will follow from Proposition 4.4 and Corollary 4.7.

If (i) holds, denote by c the non-trivial element in the inertia group at ∞. Then Lemma 6.1 implies that

$$\tilde{\omega}(c) \;=\; \tilde{\omega}(c)\eta^2(c) \;=\; \tilde{\epsilon}(c)\tilde{\chi}_p(c) \;=\; \tilde{\omega}(c)\tilde{\chi}_p(c).$$

This implies that $\tilde{\chi}_p(c) = 1$, which is a contradiction.

If (ii) holds, let $I_\mathfrak{q}$ denote any inertial subgroup (of G_K) over $\mathfrak{q}$. Now ω and ϵ agree on on e, and hence on any, such subgroup. Let θ_{p-1} denote the "fundamental character of level 1", that is the composite map

$$I_\mathfrak{q} \;\simeq\; \mathcal{O}_\mathfrak{q}^\times \;\longrightarrow\; \mathbb{Z}_p^\times \;\longrightarrow\; \mathbb{F}_p^\times \;\hookrightarrow\; \mathbb{F}^\times,$$

where the first arrow is the Norm map and the second is reduction modulo p. By Serre ([**21**], Proposition 8), we have

$$\tilde{\chi}_p \;=\; \theta_{p-1}^e$$

where $e = e(K_{\mathfrak{q}}/\mathbb{Q}_p)$. Let $p^n = |\mathcal{O}_K/\mathfrak{q}|$. Then, by hypothesis, n and e are odd. Thus,

$$\chi_p(-1) = (-1)^{(1+p+\cdots+p^{n-1})e} = (-1)^{ne} = -1.$$

This contradicts (5) and proves (1) and (2).

Now let a be any element of order 2 in G_K. Suppose that $\tilde{\chi}_p(a) = -1$ and $\tilde{\omega}(a) = \tilde{\epsilon}(a)$. Then in fact

$$\tilde{\omega}(a) = \tilde{\epsilon}(a) = +1.$$

Indeed, otherwise, $a \notin \mathrm{Gal}(\overline{K}/M)$. Then by Corollary 4.6, we have

$$1 = \rho(a^2) = \tilde{\omega}(a)\tilde{\epsilon}(a)\tilde{\chi}_p(a) = -1.$$

This is a contradiction as $p \neq 2$. This proves (3) and (4). □

Remark 6.6. It follows from the Brauer-Nesbitt theorem, that the semisimplification of $\rho|_J$ is independent of the choice of lattice. In particular, this applies if $\rho(J)$ is contained in a Cartan subgroup. Thus in this case, the extension $K(X)/M$ is independent of the choice of lattice. We call X the G_K-module associated to $\mathfrak{p}$.

7. The p-part of the conductor

In this section, we consider the ramification over p in the abelian extensions constructed in Section 6. We preserve the notation and hypotheses of that section. In addition, we shall assume throughout this section that the following hypothesis holds.

Hypothesis 7.1. $\mathrm{Gal}(K(X)/M)$ *is contained in a Cartan subgroup* C *of* $\mathrm{GL}_2(\mathbb{F})$ *and* $\mathrm{Gal}(K(X)/K)$ *is non-abelian.*

Thus, we get two characters

$$\phi_1,\ \phi_2 :\ \mathrm{Gal}(K(X)/M) \longrightarrow \overline{\mathbb{F}}^{\times}$$

such that

$$\overline{\phi}|_{\mathrm{Gal}(\overline{K}/M)} = \phi_1 \oplus \phi_2.$$

Proposition 7.2. *(cf. Shimura* [**22**]*, Corollary 7.3.1) Let* N *be the compositum of* M *and* M_ϵ*. Then,* $N(\zeta_p) \subsetneq N(X)$*. If* $([N : M], p-1) = 1$*, then* $M(\zeta_p) \subsetneq K(X)$*.*

Proof. Take an element $g \in \mathrm{Gal}(\overline{K}/N(X))$. Then $\rho(g) = 1$ and

$$\tilde{\chi}(g) = \det \rho(g) = 1.$$

This implies that $\zeta_p \in N(X)$. If $N(\zeta_p) = N(X)$, then $N(X)$ (and hence also $K(X)$) is abelian over K. This contradicts Hypothesis 7.1. Now, if $g \in \mathrm{Gal}(\overline{K}/K(X))$, then

$$\tilde{\epsilon}(g)\tilde{\chi}(g) = 1.$$

Again, by Hypothesis 7.1, $M(\zeta_p) \neq K(X)$. □

In the next result, we assume that $K = \mathbb{Q}$. We shall calculate the restriction of the characters ϕ_1, ϕ_2 to an inertia group over p using the methods of Ohta [**13**] and Momose [**12**]. By class field theory, ϕ_1 and ϕ_2 give two idèle class characters

$$\psi_1,\ \psi_2\ : M_{\mathbb{A}}^{\times} \longrightarrow \overline{\mathbb{F}}^{\times}.$$

Let v be a place of M unramified in $\mathbb{Q}(X)$.

