Descent Calculations for the Elliptic Curves of Conductor 11

Tom Fisher

April 18, 2001

Abstract

Let A be one of the three elliptic curves over $\mathbf{Q}$ with conductor 11. We show that A has Mordell-Weil rank zero over its field of 5-division points. In each case we also compute the 5-primary part of the Tate-Shafarevich group. Our calculations make use of the Galois equivariance of the Cassels-Tate pairing.

Introduction

Ever since the work of Mazur [Ma] the elliptic curves of conductor 11 have provided a testing ground for the Iwasawa theory of elliptic curves. We recall from [V1] that these curves form a single isogeny class, and have explicit Weierstrass equations

$A_0 = X_0(11)$	$y^2 + y = x^3 - x^2 - 10x - 20$	11A1
$A_1 = X_1(11)$	$y^2 + y = x^3 - x^2$	11A3
A_2	$y^2 + y = x^3 - x^2 - 7820x - 263580$	11A2

Here the labels 11A1-3 are those used in [Cr], whereas the labels A_0, A_1, A_2 are taken from [CS]. When there is no need to distinguish the three curves we shall simply write A to denote any one of them.

Coates and Howson [CH] have used the elliptic curves of conductor 11 to illustrate their work on non-abelian Iwasawa theory. A natural question to ask is

> How does the Mordell-Weil rank behave as we pass up the tower of fields given by adjoining the 5-power division points?

Although we are still unable to answer this question, we prove that the rank is zero over the field of 5-division points for each of the three curves.

It seems that Mazur [Ma, Cor. 9.10] was the first to show $\operatorname{rank} A(\mathbf{Q}) = 0$ and $\text{Ш}(A/\mathbf{Q})(5) = 0$. An extension of this result to $\mathbf{Q}(\mu_5)$, due to Greenberg, may be found in [CS]. In each case the authors put their classical descent calculations to good use in studying the behaviour of Selmer groups over the cyclotomic $\mathbf{Z}_5$-extension. For instance in [CS] it is shown that $\operatorname{rank} A(\mathbf{Q}(\mu_{5^\infty})) = 0$. It is hoped that our results will have equally striking applications.

The curves of conductor 11 are chosen since they appear first in the list of modular curves, and they do *not* admit complex multiplication. The prime 5 is chosen to make the problem more tractable. Indeed there are isogenies of degree 5 defined over $\mathbf{Q}$

$$A_1 \rightleftarrows A_0 \rightleftarrows A_2. \tag{1}$$

The curves A_0 and A_1 each have a rational point of order 5, whereas A_2 does not. By properties of the Weil pairing we deduce $A_0[5] \simeq \mu_5 \oplus \mathbf{Z}/5\mathbf{Z}$ as a Galois module. Furthermore there are exact sequences

$$0 \to \mathbf{Z}/5\mathbf{Z} \to A_1 \to A_0 \to 0 \qquad 0 \to \mu_5 \to A_2 \to A_0 \to 0. \tag{2}$$

The fields of 5-division points are $k = \mathbf{Q}(\mu_5)$, $K_1 = \mathbf{Q}(A_1[5])$ and $K_2 = \mathbf{Q}(A_2[5])$. Since K_1 and K_2 are non-abelian and of degree 20, it should come as no surprise that our descent calculations are rather more involved than those cited above. Our conclusions are

Theorem 1 *Let* $K_1 = \mathbf{Q}(A_1[5])$*. Then* $\operatorname{rank} A(K_1) = 0$ *and*

$$\begin{array}{ll}
A_0(K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \text{Ш}(A_0/K_1)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^8 \\
A_1(K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \text{Ш}(A_1/K_1)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^2 \\
A_2(K_1) \simeq \mathbf{Z}/5\mathbf{Z} & \text{Ш}(A_2/K_1)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^4 \oplus (\mathbf{Z}/25\mathbf{Z})^8.
\end{array}$$

Theorem 2 *Let* $K_2 = \mathbf{Q}(A_2[5])$*. Then* $\operatorname{rank} A(K_2) = 0$ *and*

$$\begin{array}{ll}
A_0(K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \text{Ш}(A_0/K_2)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^8 \\
A_1(K_2) \simeq \mathbf{Z}/5\mathbf{Z} & \text{Ш}(A_1/K_2)(5) = 0 \\
A_2(K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \text{Ш}(A_2/K_2)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^6 \oplus (\mathbf{Z}/25\mathbf{Z})^8.
\end{array}$$

It is easy to check that these results are compatible with the isogeny invariance of the Birch Swinnerton-Dyer conjecture, as proved by Cassels [Ca3]. Let us note that for $\mathfrak{p}|11$, inspection of the j-invariants shows that the Tamagawa factors are $c_{\mathfrak{p}}(A_0) = 5\,\mathrm{ord}_{\mathfrak{p}}(11)$ and $c_{\mathfrak{p}}(A_1) = c_{\mathfrak{p}}(A_2) = \mathrm{ord}_{\mathfrak{p}}(11)$. At each infinite place, it follows by Vélu's formulae [V2] that the periods Ω_i are related via $\Omega_1/\Omega_0 = \Omega_0/\Omega_2 = 5$.

In §1 we introduce some subfields of $\mathbf{Q}(A[5^\infty])$. In §2 we recall from [F0], [F1], a description of the Selmer groups attached to the 5-isogenies (1). The analogue of Theorems 1 and 2 for $k = \mathbf{Q}(\mu_5)$ is an easy consequence. In §3 we give explicit Kummer generators for the fields introduced in §1. In §4 we recall the definition of the Cassels-Tate pairing. Following the work of McCallum [Mc] and Beaver [B] we give a formula for the pairing in the case we need. In §5 we discuss certain Galois modules, and the alternating pairings they admit. Finally in §6 and §7 we give the descent calculations proving Theorems 1 and 2.

We have made extensive use of the computer algebra package `pari` in the course of this work. However we have striven where possible to give arguments that may be checked by hand. For the proof of Theorem 1 this goal has largely been achieved. In contrast the proof of Theorem 2 relies on us exhibiting a "non-trivial" unit in K_1K_2. Our method here was to ask `pari` to find all units in a certain degree 25 subfield. (This took 1 hour and 20 minutes on a 800MHz Pentium-III with 128Mb RAM.)

In a separate note [F2] we prove an analogue of Theorems 1 and 2 for the field $J_1 = \mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$. Again the rank is zero. Curiously our argument in that case does not require any formula for the Cassels-Tate pairing.

Acknowledgements

I would like to thank John Coates, Ralph Greenberg, Karl Rubin and Ed Schaefer for a number of valuable suggestions.

Notation and Conventions

For F a perfect field we write $G_F := \mathrm{Gal}(\overline{F}/F)$ and $H^i(F,-) = H^i(G_F,-)$. By Hilbert's theorem 90 we identify $H^1(F,\mu_5) = F^*/F^{*5}$. The number field F has ring of integers $\mathfrak{O}_F$, unit group $\mathfrak{O}_F^*$, and class group $\mathfrak{Cl}_F$. The local field $F_{\mathfrak{p}}$ has ring of integers $\mathfrak{O}_{\mathfrak{p}}$ and normalised valuation $\mathrm{ord}_{\mathfrak{p}}$. Since our interest is in descent via isogenies of odd degree we ignore the infinite places throughout.

Let C and D be elliptic curves defined over F, and let $\psi : C \to D$ be an isogeny of degree m. The Kummer exact sequence restricts to

$$0 \longrightarrow D(F)/\psi C(F) \xrightarrow{\delta} S^{(\psi)}(C/F) \longrightarrow \text{Ш}(C/F)[\psi] \longrightarrow 0.$$

We frequently avoid giving our isogeny a name by writing $S(C \to D/F)$ for $S^{(\psi)}(C/F)$. The Weil pairing is denoted $e_\psi : C[\psi] \times D[\widehat{\psi}] \to \mu_m$.

The following notation relating to the field $k = \mathbf{Q}(\mu_5)$ is used throughout. We fix ζ a primitive 5th root of unity and write $\mathrm{Ind}_\zeta : \mu_5 \to \mathbf{Q}/\mathbf{Z}$ for the map $\zeta \mapsto 1/5$. Then k has fundamental unit $\phi = 1 + \zeta + \zeta^{-1}$. (Taking $\zeta = \exp(2\pi i/5)$ this is the golden ratio.) We write $\overline{\phi} = -1/\phi = 1 - \phi$ for its conjugate. In §3 we use ϕ to define involutions η and ε on $\mathbf{P}^1_k$. The primes of k above 5 and 11 are $\mathfrak{l} = (1 - \zeta)$ and $\mathfrak{p}_i = (\pi_i)$ where $\pi_i = 2 + \zeta^i$. We write $\omega : G_{\mathbf{Q}} \to (\mathbf{Z}/5\mathbf{Z})^*$ for the cyclotomic character.

1 A description of $\mathrm{Gal}(\mathbf{Q}(A[5^\infty])/\mathbf{Q})$

Serre [Se2, §5.5] proved

Proposition 1.1 $\mathrm{Gal}(\mathbf{Q}(A[p^\infty])/\mathbf{Q}) \simeq \mathrm{GL}_2(\mathbf{Z}_p)$ *for all primes* $p \neq 5$.

In contrast for $p = 5$, $\mathbf{Q}(A[p^\infty])/\mathbf{Q}(\mu_p)$ is a pro-p extension. A description of the Galois group in this case was given by Lang and Trotter [LT]. In this section we present an alternative proof of their result and go on to compute the torsion subgroups listed as part of Theorems 1 and 2.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the kernels of the degree 25 isogenies $A_1 \to A_2$ and $A_2 \to A_1$. We shall be concerned with the fields $J_1 = k(\mathcal{C}_1)$, $J_2 = k(\mathcal{C}_2)$, $K_1 = \mathbf{Q}(A_1[5])$ and $K_2 = \mathbf{Q}(A_2[5])$.

Lemma 1.2 *The fields* J_1, J_2, K_1, K_2 *are degree 5 Kummer extensions of* k.

Proof. All is clear, except perhaps that these extensions are non-trivial. In fact $\mathcal{C}_1$ is generated by the cusps on $A_1 = X_1(11)$ and these are defined over $\mathbf{Q}(\mu_{11})^+ = \mathbf{Q}(\mu_{11}) \cap \mathbf{R}$. Thus $J_1 = \mathbf{Q}(\mu_5)\mathbf{Q}(\mu_{11})^+$ and $\mathbf{Q}(\mu_{25}) \subset J_1 J_2$. For K_1 and K_2 we must show that the exact sequences (2) do not split as G_k-modules. As explained in [CS, Chapter 4] an examination of the Tate periods shows that these exact sequences do not even split as $G_{\mathbf{Q}_{11}}$-modules. □

We pick a basis P, Q for the Tate module $T_5(A_0)$, such that the projections of P and Q in $A_0[5]$ generate $\ker(A_0 \to A_2) \simeq \mathbf{Z}/5\mathbf{Z}$ and $\ker(A_0 \to A_1) \simeq \mu_5$ respectively. Then the Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_5)$ attached to A_0 satisfies

$$\rho(\sigma) \equiv \begin{pmatrix} 1 & 0 \\ 0 & \omega(\sigma) \end{pmatrix} \pmod 5.$$

In particular

$$\rho(G_k) \subset \{\, M \in \mathrm{GL}_2(\mathbf{Z}_5) \mid M \equiv I \pmod 5 \,\}. \tag{3}$$

Lemma 1.3 *For $\sigma \in G_k$ let $\rho(\sigma) = I + 5 \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. There are isomorphisms*

$$\begin{array}{ll} \mathrm{Gal}(J_1/k) \simeq \mathbf{Z}/5\mathbf{Z}\,; \quad \sigma \mapsto a & \qquad \mathrm{Gal}(K_1/k) \simeq \mathbf{Z}/5\mathbf{Z}\,; \quad \sigma \mapsto b \\ \mathrm{Gal}(K_2/k) \simeq \mathbf{Z}/5\mathbf{Z}\,; \quad \sigma \mapsto c & \qquad \mathrm{Gal}(J_2/k) \simeq \mathbf{Z}/5\mathbf{Z}\,; \quad \sigma \mapsto d. \end{array}$$

