Canad. Math. Bull. 2024, pp. 1–17
http://dx.doi.org/10.4153/S0008439524000341
© The Author(s), 2024. Published by Cambridge University Press on behalf of Canadian Mathematical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Minimal subfields of elliptic curves

Samprit Ghosh

Abstract. For an elliptic curve E defined over a number field K and L/K a Galois extension, we study the possibilities of the Galois group $\mathrm{Gal}(L/K)$, when the Mordell–Weil rank of $E(L)$ increases from that of $E(K)$ by a small amount (namely 1, 2, and 3). In relation with the vanishing of corresponding L-functions at $s = 1$, we prove several elliptic analogues of classical theorems related to Artin's holomorphy conjecture. We then apply these to study the analytic minimal subfield, first introduced by Akbary and Murty, for the case when order of vanishing is 2. We also investigate how the order of vanishing changes as rank increases by 1 and vice versa, generalizing a theorem of Kolyvagin.

1 Introduction

Let E be an elliptic curve defined over a number field K, and let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. The famous Mordell–Weil Theorem tells us that, $E(L)$, the group of L-rational points of E, is finitely generated. Throughout this paper, we will focus on the "free part" of the Mordell–Weil group, that is, $E(L)$ modulo the torsion subgroup $E(L)_{\mathrm{tors}}$ and denote the rank of this quotient by $\mathbf{rk}E(L)$. The question of studying this free part of $E(L)$ as a $\mathbb{Z}[G]$-module is an appealing one and was raised in the works of Mazur and Swinnerton-Dyer [19], Coates and Wiles [4], and others. Toward this study, Akbary and Murty in [1] introduced the idea of a minimal subfield: $M \subseteq L$, minimal, such that $\mathbf{rk}E(M) = \mathbf{rk}E(L)$ and produced explicit examples. They gave a description of the possibilities for $\mathrm{Gal}(M/K)$ when the rank $E(L)$ is small (e.g., 1, 2, and 3). In the first part of this paper, we generalize their results from small rank to small increase in rank. We show that similar descriptions of $\mathrm{Gal}(M/K)$ holds when $\mathbf{rk}E(L) = \mathbf{rk}E(K) + t$ for $t = 1, 2$, and 3. We prove the following theorem.

Theorem 1.1 *Let L/K be a Galois extension of number fields, and let E/K be an elliptic curve such that $\mathbf{rk}E(L) = \mathbf{rk}E(K) + t$. Let M be the minimal subfield.*

(1) *If $t = 1$, then M is a quadratic extension of K.*
(2) *If $t = 2$, then M is either a cyclic extension of K with $[M : K] = 2, 3, 4, 6$ or a dihedral extension of K with $[M : K] = 4, 6, 8, 12$.*

Received by the editors April 12, 2023; revised May 4, 2024; accepted May 17, 2024.
Published online on Cambridge Core May 22, 2024.
AMS subject classification: **11G05**, **11G40**, **11M06**, 11R32, 11R33.
Keywords: Elliptic curves, Mordell–Weil rank, BSD, Artin's holomorphy conjecture, Heilbronn characters.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

(3) *If* $t = 3$, *then* $\mathrm{Gal}(M/K)$ *is isomorphic to one of the following:*
$C_n \times C_m$, *where* $n = 2, 3, 4$ *and* $m = 1, 2$,
$D_{2p} \times C_m$, *where* $p = 2, 3, 4, 6$ *and* $m = 1, 2$,
$A_4 \times C_m$, *or* $S_4 \times C_m$ *where* $m = 1, 2$.

Section 2 is largely devoted to proving the above theorem starting with a precise definition of the minimal subfield.

We then venture on a more analytic side of things. The famous Birch and Swinnerton-Dyer conjecture connects the rank of an elliptic curve to the order of vanishing of its L-function at $s = 1$. In this regard, Akbary and Murty introduced the analytic notion of the minimal subfield in [1]. Its existence is dependent on the holomorphy of $L(E/K \otimes \chi, s)$ for irreducible characters χ of the Galois group. For number fields, classical theorems of Foote–Murty and Foote–Wales, shows holomorphy of Artin L-functions when the Dedekind zeta function has a zero of small order. In Sections 4 and 5, we develop elliptic analogues of these theorems. For example, we show the following.

Theorem 1.2 *Let* E/K *be an elliptic curve and suppose that* E *satisfies the generalized Taniyama conjecture over* K. *Let* F *be a Galois extension of* K *with solvable Galois group* $G = \mathrm{Gal}(F/K)$. *Let* χ *be an irreducible character of* G. *Then* $L(E/K \otimes \chi, s)$ *is holomorphic at* $s = \omega$, *if* ω *is a zero of* $L(E/F, s)$ *of order* $r \leq p_2 - 2$, *where* p_2 *is the second smallest prime factor of* $|G|$.

We also prove that Theorem 1.2 holds for $r = 2$. These results establish existence of the analytic minimal subfield when the L-function of E over the top field has a zero of small order. Also note that these results are unconditional if we assume $K = \mathbb{Q}$ as modularity is known. In Section 6, similar to the algebraic case, we investigate the possibilities of the Galois group for the analytic minimal subfield, when the order of vanishing at $s = 1$ of $L(E/F, s)$ is 2. As an application, we show the following slight generalization of a theorem of Kolyvagin.

Theorem 1.3 *Let* $E/\mathbb{Q}$ *be an elliptic curve, and let* $K/\mathbb{Q}$ *be a solvable Galois extension.*

(i) *If* $\mathbf{rk}E(K) = \mathbf{rk}E(\mathbb{Q}) + 1$, *then* $ord_{s=1}\, L(E/K, s) \geq ord_{s=1}\, L(E/\mathbb{Q}, s) + 1$.
(ii) *If* $L(E/\mathbb{Q} \otimes \chi, s)$ *is holomorphic at* $s = 1$, *for every irreducible character* χ *of* $\mathrm{Gal}(K/\mathbb{Q})$ *and* $ord_{s=1}\, L(E/K, s) = ord_{s=1}\, L(E/\mathbb{Q}, s) + 1$, *then* $\mathbf{rk}E(K) \geq \mathbf{rk}E(\mathbb{Q}) + 1$.

In both cases, equality holds if the algebraic and the analytic minimal subfields are equal.

We also show that the holomorphy condition in Theorem 1.3(ii) can be dropped if E has CM.

1.1 Notation and terminology

We will be using a fair bit of group theory and representation theory of finite groups. In this subsection, we briefly introduce the notations and terminologies we have used.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Throughout the paper, C_n is the cyclic group of order n, D_{2n} is the dihedral group of order $2n$, Q_8 is the quaternion group of order 8, whereas, S_n and A_n are, respectively, the symmetric and the alternating group of n symbols. If V is a vector space, then by $\mathrm{GL}(V)$, we denote the group of automorphisms of V. By $\mathrm{GL}_n(K)$ (resp. $\mathrm{SL}_n(K)$), we denote the group of $n \times n$ invertible matrices (resp. matrices with determinant 1) with entries in K. When $K = \mathbb{F}_q$, a finite field with q elements, we have simply written it as $\mathrm{GL}_n(q)$ (resp. $\mathrm{SL}_n(q)$). We have used $\mathrm{PGL}_n(K)$ for the projective general linear group, defined as $\mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$. Note that, for any group G, by $Z(G)$, we denote the center of the group. We define $\widehat{\mathrm{SL}_2}(3)$ to be any nontrivial semidirect product of Q_8 by a cyclic 3-group.

