Volume 26, Number 6, 1571–1586, 2019

Growth of the analytic rank of modular elliptic curves over quintic extensions

Michele Fornea

Given $F$ a totally real number field and $E/F$ a modular elliptic curve, we denote by $G_5(E/F; X)$ the number of quintic extensions $K$ of $F$ such that the norm of the relative discriminant is at most $X$ and the analytic rank of $E$ grows over $K$, i.e., $r_{an}(E/K) > r_{an}(E/F)$. We show that $G_5(E/F; X) \asymp X$ when the elliptic curve $E/F$ has odd conductor and at least one prime of multiplicative reduction. As Bhargava, Shankar and Wang [1] showed that the number of quintic extensions of $F$ with norm of the relative discriminant at most $X$ is asymptotic to $c_5,F X$ for some positive constant $c_5,F$, our result exposes the growth of the analytic rank as a very common circumstance over quintic extensions.

1. Introduction

The arithmetic of elliptic curves is an intriguing mystery for number theorists. Given an elliptic curve $E$ over a number field $K$, it is possible to package its arithmetic information into a generating series $L(E/K, s)$. While a priori the series just converges for $\text{Re}(s) \gg 0$, conjecturally it has analytic continuation to the whole complex plane and a functional equation $s \mapsto 2 - s$ with center $s = 1$. The analytic rank is defined as the conjectural order of vanishing at the center

$$r_{an}(E/K) := \text{ord}_{s=1} L(E/K, s).$$

This analytic invariant has an algebraic doppelgänger: the $\mathbb{Z}$-rank of the finitely generated abelian group of $K$-rational points, $r_{alg}(E/K)$, also called the algebraic rank of $E/K$. The pioneering work of Birch and Swinnerton-Dyer strongly suggests the equality of the two invariants. When the elliptic curve $E$ is defined over a totally real number field $F$ and $K/F$ is a finite extension, then one expects the inequality $r_{an}(E/K) \geq r_{an}(E/F)$ to hold. Furthermore, the strict inequality should be explained by the presence of a non-torsion point in $E(K)$ linearly independent from $E(F)$. We like to
think about our main result as evidence for the fact that there should be a systematic way to produce non-torsion points over $S_5$-quintic extensions of totally real number fields, in analogy with the case of Heegner points over CM fields.

Our main result is compatible with the conjectures in [4], [5] about the growth of the analytic rank of rational elliptic curves over cyclic quintic extensions. Even though in those works growth is predicted to be a rare phenomenon, cyclic quintic extensions form a thin subset of all quintic extensions: the counting function of cyclic quintic fields is asymptotic to $\alpha X^{1/4}$ for some positive constant $\alpha > 0$ [15]. The results obtained in this work appear to be widely applicable given how all elliptic curves over a totally real number field $F$ of degree 2 over $\mathbb{Q}$ are modular and that, in general, all but finitely many $\mathbb{Q}$-isomorphism classes of elliptic curves over a totally real number field $F$ are known to be modular ([13], [1], [2], [6]).

1.1. Strategy of the proof

Let $F$ be a totally real number field, $K/F$ a $S_5$-quintic extension with a totally complex Galois closure $J$ such that the subfield of $J$ fixed by $A_5$ is a totally real quadratic extension $M/F$. Given $E/F$ a modular elliptic curve corresponding to a primitive Hilbert cuspform $f_E$ of parallel weight two, the key idea of the present work is to interpret the ratio of $L$-functions

$$\frac{L(E/K, s)}{L(E/F, s)}$$

as the twisted triple product $L$-function attached to $f_E$ and a certain Hilbert cuspform $g$ over $M$ of parallel weight one. This interpretation provides meromorphic continuation, functional equation and holomorphicity at the center. As the sign $\varepsilon_{K/F}$ of the functional equation of $L(E/K, s)/L(E/F, s)$ is then determined by the splitting behaviour in $K$ of the primes of multiplicative reduction of $E/F$, we conclude by establishing the existence of a positive proportion of quintic extensions $K/F$ for which $\varepsilon_{K/F} = -1$ by invoking [4].

The twisted triple product $L$-function attached to a modular elliptic curve $E/F$ and a cuspform $g$ of parallel weight one over a totally real quadratic extension $M/F$, is the $L$-function $L(E, \otimes-\text{Ind}_M^F(g), s)$. Here $\otimes-\text{Ind}_M^F(g)$ denotes the tensor induction of the Artin representation attached to $g$. The main technical result of our work consists in proving the existence of an eigenform $g$ such that

$$\otimes-\text{Ind}_M^F(g) \cong \text{Ind}_K^F 1 - 1$$
where 1 denotes the trivial representation. Thanks to the modularity of totally odd Artin representations [9], the problem reduces to finding the solution to a Galois embedding problem as follows.