Furthermore, the action of $\mathrm{Gal}(k/\mathbf{Q})$ *on these Galois groups is described by* $\psi = 1, \omega^{-1}, \omega$ *and* 1 *respectively.*

Proof. We check the first of these isomorphisms, the other cases being similar. Let P_r, Q_r be the projections of P, Q in $A_0[5^r]$. The image of P_2 under the 5-isogeny $A_0 \to A_1$ is a generator for $\mathcal{C}_1$. Thus for $\sigma \in G_k$

$$\begin{array}{rcl} \sigma \text{ fixes } J_1 \text{ pointwise} & \Longleftrightarrow & \sigma(P_2) - P_2 \in \ker(A_0 \to A_1) \\ & \Longleftrightarrow & aP_1 + c\,Q_1 \in \ker(A_0 \to A_1) \\ & \Longleftrightarrow & a \equiv 0 \pmod 5. \end{array}$$

It follows that the map $\sigma \mapsto a$ induces an isomorphism $\mathrm{Gal}(J_1/k) \simeq \mathbf{Z}/5\mathbf{Z}$. Finally $\mathrm{Gal}(k/\mathbf{Q})$ acts on G_k by conjugation, and we compute

$$\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}^{-1} = \begin{pmatrix} a & b\,\omega^{-1} \\ c\,\omega & d \end{pmatrix}.$$

□

Lemma 1.4 *The fields J_1, J_2, K_1, K_2 are* independent *degree 5 Kummer extensions of k.*

Proof. Given the distinct actions of $\mathrm{Gal}(k/\mathbf{Q})$ it suffices to check that J_1 and J_2 are independent. But $J_1 J_2 = \mathbf{Q}(\mu_{25})\mathbf{Q}(\mu_{11})^+$ so this is clear. $\square$

The next proposition was originally proved by Lang and Trotter [LT, Part I, Theorem 8.1]. I am grateful to John Coates for pointing out to me the simpler proof presented here.

Proposition 1.5 *The extension $\mathbf{Q}(A[5^\infty])/\mathbf{Q}$ has Galois group*

$$\rho(G_{\mathbf{Q}}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_5) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \pmod 5 \right\}.$$

Proof. We prove by induction on r that the image of $\rho(G_k)$ in $\mathrm{GL}_2(\mathbf{Z}/5^r\mathbf{Z})$ is the kernel of the map $\mathrm{GL}_2(\mathbf{Z}/5^r\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/5\mathbf{Z})$. The case $r = 2$ follows from Lemmas 1.3 and 1.4. The induction step is well known, and may be found in [LT] or [Se1]. It makes use of the identity

$$(I + 5^{r-1}M)^5 \equiv I + 5^r M \pmod{5^{r+1}}.$$

We deduce that equality holds in (3), and the proposition follows. $\square$

In §3 we find explicit Kummer generators for the extensions K_1/k and K_2/k. From these we learn that the prime above 5 is split in K_1/k and is ramified in K_2/k. We prove the easy part of Theorems 1 and 2.

Corollary 1.6 *The torsion subgroups for $A(K_1)$ and $A(K_2)$ are*

$$\begin{array}{ll} A_0(K_1)_{\mathrm{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \qquad A_0(K_2)_{\mathrm{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2 \\ A_1(K_1)_{\mathrm{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \qquad A_1(K_2)_{\mathrm{tors}} \simeq \mathbf{Z}/5\mathbf{Z} \\ A_2(K_1)_{\mathrm{tors}} \simeq \mathbf{Z}/5\mathbf{Z} & \qquad A_2(K_2)_{\mathrm{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2. \end{array}$$

Proof. Since A has good reduction at 5 and $\widetilde{A}(\mathbf{F}_5) \simeq \mathbf{Z}/5\mathbf{Z}$, it suffices to check that the 5-power torsion is as claimed. We make the observation that A_0 has no point of order 25 defined over $K_1 K_2$. Indeed if $\sigma \in G_{\mathbf{Q}}$ satisfies $\rho(\sigma) = 6I$ then σ fixes pointwise the fields K_1 and K_2, but does not fix any point of order 25 on A_0. Thus $A_0(K_i)_{\mathrm{tors}} \simeq (\mathbf{Z}/5\mathbf{Z})^2$ for $i = 1, 2$. Again for $i = 1, 2$ the inverse image of $A_0[5]$ under the 5-isogeny $A_i \to A_0$ has field of definition $J_i K_i$. The remaining statements now follow from Lemma 1.4. $\square$

The Selmer groups used in our calculations are of the most concrete nature, namely those attached to isogenies. They therefore contain contributions from torsion in the Mordell-Weil group. For this reason we make frequent implicit use of Corollary 1.6. For future reference we give another result on torsion subgroups.

Lemma 1.7 *Let* $[F : \mathbf{Q}_{11}] < \infty$*. Then* $\#A_1(F)(5) \leq 5[F : \mathbf{Q}_{11}]$.

Proof. We know that A_1 had multiplicative reduction, with Tamagawa factor $e = \mathrm{ord}(11)$. The number of smooth points over the residue field is $11^f - 1$, and the multiplication by 5 map on the formal group is an isomorphism. Hence

$$\#A_1(F)(5) \leq 5ef = 5[F : \mathbf{Q}_{11}].$$

□

2 Explicit descent via 5-isogeny

The Selmer groups attached to the 5-isogenies (1) are defined as subgroups of $H^1(F, \mu_5) = F^*/F^{*5}$ and $H^1(F, \mathbf{Z}/5\mathbf{Z}) = \mathrm{Hom}(G_F, \mathbf{Z}/5\mathbf{Z})$.

Proposition 2.1 *Let F be a number field. Then*

$$\begin{aligned}
S(A_0 \to A_1/F) &\simeq \left\{ \theta \in F^*/F^{*5} \;\middle|\; \begin{array}{c} \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 5 \textit{ for all } \mathfrak{p} \\ \textit{and } F(\sqrt[5]{\theta})/F \textit{ split at } \mathfrak{p}|11 \end{array} \right\} \\
S(A_1 \to A_0/F) &\simeq \left\{ \chi \in \mathrm{Hom}(G_F, \mathbf{Z}/5\mathbf{Z}) \;\middle|\; \chi \textit{ unramified at all } \mathfrak{p} \nmid 11 \right\} \\
S(A_2 \to A_0/F) &\simeq \left\{ \theta \in F^*/F^{*5} \;\middle|\; \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 5 \textit{ for all } \mathfrak{p} \nmid 11 \right\} \\
S(A_0 \to A_2/F) &\simeq \left\{ \chi \in \mathrm{Hom}(G_F, \mathbf{Z}/5\mathbf{Z}) \;\middle|\; \begin{array}{c} \chi \textit{ unramified at all } \mathfrak{p} \\ \textit{and } \chi \textit{ split at } \mathfrak{p}|11 \end{array} \right\}
\end{aligned}$$

(Here χ split at $\mathfrak{p}$ means $\mathfrak{p}$ splits in the fixed field of the kernel of χ.)

Proof. More generally in [F1] we considered pairs of 5-isogenous elliptic curves C_λ and D_λ with $\ker(C_\lambda \to D_\lambda) \simeq \mu_5$ and $\ker(D_\lambda \to C_\lambda) \simeq \mathbf{Z}/5\mathbf{Z}$. Explicitly D_λ has Weierstrass equation

$$y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2 \tag{4}$$

and $\mathbf{Z}/5\mathbf{Z} \hookrightarrow D_\lambda(F)$ is generated by $(x, y) = (0, 0)$. We see that $A_1 = D_1$ and $A_0 = D_{11}$. For each prime $\mathfrak{p}$ there is an exact sequence

$$C_\lambda(F_{\mathfrak{p}}) \longrightarrow D_\lambda(F_{\mathfrak{p}}) \xrightarrow{\delta_{\mathfrak{p}}} F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5}.$$

We recall [F1, Propositions 2.15 and 2.16] that $\delta_{\mathfrak{p}}$ has image

$$\operatorname{im}\delta_{\mathfrak{p}} = \begin{cases} F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5} & \text{if } \operatorname{ord}_{\mathfrak{p}}(\lambda) \neq 0 \\ \mathfrak{O}_{\mathfrak{p}}^*/\mathfrak{O}_{\mathfrak{p}}^{*5} & \text{if } \operatorname{ord}_{\mathfrak{p}}(\lambda) = \operatorname{ord}_{\mathfrak{p}}(\lambda^2 - 11\lambda - 1) = 0 \\ 1 & \text{if } \operatorname{ord}_{\mathfrak{p}}(\lambda^2 - 11\lambda - 1) > 0 \text{ and } \mathfrak{p} \nmid 5. \end{cases}$$

The descriptions of $S(A_0 \to A_1/F)$ and $S(A_2 \to A_0/F)$ now follow on taking $\lambda = 1$, respectively $\lambda = 11$. Tate local duality tells us that the images of the local connecting maps attached to an isogeny and its dual are exact annihilators with respect to the Tate pairing. The descriptions of $S(A_1 \to A_0/F)$ and $S(A_0 \to A_2/F)$ follow. □

Suppose F is number field for which we have a working knowledge of the unit group and the class group. It is now a straightforward exercise in Kummer theory to compute the Selmer groups $S(A_0 \to A_1/F)$ and $S(A_2 \to A_0/F)$. If $\mu_5 \subset F$, then the Selmer groups attached to the dual isogenies may be treated similarly. However there is a better way.

Proposition 2.2 *Let F be a number field with r_1 (resp. r_2), real (resp. pairs complex conjugate) embeddings and m primes above 11. Then*

$$\frac{\#S(A_0 \to A_1/F)}{\#S(A_1 \to A_0/F)} = \#\mu_5(F) \times 5^{r_1+r_2-1} \times 5^{-m}$$

$$\frac{\#S(A_2 \to A_0/F)}{\#S(A_0 \to A_2/F)} = \#\mu_5(F) \times 5^{r_1+r_2-1} \times 5^{m}.$$

Proof. This is an application of Cassels' formula [Ca3, Theorem 1.1]. The ratios of Tamagawa numbers are given in the introduction. □

Remark 2.3 In simple cases, for example if F has class number 1, it is a tolerable exercise in class field theory to deduce Proposition 2.2 directly from Proposition 2.1. The beauty of Cassels' formula is that the class number of F does not appear.

Example 2.4 We use Propositions 2.1 and 2.2 to compute $\operatorname{rank} A(k)$. We recall that k has class number 1, and that $\mathfrak{o}_k^*$ is generated by $\pm\zeta, \phi$, where $\phi = 1 + \zeta + \zeta^{-1}$. Writing $\pi_i = 2 + \zeta^i$ we find

$$\begin{array}{ll} S(A_0 \to A_1/k) = 0 & \text{since } \zeta, \phi \notin (\mathfrak{o}_k/\pi_1)^{*5} \\ S(A_1 \to A_0/k) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & \textit{i.e. } \operatorname{Hom}(\operatorname{Gal}(J_1K_1/k), \mathbf{Z}/5\mathbf{Z}) \\ S(A_2 \to A_0/k) \simeq (\mathbf{Z}/5\mathbf{Z})^6 & \textit{i.e. } \langle \zeta, \phi, \pi_1, \pi_2, \pi_3, \pi_4 \rangle \subset k^*/k^{*5} \\ S(A_0 \to A_2/k) = 0 & \text{since } h_k = 1. \end{array}$$

We deduce $\operatorname{rank} A(k) = 0$ and $Ш(A_i/k)(5) = 0$ for $i = 0, 1$. We further find $Ш(A_2/k)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^4$.