REMARK 7.3. We assume that the reciprocity map

$$M_{\mathbb{A}}^{\times} \longrightarrow \mathrm{Gal}(\mathbb{Q}(X)/M)$$

sends a uniformizer at v to the *inverse* of a Frobenius element at v (that is, to the geometric Frobenius).

For each place w of M, we get characters

$$M_w^{\times} \hookrightarrow M_{\mathbb{A}}^{\times} \xrightarrow{\psi_i} \overline{\mathbb{F}}^{\times}$$

by composition. Let $\psi_{i,w}$ denote the restriction of the composed character to $\mathcal{O}_w^{\times}$. (Here, $\mathcal{O}_w$ is the w-adic completion of $\mathcal{O}_M$.)

We shall also make use of the "fundamental characters" $\{\theta_{p^d-1}\}$ (see Serre [**21**], Section 1). We view them as characters of $\mathcal{O}_w^{\times}$.

THEOREM 7.4. *Suppose that $K = \mathbb{Q}$, that A has good reduction at p and that p is unramified in M. If p splits in M, say*

$$p\mathcal{O}_M = ww'$$

then

$$(\psi_{1,w}, \psi_{1,w'}, \psi_{2,w}, \psi_{2,w'}) = (\theta_{p-1}, 1, 1, \theta_{p-1}) \text{ or } (1, \theta_{p-1}, \theta_{p-1}, 1).$$

If p remains prime in M, then

$$(\psi_{1,p}, \psi_{2,p}) = (\theta_{p^2-1}, \theta_{p^2-1}^p) \text{ or } (\theta_{p^2-1}^p, \theta_{p^2-1}).$$

PROOF. Firstly, we may assume that $\mathcal{O}_E \subseteq \mathrm{End}_{\mathbb{Q}}(A)$. Indeed, there is an Abelian variety $B_{/\mathbb{Q}}$ which is $\mathbb{Q}$-isogenous to A and such that $\mathcal{O}_E \subseteq \mathrm{End}_{\mathbb{Q}}(B)$ (cf. Shimura [**22**], p. 199). For such a B, we see that $(\mathbb{Q}, B, E)$ is again a triple of type (T'), and we can identify $\Gamma(B) = \Gamma(A)$. In the notation of section 6, B will correspond to a (possibly) different choice of $\mathcal{O}_B[G_{\mathbb{Q}}]$-lattice in $V_{\mathfrak{p}}(A)$. By our Hypothesis 7.1, and the remark at the end of Section 6, the extension $\mathbb{Q}(X)/M$ is independent of the choice of lattice. Thus, we may as well assume to start with that $\mathcal{O}_E \subseteq \mathrm{End}_{\mathbb{Q}}(A)$.

Now, let w be a place of M over p. Then, $A_{/M}$ has good reduction at w. Since $e(M_w/\mathbb{Q}_p) = 1$, by a theorem of Raynaud ([**15**], 3.3.4) (see also Ribet [**16**], Theorem 2.2.4), the characters $\psi_{i,w}$ can be written, without multiplicity, as a product of fundamental characters of level f where

$$f = [\mathcal{O}_M/w : \mathbb{F}_p].$$

Also, by Serre ([**21**], Proposition 8), we have

$$\tilde{\chi}_p|_{\mathcal{O}_w^{\times}} = \theta_{p-1}.$$

Consider first the case when p splits: $p\mathcal{O}_M = ww'$. Then

$$\psi_{i,w} = \theta_{p-1}^{a_i},\ \psi_{i,w'} = \theta_{p-1}^{b_i},\ i = 1, 2 \tag{6}$$

where a_i, b_i are integers such that $0 \le a_i, b_i \le 1$. Then, from the relation

$$\psi_1\psi_2 = \tilde{\epsilon}\tilde{\chi_p},$$

we deduce that

$$\theta_{p-1}^{a_1+a_2} = \psi_{1,w}\psi_{2,w} = \theta_{p-1}$$

since ϵ is unramified at p. Let r be any rational integer prime to p. We view it as an element of $\mathbb{Z}_p^\times = \mathcal{O}_w^\times$. Then

$$r^{a_1+a_2} \equiv r \pmod{p}.$$

Since

$$0 \leq a_1 + a_2 \leq 2$$

we must have

$$a_1 + a_2 = 1.$$

Similarly, $b_1 + b_2 = 1$.