The group $G(J/M) \cong A_5$ does not afford any irreducible 2-dimensional complex representation, but it has two conjugacy classes of embeddings into $\text{PGL}_2(\mathbb{C})$. Therefore, we look for a lift of the 2-dimensional projective representation of

$$G_M \to G(J/M) \hookrightarrow \text{PGL}_2(\mathbb{C})$$

which (i) is totally odd, (ii) has controlled ramification, and (iii) whose tensor induction is $\text{Ind}_F^1 \mathbb{1} - \mathbb{1}$. Since every projective 2-dimensional representation has a minimal lift with index a power of 2 ([11], Lemma 1.1), it suffices to consider the following Galois embedding problem:

Given a finite set of primes $\Sigma_0$, is it possible to find a Galois extension $H/F$ unramified at $\Sigma_0$, containing $J/F$, and such that

$$1 \to \mathcal{C}_{2^r} \to G(H/F) \to G(J/F) \to 1$$

is a non-split extension for some $r \geq 1$?

Here $\mathcal{C}_{2^r}$ denotes the cyclic group of order $2^r$ considered as an $S_5$-module via the homomorphism $S_5 \to \{\pm 1\} \hookrightarrow \text{Aut}(\mathcal{C}_{2^r})$, taking the non-trivial element of $\{\pm 1\}$ to the automorphism $x \mapsto x^{-1}$. Theorem 3.4 provides conditions for the Galois embedding problem to have a solution.

2. On exotic tensor inductions

Let $A$, $B$ be groups, $n \in \mathbb{N}$ and $\phi : A \to S_n$ a group homomorphism. The wreath product of $B$ with $A$ is $B \wr A := B^{\oplus n} \rtimes \phi A$, where $A$ acts permuting the factors through $\phi$.

Let $G$ be a group and $Q$ a subgroup of index $n$. Denote by $\pi : G \to S_n$ the action of $G$ on right cosets by right multiplication and let $\{g_1, \ldots, g_n\}$ be a set of coset representatives. For any $g \in G$ and $i \in \{1, \ldots, n\}$, we denote by $q_i(g)$ the unique element of $Q$ such that $g \cdot g_i = g_i \pi(g) \cdot q_i(g)$. The map

$$\varphi : G \to Q \wr S_n, \quad g \mapsto (q_1(g), \ldots, q_n(g), \pi(g)),$$

is an injective group homomorphism. Moreover, a different choice of coset representatives produces a homomorphism conjugated to $\varphi$ by an element of $G$. 


Definition 2.1. Let \( Q \) be a subgroup of \( G \) of index \( n \) and \( \varrho : Q \to \text{Aut}(V) \) a representation of \( Q \). The tensor induction \( \otimes\text{-Ind}_G^Q(\varrho) \) of \( \varrho \) is defined as the composition of the arrows in the diagram

\[
\begin{array}{ccc}
G & \xrightarrow{\varphi} & \otimes\text{-Ind}_G^Q(\varrho) \\
\downarrow & & \downarrow \\
Q \wr S_n & \overset{(g,\text{id}_{S_n})}{\longrightarrow} & \text{Aut}(V) \wr S_n \overset{(\alpha,\psi)}{\longrightarrow} \text{Aut}(V^{\otimes n}),
\end{array}
\]

where \( \alpha : \text{Aut}(V)^{\otimes n} \to \text{Aut}(V^{\otimes n}) \) is given by \( \alpha(f_1, \ldots, f_n) = f_1 \otimes \cdots \otimes f_n \), and \( \psi : S_n \to \text{Aut}(V^{\otimes n}) \) by \( \sigma \mapsto [\psi(\sigma) : v_1 \otimes \cdots \otimes v_n \mapsto v_{1\sigma} \otimes \cdots \otimes v_{n\sigma}] \).

Example 2.2. Suppose \( Q \) is a subgroup of \( G \) index 2 and let \( \{1, \theta\} \) be representatives for the right cosets, then

\[
\begin{align*}
q_1(g) &= g, & q_2(g) &= \theta g \theta^{-1} & \text{if } g \in Q \\
q_1(g) &= \theta g^{-1}, & q_2(g) &= \theta g & \text{if } g \in G \setminus Q.
\end{align*}
\]

Thus,

\[
\otimes\text{-Ind}_G^Q(\varrho)(g) = \begin{cases} \varrho(g) \otimes \rho(\theta g \theta^{-1}) & g \in Q \\ [\varrho(g \theta^{-1}) \otimes \rho(\theta g)] \circ \psi(12) & g \in G \setminus Q. \end{cases}
\]

Proposition 2.3. Let \( Q \) be a subgroup of index 2 of \( G \) and \( \{1, \theta\} \) be representatives for the right cosets. If \( (V, \varrho) \) is an irreducible complex 2-dimensional representation of \( Q \) with projective image isomorphic to either \( A_4, S_4 \) or \( A_5 \), then the tensor induction

\[
(V^{[G:Q]}, \otimes\text{-Ind}_G^Q(\varrho))
\]

is reducible if and only if \( V^*(\lambda) \cong V^\theta \) for some character \( \lambda : Q \to \mathbb{C}^\times \). When that happens the decomposition type is \((3, 1)\).