3 Torsion contributions and Kummer generators

Let C_λ and D_λ be as in the proof of Proposition 2.1. Then λ is a co-ordinate on $X_1(5) \simeq \mathbf{P}^1$ and this modular curve has cusps at $\lambda = 0, \infty, \phi^5, \overline{\phi^5}$. There is an involution η on $X_1(5)$, permuting the cusps, such that $\mu_5 \hookrightarrow C_\lambda$ is isomorphic to $\mathbf{Z}/5\mathbf{Z} \hookrightarrow D_{\eta(\lambda)}$ over $F(\mu_5)$. We take

$$\eta : \lambda \mapsto (\phi^5\lambda + 1)/(\lambda - \phi^5).$$

For $\lambda \in F$ not a cusp of $X_1(5)$ there is a Kummer exact sequence

$$0 \longrightarrow \mu_5(F) \longrightarrow C_\lambda(F) \longrightarrow D_\lambda(F) \stackrel{\delta}{\longrightarrow} F^*/F^{*5}. \tag{5}$$

Lemma 3.1 *The image of $\mathbf{Z}/5\mathbf{Z} \hookrightarrow D_\lambda(F)$ under the connecting map δ is generated by λ.*

Proof. In terms of the Weierstrass equation (4), the multiples of $(0,0)$ are (λ, λ^2), $(\lambda, 0)$, and $(0, \lambda)$. We recall from [F1] that if $P = (x, y) \neq (0, 0)$ then $\delta(P) = xy + y - x^2$. The lemma follows. □

For $\lambda \in F$ we deduce $F(C_\lambda[5]) = F(\mu_5, \sqrt[5]{\lambda})$. In particular $\eta(1)$ and 11 are Kummer generators for K_1/k and K_2/k. We also learn that $X(5) \simeq \mathbf{P}^1$ with forgetful map

$$X(5) \to X_1(5)\,; \quad \tau \mapsto \tau^5.$$

The cusps of $X(5)$ are at $\tau = 0, \infty, \zeta^i\phi, \zeta^i\overline{\phi}$. Under stereographic projection these points may be viewed as the vertices of an icosahedron. There is an action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z}) \simeq A_5$ on $X(5)$ permuting the cusps, generated by $\tau \mapsto \zeta\tau$ and

$$\varepsilon : \tau \mapsto (\phi\tau + 1)/(\tau - \phi).$$

Lemma 3.2 *Suppose $\mu_5 \subset F$. Let $\tau \in F$ and put $\lambda = \eta(\tau^5)$. Then the image of $(\mathbf{Z}/5\mathbf{Z})^2 \hookrightarrow D_\lambda(F)$ under δ is generated by*

$$\lambda = \prod_{i=0}^{4} \varepsilon(\zeta^i\tau) \quad \textit{and} \quad \prod_{i=0}^{4} \varepsilon(\zeta^i\tau)^i.$$

Proof. In terms of the Weierstrass equation (4), $(\mathbf{Z}/5\mathbf{Z})^2 \hookrightarrow D_\lambda(F)$ is generated by $(0,0)$ and

$$\left(-\lambda \frac{(\zeta\tau-\phi)(\zeta^4\tau-\phi)}{(\phi\tau+1)(\tau-\phi)}, -\lambda^2 \frac{(\zeta\tau-\phi)(\zeta^2\tau-\phi)(\zeta^4\tau-\phi)^2}{(\phi\tau+1)^2(\tau-\phi)(\phi\zeta\tau+1)} \right) \tag{6}$$

We conclude as in the proof of Lemma 3.1. □

Remark 3.3 One way to construct the point (6) is to observe that in the notation of [F0], [F1] the curve

$$T = T[\lambda; \varepsilon(\tau), \varepsilon(\zeta\tau), \varepsilon(\zeta^2\tau), \varepsilon(\zeta^3\tau), \varepsilon(\zeta^4\tau)] \subset \mathbf{P}^4$$

has rational point

$$(\tau-\phi : \zeta\tau-\phi : \zeta^2\tau-\phi : \zeta^3\tau-\phi : \zeta^4\tau-\phi). \tag{7}$$

There is a diagonal action of μ_5 on T with quotient D_λ. In [F0, Appendix C] we give explicit equations for the map $T \to D_\lambda$ and this allows us to construct (6) from (7).

Applying Lemma 3.2 with $\tau = 1$ gives Kummer generators for J_1/k and K_1/k. Applying Lemma 3.2 with $\tau = \varepsilon(1) = -\phi^3$ gives Kummer generators for J_2/k and K_2/k. We re-write these Kummer generators in terms of $\zeta, \phi, \pi_1, \pi_2, \pi_3, \pi_4$ and so obtain an alternative proof of Lemma 1.4.

L	Kummer generator for L/k		$\psi^{-1}\omega$	$\mathfrak{f}(L/k)$	d_L
J_1	$\prod \varepsilon(\zeta^i)^i$	$\zeta^2\pi_1\pi_2^3\pi_3^2\pi_4^4$	ω	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$5^{15}11^{16}$
K_1	$\eta(1)$	$\phi^2\pi_1\pi_2^4\pi_3^4\pi_4$	ω^2	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$5^{15}11^{16}$
K_2	$\eta(-\phi^{15})$	$\pi_1\pi_2\pi_3\pi_4$	1	$\mathfrak{l}^2\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$5^{23}11^{16}$
J_2	$\prod \varepsilon(-\zeta^i\phi^3)^i$	$\pi_1\pi_2^3\pi_3^2\pi_4^4$	ω	$\mathfrak{l}^5\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$5^{35}11^{16}$

We recall that if L/k is the Kummer extension corresponding to $\Delta \subset k^*/k^{*5}$, then $\mathrm{Gal}(L/k) \simeq \mathrm{Hom}(\Delta, \mu_5)$ as a $\mathrm{Gal}(k/\mathbf{Q})$-module. Thus in the notation of Lemma 1.3, Δ is described by $\psi^{-1}\omega$. This is born out in our table.

The final two columns of our table record the conductor $\mathfrak{f} = \mathfrak{f}(L/k)$ and the absolute discriminant d_L. They are related via $d_L = (\mathrm{Norm}\,\mathfrak{f})^4 d_k^5$. It is clear that the primes above 11 ramify in each extension L/k. We determine the factorisation of the prime above 5.

(i) The extension J_1/k is a translate of $\mathbf{Q}(\mu_{11})^+/\mathbf{Q}$, so $\mathfrak{l}$ is inert.
(ii) The extension K_1/k has Kummer generator

$$\eta(1) = \frac{1+\phi^5}{1-\phi^5} = \overline{\phi^5}\left(1 + \frac{\phi^5 - \overline{\phi^5}}{1+\overline{\phi^5}}\right). \tag{8}$$

Since $(\phi^5 - \overline{\phi^5})^2 = 5^3$ the binomial theorem shows that $\eta(1)$ is a 5th power in $k_{\mathfrak{l}}$. Thus $\mathfrak{l}$ splits in K_1/k.
(iii) The extension K_2/k has Kummer generator 11. The minimal polynomial for $\sqrt[5]{11}-1$ is an Eisenstein polynomial. Thus 5 is totally ramified in $K_2/\mathbf{Q}$. A useful intermediate step in computing d_{K_2} is to show that $\mathbf{Q}(\sqrt[5]{11})/\mathbf{Q}$ has discriminant $5^5 11^4$.
(iv) Since $J_1 J_2 = \mathbf{Q}(\mu_{25})\mathbf{Q}(\mu_{11})^+$ it is clear that $\mathfrak{l}$ ramifies in J_2/k. We recall [W, Proposition 2.1] that $\mathbf{Q}(\mu_{25})$ has discriminant 5^{35}.

Remark 3.4 Another quick way to show that J_1/k and K_1/k are unramified above 5 is provided by Proposition 2.1 and the observation that our Kummer generators belong to $S(A_1 \to A_0/k)$.

Lemma 3.5 *(i) The 5-ray class field of k with conductor $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ is J_1K_1.*
(ii) The 5-ray class field of k with conductor $\mathfrak{l}^2\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ is $J_1K_1K_2$.

Proof. We recall from [Coh, §3.2] a well known formula of class field theory

$$[k(\mathfrak{m}) : k] = \frac{h_k \phi(\mathfrak{m})}{[\mathfrak{o}_k^* : \mathfrak{o}_k^* \cap k_{\mathfrak{m},1}]}.$$

In our case we know $h_k = 1$ and $\mathfrak{o}_k^*$ is generated by $\pm\zeta$, ϕ.
(i) For $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ we have $\phi(\mathfrak{m}) = 10^4$ and $\mathfrak{o}_k^* \cap k_{\mathfrak{m},1}$ generated by ϕ^{10}. Thus the 5-ray class field has degree 5^2, and so must equal J_1K_1.
(ii) For $\mathfrak{m} = \mathfrak{l}^2\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ we have $\phi(\mathfrak{m}) = 20.10^4$ and $\mathfrak{o}_k^* \cap k_{\mathfrak{m},1}$ generated by ϕ^{20}. Thus the 5-ray class field has degree 5^3, and so must equal $J_1K_1K_2$. $\square$

To end this section, we exhibit some (modular) units in the fields K_1 and K_2. Our descent calculations in §6 and §7 shall require further units in addition to these.

Lemma 3.6 *(i) Let $\alpha = \sqrt[5]{\eta(1)}$ and $u_i = \varepsilon(\zeta^i\alpha)$. Then u_i is a unit in $K_1 = k(\alpha)$. The extension J_2K_1/K_1 has Kummer generator $u_1u_2^2u_3^3u_4^4$.*
(i) Let $\beta = \sqrt[5]{11}$ and $u_i = \varepsilon(\zeta^i\beta)$. Then u_i is a unit in $K_2 = k(\beta)$. The extension J_1K_2/K_2 has Kummer generator $u_1u_2^2u_3^3u_4^4$.

Proof. The cusps $\zeta\overline{\phi}$, $\zeta\phi$ have minimal polynomials

$$f(x) = x^4 + 3x^3 + 4x^2 + 2x + 1, \quad g(x) = x^4 - 2x^3 + 4x^2 - 3x + 1.$$

We may check $\eta(\varepsilon(x)^5) = xf(x)/g(x)$.
(i) Each u_i is a root of $xf(x)-g(x) = 0$ and so is a unit. We apply Lemma 3.2 with $\tau = \alpha$ to give the stated Kummer generator.
(ii) Since $\eta(11) = -\phi^{15}$, each u_i is a root of $xf(x) + \phi^{15}g(x) = 0$ and so is a unit. We apply Lemma 3.2 with $\tau = \beta$ to give the stated Kummer generator.
□

4 The Cassels-Tate pairing

Let C, D, ψ be as in the Introduction. There is an exact sequence

$$0 \longrightarrow C[\psi] \longrightarrow C[m] \xrightarrow{\psi} D[\widehat{\psi}] \longrightarrow 0. \tag{9}$$

Taking Galois cohomology and restricting to Selmer groups we obtain

$$D[\widehat{\psi}](F) \longrightarrow S^{(\psi)}(C/F) \longrightarrow S^{(m)}(C/F) \longrightarrow S^{(\widehat{\psi})}(D/K).$$

Proposition 4.1 *There is an alternating pairing*

$$S^{(\widehat{\psi})}(D/K) \times S^{(\widehat{\psi})}(D/K) \to \mathbf{Q}/\mathbf{Z} \tag{10}$$

whose kernel is the image of $S^{(m)}(C/F)$.

