Math. Ann. 282, 645–666 (1988)

Mathematische Annalen

Coates-Wiles Towers in Dimension Two

David Grant*

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Let K be an imaginary quadratic field and E an elliptic curve defined over K with complex multiplication by the ring of integers of K. In 1977 Coates and Wiles proved that if $E(K)$ has positive rank, then the Hasse-Weil zeta function $L(E/K,s)$ of E has a zero at $s=1$ [2]. Such curves exist precisely when the class number of K is one. (Subsequent work [1] extended the result to a wider class of CM curves. Another proof emerged from Rubin's important work on the Tate-Shafarevich group [13, 14]. See also [10–12].)

Coates and Wiles used formal groups and Iwasawa-theoretic techniques to relate the special value of $L(E/F,s)$ to elliptic units. Employing more classical techniques, Stark and Gupta combined to give a different proof of the theorem [21, 4]. Although the two proofs have different flavors, they include the same ingredients:

Let $\mathfrak{p}$ be one of infinitely many suitably chosen primes of K, and K_n the field obtained by adjoining the $\mathfrak{p}^n$-torsion of E to K. There is a unique prime $\mathfrak{p}_n$ of K_n lying over $\mathfrak{p}$. Let Q be a point of infinite order in $E(K)$, $Q\notin \mathfrak{p}E(K)$, and $L_n(Q)=K\left(\frac{1}{\mathfrak{p}^n}Q\right)$. Let ψ be the Grössencharakter of E, and Ω a fundamental period of the minimal model of E.

Essential to both proofs are the facts that $\tilde{L}(\bar{\psi},1)=L(\bar{\psi},1)/\Omega$ is algebraic, and that for all $n\geqq 1$ there are u_n, v_n in K_n, u_n a unit and $\operatorname{ord}_{\mathfrak{p}_n}(v_n)=1$, satisfying

$$u_n\equiv 1+v_n\tilde{L}(\bar{\psi},1)\operatorname{mod}\mathfrak{p}_n^2 .$$

Both proofs then used the extensions $L_n(Q)/K_n$ to deduce that for some n, $u_n\equiv 1\operatorname{mod}\mathfrak{p}_n^2$. Hence $\mathfrak{p}$ divides $\tilde{L}(\bar{\psi},1)$ for infinitely many $\mathfrak{p}$.

Gupta achieved this by applying a conductor-discriminant formula to the towers $L_n(Q)$ and K_n to show that for some e, the conductor of $L_e(Q)/K_e$ is precisely $\mathfrak{p}_e^2$. Class field theory then shows that all units of K_e congruent to $1\operatorname{mod}\mathfrak{p}_e$ are in fact congruent to $1\operatorname{mod}\mathfrak{p}_e^2$.

* Partially supported by NSF grant DMS 85-02804 A04

The purpose of this paper is to generalize Gupta's result to analogous towers obtained from abelian surfaces. The techniques employed are a hybrid of those of Gupta and those of Coates and Wiles, including both conductor-discriminant calculations and formal groups.

The main obstacle to further progress is the inability to produce an analogue of elliptic units to relate to the special value of the L-function of A.

Let K be a totally imaginary quartic number field, and A a simple abelian surface defined over K with complex multiplication by the ring of integers of K. Such surfaces exist precisely when K is cyclic and of class number one. Let p be one of infinitely many suitably chosen rational primes such that $(p)=\mathfrak{p}$ remains prime in K. In the field K_n obtained by adjoining to K the $\mathfrak{p}^n$-torsion of A there is a unique prime $\mathfrak{p}_n$ above $\mathfrak{p}$. Let Q be a point of infinite order in $A(K)$, $Q \notin \mathfrak{p}A(K)$, and $L_n(Q)$ the field obtained by adjoining to K_n the $\mathfrak{p}^n$-division values of Q. It is easy to show that there is an $e=e(Q)$ such that $L_e(Q)/K_e$ is ramified while $L_n(Q)/K_n$ is not for all $0 \leqq n < e$. Let $\mathcal{O}_\mathfrak{p}$ denote the p-adic integers of K.

The main results of this paper are the following theorems:

Theorem 1. *The conductor of* $L_e(Q)/K_e$ *is* $\mathfrak{p}_e^2$ *or* $\mathfrak{p}_e^{p^2-p+2}$.

Which of the two possibilities occurs depends on the coordinates of Q in the formal group on the kernel of reduction modulo $\mathfrak{p}$ of A completed over $\mathcal{O}_\mathfrak{p}$. This kernel is naturally an $\mathcal{O}_\mathfrak{p}$-module, and contains a subgroup $\mathcal{A}_0(K)$ of finite index in $A(K)$. Using methods of transcendence, one can show that if the $\mathcal{O}_K$-rank of $A(K)$ is at least 5, then the $\mathcal{O}_\mathfrak{p}$-rank of $\mathcal{A}_0(K)\otimes\mathcal{O}_\mathfrak{p}$ is 2 (see the remarks at the end of Sect. 5).

Theorem 2. *If the* $\mathcal{O}_\mathfrak{p}$-rank *of* $\mathcal{A}_0(K)\otimes\mathcal{O}_\mathfrak{p}=2$, *then there are* $\mathcal{O}_\mathfrak{p}$*-independent points* Q_1 *and* Q_2 *in* $\mathcal{A}_0(K)\subsetneqq A(K)$ *such that*

$$L_{e_1}(Q_1)/K_{e_1} \text{ has conductor } \mathfrak{p}_{e_1}^2$$

and

$$L_{e_2}(Q_2)/K_{e_2} \text{ has conductor } \mathfrak{p}_{e_2}^{p^2-p+2},$$

where $e_i=e(Q_i)$. *In particular, every unit of* K_{e_1} *congruent to* $1 \bmod \mathfrak{p}_{e_1}$ *is congruent to* $1 \bmod \mathfrak{p}_{e_1}^2$.

Since we expect there to be no bound on the $\mathcal{O}_K$-rank of such $A(K)$, presumably there are A for which Theorem 2 holds.

For the explicit computations carried out in this paper, it seems best to work with fourth degree primes. On the positive side, it guarantees that there is a unique prime of K_n above $\mathfrak{p}$. On the negative side, this forces us to deal with formal groups which are not of Lubin-Tate type.

The first section of this paper culls necessary information on the number fields K and the abelian surfaces A. In section two, the theorems of complex multiplication are applied to describe K_n. This description is applied in section three to determine up to isomorphism the formal group on the kernel of the reduction modulo $\mathfrak{p}$ of A completed over $\mathcal{O}_\mathfrak{p}$. In section four we study the extensions $L_n(Q)/K_n$, reducing the conductor calculation to some rather explicit computation in the formal group. This is carried out, and Theorems 1 and 2 proved, in the final section.

Some of the results of this paper were contained in the author's Ph.D. thesis. The author takes this opportunity to record his thanks to his advisor, Harold Stark, for his continued encouragement and support, and to Kevin Coombes, for his valued counsel.

Notation. Let E/F be number fields, and $\mathfrak{p}$ a prime of F. We let $\mathfrak{f}(E/F)$ and $D(E/F)$ denote respectively the conductor and discriminant of E/F. We let $\mathcal{O}_F$ denote the ring of integers of F, $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p}$ the integers of $F_\mathfrak{p}$. We let $h(F)$ denote the class number of F.

1. Preliminaries

Throughout this paper, K will denote a number field satisfying:

$$\begin{aligned}&\text{i) } K \text{ totally imaginary, } K/\mathbb{Q} \text{ a quartic cyclic extension}\\ &\text{ii) } h(K)=1.\end{aligned} \tag{1.1}$$

Setzer has shown there are precisely seven such K [19]. Let K^+ denote the real quadratic subfield of K, σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and W the group of roots of unity of K. We have 2 cases:

Case I: $|W|=2$

Case II: $K=\mathbb{Q}(e^{2\pi i/5})$ and $|W|=10$.

The following is a elementary lemma to which we will refer repeatedly.

Lemma (1.2). *Let $K/F/E$ be a tower of number fields with* $\mathrm{Gal}(K/E)$ *cyclic, and* $[K:F]\,|\,[F:E]$. *If a prime p of E ramifies totally to F, then it must ramify totally to K.*

Proof. Let I_p denote the inertia subgroup in $\mathrm{Gal}(K/E)$ of any prime in K which divides p, and L_p its fixed field. Since $[K:F]\,|\,[F:E]\,|\,|I_p|$, and $\mathrm{Gal}(K/E)$ is cyclic, $L_p \subseteq F$, so L_p/E is both a totally ramified and unramified extension. Hence $L_p=E$.

Let U denote the units of $\mathcal{O}_K$, and ε be a fundamental unit in K^+.

Lemma (1.3). i) $h(K^+)=1$, *and* $\mathbb{N}_{K^+/\mathbb{Q}}(\varepsilon)=-1$.

ii) *every $x\in U$ is of the form $w\varepsilon^m$, for some $w\in W$, and $m\in\mathbb{Z}$.*

Proof. i) Since $K^+/\mathbb{Q}$ must be ramified at a finite prime, Lemma (1.2) implies that K/K^+ must be ramified at a finite prime. Since K/K^+ has no unramified subextensions, $h(K^+)\,|\,h(K)$ [23, p. 184]. Finally, if ε had norm 1, then class field theory implies that there is a quadratic extension L/K^+ which is unramified at all finite primes. Hence LK/K would be a quadratic extension unramified at all finite primes, a contradiction since $h(K)=1$ and K is totally imaginary.

ii) In Case I, let ξ be a fundamental unit of K: we need only show it is real. But $\sigma(\xi)=\pm\xi^{\pm1}$; hence $\sigma^2(\xi)=\xi$. In Case II, this is a classic fact about cyclotomic fields [23, p. 3].

We now briefly recall the terminology of the theory of complex multiplication. We will freely use the results of the theory as given in [7].

We assume throughout this paper that A is an abelian variety of dimension 2 with principal complex multiplication by K. That is, we have an embedding

$$i: K \to \mathrm{End}(A) \otimes \mathbb{Q} = \mathrm{End}_{\mathbb{Q}}(A)$$

such that $i(\mathcal{O}_K) = i(K) \cap \mathrm{End}(A)$.

The action of i on the tangent space of A determines a CM-type $\Phi = \{\phi_1, \phi_2\}$, where ϕ_1, ϕ_2 are non-conjugate embeddings of K into $\mathbb{C}$. The only possible choices for Φ are

$$\Phi = \{\sigma^i, \sigma^j \mid 0 \leqq \mathrm{i} < \mathrm{j} \leqq 3, \mathrm{j} \neq \mathrm{i} + 2\}. \tag{1.4}$$

Associated to Φ is its type trace and type norm

$$\mathbb{T}_\Phi(x) = \sum_{\phi \in \Phi} \phi(x), \qquad \mathbb{N}_\Phi(x) = \prod_{\phi \in \Phi} \phi(x), \quad \text{for } x \text{ in } K.$$

The reflex field K' of K is defined by $\mathbb{Q}(\mathbb{T}_\Phi(K))$. The reflex type Φ' of Φ is given by $\Phi' = \{\phi_1^{-1}, \phi_2^{-1}\}$ since $K/\mathbb{Q}$ is Galois.