Proof. If \( V^*(\lambda) \cong V^\theta \) then the tensor product factors as

\[
V \otimes V^\theta \cong \text{Ad}^0(V)(\lambda) \oplus \mathbb{C}(\lambda),
\]

where \( \text{Ad}^0(V) \) is irreducible ([3], Lemma 2.1). Frobenius reciprocity implies

\[
\text{Hom}_G(V^{[G:Q]}, \text{Ind}_G^Q(\lambda)) = \text{Hom}_Q(V \otimes V^\theta, \mathbb{C}(\lambda)) \neq 0,
\]
hence $V^\otimes[G:Q]$ is reducible. Since $(V^\otimes[G:Q])_|Q = V \otimes V^\theta$ has decomposition type $(3, 1)$, so does $V^\otimes[G:Q]$.

Now suppose $V^\otimes[G:Q]$ is reducible. If $V^\otimes[G:Q]$ contains a 1-dimensional subrepresentation then we claim that $V^\ast(\chi) \cong V^\theta$. Indeed, if $\mathbb{C}(\chi)$ is a subrepresentation of $V^\otimes[G:Q]$ then Frobenius reciprocity implies

$$0 \neq \text{Hom}_G(V^\otimes[G:Q], C(\chi)) \hookrightarrow \text{Hom}_Q(V \otimes V^\theta, \mathbb{C}(\chi|Q)).$$

We deduce that the tensor product $V \otimes V^\theta(\chi|Q)^{-1}$ has a non-zero $Q$-invariant vector, that is,

$$0 \neq H^0(Q, V \otimes V^\theta(\chi|Q)^{-1}) = \text{Hom}_Q(V^\ast(\chi|Q), V^\theta),$$

producing the isomorphism $V^\ast(\chi|Q) \cong V^\theta$ because $V$ is irreducible. By repeating the argument above we find that the decomposition type is $(3, 1)$. Finally suppose that $V^\otimes[G:Q]$ has decomposition type $(2, 2)$, then at least one of the irreducible components decomposes into a sum of characters when restricted to $Q$ ([3], Lemma 2.2). The contradiction is obtained by applying ([3], Lemma 2.1). □

3. Galois embedding problems

3.1. Cohomological computation

Let $F$ be a totally real number field, $\Sigma_0$ a finite set of places of $F$ disjoint from the set $\Sigma_\infty$ of archimedean places and the set $\Sigma_2$ of places above 2. For $\Sigma$ the complement of $\Sigma_0$, we let $G_{F,\Sigma}$ denote the Galois group of the maximal Galois extension $F_{\Sigma}$ of $F$ unramified outside $\Sigma$.

We consider $M/F$ a totally real quadratic extension unramified outside $\Sigma$, and for all $r \geq 1$ we give $\mathscr{C}_{2^r}$ the structure of $G_{F,\Sigma}$-module via the homomorphism $G_{F,\Sigma} \to G(M/F) \hookrightarrow \text{Aut}(\mathscr{C}_{2^r})$ taking the non-trivial element of $G(M/F)$ to the automorphism $x \mapsto x^{-1}$. We denote by

$$\mathcal{M}_2 := \lim_{\to, r} \mathscr{C}_{2^r}$$

the $G_{F,\Sigma}$-module obtained by taking the direct limit with respect to the natural inclusions $\mathscr{C}_{2^r} \to \mathscr{C}_{2^{r+1}}$. The dual Galois module is defined as

$$\mathscr{C}_{2^r}^\ast := \text{Hom}_{G_{F}}(\mathscr{C}_{2^r}, \mathcal{O}_{\Sigma}^\times),$$
where $\mathcal{O}_\Sigma$ is the ring of $\Sigma$-integers in $F_\Sigma$. As a $G_M$-module $\mathcal{C}_2^r$ is isomorphic to the group $\mu_{2^r}$ of $2^r$-th roots of unity with the natural Galois action, hence the field $M_r = M(\mu_{2^r})$ trivializes $\mathcal{C}_2^r$.

We are interested in analyzing the maps between the various kernels

$$\Pi^1(G_{F,\Sigma}, \mathcal{C}_2^r) := \ker \left( H^1(G_{F,\Sigma}, \mathcal{C}_2^r) \to \prod_{v \in \Sigma} H^1(F_v, \mathcal{C}_2^r) \right).$$

**Proposition 3.1.** For all $r \geq 2$ the map $(j'_r)_*: \Pi^1(G_{F,\Sigma}, \mathcal{C}_2^r) \to \Pi^1(G_{F,\Sigma}, \mathcal{C}_2^{r-2})$, induced by the dual of the natural inclusion $j_r: \mathcal{C}_2^{r-2} \to \mathcal{C}_2^r$, is zero.

