Canad. J. Math. Vol. **53** (3), 2001 pp. 449–469

Descending Rational Points on Elliptic Curves to Smaller Fields

Amir Akbary and V. Kumar Murty

Abstract. In this paper, we study the Mordell-Weil group of an elliptic curve as a Galois module. We consider an elliptic curve E defined over a number field K whose Mordell-Weil rank over a Galois extension F is 1, 2 or 3. We show that E acquires a point (points) of infinite order over a field whose Galois group is one of $C_n \times C_m$ ($n = 1, 2, 3, 4, 6$, $m = 1, 2$), $D_n \times C_m$ ($n = 2, 3, 4, 6$, $m = 1, 2$), $A_4 \times C_m$ ($m = 1, 2$), $S_4 \times C_m$ ($m = 1, 2$). Next, we consider the case where E has complex multiplication by the ring of integers $\mathcal{O}$ of an imaginary quadratic field $\mathfrak{K}$ contained in K. Suppose that the $\mathcal{O}$-rank over a Galois extension F is 1 or 2. If $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ and $h_{\mathfrak{K}}$ (class number of $\mathfrak{K}$) is odd, we show that E acquires positive $\mathcal{O}$-rank over a cyclic extension of K or over a field whose Galois group is one of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, an extension of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$, or a central extension by the dihedral group. Finally, we discuss the relation of the above results to the vanishing of L-functions.

1 Introduction

Let E be an elliptic curve defined over a number field K. By the Mordell-Weil theorem, the group $E(K)$ of points of E with coordinates in K is finitely generated. We write $\operatorname{rank}\big(E(K)\big)$ for the rank of $E(K)$ modulo torsion. Let F be a finite Galois extension of K with group G. In this paper, we consider the Mordell-Weil group $E(F)$ as a $\mathbb{Z}[G]$-module. Since the torsion subgroup $E(F)_{\mathrm{tors}}$ has been extensively studied (see for example, Serre [21]), we shall restrict ourselves to the free part of $E(F)$. The question of studying this as a Galois module was raised in the works of Mazur [10], Mazur and Swinnerton-Dyer [11], Coates and Wiles [3] Rohrlich [17], and [18], to name a few.

Philosophically, it is of interest to note one basic difference between the free part and the torsion part as Galois modules. For example, consider the Galois module of ℓ-torsion points $E[\ell]$. The field $K(E[\ell])$ obtained by adjoining the coordinates of points in $E[\ell]$ has Galois group contained in $\mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell)$. Serre's theorem tells us that if E is without complex multiplication, then for large ℓ, it is in fact equal to $\mathrm{GL}_2(\mathbb{Z}/\ell)$. On the other hand, let $K\big(E(F)_{\mathrm{free}}\big)$ be the field generated by adjoining the coordinates of any free $\mathbb{Z}[\mathrm{Gal}(F/K)]$-submodule of $E(F) \otimes \mathbb{Q}$ to K and suppose that $\operatorname{rank}\big(E(F)\big) = r$, then $\mathrm{Gal}\Big(K\big(E(F)_{\mathrm{free}}\big)/K\Big)$ is conjugate to a subgroup of $\mathrm{GL}_r(\mathbb{Z})$. This imposes two restrictions on this Galois group. Firstly, by Jordan's theorem (see for example, [6], Theorem 14.12), a finite subgroup of $\mathrm{GL}_r(\mathbb{C})$ has a normal Abelian subgroup of index bounded by a function of r alone. Secondly, this is an integral

Received by the editors May 10, 2000; revised June 25, 2000.

The first author was partially supported by Concordia Research Funds. The second author was partially supported by a grant from NSERC.

AMS subject classification: Primary: 11G05, 11G40; secondary: 11R32, 11R33.

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

representation. By the work of Nori [15], there are many restrictions on the finite subgroups of $\mathrm{GL}_r(\mathbb{Z})$. Another restriction imposed on these Galois groups arises from the fact that the height pairing on the Mordell-Weil group is respected by the action of Galois.

In another direction, there is the connection with the L function of the elliptic curve. A well known theorem of Coates and Wiles [3] for CM elliptic curves asserts that if $E(K)$ is infinite, then the L-function $L(E/K, s)$ vanishes at $s = 1$. From the work of Kolyvagin [8], a similar result is known for (modular) elliptic curves over $\mathbb{Q}$. This is in accordance with the general conjecture of Birch and Swinnerton-Dyer. Here, we shall discuss the following:

Problem 1 Let F/K be a finite *Galois* extension. If $E(F)$ is infinite, does $L(E/F, s)$ vanish at $s = 1$?

Since the extensions of Coates-Wiles and Kolyvagin theorems to Abelian extensions are known (due respectively to Arthaud [1], and Rubin [19] in the CM-case and Kato (unpublished) in the modular case), we will show that the existence of an Abelian subextension M of F/K with $E(M)$ infinite implies a positive answer to Problem 1 (see Theorem 4). So we shall consider the following related problem.

Problem 2 Let F/K be a finite *Galois* extension. If $E(F)$ is infinite, then under what conditions can we produce an Abelian subextension M of K ($K \subseteq M \subseteq F$) such that $E(M)$ is infinite?

We wish to draw the analogy of this question with a result of Stark [23] for Artin L-functions. He shows that if F/K is Galois and the Dedekind zeta function $\zeta_F(s)$ has a *simple* zero at a point $s = s_0$, then there is a subextension $K \subseteq M \subseteq F$ with the property that $\zeta_M(s_0) = 0$ and M/K is Abelian (in fact, cyclic). Moreover, if N is any other subfield satisfying $\zeta_N(s_0) = 0$, we must have $M \subseteq N$.

In Section 4, we consider an elliptic curve E defined over K whose Mordell-Weil rank over a Galois extension F is 1 or 2. If the rank of $E(F)$ is one, we observe (Theorem 1, (i)) that a Stark type result holds here. If the rank of $E(F)$ is two, we show that E acquires two points of infinite order over a cyclic extension of K with Galois group C_n ($n = 1, 2, 3, 4, 6$) contained in F or over a dihedral extension with Galois group D_n ($n = 2, 3, 4, 6$). Then we establish a similar result in the rank three case (Theorem 1(iii)). In the case that E has complex multiplication, we can also study the Mordell-Weil group $E(F)$ as an $\mathcal{O}[G]$-module. Here E has complex multiplication by the ring of integers $\mathcal{O}$ of an imaginary quadratic field $\mathfrak{K}$ contained in K. We are able to establish the analogues of the above results in the case that $E(F)$ has $\mathcal{O}$-rank 1 or 2 (Theorems 2 and 3).

In the final section, by considering the order of vanishing of the L-function of E at a point $s = \omega$, we investigate some analytic analogues of our results in Section 4. In the case of a simple zero, we prove an analogue of Stark's theorem for a certain class of elliptic curves (Corollary 1). Also, by analogy with [14], we formulate a statement for higher order zeros but it would depend on the holomorphy of the L-functions obtained by twisting the L-function of E with certain Artin characters (see Proposition 6).

It is clear that much work remains to be done to elucidate the Galois module structure of the Mordell-Weil group. We hope that the explicit results of this paper may help in this effort.

Acknowledgement We would like to thank Henri Darmon and Hershy Kisilevsky for several helpful discussions. This paper was started during the CRM workshop at St. Adele in 1992, and completed while the second author was visiting the CRM during the special year on Arithmetic Algebraic Geometry in 1998–1999. He thanks the CRM for its hospitality.

2 The Minimal Subfield

Definition Let E be an elliptic curve defined over K and let F/K be an extension (not necessarily Galois) of number fields. Suppose that $\operatorname{rank}\bigl(E(F)\bigr) = r$, then the *minimal subfield* F_r is a subfield with $K \subseteq F_r \subseteq F$, such that

(i) $\operatorname{rank}\bigl(E(F_r)\bigr) = \operatorname{rank}\bigl(E(F)\bigr)$.
(ii) If $K \subseteq M \subseteq F$ and $\operatorname{rank}\bigl(E(M)\bigr) = \operatorname{rank}\bigl(E(F)\bigr)$, then $F_r \subseteq M$.

Proposition 1 *For any finite extension F/K and elliptic curve E defined over K with* $\operatorname{rank}\bigl(E(F)\bigr) = r$*, F_r exists and is unique. Also, if F/K is Galois then F_r/K is Galois.*

Proof We need only prove that if $K \subseteq M_1, M_2 \subseteq F$ are subfields such that

$$\operatorname{rank}\bigl(E(M_1)\bigr) = \operatorname{rank}\bigl(E(M_2)\bigr) = r$$

then

$$\operatorname{rank}\bigl(E(M_1 \cap M_2)\bigr) = r.$$

Indeed, $E(M_1) \otimes \mathbb{Q} = E(M_2) \otimes \mathbb{Q}$. Hence, there is a lattice L contained in $E(M_1) \cap E(M_2)$ which is of finite index in both $E(M_1)$ and $E(M_2)$. But then L is fixed by $\operatorname{Gal}(\tilde{F}/M_1)$ and by $\operatorname{Gal}(\tilde{F}/M_2)$ where $\tilde{F}$ is the normal closure of F/K. Thus, it is fixed by $\operatorname{Gal}\bigl(\tilde{F}/(M_1 \cap M_2)\bigr)$ and so it is contained in $E(M_1 \cap M_2)$. Thus the rank of $E(M_1 \cap M_2)$ is r as claimed.