For a finite group G, we denote the set of all irreducible characters of G by $\mathrm{Irr}(G)$. If H is a subgroup of G and χ is a character of G, then $\chi|_H$ denotes the restriction of χ to H. Whereas, if ψ is a character of H, by $\mathrm{Ind}_H^G\psi$, we denote the induced character defined as

$$\mathrm{Ind}_H^G\psi\ (g) = \frac{1}{|H|}\sum_{x\in G}\psi(x^{-1}gx), \quad \text{where we take } \psi(x) = 0 \text{ for all } x \notin H.$$

We denote the usual inner product on the space of complex class functions on G by $\langle \_, \_ \rangle$. It is given by

$$\langle \alpha, \beta \rangle = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\overline{\beta(g)}.$$

Frobenius reciprocity theorem tells us that for any χ and ψ as above, we have $\langle \mathrm{Ind}_H^G\psi, \chi \rangle = \langle \psi, \chi|_H \rangle_H$, where $\langle \_, \_ \rangle_H$ is the usual inner product on the space of complex class functions on the subgroup H. We denote the regular character of G by "reg." Note that

$$\mathrm{reg} = \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\chi.$$

In general, by a *virtual character* of G, we mean a class function $\sum_{\chi\in\mathrm{Irr}(G)} a_\chi\chi$, where $a_\chi \in \mathbb{Z}$. In particular, a_χ can be negative.

We have written E/K to denote an elliptic curve E defined over the field K. We denote the L-series of E over K by $L(E/K, s)$. If F/K is a Galois extension and χ is a character of $\mathrm{Gal}(F/K)$, then the twisted L-series of E over K by χ is denoted by $L(E/K \otimes \chi, s)$, whereas, $L(s, \chi)$ has been used to denote the Artin L-function corresponding to χ of $\mathrm{Gal}(F/K)$.

2 Algebraic minimal subfield

Definition 2.1 Let E/K be an elliptic curve, and let L/K be a finite extension (not necessarily Galois) of number fields. Suppose that $\mathbf{rk}E(L) = r$. The algebraic minimal subfield M is a subfield with $K \subseteq M \subseteq L$ satisfying:

(i) $\mathbf{rk}E(M) = r$, and
(ii) if $K \subseteq F \subseteq L$ with $\mathbf{rk}E(F) = r$, then $M \subseteq F$.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Akbary and Murty showed that for any finite extension L/K and elliptic curve E/K, the minimal subfield M exists and is unique. Also, if L/K is Galois, then M/K is Galois (see [1, Proposition 1]). For any finite Galois extension L/K, the Galois group $\mathrm{Gal}(L/K)$ acts on $E(L) \otimes \mathbb{Q}$ giving us a representation (writing $r = \mathbf{rk}E(L)$)

$$\rho_L : \mathrm{Gal}(L/K) \to \mathrm{GL}(E(L) \otimes \mathbb{Q}) \cong \mathrm{GL}_r(\mathbb{Q}). \tag{2.1}$$

Proposition 2.1 *Let L/K be a finite Galois extension with $\mathbf{rk}E(L) = r$, and let M be the minimal subfield. Then*

$$\rho : \mathrm{Gal}(M/K) \to \mathrm{GL}(E(M) \otimes \mathbb{Q})$$

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

For a detailed proof, see [1, Proposition 2]. But the essential idea is that M is constructed as the fixed field of $\ker \rho_L$.

2.1 Working with the quotient space

We will write $V_F = E(F) \otimes \mathbb{Q}$ for any number field F. We will work with the quotient space V_L/V_K instead of V_L and use elementary linear algebra to prove a similar version of the above proposition. Note that dimension of this quotient space is precisely the increase in rank, i.e.,

$$\dim V_L/V_K \;=\; \mathbf{rk}E(L) - \mathbf{rk}E(K).$$

We can then consider the quotient representation coming from the Galois action. For the algebraic minimal subfield, this representation also turns out to be faithful.

Proposition 2.2 *Let L/K be a finite Galois extension with $\mathbf{rk}E(L) = r$, and let M be the algebraic minimal subfield. If $\mathbf{rk}E(L) - \mathbf{rk}E(K) = t$, then there exists a faithful representation*

$$\tilde{\rho} : \mathrm{Gal}(M/K) \to \mathrm{GL}(V_M/V_K) \cong \mathrm{GL}_t(\mathbb{Q}).$$

Moreover, $Im(\tilde{\rho})$ is conjugate to a finite subgroup of $\mathrm{GL}_t(\mathbb{Z})$.

Proof By Proposition 2.1, we know there is a faithful representation $\rho : \mathrm{Gal}(M/K) \to \mathrm{GL}(V_M)$. We can then consider the quotient representation $\tilde{\rho} : \mathrm{Gal}(M/K) \to \mathrm{GL}(V_M/V_K)$, where $\tilde{\rho}(g) \cdot (v + V_K) = \rho(g) \cdot v + V_K$.

Now, let us compute $\ker \tilde{\rho}$:

$$\begin{aligned}
&\tilde{\rho}(g)(v + V_K) = \tilde{\rho}(1)(v + V_K) \\
&\Rightarrow \rho(g)v - v \in V_K \\
&\Rightarrow \rho(g)\,(\rho(g)v - v) = \rho(g)v - v \quad [\text{Since } g \text{ acts trivially on } V_K] \\
&\Rightarrow (\rho(g)^2 - 2\rho(g) + I_t)v = 0 \quad \text{for all } v \in V_M.
\end{aligned}$$

Thus, the minimal polynomial of $\rho(g)$ divides the polynomial $x^2 - 2x + 1 = (x-1)^2$. Since $\mathrm{Gal}(M/K)$ is finite, the minimal polynomial will also divide $x^n - 1$, where

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

$n = |\mathrm{Gal}(M/K)|$. Thus, the minimal polynomial must be $x - 1$, and hence we have $\rho(g) = I_t = \rho(1)$. Since ρ is faithful, this implies $g = 1$. Thus $\tilde{\rho}$ is also faithful.

The fixed assertion is true more generally, any finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ has a conjugate in $\mathrm{GL}_n(\mathbb{Z})$. For a proof, see [23, Theorem 1 and Appendix 3, p. 124]. ∎

In the next subsection, we present a number of elementary results from group theory as lemmas. These together with Proposition 2.2 will help us to prove Theorem 1.1.

2.2 Results from group theory

Lemma 2.3 *Let $\rho : G \to \mathrm{GL}_2(\mathbb{Z})$ be a faithful representation.*

(1) *If ρ is reducible, then $G \cong C_n$ or, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where $n = 1, 2, 3, 4, 6$.*
(2) *If ρ is irreducible, then $G \cong D_{2n}$, where $n = 3, 4, 6$.*

Lemma 2.4 *Let $\rho : G \to \mathrm{GL}_3(\mathbb{Z})$ be a faithful representation. Then G is isomorphic to one of the following:*

$C_n \times C_m$, *where* $n = 1, 2, 3, 4$ *and* $m = 1, 2$,

$D_{2p} \times C_m$, *where* $p = 2, 3, 4, 6$ *and* $m = 1, 2$,

$A_4 \times C_m$, *where* $m = 1, 2$, *or*

$S_4 \times C_m$, *where* $m = 1, 2$.