**Proof.** We claim that the restriction

$$H^1(G_{M_r,\Sigma}, \mathcal{C}_2^r) \to \prod_{w \in \Sigma(M_r)} H^1(M_{r,w}, \mathcal{C}_2^r)$$

is injective, where the product is taken over all places of $M_r$ above a place in $\Sigma$. Indeed, if $\phi: G_{M_r} \to \mathcal{C}_2^r$ is in the kernel of the restriction map, then the field fixed by $\ker \phi$ is a Galois extension of $M_r$ in which the primes that split completely have density 1. Cebotarev’s density theorem implies that such extension is $M_r$ itself. By examining the commutative diagram

$$\begin{array}{ccc}
H^1(G_{M_r,\Sigma}, \mathcal{C}_2^r) & \to & \prod_{w \in \Sigma(M_r)} H^1(M_{r,w}, \mathcal{C}_2^r) \\
0 & \to & \Pi^1(G_{F,\Sigma}, \mathcal{C}_2^r) \\
0 & \to & \Pi^1(M_r/F, \mathcal{C}_2^r) \\
\end{array}$$

we see that $\Pi^1(G_{F,\Sigma}, \mathcal{C}_2^r) = \Pi^1(M_r/F, \mathcal{C}_2^r)$.

We claim that $\Pi^1(G_{F,\Sigma}, \mathcal{C}_2^r)$ is killed by multiplication by 4. Clearly, it suffices to prove that $H^1(M_r/F, \mathcal{C}_2^r)$ is killed by multiplication by 4. The
Growth of the analytic rank of modular elliptic curves

claim follows by considering the inflation-restriction exact sequence

\[ 0 \longrightarrow H^1(M/F, (\mathcal{C}'_{2r})^{G(M_r/M)}) \longrightarrow H^1(M_r/F, \mathcal{C}'_{2r}) \longrightarrow H^1(M_r/M, \mathcal{C}'_{2r}). \]

and noticing that both \( H^1(M/F, (\mathcal{C}'_{2r})^{G(M_r/M)}) \) and \( H^1(M_r/M, \mathcal{C}'_{2r}) \) are isomorphic to \( \mathbb{Z}/2\mathbb{Z} \) (Lemma 9.1.4 & Proposition 9.1.6). Now, there is a natural factorization of multiplication by 4 on \( \mathcal{C}'_{2r} \),

which induces the commutative diagram

\[
\begin{array}{ccc}
\mathcal{C}'_{2r} & \xrightarrow{[4]^*} & \mathcal{C}'_{2r} \\
\downarrow{j^*} & & \downarrow{(4)^*} \\
\mathcal{C}'_{2r-2} & \xrightarrow{(4')^*} & \mathcal{C}'_{2r-2} \\
\end{array}
\]

Therefore to complete the proof we need to show that \( \text{III}^1(G_{F,\Sigma}, \mathcal{C}'_{2r-2}) \) does not intersect \( \ker((4)^*) \) because it would provide the required inclusion \( \text{III}^1(G_{F,\Sigma}, \mathcal{C}'_{2r}) \subset \ker([j^*]) \). The exact sequence of \( G_{F,\Sigma} \)-modules

\[ 1 \longrightarrow \mathcal{C}'_{2r-2} \xrightarrow{(4')^*} \mathcal{C}'_{2r} \longrightarrow \mathcal{C}'_{2r} \longrightarrow 1 \]

produces the exact sequence of cohomology groups

\[ 1 \longrightarrow C_2 = H^0(G_{F,\Sigma}, \mathcal{C}'_{2r}) \xrightarrow{\delta} H^1(G_{F,\Sigma}, \mathcal{C}'_{2r-2}) \xrightarrow{(4')^*} H^1(G_{F,\Sigma}, \mathcal{C}'_{2r}) \]

because any complex conjugation in \( G_{F,\Sigma} \) acts by inversion and gives the equality \( \delta(H^0(G_{F,\Sigma}, \mathcal{C}'_{2r})) = \ker((4)^*) \). Finally, for every real place \( v \in \Sigma_\infty \) the connecting homomorphism

\[ \delta_v : C_2 = H^0(\mathbb{R}, \mathcal{C}'_{2r}) \hookrightarrow H^1(\mathbb{R}, \mathcal{C}'_{2r-2}) \]

is injective. In particular, the non-trivial class of \( \delta(H^0(G_{F,\Sigma}, \mathcal{C}'_{2r})) \) is not locally trivial at the real places. \( \square \)
Lemma 3.2. Let \( v \) be a place of \( F \), then the Galois cohomology group \( H^2(F_v, \mathcal{M}_2) \) is trivial.

