Journal de Théorie des Nombres de Bordeaux

David S. Dummit
Jonathan W. Sands
Brett Tangedal

Stark's conjecture in multi-quadratic extensions, revisited

Journal de Théorie des Nombres de Bordeaux, tome 15, nº 1 (2003), p. 83-97
<http://www.numdam.org/item?id=JTNB_2003__15_1_83_0>

Journal de Théorie des Nombres
de Bordeaux **15** (2003), 83–97

Stark's conjecture in multi-quadratic extensions, revisited

par DAVID S. DUMMIT*, JONATHAN W. SANDS*
et BRETT TANGEDAL

RÉSUMÉ. Les conjectures de Stark relient les unités spéciales dans les corps de nombres à certaines valeurs des fonctions L attachées à ces corps. Nous considérons le cas d'une extension abélienne, et nous établissons la relation fondamentale de la conjecture de Stark lorsque son groupe de Galois est d'exposant 2. Nous montrons que la conjecture est entièrement vérifiée pour les extensions biquadratiques ainsi que dans de nombreux autres cas.

ABSTRACT. Stark's conjectures connect special units in number fields with special values of L-functions attached to these fields. We consider the fundamental equality of Stark's refined conjecture for the case of an abelian Galois group, and prove it when this group has exponent 2. For biquadratic extensions and most others, we prove more, establishing the conjecture in full.

1. The elements of Stark's refined abelian conjecture

Units. Let:

- L/F be an abelian extension of number fields in which a distinguished (finite or infinite) prime of F denoted by $\mathfrak{v}$ splits completely. These and all number fields will be assumed to lie in a fixed algebraic closure $\overline{\mathbb{Q}}$ of the field $\mathbb{Q}$ of rational numbers.
- $|\ |_{\mathfrak{w}}$ be the normalized absolute value at a fixed prime $\mathfrak{w}$ of L above $\mathfrak{v}$.
- w_L be the order of the group μ_L of roots of unity in L.
- $U_L^{(\mathfrak{v})}$ be the group of elements of L having absolute value equal to 1 at each (finite or infinite) absolute value of L except for those associated with primes above $\mathfrak{v}$, in other words, those which are conjugates of $|\ |_{\mathfrak{w}}$. We sometimes refer to $U_L^{(\mathfrak{v})}$ as the $\mathfrak{v}$-units of L.

Manuscrit reçu le 3 décembre 2001.
* Research supported by NSF grant DMS 9624057 and NSA grant MDA 904-00-1-0024.

L-functions. Let:

- G be the abelian Galois group of the extension L/F.
- $\hat{G}$ be the character group of G.
- S be a fixed finite set of primes of F of cardinality $|S| \geq 3$, and assume that S contains $\mathfrak{v}$, all finite primes which ramify in L/F, and all infinite primes. The Stark conjecture we are concerned with must be formulated differently when $|S| = 2$, and is known to be true in this case by [4] and [5].
- $S^0 = S - \{\mathfrak{v}\}$.
- S_{fin} = the set of finite primes in S.
- $\mathfrak{p}$ run through the finite primes of F not in S.
- $\mathfrak{a}$ run through integral ideals of F, prime to the elements of S.
- $\mathbf{N}\mathfrak{a}$ denote the absolute norm of the ideal $\mathfrak{a}$.
- $\sigma_{\mathfrak{a}} \in G$ be the well-defined automorphism attached to $\mathfrak{a}$ via the Artin map.

For each $\chi \in \hat{G}$, we have the Artin L-function with Euler factors at the primes in S removed:

$$L_S(s,\chi) = \sum_{\substack{\mathfrak{a} \text{ integral} \\ (\mathfrak{a},S)=1}} \frac{\chi(\sigma_{\mathfrak{a}})}{\mathbf{N}\mathfrak{a}^s} = \prod_{\text{prime } \mathfrak{p} \notin S} \left(1 - \frac{\chi(\sigma_{\mathfrak{p}})}{\mathbf{N}\mathfrak{p}^s}\right)^{-1}.$$

It is known that $L_S(s,\chi)$ has an analytic continuation and a functional equation relating it to $L_S(1-s,\overline{\chi})$. The order of its zero at $s = 0$ is

$$r_S(\chi) = \begin{cases} |S| - 1 \\ |\{\mathfrak{q} \in S : \mathfrak{q} \text{ splits completely in the field} \\ \qquad\qquad\qquad\qquad \text{fixed by the kernel of } \chi\}| \end{cases}$$

depending on whether or not χ is the trivial character χ_0. See [5] for further background and references.

The conjecture. We first single out the key equality in Stark's refined abelian conjecture for first derivatives of L-functions which posits the existence of a special $\mathfrak{v}$-unit ϵ serving as an "L-function evaluator."

Conjecture $\mathrm{St}'(L/F,S)$. *There exists an element (often called a "Stark unit") $\epsilon \in U_L^{(\mathfrak{v})}$ such that*

$$L'_S(0,\chi) = -\frac{1}{w_L} \sum_{\sigma \in G} \chi(\sigma) \log(|\varepsilon^{\sigma}|_{\mathfrak{w}}) \quad \textit{for all } \chi \in \hat{G}.$$

Remark 1. The conditions on ϵ specify all of its absolute values and thus determine ε up to a root of unity in L. This ambiguity still remains when we impose Stark's additional condition below. Nevertheless, we sometimes refer to ε as "the" Stark unit.

The full Stark conjecture in this setting (cf. [4], [5]) says more.

Conjecture St(L/F,S). *St′(L/F,S) holds, and furthermore $L(\epsilon^{1/w_L})/F$ is an abelian Galois extension.*

2. Statements of the results

We assume from now on that there are at least 2 infinite primes ∞_1, ∞_2 in S. Otherwise St(L/F,S) is known to be true by [4] (see also [5,IV.3.9]). We may then assume that $\infty_2 \neq \mathfrak{v}$. Also assume from now on that $G = \mathrm{Gal}(L/F)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some positive integer m. We then call L/F a multiquadratic extension of rank m.

Our aim in this paper is to prove the following theorems.

Theorem 1. *Let $S_{fin} \subset S$ consist of the finite primes in S, and let $r_F(S)$ denote the 2-rank of the S_{fin}-class group of F. If $|S| > m + 1 - r_F(S)$, then St(L/F,S) holds for the multiquadratic extension L/F.*

Theorem 2. *St′(L/F,S) holds for the multiquadratic extension L/F, hence for an arbitrary multiquadratic extension.*

Theorem 3. *St(L/F, S) holds for the multiquadratic extension L/F if $\mathfrak{v}$ is a real infinite prime or a finite prime, except possibly when L is the maximal multiquadratic extension of F which is unramified outside of S and in which $\mathfrak{v}$ splits completely.*

Theorem 4. *St(L/F, S) holds for the multiquadratic extension L/F when the rank of this extension is $m = 2$, i.e. L/F is biquadratic. Thus it holds for an arbitrary biquadratic extension.*

Remark 2. St(L/F, S) was proved for the multiquadratic extension L/F in [2] and [3] under the assumption that either $|S| > m + 1$, or that no prime above 2 (i.e. no dyadic prime) is ramified in L/F.