For proofs, see [1, Section 3].

2.3 Proof of Theorem 1.1

Proof For the $t = 1$ case, by Proposition 2.2, the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$. Since the rank has increased, $M \neq K$, so we must have $[M : K] = 2$. Applying Proposition 2.2 and the above Lemmas 2.3 and 2.4, we directly get the $t = 2$ and $t = 3$ case. ∎

Theorem 1.1(1) is particularly interesting as it implies the following.

Corollary 2.5 *In any extension of odd degree, particularly in a cubic extension, the rank can not increase by* 1. *It either remains the same or jumps by at least* 2.

Remark 2.6 Note that generalization to larger values of t becomes heavily reliant on the knowledge of classification of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$. However, we present here the following easily observed result. We haven't included it as a theorem as the author is unsure of whether or not it is vacuous.

Let L/K be a solvable Galois extension of degree n such that $\mathbf{rk}E(L) = \mathbf{rk}E(K) + t$, where t is odd. Let M be its minimal subfield. If the quotient representation $\tilde{\rho} : \mathrm{Gal}(M/K) \to \mathrm{GL}_t(\mathbb{Q})$ is *irreducible*, then $t \mid n$. The proof follows from the two results stated below.

(a) Let G be a finite group. The degree of every irreducible representation of G over an algebraically closed field $\mathbf{k}$ of characteristic 0, divides the order of G.
For a proof, see [25, Section 6.5].

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

(b) **Theorem (*Dixon*)** Let G be a finite solvable irreducible subgroup of $\mathrm{GL}_n(K)$, where K is a real field and n is an odd integer. Then G is absolutely irreducible.
For a proof, see [6, Theorem 1] and [7].

Note that by *absolutely irreducible*, we mean that G is irreducible over the algebraic closure $\overline{K}$ of K. If in fact, $t = p$ is prime, then the above mentioned papers of Dixon will provide a nice description of the Galois Group. But we think that requiring $\tilde{\rho}$ to be irreducible for larger ranks, might be asking too much!

3 Analytic minimal subfield

In this section, we focus on the analytic counterpart of the algebraic minimal subfield.

Definition 3.1 Let E/K be an elliptic curve, and let F be any finite extension of K. For each zero ω of $L(E/F, s)$, the *analytic minimal subfield* F_ω is a subfield of F with $K \subseteq F_\omega \subseteq F$ such that:
(i) $\mathrm{ord}_{s=\omega}\, L(E/F_\omega, s) = \mathrm{ord}_{s=\omega}\, L(E/F, s)$, and
(ii) if $K \subseteq M \subseteq F$ and $\mathrm{ord}_{s=\omega}\, L(E/M, s) = \mathrm{ord}_{s=\omega}\, L(E/F, s)$, then $F_\omega \subseteq M$.

Proposition 3.1 *If F/K is Galois with Galois group G and $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$ for any irreducible character χ of G, then F_ω exists and is Galois over K.*

For a detailed proof, see [1, Proposition 6]. We briefly mention the construction here, as we will be using this in Section 6. The idea is to consider those characters for which the twisted L-function vanishes at ω, i.e.,

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

Then define

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

The minimal subfield F_ω is then the fixed field, K^{H_ω} of H_ω in F.

Therefore from Proposition 3.1, in order to work with F_ω, we first need to investigate holomorphy of $L(E/K \otimes \chi, s)$ at $s = \omega$. We recall some classical theorems on Artin's holomorphy conjecture. Let F/K be a Galois extension.

Theorem 3.2 ***(Stark)*** *If s_0 is a simple zero of the Dedekind zeta function $\zeta_F(s)$, then $L(s, \chi)$ is analytic at $s = s_0$ for every irreducible character χ of* $\mathrm{Gal}(F/K)$.

For a proof, see [26, Theorem 3, p. 144].

Definition 3.2 We say E satisfies the generalized Taniyama conjecture over a number field K if the L-function $L(E/K, s)$ is the L-function $L(\pi, s)$ of a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$, where $\mathbb{A}_K$ is the adèle ring of K.

Note that for $K = \mathbb{Q}$, the above conjecture is known and is called *The Modularity Theorem*. The name derives from the fact that if $E/\mathbb{Q}$ is an elliptic curve, then its L-function $L(E/\mathbb{Q}, s)$ is the L-function of a modular form. In 1995, Wiles and Taylor

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

first proved the conjecture for semi-stable elliptic curves defined over $\mathbb{Q}$ and in 2001, B. Conrad, F. Diamond, Richard Taylor, and C. Breuil, proved modularity for all elliptic curves defined over $\mathbb{Q}$. From works of Taylor, Kisin, Wintenberger, and others, the following result on "potential modularity" is also known: If E/K is an elliptic curve, where K is a totally real field, then there is a totally real extension L/K such that E/L is modular (see, for example, [3, 16, 27, 29]).

The following elliptic analogue of Stark's theorem is due to Akbary and Murty (see [1, Proposition 7]).

Theorem 3.3 ***(Akbary–Murty)*** *Let E/K be an elliptic curve and suppose that E satisfies the generalized Taniyama conjecture over K. Let F be a solvable extension of K, and let χ be an irreducible character of $G = \mathrm{Gal}(F/K)$. Then, $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$, if ω is a simple zero of $L(E/F, s)$.*

Using this, they showed, under the same assumptions of the theorem, the analytic minimal subfield F_ω exists. Moreover, F_ω is a cyclic extension of K and if ω is real, then $[F_\omega : K] \leq 2$. Regarding Artin's holomorphy conjecture, some generalizations of Theorem 3.2 of Stark, are known. These results, as stated below, are due to Foote, Murty, and Wales. They ease the condition on ω, from being a simple zero to a zero of small order. In the next section, we will prove the elliptic analogue of such theorems.

Theorem 3.4 ***(Foote–Wales)*** *Let F/K be a Galois extension of number fields with solvable Galois group G. If the Dedekind zeta function of F, $\zeta_F(s)$, has a zero at $s = s_0$ of order less than or equal to 2, then all Artin L-series $L(s, \chi)$ are analytic at $s = s_0$ for every irreducible character χ of G.*

For a proof, see the corollary of [10, Theorem II].

Theorem 3.5 ***(Foote–Murty)*** *Let F/K be a Galois extension of number fields with solvable Galois group G, and let p_2 be the second smallest prime number dividing $|G|$. If $\zeta_F(s)$ has a zero of order r at $s = s_0$, where $r \leq p_2 - 2$, then $L(s, \chi)$ is analytic at s_0 for all irreducible characters χ of G.*

For a proof, see [9, p. 8]. Also note that, in case $|G|$ has only one prime factor, i.e., $|G|$ is a prime power, then G is nilpotent and $L(s, \chi)$ is known to be analytic in such cases. The key idea behind both of the above two results, was an attempt in finding minimal counterexamples to Artin's holomorphy conjecture.