**Proof.** If \( v \) splits in \( M/F \) then \( G_{F_v} \) acts trivially on \( \mathcal{M}_2 \) and we can refer to Tate’s Theorem ([12], Theorem 4). If \( v \) is inert or ramified (so non-archimedean under our assumptions), then \( G_K \) has cohomological dimension 2 and \( H^2(F_v, \mathcal{M}_2) \) is 2-divisible. The claim follows by noting that multiplication by 2 factors through \( H^2(M_v, \mathcal{M}_2) \) which is trivial because \( \mathcal{M}_2 \) is a trivial \( G_{M_v} \)-module. \( \square \)

Theorem 3.3. Let \( F \) be a totally real number field, \( \Sigma_0 \) a finite set of places of \( F \) disjoint from the set \( \Sigma_\infty \) of archimedean places and the set \( \Sigma_2 \) of places above 2. For \( \Sigma \) the complement of \( \Sigma_0 \), we consider \( M/F \) a totally real quadratic extension unramified outside \( \Sigma \). Then \( H^2(G_{F,\Sigma}, \mathcal{M}_2) = 0 \).

**Proof.** By Lemma 3.2 it suffices to show that the restriction morphism
\[
H^2(G_{F,\Sigma}, \mathcal{M}_2) \to \bigoplus_{v \in \Sigma} H^2(F_v, \mathcal{M}_2)
\]
is injective. For every \( r \geq 2 \), consider the exact sequence
\[
0 \longrightarrow \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^r}) \longrightarrow H^2(G_{F,\Sigma}, \mathcal{C}_{2^r}) \longrightarrow \bigoplus_{v \in \Sigma} H^2(F_v, \mathcal{C}_{2^r}).
\]

Poitou-Tate duality ([12], Theorem 8.6.7) gives a commuting diagram
\[
\begin{array}{ccc}
\prod^1(G_{F,\Sigma}, \mathcal{C}_{2^r}) & \times & \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^r}) \\
\downarrow j_r & & \downarrow j_r \\
\prod^1(G_{F,\Sigma}, \mathcal{C}_{2^{r-1}}) & \times & \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^{r-1}}) \\
Q/\mathbb{Z}
\end{array}
\]
which in combination with Proposition 3.1 shows that
\[
j_r: \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^{r-1}}) \to \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^r})
\]
is zero because the pairings are perfect. Since direct limits are exact and commute with direct sums the following sequence is exact as well
\[
0 = \lim_{r \to} \prod^2(G_{F,\Sigma}, \mathcal{C}_{2^r}) \longrightarrow H^2(G_{F,\Sigma}, \mathcal{M}_2) \longrightarrow \bigoplus_{v \in \Sigma} H^2(F_v, \mathcal{M}_2). \qed
\]
3.2. Galois embedding problem

Let $n \geq 4$, $r \geq 1$ be integers. The symmetric group $S_n$ acts trivially on $\mathcal{C}_2$, and it is a classical computation that

$$H^2(S_n, \mathcal{C}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad H^2(A_n, \mathcal{C}_2) \cong \mathbb{Z}/2\mathbb{Z}.$$ 

We consider a class

$$[\omega] := \begin{bmatrix} 1 \to \mathcal{C}_2 \to \Omega \to S_n \to 1 \end{bmatrix} \in H^2(S_n, \mathcal{C}_2)$$

that does not belong to the kernel of the restriction map $H^2(S_n, \mathcal{C}_2) \to H^2(A_n, \mathcal{C}_2)$. Let $F$ be a totally real number field. A $S_n$-Galois extension $J/F$, ramified at a finite set $\Sigma_{\text{ram}}$ of places of $F$, determines a surjection $e : G_{F,\Sigma} \to S_n$ where $\Sigma$ is the complement of any finite set $\Sigma_0$ of places of $F$ disjoint from $\Sigma_{\text{ram}} \cup \Sigma_{\infty} \cup \Sigma_2$. We denote by $M = J^{A_n}$ the fixed field by $A_n$.

**Theorem 3.4.** Suppose the quadratic extension $M/F$ cut out by $A_n$ is totally real. For all $[\omega] \in H^2(S_n, \mathcal{C}_2)$ restricting to the universal central extension of $A_n$ it is possible to embed $J/F$ into a Galois extension $H/F$ unramified outside $\Sigma$, such that the Galois group $G(H/F)$ represents the non-trivial extension $i_r * [\omega]$ of $S_n$ by the $S_n$-module $\mathcal{C}_2$ for some $r \gg 0$.