We get another relation using Corollary 4.6. Let r be a rational prime $r \neq p$, congruent to 1 modulo a sufficiently high power of each prime dividing the non-p part of the conductors of ψ_1 and ψ_2. Let $e(r)$ be the idèle of M given by

$$e(r)_v = \begin{cases} r & \text{if } v|r \\ 1 & \text{otherwise.} \end{cases}$$

We view r itself as a constant idèle. Then

$$1 = \psi_i(r) = \psi_i(e(r))\psi_{i,w}(r)\psi_{i,w'}(r).$$

Now by Corollary 4.6,

$$r^{a_i+b_i} \equiv r \pmod{p}.$$

Thus,

$$a_1 + b_1 = a_2 + b_2 = 1.$$

This, together with the previous relation implies that

$$(a_1, b_1, a_2, b_2) = (1, 0, 0, 1) \text{ or } (0, 1, 1, 0).$$

Now suppose that p remains prime in M. Then, we can write

$$\psi_{i,p} = \theta_{p^2-1}^{a_i+b_ip}, \ a_i, b_i \in \mathbb{Z}, \ 0 \leq a_i, b_i \leq 1$$

for $i = 1, 2$. Proceeding in the same way as above, we find that

$$\theta_{p^2-1}^{(a_1+a_2)+(b_1+b_2)p} = \psi_{1,p}\psi_{2,p} = \theta_{p-1}.$$

Let $(\mathbb{Q}/\mathbb{Z})'$ denote the abelian group of rational numbers of order prime to p. By Serre ([**21**], Proposition 5), the map which associates to each ratonal number a/d with $(d, p) = 1$, the character θ_d^a gives an isomorphism of $(\mathbb{Q}/\mathbb{Z})'$ with the character group of the tame inertia group of the local field M_p. Thus,

$$\frac{(a_1 + a_2) + (b_1 + b_2)p}{p^2 - 1} = \frac{1}{p-1} \pmod{\mathbb{Z}[1/p]}.$$

Since $0 \leq a_i, b_i \leq 1$, this implies that

$$a_1 + a_2 = b_1 + b_2 = 1.$$

We get another relation if we choose r as in the previous paragraph. Then,

$$1 = \psi_i(r) = \psi_i(e(r))\psi_{i,p}(r)$$

and by Proposition 4.6, we have

$$r^{a_i+b_i} \equiv r \pmod{p}.$$

Therefore,

$$a_1 + b_1 = a_2 + b_2 = 1.$$

Thus,

$$(a_1, b_1, a_2, b_2) \;=\; (1,0,0,1) \text{ or } (0,1,1,0).$$

□

COROLLARY 7.5. *If p splits in M, then $\mathbb{Q}(X)/M(\zeta_p)$ is unramified over p.*

8. Numerical examples

Given an Abelian variety A of type (T'), one may try to produce explicit abelian extensions using the above theory. To do this, one has to solve two problems. The first, is to decide whether A has a non-trivial twist or not. The second is to check whether the corresponding ideal is non-trivial or not.

If we consider the Abelian variety A_f attached to a non complex-multiplication newform f of weight 2, both problems can be solved, in principle, using the Selberg trace formula. Indeed, the trace formula can be used to explicitly calculate the field generated by the Fourier coefficients of f. However, this usually entails an excessive amount of computation, since the dimension of the space $S_2(\Gamma_0(N), \epsilon)$ of cusp forms of weight 2 and a given Nebentypus character ϵ, is $\gg N$.

Shimura has extensively studied the case when f has real Nebentypus and has produced many examples, by explicit calculation, in the case that f has prime level. In this section, we give a set of examples with *non-real* Nebentypus and prime level. In these examples, the two problems mentioned above can be solved "by inspection".

Let $f \in S_2(\Gamma_0(N), \epsilon)$ be a normalized non-complex multiplication newform of weight 2, level N and character ϵ. Suppose that $\epsilon \neq 1$. We consider the triple $(\mathbb{Q}, A_f, E_f)$, where E_f is the field generated by the Fourier coefficients of f. We have seen that E_f is a CM-field. Let c denote the canonical complex conjugation of E_f, and denote by E_f^+ the maximal totally real subfield of E_f. Then $c \in \Gamma(A_f)$ and $\chi_c \;=\; \epsilon^{-1}$. We retain the notation of our previous sections and set

$$S_f \;=\; S_n(E_f/E_f^+)^{\text{odd}}$$

where n is the order of ϵ.