3.1 Automorphic representations and nilpotent Galois groups

Assuming the generalized Taniyama Conjecture for K, M. Ram Murty and V. Kumar Murty in [21] proved that if F/K is contained in a finite solvable Galois extension of K, then $L(E/F, s)$ is holomorphic. Their result is predicted by a more general conjecture in Langlands program which states that if π_1 and π_2 are cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_K)$ and $\mathrm{GL}_m(\mathbb{A}_K)$, respectively, then $\pi_1 \otimes \pi_2$ is an automorphic representation of $\mathrm{GL}_{nm}(\mathbb{A}_K)$. This is known for $m = 1$, as abelian twists

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

are automorphic. The $GL(2) \times GL(2)$ case was proved by Ramakrishnan in [22] and the $GL(2) \times GL(3)$ by Kim and Shahidi in [15]. In [2], Arthur and Clozel proved that the Langlands reciprocity is valid for all nilpotent Galois extensions using their theory of automorphic induction. Therefore, assuming the generalized Taniyama conjecture for E/K, and for an extension F/K with nilpotent $\mathrm{Gal}(F/K)$, we see that $L(E/K \otimes \chi, s)$ is automorphic for any irreducible character χ of $\mathrm{Gal}(F/K)$.

Recently Wong [30] have generalized the above result to certain cases of "nearly nilpotent" and "abelian-by-nilpotent" Galois extensions. In a subsequent section, while proving the elliptic analogue of Foote–Wales's theorem, we will use similar ideas to eliminate one of the possibilities.

4 Elliptic analogue of Foote and Murty's Theorem

Theorem 4.1 *Let E/K be an elliptic curve and suppose that E satisfies the generalized Taniyama conjecture over K. Let F be a Galois extension of K with solvable Galois group $G = \mathrm{Gal}(F/K)$. Let χ be an irreducible character of G. Then, $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$ if ω is a zero of $L(E/F, s)$ of order $r \leq p_2 - 2$, where p_2 is the second smallest prime factor of $|G|$.*

Remark 4.2 Note that if $|G|$ has only one prime factor, then G is nilpotent. Hence from the above discussion, $L(E/K \otimes \chi, s)$ is known to be automorphic.

As an immediate corollary we get the following.

Corollary 4.3 *Under the same conditions of the above theorem, the minimal subfield F_ω exists if ω is a zero of $L(E/F, s)$ of order $r \leq p_2 - 2$, where p_2 is the second smallest prime factor of $|G|$.*

4.1 Ingredients for the proof of Theorem 4.1

The following Aramata–Brauer-type theorem was proved in [21, Theorem 2].

Theorem 4.4 *Let E/K be an elliptic curve and suppose that E satisfies the generalized Taniyama conjecture over K. If F is a solvable Galois extension of K, then $L(E/F, s)$ extends to an entire function and $L(E/F, s)/L(E/K, s)$ is entire. In particular,*

$$ord_{s=\omega}\, L(E/F, s) \geq ord_{s=\omega}\, L(E/K, s).$$

We now list some results on finite groups and virtual Heilbronn characters that will be used to prove Theorem 4.1.

Let F/K be a finite Galois extension with Galois group G. Let H be a subgroup of G. Let χ and ψ denote the irreducible characters of G and H, respectively. Consider the virtual Heilbronn characters

$$\theta_G = \sum n_\chi \chi \quad \text{and} \quad \theta_H = \sum n_\psi \psi,$$

where n_χ denotes the order of zero of $L(E/K \otimes \chi, s)$ at $s = \omega$ and n_ψ denotes the order of zero of $L(E/F^H \otimes \psi, s)$ at $s = \omega$ (F^H being the fixed field of H).

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Proposition 4.5 $\theta_G|_H = \theta_H$.

For a proof, see [21, Proposition 1].

Theorem 4.6 (Blichfeldt) *Let G be a finite group admitting a faithful, irreducible complex representation ρ. If G possesses a noncentral abelian normal subgroup, then ρ is induced from a proper subgroup of G.*

For a proof, see [5, Corollary 50.7, p. 348].

Theorem 4.7 ***(Ito)*** *Let G be a solvable group, and let p be a prime such that G has a faithful character of degree $< p - 1$. Then G admits an abelian normal Sylow p-subgroup.*

For a proof, see [8, Theorem 24.6, p. 128].

Proposition 4.8 *Any solvable non-abelian group G has a normal subgroup N of prime index such that N contains $Z(G)$.*

Proof Since G is non-abelian, $G_1 = G/Z(G)$ is a nontrivial solvable group. Let H be a maximal normal subgroup of G_1. Then G_1/H is solvable and simple and hence is cyclic of prime order. Thus, the index of H in G_1 is prime. Taking N to be the pre-image of H_1 proves the proposition. ∎

We also recall the following result from Clifford's theory (see [8, pp. 53–54]).

Proposition 4.9 *Let N be a normal subgroup of G with $[G : N] = p$, a prime. Then for any irreducible character χ of G, either $\chi|_N$ is irreducible, or $\chi|_N = \sum_{i=1}^{p} \psi_i$, where ψ_i are distinct and irreducible characters of N. Moreover, $\chi = Ind_H^G \psi_i$.*

4.2 Proof of Theorem 4.1

The proof is based on the idea of minimal counterexamples as that of its classical counterpart. Assume the theorem is false and suppose F and K are chosen to form a counterexample with $[F : K]$ minimal. Thus there exists an irreducible character χ of G and a point $s = \omega$ such that ω is a zero of $L(E/F, s)$ of order satisfying the conditions in the theorem but $L(E/K \otimes \chi, s)$ has a pole at $s = \omega$, i.e., $n_\chi < 0$ in the virtual Heilbronn character θ_G at $s = \omega$.

Note that G can not be cyclic, since $L(E/K \otimes \chi, s)$ is known to be analytic for cyclic extensions F/K for every irreducible character χ of G (see, for example, the proof of [21, Theorem 2, p. 492]).

Step 1 : *Every irreducible character χ of G with $n_\chi < 0$ is faithful.*

Note that by Theorem 4.4, for every field D with $K \subseteq D \subseteq F$, we have $\mathrm{ord}_{s=\omega} L(E/D, s) \leq \mathrm{ord}_{s=\omega} L(E/F, s)$. Thus, for any character χ with a pole at $s = \omega$, one can consider $D = F^{\ker \chi}$, the fixed field of $\ker \chi$. Thus, the conditions of the hypothesis for the counterexample carries over to D, $G/\ker \chi$ and K. By minimality of $|G|$, we must have $\ker \chi = \{1\}$.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Step 2 : *For all proper subgroups H of G, θ_H is a character of H.*

We have the factorization

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

Thus $\mathrm{ord}_{s=\omega} L(E/F,s) = r = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi(1) = \theta_G(1)$. Suppose ψ is an irreducible character of H. Consider the L-series $L(E/F^H \otimes \psi, s)$. By Proposition 4.5, we have $\theta_G|_H = \theta_H$ and so $\theta_H(1) = \theta_G|_H(1) = r$. Thus, if ω is a pole, the triple $F,\ H,\ F^H$ forms a counterexample contradicting minimality. Thus, for every irreducible character ψ of H, $L(E/F^H \otimes \psi, s)$ is analytic at $s = \omega$, in particular, $n_\psi \geq 0$ which implies θ_H is a character. Note that, by assumption, θ_G is not a character.