**Proof.** Let $i_r : \mathcal{C}_2 \hookrightarrow \mathcal{C}_{2r}$ be the natural inclusion. The obstruction to the solution of the Galois embedding problem is encoded in the cohomology class $e^* i_r * [\omega] \in H^2(G_{F,\Sigma}, \mathcal{C}_{2r})$. Indeed, the triviality of the cohomology class is equivalent to the existence of a continuous homomorphism $\gamma : G_{F,\Sigma} \to \Omega_r$ such that the following diagram commutes

$$\begin{array}{cccccc}
1 & \longrightarrow & \mathcal{C}_{2r} & \longrightarrow & e^* \Omega_r & \longrightarrow & G_{F,\Sigma} & \longrightarrow & 1 \\
\gamma & \downarrow & \uparrow & \gamma & \downarrow & e & \downarrow & \downarrow & e^* i_r * [\omega] \\
1 & \longrightarrow & \mathcal{C}_2 & \longrightarrow & \Omega_r & \longrightarrow & S_n & \longrightarrow & 1.
\end{array}$$

The homomorphism $\gamma$ need not be surjective, but it still defines a non-trivial extension of $S_n$ by a submodule of $\mathcal{C}_2$, because $\Omega_r$ is a non-trivial extension. Indeed the non-triviality of the class $i_r * [\omega]$ follows by the commutativity of
the following diagram

\[
\begin{array}{ccc}
H^2(S_n, \mathbb{C}_2) & \xrightarrow{i_*} & H^2(S_n, \mathbb{C}_{2r}) \\
\downarrow & & \downarrow \\
H^2(A_n, \mathbb{C}_2) & \xrightarrow{i_*} & H^2(A_n, \mathbb{C}_{2r})
\end{array}
\]

because by hypothesis the restriction of \([\omega]\) to \(H^2(A_n, \mathbb{C}_2)\) is non-zero and the lower horizontal arrow is injective as \(H^1(A_n, \mathbb{C}_{2-1}) = 0\) for \(n \geq 4\). Finally, the obstruction to the solution of the Galois embedding problem vanishes for \(r \gg 0\) because by Theorem 3.3

\[
\lim_{r \to \infty} H^2(G_{F, \Sigma}, \mathbb{C}_2^*) = H^2(G_{F, \Sigma}, \mathbb{M}_2) = 0.
\]

\[\square\]

4. On Artin representations

Let \(K/F\) be a \(S_5\)-quintic extension ramified at a finite set \(\Sigma_{\text{ram}}\) of places of \(F\). Suppose the Galois closure \(J\) is totally complex and that the subfield of \(J\) fixed by \(A_5\) is a totally real quadratic extension \(M/F\). Let \(\Sigma\) be the complement of a finite set \(\Sigma_0\) disjoint from \(\Sigma_{\text{ram}} \cup \Sigma_{\infty} \cup \Sigma_2\).

The simple group \(A_5\) does not admit any irreducible complex 2-dimensional representation. However, there are two conjugacy classes of embeddings of \(A_5\) into \(\text{PGL}_2(\mathbb{C})\). We fix one such embedding and we consider the projective representation

\[G_{M, \Sigma} \to G(J/M) \cong A_5 \subset \text{PGL}_2(\mathbb{C}).\]

We are interested in finding a lift with specific properties. Consider the double cover \(\Omega_5^+\) of \(S_5\) where transpositions lift to involutions, and that restricts to the universal central extension of \(A_5\). By Theorem 3.4 there exists a positive integer \(r\) and a Galois extension \(H/F\), unramified outside \(\Sigma\) and containing \(J/F\), such that the sequence

\[
1 \longrightarrow \mathbb{C}_{2r} \longrightarrow G(H/F) \longrightarrow G(J/F) \longrightarrow 1
\]

is exact. Given our choice of the double cover \(\Omega_5^+\), transpositions of \(S_5 \cong G(J/F)\) lift to element of order 2 of \(G(H/F)\) and their conjugation action on \(\mathbb{C}_{2r}\) is by inversion: \(x \mapsto x^{-1}\). Let \(A_5\) denote the universal central extension
of $A_5 \cong \tilde{A}_5/\{\pm 1\}$. Complex 2-dimensional representations of the group

$$G(H/M) \cong (C_2 \times \tilde{A}_5)/((-1,-1))$$

are constructed by tensoring a character of $C_2r$ with a complex 2-dimensional representation of $\tilde{A}_5$ taking the same value at $-1$. We consider a representation

$$\varrho_K : G_{M, \Sigma} \to GL_2(\mathbb{C})$$

obtained by composing the quotient map $G_{M, \Sigma} \to G(H/M)$ with any irreducible complex 2-dimensional representation of $G(H/M)$.

**Remark 4.1.** Since the abelianization of $\tilde{A}_5$ is trivial, there is a dihedral Galois extension $D/F$ such that $\det(\varrho_K)$ factors through the quotient by the subgroup

$$G(H/D) \cong (C_2 \times \tilde{A}_5)/((-1,-1)).$$

Therefore, the composition of the determinant with the transfer map, $\det(\varrho_K) \circ V : G_F \to \mathbb{C}^\times$, is the trivial character.