PROPOSITION 8.1. *Suppose that N is squarefree, and that ϵ has conductor N and even order $n = 2q$. Suppose that $S_f \neq 1$ and let $\mathfrak{p}$ be a prime divisor of S_f. Let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and X the associated $G_{\mathbb{Q}}$ module. Then the fixed field M of ϵ^{-q} is $\mathbb{Q}(\sqrt{N})$ and*

1. *$q = p^a$ with some integer $a \geq 0$.*
2. *$\mathrm{Gal}(\mathbb{Q}(X)/M)$ is contained in a* split *Cartan subgroup of $\mathrm{GL}_2(\mathbb{F})$.*
3. *$M \subseteq M(\zeta_p) \;\subseteq \mathbb{Q}(X)$.*
4. *The conductor of $\mathbb{Q}(X)/M$ is $p\infty_1\infty_2$, where ∞_1, ∞_2 are the infinite places of M.*

Suppose that p does not divide N. Let u denote the fundamental unit of M. Then

5. *$\mathbb{Q}(X)/M(\zeta_p)$ is everywhere unramified if p splits in M.*
6. *If* Norm *$u = +1$, then $u \equiv 1 \pmod{p\mathcal{O}_M}$.*
7. *If* Norm *$u = -1$, then $u^2 \equiv 1 \pmod{p\mathcal{O}_M}$ but $u \not\equiv 1 \pmod{p\mathcal{O}_M}$.*

REMARK 8.2. Conditions (1), (6) and (7) are necessary for $S_f \neq 1$. If f has real Nebentypus, then (1) is vacuous ($a = 0$) but (6) and (7) are still necessary. The extra condition (1) in the case of non-real Nebentypus makes it more difficult for S_f

to be non-trivial. For example, consider the case of prime level. Since $\epsilon(-1) = 1$, we must have $N \equiv 1 \pmod 4$. In this case, Norm $u = -1$ and so we have

$$u^2 - 1 = (\text{Tr } u)u.$$

Thus, $u^2 - 1$ and Tr u have the same prime factors.Then (1) and (6), (7) would require that p divides $(N - 1, \text{Tr } u)$. For $N < 100$, this happens only for $N \equiv 1 \bmod 12$, i.e. $N = 13, 37, 61, 73, 97$. In all these cases $p = 3$. The first case when a prime larger than 3 divides $(N - 1, \text{Tr } u)$ is $N = 101$. In this case, $u = 10 + \sqrt{101}$ and $p = 5$. If we choose any character $\epsilon \pmod{101}$ of order 10, we find that $\dim S_2(\Gamma_0(N), \epsilon) = 8$. Without explicitly calculating the characteristic polynomial of some Hecke operators, I see no a-priori way of deciding whether there is an eigenform f in this space for which $S_f \neq 1$.

REMARK 8.3. Shimura ([**23**], p. 148) has conjectured that (for real Nebentypus and prime level), condition (6) (i.e. p divides Tr u) is also sufficient to ensure that $S_f \neq 1$ provided $p \geq 5$. Momose pointed out to me that Koike [**8**] has shown the following result. Denote by S_f^* the ideal of E_f generated by the Fourier coefficients a_n such that $a_n^c = -a_n$. Let N be squarefree with $N \equiv 1 \pmod 4$. Suppose that the norm of the fundamental unit u of $\mathbb{Q}(\sqrt{N})$ is -1. Let $p \geq 5$ be any prime which divides the trace of u. Then, there exists a cusp form $h \in S_2(\Gamma_0(N), \left(\frac{N}{\cdot}\right))$ which is an eigenform for the Hecke operators such that p divides the norm of S_h^*.

REMARK 8.4. We may conjecture that if $p \neq 2$ is a common divisor of $\phi(N)$ and the trace of u, then there exists an eigenform $h \in S_2(\Gamma_0(N), \epsilon)$ with ϵ a character of order $2p^a$ for some a, such that p divides the norm of S_h. We shall partly prove this in the case $p = 3$. By this method, we shall produce some abelian extensions which it does not seem possible to obtain using forms with real Nebentypus.

REMARK 8.5. The analogue of Koike's theorem for $p = 3$ is false. Indeed, consider $N = 37$. In this case, the space $S_2(\Gamma_0(37), \left(\frac{37}{\cdot}\right))$ is 2 dimensional and is spanned by an eigenform f and its conjugate. We have $E_f = \mathbb{Q}(\sqrt{-1})$ and $S_f^{*\text{odd}} = 1$ although 3 divides the trace of the fundamental unit $6 + \sqrt{37}$.