Step 3 : *Any irreducible χ of G with $n_\chi < 0$, is not induced from any proper subgroup of G.*

Suppose $\chi = \mathrm{Ind}_H^G \psi$ for a character ψ of a proper subgroup H of G. Then

$$L(E/K \otimes \chi, s) = L(E/F^H \otimes \psi, s) = \prod_{\phi} L(E/F^H \otimes \phi, s)^{a_\phi},$$

where characters ϕ are the irreducible constituents of ψ with coefficient a_ϕ. By the previous step, since H is a proper subgroup, the factors are analytic at $s = \omega$, in particular, $L(E/F^H \otimes \psi, s)$ is analytic at $s = \omega$ contradicting $n_\chi < 0$.

Step 4 : *There are no faithful characters of G of degree $\leq p_2 - 2$. In particular, if χ is an irreducible character of G with $n_\chi < 0$, then $\chi(1) > p_2 - 2$.*

If G has a faithful character of degree $\leq p_2 - 2$, then by Ito's Theorem 4.7, G will have normal abelian Sylow p_i-subgroups for all prime factors $p_i,\ i \geq 2$, of G. Also, all of them will be central and hence index of $Z(G)$ in G will be a power of p_1. In particular, $G/Z(G)$ will be nilpotent and hence G will be nilpotent contradicting the existence of χ.

Note that, this in particular implies G must be *non-abelian*.

Step 5 : We now decompose θ_G into three constituents θ_{nf}, θ_+, and θ_- as follows:

- θ_{nf} is the sum of all constituents $n_\lambda \lambda$ of θ_G such that λ is an irreducible character of G that is *not faithful* (hence the "nf").
- θ_+ is the sum of all constituents $n_\psi \psi$ of θ_G such that ψ is an irreducible character of G that is faithful and $n_\psi > 0$.
- $\theta_- = \sum(-n_\chi)\chi$, where $n_\chi \chi$ are all those constituents of θ_G such that χ is an irreducible character of G that is faithful and $n_\chi < 0$.

From Step 1, all the coefficients of θ_{nf} are nonnegative. Thus θ_{nf} is either a character or 0. By construction θ_- is a character (since there is at least one irreducible character χ with $n_\chi < 0$) and θ_+ is either a character or 0. Also note that, by construction, $\langle \theta_{nf}, \theta_- \rangle = 0$, as well as $\langle \theta_+, \theta_- \rangle = 0$ and $\langle \theta_+, \theta_{nf} \rangle = 0$ and

$$\theta_G = \theta_{nf} - \theta_- + \theta_+.$$

The final contradiction will come from showing $\theta_+ = \theta_-$.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Step 6 : In any finite group X, every normal subgroup appears as one of the subgroups in a chief series $X = X_1 \geq X_2 \geq \cdots \geq X_{n-1} \geq X_n = \{1\}$, where each $X_i \trianglelefteq G$. In particular, for our solvable G the chief factors G_i/G_{i+1} are elementary abelian p-groups (see [14, Corollary 8.7, p. 102]). In particular, the last chief factor $G_{n-1}/\{1\}$ is a nontrivial abelian group. That is, every normal subgroup of G contains a nontrivial abelian p-group that is normal in G. We have already seen that every abelian normal subgroup of G is central. Thus for every irreducible character λ of G that is not faithful, $\ker\lambda \cap Z(G) \neq 1$. By Proposition 4.8, G has a normal subgroup $N \supseteq Z(G)$ of prime index, say p.

Step 7 : $\langle \theta_-|_N, \theta_{nf}|_N \rangle_N = 0$

First, we note that $\chi|_N$ is irreducible for every irreducible constituent χ of θ_-. Since, if not, then from Proposition 4.9, we have $\chi|_N = \psi_1 + \cdots + \psi_p$ for some irreducible characters ψ_i of N and $\chi = \mathrm{Ind}_H^G \psi_1$, contradicting Step 3. Now for any irreducible constituent λ of θ_{nf}, we have seen $\ker\lambda \cap Z(G) \neq \{1\}$, i.e., $\lambda|_N$ is not faithful as $N \supseteq Z(G)$. Again by Proposition 4.9, either $\lambda|_N$ is irreducible, or is induced from irreducible constituents, thus they are also not faithful. Hence $\langle \theta_-|_N, \theta_{nf}|_N \rangle_N = 0$.

Step 8 : $\theta_+|_N = \theta_-|_N$

By Step 2, θ_N is a character. Also, by Proposition 4.5, $\theta_N = \theta_G|_N = \theta_+|_N - \theta_-|_N + \theta_{nf}|_N$. Therefore, by Step 7, either $\theta_+|_N = \theta_-|_N$ or $\theta_+|_N = \theta_-|_N + \phi$ for some character ϕ of N. Assume the latter, then

$$r = \theta_G(1) = \theta_G|_N(1) = \phi(1) + \theta_{nf}(1). \tag{4.1}$$

Let ϕ_1 be an irreducible constituent of ϕ, and hence of $\theta_+|_N$. If ψ is an irreducible constituent of θ_+ such that ϕ_1 occurs in $\psi|_N$, we see that $\psi|_N \neq \phi_1$. This is because $\phi_1(1) \leq r$ by (4.1), where as ψ being faithful, $\psi|_N(1) > p_2 - 1 \geq r$ by Step 4. Applying Proposition 4.9 again, $\psi_N = \phi_1 + \cdots + \phi_p$. These are distinct G-conjugate irreducible characters of N. Since, ϕ_1 is an irreducible constituent of ϕ and $\phi = (\theta_+ - \theta_-)|_N$ is a G-stable character of N, each ϕ_i must also appear as a constituent of ϕ. Thus, we have $\psi(1) = \phi_1(1) + \cdots + \phi_p(1) \leq \phi(1) \leq r$. This contradicts $\psi(1) = \psi|_N(1) > r$ computed above, thus $\theta_+|_N = \theta_-|_N$.

Final Step : Let $g \in G \setminus N$, and let H be the subgroup generated by g and $Z(G)$. Since, H is abelian, $H \neq G$. Let λ be a constituent of θ_{nf}, then from Step 6, we have $\ker\lambda \cap Z(G) \neq \{1\}$. Thus, the same holds for $\mathrm{Ind}_H^G(\lambda|_H)$. Let χ be an irreducible constituent of θ_-, hence is faithful and so $\langle \chi, \mathrm{Ind}_H^G(\lambda|_H) \rangle = 0$. Hence by Frobenius reciprocity, $\langle \chi|_H, \lambda|_H \rangle = 0$ and so, like in Step 7, $\langle \theta_-|_H, \theta_{nf}|_H \rangle_H = 0$. Now $\theta_H = \theta_G|_H = \theta_+|_H - \theta_-|_H + \theta_{nf}|_H$. As before, either $\theta_+|_H - \theta_-|_H$ is zero or a character and arguing in the exact same way as Step 8, we get $\theta_+|_H = \theta_-|_H$. Hence, $\theta_+(g) = \theta_-(g)$ for all $g \in G \setminus N$. Combining this with Step 8, gives $\theta_+ = \theta_-$. This is a contradiction and hence the theorem is proved.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

5 Elliptic analogue of Foote and Wales's Theorem

Theorem 5.1 *Let E/K be an elliptic curve and suppose that E satisfies the generalized Taniyama conjecture over K. Let F be a Galois extension of K with solvable Galois group $G = \mathrm{Gal}(F/K)$. Let χ be an irreducible character of G. Then, $L(E/K \otimes \chi, s)$ is holomorphic at $s = \omega$, if ω is a zero of $L(E/F, s)$ of order ≤ 2.*

The proof of this theorem follows its counterpart more directly than the previous one, because of the following theorem.