For $\alpha \in K$, let $\Phi(\alpha)$ denote $(\phi_1(\alpha), \phi_2(\alpha))$ in $\mathbb{C}^2$. There is an analytic isomorphism

$$\theta: \mathbb{C}^2/\Phi(\mathfrak{a}) \to A(\mathbb{C})$$

for some lattice $\mathfrak{a}$ of K. Since the complex multiplication is principal, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$.

Let $\mathcal{C}$ be a polarization on A. Then a basic polar divisor of $\mathcal{C}$ determines a Riemann form E on $\mathbb{C}^n/\Phi(\mathfrak{a})$ and a Rosati involution on $\mathrm{End}_{\mathbb{Q}}(A)$. If $i(K)$ is stable under this involution, the Riemann form E is called Φ-admissible. If this is the case we say the triple $(A, i, \mathcal{C})$ is of type $(F, \Phi, \mathfrak{a}, \underset{\sim}{E})$ with respect to θ.

We say that $(A, i, \mathcal{C})$ is defined over L whenever A, $i(\mathcal{O}_K)$, and $\mathcal{C}$ are. If $(A', i', \mathcal{C}')$ is of type $(K, \Phi', \mathfrak{a}', E')$, then a homomorphism of $(A, i, \mathcal{C})$ into $(A', i', \mathcal{C}')$ is a homomorphism of A into A' which commutes with the actions of i and i', and such that the pullback of $\mathcal{C}'$ is contained in $\mathcal{C}$.

The group $\mathrm{Aut}(A, i, \mathcal{C})$ is finite, and equal to $i(W)$.

The field of moduli $M(A, i, \mathcal{C})$ of $(A, i, \mathcal{C})$ is the fixed field of those $\tau \in \mathrm{Aut}(\mathbb{C})$ such that $(A, i, \mathcal{C})$ is isomorphic over $\mathbb{C}$ to $(A^\tau, i^\tau, \mathcal{C}^\tau)$, where i^τ is the composite of i and the induced map $\mathrm{End}(A) \to \mathrm{End}(A^\tau)$.

Proposition (1.5). *Suppose $K/\mathbb{Q}$ is cyclic, quartic, totally imaginary of class number one; A is an abelian surface with principal complex multiplication by K; $\mathcal{C}$ is any polarization of A; and i, Φ, θ, $\mathfrak{a}$, E are as above. Then*

i) *A is simple.*

ii) *$K' = K$.*

iii) *$\mathcal{C}$ is Φ-admissible and $(A, i, \mathcal{C})$ is of type $(K, \Phi, \mathfrak{a}, E)$ with respect to θ.*

iv) *$(A, i, \mathcal{C})$ has a model defined over $M(A, i, \mathcal{C})$.*

v) *$M(A, i, \mathcal{C}) = K$.*

Proof. i) Since $K/\mathbb{Q}$ is Galois, [7, p. 13] states that A is simple if and only if the only $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\Phi\tau = \Phi$ is $\tau = 1$. It is easy to verify that all the CM-types in (1.4) have this property.

ii) Since $K/\mathbb{Q}$ is Galois, $K' \subsetneqq K$, so $K'/\mathbb{Q}$ is Galois. Hence $K'' \subsetneqq K' \subsetneqq K$ and A simple implies $K'' = K$ [7, p. 24].

iii) This is automatic for A simple [7, p. 20, Theorem 4.5].

iv) Shimura has proved this for $[K:\mathbb{Q}]=4$, $(A,i,\mathscr{C})$ of type $(K,\Phi,\mathfrak{a},E)$, and A simple [20].

v) It is always the case that $K'\subseteqq M(A,i,\mathscr{C})$. If $(A,i,\mathscr{C})$ is principal, and of type $(K,\Phi,\mathfrak{a},E)$, then $M(A,i,\mathscr{C})\subseteqq K'(1)$, the Hilbert class field of K' [7, p. 137]. But $K'=K$, which has class number one.

From now on we shall assume that $(A,i,\mathscr{C})$ is of type $(K,\Phi,\mathfrak{a},E)$ and defined over K.

2. Fields of Division Values

Let $p\equiv 5 \pmod 6$ be a rational prime such that:

i) $\mathfrak{p}=p\mathcal{O}_K$ is a prime of $\mathcal{O}_K$,

ii) A has good reduction at $\mathfrak{p}$, and

iii) p is prime to the degree d of the polarization $\mathscr{C}$.

In Case II when $K=\mathbb{Q}(e^{2\pi i/5})$, we further demand that $p\equiv 7$ or $18 \bmod 25$. In either case, there are infinitely many such p. Our goal is to study the fields K_n obtained by adjoining the p^n-torsion of A to K.

We denote the units of $\mathcal{O}_K$ congruent to 1 mod $\mathfrak{p}^n$ by U_n, and the residue field at $\mathfrak{p}$ by k. We write the action of $\alpha\in\mathcal{O}_K$ on a point Q of A as $i(\alpha)(Q)=\alpha * Q$.

For $n\geqq 1$, let A_pn denote the points of order p^n on A, $A^{(p)}=\bigcup_n A_{p^n}$, and $T_p=\varprojlim_n A_pn$, the Tate module. There is a canonical injection

$$\mathrm{Gal}(K(A^{(p)})/K)\to\mathcal{O}_{\mathfrak{p}}^{\times} \quad \text{by} \quad \sigma\mapsto\alpha,$$

where $\sigma(t)=\alpha * t$ for all t in T_p. Since $K'=K$ is of class number one, the main theorem of complex multiplication [7, p. 103] tells us that the image of the Galois group is precisely $\mathbb{N}_{\Phi'}(\mathcal{O}_{\mathfrak{p}}^{\times})$. Since $\mathbb{N}_{\Phi'}(U_n)\subseteqq U_n$, we find

$$\begin{aligned}\mathrm{Gal}(K_n/K)&\cong\mathbb{N}_{\Phi'}(\mathcal{O}_{\mathfrak{p}}^{\times})/(U_n\cap\mathbb{N}_{\Phi'}(\mathcal{O}_{\mathfrak{p}}^{\times}))\\ &\cong\mathbb{N}_{\Phi'}(\mathcal{O}_{\mathfrak{p}}^{\times}/U_n)\cong\mathbb{N}_{\Phi'}((\mathcal{O}_K/\mathfrak{p}^n)^{\times}).\end{aligned}\tag{2.1}$$

From (1.4), the only choices for Φ' are $\{\sigma^i,\sigma^j\}$, $0\leqq i<j\leqq 3$, $j\neq i+2$. Hence

$$\mathbb{N}_{\Phi'}(\mathcal{O}_{\mathfrak{p}}^{\times})=\mathbb{N}_{\{1,\sigma^{j-i}\}}(\sigma^i(\mathcal{O}_{\mathfrak{p}}^{\times}))=\begin{cases}\mathbb{N}_{\{1,\sigma\}}(\mathcal{O}_{\mathfrak{p}}^{\times}) & \text{or}\\ \mathbb{N}_{\{1,\sigma^{-1}\}}(\mathcal{O}_{\mathfrak{p}}^{\times}).\end{cases}$$

Therefore, changing our choice of generator of $\mathrm{Gal}(K/\mathbb{Q})$ if necessary, we can assume without loss of generality that $\Phi'=\{1,\sigma\}$.

Lemma (2.2). *The kernel of* $\mathbb{N}_{\Phi'}:(\mathcal{O}_K/\mathfrak{p}^n)^{\times}\to(\mathcal{O}_K/\mathfrak{p}^n)^{\times}$ *is a subgroup of order* $p^{n-1}(p+1)$.

Proof. We proceed by induction. For $n=1$, we can identify $\mathcal{O}_K/\mathfrak{p}=k$ with $\mathbb{F}_{p^4}$ and $\mathrm{Gal}(K/\mathbb{Q})=\langle\sigma\rangle$ with $\mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)$. For $a\in\mathbb{F}_{p^4}$,

$$\mathbb{N}_{\Phi'}(a)=a\sigma a=1$$

implies $\sigma a\sigma^2 a=1$, or $a=\sigma^2 a$. Hence we are just counting the kernel of $\mathbb{N}((\mathbb{F}_{p^2})^{\times}/\mathbb{F}_p^{\times})$, which has order $p+1$ by Hilbert's theorem 90.

For $n>1$, consider the projection

$$\pi:\{a\in\mathcal{O}_K/\mathfrak{p}^n \mid a\sigma a\equiv 1 \bmod \mathfrak{p}^n\}\rightarrow\{a\in\mathcal{O}_K/\mathfrak{p}^{n-1} \mid a\sigma a\equiv 1 \bmod \mathfrak{p}^{n-1}\}.$$

First we compute the kernel of π. Let $a\in\mathcal{O}_K/\mathfrak{p}^n$ be such that

$$a\sigma a\equiv 1 \bmod \mathfrak{p}^n \quad \text{and} \quad a\equiv 1+bp^{n-1} \bmod \mathfrak{p}^n \quad \text{for some } b\in\mathcal{O}_K/\mathfrak{p}.$$

Then

$$\sigma a\equiv 1+(\sigma b)p^{n-1} \bmod \mathfrak{p}^n$$

so $b+\sigma b=0$. Therefore $\sigma b+\sigma^2 b=0$, and $\sigma^2 b=b$. Hence we have a bijection between the kernel of π and the kernel of $\mathrm{Tr}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, which is of order p. It remains to be shown that π is surjective. We need the following lemma:

Lemma (2.3). *Let* $G=\mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)=\langle\sigma\rangle$. *Then for* $b\in\mathbb{F}_{p^4}$

$$b-\sigma b+\sigma^2 b-\sigma^3 b=0 \Leftrightarrow b=c+\sigma c, \quad \textit{for some } c\in\mathbb{F}_p.$$

Proof. This is a restatement of $H^1(G,\mathbb{F}_p4)=0$.

Now to show that π is surjective, we need to show that if

$$a\sigma a\equiv 1+bp^{n-1} \bmod \mathfrak{p}^n$$

for $a\in\mathcal{O}_K/\mathfrak{p}^n$, then there is a $d\in\mathcal{O}_K/\mathfrak{p}$ such that

$$(a+dp^{n-1})\sigma(a+dp^{n-1})\equiv 1 \bmod \mathfrak{p}^n.$$

But this holds if and only if

$$a\sigma a+(d\sigma a+a\sigma d)p^{n-1}\equiv 1 \bmod \mathfrak{p}^n$$

that is,

$$b=-d\sigma a-a\sigma d \bmod \mathfrak{p}.$$

Note that the identity

$$\frac{a\sigma a\cdot\sigma^2(a\sigma a)}{\sigma(a\sigma a)\cdot\sigma^3(a\sigma a)}=1 \tag{2.4}$$

implies $b-\sigma b+\sigma^2 b-\sigma^3 b\equiv 0 \bmod \mathfrak{p}$, hence by Lemma (2.3), $b=c+\sigma c$ for some $c\in\mathcal{O}_K/\mathfrak{p}$. *Let* $\bar{a}$ be the image of a in $\mathcal{O}_K/\mathfrak{p}$. As before, $\bar{a}\sigma\bar{a}=1$ implies $\sigma^2\bar{a}=\bar{a}$, so we can take $d=-c/\sigma\bar{a}$.