3. The relative quadratic case

Assume K/F is a relative quadratic extension. This section summarizes some basic results from [3] and [5] on St(K/F,S).

We set:

- $\mathrm{Gal}(K/F) = \langle\tau\rangle$ of order 2.
- $\eta_K = 1$ if S contains two split primes of K/F.
- η_K = generator of the infinite cyclic group $U_K^{(\mathfrak{v})}/\mu_K$ with $|\eta_K|_{\mathfrak{w}} < 1$, otherwise. Note that since ∞_2 does not split in this case, we may also describe $U_K^{(\mathfrak{v})}$ as the S-units u of K such that $u^{1+\tau}$=1. If $\mathfrak{w}$ is a real infinite prime, choose η_K to be positive in the embedding induced by

$\mathfrak{w}$. Since $\eta_K^{1+\tau} = 1$, this then implies that η_K is positive at both of the primes above $\mathfrak{v}$.

- $\mathrm{Cl}_F(S) = \mathrm{Cl}_F(S_{fin}) = S_{fin}$-ideal class group of F, the quotient of the ideal class group $\mathrm{Cl}(F)$ of F by the subgroup generated by the ideal classes of the primes in S_{fin}.
- $S_K =$ the set of primes of K lying above those in S.
- $\mathrm{Cl}_K(S) = S_K$-ideal class group of K.
- $H_K = H_K(S) = \mathrm{Cl}_K(S)/\iota(\mathrm{Cl}_F(S))$, the cokernel of the map ι induced by extension of ideals.
- $M_K = M_K(S) = |H_K|$, the order of this group.

Theorem (Stark-Tate, cf. [Ta, IV.5.4]). *St(K/F,S) holds with Stark unit*

$$\varepsilon_K = \eta_K^{M_K \cdot 2^{|S|-3}},$$

and $K(\eta_K{}^{1/w_K})/F$ is abelian.

Remark 3. The extra factor e^+ in [5, IV.5.4] equals 1 when $\eta_K \neq 1$ as this implies that the infinite prime ∞_2 of F does not split in K.

4. Passage to the multiquadratic case via L-function properties

We have assumed that L/F is multiquadratic with the distinguished prime $\mathfrak{v}$ of F splitting completely in L, and that $\infty_2 \neq \mathfrak{v}$ is an infinite prime of F. From now on, we also assume that:

- ∞_2 does not split completely in L/F. (Otherwise $\mathrm{St}(L/F)$ is trivially true with $\varepsilon = 1$.)
  Let:
- $\tau =$ complex conjugation at ∞_2 in L/F.
- K_i for $i = 1, 2, \ldots, 2^{(m-1)}$ be the relative quadratic extensions of F in L which are not fixed by τ. (These generate L.)
- $\eta_i = \eta_{K_i}$.
- $M_i = M_{K_i}$.
- $w_i = w_{K_i}$.

Proposition 1. *If*

$$\varepsilon = \prod_{i=1}^{2^{m-1}} \eta_i^{M_i \cdot 2^{|S|-m-2}(w_L/w_i)}$$

lies in L, then it is the Stark unit ε_L satisfying St'(L/F,S).

Proof. (This is a straightforward adaptation of the proof of Theorem 2.6 of [3].) Clearly $\varepsilon \in U_L^{(\mathfrak{v})}$ because each $\eta_i \in U_{K_i}^{(\mathfrak{v})} \subset U_L^{(\mathfrak{v})}$. In particular, $\varepsilon^{1+\tau} = 1$ because this represents the absolute value of ε above ∞_2. We now show that ε is an L-function evaluator.

Fix an arbitrary character $\chi \in \hat{G}$. If $\chi(\tau) = 1$, then $r_S(\chi) > 1$ by the formula for this quantity, and therefore $L'_S(\chi, 0) = 0$. At the same time,

$$-\frac{1}{w_L}\sum_{\sigma\in G}\chi(\sigma)\log(|\varepsilon^{\sigma}|_{\mathfrak{w}}) = -\frac{1}{2}\frac{1}{w_L}\sum_{\sigma\in G}\chi(\sigma)\log(|\varepsilon^{(1+\tau)\sigma}|_{\mathfrak{w}}) = 0,$$

by the observation in the last paragraph. So ε is an L-function evaluator for this type of χ.

Now suppose that $\chi(\tau) = -1$. The fixed field of the kernel of χ must then be one of the K_i for some $i = i(\chi)$. Letting $G_i = \mathrm{Gal}(L/K_i)$, we observe that

$$\sum_{\sigma\in G_i}\chi(\sigma) = \begin{cases} 2^{m-1}, & \text{if } i = i(\chi) \\ 0, & \text{otherwise.}\end{cases}$$

We use the definition of ε, the fact that $\chi(\tau) = -1$, and the fact that G_i fixes η_i, along with the evaluation of the last sum and finally the Stark-Tate theorem for relative quadratic extensions and the inflation property of Artin L-functions to see that

$$\begin{aligned}
-\frac{1}{w_L}\sum_{\sigma\in G}\chi(\sigma)\log(|\varepsilon^{\sigma}|_{\mathfrak{w}}) &= -\frac{1}{w_L}\sum_{\sigma\in G}\frac{1}{2^{m-1}} \\
&\qquad\times\sum_{i=1}^{2^{m-1}}\chi(\sigma)(w_L/w_i)\log(|\eta_i^{M_i 2^{|S|-3}\sigma}|_{\mathfrak{w}}) \\
&= \sum_{i=1}^{2^{m-1}}\frac{-1}{w_i}\frac{1}{2^{m-1}}\sum_{\sigma\in G}\chi(\sigma)\log(|\eta_i^{M_i 2^{|S|-3}\sigma}|_{\mathfrak{w}}) \\
&= \sum_{i=1}^{2^{m-1}}\frac{-1}{w_i}\frac{1}{2^{m-1}}\sum_{\sigma\in G_i}\chi(\sigma)\log(|\eta_i^{M_i 2^{|S|-3}(1-\tau)\sigma}|_{\mathfrak{w}}) \\
&= \sum_{i=1}^{2^{m-1}}\frac{-1}{w_i}\frac{1}{2^{m-1}}\sum_{\sigma\in G_i}\chi(\sigma)\log(|\eta_i^{M_i 2^{|S|-3}(1-\tau)}|_{\mathfrak{w}}) \\
&= \frac{-1}{w_{i(\chi)}}\log(|(\eta_{i(\chi)}^{M_{i(\chi)}2^{|S|-3}})^{(1-\tau)}|_{\mathfrak{w}}) = L'_S(0,\chi).
\end{aligned}$$

So ε is an L-function evaluator for this type of χ as well, and the proof is complete. □

5. Class field theory

Recall that $H_K = \mathrm{Cl}_K(S)/\iota(\mathrm{Cl}_F(S))$.