8.1. Proof of Proposition 8.1.

PROOF. The first assertion (1) follows from Corollary 5.17. Next, since condition (1) of Theorem 6.5 is satisfied, $\text{Gal}(\mathbb{Q}(X)/M)$ is contained in a Cartan subgroup C (say) of $\text{GL}_2(\mathbb{F})$. Now assertion (3) follows from Proposition 7.2.

To see that we can take C to be split, let w_N denote the Atkin-Lehner involution of level N. It induces an automorphism of A_f which is defined over M_ϵ, and which is of order 2. Furthermore, for all $g \in G_{\mathbb{Q}}$, we have

$$w_N^g = \overline{\epsilon}(g) w_N \tag{7}$$

and w_N commutes with the action of E_f^+. Thus, if we let

$$X_\pm = (1 \pm w_N)X$$

then we see that

(a) $X = X_+ \oplus X_-$
(b) there exists a $\delta \in G_{\mathbb{Q}}$ such that $X_\pm^\delta = X_\mp$.
(c) $X_\pm$ is an $\mathbb{F}$-vector space of dimension 1
(d) the decomposition of (a) is rational over M.

Indeed, (a) is clear. For (b), we note that since ϵ has even order, there exists a $\delta \in G_{\mathbb{Q}}$ such that $\epsilon(\delta) = -1$. Then, we have from (7)

$$w_N^{\delta} \;=\; -w_N$$

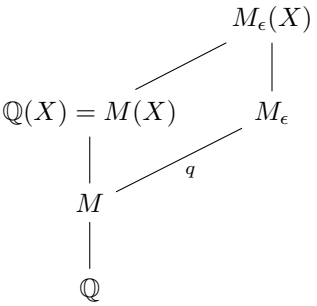
and (b) follows. In particular, both $X_{\pm}$ are non-zero.

Let $\mathcal{O}_+$ denote the ring of integers of E_f^+, and let $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_+$. Then $\mathcal{O}_+$ acts on $X_{\pm}$ and this action factors through $\mathfrak{q}$. This gives $X_{\pm}$ the structure of an $\mathcal{O}_+/\mathfrak{q} \simeq \mathbb{F}$ vector space. Moreover, from (a) and (b) it follows that it is of dimension 1. Finally, (d) follows from (7) and the fact that $\zeta_q \equiv 1 \pmod{\mathfrak{p}}$ (cf. (1) and Corollary 5.17). Putting all of these observations together, we see that $\mathrm{Gal}(\mathbb{Q}(X)/M)$ is contained in the split Cartan subgroup

$$C \;=\; \mathrm{Aut}_{\mathbb{F}}(X_+) \;\times\; \mathrm{Aut}_{\mathbb{F}}(X_-).$$

This proves (2).

By Proposition 4.8, we know that the ramification over p is tame, and so (4) will follow from (3) if we show that $\mathbb{Q}(X)/M$ is unramified over $N/(N,p)$. To show this, we consider the diagram of fields below.



We have $[M_\epsilon : M] = q$ whereas $[\mathbb{Q}(X) : M]$ divides $(q-1)^2$ and is, in particular, prime to q. Therefore, $\mathbb{Q}(X) \cap M_\epsilon = M$. On the other hand, the hypotheses on N and ϵ ensure that A_f acquires everywhere good reduction over M (by Deligne and Rapaport [**5**]). Thus, $M_\epsilon(X)/M_\epsilon$ is unramified at the primes dividing $N/(N,p)$. Combining these two observations, we deduce that $\mathbb{Q}(X)/M$ is unramified at primes dividing $N/(N,p)$ also. Thus (4) is proved. We note that (5) is just (4) combined with Corollary 7.5. To prove (6), let α be any totally positive unit of M. Let ϕ_1, ϕ_2 be the characters

$$\mathrm{Gal}(\mathbb{Q}(X)/M) \;\longrightarrow\; \overline{\mathbb{F}}^{\times}$$

obtained from the Cartan subgroup C. Let ψ_1, ψ_2 be the associated Hecke characters. Then

$$\psi_1(\alpha) \;=\; \psi_2(\alpha) \;=\; 1.$$

Suppose p splits in M, say $p\mathcal{O}_M \;=\; ww'$. By Theorem 7.4, we may assume that

$$(\psi_{1,w}, \psi_{1,w'}, \psi_{2,w}, \psi_{2,w'}) \;=\; (\theta_{p-1}, 1, 1, \theta_{p-1}).$$

Then

$$1 \;=\; \psi_1(\alpha) \;=\; \psi_{1,w}(\alpha) \;=\; \alpha \pmod{w}.$$

Similarly,

$$\alpha \pmod{w'} \;=\; 1.$$

Thus, $\alpha \equiv 1 \pmod{p\mathcal{O}_M}$. If p does not split in M, we find in a similar manner that $\alpha \equiv 1 \pmod{p\mathcal{O}_M}$.