Corollary (2.5). $\mathrm{Gal}(K_n/K)$ *has order* $p^{3n-3}(p^3-p^2+p-1)$.

The Kummer variety V of A is the quotient of A by $\mathrm{Aut}(A,i,\mathscr{C})=i(W)$. Let $h:A\rightarrow V$ be the natural projection. The following is a main result from the theory of complex multiplication which simplifies considerably in light of Proposition (1.5).

Lemma (2.6) [7, p. 138]. *The field* $E_n=K(h(A_{p^n}))$ *is a class field over* K *of conductor dividing* $\mathfrak{p}^n$. *Its Galois group over* K *is isomorphic to* $I(\mathfrak{p})/H(\mathfrak{p}^n)$, *where* $I(\mathfrak{p})$ *is the group of fractional ideals prime to* $\mathfrak{p}$, *and* $H(\mathfrak{p}^n)$ *consists of those ideals* $\mathfrak{B}$ *prime to* $\mathfrak{p}$ *such that:*

There exists $\beta \in K$ satisfying

i) $\mathbb{N}_{\Phi'}(\mathscr{B}) = \mathscr{B}\sigma(\mathscr{B}) = (\beta)$

ii) $\mathbb{N}_{K/\mathbb{Q}}(\mathscr{B}) = \beta\sigma^2\beta$

iii) $\beta \equiv 1 \bmod \mathfrak{p}^n$.

Corollary (2.7). 1) *The group $H(\mathfrak{p}^n)$ consists of ideals (α) such that:*

$$\alpha\sigma\alpha \equiv w \bmod \mathfrak{p}^n, \quad \textit{for some } w \in W.$$

2) $\mathrm{Gal}(K_n/E_n) \cong W.$

Proof. 1) Suppose $\mathscr{B} \in H(\mathfrak{p}^n)$. Then $\mathscr{B} = (\alpha)$, for some $\alpha \in \mathcal{O}_K$, so i) implies $\alpha\sigma\alpha = w\varepsilon^i\beta$ for some $w \in W$; ii) implies $i=0$, so iii) implies $\alpha\sigma\alpha \equiv w \bmod \mathfrak{p}^n$.

2) By Lemma (1.3), $\mathbb{N}_{\Phi'}(U) = W$, so the choice of the generator α is irrelevant. Also, since W injects into $\mathcal{O}/\mathfrak{p}^n$, we see that the kernel of the projection

$$(\mathcal{O}_K/\mathfrak{p}^n)^\times \to I(\mathfrak{p})/H(\mathfrak{p}^n)$$

is precisely $\{w\alpha \mid \mathbb{N}_{\Phi'}(\alpha) = 1\}$. Hence by (2.1), $\mathrm{Gal}(K_n/E_n) \cong W$.

An important observation is that since K is totally imaginary and of class number one, E_n is totally ramified over K. We will let $\mathscr{B}_n$ denote the unique prime of E_n over $\mathfrak{p}$. Set $E_0 = K$.

Lemma (2.8). *If $K \subseteqq L \subseteqq E_n$ and* $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}(E_n/K)) \leqq i$, *then $L \subseteqq E_i$.*

Proof. It suffices to show this for $i = n-1$. For $n=1$, the result is immediate because K has no unramified abelian extensions. For $n>1$, the class group H belonging to L/K via class field theory contains those (a) such that $a\sigma a \equiv w \bmod \mathfrak{p}^n$ for some $w \in W$, as well as those for which $a \equiv 1 \bmod \mathfrak{p}^{n-1}$. We seek to show it contains all (a) with $a\sigma a \equiv w \bmod \mathfrak{p}^{n-1}$ for some $w \in W$. But for such an a,

$$a\sigma a \equiv w + bp^{n-1} \bmod \mathfrak{p}^n \quad \text{for some } b \in \mathcal{O}_K/\mathfrak{p}.$$

And by the identity (2.4),

$$(b/w) - \sigma(b/w) + \sigma^2(b/w) - \sigma^3(b/w) = 0.$$

Hence by Lemma (2.3), $b/w = c + \sigma c$ for some $c \in \mathcal{O}_K/\mathfrak{p}$. Setting $d = 1 + cp^{n-1} \bmod \mathfrak{p}^n$, we have (d) and (σd) in H. Since

$$(a/d)\sigma(a/d) \equiv (w + bp^{n-1})(1 - (c + \sigma c)p^{n-1}) \equiv w \bmod \mathfrak{p}^n$$

it follows that (a/d) – and hence (a) – is in H.

Lemma (2.9). 1) $\mathfrak{p}$ *ramifies totally in K_n/K. We let $\mathfrak{p}_n$ denote the unique prime of K_n over $\mathfrak{p}$.*

2) *A has good reduction everywhere over K_1.*

3) *K_n/K_1 is unramified outside $\mathfrak{p}_1$.*

4) *Let ψ be any non-trivial first-degree character on* $\mathrm{Gal}(K_n/K_1)$, *and* $\mathfrak{f}(\psi)$ *its conductor. Then* $\mathrm{ord}_{\mathfrak{p}_1}\mathfrak{f}(\psi) \geqq p^3 - p^2 + p$.

Proof. 1) Consider the tower:

$$\begin{tikzcd}
K_n \arrow[dr, dash, "|W|"] \arrow[dd, dash, "p^{3n-3}"'] & \\
& E_n \arrow[dd, dash, "p^{3n-3}"] \\
K_1 \arrow[dr, dash, "|W|"'] & \\
& E_1 \arrow[d, dash, "(1/|W|)(p^3-p^2+p-1)"] \\
& K
\end{tikzcd}$$

In Case I, $|W|=2$ and $2\,|\,(1/2)(p^2+1)(p-1)$ since p is odd. In Case II, $|W|=10$ and $10\,|\,(1/10)(p^2+1)(p-1)$ since p is odd, and in this case we took $p\equiv 7$ or $18 \bmod 25$. Since $\mathrm{Gal}(K_1/K)$ is cyclic, Lemma (1.2) shows $\mathfrak{p}$ ramifies totally in K_1. But now $\mathscr{P}_1$ ramifies totally in K_1 and in E_n, and $(|W|,p)=1$, so $\mathscr{P}_1$ – and hence $\mathfrak{p}$ – ramifies totally in K_n.

2) This follows essentially by the argument given in [2, Theorem 2]. Let $\mathfrak{q}\nmid\mathfrak{p}_1$ be any prime in K_1, $\mathscr{Q}$ an extension of $\mathfrak{q}$ to $\bar{K}_1$ (the algebraic closure of K_1), and $I_{\mathscr{Q}}$ its inertia group. Then the image of the natural map

$$\varrho:\mathrm{Gal}(\bar{K}_1/K_1)\to\mathrm{Aut}(T_p)\cong\mathcal{O}_p^\times$$

is contained in U_1, since $A_p\subseteq K_1$. However, by [7, p. 100], A has potentially good reduction at $\mathfrak{q}$, so by [18, p. 496], $\varrho(I_{\mathscr{Q}})$ is a finite group. Since there are no non-trivial finite subgroups of U_1, $I_{\mathscr{Q}}$ acts trivially on T_p, and so A has good reduction at $\mathfrak{q}$ by the criterion of Néron-Ogg-Shafarevich.

3) By (2) and the criterion of Néron-Ogg-Shafarevich, K_n/K_1 can only be ramified at primes of K_1 dividing p.

4) By (3), we know $\mathfrak{f}(\psi)$ is a power of $\mathfrak{p}_1$. Let $L(\psi)$ be the fixed field of the kernel of ψ, and $M=L(\psi)\cap E_n$.

$$\begin{tikzcd}
L(\psi) \arrow[d, dash, "p"'] \arrow[dr, dash, "|W|"] & \\
K_1 \arrow[dr, dash, "|W|"'] & M. \arrow[d, dash, "p"] \\
& E_1
\end{tikzcd} \tag{2.10}$$

Let χ be any non-trivial first degree character on $\mathrm{Gal}(M/K)$, and $L(\chi)$ its fixed field. By (2.8), either $L(\chi)\subseteq E_1$ or $\mathrm{ord}_\mathfrak{p}\mathfrak{f}(\chi)\geqq 2$.

So by the conductor-discriminant formula,

$$\begin{aligned}\mathrm{ord}_\mathfrak{p}D(M/K)&=\mathrm{ord}_\mathfrak{p}D(E_1/K)+\sum_{L(\chi)\notin E_1}\mathrm{ord}_\mathfrak{p}\mathfrak{f}(\chi)\\&\geqq(1/|W|)(p^3-p^2+p-1)-1+2(p-1)(1/|W|)(p^3-p^2+p-1)\end{aligned}$$

since E_1/K is totally ramified. However,

$$D(M/K)=\mathbb{N}_{E_1/K}(D(M/E_1))(D(E_1/K))^p$$

so $\mathrm{ord}_{\mathscr{P}}D(M/E_1)\geqq(p-1)((1/|W|)(p^3-p^2+p-1)+1)$.

Finally, since $p \nmid |W|$, computing $D(L(\psi)/E_1)$ both ways up the tower (2.10) yields:

$$\operatorname{ord}_{\mathfrak{p}_1} D(L(\psi)/K_1) \geqq (p-1)(p^3-p^2+p)$$

hence $\operatorname{ord}_{\mathfrak{p}_1} \mathfrak{f}(\psi) \geqq p^3-p^2+p$.

3. Formal Groups

Let $\mathscr{A} = A \times_{\operatorname{Spec}(K)} \operatorname{Spec}(K_\mathfrak{p})$, and $N(\mathscr{A})$ be the Néron model of $\mathscr{A}$. The kernel of reduction of $\mathscr{A}$ modulo $\mathfrak{p}$ is the formal group functor $\mathscr{A}_0$ over $\operatorname{Spec}(\mathcal{O}_\mathfrak{p})$ defined by:

$$0 \to \mathscr{A}_0(R) \to N(\mathscr{A})(R) \to N(\mathscr{A})(R/\mathfrak{p}R) \to 0,$$

where R is any $\mathcal{O}_\mathfrak{p}$-algebra.