Theorem 5.2 ***(Foote–Wales)*** *Let G be a finite group with a virtual character θ satisfying the following conditions:*

(1) *$\theta(1) \leq 2$,*
(2) *θ is not a character of G but $\theta|_H$ is a character for every proper subgroup H of G, and*
(3) *if χ is any irreducible constituent of θ such that $\langle \theta, \chi \rangle < 0$, then χ is faithful, nonlinear and is not induced from any proper subgroup of G.*

Then $\theta(1) = 2$ and $G \cong \mathrm{SL}_2(p)$, for some prime $p \geq 5$, or $\widehat{\mathrm{SL}_2}(3)$.

Note that in their notation, $\widehat{\mathrm{SL}_2}(3)$ denotes any nontrivial semidirect product of Q_8 (the quaternion group of order 8) by a cyclic 3-group. For a proof, see [10, Theorem III].

Additionally, we are assuming that G is solvable and so G cannot be $\mathrm{SL}_2(p)$ ($p \geq 5$). For $\widehat{\mathrm{SL}_2}(3)$, Foote and Wales in [10, p. 229] tackles this possibility by quoting a deep result of Langlands which shows that Artin's holomorphy conjecture is true in the case when $G/Z(G) \cong A_4$. We address this in our next proposition. The proof can be seen as consequence of a result of Wong (see [30, Theorem 1.3]). But for the sake of completeness, we present it here.

Proposition 5.3 *Suppose that E satisfies the generalized Taniyama conjecture over K. Let F be a Galois extension of K with solvable Galois group isomorphic to $\widehat{\mathrm{SL}_2}(3)$. Let χ be an irreducible character of G. Then, $L(E/K \otimes \chi, s)$ is automorphic and hence entire.*

Proof Note that $Q_8 \trianglelefteq \widehat{\mathrm{SL}_2}(3)$ and the quotient is a 3-group, in particular, is nilpotent. A result of Horváth (see [12, Proposition 2.7]) says that this makes $\widehat{\mathrm{SL}_2}(3)$ an "SM-group relative to Q_8." What this means in our context, is that, every irreducible character χ of $\widehat{\mathrm{SL}_2}(3)$, is induced from an irreducible character ψ of a subnormal subgroup H containing Q_8. Moreover, $\psi|_{Q_8}$ is irreducible and hence $\psi(1) = \psi|_{Q_8}(1) \leq 2$. Further note that, in the degree 2 case, ψ can not be the icosahedral type (recall, this is the case when the image of the degree 2 representation in $\mathrm{PGL}_2(\mathbb{C})$ is isomorphic to A_5). This is because, the only prime factors of $\widehat{\mathrm{SL}_2}(3)$, and hence of H, are 2 and 3. In particular, 5 is not a prime factor of H.

Now if ψ is of degree 1, then, from Artin reciprocity, ψ can be seen as an idèle class character. If ψ is of degree 2, from theorems of Langlands and Tunnell (see [18, 28]), ψ is associated with a cuspidal automorphic representation π_ψ of $\mathrm{GL}_2(\mathbb{A}_{K^H})$. Since H

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

is subnormal, there exists a subnormal series

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t = \widehat{\mathrm{SL}_2}(3).$$

Moreover, since we assumed solvability, H_{i+1}/H_i is of prime degree. Therefore, by repeated application of Arthur and Clozel's theory of base change for cyclic extensions (see [2, Theorem 4.2]), the base change map $B(\pi) \in \mathrm{GL}_2(\mathbb{A}_{K^H})$ exists. Recall, we are writing, $L(E/K, s) = L(\pi, s)$. For a short exposition on the base change map, see [21, Section 3], we're following their notation. Now

$$L(E/K \otimes \chi, s) = L(E/K \otimes \mathrm{Ind}_H^G \psi, s) = L(E/K^H \otimes \psi, s) = L(B(\pi) \otimes \pi_\psi, s).$$

Since functoriality is known in cases of $\mathrm{GL}(n) \times \mathrm{GL}(1)$ and $\mathrm{GL}(2) \times \mathrm{GL}(2)$, the latter due to Ramakrishnan [22], and we saw that either ψ is an idèle class character or an automorphic representation of $\mathrm{GL}(2)$, so $L(E/K \otimes \chi, s)$ is automorphic and hence entire. ∎

5.1 Proof of Theorem 5.1

As in Theorem 4.1, assume the statement is false and take a counterexample F/K with $[F : K]$ minimal. Thus, there exists an irreducible character ψ of $G = \mathrm{Gal}(F/K)$ and a point $s = \omega$ such that ω is a zero of $L(E/F, s)$ of order ≤ 2 but $L(E/K \otimes \psi, s)$ has a pole at $s = \omega$.

Set $\theta = \theta_G = \sum n_\chi \chi$. Note that $n_\psi < 0$. Since we have the factorization

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

so, $\theta_G(1) = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi(1) = \mathrm{ord}_{s=\omega} L(E/F, s) \leq 2$. Moreover, we can then carry out Steps 1–4, as it is, in the proof of Theorem 4.1. Hence, all the conditions of Theorem 5.2 are satisfied. But then the solvability assumption eliminates $\mathrm{SL}_2(p)$ and Proposition 5.3 eliminates $\widehat{\mathrm{SL}_2}(3)$ giving us a contradiction.

6 Applications to minimal subfields

We now look at some applications of our theorems in the context of analytic and algebraic minimal subfields.

Theorem 6.1 *Let E/K be an elliptic curve, and let F/K be a finite Galois extension with solvable Galois group $G = \mathrm{Gal}(F/K)$. Suppose that E satisfies the generalized Taniyama conjecture over K and $L(E/F, s)$ has a zero at ω of order two. Then the analytic minimal subfield F_ω exists. Further, if ω is real, then $G = \mathrm{Gal}(F_\omega/K)$ satisfies one of the following:*

(i) *G is either cyclic or dihedral.*
(ii) *$Z(G) \cong \mathbb{Z}/2\mathbb{Z}$ and $G/Z(G) \cong D_{2n}, A_4$ or, S_4.*

Proof By Theorem 5.1, $L(E/K \otimes \chi, s)$ is holomorphic for every irreducible character χ of G. Hence, by Proposition 3.1, F_ω exists.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Now suppose ω is real. We have the factorization

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

Since $\mathrm{ord}_{s=\omega}\, L(E/F,s) = 2$, then there exists $\chi \in \mathrm{Irr}(G)$ such that $\mathrm{ord}_{s=\omega}\, L(E/K \otimes \chi, s) \geq 1$. Since ω is real, we have

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

Case I : $\chi \neq \overline{\chi}$. Hence $\chi(1) = 1 = \overline{\chi}(1)$. Thus, χ is one-dimensional. Then F_ω, being the fixed field of $\ker \chi \cap \ker \overline{\chi} = \ker \chi$, is cyclic.