If F/K is Galois, we can apply this argument to M and a conjugate of M, and from this, we see that the minimal subfield is necessarily Galois over K. ■

Now we give another description of the minimal subfield. Let F/K be a finite Galois extension, then since $\operatorname{Gal}(F/K)$ acts on $E(F) \otimes \mathbb{Q}$, we have a representation

$$\rho\colon \operatorname{Gal}(F/K) \to \operatorname{Aut}\bigl(E(F) \otimes \mathbb{Q}\bigr) \simeq \mathrm{GL}_r(\mathbb{Q})$$

where $\operatorname{rank}\bigl(E(F)\bigr) = r$. Then, there exists a free submodule of $E(F) \otimes \mathbb{Q}$ of rank r on which $\operatorname{Gal}(F/K)$ acts. For example, if $m = |E(F)_{\mathrm{tors}}|$, then we can take $mE(F)$. Each such submodule X (say) gives a representation

$$\rho_X\colon \operatorname{Gal}(F/K) \to \operatorname{Aut}(X) \simeq \mathrm{GL}_r(\mathbb{Z}).$$

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

Moreover, different choices of X yield representations isomorphic over $\mathbb{Q}$. In particular, $\operatorname{Ker}(\rho_X)$ is equal to $\operatorname{Ker}(\rho)$ and is independent of X. Thus, the field $K(X)$ obtained by adjoining the coordinates of points in X to K is independent of the choice of X. We denote this field by $K\big(E(F)_{\text{free}}\big)$.

Proposition 2 *Let F/K be a finite Galois extension. If $\operatorname{rank}\big(E(F)\big) = r \geq 1$, then*

(i) there is a subextension M, Galois over K such that $E(M) \otimes \mathbb{Q} = E(F) \otimes \mathbb{Q}$ and the representation

$$\rho_f \colon \operatorname{Gal}(M/K) \to \operatorname{Aut}\big(E(M) \otimes \mathbb{Q}\big)$$

is faithful. Moreover, $\operatorname{Im}(\rho_f)$ is conjugate to a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$.

(ii) $M = K\big(E(F)_{\text{free}}\big)$.

(iii) M is the minimal subfield defined in the beginning of the section.

Proof (i) Suppose that ρ is the representation of $\operatorname{Gal}(F/K)$ in $E(F) \otimes \mathbb{Q}$. Let M be the fixed field of $\ker \rho$. Since

$$(E(F) \otimes \mathbb{Q})^{\operatorname{Ker} \rho} = (E(F) \otimes \mathbb{Q})^{\operatorname{Gal}(F/M)} = E(M) \otimes \mathbb{Q}$$

(see [17], p. 126) and since M is the fixed field of $\ker \rho$, $\operatorname{Gal}(F/M)$ acts trivially on $E(F) \otimes \mathbb{Q}$. This shows that $E(F) \otimes \mathbb{Q} = E(M) \otimes \mathbb{Q}$ and ρ_f is faithful. The argument before the proposition shows that $\operatorname{Im}(\rho_f)$ is conjugate to a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$.

(ii) This is clear from the argument before the proposition.

(iii) Let $K \subseteq L \subseteq F$ and $\operatorname{rank}\big(E(L)\big) = \operatorname{rank}\big(E(F)\big)$, then from the proof of Proposition 1, we know that $\operatorname{rank}\big(E(L \cap M)\big) = \operatorname{rank}\big(E(M)\big)$ and $E(M) \otimes \mathbb{Q} = E(L \cap M) \otimes \mathbb{Q}$. This shows that $\operatorname{Gal}\big(M/(L \cap M)\big)$ acts trivially on $E(M) \otimes \mathbb{Q}$ and therefore it is contained in the kernel of the representation ρ_f. But $\ker \rho_f = \{\mathrm{id}\}$, which implies that $\operatorname{Gal}\big(M/(L \cap M)\big) = \{\mathrm{id}\}$. Thus $L \cap M = M$ and therefore $M \subseteq L$. This proves that M is the minimal subfield. ■

Proposition 3 *Let F/K be a finite Galois extension, then the degree of the minimal subfield F_r over K is bounded as a function of r alone.*

Proof By Proposition 2, we can consider $\operatorname{Gal}(F_r/K)$ as a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$ (and therefore $\mathrm{GL}_r(\mathbb{C})$). By Jordan's theorem a finite subgroup of $\mathrm{GL}_r(\mathbb{C})$ has a normal Abelian subgroup G_1 whose index is bounded by a function of r alone. So it is enough to prove that the order of G_1 is bounded by a function of r alone.

Now, let L be the fixed field of G_1 in F_r/K, and let ρ_1 be the restriction of the representation ρ_f (defined in Proposition 2) to $G_1 = \operatorname{Gal}(F_r/L)$. Then

$$\rho_1 = \psi_1 \oplus \psi_2 \oplus \cdots \oplus \psi_r$$

where ψ_i's are one dimensional characters of G_1. Since the values of the ψ_i satisfy a degree r polynomial over $\mathbb{Q}$, if ψ_i takes values in $\mathbb{Q}(\zeta_{m_i})$, we must have $\phi(m_i) \leq r$. Since ρ_1 is faithful, this implies that the order of G_1 is bounded by a function of r alone. ■

3 Group Theoretic Lemmas

In this section, we collect some group theoretic results which will be needed in the sequel.

Lemma 1 *Let the representation $\rho\colon G \to \mathrm{GL}_2(\mathbb{Z})$ be faithful, then*

(i) if ρ is reducible, G is cyclic C_n $(n = 1, 2, 3, 4, 6)$ or $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \simeq D_2$.
(ii) if ρ is irreducible, G is dihedral D_n $(n = 3, 4, 6)$.

Proof (i) Suppose that ρ is reducible. Let χ be the character of ρ. Then $\chi = \psi_1 + \psi_2$ over $\mathbb{C}$, where ψ_1 and ψ_2 are one dimensional characters of G. As the characteristic polynomial of ρ has coefficients in $\mathbb{Z}$, we must have $\psi_1 = \overline{\psi_2}$ or ψ_1 and ψ_2 characters of order 2. Since ρ is faithful, in the latter case, $G \simeq \mathbb{Z}/2$ or $G \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2 \simeq D_2$ and in the former case, G is cyclic.

Now if r is a generator of the cyclic group G and $\mathrm{ord}(r) = n$, then $\rho(r)$ is conjugate to a diagonal matrix over $\mathbb{C}$ like

$$\begin{pmatrix} e^{\frac{2\pi i h}{n}} & 0 \\ 0 & e^{-\frac{2\pi i h}{n}} \end{pmatrix}$$

where $0 \leq h < n$ and $(h, n) = 1$. Here, $e^{\frac{2\pi i h}{n}}$ is a primitive n-th root of unity which is also a root of a quadratic polynomial over $\mathbb{Z}$ (*i.e.* the characteristic polynomial of the above matrix). Therefore $\phi(n) = [\mathbb{Q}(e^{\frac{2\pi i h}{n}}) : \mathbb{Q}] \leq 2$ and so $n = 1, 2, 3, 4, 6$.

(ii) Since ρ is faithful, we can consider G as a finite subgroup of $\mathrm{GL}_2(\mathbb{R})$. We know that a finite subgroup of $\mathrm{GL}_2(\mathbb{R})$ is conjugate to a subgroup of $\mathrm{O}_2(\mathbb{R})$ and is therefore cyclic or dihedral (see [16], p. 22, Theorem 9). As ρ is irreducible, $G \simeq D_n = \langle r, s; r^n = 1, s^2 = 1, srs = r^{-1}\rangle$. Let $H = \langle r\rangle$, then $\chi|_H = \psi_1 + \psi_2$ over $\mathbb{C}$, where $\psi_1(r) = e^{\frac{2\pi i h}{n}}$ and $\psi_2(r) = e^{-\frac{2\pi i h}{n}}$ (see [20], p. 37), so by reasoning similar to part (i), $\mathrm{ord}(H) = n = 1, 2, 3, 4, 6$. Moreover, $n \neq 1, 2$ since in these cases D_n is Abelian. ∎

Let H_1 and H_2 be subgroups of a group G and let $x \in G$. Set

$$J(H_1, H_2, x) = H_2 \cup \{xg \mid g \in H_1, g \notin H_2\}.$$

Lemma 2 *Let H_1 and H_2 be subgroups of a group G such that $H_2 \subset H_1$ and $[H_1 : H_2] = 2$. Let $x \in G - H_2$ be an element of order 2 which commutes with all elements of H_1. Then*

(i) $J(H_1, H_2, x)$ is a subgroup of G.
(ii) $H_1 \simeq H_2 \times C_2$ if $x \in H_1$.
(iii) $H_1 \simeq J(H_1, H_2, x)$ if $x \notin H_1$.

Proof It is straightforward. ∎

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

Lemma 3 *Let the representation* $\rho\colon G \to \mathrm{GL}_3(\mathbb{Z})$ *be faithful, then* G *is isomorphic to one of the following:*

$$C_n \times C_m, \quad D_p \times C_m, \quad A_4 \times C_m, \quad S_4 \times C_m$$

where $n = 1, 2, 3, 4, 6$, $p = 2, 3, 4, 6$ *and* $m = 1, 2$.