Since $N(\mathscr{A})$ is smooth, $\mathscr{A}_0$ is represented by a two-dimensional formal group law $\mathscr{F}$ over $\mathcal{O}_\mathfrak{p}$. If R is any $\mathcal{O}_\mathfrak{p}$-algebra, we let $\mathscr{F}(R)$ denote the R-points of $\mathscr{F}$. In particular, if L is any extension of $K_\mathfrak{p}$ whose ring of integers has maximal ideal $\mathfrak{m}$, then

$$\mathscr{A}_0(L) \cong \mathscr{F}(L) \cong \mathfrak{m} \times \mathfrak{m}.$$

Specifically, if we take local parameters at the origin, t_1, t_2, we can write the isomorphism as

$$\mathscr{A}_0(L) \ni u \mapsto (t_1(u), t_2(u)) \in \mathfrak{m} \times \mathfrak{m}.$$

Then the formal group law $+_\mathscr{F}$ is given by

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} +_\mathscr{F} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} f_1(x_1, x_2, y_1, y_2) \\ f_2(x_1, x_2, y_1, y_2) \end{bmatrix},$$

where the $f_i \in \mathcal{O}_\mathfrak{p}[[x_1, x_2, y_1, y_2]]$, $i=1,2$, satisfy

$$t_i(u+v) = f_i(t_1(u), t_2(u), t_1(v), t_2(v)).$$

If $\phi \in \mathcal{O}_K = \operatorname{End}(A)$, then ϕ determines formal power series $\phi_i \in S = \mathcal{O}_\mathfrak{p}[[x_1, x_2]]$, $i=1,2$, via

$$t_i(\phi * u) = \phi_i(t_1(u), t_2(u)).$$

These ϕ_i determine an endomorphism $[\phi]_\mathscr{F}$ of $\mathscr{F}$ given by

$$[\phi]_\mathscr{F} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \phi_1(x_1, x_2) \\ \phi_2(x_1, x_2) \end{bmatrix}.$$

By reducing $[\ ]_\mathscr{F} \bmod \mathfrak{p}$, we get an endomorphism $[\ ]_{\bar{\mathscr{F}}}$ on the reduced formal group law $\bar{\mathscr{F}}$ defined over k.

Set $S^+ = \{\alpha \in S \mid \alpha(0,0) = 0\}$, and let $\delta = (\delta_1, \delta_2)$, where $\delta_1, \delta_2 \in S^+$. We get a map $\delta: S^+ \times S^+ \to S^+ \times S^+$ by $\delta(f, g) = (\delta_1(f, g), \delta_2(f, g))$. Recall that δ is invertible if and only if the determinant of the jacobian matrix $\operatorname{jac}(\delta)$ is a unit in $\mathcal{O}_\mathfrak{p}$. We let T denote the group of all such invertible δ.

Our choice of $\mathscr{F}$ is not unique. Indeed we will soon replace $\mathscr{F}$ with an isomorphic formal group law which it is more convenient to work with.

Recall that $k[[x_1, x_2]]$ is a free $[\mathfrak{p}]_{\mathscr{F}} k[[x_1, x_2]]$ module. If this rank is finite, it is of the form p^h, and h is called the height of $\mathscr{F}$ [5, p. 151–152].

Lemma (3.1). *The formal group law* $\mathscr{F}$ *has height* 4.

Proof. Let $\tilde{\mathscr{A}}$ denote the special fibre of $N(\mathscr{A})$. By the theory of complex multiplication, the Frobenius on $\tilde{\mathscr{A}}$ is induced by $i(\phi_{\mathfrak{p}})$, where $\phi_{\mathfrak{p}}$ is an element in $\mathcal{O}_K$ such that for every complex absolute value $|\ |$, $|\phi_{\mathfrak{p}}| = (\mathbb{N}_{K/\mathbb{Q}}(\mathfrak{p}))^{1/2} = p^2$ [7, pp. 86–88]. Hence the Frobenius is given by $[wp^2]_{\mathscr{F}}$ for some $w \in W$. Therefore

$$[p^2]_{\mathscr{F}} k[[x_1, x_2]] = [w^{-1}]_{\mathscr{F}} k[[x_1^{p^4}, x_2^{p^4}]] = k[[x_1^{p^4}, x_2^{p^4}]]$$

since $[w^{-1}]_{\mathscr{F}}$ is an automorphism. So $k[[x_1, x_2]]$ is a $[p^2]_{\mathscr{F}} k[[x_1, x_2]]$-module of rank p^8, and hence a $[p]_{\mathscr{F}} k[[x_1, x_2]]$-module of rank p^4.

Lemma (3.2) [5, pp. 360–361]. *There are formal group laws* $\mathscr{g}$ *and* $\mathscr{h}$ *over* k, *and isomorphisms*

$$\mathscr{a} : \bar{\mathscr{F}} \to \mathscr{g}$$
$$\mathscr{b} : \bar{\mathscr{F}} \to \mathscr{h}$$

such that the homomorphism

$$\mathscr{c} = \mathscr{b} \circ [p]_{\mathscr{F}} \circ \mathscr{a}^{-1} : \mathscr{g} \to \mathscr{h}$$

is of the form:

$$\mathscr{c}(x_1, x_2) = ((x_1)^{p^{n_1}}, (x_2)^{p^{n_2}})$$

where $n_1 \geqq n_2$, *and* $n_1 + n_2 = 4$.

Corollary (3.3). *There are formal group laws* $\mathscr{G}$ *and* $\mathscr{H}$ *over* $\mathcal{O}_{\mathfrak{p}}$, *and isomorphisms*

$$\alpha : \mathscr{F} \to \mathscr{G}$$
$$\beta : \mathscr{F} \to \mathscr{H}$$

such that the homomorphism

$$\gamma = \beta \circ [p]_{\mathscr{F}} \circ \alpha^{-1} : \mathscr{G} \to \mathscr{H}$$

is of the form:

$$\gamma(x_1, x_2) \equiv ((x_1)^{p^{n_1}}, (x_2)^{p^{n_2}}) \bmod \mathfrak{p},$$

where $n_1 \geqq n_2$, *and* $n_1 + n_2 = 4$.

Proof. Lift $\mathscr{a}$ and $\mathscr{b}$ to power series α and β with coefficients in $\mathcal{O}_{\mathfrak{p}}$, and without constant term. Since $\mathscr{a}$ and $\mathscr{b}$ are isomorphisms, the determinants of $\operatorname{jac}(\alpha)$ and $\operatorname{jac}(\beta)$ are units in $\mathcal{O}_{\mathfrak{p}}$, and hence α, $\beta \in T$. So define

$$u +_{\mathscr{G}} v = \alpha(\alpha^{-1}(u) +_{\mathscr{F}} \alpha^{-1}(v))$$
$$u +_{\mathscr{H}} v = \beta(\beta^{-1}(u) +_{\mathscr{F}} \beta^{-1}(v)).$$

Then $\gamma = \beta \circ [p]_{\mathscr{F}} \circ \alpha^{-1}$ has the desired property.

Corollary (3.4). *There is a formal group law $\mathcal{G}$ over $\mathcal{O}_{\mathfrak{p}}$, and an isomorphism, $\alpha : \mathcal{F} \to \mathcal{G}$, such that*

$$[p]_{\mathcal{G}} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \equiv \delta \begin{bmatrix} (x_1)^{n_1} \\ (x_2)^{n_2} \end{bmatrix} \bmod \mathfrak{p},$$

where $n_1 \geqq n_2$, $n_1 + n_2 = 4$, and $\delta \in T$.

Proof. Take $\mathcal{G}$ as in (3.3). Since α is an isomorphism,

$$[p]_{\mathcal{G}} = \alpha \circ [p]_{\mathcal{F}} \circ \alpha^{-1} = \alpha \circ \beta^{-1} \circ \gamma$$

so we can take $\delta = \alpha \circ \beta^{-1}$.

By transport of structure, we set $[\phi]_{\mathcal{G}} = \alpha \circ [\phi]_{\mathcal{F}} \circ \alpha^{-1}$ for all $\phi \in \mathcal{O}_K$. Likewise, if L is any extension of $K_{\mathfrak{p}}$ whose ring of integers has maximal ideal $\mathfrak{m}$, then setting $(s_1(u), s_2(u)) = \alpha \circ (t_1(u), t_2(u))$, gives us an isomorphism

$$\mathcal{A}_0(L) \cong \mathfrak{m} \times \mathfrak{m}$$

by

$$u \mapsto (s_1(u), s_2(u)).$$

Let $(d^0 \geqq n)(z_1, \ldots, z_m)$ denote a power series in $z_1, \ldots, z_m$, all of whose terms have total degree greater than or equal to n.

Proposition (3.5). *For some $\delta \in T$,*

$$[p]_{\mathcal{G}} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \equiv \delta \begin{bmatrix} (x_1)^{p^3} \\ (x_2)^{p} \end{bmatrix} \bmod \mathfrak{p}.$$

Proof. Since $\operatorname{jac}([p]_{\mathcal{G}})$ is the zero matrix, [5, pp. 150–151] implies n_1, $n_2 \geqq 1$. It remains only to rule out the possibility that $n_1 = n_2 = 2$. Suppose this were the case. Let $u \in A_p$, $u \neq 0$. Then $u \in \mathcal{A}_0((K_1)_{\mathfrak{p}_1})$, and by assumption,

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = [p]_{\mathcal{G}} \begin{bmatrix} s_1(u) \\ s_2(u) \end{bmatrix} \equiv \delta \begin{bmatrix} s_1(u)^{p^2} \\ s_2(u)^{p^2} \end{bmatrix} \bmod \mathfrak{p}.$$

As in any formal group:

$$[p]_{\mathcal{G}} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} p x_1 + (d^0 \geqq 2)(x_1, x_2) \\ p x_2 + (d^0 \geqq 2)(x_1, x_2) \end{bmatrix}.$$

Let $\operatorname{jac}(\delta)^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then together we have

$$\begin{aligned} \begin{bmatrix} 0 \\ 0 \end{bmatrix} &= \delta^{-1} [p]_{\mathcal{G}} \begin{bmatrix} s_1(u) \\ s_2(u) \end{bmatrix} \\ &= \begin{bmatrix} a p s_1(u) + b p s_2(u) + s_1(u)^{p^2} + p(d^0 \geqq 2)(s_1(u), s_2(u)) \\ c p s_1(u) + d p s_2(u) + s_2(u)^{p^2} + p(d^0 \geqq 2)(s_1(u), s_2(u)) \end{bmatrix}. \end{aligned} \qquad \begin{matrix} (3.6\text{I}) \\ (3.6\text{II}) \end{matrix}$$

By symmetry, there are only two cases to rule out:

i) $\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) < \operatorname{ord}_{\mathfrak{p}_1}(s_2(u))$

ii) $\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) = \operatorname{ord}_{\mathfrak{p}_1}(s_2(u))$.

Case (i). If $a \not\equiv 0 \bmod \mathfrak{p}$, then comparing the terms of (3.6I) of least valuation at $\mathfrak{p}_1$ yields:

$$\operatorname{ord}_{\mathfrak{p}_1}(aps_1(u)) = \operatorname{ord}_{\mathfrak{p}_1}(s_1(u)^{p^2}),$$

or

$$p^3 - p^2 + p - 1 = (p^2 - 1)\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)),$$

an impossibility.