Now if Norm $u = +1$, then u is totally positive so $u \equiv 1 \pmod{p}$. On the other hand, if Norm $u = -1$, then u^2 is totally positive, so $u^2 \equiv 1 \pmod{p}$. Moreover, $u \not\equiv 1 \pmod{p}$ for otherwise we would have

$$-1 = uu' \equiv 1 \pmod{p}$$

contradicting the fact that p is odd. (Here, u' denotes the conjugate of u.) This proves the Proposition. □

8.2. Numerical Examples. Now we find a set of examples which satisfy the hypotheses of Proposition 8.1.

LEMMA 8.6. *Let $M = \mathbb{Q}(\sqrt{N})$ with a positive squarefree integer $N \equiv 1 \pmod 4$. Suppose that $\mathrm{Norm}_{M/\mathbb{Q}} u = -1$ where u is the fundamental unit of M. Then $3 | \mathrm{Tr}_{M/\mathbb{Q}} u$ if and only if $N \equiv 1 \pmod 3$.*

PROOF. This is due to Shimura ([**23**], p. 186). □

LEMMA 8.7. *Let N be a positive integer and ϵ an even character modulo N of conductor r. Then $\dim S_2(\Gamma_0(N), \epsilon)$ is equal to*

$$\frac{1}{12} N \prod_{p|N} \left(1 + \frac{1}{p}\right) - \frac{1}{2} \sum_{\substack{d|N \\ (d, N/d)|(N/r)}} \phi((d, N/d)) - \frac{1}{4} \sum{}' \epsilon(x) - \frac{1}{3} \sum{}'' \epsilon(x)$$

where the first sum is over $x \pmod N$ satisfying $x^2 + 1 \equiv 0 \pmod N$ and the second sum is over $x \pmod N$ satisfying $x^2 + x + 1 \equiv 0 \pmod N$.

PROOF. See Cohen and Oesterlé [**3**]. □

LEMMA 8.8. *Let N be a prime $\equiv 13 \bmod 24$. Let a be the largest power of 3 that divides $N - 1$. Let ϵ be the even character modulo N of order $2 \cdot 3^a$. Then $\dim S_2(\Gamma_0(N), \epsilon)$ is $(N-1)/12$. In particular, it is odd.*

PROOF. Let g be a primitive root modulo N and ζ a primitive 3^a-th root of unity, such that $\epsilon(g) = -\zeta$. If $x^2 + 1 \equiv 0 \pmod N$, then

$$x = \pm g^{(N-1)/4}.$$

Thus,

$$\epsilon(x) = (-1)^{(N-1)/4} = -1.$$

Similarly, if $x^2 + x + 1 \equiv 0 \pmod N$, then

$$x = g^{(N-1)/3} \text{ or } g^{2(N-1)/3}.$$

Thus,

$$\epsilon(x) = \zeta_3 \text{ or } \zeta_3^2$$

where ζ_3 is a primitive cube root of 1. Thus, by Lemma 8.7,

$$\dim S_2(\Gamma_0(N), \epsilon) = \frac{1}{12}(N+1) - 1 + \frac{1}{2} + \frac{1}{3} = (N-1)/12.$$

□

LEMMA 8.9. *Let N be an arbitrary positive integer and ϵ an even character modulo N. Suppose that the dimension of $S_2(\Gamma_0(N), \epsilon)$ is odd. Then, there exists an eigenform $f \in S_2(\Gamma_0(N), \epsilon)$ such that the degree $[E_f : \mathbb{Q}(\epsilon)]$ is odd.*

PROOF. Choose a basis X of $S_2(\Gamma_0(N),\epsilon)$ consisting of eigenforms for all the Hecke operators T_n with $(n,N)=1$. Choose a maximal subset Y of X such that no two elements of Y are Galois conjugates of one another. Then

$$\dim S_2(\Gamma_0(N),\epsilon) \;=\; \sum_{h\in Y}[E_h:\mathbb{Q}(\epsilon)].$$

Indeed, viewing the E_h as subfields of $\mathbb{C}$, we have

$$X \;\subseteq\; Y' \;=\; \{h^\sigma \mid h\in Y,\ \sigma\ \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q}(\epsilon))\}$$