**Proposition 4.2.** The tensor induction

$$\otimes\text{Ind}^F_M(\varrho_K) : G_F \to GL_4(\mathbb{C})$$

factors through $G_J$ and induces a faithful representation

$$\otimes\text{Ind}^F_M(\varrho_K) : S_5 \to GL_4(\mathbb{C})$$

isomorphic to the standard representation of $S_5$.

**Proof.** By construction the action by conjugation of $G(J/F)$ on $G(H/J)$ factors through $G(M/F)$ and sends every element to its inverse. Let $\theta \in G_F$ be an element mapping to a transposition in $G(J/F) \cong S_5$, then

$$\ker (\otimes\text{Ind}^F_M(\varrho_K)) \cap G_M$$

$$= \ker \left( \varrho_K \otimes (\varrho_K) \theta \right)$$

$$= \{ h \in G_M \mid \exists \alpha \in \mathbb{C}^\times \text{ with } \varrho_K(h) = \alpha^2, \varrho_K(h) = \alpha^{-1}I_2 \}$$

$$= G_J.$$ 

Thus, $\otimes\text{Ind}^F_M(\varrho_K)$ induces a 4-dimensional representation

$$\otimes\text{Ind}^F_M(\varrho_K) : S_5 \to GL_4(\mathbb{C}).$$
By Proposition 2.3 $\otimes$-Ind$^F_M(\varrho_K)$ has either decomposition type $(3, 1)$ or it is irreducible. It follows that it has to be irreducible because $S_5$ does not admit irreducible complex representations of dimension 3. Finally, $S_5$ has only two irreducible complex 4-dimensional representations: the standard representation and its twist by the sign character sign : $S_5 \to \{\pm 1\}$. One can distinguish between them by computing the trace of transpositions.

Recall that our input was the central extension $\Omega^+_{5}$ of $S_5$ chosen because transpositions of $S_5$ lift to involutions. Therefore $\theta^2 \in G_H$ and $\varrho_K(\theta^2) = \mathbb{1}_2$, and we can compute that

$$\otimes$-Ind$^F_M(\varrho_K)(\theta) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}$$

has trace equal to 2. □

**Corollary 4.3.** Let $K/F$ be a $S_5$-quintic extension whose Galois closure $J$ is totally complex and contains a totally real quadratic extension $M/F$. Let $\Sigma$ be the complement of any finite set $\Sigma_0$ of places of $F$ disjoint from $\Sigma_{\text{ram}} \cup \Sigma_{\infty} \cup \Sigma_2$, then there exists a totally odd 2-dimensional Artin representation $\varrho_K : G_{M, \Sigma} \to GL_2(\mathbb{C})$ such that

$$\otimes$-Ind$^F_M(\varrho_K) \cong \text{Ind}_K^F \mathbb{1} - \mathbb{1}.$$

**Proof.** Thanks to Proposition 4.2 we only have to check that the representation $\varrho_K : G_{M, \Sigma} \to GL_2(\mathbb{C})$ considered there is totally odd. By assumption the Galois closure $J$ is totally complex, thus the projectivization of $\varrho_K$ is a faithful representation of $G(J/M)$, which contains every complex conjugation of $M$. □

5. Growth of the analytic rank

Let $M/F$ be a quadratic extension of totally real number fields, $E_{1,F}$ a modular elliptic curve of conductor $N$, and $g$ a primitive Hilbert cuspform over $M$ of parallel weight one and level $\Omega$. Attached to this data, there is a unitary cuspidal automorphic representation $\Pi = \Pi_{g,E}$ of the algebraic group $G = \text{Res}_{M \times F/F}(GL_{2,M \times F})$. Let $\phi : G_F \to S_3$ be the homomorphism mapping the absolute Galois group of $F$ to the symmetric group over 3 elements associated with the étale cubic algebra $(M \times F)/F$. The $L$-group
$L^G$ is given by the semi-direct product $GL_2(\mathbb{C})^3 \rtimes G_F$ where $G_F$ acts on the first factor through $\phi$.

**Definition 5.1.** The twisted triple product $L$-function associated with the unitary automorphic representation $\Pi$ is given by the Euler product

$$L(s, \Pi, r) = \prod_v L_v(s, \Pi_v, r)^{-1}$$

where $\Pi_v$ is the local representation at the place $v$ of $F$ appearing in the restricted tensor product decomposition $\Pi = \bigotimes_v \Pi_v$, and $r$ describes the action of $L^G$ on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ which restricts to the natural 8-dimensional representation of $GL_2(\mathbb{C})^3$ and for which $G_F$ acts via $\phi$ permuting the vectors.

**Remark 5.2.** ([8], page 111). When $\Pi_v$ is ramified, let $q_v$ be the cardinality of the residue field of $F_v$, then the local $L$-factor at $v$ of $L(s, \Pi, r)$ is given by

$$L_v\left(\frac{1+s}{2}, \Pi_v, r\right) = P_v(q_v^{-s})$$

for a certain polynomial $P_v(X) \in 1 + X\mathbb{C}[X]$. In particular, it is non-vanishing at $s = 1/2$.