Proposition 2. *Let K be any of the K_i for which $\eta_i \neq 1$. Then* $\mathrm{rank}_2(H_K) \geq \mathrm{rank}_2(\mathrm{Cl}_F(S)) = r_F(S)$, *with equality holding if* $|S| = 3$.

Proof. We will show that the norm map induces a surjective homomorphism $H_K/H_K^2 \to \mathrm{Cl}_F(S)/\mathrm{Cl}_F(S)^2$ which is an isomorphism when $|S| = 3$.

The assumption that $\eta_i \neq 1$ implies that ∞_2 and the other primes of S^0 do not split in K/F. Thus the complex conjugation τ at ∞_2 restricts to a generator of $\mathrm{Gal}(K/F)$.

Let I_K denote the group of fractional ideals of K, P_K denote the subgroup of principal fractional ideals, and $\tilde{I_F}$ denote the subgroup of fractional ideals of K which are extended from fractional ideals of F. Also let $S_{\mathrm{fin}}(K)$ denote the set of ideals of K which lie above those in S_{fin}. This contains all of the ideals of K which are ramified over F. From the factorization of ideals into primes, we see that $\tilde{I_F}\langle S_{\mathrm{fin}}(K)\rangle = I_K^{1+\tau} J_K \langle S_{\mathrm{fin}}(K)\rangle$, where J_K denotes the group generated by the prime ideals of K which are inert over F. Then

$$\begin{aligned} H_K/H_K^2 \cong I_K/P_K I_K^2 \tilde{I_F}\langle S_{\mathrm{fin}}(K)\rangle &= I_K/P_K I_K^2 I_K^{1+\tau} J_K \langle S_{\mathrm{fin}}(K)\rangle \\ &= I_K/P_K I_K^2 I_K^{\tau-1}\langle S_{\mathrm{fin}}(K)\rangle J_K. \end{aligned}$$

Under the Artin map of class field theory, I_K/P_K ($= \mathrm{Cl}_K$) corresponds to the maximal unramified abelian extension (Hilbert Class Field) $\mathcal{H}$ of K, in the sense that this map induces an isomorphism of I_K/P_K with $\mathrm{Gal}(\mathcal{H}/K)$. From this it is clear that $I_K/P_K I_K^2$ corresponds to the maximal abelian unramified elementary 2-extension of K in the same way. Similarly, $I_K/P_K I_K^2 I_K^{\tau-1}$ corresponds to the maximal abelian unramified elementary 2-extension $\mathcal{F}$ of K having the property that τ acts (by conjugation) trivially on $\mathrm{Gal}(\mathcal{F}/K)$. By maximality, $\mathcal{F}/F$ is Galois.

Let $G_{\mathcal{F}} = \mathrm{Gal}(\mathcal{F}/F)$ and $N_{\mathcal{F}} = \mathrm{Gal}(\mathcal{F}/K)$. Then $N_{\mathcal{F}}$ is normal of index 2 in $G_{\mathcal{F}}$, and τ acts trivially on $N_{\mathcal{F}}$. So $N_{\mathcal{F}}$ and any lift of τ commute with $N_{\mathcal{F}}$, which suffices to show that $N_{\mathcal{F}}$ lies in the center of $G_{\mathcal{F}}$. Now $G_{\mathcal{F}}/N_{\mathcal{F}}$ is cyclic of order 2, so that $G_{\mathcal{F}}$ modulo its center is cyclic. This implies that $G_{\mathcal{F}}$ is abelian. Hence in fact $\mathcal{F}/F$ is an abelian extension.

We now know that $I_K/P_K I_K^2 I_K^{\tau-1}$ corresponds to the maximal unramified elementary 2-extension $\mathcal{F}$ of K which is abelian over F. So the extension $I_K/P_K I_K^2 I_K^{\tau-1}\langle S_{\mathrm{fin}}(K)\rangle$ corresponds to the maximal such extension $\mathcal{L}_K$ of K in which all primes of $S_{\mathrm{fin}}(K)$ split completely.

For each finite or infinite prime $\mathfrak{p} \in S^0$, let $D_{\mathfrak{p}}$ denote its decomposition group in the abelian extension $\mathcal{L}_K/F$. Under our assumptions, such a prime $\mathfrak{p}$ does not split in the quadratic extension K/F, while the prime $\mathfrak{P}$ above it in K splits completely in $\mathcal{L}_K/K$. Thus $D_{\mathfrak{p}} = \langle \tau_{\mathfrak{p}} \rangle$ has order 2. Let D be the subgroup of $\mathrm{Gal}(\mathcal{L}_K/F)$ generated by all the $D_{\mathfrak{p}}$ for finite and infinite primes $\mathfrak{p} \in S^0$ except ∞_2. Hence D is an elementary abelian 2-group with

2-rank $\mathrm{rank}_2(D) \leq |S| - 2$. Let $\mathcal{L}'_F$ be the fixed field of D. Since $\mathcal{L}'_F \subset \mathcal{L}_K$, no primes ramify in $\mathcal{L}'_F/K$. Also, only primes in S^0 can ramify in K/F. So only primes in S^0 can ramify in $\mathcal{L}'_F/F$. The definition of $\mathcal{L}'_F$ requires that the primes in S^0 other than ∞_2 split completely in $\mathcal{L}'_F/F$. Hence $\mathcal{L}'_F/F$ can ramify only at ∞_2. Thus $\mathcal{L}'_F$ is contained in the ray class field modulo ∞_2 for F. But the ray classes modulo ∞_2 are the same as the ray classes modulo 1, due to the presence of the unit -1. Thus $\mathcal{L}'_F/F$ is unramified at ∞_2 as well, and is therefore everywhere unramified, with all primes in S splitting completely.

The fact that ∞_2 splits in $\mathcal{L}'_F/F$ but not in the quadratic extension K/F implies that $\mathcal{L}'_F \cap K = F$. Thus the elementary abelian 2-group $N_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}_K/K)$ and the elementary abelian 2-group $D = \mathrm{Gal}(\mathcal{L}_K/\mathcal{L}_{F'})$ generate the abelian group $\mathrm{Gal}(\mathcal{L}_K/F)$, which is therefore also an elementary abelian 2-group. Hence if $\mathfrak{q}$ is any prime of F which is inert in K, we may consider the Frobenius of the extended prime $\mathfrak{Q}$ of K in the extension $\mathcal{L}_K/K$ and use the properties of the Frobenius in relative extensions (see [1, III.2.4]): $\sigma(\mathfrak{Q}, \mathcal{L}_K/K) = \sigma(\mathfrak{q}, \mathcal{L}_K/F)^2 = 1$. This shows that J_K has trivial image in $\mathrm{Gal}(\mathcal{L}_K/K)$ under the Artin map.