If $a \equiv 0 \bmod \mathfrak{p}$, then $c \not\equiv 0 \bmod \mathfrak{p}$. So comparing terms of (3.6II) of least valuation at $\mathfrak{p}_1$ gives us

$$\operatorname{ord}_{\mathfrak{p}_1}(cps_1(u)) = \operatorname{ord}_{\mathfrak{p}_1}(s_2(u)^{p^2});$$

so

$$p^3 - p^2 + p - 1 + \operatorname{ord}_{\mathfrak{p}_1}(s_2(u)) > (p^2)\operatorname{ord}_{\mathfrak{p}_1}(s_2(u)),$$

or

$$(p^3 - p^2 + p - 1)/(p^2 - 1) > \operatorname{ord}_{\mathfrak{p}_1}(s_2(u)) > \operatorname{ord}_{\mathfrak{p}_1}(s_1(u)).$$

Hence

$$p - 1 > \operatorname{ord}_{\mathfrak{p}_1}(s_1(u)). \tag{3.7}$$

However, (3.6I) implies

$$\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)^{p^2}) \geqq \operatorname{ord}_{\mathfrak{p}_1}(p) = p^3 - p^2 + p - 1;$$

so

$$\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) \geqq p,$$

which contradicts (3.7).

Case (ii). Say $\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) = \operatorname{ord}_{\mathfrak{p}_1}(s_2(u)) = m$. Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible, either

$$1)\ \operatorname{ord}_{\mathfrak{p}_1}(as_1(u) + bs_2(u)) = m,$$

or

$$2)\ \operatorname{ord}_{\mathfrak{p}_1}(cs_1(u) + ds_2(u)) = m.$$

Comparing terms of least valuation at $\mathfrak{p}_1$ in (3.6I) [if (1) holds] or (3.6II) [if (2) holds], we find

$$p^3 - p^2 + p - 1 + m = p^2 m,$$

an impossibility. Q.E.D.

Proposition (3.8). *Let $u \in A_p$, $u \neq 0$. Then*

$$\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) = 1, \quad \operatorname{ord}_{\mathfrak{p}_1}(s_2(u)) = p^2 - p + 1.$$

Proof. Let $\begin{bmatrix} AB \\ CD \end{bmatrix} = \mathrm{jac}(\delta)$. We have

$$[p^2]_{\mathscr{G}} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = [p]_{\mathscr{G}} \begin{bmatrix} Ax_1^{p^3} + Bx_2^{p} + (d^0 \geqq 2)(x_1^{p^3}, x_2^{p}) \\ Cx_1^{p^3} + Dx_2^{p} + (d^0 \geqq 2)(x_1^{p^3}, x_2^{p}) \end{bmatrix} \bmod \mathfrak{p}$$

$$= \begin{bmatrix} BD^p x_2^{p^2} + (d^0 \geqq 2p^2)(x_1, x_2) \\ D^{p+1} x_2^{p^2} + (d^0 \geqq 2p^2)(x_1, x_2) \end{bmatrix} \bmod \mathfrak{p}.$$

But since for some $w \in W$, $[p^2 w]_{\mathscr{G}}$ is the Frobenius,

$$[p^2]_{\mathscr{G}} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in k[[x_1^{p^4}, x_2^{p^4}]];$$

hence $D \equiv 0 \bmod \mathfrak{p}$. So if $\mathrm{jac}(\delta)^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $a \equiv 0 \bmod \mathfrak{p}$, and therefore $b, c \not\equiv 0 \bmod \mathfrak{p}$.

As in the previous proof:

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \delta^{-1} [p]_{\mathscr{G}} \begin{bmatrix} s_1(u) \\ s_2(u) \end{bmatrix}$$

$$= \begin{bmatrix} aps_1(u) + bps_2(u) + s_1(u)^{p^3} + p(d^0 \geqq 2)(s_1(u), s_2(u)) \\ cps_1(u) + dps_2(u) + s_2(u)^p + p(d^0 \geqq 2)(s_1(u), s_2(u)) \end{bmatrix}. \quad \begin{matrix} (3.9\text{I}) \\ (3.9\text{II}) \end{matrix}$$

If $\mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) \geqq \mathrm{ord}_{\mathfrak{p}_1}(s_2(u))$, then comparing terms in (3.9I) of least valuation at $\mathfrak{p}_1$ yields

$$\mathrm{ord}_{\mathfrak{p}_1}(bps_2(u)) = \mathrm{ord}_{\mathfrak{p}_1}(s_1(u)^{p^3})$$

or

$$p^3 - p^2 + p - 1 + \mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) \geqq (p^3)\, \mathrm{ord}_{\mathfrak{p}_1}(s_1(u)),$$

a contradiction.

So $\mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) < \mathrm{ord}_{\mathfrak{p}_1}(s_2(u))$, and comparing terms in (3.9II) of least valuation at $\mathfrak{p}_1$ gives us

$$\mathrm{ord}_{\mathfrak{p}_1}(cps_1(u)) = \mathrm{ord}_{\mathfrak{p}_1}(s_2(u)^p),$$

or

$$p^3 - p^2 + p - 1 + \mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) = (p)\, \mathrm{ord}_{\mathfrak{p}_1}(s_2(u)). \tag{3.10}$$

Hence

$$p^2 + 1 > \mathrm{ord}_{\mathfrak{p}_1}(s_2(u)) \geqq p^2 - p + 1. \tag{3.11}$$

By (3.10) $\mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) \equiv 1 \bmod p$. Say $\mathrm{ord}_{\mathfrak{p}_1}(s_1(u)) = 1 + kp$. Then (3.10) implies

$$\mathrm{ord}_{\mathfrak{p}_1}(s_2(u)) = p^2 - p + 1 + k.$$

So by (3.11),

$$p > k \geqq 0.$$

Assume that $k \neq 0$. Since

$$\operatorname{ord}_{\mathfrak{p}_1}(bps_2(u)) = p^3 + k$$
$$\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)^{p^3}) = p^4 k + p^3$$

the terms in (3.9ɪ) of least valuation at $\mathfrak{p}_1$ must be $bps_2(u)$ and $eps_1(u)^i$ for some $e \not\equiv 0 \bmod \mathfrak{p}$ and $i > 1$. Equating their valuation at $\mathfrak{p}_1$ yields

$$i(pk+1) = p^2 - p + 1 + k. \tag{3.12}$$

Hence $i \equiv 1 + k \bmod p$; since $i > 1$, $i = 1 + k + pj$ for some $j \geqq 0$. But this contradicts (3.12) unless $j = 0$. Plugging $i = 1 + k$ into (3.12) gives us

$$p = k^2 + k + 1.$$

However, this is impossible since we have been assuming all along that $p \equiv 2 \bmod 3$. Therefore $k = 0$, $\operatorname{ord}_{\mathfrak{p}_1}(s_1(u)) = 1$, and $\operatorname{ord}_{\mathfrak{p}_1}(s_2(u)) = p^2 - p + 1$.

Remark. This is the only place where we need $p \equiv 2 \bmod 3$. The results of this paper hold equally well for primes $p \equiv 1 \bmod 6$ which remain prime in K, are prime to the degree of the polarization, and at which A has good reduction, so long as they are not of the form $k^2 + k + 1$.

4. The Tower

Suppose now that the $\mathcal{O}_K$-rank of $A(K)$ is positive. Let $Q = Q_0$ be a point of infinite order in $A(K)$ which does not lie in $pA(K)$. There is an integer λ prime to p such that $\lambda * Q \in \mathscr{A}_0$, so we will assume that $Q \in \mathscr{A}_0$. Choose $Q_n \in A(\bar{K})$ recursively so that $p * Q_n = Q_{n-1}$. Let $M_n(Q) = K(Q_n)$, and $L_n(Q) = K_n(Q_n)$.

For $n \geqq 1$, $L_n(Q)/K$ is a normal extension and we get an embedding

$$\begin{gathered} \operatorname{Gal}(L_n(Q)/K) \to Gl_2(\mathcal{O}_K/\mathfrak{p}^n), \\ \tau \mapsto \begin{pmatrix} 1 & a_\tau \\ 0 & b_\tau \end{pmatrix} \end{gathered} \tag{4.1}$$

via the action

$$\tau(Q_n) = Q_n + a_\tau, \qquad \tau(a) = b_\tau * a,$$

where $a, a_\tau \in A_p n \cong \mathcal{O}_K/\mathfrak{p}^n$, and $b_\tau \in (\mathcal{O}_K/\mathfrak{p}^n)^\times$.

Lemma (4.2). $\operatorname{Gal}(L_n(Q)/K_n) \cong A_{p^n}$.

Proof. When $n = 1$, Ribet [9] gives a sufficient criterion for the lemma to hold, which reduces in our case to

$$\mathbb{Z}/p\mathbb{Z}[\operatorname{Gal}(K_1/K)] = k = \mathbb{F}_{p^4}. \tag{4.3}$$

But (4.3) holds since $|\operatorname{Gal}(K_1/K)| = (p^2+1)(p-1) > p^2$: hence there is an element of $\operatorname{Gal}(K_1/K)$ which is not in $\mathbb{F}_{p^2}$. The validity of the lemma for $n > 1$ can be deduced from that of $n = 1$ by modifying an argument of Lang's for elliptic curves [6, pp. 117–118].

From Corollary (2.5) and Lemma (4.2) we have the following tower of fields

$$\begin{tikzcd}
 & L_n(Q) \arrow[dl, dash, "p^{3n-3}(p^2+1)(p-1)"'] \arrow[dr, dash, "p^{4n}"] \arrow[dd, dash, dashed] & \\
M_n(Q) \arrow[dd, dash, dashed, "p^{4n-4}"'] & & K_n \arrow[dd, dash, dashed, "p^{3n-3}"] \\
 & L_1(Q) \arrow[dl, dash] \arrow[dr, dash] & \\
M_1(Q) \arrow[dr, dash, "p^4"'] & & K_1 \arrow[dl, dash, "(p^2+1)(p-1)"] \\
 & K &
\end{tikzcd}$$

If χ is a character on a subgroup H of $\mathrm{Gal}(L_n(Q)/K)$, we let χ^* denote the corresponding induced character on $\mathrm{Gal}(L_n(Q)/K)$. Let $\mathrm{char}(n) = \{\chi \in \widehat{\mathrm{Gal}}(L_n(Q)/K_n) \mid \chi^{p^{n-1}} \neq 1\}$.

Proposition (4.4). *Let $\psi \in \mathrm{char}(n)$ be arbitrary. Then the map*

$$\mathrm{ind}: \chi \mapsto \chi^*$$

sends $p^{3n-3}(p^3-p^2+p-1)$ distinct elements of $\mathrm{char}(n)$ *to ψ^*.*

Proof. The proof involves simple counting arguments and Frobenius reciprocity. It follows precisely the argument used in [4, Proposition 2]. Details can be found in [3].

Our goal is to calculate the conductor $\mathfrak{f}(\chi)$ for all $\chi \in \mathrm{char}(n)$. By the following lemma, we know that $\mathfrak{f}(\chi)$ must be a power of $\mathfrak{p}_n$.

Lemma (4.5). *$L_n(Q)/K_n$ is unramified outside $\mathfrak{p}_n$.*

Proof. Since $\mathfrak{p}_n$ is the unique prime of K_n over p, this follows from Corollary (2.9) [8, p. 144].