Case II : $\chi = \overline{\chi}$ and $\chi(1) = 1$. Thus, χ is a real irreducible linear character. Since the order of vanishing of $L(E/F,s)$ at ω is 2, there exists another such character. Hence, $\mathrm{Gal}(F_\omega)/K$ is a subgroup of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Case III : $\chi = \overline{\chi}$ and $\chi(1) = 2$. Since F_ω is the fixed field of $\ker \chi$, $\mathrm{Gal}(F_\omega/K)$ admits a faithful degree 2 irreducible representation coming from the quotient representation corresponding to χ. Let the character of this representation be denoted by $\tilde{\chi}$. Therefore, we know that $G/Z(G)$ is isomorphic to a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ and therefore is isomorphic to C_n, D_n, A_4, S_4, or A_5 (see [24, Proposition 16 and Section 2.5]). By the solvability condition, A_5 can be eliminated. Since $\chi = \overline{\chi}$, we have $\tilde{\chi} = \overline{\tilde{\chi}}$, and so $Z(G) = \{1\}$ or $\mathbb{Z}/2\mathbb{Z}$. Now $G/Z(G)$ cannot be cyclic as that will imply G is abelian. Note that when $Z(G) = \{1\}$, then the only possibilities are D_{2n} and S_4. (This is because A_4 does not have any two-dimensional irreducible representations.) Moreover, if $G \cong S_4$, then, by [25, Proposition 24, p. 61] (take $A = A_4$), there are two possibilities. We show that both of them lead to contradictions. Suppose $\tilde{\chi}|_{A_4}$ is isotypic (i.e., it is a direct sum of isomorphic irreducible representations). Since A_4 does not have any two-dimensional irreducible representation, $\tilde{\chi}|_{A_4}$ is also reducible and isotypic and so, $A_4 \subseteq Z(G)$, a contradiction. Thus, there exists an irreducible representation ψ of A_4 such that $\tilde{\chi} = \mathrm{Ind}_{A_4}^{S_4} \psi$ with $\psi(1) = 1$. But we also know that every representation of A_4 of dimension 1 has V_4 in its kernel, therefore, $V_4 \subseteq \ker \psi$. Since $V_4 \trianglelefteq S_4$, hence $V_4 \subset \ker \mathrm{Ind}_{A_4}^{S_4} \psi = \ker \tilde{\chi}$, contradicting faithfulness of $\tilde{\chi}$. ∎

We now look at more applications of our results in relation to the celebrated Birch and Swinnerton-Dyer conjecture. The BSD conjecture predicts that the rank of $E(K)$ is equal to the order of vanishing of $L(E/K,s)$ at $s = 1$. Due to work of Gross and Zagier [11] and Kolyvagin [17], this is known for $K = \mathbb{Q}$ and $\mathrm{ord}_{s=1} L(E/\mathbb{Q},s) \leq 1$. In the next theorem, we prove a slight generalization to this result, namely, we look at the case when rank increases by 1 in a solvable extension.

Theorem 6.2 *Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a solvable Galois extension.*

(i) *If* $\mathbf{rk}E(K) = \mathbf{rk}E(\mathbb{Q}) + 1$, *then* $ord_{s=1}\, L(E/K,s) \geq ord_{s=1}\, L(E/\mathbb{Q},s) + 1$.

(ii) *If $L(E/\mathbb{Q} \otimes \chi, s)$ is holomorphic at $s = 1$ for every irreducible character χ of* $\mathrm{Gal}(K/\mathbb{Q})$, *and* $ord_{s=1}\, L(E/K,s) = ord_{s=1}\, L(E/\mathbb{Q},s) + 1$, *then* $\mathbf{rk}E(K) \geq \mathbf{rk}E(\mathbb{Q}) + 1$.

In both cases, equality holds if the algebraic and the analytic minimal subfields are equal.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Proof (i) Let M be the algebraic minimal subfield. By Theorem 1.1, M is a quadratic extension of $\mathbb{Q}$, say of discriminant D. Consider the twisted elliptic curve E_D. Then we have

$$\mathbf{rk}E(M) = \mathbf{rk}E(\mathbb{Q}) + \mathbf{rk}E_D(\mathbb{Q})$$

(see, e.g., [13, Proposition 20.5.4, p. 357]). Thus, $\mathbf{rk}E_D(\mathbb{Q}) = 1 = \mathrm{ord}_{s=1}L(E_D/\mathbb{Q}, s)$. We also have $L(E/M, s) = L(E/\mathbb{Q}, s) \cdot L(E_D/\mathbb{Q}, s)$. Thus,

$$\mathrm{ord}_{s=1}L(E/K, s) \geq \mathrm{ord}_{s=1}L(E/M, s) = \mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) + 1,$$

where the first inequality follows directly from Theorem 4.4. Note that equality holds if $M = F_1$ (the analytic minimal subfield at $s = 1$).

(ii) The holomorphy condition ensures that the analytic minimal subfield exists. We have the factorization

$$L(E/K, s) = \prod_{\chi} L(E/\mathbb{Q} \otimes \chi, s)^{\chi(1)}.$$

Since the order of zero increases by 1, we see that there is a nontrivial character χ of degree 1 such that $L(E/\mathbb{Q} \otimes \chi, 1) = 0$. Since the analytic minimal subfield F_1 is the fixed field of $\ker \chi$, thus it is cyclic. Moreover, as $\mathrm{ord}_{s=1}L(E/\mathbb{Q} \otimes \chi, s) = \mathrm{ord}_{s=1}L(E/\mathbb{Q} \otimes \overline{\chi}, s)$, we have $\chi = \overline{\chi}$, and so $[F_1 : \mathbb{Q}] = 2$. Suppose F_1 is of discriminant D. Since, $L(E/F_1, s) = L(E/\mathbb{Q}, s) \cdot L(E_D/\mathbb{Q}, s)$, we have $\mathrm{ord}_{s=1}L(E_D/\mathbb{Q}, s) = 1$, and therefore $\mathbf{rk}E_D(\mathbb{Q}) = 1$. Thus $\mathbf{rk}E(K) \geq \mathbf{rk}E(F_1) = \mathbf{rk}E(\mathbb{Q}) + 1$. ∎

Corollary 6.3 *If* $ord_{s=1}\ L(E/\mathbb{Q}, s) = \mathbf{rk}E(\mathbb{Q})$ *and* $K/\mathbb{Q}$ *is a quadratic extension, then*

$$\mathbf{rk}E(K) = \mathbf{rk}E(\mathbb{Q}) + 1 \textit{ if and only if } ord_{s=1}L(E/K, s) = ord_{s=1}L(E/\mathbb{Q}) + 1.$$

The corollary follows from the fact that in this case both of the minimal subfields are equal to K. Also note that it is unconditional, as holomorphy of $L(E/\mathbb{Q} \otimes \chi, s)$ is known in cyclic case.

The holomorphy condition of $L(E/\mathbb{Q} \otimes \chi)$ in Theorem 6.2(ii) can be relaxed if E has complex multiplication. We discuss this next.