We return now to the isomorphism from $I_K/P_K I_K^2 I_K^{\tau-1}\langle S_{\mathrm{fin}}(K)\rangle$ to $N_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}_K/K)$ which is induced by the Artin map as described above. Since the image of J_K lies in the kernel of this isomorphism, we conclude that

$$(1) \qquad H_K/H_K^2 \cong I_K/P_K I_K^2 I_K^{\tau-1}\langle S_{\mathrm{fin}}(K)\rangle J_K \cong \mathrm{Gal}(\mathcal{L}_K/K) = N_{\mathcal{L}}$$

Now we observe that $\mathcal{L}'_F$ has an intrinsic definition in terms of F. Since $\mathcal{L}'_F/F$ is an unramified elementary abelian 2-extension in which all primes of S split completely, it is contained in the maximal such extension, which we denote by $\mathcal{L}_F$. Then $\mathcal{L}_F \cdot K$ is an unramified elementary abelian 2-extension of K in which all primes of $S_{\mathrm{fin}}(K)$ (indeed $S(K)$, as unramified is the same as split for the infinite primes) split completely, and is abelian over F. But $\mathcal{L}_K$ was defined to be the maximal such extension, so $\mathcal{L}_K \supset \mathcal{L}_F$. As all primes in S split completely in $\mathcal{L}_F/F$, $\mathcal{L}_F$ must be fixed by the decomposition groups generating D. This means that $\mathcal{L}_F \subset \mathcal{L}'_F$. We conclude that $\mathcal{L}_F = \mathcal{L}'_F$.

Finally define $D_0 = \mathrm{Gal}(\mathcal{L}_K/(K \cdot \mathcal{L}_F))$, which has index 2 in $D = \mathrm{Gal}(\mathcal{L}_K/\mathcal{L}_F)$. Thus D_0 is an elementary abelian 2-group with $\mathrm{rank}_2(D_0) \leq |S| - 3$. Then we have an exact sequence:

$$(2) \qquad 1 \to D_0 \to N_{\mathcal{L}} \to \mathrm{Gal}(\mathcal{L}_F/F) \to 1$$

This simply comes from the natural restriction map identifying $N_{\mathcal{L}}/D_0 \cong \mathrm{Gal}((K \cdot \mathcal{L}_F)/K)$ with $\mathrm{Gal}(\mathcal{L}_F/F)$.

Interpreting $\mathrm{Gal}(\mathcal{L}_F/F)$ via the class field theory of F, we have

$$(3) \qquad \mathrm{Gal}(\mathcal{L}_F/F) \cong I_F/P_F I_F^2\langle S_{\mathrm{fin}}\rangle \cong \mathrm{Cl}_F(S_{\mathrm{fin}})/\mathrm{Cl}_F(S_{\mathrm{fin}})^2$$

Thus in terms of class groups (using (1) and (3)), the exact sequence(2) becomes

$$1 \to C_0 \to H_K/H_K^2 \to \mathrm{Cl}_F(S_{\mathrm{fin}})/\mathrm{Cl}_F(S_{\mathrm{fin}})^2 \to 1, \tag{4}$$

where the kernel C_0 is an elementary abelian 2-group of rank $\leq |S|-3$ and the map on the right is induced by the norm map on ideals. The conclusion of the theorem follows. □

Corollary 1. *The integer $2^{r_F(S)}$ divides M_i when $\eta_i \neq 1$.*

Proof. This is clear since $r_F(S) = \mathrm{rank}_2(\mathrm{Cl}_F(S_{\mathrm{fin}})) \leq \mathrm{rank}_2(H_K)$ for $K = K_i$. □

6. Proof of Theorem 1

The assumption is that $|S| \geq m + 2 - r_F(S)$. In view of Proposition 1, we consider

$$\varepsilon = \prod \eta_i^{M_i \cdot 2^{|S|-m-2}(w_L/w_i)},$$

where the product may clearly be taken over i for which $\eta_i \neq 1$. For such i, the expression $e_i = M_i \cdot 2^{|S|-m-2}$ is an integer multiple of $2^{r_F(S)} \cdot 2^{|S|-m-2}$, by Corollary 1, and this in turn is integral by assumption. Thus e_i is integral and so

$$\varepsilon = \prod \eta_i^{e_i(w_L/w_i)}$$

does in fact lie in L, since each η_i lies in $K_i \subset L$. Then $\mathrm{St}'(L/F,S)$ holds by Proposition 1. Furthermore

$$\varepsilon^{1/w_L} = \prod \eta_i^{e_i/w_i},$$

and each η_i^{1/w_i} lies in an abelian extension of F, by the Stark-Tate theorem. As the composite of abelian extensions is abelian, we conclude that ε^{1/w_L} lies in an abelian extension of F. This completes the proof of Theorem 1.

7. Kummer theory

Let:

- $\mathfrak{m}_S = \prod_{\mathfrak{p} \in S_{\mathrm{fin}}} \mathfrak{p}$
- $\mathcal{L} = \mathcal{L}_S$ be the composite of all quadratic extensions of F in $\overline{\mathbb{Q}}$ with relative discriminant dividing $4\mathfrak{m}_S$.
- $\mathcal{O}_F$ be the ring of integers of F.
- $\mathcal{O}_F(S_{fin})$ be the ring of S_{fin}-integers of $\mathcal{O}_F$.

Lemma 1. *Suppose $[K : F] = 2$. Then $K = F(\sqrt{\gamma})$ for some $\gamma \in F$ which generates a fractional ideal of F of the form $(\gamma) = \mathfrak{a}^2\mathfrak{b}$ with $\mathfrak{b}$ supported in S_{fin} if and only if the relative discriminant $\delta(K/F)$ of K over F divides $4\mathfrak{m}_S$. In particular, if K/F is unramified outside S, then $\delta(K/F)|4\mathfrak{m}_S$.*

Proof. First suppose that $K = F(\sqrt{\gamma})$ with $(\gamma) = \mathfrak{a}^2\mathfrak{b}$ and $\mathfrak{b}$ supported in S_{fin}. The relative discriminant may be computed locally, so we reduce to the case of an extension of local fields $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ by passing to the completions at a fixed arbitrary prime $\mathfrak{p}$ of F and a prime $\mathfrak{P}$ over $\mathfrak{p}$ in K. That is, the $\mathfrak{p}$-part $\left(\delta(K/F)\right)_{\mathfrak{p}}$ of the relative discriminant of K/F equals the relative discriminant of $K_{\mathfrak{P}}/F_{\mathfrak{p}}$, and it suffices to show that this divides $4\mathfrak{m}_S$ for each $\mathfrak{p}$. Let π be a uniformizing parameter for the ring of integers $\mathcal{O}_{\mathfrak{p}}$ of $F_{\mathfrak{p}}$. Then $\gamma = u\pi^{2e+a}$ where u is a unit of $\mathcal{O}_{\mathfrak{p}}$ and a equals 0 or 1. So $K_{\mathfrak{P}} = F_{\mathfrak{p}}(\sqrt{\gamma}) = F_{\mathfrak{p}}(\sqrt{u\pi^a})$. We treat the two possibilities for a individually.