Proof Since ρ is faithful we consider G as a finite subgroup of $\mathrm{O}_3(\mathbb{R})$. First suppose that $G \subset \mathrm{SO}_3(\mathbb{R})$. Then it is known that G is either cyclic, dihedral, A_4, S_4 or A_5 (see [16], p. 35, Theorem 11). Note that in this case if $A \in G$, then there is an orthonormal matrix P such that

$$P^{-1}AP = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(see [16], p. 35, Corollary 1), with $\mathrm{tr}(P^{-1}AP) \in \mathbb{Z}$. Therefore $2\cos\alpha \in \mathbb{Z}$. It is easily seen from here that if $G \subset \mathrm{SO}_3(\mathbb{R})$, the order of any element of G must be 2, 3, 4 or 6, and therefore G must be one of the following

$$(*) \qquad C_n (n = 1, 2, 3, 4, 6), \quad D_p (p = 2, 3, 4, 6), \quad A_4, \quad S_4.$$

Now suppose that $G \not\subset \mathrm{SO}_3(\mathbb{R})$. Let $G_s = G \cap \mathrm{SO}_3(\mathbb{R})$ and note that $-I$ (I is the identity matrix) is an element of order 2 in $\mathrm{O}_3(\mathbb{R})$ which is not in G_s and it commutes with all elements of G. Therefore, by Lemma 2, either $G \simeq G_s \times C_2$ or $G \simeq J(G, G_s, -I)$. G_s and $J(G, G_s, -I)$ are finite subgroups of $\mathrm{SO}_3(\mathbb{R})$ and therefore they are in the list given in $(*)$. This completes the proof. ■

Now let $\mathcal{O}$ denote the ring of integers of an imaginary quadratic field $\mathfrak{K}$. We fix an embedding $\mathfrak{K} \hookrightarrow \mathbb{C}$.

Notation We denote the center of a group G by $\mathrm{Cent}(G)$.

Lemma 4 *Let* G *be a group with a normal subgroup* H *of prime index. Let* $\rho\colon G \to \mathrm{GL}_2(\mathcal{O})$ *be a faithful and irreducible representation of* G*, and let* χ *be the character of* ρ*. Then*

(i) *either* $\chi = \mathrm{Ind}_H^G \psi$, $\psi(1) = 1$ *or* $\chi|_H$ *is irreducible. In the case that* $\chi = \mathrm{Ind}_H^G \psi$, $\psi(1) = 1$, *let us set* $N = \mathrm{Ker}\,\psi$.

(ii) *If* $N = \{\mathrm{id}\}$, *then* $H \simeq C_n$ $(n = 2, 3, 4, 6, 8, 12)$.

(iii) *If* $N \neq \{\mathrm{id}\}$ *and* $[G : H] = 2$ *then for all* $\sigma \in G - H$ *we have* $N \cap \sigma^{-1} N \sigma = \{\mathrm{id}\}$.

Proof (i) By Proposition 24 of [20] (p. 61), there exists a subgroup J of G, unequal to G and containing H such that either $\chi = \mathrm{Ind}_J^G \psi$, $\psi(1) = 1$ or $\chi|_J$ is isotypic. Since H has prime index in G then $J = H$.

If $\chi|_H$ is isotypic and reducible then $H \subset \mathrm{Cent}(G)$. But G/H is cyclic and therefore $G/\mathrm{Cent}(G)$ is also cyclic. This implies that G is Abelian which is a contradiction since G has a two dimensional irreducible representation. The only other possibility is that $\chi|_H$ is irreducible.

(ii) Since ψ is faithful, H is isomorphic to a finite subgroup of $\mathbb{C}^\times$ and therefore is cyclic. A characteristic polynomial argument similar to the one in Lemma 1 shows that the order n, say, of this group can only be 2, 3, 4, 5, 6, 8, 10 or 12 ($n \neq 1$, since G cannot be Abelian). Since H is cyclic, $\chi|_H = \psi + \psi'$.

Now if $n = 5$, ψ and ψ' take values in the group of 5-th roots of unity, and therefore $\chi|_H$ takes values in $\mathbb{Q}(\zeta_5) \cap \mathfrak{K} = \mathbb{Q}$. The characteristic polynomial of $\rho|_H$ has real coefficients and so either ψ and ψ' are both real or ψ' is the complex conjugate of ψ. Since ψ has order 5, the first case cannot occur. Hence, we are in the second case, and this implies that the character $\chi|_H$ takes values in $\mathbb{Q}(\zeta_5)^+$ which is not $\mathbb{Q}$ and this is a contradiction. Therefore, $n \neq 5$. In a similar way, we can show that $n \neq 10$.

(iii) If $N \neq \{\mathrm{id}\}$ then N cannot be normal in G. Indeed, if $N \lhd G$ then $N \subset \operatorname{Ker} \chi$ and this is not possible as ρ is faithful. Now $[G : H] = 2$ and therefore there exists exactly one conjugate of N, say $N' = \sigma^{-1} N \sigma$. Then $N \cap N' = \{\mathrm{id}\}$ because $N \cap N' \subset \operatorname{Ker} \chi$, $N \cap N' \lhd G$ and ρ is faithful. ∎

Remark 1 If $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, in part (ii) of Lemma 2, we can prove that n is not equal to 8 and 12. This is true since in these cases $\chi|_H$ takes values in $\mathbb{Q}(\zeta_8)^+$ or $\mathbb{Q}(\zeta_{12})^+$ which are not $\mathbb{Q}$.

Lemma 5 *Let $5 \nmid d_{\mathfrak{K}}$ (discriminant of $\mathfrak{K}$). Then, the order of any finite subgroup of* $\mathrm{GL}_2(\mathcal{O})$ *is not divisible by 5.*

Proof Let G be a finite subgroup of $\mathrm{GL}_2(\mathcal{O})$. By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes $q \equiv 2 \pmod 5$ such that q splits completely in $\mathcal{O}$. Let $q = \mathfrak{q}_1 \mathfrak{q}_2$ in $\mathcal{O}$. We choose q large enough such that the restriction of the reduction map

$$\mathrm{GL}_2(\mathcal{O}) \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{q}_1\mathcal{O})$$

to G is injective. But $\operatorname{Card}\big(\mathrm{GL}_2(\mathcal{O}/\mathfrak{q}_1\mathcal{O})\big) = \operatorname{Card}\big(\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})\big) = (q^2-1)(q^2-q) \equiv 1 \pmod 5$. This proves the lemma. ∎

Lemma 6 *Let G be a subgroup of* $\mathrm{GL}_2(\mathcal{O})$*, then either G is Abelian or* $\operatorname{Cent}(G) \simeq \{\mathrm{id}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$.

Proof We consider G as a subgroup of $\mathrm{GL}_2(\mathfrak{K})$. Let

$$C(G) = \{\alpha \in \mathrm{GL}_2(\mathfrak{K}) : \alpha\gamma = \gamma\alpha \text{ for all } \gamma \in G\}.$$

Then, G is either Abelian or

$$C(G) = \left\{ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} : c \in \mathfrak{K}^* \right\}$$

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

(see [22], p. 179, Problem 2.6(a)). Now the lemma follows from the facts that

$$\mathrm{Cent}(G) = C(G) \cap G$$

and $\mathcal{O}^* \simeq \{\mathrm{id}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$. ■

4 $E(F)$ of $\mathbb{Z}$-rank 1, 2, 3 or $\mathcal{O}$-rank 1 or 2

In this section, we assume that $E(F)$ is infinite of either $\mathbb{Z}$-rank ≤ 3 or $\mathcal{O}$-rank ≤ 2. We apply the results of the previous section to determine the minimal subfield in the case that $E(F)$ has $\mathbb{Z}$-rank 1, 2 or 3. We also consider the case that E has multiplication by the ring of integers $\mathcal{O}$ of an imaginary quadratic field $\mathfrak{K}$ and $E(F)$ has $\mathcal{O}$-rank 1 or 2. In the latter situation, we are able to determine the minimal subfield in all cases but one.

Theorem 1 *Let E be an elliptic curve defined over K and let F be a finite Galois extension of K. Let M be the minimal subfield.*

(i) *If* $\mathrm{rank}\big(E(F)\big) = 1$, *then M is a cyclic subextension of K and* $[M : K] = 1$ *or* 2.
(ii) *If* $\mathrm{rank}\big(E(F)\big) = 2$, *then M is either a cyclic subextension of K and* $[M : K] = 1, 2, 3, 4, 6$ *or a dihedral subextension of K and* $[M : K] = 4, 6, 8, 12$.
(iii) *If* $\mathrm{rank}\big(E(F)\big) = 3$, *then* $\mathrm{Gal}(M/K)$ *is one of the following:*

$$C_n \times C_m, \quad D_p \times C_m, \quad A_4 \times C_m, \quad S_4 \times C_m$$

where $n = 1, 2, 3, 4, 6$, $p = 2, 3, 4, 6$ *and* $m = 1, 2$.

Proof (i) M/K is the subextension given in Proposition 2. It is clear that since ρ_f is faithful, $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of $\mathrm{GL}_1(\mathbb{Z}) \simeq \mathbb{Z}^* = \{\pm 1\}$ which is cyclic and has order 1 or 2.

(ii), (iii) Let ρ_f be the faithful representation given in Proposition 2. Applying Lemmas 1 and 3 on ρ_f imply the results. ■

Now we show that in part (ii) of Theorem 1, M cannot be a dihedral extension of degree 12 of K, if we assume the Birch and Swinnerton-Dyer conjecture and some other assumptions.

Let M be a dihedral extension of $\mathbb{Q}$ and let C be the fixed field of the cyclic subgroup H of the dihedral Galois group in $M/\mathbb{Q}$. So $[C : \mathbb{Q}] = 2$ and $[M : C] = n$ (say) ($n \geq 3$). We have

$$L(E/M, s) = L(E/C, s) \prod_i L(E/\mathbb{Q} \otimes \mathrm{Ind}_H^G \psi_i, s)^2$$

where ψ_i are characters of $H = \mathrm{Gal}(M/C)$. Since G is dihedral, the twisted L-function $L(E/\mathbb{Q} \otimes \mathrm{Ind}_H^G \psi_i, s)$ has root number ± 1, depending on the parity of the order of vanishing of the twisted L-function at $s = 1$.

Now assume that the Birch and Swinnerton-Dyer conjecture is true. Then the assumption that $\mathrm{rank}\big(E(M)\big) = 2$, and the above factorization of L-functions implies that we have the following possibilities:

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

(i) $L(E/C,1)=0$.
(ii) exactly one of the factors $L(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i, s)$ has a simple zero at $s=1$.