Proof. See Cassels [Ca2] or Milne [Mi]. □

We recall the definition of the pairing in the case m is odd. Our treatment follows that of McCallum [Mc]. For $(*)$ a global element or map, we write $(*)_{\mathfrak{p}}$ for the corresponding local object. The following commutative diagram is considered both in its own right and with F replaced by $F_{\mathfrak{p}}$ for each prime $\mathfrak{p}$.

$$\begin{array}{ccccc}
C(F) & \xrightarrow{\psi} & D(F) & \xrightarrow{\delta_\psi} & H^1(F, C[\psi]) \\
\| & & \downarrow{\scriptstyle\widehat{\psi}} & & \downarrow{\scriptstyle\iota} \\
C(F) & \xrightarrow{\times m} & C(F) & \xrightarrow{\delta_m} & H^1(F, C[m]) \\
\downarrow{\scriptstyle\psi} & & \| & & \downarrow{\scriptstyle\psi} \\
D(F) & \xrightarrow{\widehat{\psi}} & C(F) & \xrightarrow{\delta_{\widehat{\psi}}} & H^1(F, D[\widehat{\psi}])
\end{array}$$

To define the pairing we take $x, y \in S^{(\widehat{\psi})}(D/F) \subset H^1(K, D[\widehat{\psi}])$ and suppose given $x_1 \in H^1(F, C[m])$ lifting x. At each prime $\mathfrak{p}$ we choose $x_{\mathfrak{p},1} \in \operatorname{im} \delta_{m,\mathfrak{p}}$ such that $\psi(x_{\mathfrak{p},1}) = x_{\mathfrak{p}}$. Then $\psi(x_{\mathfrak{p},1} - x_{1,\mathfrak{p}}) = 0$ and so there exists $\xi_{\mathfrak{p}} \in H^1(F_{\mathfrak{p}}, C[\psi])$ with $\iota(\xi_{\mathfrak{p}}) = x_{\mathfrak{p},1} - x_{1,\mathfrak{p}}$. We define

$$\langle x, y \rangle = \sum_{\mathfrak{p}} (\xi_{\mathfrak{p}}, y_{\mathfrak{p}})_{\mathfrak{p}} \tag{11}$$

where $(\cdot,\cdot)_{\mathfrak{p}}$ is the Tate pairing $H^1(F_{\mathfrak{p}}, C[\psi]) \times H^1(F_{\mathfrak{p}}, D[\widehat{\psi}]) \to \mathbf{Q}/\mathbf{Z}$. Using Tate local duality and the product formula for the Tate pairing we may check that the definition is independent of all choices. It is clear that $\langle x, y \rangle = 0$ whenever x is in the image of $S^{(m)}(C/F)$.

Remark 4.2 More generally, the Cassels-Tate pairing is defined on the Tate-Shafarevich group $Ш(D/F)$. The restriction to $Ш(D/F)[\widehat{\psi}]$ is the pairing induced by (10). We may implicit use of this fact in due course.

Remark 4.3 Suppose C, D, ψ are defined over $F_0 \subset F$. If F is a normal extension of F_0 then (10) is $\mathrm{Gal}(F/F_0)$-equivariant. It is to be understood that the Galois action on $\mathbf{Q}/\mathbf{Z}$ is trivial.

We give a formula for (10) in the case where ψ is the 5-isogeny $A_1 \to A_0$ and F contains $K_1 = \mathbf{Q}(A_1[5])$. The exact sequence (9) becomes

$$0 \longrightarrow A_1[\psi] \longrightarrow A_1[5] \xrightarrow{\psi} A_0[\widehat{\psi}] \longrightarrow 0. \tag{12}$$

We choose a section for the map ψ in (12) and use this to construct x_1 from x. As McCallum [Mc] observes we may now express (11) as a sum of local pairings

$$\langle x, y \rangle = \sum_{\mathfrak{p}} \langle x_{\mathfrak{p}}, y_{\mathfrak{p}} \rangle_{\mathfrak{p}}.$$

Furthermore the local pairing is trivial outside the usual set of bad primes, in our case those above 5 and 11. The description of $S(A_0 \to A_1/F)$ given in Proposition 2.1 tells us that x, y are already trivial at $\mathfrak{p}|11$. So it only remains to compute the local pairing at $\mathfrak{p}|5$.

In §3 we saw that K_1/k has Kummer generator $\eta(1) = (1+\phi^5)/(1-\phi^5)$. We put $\alpha = \sqrt[5]{\eta(1)}$. By (8) the primes above 5 split in K_1/k. We label them $\mathfrak{L}_0, \mathfrak{L}_1, \ldots, \mathfrak{L}_4$ such that $\alpha \equiv \zeta^i \phi \pmod{\mathfrak{L}_i^2}$.

Lemma 4.4 *Let F be a number field with $F \supset K_1$. Let $\mathfrak{p}|5$ be a prime and let $e = e(\mathfrak{p}/5)$. Then there exists $i = i(\mathfrak{p})$ in $\mathbf{Z}/5\mathbf{Z}$ such that $\alpha \equiv \zeta^i \phi \pmod{\mathfrak{p}^{e/2}}$.*

Proof. We have $i = i(\mathfrak{p})$ if and only if $\mathfrak{p}|\mathfrak{L}_i$. $\square$

Proposition 4.5 *Let F be a number field with $F \supset K_1$. Then the Cassels-Tate pairing on $S(A_0 \to A_1/F) \subset F^*/F^{*5}$ is given, up to scalars, by*

$$\langle \theta, \theta' \rangle = \textstyle\sum_{\mathfrak{p}|5} \mathrm{Ind}_\zeta (\theta, \theta')_{\mathfrak{p}}^{i(\mathfrak{p})}$$

where $(\cdot, \cdot)_{\mathfrak{p}}$ is the Hilbert norm residue symbol.

Remark 4.6 To remove the qualifier "up to scalars" we must specify the isomorphism $A_0[\widehat{\psi}] \simeq \mu_5$ used to embed $S(A_0 \to A_1/F)$ inside F^*/F^{*5}. For the proof of Theorems 1 and 2, a formula "up to scalars" is good enough.

Lemma 4.7 *Let $P \in A_1[\psi]$ and $Q \in A_0[\widehat{\psi}]$ with $e_\psi(P, Q) = \zeta$. Then we may label the inverse image $\psi^{-1}(Q) = \{Q_0, Q_1, \ldots, Q_4\}$ such that Q_i belongs to the kernel of reduction mod $\mathfrak{L}_i$.*

Proof. Let $\widetilde{\ }$ denote reduction mod $\mathfrak{L}_i$. By inspection of the Weierstrass equation (4) the reduction $\widetilde{A}_1(\mathbf{F}_5) \simeq \mathbf{Z}/5\mathbf{Z}$ is generated by $\widetilde{P}$. The kernel of the reduction map $A_1[5] \to \widetilde{A}_1(\mathbf{F}_5)$ is cyclic of order 5. We choose a generator Q_i with $\psi(Q_i) = Q$. Then $\mathrm{Gal}(K_1/k)$ permutes both the $\mathfrak{L}_i$ and the Q_i. $\square$

The Weil pairing and Hilbert's theorem 90 allow us to identify

$$\begin{array}{rcl} H^1(F, A_1[\psi]) & = & \mathrm{Hom}(A_0[\widehat{\psi}], F^*/F^{*5}) \\ H^1(F, A_1[5]) & = & \mathrm{Hom}(A_1[5], F^*/F^{*5}) \\ H^1(F, A_0[\widehat{\psi}]) & = & \mathrm{Hom}(A_1[\psi], F^*/F^{*5}). \end{array} \tag{13}$$

We give a more precise version of Proposition 4.5.

Lemma 4.8 *Let F be a number field with $F \supset K_1$. Let P, $Q_i \in A_1[5]$ be chosen as in Lemma 4.7. Then the Cassels-Tate pairing on $S(A_0 \to A_1/F) \subset$ $\mathrm{Hom}(A_1[\psi], F^*/F^{*5})$ is given by*

$$\langle x, y \rangle = \textstyle\sum_{\mathfrak{p}|5} \mathrm{Ind}_\zeta (x(Q_1 - Q_0), y(P))_{\mathfrak{p}}^{i(\mathfrak{p})}.$$

Proposition 4.5 follows immediately from Lemma 4.8, since P and $Q_1 - Q_0$ are both generators for $A_1[\psi]$.

Lemma 4.9 *Let $\mathfrak{p}|5$ with $i = i(\mathfrak{p})$. Then the local connecting map* $\delta_{5,\mathfrak{p}} : A_1(F_\mathfrak{p}) \to \mathrm{Hom}(A_1[5], F_\mathfrak{p}^*/F_\mathfrak{p}^{*5})$ *has image*

$$\left\{\, x \in \mathrm{Hom}(A_1[5], \mathfrak{O}_\mathfrak{p}^*/\mathfrak{O}_\mathfrak{p}^{*5}) \,\middle|\, F_\mathfrak{p}(\sqrt[5]{x(Q_i)})/F_\mathfrak{p} \text{ is unramified} \right\}. \tag{14}$$

Proof. Let $x = \delta_{5,\mathfrak{p}}(T)$ for some $T \in A_1(F_\mathfrak{p})$. The description of $\operatorname{im}\delta_{\widehat{\psi},\mathfrak{p}}$ used in the proof of Proposition 2.1 shows that $x(P)$ is a unit. Let $T' \in A_1(\overline{F}_\mathfrak{p})$ with $5T' = T$. Then x is represented by the cocycle $\sigma(T') - T'$ in $H^1(F_\mathfrak{p}, A_1[5])$. But if σ belongs to the inertia subgroup, then $\sigma(T') - T'$ belongs to the kernel of reduction mod $\mathfrak{p}$ and $e_5(Q_i, \sigma(T') - T') = 1$. Hence $x(Q_i)$ is unramified.

We have shown that $\operatorname{im}\delta_{5,\mathfrak{p}}$ belongs to (14). But $\operatorname{im}\delta_{5,\mathfrak{p}} \subset H^1(F_\mathfrak{p}, A_1[5])$ is a maximal isotropic subspace with respect to the Tate pairing. A counting argument completes the proof of the lemma. □

The identifications (13) allow us to express the Tate pairing in terms of the Hilbert norm residue symbol.

Lemma 4.10 *The Tate pairing $H^1(F_\mathfrak{p}, A_1[\psi]) \times H^1(F_\mathfrak{p}, A_0[\widehat{\psi}]) \to \mathbf{Q}/\mathbf{Z}$ is given by*

$$(x, y)_\mathfrak{p} = \mathrm{Ind}_\zeta(x(Q), y(P))_\mathfrak{p}^{-1}$$

where $(\cdot,\cdot)_\mathfrak{p}$ on the right is the Hilbert norm residue symbol.

Proof. We recall $e_\psi(P, Q) = \zeta$. The lemma follows by a standard cup product calculation. □

Proof of Lemma 4.8. The map ψ in (12) has section $Q \mapsto Q_0$. Let x, y belong to $S(A_0 \to A_1/F)$. By (13) we view x, y as maps $A_1[\psi] \to F^*/F^{*5}$. Then $x_1 : A_1[5] \to F^*/F^{*5}$ extends x via $Q_0 \mapsto 1$. For each $\mathfrak{p}|5$ we extend $x_\mathfrak{p}$ to $x_{\mathfrak{p},1} : A_1[5] \to F_\mathfrak{p}^*/F_\mathfrak{p}^{*5}$ via $Q_{i(\mathfrak{p})} \mapsto 1$. Then $x_{\mathfrak{p},1} \in \operatorname{im}\delta_{5,\mathfrak{p}}$ and $\xi_\mathfrak{p}(Q) = x(Q_0 - Q_{i(\mathfrak{p})}) = x(Q_1 - Q_0)^{-i(\mathfrak{p})}$. The local pairing is

$$\begin{aligned} \langle x_\mathfrak{p}, y_\mathfrak{p}\rangle_\mathfrak{p} &= (\xi_\mathfrak{p}, y_\mathfrak{p})_\mathfrak{p} \\ &= \mathrm{Ind}_\zeta(\xi_\mathfrak{p}(Q), y_\mathfrak{p}(P))_\mathfrak{p}^{-1} \\ &= \mathrm{Ind}_\zeta(x_\mathfrak{p}(Q_1 - Q_0), y_\mathfrak{p}(P))_\mathfrak{p}^{i(\mathfrak{p})}. \end{aligned}$$

This completes the proof of Lemma 4.8 and so of Proposition 4.5. □

5 Some Galois modules

The polynomials $x^5 + 2x^4 + 6x^3 - 2x^2 + 4x - 1$ and $x^5 - 11$ have splitting fields $K_1 = \mathbf{Q}(A_1[5])$ and $K_2 = \mathbf{Q}(A_2[5])$. In each case the Galois group is

$$G := \langle\, \sigma, \tau \mid \sigma^4 = \tau^5 = 1, \sigma\tau\sigma^{-1} = \tau^2 \,\rangle.$$

In preparation for the proof of Theorems 1 and 2, we give some preliminaries on $\mathbf{Z}/5\mathbf{Z}[G]$-modules. We define $\psi : G \to (\mathbf{Z}/5\mathbf{Z})^*$ via $\sigma \mapsto 2$ and $\tau \mapsto 1$. Any $\mathbf{Z}/5\mathbf{Z}[G]$-module M may be decomposed into σ-eigenspaces

$$M = M^1 \oplus M^{\psi} \oplus M^{\psi^2} \oplus M^{\psi^3} \tag{15}$$

where $M^{\chi} = \{x \in M | \sigma x = \chi(\sigma)x\}$. If $M = M^{\chi}$ we say that M is described by χ. In particular ψ describes the action of G on $\langle\tau\rangle$ via conjugation.