We have a filtration $\mathscr{A}_0(K_\mathfrak{p}) \supsetneqq \mathscr{A}_1(K_\mathfrak{p}) \supsetneqq \dots$ defined by

$$\mathscr{A}_i(K_\mathfrak{p}) = \{u \in \mathscr{A}_0(K_\mathfrak{p}) \mid \mathrm{ord}_\mathfrak{p}(s_j(u)) > i; \quad j = 1, 2\}, \tag{4.6}$$

where

$$[p]_\mathscr{G} : \mathscr{A}_i(K_\mathfrak{p}) \to \mathscr{A}_{i+1}(K_\mathfrak{p})$$

is an isomorphism for all $i \geqq 0$ [17].

Lemma (4.7). *Let e be the smallest integer such that $Q \notin \mathscr{A}_e(K_\mathfrak{p})$.*

i) *For $1 \leqq n < e$, $\mathfrak{p}_n$ splits completely in $L_n(Q)$.*

ii) *$L_e(Q)/K_e$ is ramified over $\mathfrak{p}_e$.*

Proof. i) By (4.6) there is a $\tilde{Q}_n \in \mathscr{A}_{e-n-1}(K_\mathfrak{p})$ such that $[p^n]_\mathscr{G} \tilde{Q}_n = Q$. Hence $Q_n = \tilde{Q}_n + u$ for some $u \in A_{p^n}$, and $Q_n \in \mathscr{A}_0((K_n)_{\mathfrak{p}_n})$.

ii) The proof uses Sah's lemma [15] and Corollary (2.5) and is easily adapted from either [2] or [4].

Lemma (4.8). *Let e be as above, and* $G = \mathrm{Gal}(L_e(Q)/K_e)$.

i) *Let* $b \geqq 0$. *The number of* $\chi \in \mathrm{char}(e)$ *such that* $\mathfrak{f}(\chi)$ *divides* $(\mathfrak{p}_e)^b$ *is either* 0 *or* $p^{4e-4}(p^4-1)$.

ii) *All* $\chi \in \mathrm{char}(e)$ *have the same conductor, and* $L_e(Q)/K_eL_{e-1}(Q)$ *is totally ramified at any of the primes* $\mathfrak{q}$ *in* $K_eL_{e-1}(Q)$ *which lie above* $\mathfrak{p}_e$.

Proof. i) Take $\chi \in \mathrm{char}(e)$. Since $\chi^{p^{e-1}} \neq 1$, its fixed field $L(\chi)$ is not contained in $K_eL_{e-1}(Q)$. Hence if $\bar{\chi}$ is the restriction of χ to $\mathrm{Gal}(L_e(Q)/K_eL_{e-1}(Q))$, then $\bar{\chi} \neq 1$, and the fixed field $L(\bar{\chi}) = L(\chi)L_{e-1}(Q)$ is of degree p over $K_eL_{e-1}(Q)$. Since $L_{e-1}(Q)K_e/K_e$ is unramified, $\mathfrak{f}(\bar{\chi}) = \mathfrak{f}(\chi)$.

Let $b \geqq 0$. We want to count the number N of $\chi \in \mathrm{char}(e)$ such that $\mathfrak{f}(\chi)$ divides $(\mathfrak{p}_e)^b$.

Let T be the maximal subfield in $L_e(Q)$ such that $T/K_eL_{e-1}(Q)$ has conductor $(\mathfrak{p}_e)^b$. Then $[T : K_eL_{e-1}(Q)] = p^a$ where $a = 0, 1, 2, 3$, or 4.

On one hand, Proposition (4.4) implies that N is a multiple of $p^{3e-3}(p^3-p^2+p-1)$. On the other hand, $\mathfrak{f}(\chi) = \mathfrak{f}(\bar{\chi})$ divides $(\mathfrak{p}_e)^b$ if and only if $L(\bar{\chi}) \subseteqq T$. But there are p^{4e-4} of the χ which restrict to a given $\bar{\chi}$, $p-1$ of the $\bar{\chi}$ which determine a given $L(\bar{\chi})$, and $(p^a-1)/(p-1)$ subfields of T with degree p over $K_eL_{e-1}(Q)$. Therefore $N = p^{4e-4}(p^a-1)$, and

$$p^{3e-3}(p^3-p^2+p-1) \mid p^{4e-4}(p^a-1)$$

which only holds when $a = 0$ or $a = 4$.

ii) Let $f(\chi) = \mathrm{ord}_{\mathfrak{p}_e}(\mathfrak{f}(\chi))$. By the choice of e, for some $\xi \in \mathrm{char}(e)$ we have $f(\xi) > 0$, and we can choose ξ so that $f(\xi) > 0$ is minimal. Applying (*i*) with $b = 0$ we see that for all $\chi \in \mathrm{char}(e)$, $f(\chi) > 0$, hence applying (*i*) again with $b = f(\xi)$ we see that for all $\chi \in \mathrm{char}(e)$, $f(\chi) = f(\xi)$.

Finally, let $I_\mathfrak{q}$ be the fixed field of the inertia group of $\mathfrak{q}$ in L_e. If $I_\mathfrak{q} \neq K_eL_{e-1}(Q)$ then there is a $\chi \in \mathrm{char}(e)$ such that $L(\bar{\chi}) \subseteqq I_\mathfrak{q}$.

Corollary (4.9). *For any* χ *in* $\mathrm{char}(e)$

$$\mathfrak{f}(L_e(Q)/K_e) = \mathfrak{f}(\chi)\,.$$

Proof. $\mathfrak{f}(L_e(Q)/K_e) = gcd(\mathfrak{f}(\chi))$.

We will let $\mathfrak{f}(Q)$ denote the common value $\mathrm{ord}_{\mathfrak{p}_e}(\mathfrak{f}(\chi)) = \mathrm{ord}_{\mathfrak{p}_e}(\mathfrak{f}(L_e(Q)/K_e))$. The next section is devoted to calculating $\mathfrak{f}(Q)$.

5. Conductor Calculations

For any $\phi \in \mathcal{O}_K = \mathrm{End}(A)$, let $\mathcal{G}_\phi$ denote the kernel of $[\phi]_\mathcal{G}$. Then for any $n \geqq 1$,

$$(K_n)_{\mathfrak{p}_n} = K_\mathfrak{p}(\mathcal{G}_{p^n})$$

and by (4.7), there is a prime π of $M_{e-1}(Q)$ over $\mathfrak{p}$ such that

$$(M_{e-1}(Q))_\pi = K_\mathfrak{p}\,.$$

Therefore, if π_e is any prime of $L_{e-1}(Q)K_e$ over π, and π_1 its restriction to $K_1(Q_{e-1})$ we have

$$(L_{e-1}(Q)K_e)_{\pi_e} = (K_e)_{\mathfrak{p}_e}\,,$$

and

$$(K_1(Q_{e-1}))_{\pi_1} = (K_1)_{\mathfrak{p}_1}\,.$$

By Lemma (4.8), there is a unique prime $\mathscr{P}_e$ of $L_e(Q)$ over π_e, and $(L_e(Q))_{\mathscr{P}_e}/(L_{e-1}(Q)K_e)_{\pi_e}$ is a totally ramified extension of conductor $(\pi_e)^{\mathfrak{f}(Q)}$. Let $\mathscr{P}_1$ and $\mathscr{P}$ be respectively the restrictions of $\mathscr{P}_e$ to $K_1(Q_e)$ and $M_e(Q)$. Then we have the following tower of local fields, where all extensions are totally ramified:

$$\begin{tikzcd}
(K_e)_{\mathfrak{p}_e}(Q_e) = (L_e(Q))_{\mathscr{P}_e} \arrow[d, dash] \arrow[dr, dash, "p^4"] & \\
(K_1)_{\mathfrak{p}_1}(Q_e) = (K_1(Q_e))_{\mathscr{P}_1} \arrow[d, dash] \arrow[dr, dash, "p^4"] & (K_e)_{\mathfrak{p}_e} \arrow[d, dash, "p^{3e-3}"] \\
K_{\mathfrak{p}}(Q_e) = (M_e(Q))_{\mathscr{P}} \arrow[dr, dash, "p^4"] & (K_1)_{\mathfrak{p}_1} \arrow[d, dash, "p^3-p^2+p-1"] \\
 & K_{\mathfrak{p}}
\end{tikzcd}$$

Since Q_{e-1} is in $\mathscr{A}_0(K_{\mathfrak{p}})$ but not in $\mathscr{A}_1(K_{\mathfrak{p}})$, we have $\operatorname{ord}_{\mathfrak{p}}(s_1(Q_{e-1}))$ or $\operatorname{ord}_{\mathfrak{p}}(s_2(Q_{e-1}))$ equal to one. Hence if we set

$$\begin{bmatrix}\tilde{s}_1\\ \tilde{s}_2\end{bmatrix} = \delta^{-1}\begin{bmatrix}s_1\\ s_2\end{bmatrix}$$

one of these three cases holds:

Case A) $\quad \operatorname{ord}_{\mathfrak{p}}\tilde{s}_1(Q_{e-1}) > 1$ and $\operatorname{ord}_{\mathfrak{p}}\tilde{s}_2(Q_{e-1}) = 1$

Case B) $\quad \operatorname{ord}_{\mathfrak{p}}\tilde{s}_1(Q_{e-1}) = 1$ and $\operatorname{ord}_{\mathfrak{p}}\tilde{s}_2(Q_{e-1}) > 1$

Case C) $\quad \operatorname{ord}_{\mathfrak{p}}\tilde{s}_1(Q_{e-1}) = 1$ and $\operatorname{ord}_{\mathfrak{p}}\tilde{s}_2(Q_{e-1}) = 1\,.$

Proposition (5.1).

$$\operatorname{ord}_{\mathfrak{p}_1} D((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}) = \begin{cases} 2(p^4-1) & \textit{in Case A} \\ (p^2-p+2)(p^4-1) & \textit{in Cases B and C}\,. \end{cases}$$

Proof. From (3.9I) and (3.9II) we have

$$\begin{bmatrix}\tilde{s}_1(Q_{e-1})\\ \tilde{s}_2(Q_{e-1})\end{bmatrix} = \delta^{-1}[p]_{\mathscr{G}}\begin{bmatrix}s_1(Q_e)\\ s_2(Q_e)\end{bmatrix}$$

$$= \begin{bmatrix} aps_1(Q_e)+bps_2(Q_e)+s_1(Q_e)^{p^3}+p(d^0\geqq 2)(s_1(Q_e),s_2(Q_e)) \\ cps_1(Q_e)+dps_2(Q_e)+s_2(Q_e)^{p}+p(d^0\geqq 2)(s_1(Q_e),s_2(Q_e)) \end{bmatrix}. \quad \begin{matrix}(5.2\text{I})\\(5.2\text{II})\end{matrix}$$