In the first case, we must have $L(E/C,s)$ vanishing to order 2 at $s=1$ and none of the two-dimensional twists vanishes. In particular, all the root numbers must satisfy

$$w(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i)=1$$

for all i. In the second case, $L(E/C,1)\neq 0$ and there is a unique i such that $L(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i, 1)=0$. Since this zero is simple

$$w(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i)=-1.$$

Moreover, as none of the others vanish, all of the other root numbers are equal to +1.

Now it is clear that if M is the minimal subfield then (i) cannot be true and thus we are in the situation (ii).

Proposition 4 *Let E be a modular elliptic curve of conductor N defined over $\mathbb{Q}$ and suppose that the Birch and Swinnerton-Dyer conjecture is true. Also with the above notation assume that N and conductor of $\operatorname{Ind}_H^G \psi_i$'s are relatively prime and for all i, $\chi_i=\det(\operatorname{Ind}_H^G \psi_i)$ is even. Then, in part (ii) of Theorem 1 (for $K=\mathbb{Q}$) the minimal subfield M cannot be a dihedral extension of degree* 12.

Proof Let M be the minimal subfield in Theorem 1 and follow the notations before the proposition. By a result of Rohrlich (see [17], p. 125, Proposition 1), the root number can be calculated as follows. Let χ_i be the determinant of $\operatorname{Ind}_H^G \psi_i$. If χ_i is even, then

$$w(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i)=\chi_i(N).$$

Now, χ_i is a quadratic character which can be computed by the following formula:

$$\chi_i=\epsilon\psi_i\circ \mathrm{Ver}$$

where ϵ is the character of $C/\mathbb{Q}$ and Ver is the transfer map (Verlagerung) given by

$$\mathrm{Ver}(g)=\begin{cases} g^2 & \text{if } g\notin H\\ g\cdot \delta g\delta^{-1} & \text{if } g\in H.\end{cases}$$

Here, δ is a fixed element of $G-H$ of order 2. Now, $\psi(\delta g\delta^{-1})=\overline{\psi(g)}$ and so $\psi\circ\mathrm{Ver}$ is trivial on H. Moreover, $\mathrm{Ver}(\delta)=1$. Hence, $\psi_i\circ\mathrm{Ver}=1$ and $\chi_i=\epsilon$ is a quadratic character independent of ψ_i. Thus, the root numbers $w(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i)$'s are all equal. But from the argument before the proposition, we know that there is a unique i such that $w(E/\mathbb{Q}\otimes \operatorname{Ind}_H^G \psi_i)=-1$ and all of the others are +1. Now since the number of irreducible two dimensional characters of D_n is $\frac{n-1}{2}$ if n is odd and $\frac{n-2}{2}$ if n is even, we have $\epsilon(N)=-1$ and $n=3$ or 4. ■

Now let E be an elliptic curve defined over a number field K which has complex multiplication by $\mathcal{O}$, the ring of integers of an imaginary quadratic number field $\mathfrak{K}$

contained in K ($\mathfrak{K} \subseteq K$), and let F be a finite Galois extension of K. (We fix once and for all an embedding $\mathfrak{K} \hookrightarrow \mathbb{C}$.) Since E has complex multiplication by $\mathcal{O}$ and E is defined over K, we can fix an isomorphism between the ring of endomorphisms of E and $\mathcal{O}$ and equip $E(F)$ with an $\mathcal{O}$ action. (Note that all the endomorphisms of E are defined over K.)

We consider the submodule $mE(F)$ of the $\mathcal{O}$-module $E(F)$, where m is the order of the $\mathcal{O}$-torsion submodule of $E(F)$, then $mE(F)$ is a finitely generated torsion free module over $\mathcal{O}$ which is projective since $\mathcal{O}$ is a Dedekind domain. Moreover, there exist free $\mathcal{O}$-modules M_1 and M_2, such that

$$M_1 \subset mE(F) \subset M_2$$

and M_1 and M_2 have the same rank. We call this common rank, the $\mathcal{O}$-rank of $E(F)$. (For the above algebraic facts, see [9], p. 168, Problems 11 and 13.) Note that $2\,\mathrm{rank}_{\mathcal{O}}\big(E(F)\big) = \mathrm{rank}\big(E(F)\big)$.

Remark 2 If the field of complex multiplication $\mathfrak{K}$ is not contained in K, still we can consider $E(F)$ as an $\mathcal{O}$-module if we assume that $\mathfrak{K}K \subset F$. Also, we want to mention that the upcoming results in this section are also valid for elliptic curves with complex multiplication by a non-maximal order in $\mathfrak{K}$.

Now we can consider the $\mathfrak{K}$-module $mE(F) \otimes_{\mathcal{O}} \mathfrak{K} = E(F) \otimes_{\mathcal{O}} \mathfrak{K}$ as a representation space for $\mathrm{Gal}(F/K)$ to get the following representation:

$$\rho\colon \mathrm{Gal}(F/K) \to \mathrm{Aut}\big(E(F) \otimes_{\mathcal{O}} \mathfrak{K}\big) \simeq \mathrm{GL}_r(\mathfrak{K})$$

where $r = \mathrm{rank}_{\mathcal{O}}\big(E(F)\big)$. It is clear that we can define an $\mathcal{O}$-analogue of the minimal subfield and establish an $\mathcal{O}$-analogue of Propositions 1, 2 and 3. Note that in the $\mathcal{O}$-analogue of Proposition 2, we have to assume that r and $h_{\mathfrak{K}}$ (the class number of $\mathfrak{K}$) are relatively prime to make sure that $\mathrm{Im}(\rho_f)$ is conjugate to a finite subgroup of $GL_r(\mathcal{O})$. (For more explanation about this condition see [4], Theorem 23.17, p. 530.) Also note that if $\mathrm{rank}_{\mathcal{O}}\big(E(F)\big) = r$ then the $\mathcal{O}$-minimal subfield is the same as the minimal subfield F_{2r} defined in the beginning of Section 2.

Proposition 5 *If* $\mathrm{rank}_{\mathcal{O}}\big(E(F)\big) = 1$, *then the minimal subfield is a cyclic subextension M of K and* $[M : K] = 1, 2, 3, 4$ *or* 6.

Proof Since $(h_{\mathfrak{K}}, 1) = 1$, the argument before the proposition implies that $\mathrm{Im}(\rho_f)$ can be considered as a subgroup of $\mathrm{GL}_1(\mathcal{O})$. Now the proof is exactly the $\mathcal{O}$-analogue of part (i) of Theorem 1. Note that $\mathrm{GL}_1(\mathcal{O}) \simeq \mathcal{O}^*$ which is cyclic and has order 1, 2, 4 or 6. ■

If $\mathrm{rank}_{\mathcal{O}}\big(E(F)\big) = 2$ and $h_{\mathfrak{K}}$ is odd, then $\rho\big(\mathrm{Gal}(F/K)\big)$ is isomorphic to a finite subgroup of $\mathrm{GL}_2(\mathcal{O})$. We apply the group theoretic lemmas of the previous section to obtain some useful information about the representation ρ and the group $\mathrm{Gal}(F/K)$.

Theorem 2 *Suppose that $h_{\mathfrak{K}}$ is odd and $\operatorname{rank}_{\mathcal{O}}\big(E(F)\big) = 2$. Then there is a Galois subextension $K \subseteq S \subseteq F$ with $\operatorname{rank}_{\mathcal{O}}\big(E(S)\big) > 0$ such that $G = \operatorname{Gal}(S/K)$ is one of the following:*

(i) *G is cyclic of order $1, 2, 3, 4, 6, 8$, or 12.*
(ii) *$G/\operatorname{Cent}(G) \simeq D_n$. More precisely G satisfies one of the following:*
  (a) $G \simeq D_3$.
  (b) $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$ *and* $G/\operatorname{Cent}(G) \simeq D_n$ $(n = 2, 3, 4, 6, 8)$.
  (c) $\operatorname{Cent}(G) \simeq \mathbb{Z}/3\mathbb{Z}$ *and* $G/\operatorname{Cent}(G) \simeq D_n$ $(n = 2, 3, 4, 6)$.
  (d) $\operatorname{Cent}(G) \simeq \mathbb{Z}/4\mathbb{Z}$ *and* $G/\operatorname{Cent}(G) \simeq D_n$ $(n = 2, 3, 4)$.
  (e) $\operatorname{Cent}(G) \simeq \mathbb{Z}/6\mathbb{Z}$ *and* $G/\operatorname{Cent}(G) \simeq D_n$ $(n = 2, 3, 6)$.
(iii) $\operatorname{Cent}(G) \neq \{id\}$ *and* $G/\operatorname{Cent}(G) \simeq A_4$ *or* S_4.

In (ii) and (iii), $\operatorname{rank}_{\mathcal{O}}\big(E(S)\big) = 2$. *In fact, S is the minimal subfield in these cases.*

Proof Let $\rho\colon \operatorname{Gal}(F/K) \to GL_2(\mathcal{O})$ be the representation of $\operatorname{Gal}(F/K)$ in $E(F) \otimes_{\mathcal{O}} \mathfrak{K}$ and χ be its character. By the $\mathcal{O}$-analogue of Proposition 2, we can assume that ρ is faithful. Also we know that $G/\operatorname{Cent}(G)$ is isomorphic to a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ and therefore (see [21]) is isomorphic to C_n, D_n, A_4, S_4 or A_5. By Lemma 5, $G/\operatorname{Cent}(G)$ cannot be isomorphic to A_5. Note that since $h_{\mathfrak{K}}$ is odd, $\mathfrak{K} = \mathbb{Q}(\sqrt{-p})$ for prime p with $-p \equiv 1 \pmod 4$ or $\mathfrak{K} = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$, and therefore $5 \nmid d_{\mathfrak{K}}$.