Lemma 5.1 *Let M be a $\mathbf{Z}/5\mathbf{Z}[G]$-module with $M/(\tau-1)M \simeq \mathbf{Z}/5\mathbf{Z}$ as an abelian group. Then*
(i) $M/(\tau-1)M$ is described by some character $\chi : G \to (\mathbf{Z}/5\mathbf{Z})^*$.
(ii) M has dimension $d := \dim_{\mathbf{Z}/5\mathbf{Z}} M$ with $d \leq 5$.
(iii) The pair (χ, d) uniquely determines M as a G-module.
(iv) If $d \leq 4$ then $\mathrm{End}_G(M) \simeq \mathbf{Z}/5\mathbf{Z}$.

Proof. (i) This is clear.
(ii) Let $M_i = (\tau-1)^i M$. The decreasing filtration of $\mathbf{Z}/5\mathbf{Z}[G]$-modules

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots \tag{16}$$

satisfies $\dim_{\mathbf{Z}/5\mathbf{Z}} M_i/M_{i+1} \geq \dim_{\mathbf{Z}/5\mathbf{Z}} M_{i+1}/M_{i+2}$. But $\dim_{\mathbf{Z}/5\mathbf{Z}} M_0/M_1 = 1$, so $d = \min\{i \mid M_i = 0\}$. Since $(\tau-1)^5 \equiv 0 \pmod 5$ we must have $d \leq 5$.
(iii) We pick $x \in M^{\chi}$ a generator for $M/(\tau-1)M$. Then M has basis $x, (\tau-1)x, \ldots, (\tau-1)^{d-1}x$ as a $\mathbf{Z}/5\mathbf{Z}$-vector space. The actions of σ and τ on this basis are uniquely determined.
(iv) The quotient M_i/M_{i+1} is described by $\chi\psi^i$. Thus for $d \leq 4$ the decomposition (15) is into 1-dimensional spaces, and the element x in the proof of (iii) is uniquely determined up to scalars. □

We write $M(\chi, d)$ for the $\mathbf{Z}/5\mathbf{Z}[G]$-module described in Lemma 5.1. We abbreviate $M(\chi) = M(\chi, 1)$. The filtration (16) becomes

$$M(\chi, d) \supset M(\chi\psi, d-1) \supset \ldots \supset M(\chi\psi^{d-1}, 1) \supset 0.$$

For M a G-module we recall that $M^* := \mathrm{Hom}(M, \mathbf{Z}/5\mathbf{Z})$ is a G-module via $g\theta = \theta.g^{-1}$.

Lemma 5.2 $M(\chi,d)^* \simeq M(\chi^{-1}\psi^{1-d},d)$.

Proof. The case $d=1$ is clear. The general case follows from Lemma 5.1 and the observation $\mathrm{coker}(\tau-1|M^*) \simeq \ker(\tau-1|M)^*$. $\square$

With properties of the Cassels-Tate pairing in mind, we say that a bilinear form $\langle\ ,\ \rangle : M \times N \to \mathbf{Q}/\mathbf{Z}$ is G-equivariant if $\langle gx, gy\rangle = \langle x, y\rangle$ for all $g \in G$. Equivalently $M \to N^*$ is a G-module homomorphism.

Lemma 5.3 *Any non-zero G-equivariant pairing on $M(\chi,d)$ has odd rank. In particular there are no non-zero alternating G-equivariant pairings.*

Proof. Suppose $f : M(\chi,d) \to M(\chi^{-1}\psi^{1-d},d)$ is a G-module map of rank r. Then $\mathrm{im}\, f = M(\chi^{-1}\psi^{1-r},r)$. We deduce $\chi = \chi^{-1}\psi^{1-r}$ and so r is odd. $\square$

Lemma 5.4 *Assume $d \le 4$. Then any non-zero alternating G-equivariant pairing on $M := M(\chi,d) \oplus M(\chi^{-1}\psi^{1-d},d)$ is non-degenerate.*

Proof. We claim that, up to scalars, M admits a unique alternating G-equivariant pairing. By Lemma 5.3 any such pairing is trivial when restricted to either summand. We are reduced to showing that there is a unique G-equivariant bilinear form

$$M(\chi,d) \times M(\chi^{-1}\psi^{1-d},d) \to \mathbf{Z}/5\mathbf{Z}.$$

Lemma 5.2 gives the existence. Lemma 5.1(iv) gives the uniqueness up to scalars. Finally we observe that the pairing constructed is non-degenerate. $\square$

We give an example typical of the G-modules we encounter. The group G acts on the affine line $\mathbf{Z}/5\mathbf{Z}$ via $\sigma : x \mapsto 2x$ and $\tau : x \mapsto x+1$. The corresponding permutation representation, with coefficients in $\mathbf{Z}/5\mathbf{Z}$, is $M(1,5)$. We construct further G-modules using $M(\chi_1\chi_2,d) = M(\chi_1) \otimes M(\chi_2,d)$.

6 Descent calculations over $K_1 = \mathbf{Q}(A_1[5])$

We recall that K_1/k has Kummer generator $\eta(1) = (1+\phi^5)/(1-\phi^5)$. We put $\alpha = \sqrt[5]{\eta(1)}$. Then $\mathrm{Gal}(K_1/\mathbf{Q}) \simeq G$ via

$$\begin{array}{ll} \sigma(\zeta) = \zeta^3 & \sigma(\alpha) = -1/\alpha \\ \tau(\zeta) = \zeta & \tau(\alpha) = \zeta\alpha. \end{array}$$

The cyclotomic character ω, and the character ψ of §5 are related via $\psi = \omega^{-1}$. The primes 5 and 11 factor in K_1 as

$$(5) = \mathfrak{L}_0^4\mathfrak{L}_1^4\mathfrak{L}_2^4\mathfrak{L}_3^4\mathfrak{L}_4^4 \qquad (11) = \mathfrak{P}_1^5\mathfrak{P}_2^5\mathfrak{P}_3^5\mathfrak{P}_4^5$$

with $\alpha \equiv \zeta^i\phi \pmod{\mathfrak{L}_i^2}$ and $\mathfrak{P}_i|\mathfrak{p}_i$. In §3 we saw that $H_1 := J_1K_1$ is the 5-ray class field of k for conductor $(11) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.

Lemma 6.1 *The extension H_1/K_1 is unramified at all primes. Furthermore the primes above 5 and 11 are inert in this extension.*

Proof. Only primes above 11 ramify in H_1/k. By considering suitable ratios of our Kummer generators for J_1/k and K_1/k we see that $\mathfrak{p}_i$ cannot be totally ramified in H_1/k. Hence H_1/K_1 is unramified as claimed. Now H_1/K_1 is a translate of $\mathbf{Q}(\mu_{11})^+/\mathbf{Q}$. Since 5 is inert in $\mathbf{Q}(\mu_{11})^+/\mathbf{Q}$ and $\mathfrak{L}_i$ has residue field $\mathbf{F}_5$, it follows that $\mathfrak{L}_i$ is inert. Finally the definitions of J_1 and K_1 give $\#A_1(H_1)(5) \geq 5^3$, so by Lemma 1.7 the $\mathfrak{P}_i$ are inert. □

Proposition 6.2 *The 5-class group of K_1 is $\mathfrak{Cl}_{K_1}(5) \simeq \mathbf{Z}/5\mathbf{Z}$. It is generated by any prime above 5 or 11.*

Proof. Let $B = \mathfrak{Cl}_{K_1}(5)$. By Lemma 3.5(i) we know that H_1 is the maximal unramified 5-extension of K_1 which is abelian over k. Thus

$$B/(\tau - 1)B \simeq \mathrm{Gal}(H_1/K_1) \simeq \mathbf{Z}/5\mathbf{Z}$$

as abelian groups. By Lemma 6.1, $\mathfrak{P}_1$ is inert in H_1/K_1 and so generates $B/(\tau-1)B$. Since $(\tau - 1)^5 \subset 5\mathbf{Z}_5[\tau]$ it follows that $\mathfrak{P}_1$ generates B as a $\mathbf{Z}_5[\tau]$-module. But $\tau(\mathfrak{P}_1) = \mathfrak{P}_1$ and $\mathfrak{P}_1^5 = \mathfrak{p}_1$ is principal. Thus $B \simeq \mathbf{Z}/5\mathbf{Z}$ as claimed. By Lemma 6.1, B is generated by any prime above 5 or 11. □

Remark 6.3 Since $\sigma(\mathfrak{L}_0) = \mathfrak{L}_0$ and $\tau(\mathfrak{P}_1) = \mathfrak{P}_1$ the action of G on $\mathfrak{Cl}_{K_1}(5)$ is trivial. In particular $\mathfrak{P}_1 \sim \mathfrak{P}_2 \sim \mathfrak{P}_3 \sim \mathfrak{P}_4$.

We turn our attention to the units in K_1. We write

$$u_i = \frac{\phi\zeta^i\alpha + 1}{\zeta^i\alpha - \phi} \qquad v_i = \frac{\zeta^i\alpha + 1}{\zeta^i\alpha - 1}.$$

The u_i are units by Lemma 3.6. For the v_i we have $(v_i+1)^5/(v_i-1)^5 = (1+\phi^5)/(1-\phi^5)$. Thus each v_i is a root of

$$\phi^5(x^5+10x^3+5x)-(5x^4+10x^2+1)=0$$

and so is a unit. It is easy to check

$$\begin{array}{ll} \sigma(u_i)=u_{2i} & \sigma(v_i)=-1/v_{2i} \\ \tau(u_i)=u_{i+1} & \tau(v_i)=v_{i+1} \end{array}$$

and we have relations $\prod u_i = 1$, $\prod v_i = \phi^{-5}$. Thus the subgroups of K_1^*/K_1^{*5} generated by u_1, u_2, u_3, u_4 and v_1, v_2, v_3, v_4 are quotients of the G-modules $M(1,4)$ and $M(\omega^2, 4)$.