Case (A). Comparing terms of (5.2II) with least valuation at $\mathscr{P}$ gives us

$$\operatorname{ord}_{\mathscr{P}}(\tilde{s}_2(Q_{e-1})) = \operatorname{ord}_{\mathscr{P}}(s_2(Q_e)^p)\,,$$

or

$$\operatorname{ord}_{\mathscr{P}}(s_2(Q_e)) = p^3\,. \tag{5.3}$$

Since all other terms of (5.2I) have order at $\mathscr{P}$ at least p^4+1,

$$\operatorname{ord}_{\mathscr{P}}(s_1(Q_e)^{p^3}) \geqq p^4+1\,,$$

so

$$\operatorname{ord}_{\mathscr{P}}(s_1(Q_e)) \geqq p+1\,. \tag{5.4}$$

Hence $s_1(Q_e)$ has a $\mathscr{P}_1$-adic expansion $\sum a_i\varpi_1^i$, where ϖ_1 is a uniformizer, the a_i are in k, and the first non-zero coefficient occurs at some

$$i_0 \geqq (p+1)(p^3-p^2+p-1) = p^4-1\,.$$

Let σ, $\tau \in \operatorname{Gal}((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1})$, with $\sigma \neq \tau$. Then $\sigma s_1(Q_e) = s_1(Q_e+u)$, $\tau s_1(Q_e) = s_1(Q_e+v)$ for some u, $v \in A_{\mathfrak{p}}$, $u \neq v$. From the formal group law $\mathscr{G}$,

$$\begin{aligned} &s_1(Q_e+u) - s_1(Q_e+v) \\ &\quad = s_1(u-v) + (d^0 \geqq 2)(s_1(Q_e+v), s_2(Q_e+v), s_1(u-v), s_2(u-v))\,. \end{aligned} \tag{5.5}$$

Now by (3.8), (5.3), and (5.4):

$$\begin{aligned} \operatorname{ord}_{\mathscr{P}_1}(s_1(Q_e+v)) &\geqq (p+1)(p^3-p^2+p-1) = p^4-1\,,\\ \operatorname{ord}_{\mathscr{P}_1}(s_2(Q_e+v)) &= p^3(p^3-p^2+p-1) = p^6-p^5+p^4-p^3\,,\\ \operatorname{ord}_{\mathscr{P}_1}(s_1(u-v)) &= p^4\,,\\ \operatorname{ord}_{\mathscr{P}_1}(s_2(u-v)) &= p^6-p^5+p^4\,. \end{aligned}$$

Therefore the term of least valuation at $\mathscr{P}_1$ on the right side of (5.5) is $s_1(u-v)$, so (5.4) must be an equality, $i_0 = p^4-1$, and

$$\begin{aligned} p^4 &= \operatorname{ord}_{\mathscr{P}_1}(s_1(Q_e+u) - s_1(Q_e+v))\\ &= \operatorname{ord}_{\mathscr{P}_1}\left(\sum_{i \geqq i_0} a_i((\sigma\varpi_1)^i - (\tau\varpi_1)^i)\right)\\ &= \operatorname{ord}_{\mathscr{P}_1}\left((\sigma\varpi_1 - \tau\varpi_1)\sum_{i \geqq i_0} a_i\left(\sum_{j=0}^{i-1}(\sigma\varpi_1)^j(\tau\varpi_1)^{i-1-j}\right)\right)\\ &= \operatorname{ord}_{\mathscr{P}_1}(\sigma\varpi_1 - \tau\varpi_1) + i_0 - 1\,. \end{aligned}$$

Hence $\operatorname{ord}_{\mathscr{P}_1}(\sigma\varpi_1 - \tau\varpi_1) = 2$, and

$$D((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}) = \mathscr{P}_1^{2p^4(p^4-1)} = \mathfrak{p}_1^{2(p^4-1)}\,.$$

Case (B). Comparing terms of (5.2I) with least valuation at $\mathscr{P}$ gives us

$$\operatorname{ord}_{\mathscr{P}}(\tilde{s}_1(Q_{e-1})) = \operatorname{ord}_{\mathscr{P}}(s_1(Q_e)^{p^3})\,, \quad \text{or}$$

$$\operatorname{ord}_{\mathscr{P}}(s_1(Q_e)) = p\,. \tag{5.6}$$

By (5.2II), $\mathfrak{p}$ divides $s_2(Q_e)^p$, and since $c \not\equiv 0 \bmod \mathfrak{p}$, the terms of (5.2II) with least valuation at $\mathscr{P}$ are $cps_1(Q_e)$ and $s_2(Q_e)^p$. Hence

$$\operatorname{ord}_{\mathscr{P}}(s_2(Q_e)) = p^3+1\,. \tag{5.7}$$

So again by (5.5), (5.6), and (5.7), with σ, τ, u, v as above:

$$\operatorname{ord}_{\mathscr{P}_1}(s_1(Q_e+u)-s_1(Q_e+v))=\operatorname{ord}_{\mathscr{P}_1}s_1(u-v)=p^4. \tag{5.8}$$

Since $(K_1)_{\mathfrak{p}_1}(Q_e)/K_{\mathfrak{p}}(Q_e)$ is totally and tamely ramified, we can pick uniformizers $\not{p}$ and $\not{p}_1$ for $\mathscr{P}$ and $\mathscr{P}_1$ respectively, such that $\not{p}=(\not{p}_1)^{p^3-p^2+p-1}$. Now by (5.6), we have a $\mathscr{P}$-adic expansion

$$s_1(Q_e)=a_p\not{p}^p+a_{p+1}\not{p}^{p+1}+\dots,$$

where the coefficients are in k, and $a_p\neq 0$. So by (5.8),

$$\operatorname{ord}_{\mathscr{P}_1}(a_p((\sigma\not{p})^p-(\tau\not{p})^p)+a_{p+1}((\sigma\not{p})^{p+1}-(\tau\not{p})^{p+1})=p^4$$

since $\operatorname{ord}_{\mathscr{P}_1}(\not{p}^n)>p^4$ for $n>p+1$. Since $(K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}$ is a totally-ramified abelian p-extension, $\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1)\geqq 2$. So the analysis of Case (A) shows $\operatorname{ord}_{\mathscr{P}_1}((\sigma\not{p})^{p+1}-(\tau\not{p})^{p+1})\geqq p^4$, with equality holding if and only if $\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1)=2$. Hence

$$\operatorname{ord}_{\mathscr{P}_1}((\sigma\not{p})^p-(\tau\not{p})^p)\geqq p^4 \tag{5.9}$$

with equality holding if $\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1)>2$. Note that

$$\begin{aligned}(\sigma\not{p})^p-(\tau\not{p})^p&=(\sigma\not{p}_1)^{p(p^3-p^2+p-1)}-(\tau\not{p}_1)^{p(p^3-p^2+p-1)}\\&=((\sigma\not{p}_1)^p-(\tau\not{p}_1)^p)\left(\sum_{i=0}^{p^3-p^2+p-2}(\sigma\not{p}_1)^{pi}(\tau\not{p}_1)^{p(p^3-p^2+p-2-i)}\right).\end{aligned}$$

So,

$$\operatorname{ord}_{\mathscr{P}_1}((\sigma\not{p})^p-(\tau\not{p})^p)=\operatorname{ord}_{\mathscr{P}_1}((\sigma\not{p}_1)^p-(\tau\not{p}_1)^p)+p^4-p^3+p^2-2p.$$

Combining this with (5.9) yields:

$$\operatorname{ord}_{\mathscr{P}_1}((\sigma\not{p}_1)^p-(\tau\not{p}_1)^p)\geqq p^3-p^2+2p \tag{5.10}$$

with equality holding if $\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1)>2$.

By the Weil pairing, the pth-roots of unity μ_p are contained in $K(A_p,(A^\vee)_p)$, where $A^\vee$ is the dual of A. But A is isogenous to $A^\vee$, the isogeny and its dual being defined over $K(A_d)$, where d is the degree of the polarization $\mathscr{C}$. Hence $\mu_p\subseteqq K(A_d,A_p)$. But since we chose p to be prime to d, and to be a prime of good reduction, $\mathfrak{p}$ is unramified in $K(A_d)$. Hence $\mu_p\subseteqq K(A_p)$, since $\mathfrak{p}$ ramifies totally in $K(\mu_p)$.

Let ζ_p be a primitive pth-root of unity. Then

$$(\sigma\not{p}_1)^p-(\tau\not{p}_1)^p=\prod_{i=0}^{p-1}(\sigma\not{p}_1-\zeta_p^i\tau\not{p}_1)$$

and (5.10) implies

$$\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\zeta_p^i\tau\not{p}_1)=\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1) \tag{5.11}$$

for $0<i<p$ because $\operatorname{ord}_{\mathscr{P}_1}(1-\zeta_p^i)=p^4(p^2+1)$.

Hence by (5.10) and (5.11),

$$\operatorname{ord}_{\mathscr{P}_1}(\sigma\not{p}_1-\tau\not{p}_1)\geqq p^2-p+2. \tag{5.12}$$

Therefore (5.9) and (5.10) are indeed equalities, and so (5.12) is an equality as well. Hence

$$D((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}) = \mathscr{P}_1^{p^4(p^4-1)(p^2-p+2)} = \mathfrak{p}_1^{(p^4-1)(p^2-p+2)}.$$

Case (C). Comparing terms of (5.2II) and (5.2II) of least valuation at $\mathscr{P}$ gives us

$$\operatorname{ord}_{\mathscr{P}}(s_1(Q_e)) = p, \qquad \operatorname{ord}_{\mathscr{P}}(s_2(Q_e)) = p^3.$$

So (5.8) still holds, and we get the same discriminant as in case (B).

Corollary (5.13). *Let ψ be any non-trivial first degree character on* $\operatorname{Gal}((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1})$. *Then*

$$\operatorname{ord}_{\mathfrak{p}}(\tilde{s}_1(Q_{e-1})) > 1 \Rightarrow \operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\psi) = 2,$$

$$\operatorname{ord}_{\mathfrak{p}}(\tilde{s}_1(Q_{e-1})) = 1 \Rightarrow \operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\psi) = p^2 - p + 2 .\,.$$

Proof. This is immediate from (5.1) because $(K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}$ is a totally-ramified abelian p-extension.

It is easy to see that the identifications (4.1) give us isomorphisms

$$\operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_e)_{\mathfrak{p}_e}) \cong \operatorname{Gal}((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1}), \tag{5.14}$$

$$\operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_1)_{\mathfrak{p}_1}) \cong \operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_e)_{\mathfrak{p}_e}) \times \operatorname{Gal}((K_e)_{\mathfrak{p}_e})/(K_1)_{\mathfrak{p}_1}). \tag{5.15}$$

Proposition (5.16). *Let ψ be any non-trivial first degree character on* $\operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_e)_{\mathfrak{p}_e})$, and $\tilde{\psi}$ the character on $\operatorname{Gal}((K_1)_{\mathfrak{p}_1}(Q_e)/(K_1)_{\mathfrak{p}_1})$ *induced by* (5.14). *Then*

$$\operatorname{ord}_{\mathfrak{p}_e}\mathfrak{f}(\psi) = \operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\tilde{\psi}).$$

Proof. Let ψ^* be the character on $\operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_1)_{\mathfrak{p}_1})$ induced from ψ. By a standard property of conductors [16]

$$\operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\psi^*) = \operatorname{ord}_{\mathfrak{p}_e}\mathfrak{f}(\psi) + \operatorname{ord}_{\mathfrak{p}_1}(D((K_e)_{\mathfrak{p}_e}/(K_1)_{\mathfrak{p}_1})) \tag{5.17}$$

since $(K_e)_{\mathfrak{p}_e}/(K_1)_{\mathfrak{p}_1}$ has residue degree 1.