Assume the central character $\omega_{\Pi}$ of $\Pi$ is trivial when restricted to $A_F^\times$, then the complex $L$-function $L(s, \Pi, r)$ has meromorphic continuation to $\mathbb{C}$ with possible poles at $0, \frac{1}{4}, \frac{3}{4}, 1$ and functional equation

$$L(s, \Pi, r) = \epsilon(s, \Pi, r)L(1-s, \Pi, r)$$

([8], Theorems 5.1, 5.2, 5.3). When all the primes dividing $\mathfrak{N}$ are unramified in $M/F$ and $(\mathfrak{N}, \mathfrak{Q}) = 1$, the sign of the functional equation can be computed as follows ([10], Theorems B, D & Remark 4.1.1):

write $\mathfrak{N} = \mathfrak{N}^+\mathfrak{N}^-$, where $\mathfrak{N}^-$ is the square-free part of $\mathfrak{N}$. If all the prime factors of $\mathfrak{N}^+$ are split in $M/F$, then the sign of the functional equation is determined by the number of prime divisors of $\mathfrak{N}^-$ which are inert in $M/F$

$$\epsilon\left(\frac{1}{2}, \Pi, r\right) = \left(\frac{M/F}{\mathfrak{N}^-}\right)$$.
Theorem 5.3. Let $E/F$ be a modular elliptic curve of odd conductor $\mathfrak{N}$ and let $K/F$ be a $S_5$-quintic extension with totally complex Galois closure $J$. Suppose $J$ is unramified at $\mathfrak{N}$ and contains a totally real quadratic extension $M/F$, then the ratio of $L$-functions

$$L(E/K, s)/L(E/F, s)$$

has meromorphic continuation to the whole complex plane and it is holomorphic at $s = 1$. Furthermore, if all prime factors of $\mathfrak{N}^+$ are split in $M/F$, then

$$\text{ord}_{s=1} \frac{L(E/K, s)}{L(E/F, s)} \equiv 1 \pmod{2} \iff \left( \frac{M/F}{\mathfrak{N}^+} \right) = -1.$$

Proof. By Corollary 4.3 and the modularity of totally odd Artin representations of the absolute Galois group of totally real number fields ([9], Theorem 0.3), there is a primitive Hilbert cuspform $g$ of parallel weight one over $M$, and level $Q$ prime to $N$, such that $\varrho_g = \varrho_K$. A direct inspection of the Euler product of the twisted triple product $L$-function $L(s, \Pi, r)$ attached to $\Pi = \Pi_{g, E}$ produces the equality of incomplete $L$-functions

$$L_S(s, \Pi, r) = L_S\left( E, \otimes \text{Ind}_{M/F}^E(g), s + \frac{1}{2} \right) = \frac{L_S(E/K, s + \frac{1}{2})}{L_S(E/F, s + \frac{1}{2})},$$

where $S$ is any finite set containing the primes dividing $\mathfrak{N}Q$ and the primes that ramify in $M/F$. As Remark 4.1 ensures the triviality of the central character $\omega_{\Pi}$ when restricted to $\mathbb{A}_F^\times$; meromorphic continuation, holomorphicity at the center and the criterion for the parity of the order of vanishing at the center of $L(E/K, s)/L(E/F, s)$ follow. □

Corollary 5.4. Let $E/F$ be an elliptic curve of odd conductor $\mathfrak{N}$ and at least one prime of multiplicative reduction. Denote by $G_5(E/F; X)$ the number of quintic extensions $K$ of $F$ such that the norm of the relative discriminant is at most $X$ and the analytic rank of $E$ grows over $K$, i.e., $r_{an}(E/K) > r_{an}(E/F)$. Then $G_5(E; X) \asymp_{+\infty} X$.

Proof. By Theorem 5.3, $G_5(E/F; X)$ contains all $S_5$-quintic extension $K/F$ such that their Galois closure is totally complex, they contain a totally real quadratic extension of $F$, the prime divisors of $\mathfrak{N}$ are unramified in $K$ and have certain splitting behaviour. Then $G_5(E/F; X) \gg_{+\infty} X$ by ([1], Theorem 2), and $X \gg_{+\infty} G_5(E/F; X)$ by ([1], Theorem 1). □
Acknowledgements

This work would not have been possible without the constant guidance and support of my Ph.D. advisors Henri Darmon and Adrian Iovita. I would like to thank Jan Vonk for pointing out the relevance of the author’s work for statistical questions about elliptic curves, and I am grateful to Chantal David and Hershy Kisilevsky for useful comments on a first draft of the paper. Finally, I would like to thank the anonymous referee for the valuable feedback on the paper.

References


McGill University, Montreal QC H3A 0B9, Canada
E-mail address: michele.fornea@mail.mcgill.ca

Received March 21, 2018