When $a = 0$ we have $K_{\mathfrak{P}} = F_{\mathfrak{p}}(\sqrt{u})$. Then the relative discriminant $\delta(K_{\mathfrak{P}}/F_{\mathfrak{p}})$ divides the discriminant of the polynomial $x^2 - u$ which is $(4u) = (4)$, and this clearly divides $4\mathfrak{m}_S$.

When $a = 1$, it evidently must be the case that $\mathfrak{p}$ divides $\mathfrak{b}$, and therefore $\mathfrak{p}$ divides $\mathfrak{m}_S$. We have $K_{\mathfrak{P}} = F_{\mathfrak{p}}(\sqrt{u\pi}) = F_{\mathfrak{p}}(\sqrt{\pi'})$, where π' is another uniformizing parameter. Thus $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is an Eisenstein extension for which it is known that $\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{p}}(\sqrt{\pi'})$. Therefore $\delta(K_{\mathfrak{P}}/F_{\mathfrak{p}})$ equals the discriminant of $x^2 - \pi'$, namely $(4\pi') = 4\mathfrak{p}$. Again this divides $4\mathfrak{m}_S$, as $\mathfrak{p}$ divides $\mathfrak{m}_S$. This completes the first half of the proof.

Next assume that the relative discriminant $\delta(K/F)$ of K over F divides $4\mathfrak{m}_S$. Since K/F is a relative quadratic extension, we know that $K = F(\sqrt{\gamma})$ for some $\gamma \in F$. Write $(\gamma) = \mathfrak{a}^2\mathfrak{b}$, and $\mathfrak{b}$ a square free fractional ideal. If a prime $\mathfrak{p}$ appears in the factorization of $\mathfrak{b}$, let $\mathfrak{P}$ be a prime above $\mathfrak{p}$ in K. Then we are in the situation appearing in the first half of the proof where $a = 1$ and $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is an Eisenstein extension. In this case we saw that $\delta(K_{\mathfrak{P}}/F_{\mathfrak{p}}) = 4\mathfrak{p}$. We are assuming that this divides $4\mathfrak{m}_S$, so may clearly conclude that $\mathfrak{p}$ divides $\mathfrak{m}_S$ and thus $\mathfrak{p}$ is in S_{fin}. This shows that $\mathfrak{b}$ is supported in S_{fin}, and concludes the proof. □

Proposition 3. *The field $\mathcal{L} = \mathcal{L}_S$ contains $L(\{\sqrt{\eta_i} : i = 1 \ldots, 2^{m-1}\})$.*

Proof. We show that $\mathcal{L}$ contains $L(\{\sqrt{\eta_i} : i = 1 \ldots 2^{m-1}\})$ by showing that $\mathcal{L}$ contains L and each $\sqrt{\eta_i}$. First, each K_i/F is a quadratic extension, so $K_i = F(\sqrt{\gamma_i})$. We may write $(\gamma_i) = \mathfrak{a}^2\mathfrak{b}$ with $\mathfrak{b}$ square free. Then K_i is ramified at the divisors of $\mathfrak{b}$, by Kummer theory. Since K_i/F is unramified outside S, we conclude that $\mathfrak{b}$ is supported in S_{fin}. It now follows from the Lemma that K_i is a quadratic extension of F with relative discriminant dividing $4\mathfrak{m}_S$. But $\mathcal{L}$ was defined to be the composite of all such extensions. Thus $\mathcal{L}$ contains the composite of all the K_i, which is L, as we observed in the beginning of section III.

Having shown that $\mathcal{L}$ contains L, we proceed to show that $\mathcal{L}$ contains each $\sqrt{\eta_i}$. This is trivial if $\eta_i = 1$, so we may assume that we are not in this situation. Then the image of η_i generates the infinite cyclic group $U_{K_i}^{(\mathfrak{v})}/\mu_{K_i}$. Thus η_i is not a square in K_i, and η_i does not lie in F. So

$F(\sqrt{\eta_i})$ is an extension of degree 4 over F. We know that $\eta_i^\tau = 1/\eta_i$, so the conjugates of $\sqrt{\eta_i}$ over F are $\pm\sqrt{\eta_i}$ and $\pm 1/\sqrt{\eta_i}$. Thus $F(\sqrt{\eta_i})/F$ is a Galois extension of degree 4. It is in fact the composite of the relative quadratic extension $K_i = F(\eta_i)$ in which ∞_2 ramifies, and the relative quadratic extension $K_i' = F(\sqrt{\eta_i} + 1/\sqrt{\eta_i})$ in which ∞_2 splits. We have already seen that K_i lies in $\mathcal{L}$, so we now show that K_i' lies in $\mathcal{L}$. This will imply that the composite $F(\sqrt{\eta_i})$ lies in $\mathcal{L}$, as desired.

Above we saw that $\delta(K_i/F)|4\mathfrak{m}_S$. In fact, $\delta(K_i/F)|4\mathfrak{m}_{S^0}$, since this extension is unramified at $\mathfrak{v}$. Since η_i lies in $U_{K_i}^{(\mathfrak{v})}$, the Lemma yields $\delta(K_i(\sqrt{\eta_i})/K_i)|4\mathfrak{v}$. Hence

$$\delta(K_i(\sqrt{\eta_i})/F) = (N_{K_i/F}\delta(K_i(\sqrt{\eta_i})/K_i))\delta(K_i/F)^2,$$

which divides $16\mathfrak{v}^2\delta(K_i/F)^2$. Similarly, $\delta(K_i'/F)^2$ divides $\delta(K_i(\sqrt{\eta_i})/F)$, and thus divides $16\mathfrak{v}^2\delta(K_i/F)^2$. We conclude that $\delta(K_i'/F)|4\mathfrak{v}\delta(K_i/F)$.

We examine this divisibility statement one prime at a time and show that it implies $\delta(K_i'/F)_\mathfrak{p}|4\mathfrak{m}_S$ for each $\mathfrak{p}$. Observe that K_i/F is unramified outside of S, so $\delta(K_i/F)_\mathfrak{p} = (1)$ for $\mathfrak{p}$ not dividing $\mathfrak{m}_S$. Consequently $\delta(K_i'/F)_\mathfrak{p}|4\mathfrak{v}$ which divides $4\mathfrak{m}_S$ in this case.