Proposition 6.4 *The units $\zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4$ generate a subgroup of $\mathfrak{O}_{K_1}^*$ of index prime to 5.*

Proof. By Dirichlet it suffices to check that the elements listed are independent in K_1^*/K_1^{*5}. There is a G-module homomorphism

$$M := M(\omega)\oplus M(\omega^2)\oplus M(1,4)\oplus M(\omega^2,4)\to K_1^*/K_1^{*5}$$

where the summands correspond to ζ, ϕ, $\langle u_1, u_2, u_3, u_4\rangle$ and $\langle v_1, v_2, v_3, v_4\rangle$. We suppose for a contradiction that this map has non-trivial kernel. Then this kernel meets

$$\begin{aligned} \ker(\tau-1|M) &= M(\omega)\oplus M(\omega^2)\oplus M(\omega)\oplus M(\omega^3) \\ &= \langle\, \zeta, \phi, u_1u_2^2u_3^3u_4^4, v_1v_2^2v_3^3v_4^4 \,\rangle. \end{aligned}$$

Dividing into σ-eigenspaces we learn that one of the elements

$$\zeta^i(u_1u_2^2u_3^3u_4^4)^j, \quad \phi, \quad v_1v_2^2v_3^3v_4^4$$

is a 5th power. For ζ and ϕ this is clearly false, since no unit can be a Kummer generator for K_1/k. The smallest prime to split completely in $K_1/\mathbf{Q}$ is $p=101$. Reducing modulo primes above p we obtain a contradiction. $\square$

Remark 6.5 Further to the proof Proposition 6.4, a brutal computer calculation shows

$$\begin{array}{ll} \pi_1\pi_2^3\pi_3^2\pi_4^4 \equiv (u_1u_2^2u_3^3u_4^4)^3 & \pmod{K_1^{*5}} \\ \pi_1\pi_2^2\pi_3^3\pi_4^4 \equiv (v_1v_2^2v_3^3v_4^4)^3 & \pmod{K_1^{*5}}. \end{array}$$

Remark 6.6 According to `pari` the field K_1 has class number 5, and

$$\phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4$$

is a set of fundamental units. However `pari` assumes the Generalised Riemann Hypothesis, whereas our results are unconditional.

We apply Propositions 2.1 and 2.2 in the case $F = K_1$.

Proposition 6.7 *The Selmer groups attached to the 5-isogenies (1) are*

$$\begin{array}{ll} S(A_0 \to A_1/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^8 & S(A_2 \to A_0/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^{14} \\ S(A_1 \to A_0/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & S(A_0 \to A_2/K_1) = 0. \end{array}$$

Proof. By Propositions 6.2 and 6.4 the space

$$\{ \theta \in K_1^*/K_1^{*5} \mid \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 5 \text{ for all } \mathfrak{p} \}$$

has basis $\zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, 11$. Here 11 is a contribution from the class group or "virtual unit". We choose characters $(\mathfrak{O}_{K_1}/\mathfrak{P}_i)^* \to \mathbf{Z}/5\mathbf{Z}$ and compute these characters on our basis. Notice that by inspection of our Kummer generator for K_1/k we have $11 \equiv (1+\phi^5)^2 \equiv (1-\phi^5)^2 \pmod{K_1^{*5}}$. Thus our table is easily computed by hand.

	$\mathfrak{P}_1$	$\mathfrak{P}_2$	$\mathfrak{P}_3$	$\mathfrak{P}_4$
ζ	1	3	2	4
ϕ	2	3	3	2
u_i	2	2	2	2
v_i	0	0	0	0
11	2	2	2	2

By Proposition 2.1 we deduce

$$S(A_0 \to A_1/K_1) \simeq \langle u_1', u_2', u_3', u_4', v_1, v_2, v_3, v_4 \rangle \subset K_1^*/K_1^{*5}$$

where $u_i' = u_i/11$. Propositions 2.1 and 6.2 show that $S(A_0 \to A_2/K_1)$ is trivial. The remaining statements follow by Proposition 2.2. □

Proposition 6.7 furnishes the estimate $\mathrm{rank}\, A(K_1) \leq 8$. We improve on this by computing the Cassels-Tate pairing

$$S(A_0 \to A_1/K_1) \times S(A_0 \to A_1/K_1) \to \mathbf{Q}/\mathbf{Z}. \tag{17}$$

As a G-module we have

$$S(A_0 \to A_1/K_1) \simeq M(1,4) \oplus M(\omega^2,4)$$

where the summands correspond to $\langle u_1', u_2', u_3', u_4' \rangle$ and $\langle v_1, v_2, v_3, v_4 \rangle$. By Lemma 5.3 the pairing (17) is trivial when restricted to either summand. It therefore suffices for us to compute the entries $\langle u_r', v_s \rangle$. By Proposition 4.5 and the action of $\mathrm{Gal}(K_1/k)$ we have

$$\begin{aligned}\langle u_r', v_s \rangle &= \textstyle\sum_{i=0}^4 \mathrm{Ind}_\zeta (u_r', v_s)_{\mathfrak{L}_i}^i \\ &= \textstyle\sum_{i=0}^4 \mathrm{Ind}_\zeta (u_{r-i}', v_{s-i})_{\mathfrak{L}_0}^i\end{aligned}$$

We recall that $\mathfrak{L}_0$ is the prime of K_1 above 5 such that $\alpha \equiv \phi \pmod{\mathfrak{L}_0^2}$. But α is a 5th root of

$$\eta(1) = \frac{1+\phi^5}{1-\phi^5} = -\phi^{15}\left(1 + \frac{10(\overline{\phi^5} - \phi^5)}{1+10\phi^5}\right). \tag{18}$$

The binomial theorem gives $\alpha \equiv -\phi^3 \pmod{\mathfrak{L}_0^6}$ and for $r \neq 0$ it follows

$$\begin{aligned} u_r &\equiv (\zeta^r\phi^4 - 1)/(\zeta^r\phi^3 + \phi) \qquad \pmod{\mathfrak{L}_0^6} \\ v_s &\equiv (\zeta^s\phi^3 - 1)/(\zeta^s\phi^3 + 1) \qquad \pmod{\mathfrak{L}_0^6}. \end{aligned}$$

Using these approximations we are reduced to computing the Hilbert norm residue symbol at the prime $\mathfrak{l} = (1-\zeta)$ of $k = \mathbf{Q}(\mu_5)$. This is straightforward, if tedious, to do by hand. See [CF, Exercises 1 and 2]. We find

$(\ ,\ )_{\mathfrak{L}_0}$	v_0	v_1	v_2	v_3	v_4
u_0'	1	ζ^2	ζ^4	ζ	ζ^3
u_1'	ζ^3	ζ^2	ζ^4	1	ζ
u_2'	ζ	1	ζ^4	ζ^2	ζ^3
u_3'	ζ^4	ζ^2	ζ^3	ζ	1
u_4'	ζ^2	ζ^4	1	ζ	ζ^3

$5\langle\ ,\ \rangle$	v_0	v_1	v_2	v_3	v_4
u_0'	0	4	1	1	4
u_1'	4	0	4	1	1
u_2'	1	4	0	4	1
u_3'	1	1	4	0	4
u_4'	4	1	1	4	0

The matrix on the right has rank 3, and so the pairing (17) has rank 6. The kernel is generated by $u_1u_2^2u_3^3u_4^4$ and $v_1v_2^2v_3^3v_4^4$. By Corollary 1.6 and Lemma 3.6 the first of these elements is accounted for by torsion, whereas the second is not.

By Propositions 4.1 and 6.7 we deduce

$$S(A_1 \xrightarrow{\times 5} A_1/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^4.$$

This furnishes the estimate $\operatorname{rank} A(K_1) \le 2$. Since $\operatorname{rank} A(k) = 0$ the action of $\mathrm{Gal}(K_1/k)$ on $A(K_1) \otimes \mathbf{Q}$ forces $\operatorname{rank} A(K_1) \equiv 0 \pmod 4$. Thus $\operatorname{rank} A(K_1) = 0$ and $Ш(A_1/K_1)[5] \simeq (\mathbf{Z}/5\mathbf{Z})^2$. However, to identify the 5-primary part of the Tate-Shafarevich group we must work harder.

We aim to compute $S(A_0 \overset{\times 5}{\to} A_0/K_1)$ as a G-module. To identify it as an abelian group we make use of the exact sequences

$$\begin{array}{l} 0 \longrightarrow S(A_0 \to A_1/K_1) \longrightarrow S(A_0 \overset{\times 5}{\to} A_0/K_1) \overset{\psi_1}{\longrightarrow} S(A_1 \to A_0/K_1) \\ 0 \longrightarrow S(A_0 \to A_2/K_1) \longrightarrow S(A_0 \overset{\times 5}{\to} A_0/K_1) \overset{\psi_2}{\longrightarrow} S(A_2 \to A_0/K_1) \end{array} \tag{19}$$

The images of the maps ψ_1 and ψ_2 are the kernels of the Cassels-Tate pairings

$$\begin{array}{l} \Psi_1 : S(A_1 \to A_0/K_1) \times S(A_1 \to A_0/K_1) \to \mathbf{Z}/5\mathbf{Z} \\ \Psi_2 : S(A_2 \to A_0/K_1) \times S(A_2 \to A_0/K_1) \to \mathbf{Z}/5\mathbf{Z} \end{array} \tag{20}$$

Lemma 6.8 *The pairings Ψ_1 and Ψ_2 have ranks 0 and 4 respectively.*

Proof. The alternating pairing Ψ_1 is defined on $S(A_1 \to A_0/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^2$. By Corollary 1.6 this Selmer group contains a contribution from torsion. Hence Ψ_1 is trivial. The exact sequences (19), together with Propositions 4.1 and 6.7, now tell us that $S(A_0 \overset{\times 5}{\to} A_0/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^{10}$ and that the pairing Ψ_2 has rank 4. □

The exact sequences (19) provide inclusions

$$S(A_0 \to A_1/K_1) \subset S(A_0 \overset{\times 5}{\to} A_0/K_1) \subset S(A_2 \to A_0/K_1) \subset K_1^*/K_1^{*5} \tag{21}$$

By Remark 6.5 there exist w_1, w_2 in K_1 with

$$\begin{aligned} w_1^5 &= \pi_1 \pi_2^{-2} \pi_3^2 \pi_4^{-1} (u_1 u_2^2 u_3^3 u_4^4)^2 \\ w_2^5 &= \pi_1 \pi_2^2 \pi_3^{-2} \pi_4^{-1} (v_1 v_2^2 v_3^3 v_4^4)^2. \end{aligned}$$

A rather tedious calculation suggests we write $x_1 = w_1 u_2^2 u_3 u_4^3 (v_1 v_2^2 v_3^3 v_4^4)^3$ and $x_2 = w_2 v_1^3 v_2^3 (u_1 u_2^2 u_3^3 u_4^4)^3$, whereupon, multiplying x_2 by a 5th root of unity if necessary

$$\begin{array}{llll} \sigma(x_1) \equiv x_1^3 & \pmod{K_1^{*5}} & \sigma(x_2) \equiv x_2^2 & \pmod{K_1^{*5}} \\ \tau(x_1) \equiv x_1 u_2^3 u_3 u_4^3 & \pmod{K_1^{*5}} & \tau(x_2) \equiv x_2 \phi^2 v_2^3 v_3 v_4^3 & \pmod{K_1^{*5}} \end{array} \tag{22}$$

Proposition 6.9 *Multiplying x_1 by a 5th root of unity if necessary, the Selmer groups (21) are*

$$\begin{aligned} S(A_0 \to A_1/K_1) &\simeq \langle u_1', u_2', u_3', u_4', v_1, v_2, v_3, v_4 \rangle \\ S(A_0 \overset{\times 5}{\to} A_0/K_1) &\simeq \langle u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, 11, x_1 \rangle \\ S(A_2 \to A_0/K_1) &\simeq \langle \zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, 11, \alpha, x_1, x_2 \rangle. \end{aligned}$$

Proof. The descriptions of $S(A_0 \to A_1/K_1)$ and $S(A_2 \to A_0/K_1)$ follow from Proposition 2.1. Now $S(A_0 \overset{\times 5}{\to} A_0/K_1)$ is the kernel of the pairing Ψ_2 and this pairing induces a pairing on the quotient

$$\frac{S(A_2 \to A_0/K_1)}{S(A_0 \to A_1/K_1)} \simeq \langle \zeta, \phi, 11, \alpha, x_1, x_2 \rangle. \tag{23}$$

Decomposing into σ-eigenspaces, we learn that $S(A_0 \overset{\times 5}{\to} A_0/K_1)$ has basis

$$u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, 11, z$$

for some $z = \zeta^i x_1^j$. Since we consider ourselves free to multiply x_1 by a 5th root of unity, it only remains to show $\zeta \notin S(A_0 \overset{\times 5}{\to} A_0/K_1)$. To do this we identify (23) as a G-module. By (22)

$$\begin{aligned} \tau(x_1) &\equiv x_1 11^2 \qquad \bmod \langle u_1', u_2', u_3', u_4', K_1^{*5} \rangle \\ \tau(x_2) &\equiv x_2 \phi^2 \qquad \bmod \langle v_1, v_2, v_3, v_4, K_1^{*5} \rangle \end{aligned}$$

whereas $\tau(\alpha) = \zeta\alpha$ and $\zeta, \phi, 11 \in k$ are fixed by τ. Thus

$$\frac{S(A_2 \to A_0/K_1)}{S(A_0 \to A_1/K_1)} \simeq M(\omega, 2) \oplus M(\omega^2, 2) \oplus M(\omega^3, 2).$$

By Lemma 5.4 the pairing Ψ_2 restricted to

$$M(\omega^2, 2) \oplus M(\omega^3, 2) \simeq \langle \zeta, \phi, \alpha, x_2 \rangle$$

is either zero or non-degenerate. But it cannot be zero by our earlier consideration of σ-eigenspaces. Thus $\zeta \notin S(A_0 \overset{\times 5}{\to} A_0/K_1)$ and we are done. $\square$

Remark 6.10 An alternative proof of Proposition 6.9 is given by computing Ψ_2 via the formula of [F0, §7.3].