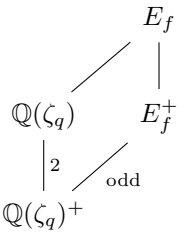
and the forms in Y' are independent. Now, since $S_2(\Gamma_0(N),\epsilon)$ has odd dimension, one at least of the $[E_h:\mathbb{Q}(\epsilon)]$ must be odd. This proves the lemma. □

THEOREM 8.10. *Let N be a prime $\equiv 13 \bmod 24$ and let a be the highest power of 3 that divides $N-1$. Let ϵ be the even character $\pmod N$ of order $2\cdot 3^a$. Then, there exists a normalized eigenform $f\in S_2(\Gamma_0(N),\epsilon)$ and a prime $\mathfrak{p}$ of E_f which lies over 3, such that $\mathfrak{p}$ divides S_f. Let X be the associated $G_{\mathbb{Q}}$-module, and $M=\mathbb{Q}(\sqrt{N})$. Then, $\mathbb{Q}(X)$ contains the unique class field of conductor $3\infty_1\infty_2$ and degree 4 over M.*

PROOF. By Lemma 8.8, the dimension of $S_2(\Gamma_0(N),\epsilon)$ is odd. Then by Lemma 8.9, we can choose a normalized eigenform f such that the degree $[E_f:\mathbb{Q}(\epsilon)]$ is odd. Let $n=2q$ with $q=3^a$. Then, by Corollary 5.17, we have

$$S_f \;=\; \mathfrak{d}(E_f/E_f^+)^{\mathrm{odd}} \;\supseteq\; (1-\zeta_q)\mathcal{O}_{E_f}.$$

Now by the diagram of fields below, it follows that $\mathfrak{d}(E_f/E_f^+)^{\mathrm{odd}} \;\neq\; 1$. We thus may apply Proposition 8.1 to deduce that $\mathbb{Q}(X)/M$ is abelian of conductor $3\infty_1\infty_2$. Let h denote the class number of M.



We claim that the $3\infty_1\infty_2$ ray class field H of M is of degree $4h$ over M. Indeed, let u be the fundamental unit of M. Since N is a prime $\equiv 1 \pmod 4$, we have $Norm\ u \;=\; -1$. By Proposition 8.1 (4), we deduce that $u^2 \;\equiv 1 \pmod 3$ but $u\not\equiv 1 \pmod 3$, Since $N\equiv 1 \pmod 3$, it follows that 3 splits in M. Putting these two facts together, we see that H has degree $2\cdot h\cdot(3-1)^2/2 \;=\; 4h$ over M (cf. Lang ([**9**], p. 127)).

Since N is prime, h is odd. Therefore, H contains a unique field H' (say) of degree 4 over M and of conductor $3\infty_1\infty_2$. To show that $\mathbb{Q}(X)\supseteq H'$ it is enough to show that 4 divides the degree $[\mathbb{Q}(X):M]$. Since 3 splits in M, this follows, for example, from Theorem 7.4. □

COROLLARY 8.11. *If the class number $h(N)$ of $\mathbb{Q}(\sqrt{N})$ is prime to* Norm $\mathfrak{p}-1$, *then $\mathbb{Q}(X)/M$ is the unique class field of conductor $3\infty_1\infty_2$ and degree 4. In particular, this is the case if $h(N)=1$.*

PROOF. Since the order of $\mathrm{Gal}(\mathbb{Q}(X)/M)$ divides $(Norm\ \mathfrak{p}\ -1)^2$, and also $4h$, it follows that this order is in fact 4. The rest of the assertion follows from Theorem 8.10. □

REMARK 8.12. From the tables in Cohen and Roblot [**2**], we see that if D is a prime such that $D \equiv 1 \pmod 4$ and $D < 573$, then $h(D) \leq 5$ and is odd. It is easily checked that 3 and 5 are coprime to any number of the form $3^b - 1$ with b not divisible by 4. Thus, if $N \equiv 13 \pmod{24}$ is a prime with $N < 573$, then $\mathbb{Q}(X)/M$ is the unique class field of conductor $3\infty_1\infty_2$ and degree 4.