Now for $\mathfrak{p}$ dividing $\mathfrak{m}_S$, the lemma applied to K_i'/F implies that $\delta(K_i'/F)_\mathfrak{p}$ divides $4\mathfrak{p}$ which in turn divides $4\mathfrak{m}_S$. This shows that $\delta(K_i'/F)$ divides $4\mathfrak{m}_S$. Hence K_i' lies in $\mathcal{L}$, by its very definition. □

Proposition 4. $[\mathcal{L}_S : F] = 2^{r_F(S)+|S|}$

Proof. Let $\{[\mathfrak{a}_i] : i = 1, \ldots, t\}$ be a minimal set of generators for the 2-torsion subgroup $\mathrm{Cl}_F(S_{\mathrm{fin}})[2]$ of the S_{fin}-class group $\mathrm{Cl}_F(S_{\mathrm{fin}})$. So $t = \mathrm{rank}_2(\mathrm{Cl}_F(S_{\mathrm{fin}})) = r_F(S)$. We view $\mathrm{Cl}_F(S_{\mathrm{fin}})$ as the group of invertible ideals modulo principal fractional ideals of $\mathcal{O}_F(S_{\mathrm{fin}})$, the ring of elements of F which are integral at all finite primes not in S_{fin}. Using Chebatorev's density theorem, we choose the representatives $\mathfrak{a}_i$ to be prime ideals of $\mathcal{O}_F(S_{\mathrm{fin}})$. The units of this ring are denoted $U_F(S_{\mathrm{fin}})$ and called the S_{fin}-units. Now $\mathfrak{a}_i^2 = \alpha_i\mathcal{O}_F(S_{\mathrm{fin}})$ for some α_i. Let $A = \langle\{\alpha_i : i = 1, \ldots, t\}\rangle U_F(S_{\mathrm{fin}})$.

We begin by noting that $A \cong \langle\{\alpha_i\}\rangle \times U_F(S_{\mathrm{fin}})$. For a non-trivial element of $\langle\{\alpha_i\}\rangle$ generates an ideal which is a non-trivial product of the prime ideals $\mathfrak{a}_i$, while each element of $U_F(S_{\mathrm{fin}})$ generates the unit ideal. Thus by the Dirichlet-Chevalley-Hasse unit theorem,

$$\mathrm{rank}_2(A) = \mathrm{rank}_2(\langle\{\alpha_i\}\rangle) + \mathrm{rank}_2(U_F(S_{\mathrm{fin}})) = t + |S| = r_F(S) + |S|.$$

We will establish a one-to-one correspondence between the non-trivial elements of A/A^2 and the relative quadratic extensions K/F contained in $\mathcal{L}$. This implies that $\mathrm{rank}_2(\mathrm{Gal}(\mathcal{L}/F)) = \mathrm{rank}_2(A/A^2)$, which combined with the displayed equality yields the statement of the proposition.

Now observe that $A \cap (F^\times)^2 = A^2$ as follows. If $\gamma^2 \in (F^\times)^2$ lies in A, then $\gamma^2 = \prod_i \alpha_i^{c_i}u$, for some $u \in U_F(S_{\mathrm{fin}})$. Hence $\gamma^2\mathcal{O}_F(S_{\mathrm{fin}}) = \prod_i \mathfrak{a}_i^{2c_i}$

and therefore $\gamma\mathcal{O}_F(S_{\text{fin}}) = \prod_i \mathfrak{a}_i^{c_i}$. The fact that this is a principal ideal generated by the $\mathfrak{a}_i$ implies by their definition that all of the exponents are even, $c_i = 2b_i$. We now have $\gamma^2 = \prod_i \alpha_i^{2b_i} u$, and this shows that $u = v^2$ is a square. Clearly $v \in U_F(S_{\text{fin}})$, so $\gamma = \prod_i \alpha_i^{b_i} v$, after choosing the correct sign for v. From this we see that $\gamma^2 \in A^2$, which was to be proved.

Given a γ representing a non-trivial class in A/A^2, this will correspond to the field $K = F(\sqrt{\gamma})$. According to the last paragraph, K will in fact be a relative quadratic extension of F. We check that K lies in $\mathcal{L}$ by showing that the relative discriminant $\delta(K/F)$ divides $4\mathfrak{m}_S$. The fact that $\gamma \in A$ means that $\gamma = u \prod \alpha_i^{e_i}$ for some integers e_i and some $u \in U_F(S_{\text{fin}})$. Then the principal $\mathcal{O}_F$-ideal generated by γ is $(\gamma) = \prod \tilde{\mathfrak{a}}_i{}^{2e_i}(v) = \mathfrak{a}^2\mathfrak{b}$, where $\mathfrak{b} = (v)$, and $\tilde{\mathfrak{a}}_i$ is the (prime) ideal of $\mathcal{O}_F$ supported outside of S_{fin} such that $\tilde{\mathfrak{a}}_i\mathcal{O}_F(S_{\text{fin}}) = \mathfrak{a}_i$. Since $\mathfrak{b} = (v)$ is supported in S_{fin}, Lemma 1 allows us to conclude that $\delta(K/F)$ divides $4\mathfrak{m}_S$, as desired.

Conversely, given a relative quadratic extension K/F contained in $\mathcal{L}$, we will produce the corresponding $\gamma \in A$. First we note that the relative discriminant of a relative quadratic extension is equal to the finite part of its conductor, by the conductor-discriminant theorem. Thus every relative quadratic extension of F with discriminant dividing $4\mathfrak{m}_S$ is contained in the ray class field of F with conductor equal to $4\mathfrak{m}_S$ multiplied by all of the infinite primes. Hence the field $\mathcal{L}$ generated by all of these relative quadratic extensions is also contained in this ray class field. Then any quadratic extension of F contained in $\mathcal{L}$ will have conductor dividing the product of $4\mathfrak{m}_S$ with all of the infinite primes, so that its discriminant also divides $4\mathfrak{m}_S$. We can conclude that the discriminant of our given K divides $4\mathfrak{m}_S$. Lemma 1 now implies that $K = F(\sqrt{\gamma'})$, where $(\gamma') = \mathfrak{a}^2\mathfrak{b}$ and $\mathfrak{b}$ is supported in S_{fin}. Hence $\gamma'\mathcal{O}_F(S_{\text{fin}}) = (\mathfrak{a}\mathcal{O}_F(S_{\text{fin}}))^2$, so that $\mathfrak{a}\mathcal{O}_F(S_{\text{fin}})$ represents an element of $\mathrm{Cl}_F(S_{\text{fin}})[2]$. But this group is generated by the images of the $\mathfrak{a}_i$. Thus $\mathfrak{a}\mathcal{O}_F(S_{\text{fin}}) = \prod \mathfrak{a}_i^{c_i}\beta\mathcal{O}_F(S_{\text{fin}})$ for some $\beta \in F$. Then $\gamma'\mathcal{O}_F(S_{\text{fin}}) = \prod \mathfrak{a}_i^{2c_i}\beta^2\mathcal{O}_F(S_{\text{fin}}) = \prod \alpha_i^{c_i}\beta^2\mathcal{O}_F(S_{\text{fin}})$. Let $\gamma = \gamma'/\beta^2$. We clearly have $K = F(\sqrt{\gamma'}) = F(\sqrt{\gamma})$, while $\gamma\mathcal{O}_F(S_{\text{fin}}) = (\prod \mathfrak{a}_i^{c_i})^2\mathcal{O}_F(S_{\text{fin}}) = (\prod \alpha_i^{c_i})\mathcal{O}_F(S_{\text{fin}})$. Thus $\gamma = u\prod \alpha_i^{c_i}$ for some $u \in U_F(S_{\text{fin}})$ and therefore $\gamma \in A$. □

Corollary 2. 1. *We have* $[\mathcal{L} : L] = 2^{r_F(S)+|S|-m}$.