If ρ is reducible, let χ be the character of ρ. We have $\chi = \psi_1 + \psi_2$ over $\mathbb{C}$, where ψ_1 and ψ_2 are one dimensional characters of G. Let S be the fixed field of $\operatorname{Ker}\psi_1$ in F/K. Then ψ_1 is a faithful and irreducible character of $\operatorname{Gal}(S/K)$, which implies that $\operatorname{Gal}(S/K)$ is cyclic and $\operatorname{rank}_{\mathcal{O}}\big(E(S)\big) \neq 0$. Indeed, (see [17], p. 126)

$$\big(E(F)\otimes_{\mathcal{O}}\mathbb{C}\big)^{\operatorname{Gal}(F/S)} = E(S)\otimes_{\mathcal{O}}\mathbb{C}.$$

Now a characteristic polynomial argument similar to the one in Lemma 1 implies that $[S : K] = 1, 2, 3, 4, 6, 8$ or 12.

Thus, we may suppose that ρ is irreducible. Then, since G is not Abelian, $G/\operatorname{Cent}(G)$ cannot be cyclic. Suppose that $G/\operatorname{Cent}(G)$ is isomorphic to A_4 or S_4. In this case, we must have $\operatorname{Cent}(G) \neq \{1\}$. Indeed, G is not isomorphic to A_4, since A_4 does not have any 2-dimensional irreducible representation. This also implies that if $G \simeq S_4$, and χ is the character of ρ then $\chi = \operatorname{Ind}_{A_4}^{S_4}\psi$, $\psi(1) = 1$ (see part (i) of Lemma 4). But it is known that any 1-dimensional representation of A_4 is trivial on the Klein 4-group V_4 (see [20], p. 42). Since $V_4 \lhd S_4$, we have

$$V_4 \subset \operatorname{Ker}(\operatorname{Ind}_{A_4}^{S_4}\psi) = \operatorname{Ker}\chi.$$

However, χ is the character of the faithful representation ρ. This is a contradiction. Therefore, G is not isomorphic to S_4.

It remains to analyze the possibility $G/\operatorname{Cent}(G) \simeq D_n$. Let A be the cyclic subgroup of order n in D_n. Let L be the fixed field of $\operatorname{Cent}(G)$ in F/K and M be the fixed

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

$[R:M]$	$[R\cap R^\sigma:M]$	$[F:M]$
2	1	4
3	1	9
4	1, 2	8, 16
6	1, 2, 3	12, 18, 36.

Table 1

field of A in L/K. If $H = \mathrm{Gal}(F/M)$ then $H/\mathrm{Cent}(G) \simeq A$ is cyclic and therefore H is Abelian. Clearly H has index 2 in G, thus by part (i) of Lemma 4, $\chi = \mathrm{Ind}_H^G \psi$, $\psi(1) = 1$. Let $N = \mathrm{Ker}\,\psi$.

By part (ii) of Lemma 4 if $N = \{\mathrm{id}\}$, then $H \simeq C_n$ $(n = 2, 3, 4, 6, 8, 12)$. By Lemma 6, $\mathrm{Cent}(G) \simeq \{\mathrm{id}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. As $\mathrm{Cent}(G) \subseteq H$, we have the following possibilities. If $\mathrm{Cent}(G) \simeq \{\mathrm{id}\}$ then $G \simeq D_n$. In this case n must be odd, since $\mathrm{Cent}(D_n) \neq \{\mathrm{id}\}$ for n even. This proves that $G \simeq D_3$. If $\mathrm{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$ then $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 1, 2, 3, 4, 6)$. But $n \neq 1$ since in that case G is Abelian. Similarly, if $\mathrm{Cent}(G) \simeq \mathbb{Z}/3\mathbb{Z}$ then $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 2, 4)$, if $\mathrm{Cent}(G) \simeq \mathbb{Z}/4\mathbb{Z}$ then $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 2, 3)$ and if $\mathrm{Cent}(G) \simeq \mathbb{Z}/6\mathbb{Z}$ then $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 2)$.

Now suppose that $N \neq \{\mathrm{id}\}$. First note that since $\chi = \mathrm{Ind}_H^G \psi$, $\psi(1) = 1$, then $\chi|_H = \psi + \psi^\sigma$ where $\sigma \in G - H$ and $\psi^\sigma(x) = \psi(\sigma^{-1} x \sigma)$ for $x \in H$ (See [20], Proposition 22, p. 58). This shows that $\mathrm{Ker}\,\psi^\sigma = \sigma^{-1} N \sigma \neq \{\mathrm{id}\}$. Let R be the fixed field of N in F/M, since F is the minimal subfield and $K \subset R \subsetneq F$, it is clear that $\mathrm{rank}_{\mathcal{O}}\big(E(R)\big) = 1$. In a similar way, we can show that $\mathrm{rank}_{\mathcal{O}}\big(E(R^\sigma)\big) = 1$ (R^σ is the fixed field of $\sigma^{-1} N \sigma$ in F/M).

Now since $\mathrm{rank}_{\mathcal{O}}\big(E(R)\big) = 1$, the action of $\mathrm{Gal}(R/M)$ on $E(R) \otimes_{\mathcal{O}} \mathfrak{K}$ is given by ψ. This shows that R is the minimal subfield and therefore it is cyclic of degree 1, 2, 3, 4, 6 (Proposition 5). A similar statement holds for R^σ.

By part (iii) of Lemma 4,

$$\mathrm{Ker}\,\psi \cap \mathrm{Ker}\,\psi^\sigma = N \cap \sigma^{-1} N \sigma = \{\mathrm{id}\}.$$

This implies that $F = RR^\sigma$. Hence,

$$|H| = [F:M] = \frac{[R:M][R^\sigma:M]}{[R\cap R^\sigma:M]} = \frac{[R:M]^2}{[R\cap R^\sigma:M]}.$$

An easy calculation implies that $[F:M] = 4, 8, 9, 12, 16, 18, 36$, which can be checked from Table 1.

Note that $[R:M] \neq 1$, since otherwise $R = R^\sigma = M$.

By Lemma 6, $\mathrm{Cent}(G) \simeq \{\mathrm{id}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. If $|\mathrm{Cent}(G)| = 1$ then $G \simeq D_n$, this implies that $N \triangleleft G$ and therefore $N \subset \mathrm{Ker}\,\chi$ which is a contradiction since $N \neq \{\mathrm{id}\}$ and χ is faithful. If $|\mathrm{Cent}(G)| = 4$ and $N \neq \{\mathrm{id}\}$, then the proof of Lemma 6 shows that $\mathfrak{K} = \mathbb{Q}(\sqrt{-1})$ and therefore $[R:M] = 2, 4$, thus $[F:M] = 8, 16$ and so $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 2, 4)$. If $|\mathrm{Cent}(G)| = 6$ and $N \neq \{\mathrm{id}\}$, then $[F:M] = 12, 18, 36$ and so $G/\mathrm{Cent}(G) \simeq D_n$ $(n = 4, 6, 12)$.

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

$[R : M_2]$	$[R \cap R^\sigma : M_2]$	$[M_2 : M]$	$[F : M]$
2	1	1, 3	4, 12
4	1, 2	1	8, 16.

Table 2

If $|\operatorname{Cent}(G)| = 2$, we can refine the above argument to show that $[F : M]$ cannot be 9, 18 or 36. Since $H = \operatorname{Gal}(F/M)$ contains $\operatorname{Cent}(G)$, the order of H is even and so $[F : M] \neq 9$. To show that $[F : M] \neq 18$ or 36, recall that $N \neq \{\mathrm{id}\}$ and $|\operatorname{Cent}(G)| = 2$. We first claim that N is a 2-group (in fact, it is a cyclic[1] 2-group). This is true, because as N and H are Abelian, they can be written as a direct sum of their Sylow subgroups

$$N = N_2 \oplus N_{\mathrm{odd}}, \quad H = H_2 \oplus H_{\mathrm{odd}}$$

where N_2 (respectively H_2) is the 2-primary part of N (respectively H). Since $H/\operatorname{Cent}(G)$ is cyclic and $|\operatorname{Cent}(G)| = 2$, it follows that H_{odd} is cyclic. Moreover, $H_{\mathrm{odd}} \lhd G$, and since $N_{\mathrm{odd}} \subset H_{\mathrm{odd}}$ and H_{odd} is cyclic, $N_{\mathrm{odd}} \lhd G$. This shows that for $\sigma \in G - H$

$$N_{\mathrm{odd}} \subset N \cap \sigma^{-1} N \sigma = \{\mathrm{id}\}$$

and therefore $N = N_2$.

Now let M_2 be the fixed field of H_2 in F/M. Since N is a subgroup of H_2, it is clear that R (the fixed field of N in F/M) is a Galois extension of M_2, and since R/M is cyclic with $[R : M] = 1, 2, 3, 4, 6$, R is a cyclic extension of M_2 and $[R : M_2] = 1, 2, 4$. A similar statement holds for R^σ/M_2. We have

$$|H| = [F : M_2][M_2 : M] = \frac{[R : M_2]^2}{[R \cap R^\sigma : M_2]}[M_2 : M].$$

Table 2 summarizes the possibilities for $[F : M]$ in this case.

So if $|\operatorname{Cent}(G)| = 2$ and $N \neq \{\mathrm{id}\}$, then $[F : M] = 4, 8, 12, 16$ and so $G/\operatorname{Cent}(G) \simeq D_n$ ($n = 2, 4, 6, 8$). Similarly, if $|\operatorname{Cent}(G)| = 3$ and $N \neq \{\mathrm{id}\}$, we can prove that $N = N_{\mathrm{odd}}$, and $[F : M] = 9, 18$ and so $G/\operatorname{Cent}(G) \simeq D_n$ ($n = 3, 6$).