It follows by Frobenius reciprocity and (5.15) that

$$\psi^* = \bigoplus_{\chi} \chi\tilde{\psi}$$

where the sum is over all first degree characters of $\operatorname{Gal}((K_e)_{\mathfrak{p}_e}/(K_1)_{\mathfrak{p}_1})$. From (5.13), $\operatorname{ord}_{\mathfrak{p}}\mathfrak{f}(\tilde{\psi}) = 2$ or $p^2 - p + 2$. By (2.9), if $\chi \neq 1$, then $\operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\chi) \geqq p^3 - p^2 + p$, so $\mathfrak{f}(\chi\tilde{\psi}) = \mathfrak{f}(\chi)$. Therefore

$$\operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\psi^*) = \sum_{\chi \neq 1} \operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\chi) + \operatorname{ord}_{\mathfrak{p}_1}\mathfrak{f}(\tilde{\psi})$$

and combining this with (5.17) and the conductor-discriminant formula yields the desired result.

Proofs of Theorem 1 and 2. The proof of Theorem 1 is immediate from (5.13) and (5.16) since by (4.9), $\mathfrak{f}(L_e(Q)/K_e) = \mathfrak{f}(\psi)$ for any first degree character of $\operatorname{Gal}(L_e(Q)/K_e)$ which is non-trivial when restricted to $\operatorname{Gal}(L_e(Q)/K_eL_{e-1}(Q)) \cong \operatorname{Gal}((K_e)_{\mathfrak{p}_e}(Q_e)/(K_e)_{\mathfrak{p}_e})$.

For $i=1, 2$, let P_i be of infinite order in $A(K)$, $P_i \notin \mathfrak{p}A(K)$. For some λ_i in $\mathcal{O}_K$ prime to $\mathfrak{p}$, $\lambda_i * P_i \in \mathscr{A}_0$, and so we will assume that $P_i \in \mathscr{A}_0$. Note that (4.6) gives $\mathscr{A}_0$ the structure of an $\mathcal{O}_\mathfrak{p}$-module.

For Theorem 2, we suppose that the P_i are $\mathcal{O}_\mathfrak{p}$-independent.

For each $P \in \mathscr{A}_0(K_\mathfrak{p})$ we let $l(P)$ denote its level in the filtration (4.6). That is, $l(P)=i$ if P is in $\mathscr{A}_i(K_\mathfrak{p})$ but not in $\mathscr{A}_{i+1}(K_\mathfrak{p})$. Renumbering if necessary, we may assume $l(P_1) \leqq l(P_2)$.

For $n \geqq 2$, recursively choose $P_{n+1} \in A(K)$ as follows:

If

$$P_n \equiv (\varepsilon_n p^{l(P_n)-l(P_1)}) * P_1 \bmod (\mathscr{A}_{l(P_n)+1}(K_\mathfrak{p}))$$

for some

$$\varepsilon_n \in \mathcal{O}_K,$$

then set

$$P_{n+1} = P_n - (\varepsilon_n p^{l(P_n)-l(P_1)}) * P_1 . \tag{5.18}$$

Since P_1 and P_2 are independent over $\mathcal{O}_\mathfrak{p}$, the process (5.18) must terminate, and hence for some $n \geqq 2$, $(p^{l(P_n)-l(P_1)}) * P_1$ and $P_n = P_2 - \left(\sum_{i=2}^{n-1} \varepsilon_i p^{l(P_i)-l(P_1)}\right) * P_1$ are $\mathcal{O}_\mathfrak{p}$-independent in $\mathscr{A}_{l(P_n)}(K_\mathfrak{p})/A_{l(P_n)+1}(K_\mathfrak{p})$.

Therefore there exist $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$, $R_1, R_2 \in A(K)$, and $\tilde{R}_1, \tilde{R}_2 \in \mathscr{A}_0(K_\mathfrak{p})$ such that

$$\begin{gathered}
R_1 = (\alpha p^{l(P_n)-l(P_1)}) * P_1 + \beta * P_n, \quad R_2 = (\gamma p^{l(P_n)-l(P_1)}) * P_1 + \delta * P_n, \\
[p^{l(P_n)}]_{\mathscr{G}} \tilde{R}_1 = R_1, \quad [p^{l(P_n)}]_{\mathscr{G}} \tilde{R}_2 = R_2, \\
\operatorname{ord}_\mathfrak{p} \tilde{s}_1(\tilde{R}_1) > 1, \quad \operatorname{ord}_\mathfrak{p} \tilde{s}_2(\tilde{R}_1) = 1, \\
\operatorname{ord}_\mathfrak{p} \tilde{s}_1(\tilde{R}_2) = 1, \quad \operatorname{ord}_\mathfrak{p} \tilde{s}_2(\tilde{R}_2) \geqq 1 .
\end{gathered} \tag{5.19}$$

Finally, for $i=1, 2$, suppose R_i is in $p^{j_i}A(K)$ but not in $p^{j_i+1}A(K)$.

Let Q_i be the unique point of $A(K)$ such that $p^{j_i} * Q_i = R_i$. Then by (5.13), (5.16), and (5.19), $\mathfrak{f}(Q_1)=2$, and $\mathfrak{f}(Q_2)=p^2-p-2$.

Set $e_i = e(Q_i)$. Comparing ray class fields of K_{e_1} of conductors $\mathfrak{p}_{e_1}$ and $\mathfrak{p}_{e_1}^2$ as in [4, Proposition 5], it follows readily that $\mathfrak{f}(Q_1)=2$ implies that every unit u of K_{e_1}, with $u \equiv 1 \bmod \mathfrak{p}_{e_1}$, actually satisfies $u \equiv 1 \bmod \mathfrak{p}_{e_1}^2$.

Remarks. 1) Similarly, from (4.9) we see that $\mathfrak{f}(Q_2)=p^2-p+2$ implies that every unit u of K_{e_2}, with $u \equiv 1 \bmod \mathfrak{p}_{e_2}^{p^2-p+1}$, actually satisfies $u \equiv 1 \bmod \mathfrak{p}_{e_2}^{p^2-p+2}$.

2) Spurred by visions of a generalized Leopoldt's conjecture, one might hope that the $\mathcal{O}_K$-rank of $A(K)$ being at least 2 would be sufficient to insure that the $\mathcal{O}_\mathfrak{p}$-rank of $\mathscr{A}_0(K) \otimes \mathcal{O}_\mathfrak{p}$ were 2 (see [22]). From Waldschmidt's work we can derive a weaker claim: If the $\mathcal{O}_K$-rank of $A(K)$ is at least 5 then the $\mathcal{O}_\mathfrak{p}$-rank of $\mathscr{A}_0(K) \otimes \mathcal{O}_\mathfrak{p}$ is 2.

Fix a logarithm map, $\log: \mathscr{A}_0(K_\mathfrak{p}) \to T_\mathscr{A}(K_\mathfrak{p})$ into the tangent space of $\mathscr{A}$ (considered as column vectors). Then since $\mathscr{A}$ is simple, Waldschmidt [22] has shown that if Q_i, with $1 \leqq i \leqq 5$, in $\mathscr{A}_0(K)$ are $\mathbb{Z}$-independent, then the $K_\mathfrak{p}$-rank of the 2 × 5 matrix

$$[\log(Q_i)]_{1 \leqq i \leqq 5}$$

is 2.

To prove the claim, suppose to the contrary that we have 5 $\mathcal{O}_K$-independent points Q_i in $\mathscr{A}_0(K)$ which have $\mathcal{O}_\mathfrak{p}$-rank 1 in $\mathscr{A}_0(K_\mathfrak{p})$. Since $\mathcal{O}_\mathfrak{p} = \mathcal{O}_K \mathbb{Z}_p$, we can assume the Q_i were chosen to have $\mathbb{Z}_p$-rank 1. But since complex multiplication by elements of $\mathbb{Z}_p$ act via diagonal matrices on $T_{\mathscr{A}}(K_\mathfrak{p})$, this violates Waldschmidt's result.

References

1. Arthaud, N.: On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I. Compos. Math. **37**, 209–232 (1978)
2. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223–251 (1977)
3. Grant, D.: Theta functions and division points on abelian varieties of dimension two. Thesis, M.I.T. 1985
4. Gupta, R.: Ramification in the Coates-Wiles tower. Invent. Math. **81**, 59–69 (1985)
5. Hazewinkel, M.: Formal groups and applications. New York: Academic Press 1978
6. Lang, S.: Elliptic curves: diophantine analysis. Berlin Heidelberg New York: Springer 1978
7. Lang, S.: Complex multiplication. Berlin Heidelberg New York: Springer 1983
8. Lang, S.: Diophantine geometry. Berlin Heidelberg New York: Springer 1983
9. Ribet, K.: Dividing rational points on abelian varieties of CM-type. Compos. Math. **33**, 69–74 (1976)
10. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **64**, 455–470 (1981)
11. Rubin, K.: Congruences for special values of L-functions of elliptic curves with complex multiplication. Invent. Math. **71**, 339–364 (1983)
12. Rubin, K.: Elliptic curves and $\mathbb{Z}_p$-extensions. Compos. Math. **56**, 237–250 (1985)
13. Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. Invent. Math. **89**, 527–560 (1987)
14. Rubin, K.: Global units and ideal class groups. Invent. Math. **89**, 511–526 (1987)
15. Sah, H.: Automorphisms of finite groups. J. Algebra **10**, 47–68 (1968)
16. Serre, J.-P.: Local class field theory. Algebraic number theory. Cassels, J.W.S., Fröhlich, A. (eds.) pp. 128–161, London: Academic Press 1967
17. Serre, J.-P.: Lie algebras and Lie groups. Reading: Benjamin 1965
18. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **88**, 492–517 (1968)
19. Setzer, B.: The determination of all imaginary quartic, abelian number fields with class number 1. Math. Comp. **35**, 1383–1386 (1980)
20. Shimura, G.: On the zeta function of an abelian variety with complex multiplication. Ann. Math. (2) **94**, 504–533 (1971)
21. Stark, H.: The Coates-Wiles theorem revisited. Number theory related to Fermat's last theorem (Progress in Math., Vol. 26). Boston: Birkhäuser 1982
22. Waldschmidt, M.: Dépendance de logarithmes dans les groupes algébriques. Approximations Diophantiennes et nombres transcendants, (Progress in Math., Vol. 31). Boston: Birkhäuser 1983
23. Washington, L.: Introduction to cyclotomic fields. Berlin Heidelberg New York: Springer 1982

Received April 11, 1987; in revised form April 11, 1988