Let G be a finite group and $H \leq G$ be any subgroup. For every complex character ψ of H, we attach a complex number $n(H, \psi)$ satisfying:

(i) $n(H, \psi + \psi') = n(H, \psi) + n(H, \psi')$, and
(ii) $n(G, \mathrm{Ind}_H^G \psi) = n(H, \psi)$.

Define $\theta_H = \sum_{\psi \in \mathrm{Irr}(G)} n(H, \psi)\psi$. Then we have, $\theta_G|_H = \theta_H$ (see [21, Proposition 1, p. 484]). The following is proved in [20, Theorem 14].

Theorem 6.4 ***(M. Ram Murty)*** *Suppose* $n(H, 1) \geq n(G, 1)$ *for every cyclic subgroup* H *of* G. *Then*

$$\sum_{\chi \neq 1} |n(G, \chi)|^2 \leq \left(n(G, \mathrm{reg}) - n(G, 1)\right)^2,$$

*where "*reg*" denotes the regular character of* G.

We also note the following theorem from [21, Theorem 1].

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

Theorem 6.5 ***(M. Ram Murty and V. Kumar Murty)*** *Let E be an elliptic curve defined over K. Suppose that E has complex multiplication (CM) and F is a finite extension of K. If F is contained in a solvable extension of K, then $L(E/F, s)/L(E/K, s)$ is entire.*

Combining the above two theorems, we get the following.

Theorem 6.6 *Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a solvable Galois extension with Galois group G. Suppose E has complex multiplication. If $ord_{s=1}\, L(E/K, s) = ord_{s=1}\, L(E/\mathbb{Q}, s) + 1$, then $\mathbf{rk}E(K) \geq \mathbf{rk}E(\mathbb{Q}) + 1$.*

Proof Let $n(H, \psi) = \mathrm{ord}_{s=1} L(E/K^H \otimes \psi, s)$. For any cyclic subgroup H of G, $L(E/K^H \otimes \psi, s)$ is entire, moreover by Theorem 6.5, $L(E/K^H, s)/L(E/\mathbb{Q}, s)$ is entire and so conditions of Theorem 6.4 are satisfied. In particular,

$$\sum_{\chi \neq 1} n(G, \chi)^2 \leq 1.$$

Thus, it must be that, there exists a linear character χ_1, such that $n(G, \chi_1) = 1$ and $n(G, \chi) = 0$ for all $\chi \neq 1, \chi_1$. That is, $L(E/\mathbb{Q} \otimes \chi, s)$ is holomorphic at $s = 1$ for all irreducible characters χ of G. Thus, the condition of Theorem 6.2(ii) is satisfied and we have $\mathbf{rk}E(K) \geq \mathbf{rk}E(\mathbb{Q}) + 1$ if $\mathrm{ord}_{s=1}\, L(E/K, s) = \mathrm{ord}_{s=1}\, L(E/\mathbb{Q}, s) + 1$. ■

Acknowledgments I would like to thank Prof. V. Kumar Murty for several valuable suggestions and encouragement. I also thank all past and present members of the GANITA Lab for patiently listening to the talks I gave while preparing the draft of this article and for providing their helpful inputs.

References

[1] A. Akbary and V. Kumar Murty, *Descending rational points on elliptic curves to smaller fields*. Canad. J. Math. **53**(2001), no. 3, 449–469.
[2] J. Arthur and L. Clozel, *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies, 120, Princeton University Press, Princeton, NJ, 1990.
[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3 -adic exercises*. J. Amer. Math. Soc. **14**(2001), no. 4, 843–939.
[4] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*. Invent. Math. **39**(1977), 223–251.
[5] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons Inc., New York, 1962.
[6] J. D. Dixon, *Irreducible solvable linear groups of odd degree*. J. Algebra **47**(1977), 305–312.
[7] J. D. Dixon, *Comments and corrections to my paper 'irreducible solvable linear groups of odd degree'*. J. Algebra **55**(1978), 188–190.
[8] W. Feit, *Characters of finite groups*, Benjamin, New York, 1967.
[9] R. Foote and V. Kumar Murty, *Zeros and poles of Artin L-series*. Math. Proc. Cambridge Philos. Soc. **105**(1989), 5–11.
[10] R. Foote and D. Wales, *Zeros of order 2 of Dedekind zeta functions and Artin's conjecture*. J. Algebra **131**(1990), 226–257.
[11] B. H. Gross and D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84**(1986), no. 2, 225–320.
[12] E. Horváth, *On some questions concerning subnormally monomial groups*. In: C. M. Campbell, T. C. Hurley, E. F. Robertson, S. J. Tobin, and J. J. Ward (eds.), *Proceedings of the Conference Groups '93 Galway/St Andrews*, Vol. 2, Cambridge University Press, Cambridge, pp. 314–321.

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press

[13] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. 2nd ed., Springer, New York, 1990.
[14] I. Isaacs Martin, *Algebra: A graduate course*, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2009.
[15] H. Kim and F. Shahidi, "Functorial products for $GL_2 \times GL_3$ and functorial symmetric cube for GL_2", *with an appendix by Colin J. Bushnell and Guy Henniart*. Ann. Math. **155**(2002), no. 3, 837–893.
[16] M. Kisin, *Moduli of finite flat group schemes, and modularity*. Ann. Math. **170**(2009), no. 3, 1085–1180.
[17] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves*. Math. USSR-Izv. **32**(1989), 523–542.
[18] R. P. Langlands, *Base change for $GL(2)$*. In: *Annals of mathematics studies*, 96, Princeton University Press, Princeton, NJ, 1980.
[19] B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil curves*. Invent. Math. **25**(1974), 1–61.
[20] M. R. Murty, *On Artin L-functions*. In: *Class field theory: Its centenary and prospect* (Tokyo, 1998), Advanced Studies in Pure Mathematics, 30, Mathematical Society of Japan, Tokyo, 2001, pp. 13–29.
[21] M. R. Murty and V. Kumar Murty, *Base change and the Birch–Swinnerton-Dyer conjecture*. A tribute to Emil Grosswald: number theory and related analysis, Contemp. Math., **143**, 481–494., Amer. Math. Soc., Providence, RI (1993).
[22] D. Ramakrishnan, *Modularity of the Rankin–Selberg L-series, and multiplicity one for $SL(2)$*. Ann. Math. **152**(2000), no. 1, 45–111.
[23] J.-P. Serre, *Lie algebras and lie groups*, Lecture Notes in Mathematics, Springer, Berlin, 1964.
[24] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.
[25] J.-P. Serre, *Linear representations of finite groups*, GTM 42, Springer, New York, 1996.
[26] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*. Invent. Math. **23**(1974), 135–152.
[27] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141**(1995), no. 3, 553–572.
[28] J. Tunnell, *Artin's conjecture for representations of octahedral type*. Bull. Amer. Math. Soc. N. S. **5**(1981), no. 2, 173–175.
[29] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. Math. **141**(1995), 443–551.
[30] P.-J. Wong, *Base change, tensor product and the Birch–Swinnerton-Dyer conjecture*. J. Ramanujan Math. Soc. **33**(2018), no. 1, 99–109.

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, MS 476, Alberta, T2N 1N4, Canada
e-mail: samprit.ghosh@ucalgary.ca

https://doi.org/10.4153/S0008439524000341 Published online by Cambridge University Press