Now it is easy to verify the list given in part (ii) of the statement of the theorem. This completes the proof. ∎

Remark 3 It might be of interest to note that a group G with cyclic center $\operatorname{Cent}(G)$ having the property that $G/\operatorname{Cent}(G) \simeq D_n$ is necessarily a product HK with H and K Abelian, with $H \cap K = \operatorname{Cent}(G)$. Moreover, if $\operatorname{Cent}(G)$ has order m, then H has order mn and K has order $2m$. In some cases, we can say more. For example, if $n = 3$ and $m = 2, 3, 4$, then $G \simeq \operatorname{Cent}(G) \times D_n$.

[1] Note that $N \cap \operatorname{Cent}(G) = \{\mathrm{id}\}$ and $N \simeq N/N \cap \operatorname{Cent}(G) \simeq N\operatorname{Cent}(G)/\operatorname{Cent}(G) \subset H/\operatorname{Cent}(G) \simeq A$, where A is the cyclic subgroup of order n in D_n.

Definition The *generalized quaternion group* Q_{4n} is defined with the following presentations:

$$Q_{4n} = \langle x, y : x^{2n} = 1, x^n = y^2, yxy^{-1} = x^{-1} \rangle.$$

Theorem 3 *Suppose that $h_{\mathfrak{K}}$ is odd and $\operatorname{rank}_{\mathcal{O}}\big(E(F)\big) = 2$ and $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$. Then there is a Galois subextension S with $K \subseteq S \subseteq F$ and $\operatorname{rank}_{\mathcal{O}}\big(E(S)\big) > 0$ such that $G = \operatorname{Gal}(S/K)$ is one of the following:*

(i) *G is cyclic of order $1, 2, 3, 4$ or 6.*
(ii) *G is isomorphic to D_n $(n = 3, 4, 6)$ or Q_{4n} $(n = 2, 3)$.*
(iii) *$G \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ or G is isomorphic to an extension of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$ with $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$. This can occur only if $d_{\mathfrak{K}} \not\equiv 1 \pmod 8$.*

In (ii) and (iii), $\operatorname{rank}_{\mathcal{O}}\big(E(S)\big) = 2$. In fact, S is the minimal subfield in these cases.

Proof First note that since $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ in part (ii) of Lemma 4, $n \neq 8, 12$ (see Remark 1). Applying this fact in the proof of Theorem 2 implies (i) if ρ (defined in the proof of Theorem 2) is reducible. In the case that ρ is irreducible and $G/\operatorname{Cent}(G) \simeq D_n$, from the assumptions of the theorem, we conclude that $G \simeq D_3$ or $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$ and $G/\operatorname{Cent}(G) \simeq D_n (n = 2, 3)$[2]. Now it is easy to verify the list given in part (ii) of the statement of the theorem, by referring to the list of non-Abelian groups of order 8 and 12 (see for example [5], Appendix B, p. 238).

So, we may suppose that ρ is irreducible and $G/\operatorname{Cent}(G)$ is isomorphic to either A_4 or S_4 and that $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$.

Let $G/\operatorname{Cent}(G) \simeq A_4$. Suppose that L is the fixed field of $\operatorname{Cent}(G)$ in F/K and M is the fixed field of V_4 (Klein's 4-group) in L/K. Set $H \simeq \operatorname{Gal}(F/M)$. Since $H/\operatorname{Cent}(G) \cong V_4$ and $V_4 \triangleleft A_4$, it follows that $H \triangleleft G$, also it is clear that $[G : H] = 3$. Suppose that $\chi|_H$ is reducible. Then, by part (i) of Lemma 4, $\chi = \operatorname{Ind}_H^G \psi$, $\psi(1) = 1$. This can never happen because $[G : H] = 3$ and χ is 2 dimensional.

Thus $\chi|_H$ is irreducible. Note that H is the 2-Sylow subgroup of G and it is of order 8. As it is necessarily non-Abelian, it is isomorphic to either D_4 or Q_8 (the quaternion group of order 8). In either case, G is the semidirect product of H and $\mathbb{Z}/3\mathbb{Z}$.

If $H \simeq Q_8$, then $G \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. This group has three 2-dimensional irreducible representations. For two of these, the character takes values in $\mathbb{Q}(\sqrt{-3})$ (see for example [13], p. 61) and hence we can exclude these. The remaining representation has character values in $\mathbb{Z}$. If the restriction of this representation to Q_8 is irreducible (as we are assuming), it is a representation of Schur index 2 (see [20], p. 94, Exercise 12.3) and it is realizable over $\mathfrak{K}$ if and only if $\mathfrak{K}$ can be embedded in the quaternion algebra $\mathbb{D}$ over $\mathbb{Q}$ which is ramified at 2 and ∞. But if $d_{\mathfrak{K}} \equiv 1 \pmod 8$, then $\mathfrak{K}$ cannot be embedded in $\mathbb{D}$ as the prime 2 splits in this field. Thus, if $d_{\mathfrak{K}} \equiv 1 \pmod 8$ this case cannot occur.

If $H \simeq D_4$, then let J be the cyclic subgroup of order 4. Let A be a 3-Sylow subgroup of G. It acts by conjugation on J (as J contains all elements of order 4 in

[2]Note that $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$, however, $n = 4, 6, 8$ never occur. This is true since $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and therefore in the proof of Theorem 2 if $N = \{\mathrm{id}\}$, then $H \simeq C_n (n = 2, 3, 4, 6)$ and if $N \neq \{\mathrm{id}\}$, then in Table 1, $[R : M] = 2$.

D_4). Moreover, it must act trivially as $\mathrm{Aut}(J)$ is cyclic of order 2. Hence, AJ is cyclic of order 12. Let P be the quadratic extension of K which is fixed by AJ. Restricting our representation ρ to AJ, we find it is reducible and given by two characters ψ_1 and ψ_2 (say). ψ_1 and ψ_2 take values in the group of 12-th roots of unity. The character of ρ on H thus takes values in $\mathbb{Q}(\zeta_{12}) \cap \mathfrak{K} = \mathbb{Q}$ (as $\mathfrak{K} \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$). In particular, it is real and so either ψ_1 and ψ_2 are both real or ψ_2 is the complex conjugate of ψ_1. Since $\rho|_H$ is faithful, the first case cannot occur as it would imply that H has order at most 4. Hence, we are in the second case, and this implies that ψ_1 is of order 12. But then, the character takes values in $\mathbb{Q}(\zeta_{12})^+$ which is not $\mathbb{Q}$ and this is a contradiction. Thus, this case also cannot occur.

Let $G/\mathrm{Cent}(G) \simeq S_4$. Again let L be the fixed field of $\mathrm{Cent}(G)$ in F/K, M be the fixed field of A_4 in L/K and $H = \mathrm{Gal}(F/M)$. Suppose first that $\chi|_H$ is reducible. Then by part (i) of Lemma 4, $\chi = \mathrm{Ind}_H^G \psi$, $\psi(1) = 1$. Let $N = \mathrm{Ker}\,\psi$. It is clear that $N \neq \{\mathrm{id}\}$, since otherwise by part (ii) of Lemma 4, H is cyclic which is impossible. Let R be the fixed field of N, then $\mathrm{rank}_{\mathcal{O}}\big(E(R)\big) > 0$. Since ρ is faithful, we must have $\mathrm{rank}_{\mathcal{O}}\big(E(R)\big) = 1$. This implies that R is the minimal subfield and therefore it is cyclic of order 1 or 2 (Proposition 5). Since $N \cap \sigma^{-1} N \sigma = \{\mathrm{id}\}$, we have $F = RR^{\sigma}$ and then by a calculation similar to one used in the proof of Theorem 2, we deduce $[F : M] = 4$ and hence $[F : K] = 8$, contradicting our assumption that $G/\mathrm{Cent}(G) \simeq S_4$.

Now consider the case $\chi_1 = \chi|_H$ is irreducible. We argue as in the A_4 case. Let us set H_1 to be the 2-Sylow subgroup of H. Note that it is a normal subgroup. Now, if we have $\chi_1|_{H_1}$ reducible, this would force ρ_1 to be the induction of a character from H_1 to H (by part (i) of Lemma 4) contradicting the fact that ρ_1 is a 2-dimensional representation. On the other hand, if $\chi_1|_{H_1}$ is irreducible, then H_1 is either the quaternion group of order 8 or the dihedral group of order 8 and both of these cases are dealt with as in the A_4 case using the fact that our representation has to be realizable over $\mathfrak{K}$. This shows that if $d_{\mathfrak{K}} \not\equiv 1 \pmod 8$, then $H \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and therefore G is an extension of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$. This completes the proof of the theorem. ■

5 Vanishing of L-Functions

5.1 Non-CM Case

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $L(E/\mathbb{Q}, s)$ be the L-function of E over $\mathbb{Q}$. Kolyvagin [8] proved that for a (modular) elliptic curve E if $\mathrm{rank}\big(E(\mathbb{Q})\big) \geq 1$ then $L(E/\mathbb{Q}, 1) = 0$ (see [7], p. 356, Theorem 20.5.2.(b)). This result is generalized to any finite Abelian extension of $\mathbb{Q}$ by Kato (unpublished).

Theorem 4 *Let E be a modular elliptic curve defined over $\mathbb{Q}$ and let F be a finite solvable extension of $\mathbb{Q}$. Suppose that $\mathrm{rank}\big(E(F)\big) \geq 1$.*

(i) If $E(F) \otimes \mathbb{Q}$ is an Abelian $\mathrm{Gal}(F/\mathbb{Q})$ module then $L(E/F, 1) = 0$.
(ii) If $\mathrm{rank}\big(E(F)\big) = 1$ then $L(E/F, 1) = 0$.
(iii) If $\mathrm{rank}\big(E(F)\big) = 2$ then either $L(E/F, 1) = 0$ or the minimal subfield is a dihedral extension of $\mathbb{Q}$ of degree 6, 8 or 12.