9. Remarks on other work

Brown and Ghate [**1**] consider a quadratic field $F = \mathbb{Q}(\sqrt{D})$. Let χ_D denote the associated quadratic Dirichlet character modulo $|D|$. Consider a cusp form f of some weight $k \geq 2$ for the congruence subgroup $\Gamma_0(|D|)$ with Nebentypus χ_D and assume that f is a normalized Hecke eigenform. Factor $D = D_1D_2$ and assume that $F_1 = \mathbb{Q}(\sqrt{D_1})$ is a real quadratic field. Assume that f has a twist by (γ, χ_{D_1}) for some automorphism γ of the field E_f of Fourier coefficients of f. Let $\mathfrak{p}$ be a prime that divides the different of E_f/E_f^γ and p the rational prime below it. Assume that $(p, 2D) = 1$ and that f is ordinary at $\mathfrak{p}$. Assume also that the mod $\mathfrak{p}$ representation associated to f is absolutely irreducible. Then, they use Shimura's method to construct some abelian extensions of F_1.

The case $F_1 = F$ is considered by Hida [**7**]. However, Hida allows forms of any weight $k \geq 2$ and he restricts his attention to identifying and characterizing 'dihedral primes' (that is primes such as $\mathfrak{p}$ above at which the mod $\mathfrak{p}$ representation is dihedral) and does not explicitly discuss the construction of class fields. Of course, for weight larger than 2, one does not have a corresponding Abelian variety so it is not at first clear how one might generate class fields. However, Brown and Ghate remark that one can work in a Hida family which contains a form of weight 2 congruent to the form of higher weight, and this form can then be used to generate some class fields.

The work of Darmon and Green [**4**] takes a completely different approach to the construction of class fields of real quadratic fields. Their attempt is to generalize the construction of Heegner points and they propose a conjectural construction of Stark-Heegner points. The construction is local, and it is conjectured that the points are actually global and defined over a ring class field of a real quadratic field. This theory is very intriguing given that there are very few general ways of producing rational points on curves or higher dimensional varieties.

References

[1] Alexander F. Brown and Eknath P. Ghate, *Dihedral congruence primes and class fields of real quadratic fields*, J. Number Theory **95** (2002), no. 1, 14–37, DOI 10.1006/jnth.2001.2753. MR1916078

[2] Henri Cohen and Xavier-François Roblot, *Computing the Hilbert class field of real quadratic fields*, Math. Comp. **69** (2000), no. 231, 1229–1244, DOI 10.1090/S0025-5718-99-01111-4. MR1651747

[3] Henri Cohen and Joseph Oesterlé, *Dimensions des espaces de formes modulaires* (French), Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 69–78. Lecture Notes in Math., Vol. 627. MR0472703

[4] Henri Darmon and Peter Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Experiment. Math. **11** (2002), no. 1, 37–55. MR1960299

[5] Pierre Deligne, *Courbes elliptiques: formulaire d'après J. Tate* (French), Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 53–73. Lecture Notes in Math., Vol. 476. MR0387292

[6] Koji Doi and Masatoshi Yamauchi, *On the Hecke operators for* $\Gamma_0(N)$ *and class fields over quadratic number fields*, J. Math. Soc. Japan **25** (1973), 629–643, DOI 10.2969/jmsj/02540629. MR0344226

[7] Haruzo Hida, *Global quadratic units and Hecke algebras*, Doc. Math. **3** (1998), 273–284. MR1650571

[8] Masao Koike, *Congruences between cusp forms and linear representations of the Galois group*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), Japan Soc. Promotion Sci., Tokyo, 1977, pp. 109–116. MR0466024

[9] Serge Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970. MR0282947

[10] Vijayakumar Pedaprolu Murty, *ALGEBRAIC CYCLES ON ABELIAN VARIETIES*, ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University. MR2632244

[11] Fumiyuki Momose, *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 1, 89–109. MR617867

[12] Fumiyuki Momose, *Galois action on some ideal section points of the abelian variety associated with a modular form and its application*, Nagoya Math. J. **91** (1983), 19–36. MR716785

[13] Masami Ohta, *On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 299–308. MR0419368

[14] Masami Ohta, *The representation of Galois group attached to certain finite group schemes, and its application to Shimura's theory*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), Japan Soc. Promotion Sci., Tokyo, 1977, pp. 149–156. MR0457445

[15] Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$ (French), Bull. Soc. Math. France **102** (1974), 241–280. MR0419467

[16] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR0457455

[17] Kenneth A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275, DOI 10.1007/BF01425561. MR0419358

[18] Kenneth A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), no. 1, 43–62, DOI 10.1007/BF01457819. MR594532

[19] Kenneth A. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight* 2, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser, Boston, Mass., 1981, pp. 263–276. MR633903

[20] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[21] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR0387283

[22] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1. MR0314766

[23] Goro Shimura, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. (2) **95** (1972), 130–190, DOI 10.2307/1970859. MR0314801

Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Canada M5S 2E4

Email address: murty@math.toronto.edu