2. *Let* ζ_i *be a generator of* μ_{K_i}. *When* η_i *is not equal to* 1, *the exponent* $M_i \cdot 2^{|S|-m-2}(w_L/w_i)$ *is in* $\frac{1}{2}\mathbb{Z}$. *If it is not in* $\mathbb{Z}$, *then either* $L = \mathcal{L}$ *or* $[\mathcal{L} : L] = 2$ *and* $\sqrt{\zeta_i} \notin L$.

Proof. 1. From the fact that $[L : F] = 2^m$ and Propositions 3 and 4, we conclude that $[\mathcal{L} : L] = 2^{r_F(S)+|S|-m}$, and thus this rational number is in fact an integer.

2. Now we can see that $2^{r_F(S)+|S|-m-2} = [\mathcal{L} : L]/4$ lies in $\frac{1}{4}\mathbb{Z}$. By Corollary 1, it follows that $M_i \cdot 2^{|S|-m-2}$ is in $\frac{1}{4}\mathbb{Z}$, and that if it does not lie in $\frac{1}{2}\mathbb{Z}$, we must have $L = \mathcal{L}$. In this case, note that the ambiguity up to a root of unity in the choice of η_i allows us to conclude from Proposition 3 that $L = \mathcal{L}$ contains both $\sqrt{\eta_i}$ and $\sqrt{\zeta_i \eta_i}$ and therefore $\sqrt{\zeta_i} \in L$. Thus w_L/w_i is even and $M_i \cdot 2^{|S|-m-2}(w_L/w_i)$ lies in $\frac{1}{2}\mathbb{Z}$. Finally, since $[\mathcal{L} : L]$ is a power of 2, the only other situation in which $2^{r_F(S)+|S|-m-2} = [\mathcal{L} : L]/4$ is not integral clearly occurs when $[\mathcal{L} : L] = 2$ and it is half-integral. Then $M_i \cdot 2^{|S|-m-2}$ is in $\frac{1}{2}\mathbb{Z}$, so $M_i \cdot 2^{|S|-m-2}(w_L/w_i)$ is integral unless w_L/w_i is odd, i.e. $\sqrt{\zeta_i} \notin L$. □

8. Proofs of Theorems 2 and 3

Under our standing assumptions that L/F is multiquadratic, and that in order to avoid special cases of the conjecture which have already been proved, S contains at least two infinite primes and one other finite or infinite prime, we now have:

- $\varepsilon = \prod \eta_i^{M_i \cdot 2^{|S|-m-2}(w_L/w_i)}$ by Proposition 1.
- The exponent $M_i \cdot 2^{|S|-m-2}(w_L/w_i)$ is either integral or half-integral when $\eta_i \neq 1$, by Corollary 2.
- If it is half-integral for some i, then either $\mathcal{L} = L$ or we have both $[\mathcal{L} : L] = 2$ and $\sqrt{\zeta_i} \notin L$, also by Corollary 2.

If $\mathcal{L} = L$, then $\sqrt{\eta_i} \in L$ for all i, since $\sqrt{\eta_i} \in \mathcal{L}$, by Proposition 3. If $[\mathcal{L} : L] = 2$ and $\sqrt{\zeta_i} \notin L$ for some i, notice that both $\sqrt{\eta_i}$ and $\sqrt{\zeta_i \eta_i}$ lie in $\mathcal{L}$ by Proposition 3 again and the ambiguity in η_i. If neither of them lie in L, then $L(\sqrt{\eta_i}) = \mathcal{L} = L(\sqrt{\zeta_i \eta_i})$. This implies that $\sqrt{\zeta_i} \in L$, which is not the case. Hence either $\sqrt{\eta_i} \in L$ or $\sqrt{\zeta_i \eta_i} \in L$. By renaming η_i, we may again assume $\sqrt{\eta_i} \in L$.

Thus in all cases, Theorem 2 follows from Proposition 1.

Turning to the proof of Theorem 3, we now assume that $\mathfrak{v}$ is either real or finite. When L is not the maximal multiquadratic extension $\mathcal{M}$ of F which is unramified outside of S and in which $\mathfrak{v}$ splits completely, we claim that $4|[\mathcal{L} : L]$. Then by Corollary 2, $r_F(S) + |S| - m - 2 \geq 0$, and the result will follow from Theorem 1.

To establish the claim, we first show that $\mathfrak{v}$ is not split completely in $\mathcal{L}_S/F$. When $\mathfrak{v}$ is real, this is clear since the definition of $\mathcal{L}_S$ implies that $\sqrt{-1} \in \mathcal{L}_S$ and thus $\mathcal{L}_S$ is totally imaginary. When $\mathfrak{v}$ is finite, we proceed by contradiction. Suppose $\mathfrak{v}$ splits completely in $\mathcal{L}_S/F$. Then $\mathfrak{v}$ is unramified in $\mathcal{L}_S$, so clearly $\mathcal{L}_S = \mathcal{L}_{S^0}$. From Corollary 2, we then get $2^{r_F(S)+|S|} = [\mathcal{L}_S : F] = [\mathcal{L}_{S^0} : F] = 2^{r_F(S^0)+|S^0|} = 2^{r_F(S^0)+|S|-1}$, so that $r_F(S) = r_F(S^0) - 1$. Now $2^{r_F(S^0)} = |\mathrm{Cl}_F(S^0)/\mathrm{Cl}_F(S^0)^2|$, so the class $[\mathfrak{v}]$

of $\mathfrak{v}$ must be non-trivial in this group. By class field theory, $\mathfrak{v}$ is then not split completely in the maximal unramified multiquadratic extension of F in which every finite prime of S^0 splits completely. However, this extension is contained in $\mathcal{L}_S$, by Lemma 1, and we have assumed that $\mathfrak{v}$ splits completely in $\mathcal{L}_S$, a contradiction.