As a G-module we have

$$S(A_0 \stackrel{\times 5}{\to} A_0/K_1) \simeq M(1) \oplus M(\omega, 5) \oplus M(\omega^2, 4)$$

where the summands correspond to 11, $\langle u_1, u_2, u_3, u_4, x_1 \rangle$ and $\langle v_1, v_2, v_3, v_4 \rangle$. The contributions from torsion are 11 and $u_1 u_2^2 u_3^3 u_4^4$. Thus

$$\frac{S(A_0 \stackrel{\times 5}{\to} A_0/K_1)}{\operatorname{im}(\delta|A_0[5])} \simeq M(\omega, 4) \oplus M(\omega^2, 4). \tag{24}$$

Our earlier calculation of the pairing (17) shows that the Cassels-Tate pairing on (24) is non-zero. By Lemma 5.4 the Cassels-Tate pairing on (24) is non-degenerate. It follows that $Ш(A_0/K_1)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^8$.

Earlier we saw $Ш(A_1/K_1)[5] \simeq (\mathbf{Z}/5\mathbf{Z})^2$. We claim that $Ш(A_1/K_1)$ contains no element of order 25. Indeed, from the exact sequences

$$A_1(K_1) \xrightarrow{\psi} A_0(K_1) \longrightarrow S(A_1 \to A_0/K_1) \longrightarrow Ш(A_1/K_1)[\psi] \longrightarrow 0$$
$$0 \longrightarrow Ш(A_1/K_1)[\psi] \longrightarrow Ш(A_1/K_1)(5) \xrightarrow{\psi} Ш(A_0/K_1)(5)$$

we learn that $Ш(A_1/K_1)(5)$ is finite and contains no copy of $(\mathbf{Z}/25\mathbf{Z})^2$. Our claim is now a well known consequence of the Cassels-Tate pairing.

Finally the exact sequence

$$S(A_2 \to A_0/K_1) \longrightarrow S(A_2 \stackrel{\times 5}{\to} A_2/K_1) \longrightarrow S(A_0 \to A_2/K_1) = 0$$

shows that $S(A_2 \stackrel{\times 5}{\to} A_2/K_1) \simeq (\mathbf{Z}/5\mathbf{Z})^{13}$. By Lemma 6.8 the Cassels-Tate pairing on this Selmer group has rank 4. Since the multiplication by 5 map on A_2 factors through A_0 and $Ш(A_0/K_1)(5)$ is 5-torsion, we deduce

$$Ш(A_2/K_1)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^4 \oplus (\mathbf{Z}/25\mathbf{Z})^8.$$

This completes the proof of Theorem 1.

7 Descent calculations over $K_2 = \mathbf{Q}(A_2[5])$

We recall that K_2/k has Kummer generator 11. We put $\beta = \sqrt[5]{11}$. Then $\operatorname{Gal}(K_2/\mathbf{Q}) \simeq G$ via

$$\begin{array}{ll} \sigma(\zeta) = \zeta^2 & \qquad \sigma(\beta) = \beta \\ \tau(\zeta) = \zeta & \qquad \tau(\beta) = \zeta\beta. \end{array}$$

The cyclotomic character ω and the character ψ of §5 are equal. The primes above 5 and 11 ramify in K_2/k. We write

$$(5) = \mathfrak{L}^{20} \qquad (11) = \mathfrak{P}_1^5 \mathfrak{P}_2^5 \mathfrak{P}_3^5 \mathfrak{P}_4^5$$

with $\mathfrak{P}_i | \mathfrak{p}_i$. In §3 we saw that $H_2 := J_1 K_1 K_2$ is the 5-ray class field of k for conductor $\mathfrak{l}^2 \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4$.

Lemma 7.1 *The extension H_2/K_2 is unramified at all primes.*
(i) The primes above 5 are inert in J_1K_2/K_2 and split in K_1K_2/K_2.
(ii) The primes above 11 are split in J_1K_2/K_2 and inert in K_1K_2/K_2.

Proof. Only primes above 11 ramify in J_1/k and K_1/k. By considering ratios of Kummer generators we see that the extensions J_1K_2/K_2 and K_1K_2/K_2 are unramified. Hence the composite H_2/K_2 is unramified.
(i) The extensions J_1K_2/K_2 and K_1K_2/K_2 are translates of $\mathbf{Q}(\mu_{11})^+/\mathbf{Q}$ and K_1/k. Since 5 is totally ramified in $K_2/\mathbf{Q}$ our claims follow.
(ii) The Kummer generator for J_1K_2/K_2 belongs to $S(A_0 \to A_2/K_2)$. By Proposition 2.1 the primes above 11 split in J_1K_2/K_2. By Lemma 6.1 the primes above 11 cannot split completely in H_2/K_2. They are therefore inert in K_1K_2/K_2. $\square$

Proposition 7.2 *The 5-class group of K_2 is $\mathfrak{Cl}_{K_2}(5) \simeq (\mathbf{Z}/5\mathbf{Z})^2$. It is generated by the primes above 5 and 11.*

Proof. Let $B = \mathfrak{Cl}_{K_2}(5)$. By Lemma 3.5(ii) we know that H_2 is the maximal unramified 5-extension of K_2 which is abelian over k. Thus

$$B/(\tau - 1)B \simeq \mathrm{Gal}(H_2/K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^2$$

as abelian groups. By Lemma 7.1, the primes $\mathfrak{P}_1$ and $\mathfrak{L}$ generate $B/(\tau-1)B$. Since $(\tau - 1)^5 \subset 5\mathbf{Z}_5[\tau]$ it follows that $\mathfrak{P}_1$ and $\mathfrak{L}$ generate B as a $\mathbf{Z}_5[\tau]$-module. But $\tau(\mathfrak{P}_1) = \mathfrak{P}_1$, $\tau(\mathfrak{L}) = \mathfrak{L}$ and $\mathfrak{P}_1^5 = \mathfrak{p}_1$, $\mathfrak{L}^5 = \mathfrak{l}$ are principal. Thus $B \simeq (\mathbf{Z}/5\mathbf{Z})^2$ as claimed. $\square$

Remark 7.3 The action of τ on $\mathfrak{Cl}_{K_2}(5)$ is trivial. By Lemma 1.3 we have $\mathfrak{Cl}_{K_2}(5) \simeq \mathrm{Gal}(H_2/K_2) \simeq M(1) \oplus M(\omega^3)$. In particular $\mathfrak{P}_1 \sim \mathfrak{P}_2^2 \sim \mathfrak{P}_3^3 \sim \mathfrak{P}_4^4$.

We now give a description of the units in K_2. Substituting β^5 for λ in the identity $(\lambda - \phi^5)(\lambda - \overline{\phi^5}) = \lambda^2 - 11\lambda - 1$ we learn $\mathrm{Norm}_{K_2|\mathbf{Q}}(\beta - \phi) = 1$. Thus $\beta - \phi$ is a unit. We choose to work with the units

$$u_i = \frac{\phi\zeta^i\beta + 1}{\zeta^i\beta - \phi} \qquad v_i = (\zeta^i\beta)^2 - \zeta^i\beta - 1.$$

It is easy to check

$$\begin{array}{ll} \sigma(u_i) = -1/u_{2i} & \sigma(v_i) = v_{2i} \\ \tau(u_i) = u_{i+1} & \tau(v_i) = v_{i+1} \end{array}$$

and we have relations $\prod u_i = -\phi^{15}$, $\prod v_i = -1$. Thus the subgroups of K_2^*/K_2^{*5} generated by u_1, u_2, u_3, u_4 and v_1, v_2, v_3, v_4 are quotients of the G-modules $M(\omega^2, 4)$ and $M(1, 4)$.

Lemma 7.4 *The extension K_1K_2/K_2 has Kummer generator $\phi v_1 v_2^4 v_3^4 v_4$.*

Proof. By Lemma 7.1 and Proposition 7.2 it is sufficient to show that the stated element is (i) a 5th power locally at the prime $\mathfrak{L}$ above 5, and (ii) not a 5th power locally at the primes $\mathfrak{P}_i$ above 11. A suitable version of Hensel's lemma shows that $a \in \mathfrak{O}_{K_2}$ is a 5th power locally at $\mathfrak{L}$ if and only if $x^5 \equiv a \pmod{\mathfrak{L}^{26}}$ is soluble. We prove (i) by using `pari` to perform calculations in the group $(\mathfrak{O}_{K_2}/\mathfrak{L}^{26})^*$. Since $\phi v_1 v_2^4 v_3^4 v_4 \equiv \phi \pmod{\mathfrak{P}_i}$, claim (ii) is clear without computer calculation. This completes the proof of the lemma. Of course more brutal computer calculations are possible, showing

$$\phi^2 \pi_1 \pi_2^4 \pi_3^4 \pi_4 \equiv (\phi v_1 v_2^4 v_3^4 v_4)^{-1} \pmod{K_2^{*5}}.$$

$\square$

A consequence of Lemma 7.4 is that $K_2(\sqrt[5]{v_1 v_2^2 v_3^3 v_4^4})/K_2$ is unramified at all primes. Furthermore this extension is split at the primes above 5 and 11. By Proposition 7.2 we deduce

$$v_1 v_2^2 v_3^3 v_4^4 = w^5$$

for some $w \in K_2$. Multiplying w by a 5th root of unity if necessary

$$\begin{array}{ll} \sigma(w) \equiv w^3 & \mathrm{mod}\ \langle v_1, v_2, v_3, v_4 \rangle \\ \tau(w) \equiv w v_0 & \pmod{K_2^{*5}}. \end{array}$$

Proposition 7.5 *The units* $\zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, w$ *generate a subgroup of* $\mathfrak{O}_{K_2}^*$ *of index prime to 5.*

Proof. By Dirichlet it suffices to check that the elements listed are independent in K_2^*/K_2^{*5}. There is a G-module homomorphism

$$M := M(\omega) \oplus M(\omega^2) \oplus M(\omega^2, 4) \oplus M(\omega^3, 4) \to K_2^*/K_2^{*5}$$

where the summands correspond to ζ, ϕ, $\langle u_1, u_2, u_3, u_4 \rangle$ and $\langle v_1, v_2, v_3, w \rangle$. We suppose for a contradiction that this map has non-trivial kernel. Then this kernel meets

$$\begin{aligned} \ker(\tau - 1|M) &= M(\omega) \oplus M(\omega^2) \oplus M(\omega) \oplus M(\omega^2) \\ &= \langle\, \zeta, \phi, u_1 u_2^2 u_3^3 u_4^4, v_1 v_2^4 v_3^4 v_4 \,\rangle. \end{aligned}$$

Dividing into σ-eigenspaces we learn that one of the elements

$$\zeta^i (u_1 u_2^2 u_3^3 u_4^4)^j, \quad \phi^i (v_1 v_2^4 v_3^4 v_4)^j$$

is a 5th power. By Lemmas 3.6 and 7.4 these elements are Kummer generators for $J_1 J_2 K_2/K_2$ and for $K_1 K_2(\sqrt[5]{\phi})/K_2$. This gives the required contradiction. $\square$

Remark 7.6 According to `pari` the field K_2 has class number 25, whereas ϕ, $\beta - \phi$ and its conjugates, generate a subgroup of index 5 in $\mathfrak{O}_{K_2}^*/(\text{torsion})$. Again this is conditional on the Generalised Riemann Hypothesis.