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

(iv) *If* $\operatorname{rank}\big(E(F)\big) = 3$ *then either* $L(E/F, 1) = 0$ *or* $\operatorname{Gal}(M/K)$ *(M is the minimal subfield) is one of the following:*

$$A_4, S_4, A_4 \times C_2, S_4 \times C_2.$$

Proof (i) Since $E(F) \otimes \mathbb{Q}$ is an Abelian Galois module, by Proposition 2, there is an Abelian subextension M of $\mathbb{Q}$ such that $\operatorname{rank}\big(E(M)\big) \geq 1$. Now Kato's generalization of Kolyvagin's theorem implies the vanishing of $L(E/M, s)$ at $s = 1$. By Theorem 2 of [12], $L(E/F, s)$ is divisible by $L(E/M, s)$. Hence, $L(E/F, s)$ also vanishes at $s = 1$. This completes the proof.

(ii) By part (i) of Theorem 1, $E(F) \otimes \mathbb{Q}$ is a cyclic Galois module, and the result follows from part (i).

(iii) It follows from part (ii) of Theorem 1 and (i).

(iv) Let $\rho_f\colon \operatorname{Gal}(M/K) \to \mathrm{GL}_3(\mathbb{Z})$ be the faithful representation given in Proposition 2. We prove that if ρ_f is reducible then $L(E/F, 1) = 0$. Let ρ_f be reducible, then since its degree is 3, ρ_f has a one dimensional representation ψ of $\operatorname{Gal}(M/K)$ as a direct summand. Let M_1 be the fixed field of $\ker\psi$ in M/K. It is clear that E has a point of infinite order on M_1 and M_1 is at most quadratic over $\mathbb{Q}$. As in (i), we conclude that $L(E/M_1) = 0$ which implies $L(E/F, 1) = 0$.

Now note that in part (iii) of Theorem 1, the only groups with a possible three dimensional irreducible representation, are those given in the statement of the theorem. This completes the proof. ■

Remark 4 If $M/\mathbb{Q}$ is a dihedral extension of degree $2n$ such that the fixed field C of the cyclic subgroup of order n of $\operatorname{Gal}(M/\mathbb{Q})$ is imaginary quadratic and of discriminant prime to the conductor of E, and $\big(E(M) \otimes \mathbb{C}\big)^{\chi} \neq 0$ is infinite (χ is a two dimensional character of $\operatorname{Gal}(M/\mathbb{Q})$), then by recent work of Bertolini and Darmon [2], $L(E/\mathbb{Q} \otimes \chi, 1) = 0$. Applying this with the factorization of the L-function of E over M (see the paragraph before Proposition 4) and part (ii) of Theorem 1, we deduce that if F is a finite solvable extension of $\mathbb{Q}$ such that any quadratic subfield is imaginary and of discriminant prime to the conductor of E, and $\operatorname{rank}\big(E(F)\big) = 2$ then $L(E/F, 1) = 0$.

5.2 CM **Case**

Let E be an elliptic curve defined over an imaginary quadratic field K and having complex multiplication by $\mathcal{O}$, the ring of integers of K. Let $L(E/K, s)$ be the L-function of E over K. It is known that $L(E/K, s)$ is the product of two Hecke L-series of K (see [22], p. 175, Theorem 10.5) and therefore it is defined on the whole complex plane. Coates and Wiles [3] proved that if $\operatorname{rank}\big(E(K)\big) \geq 1$ then $L(E/K, 1) = 0$. Arthaud [1] generalized this result to any finite Abelian extension of K. She proved that if F is a finite Abelian extension of K such that $\operatorname{rank}\big(E(F)\big) \geq 1$ then $L(E/F, 1) = 0$. The work of Rubin [19] established this under some conditions even if E is not defined over K.

Theorem 5 *Let E be an elliptic curve defined over an imaginary quadratic field K and*

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

having complex multiplication by $\mathcal{O}$, the ring of integers of K. Let F/K be a finite Galois extension and let $\operatorname{rank}_{\mathcal{O}}\big(E(F)\big) \geq 1$.

(i) *If $E(F) \otimes_{\mathcal{O}} K$ is an Abelian $K[G]$-module then $L(E/F, 1) = 0$.*
(ii) *If $\operatorname{rank}_{\mathcal{O}}\big(E(F)\big) = 1$ then $L(E/F, 1) = 0$.*
(iii) *If $\operatorname{rank}_{\mathcal{O}}\big(E(F)\big) = 2$ and $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then either $L(E/F, 1) = 0$ or the Galois group of the minimal subfield over K is isomorphic to one of the following:*

a) D_n $(n = 3, 4, 6)$, Q_{4n} $(n = 2, 3)$.

b) $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ *or an extension of* $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ *by* $\mathbb{Z}/2\mathbb{Z}$ *with* $\operatorname{Cent}(G) \simeq \mathbb{Z}/2\mathbb{Z}$. *This can occur only if $K \neq \mathbb{Q}(\sqrt{-7})$.*

Proof (i) By the $\mathcal{O}$-analogue of Proposition 2, there is an Abelian subextension M of K such that $\operatorname{rank}_{\mathcal{O}}\big(E(M)\big) \geq 1$. Now by Arthaud's theorem [1], $L(E/M, 1) = 0$. By Theorem 1 of [12], $L(E/F, s)$ is divisible by $L(E/M, s)$. Hence $L(E/F, 1) = 0$.

(ii) By Proposition 5, $E(F) \otimes_{\mathcal{O}} K$ is a cyclic $K[G]$-module, and the result follows from part (i).

(iii) It follows from Theorem 3 and (i). Note that since the j-invariant $j(E) \in K$ then $h_K = 1$, and $K = \mathbb{Q}(\sqrt{-7})$ is the only imaginary quadratic number field with $h_K = 1$ that for it $d_K \equiv 1 \pmod 8$. ■

6 Elliptic Analogue of Stark's Theorem

In this section, we investigate the analytic analogue of the minimal subfield. In this, we are guided by the results of Stark [23] about simple zeros of Dedekind zeta functions.

Definition Let E be an elliptic curve defined over K and let F be an extension of K. For each zero ω of $L(E/F, s)$, the *analytic minimal subfield* F_ω is a subfield over K with $K \subseteq F_\omega \subseteq F$ such that

(i) $\operatorname{ord}_{s=\omega} L(E/F_\omega, s) = \operatorname{ord}_{s=\omega} L(E/F, s)$.
(ii) If $K \subseteq M \subseteq F$ and $\operatorname{ord}_{s=\omega} L(E/M, s) = \operatorname{ord}_{s=\omega} L(E/F, s)$, then $F_\omega \subseteq M$.

Proposition 6 *Let F/K be a Galois extension with Galois group G, and suppose that $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$ for any irreducible character χ of G. Then the analytic minimal subfield F_ω exists and it is Galois over K.*

Proof We have the factorization

$$L(E/F, s) = \prod_{\chi \in \operatorname{Irr}(G)} L(E/K \otimes \chi, s)^{\chi(1)}$$

where $\operatorname{Irr}(G)$ is the set of irreducible characters of G. Consider the set

$$Z_\omega = \{\chi \mid L(E/K \otimes \chi, \omega) = 0\}.$$

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

Define

$$H_\omega = \bigcap_{\chi \in Z_\omega} \operatorname{Ker} \chi.$$

Then H_ω is a normal subgroup of G and we let F_ω denote its fixed field, which is Galois over K. Using the holomorphy of $L(E/K \otimes \chi, s)$, it is easy to see that $\operatorname{ord}_{s=\omega} L(E/F, s) = \operatorname{ord}_{s=\omega} L(E/F_\omega, s)$.

Now let M be any field between F and K. Put $H = \operatorname{Gal}(F/M)$ and let 1_H be the identity character of H. We have

$$\operatorname{Ind}_H^G 1_H = \sum_{\chi \in \operatorname{Irr}(G)} a_\chi \chi, \quad 0 \le a_\chi \le \chi(1),\ a_\chi \in \mathbb{Z}.$$

Thus,

$$L(E/M, s) = L(E/K \otimes \operatorname{Ind}_H^G 1_H, s) = \prod_{\chi \in \operatorname{Irr}(G)} L(E/K \otimes \chi, s)^{a_\chi}.$$

This shows that if $\operatorname{ord}_{s=\omega} L(E/M, s) = \operatorname{ord}_{s=\omega} L(E/F, s)$, then

$$\sum a_\chi n_\chi = \sum \chi(1) n_\chi$$

where n_χ denotes the order of $L(E/K \otimes \chi, s)$ at $s = \omega$. Hence, $a_\chi = \chi(1)$ for all $\chi \in Z_\omega$. We have

$$a_\chi = \langle \operatorname{Ind}_H^G 1_H, \chi \rangle_G = \langle 1_H, \chi|_H \rangle_H = \frac{1}{|H|} \sum_{g \in H} \chi(g).$$

Now if $a_\chi = \chi(1)$, then as $|\chi(g)| \le \chi(1)$, we must have $\chi(g) = \chi(1)$ for all $g \in H$ and therefore $H \subset \operatorname{Ker} \chi$ and this holds for all $\chi \in Z_\omega$. In other words $H \subset H_\omega$. This proves that $F_\omega \subseteq M$. ∎

Definition We say that E satisfies the Taniyama conjecture over a field K if the L-function $L(E/K, s)$ is the L-function $L(\pi, s)$ of an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_K)$, where $\mathbb{A}_K$ is the adèle ring of K.

Proposition 7 *Suppose that E satisfies the Taniyama conjecture over K. Let F be a solvable extension of K and let χ be a character of $G = \operatorname{Gal}(F/K)$. Then, $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$ if ω is a simple zero of $L(E/F, s)$.*

Proof Let H be a subgroup of G and let χ and ψ denote irreducible characters of G and H. Set

$$\theta_G = \sum_\chi n_\chi \chi, \quad \theta_H = \sum_\psi n_\psi \psi$$

where n_χ and n_ψ denote the orders of zeros of $L(E/K \otimes \chi, s)$ and $L(E/F^H \otimes \psi, s)$ at $s = \omega$ respectively (F^H is the fixed field of H in F/K). By Proposition 1 of [12]

$$(*) \qquad \theta_G|_H = \theta_H.$$

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

Suppose g is an element of G and let $H = \langle g \rangle$ be the cyclic group generated by g. Then, $L(E/F^H \otimes \psi, s)$ is analytic (see [12], p. 492, Proof of Theorem 2) and since

$$L(E/F, s) = \prod_{\psi} L(E/F^H \otimes \psi, s)^{\psi(1)}$$

and $\operatorname{ord}_{s=\omega} L(E/F, s) = 1$, then $\theta_H = \psi$ for some irreducible character ψ of H. From $(*)$, $\theta_G(g)$ is a root of unity and therefore

$$\begin{aligned}\sum_{\chi} {n_\chi}^2 &= \Big\langle \sum_{\chi} n_\chi \chi, \sum_{\chi} n_\chi \chi \Big\rangle \\ &= \frac{1}{|G|} \sum_{g \in G} |\theta_G(g)|^2 = 1.\end{aligned}$$

This shows that all n_χ's except one are 0. By taking $H = \langle 1 \rangle$, we have $\theta_G(1) = 1$ and thus the remaining n_χ is 1. This proves that $L(E/K \otimes \chi, s)$ is analytic at $s = \omega$. ■

Corollary 1 *Under the assumptions of the above proposition F_ω exists. Moreover, F_ω is a cyclic extension of K. If ω is real, $[F_\omega : K] \leq 2$.*

Proof By the previous proposition $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$, thus if $\operatorname{ord}_{s=\omega} L(E/F, s) = 1$ then there is a $\chi \in \operatorname{Irr}(G)$ such that $\operatorname{ord}_{s=\omega} L(E/K \otimes \chi, s) = 1$ and $\chi(1) = 1$. Now by Proposition 6, F_ω is the fixed field of $\operatorname{Ker} \chi$. Since χ is one dimensional F_ω is a cyclic extension of K. Moreover, if ω is real

$$\operatorname{ord}_{s=\omega} L(E/K \otimes \bar{\chi}, s) = \operatorname{ord}_{s=\omega} L(E/K \otimes \chi, s).$$

Hence, $\chi = \bar{\chi}$. ■

Remark 5 Let F be a Galois extension of K, then Corollary 1 is still true if E is an elliptic curve with complex multiplication. Note that in this case, we can remove the hypothesis that F/K is solvable, as E satisfies the Taniyama conjecture over any Galois extension of K (see [12], p. 488, Lemma 2).

Corollary 2 *Let E be an elliptic curve defined over a number field K. Suppose that E has complex multiplication by an order in an imaginary quadratic field contained in K. Let F be a Galois extension of K and let χ be a character of $G = \operatorname{Gal}(F/K)$. Then, $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$ if ω is a double zero of $L(E/F, s)$, and ω is real. Moreover, F_ω exists and F_ω is a cyclic extension of K.*

Proof We have the factorization

$$L(E/K, s) = L(\psi_K, s) L(\bar{\psi}_K, s)$$

where ψ_K is a Hecke character of K. Over F,

$$L(E/F, s) = L(\psi_F, s) L(\overline{\psi_F}, s)$$

https://doi.org/10.4153/CJM-2001-019-5 Published online by Cambridge University Press

where ψ_F denotes the restriction of ψ_K to $\mathrm{Gal}(\bar{F}/F)$. As ω is real, both factors on the right vanish at $s = \omega$. As $\mathrm{ord}_{s=\omega} L(E/F, s) = 2$, it follows that

$$\mathrm{ord}_{s=\omega} L(\psi_F, s) = \mathrm{ord}_{s=\omega} L(\overline{\psi_F}, s) = 1.$$

Now the argument of Proposition 7 implies that all $L(\psi_K \otimes \chi, s)$ are holomorphic at $s = \omega$ and that F_ω exists and is a cyclic extension of K. ■

Finally, we show that we can replace the assumption of holomorphy in the statement of Proposition 6, with a milder condition if we assume that E has complex multiplication and F is contained in a solvable extension of K (F/K is not necessarily Galois).

Proposition 8 *Suppose that F/K has solvable normal closure, and let E be an elliptic curve defined over K which has complex multiplication. Suppose that for any two subfields M_1 and M_2 with the property that*

$$\mathrm{ord}_{s=\omega} L(E/M_1, s) = \mathrm{ord}_{s=\omega} L(E/M_2, s) = \mathrm{ord}_{s=\omega} L(E/F, s)$$

the quotient

$$\frac{L(E/M_1M_2, s)L(E/M_1 \cap M_2, s)}{L(E/M_1, s)L(E/M_2, s)}$$

is holomorphic at $s = \omega$. Then the analytic minimal subfield F_ω exists.

Proof Let $\mathcal{S}$ be the set of subfields M of F with

$$\mathrm{ord}_{s=\omega} L(E/M, s) = \mathrm{ord}_{s=\omega} L(E/F, s).$$

We prove that $\mathcal{S}$ is closed under intersections and thus has a minimal element. Let M_1 and M_2 be in $\mathcal{S}$, then by the hypothesis

$$\frac{L(E/M_1M_2, s)L(E/M_1 \cap M_2, s)}{L(E/M_1, s)L(E/M_2, s)}$$

is holomorphic at ω. Moreover, by the main result of [12] (see Theorem 1), $L(E/M_1, s)$ divides $L(E/M_1M_2, s)$ and $L(E/M_1M_2, s)$ divides $L(E/F, s)$. Thus,

$$\mathrm{ord}_{s=\omega} L(E/M_1, s) \le \mathrm{ord}_{s=\omega} L(E/M_1M_2, s) \le \mathrm{ord}_{s=\omega} L(E/F, s)$$

and therefore we have equality throughout. Hence,

$$\mathrm{ord}_{s=\omega} L(E/M_1 \cap M_2, s) \ge \mathrm{ord}_{s=\omega} L(E/F, s).$$

The reverse inequality also holds (as $L(E/M_1 \cap M_2, s)$ divides $L(E/F, s)$). This proves that $\mathcal{S}$ has a minimal element F_ω. ■

Remark 6 Note that the assumption of holomorphy in the previous proposition is implied by the holomorphy of $L(E/K \otimes \chi, s)$ at $s = \omega$ (see [23], p. 151, Lemma 12).

Remark 7 Proposition 8 is also true, in the case that E satisfies the Taniyama conjecture over K and F is a solvable extension of K.

References

[1] N. Arthaud, *On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication, I*. Comp. Math. **37**(1978), 209–232.
[2] M. Bertolini and H. Darmon, *The p-adic Birch and Swinnerton-Dyer conjecture*. in preparation.
[3] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*. Invent. Math. **39**(1977), 223–251.
[4] C. W. Curtis and I. Reiner, *Methods of representation theory, Volume I*. Wiley Interscience, New York, 1981.
[5] J. F. Humphreys, *A course in group theory*. Oxford University Press, 1996.
[6] M. Isaacs, *Character Theory of Finite Groups*. Academic Press, New York, 1976.
[7] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. Second Edition, Springer-Verlag, 1990.
[8] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(\mathbb{Q})$ for a class of Weil curves*. Math. USSR-Izv. **32**(1989), 523–542.
[9] S. Lang, *Algebra*. Third Edition, Addison-Wesley, 1993.
[10] B. Mazur, *Rational points on Abelian varieties in towers of number fields*. Invent. Math. **18**(1972), 183–266.
[11] B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil curves*. Invent. Math. **25**(1974), 1–61.
[12] M. R. Murty and V. K. Murty, *Base change and the Birch-Swinnerton-Dyer conjecture*. Contemporary Math. **143**(1993), 481–494.
[13] V. K. Murty, *Holomorphy of Artin L-functions*. In: Proc. Ramanujan Centennial Intl. Conf. (ed. R. Balakrishnan et. al.), Ramanujan Math. Society, Madras, 1988, 55–66.
[14] ———, *Class numbers of* CM*-fields with solvable normal closure*. Compositio Math., to appear.
[15] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$. Invent. Math. **88**(1987), 257–275.
[16] E. Rees, *Notes on Geometry*. Springer-Verlag, 1983.
[17] D. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*. In: Automorphic forms and analytic number theory, (ed. R. Murty), CRM, Montréal, 1990, 123–133.
[18] ———, Galois theory, elliptic curves, and root numbers. Comp. Math. **100**(1996) 311–349.
[19] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*. Invent. Math. **64**(1981), 455–470.
[20] J.-P. Serre, *Linear Representations of Finite Groups*. Springer-Verlag, 1977.
[21] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.
[22] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
[23] H. Stark, Some effective cases of the Brauer-Siegel theorem. Invent. Math. **23**(1974), 135–152.

Current Address:
Department of Mathematics
and Computer Science
University of Lethbridge
4401 University Drive West
Lethbridge, Alberta
T1K 3M4
e-mail: akbary@cs.uleth.ca

Department of Mathematics and Statistics
Concordia University
1455 de Maisonneuve Blvd. West
Montréal, Quebec
H3G 1M8
e-mail: akbary@cicma.concordia.ca

Department of Mathematics
University of Toronto
100 St. George Street
Toronto, Ontario
M5S 3G3
e-mail: murty@math.toronto.edu