We apply Propositions 2.1 and 2.2 in the case $F = K_2$.

Proposition 7.7 *The Selmer groups attached to the 5-isogenies (1) are*

$$\begin{array}{ll} S(A_0 \to A_1/K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^8 & S(A_2 \to A_0/K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^{15} \\ S(A_1 \to A_0/K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^2 & S(A_0 \to A_2/K_2) \simeq \mathbf{Z}/5\mathbf{Z}. \end{array}$$

Proof. By Propositions 7.2 and 7.5 the space

$$\{\, \theta \in K_2^*/K_2^{*5} \mid \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 5 \ \text{for all } \mathfrak{p} \,\} \tag{25}$$

has basis $\zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, w, \pi_1, 1 - \zeta$. Here π_1 and $1 - \zeta$ are contributions from the class group or "virtual units". We choose characters

$(\mathfrak{O}_{K_2}/\mathfrak{P}_i)^* \to \mathbf{Z}/5\mathbf{Z}$ and compute these characters on a basis for (25)

	$\mathfrak{P}_1$	$\mathfrak{P}_2$	$\mathfrak{P}_3$	$\mathfrak{P}_4$
ζ	1	3	2	4
ϕ	2	3	3	2
u_i	3	2	2	3
v_i	0	0	0	0
w	2	4	1	3
$\pi_1\pi_2^2\pi_3^3\pi_4^4$	3	1	4	2
$2\phi - 1$	2	2	2	2

By Proposition 2.1 we deduce

$$S(A_0 \to A_1/K_2) \simeq \langle u_1', u_2', u_3', u_4', v_1, v_2, v_3, w' \rangle \subset K_2^*/K_2^{*5}$$

where $u_i' = u_i\phi$ and $w' = w\pi_1\pi_2^2\pi_3^3\pi_4^4$. Propositions 2.1 and 7.2 give $S(A_0 \to A_2/K_2) \simeq \mathbf{Z}/5\mathbf{Z}$. The remaining statements follow by Proposition 2.2. $\square$

Proposition 7.7 furnishes the estimate $\operatorname{rank} A(K_2) \leq 8$. We improve on this by computing the Cassels-Tate pairing on $S(A_0 \to A_1/K_2)$. As a G-module we have

$$S(A_0 \to A_1/K_2) \simeq M(\omega^2, 4) \oplus M(\omega^3, 4). \tag{26}$$

By [Ca1, §7 (5)] there is a commutative diagram

$$\begin{array}{ccccccc} \langle \cdot, \cdot \rangle_{K_2} & : & S(A_0 \to A_1/K_2) & \times & S(A_0 \to A_1/K_2) & \to & \mathbf{Q}/\mathbf{Z} \\ & & \uparrow \mathit{cores} & & \downarrow \mathit{res} & & \| \\ \langle \cdot, \cdot \rangle_{K_1K_2} & : & S(A_0 \to A_1/K_1K_2) & \times & S(A_0 \to A_1/K_1K_2) & \to & \mathbf{Q}/\mathbf{Z} \end{array}$$

where *res* and *cores* are the maps $K_2^*/K_2^{*5} \rightleftarrows (K_1K_2)^*/(K_1K_2)^{*5}$ induced by the natural inclusion and norm map respectively. We compute $\langle c, d \rangle_{K_2}$ where

$$c = \beta^4 + 3\beta^3 + 4\beta^2 + 2\beta + 1, \qquad d = \beta^2 - \beta - 1.$$

A computer search yields a unit $\gamma \in K_1K_2$ with $\operatorname{Norm}_{K_1K_2|K_2}(\gamma) = c^2$. An explicit expression for 55γ in terms of $u = \varepsilon(\alpha)$ and β is

$$\begin{aligned} &(271858\beta^4 - 724855\beta^3 + 1158870\beta^2 - 663207\beta - 928521)u^4 \\ &\quad +(942679\beta^4 - 1424893\beta^3 + 1970490\beta^2 - 2288047\beta - 1777424)u^3 \\ &\quad +(2185832\beta^4 - 3700207\beta^3 + 8323117\beta^2 - 6646061\beta - 10380876)u^2 \\ &\quad +(-25520\beta^4 + 52792\beta^3 - 893918\beta^2 + 423925\beta + 1617231)u \\ &\quad +(1351406\beta^4 - 2180822\beta^3 + 4850841\beta^2 - 4066025\beta - 6097410) \end{aligned}$$

By Lemma 7.1, the primes above 11 are inert in K_1K_2/K_2. Any non-trivial character $\mathbf{F}_{11^5}^* \to \mathbf{Z}/5\mathbf{Z}$ factors via the norm map $\mathbf{F}_{11^5}^* \to \mathbf{F}_{11}^*$. So by Proposition 2.1, γ belongs to $S(A_0 \to A_1/K_1K_2)$. The prime 5 factors as

$$\begin{array}{rcll} (5) & = & \mathfrak{L}_0^4\mathfrak{L}_1^4\mathfrak{L}_2^4\mathfrak{L}_3^4\mathfrak{L}_4^4 & \text{in } K_1 \\ (5) & = & \mathfrak{L}^{20} & \text{in } K_2 \\ (5) & = & \mathbf{L}_0^{20}\mathbf{L}_1^{20}\mathbf{L}_2^{20}\mathbf{L}_3^{20}\mathbf{L}_4^{20} & \text{in } K_1K_2 \end{array}$$

with $\mathbf{L}_i|\mathfrak{L}_i$. Proposition 4.5 and the above diagram give

$$\begin{array}{rcl} \langle c^2, d\rangle_{K_2} & = & \langle \gamma, d\rangle_{K_1K_2} \\ & = & \sum_{i=0}^4 \operatorname{Ind}_\zeta(\gamma, d)^i_{\mathbf{L}_i} \\ & = & \sum_{i=0}^4 \operatorname{Ind}_\zeta(\gamma_i, d)^i_{\mathfrak{L}} \end{array}$$

where $\gamma_i \in K_2$ is chosen $\mathbf{L}_i$-adically close to γ. To do this we use (18) and the binomial theorem to choose $\alpha_i \in k$ $\mathfrak{L}_i$-adically close to α. Then we substitute $\varepsilon(\alpha_i)$ for $u = \varepsilon(\alpha)$ in our expression for γ.

We compute the Hilbert norm residue symbol $(\cdot,\cdot)_{\mathfrak{L}}$ using the product formula and Euler's criterion. Finally a computer calculation shows

$$\langle c, d\rangle_{K_2} \neq 0.$$

This calculation, together with Lemma 5.4, shows that the Cassels-Tate pairing on (26) is non-degenerate. By Proposition 4.1 it follows that $S(A_1 \stackrel{\times 5}{\to} A_1/K_2) \simeq \mathbf{Z}/5\mathbf{Z}$. Thus rank $A(K_2) = 0$ and $\text{Ш}(A_1/K_2)(5) = 0$.

From the exact sequences

$$A_0(K_2) \xrightarrow{\widehat{\psi}} A_1(K_2) \longrightarrow S(A_0 \to A_1/K_2) \longrightarrow \text{Ш}(A_0/K_2)[\widehat{\psi}] \longrightarrow 0$$

$$0 \longrightarrow \text{Ш}(A_0/K_2)[\widehat{\psi}] \longrightarrow \text{Ш}(A_0/K_2)(5) \xrightarrow{\widehat{\psi}} \text{Ш}(A_1/K_2)(5)$$

we learn $\text{Ш}(A_0/K_2)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^8$. Proposition 4.1 and the exact sequences

$$0 \longrightarrow S(A_0 \to A_2/K_2) \longrightarrow S(A_0 \stackrel{\times 5}{\to} A_0/K_2) \longrightarrow S(A_2 \to A_0/K_2)$$

$$0 \longrightarrow S(A_2 \to A_0/K_2) \longrightarrow S(A_2 \stackrel{\times 5}{\to} A_2/K_2) \longrightarrow S(A_0 \to A_2/K_2)$$

show that $S(A_2 \stackrel{\times 5}{\to} A_2/K_2) \simeq (\mathbf{Z}/5\mathbf{Z})^{16}$ and that the Cassels-Tate pairing on this Selmer group has rank 6. Since the multiplication by 25 map on A_2 factors through A_1 and $\text{Ш}(A_1/K_2)(5) = 0$, we deduce

$$\text{Ш}(A_2/K_2)(5) \simeq (\mathbf{Z}/5\mathbf{Z})^6 \oplus (\mathbf{Z}/25\mathbf{Z})^8.$$

This completes the proof of Theorem 2.

References

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, `pari/gp`, a computer algebra package, `http://www.parigp-home.de`

[B] C.D. Beaver, 5-Torsion in the Shafarevich-Tate group of a family of elliptic curves, *Journal of Number Theory* **82** (2000) 25-46

[Ca1] J.W.S. Cassels, Arithmetic on curves of genus 1, I. On a conjecture of Selmer, *J. Reine Angew. Math.* **202** (1959) 52-99

[Ca2] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962) 95-112

[Ca3] J.W.S. Cassels, Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965) 180-199

[CF] J.W.S. Cassels and A. Frohlich, editors, *Algebraic Number Theory*, Academic Press (1967)

[Co] J. Coates, Fragments of GL_2 Iwasawa theory of elliptic curves without complex multiplication, in *Arithmetic theory of elliptic curves*, Cetraro 1997, Lect. Notes in Math. **1716** Springer (1999)

[CH] J. Coates and S. Howson, Euler characteristics and elliptic curves II, *J. Math Soc. Japan* **53** (2001) 175-235

[CS] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TIFR Lect. on Math. **88** Narosa (2000)

[Coh] H. Cohen, *Advanced topics in computational number theory*, GTM **193** Springer (2000)

[Cr] J.E. Cremona, *Algorithms for modular elliptic curves (second edition)*, Cambridge (1997)

[F0] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, Cambridge PhD Thesis (2000)

[F1] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over **Q**, *J. Eur. Math. Soc.*, published online 15th February 2001

[F2] T.A. Fisher, *Rational points on $X(11)$ over $\mathbf{Q}(\mu_{11})$ via Galois equivariance of the Cassels-Tate pairing*, preprint

[G] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves*, Cetraro 1997, Lect. Notes in Math. **1716** Springer (1999)

[LT] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lect. Notes in Math. **504** Springer (1976)

[Ma] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972) 183-266

[Mc] W.G. McCallum, On the Tate-Shafarevich group of the jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988) 637-666

[Mi] J.S. Milne, *Arithmetic duality theorems*, Persp. in Math. **1** Academic Press (1986)

[Se1] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin (1968)

[Se2] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259-331

[Si] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106** Springer (1986)

[V1] J. Vélu, Courbes elliptiques sur $\mathbf{Q}$ ayant bonne réduction en dehors de $\{11\}$, *C. R. Acad. Sc. Paris* **273** (1971) 73-75

[V2] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris* **273** (1971) 238-241

[W] L.C. Washington, *Introduction to cyclotomic fields (second edition)*, GTM **83** Springer (1997)