Let $\mathcal{L}_S^{\mathfrak{v}}$ denote the splitting field of $\mathfrak{v}$ in $\mathcal{L}_S$. By the claim we have just established, $2|[\mathcal{L}_S : \mathcal{L}_S^{\mathfrak{v}}]$. Since $\mathfrak{v}$ splits completely in $L \subset \mathcal{L}_S$, we also have $\mathcal{L}_S^{\mathfrak{v}} \supset L$ and $2|[\mathcal{L}_S^{\mathfrak{v}} : L]$ unless $L = \mathcal{L}_S^{\mathfrak{v}}$. Thus $4|[\mathcal{L}_S : L]$ unless $L = \mathcal{L}_S^{\mathfrak{v}}$. From the definitions and Lemma 1 again, it follows that $L \subset \mathcal{M} \subset \mathcal{L}_S^{\mathfrak{v}}$. Thus in the exceptional case of $L = \mathcal{L}_S^{\mathfrak{v}}$, we have $L = \mathcal{M}$, the maximal multiquadratic extension of F which is unramified outside of S and in which $\mathfrak{v}$ splits completely.

9. The biquadratic case: proof of Theorem 4

We now assume that $m = 2$ and turn to the proof of Theorem 4. Since $|S| \geq 3$, Theorem 1 reduces us to the case where $|S| = 3$ and $r_F(S) = 0$. By Remark 2, we may assume that some prime $\mathfrak{p}_2$ over 2 ramifies in L/F, so that $S = \{\infty_1, \infty_2, \mathfrak{p}_2\}$, and we must have $\mathfrak{v} = \infty_1$ splitting in L/F. (This is the only time we will make use of [3].) Then by Proposition 2, we have that M_i is odd for $\eta_i \neq 1$. Thus

$$\varepsilon = \sqrt{\eta_1}^{M_1(w_L/w_1)} \sqrt{\eta_2}^{M_2(w_L/w_2)}, \text{ with both } M_i \text{ odd.}$$

By Theorem 2, $\varepsilon \in L$ satisfies $\mathrm{St}'(L/F)$ and indeed the proof shows that we may take $\sqrt{\eta_i}^{(w_L/w_i)} \in L$ for $i = 1, 2$.

Temporarily fix $i = 1$ or 2. Notice that ∞_2 ramifies in K_i, and only one other prime (namely $\mathfrak{p}_2$) is allowed to ramify over F. But some other prime must ramify, for otherwise K_i is contained in the ray class field for F modulo ∞_2. But the ray class group modulo ∞_2 is the same as the ray class group modulo 1, due to the presence of the unit -1. This would imply that K_i is unramified at ∞_2, a contradiction. Thus $\eta_i \neq 1$.

It remains to check that $L(\varepsilon^{1/w_L})$ is abelian over F. For this we use a standard lemma (see [5, p. 83, Prop. 1.2]).

Lemma 2. *Suppose L/F is a finite abelian extension of number fields with Galois group G. Let $\mathcal{A}$ be the annihilator ideal of the group of roots of unity μ_L considered as a module over the group ring $\mathbb{Z}[G]$. Let T be a set of $\mathbb{Z}[G]$-generators for $\mathcal{A}$. Then an element u in the multiplicative group L^* has the property that $L(u^{1/w_L})/F$ is abelian, if and only if there exists a collection of $a_\alpha \in L^*$, indexed by $\alpha \in T$ such that both of the following conditions hold:*

a. $a_\alpha^{w_L} = u^\alpha \quad \forall \alpha \in T$
b. $a_\alpha^\beta = a_\beta^\alpha \quad \forall \alpha, \beta \in T.$

Recall that $\tau \in G$ is the complex conjugation in L over ∞_2. Also let τ_1 be the element of order 2 in G which fixes K_1. Thus τ and τ_1 generate G.

First consider the number of roots of unity w_L in L. Suppose $w_L > 2$. Then L has no real embeddings, and the split prime ∞_1 of F must be complex, while ∞_2 is real. Hence F is a non-Galois cubic extension of $\mathbb{Q}$ and $[L : \mathbb{Q}] = 12$.

If L contains a pth root of unity ζ_p for some odd prime p, then L/F must ramify at some prime over p, because $F(\zeta_p)/F$ does. But the only finite prime which can ramify in L/F is $\mathfrak{p}_2 \in S$. If L contains a 16th root of unity, then $[L : \mathbb{Q}] = 12$ must be divisible by $\phi(16) = 8$, a contradiction. Thus the number of roots of unity in L is w_L =2, 4, or 8.

Case 1: $w_L = 2$. When $w_L = 2$, the above arguments show that we may take $K(\sqrt{\eta_1}) = L = K(\sqrt{\eta_2})$. Since τ is a complex conjugation and $\eta_i^{1+\tau} = 1$ for $i = 1, 2$; we conclude that $\sqrt{\eta_i}^{1+\tau} = 1$ for $i = 1, 2$. Using this, one can verify that the conditions of Lemma 2 hold for $\varepsilon = \sqrt{\eta_1}^{M_1}\sqrt{\eta_2}^{M_2} \in L$ upon setting $a_{w_L} = \varepsilon$, $a_{1+\tau} = 1$, and $a_{1+\tau_1} = \sqrt{\eta_1}^{M_1}$. Thus St$(L/F,\, S)$ holds in this case.

Now if $4|w_L$, then L contains $F(\sqrt{-1})$, which must be either K_1 or K_2. By renumbering, we may assume that it is K_2. Thus $w_1 = 2$.

Case 2: $w_L = 4$. Now $w_1 = 2$, $w_2 = 4$, and $\varepsilon = {\eta_1}^{M_1}\sqrt{\eta_2}^{M_2} \in L$. We have noticed above that $\mathcal{L}$ contains the square roots of all the roots of unity in the K_i. Thus $\mathcal{L}$ contains an 8th root of unity ζ_8. Put $a_{w_L} = \varepsilon$, $a_{\tau+1} = 1$, and $a_{\tau_1 - 3} = \zeta_8(\sqrt{\eta_1})^{-M_1}(\sqrt{\eta_2})^{-M_2}$. The argument above shows that $\sqrt{\eta_1}$ and ζ_8 lie in $\mathcal{L}$, but not L, although their squares lie in L. Thus $\zeta_8\sqrt{\eta_1}^{M_1} \in L$, since M_1 is odd. Also $\sqrt{\eta_2} \in L$, so we have confirmed that $a_{\tau_1-3} \in L$. Again the conditions of Lemma 2 hold and St$(L/F,S)$ is proved in this case.

Case 3: $w_L = 8$. Now $w_1 = 2$, $w_2 = 4$, and $\varepsilon = {\eta_1}^{2M_1}{\eta_2}^{M_2} \in L$. Put $a_{w_L} = \varepsilon$, $a_{\tau+1} = 1$, and $a_{\tau_1-3} = (\sqrt{\eta_1})^{-M_1}(\sqrt{\eta_2})^{-M_2}$. We know that $\sqrt{\eta_1}$ and $\sqrt{\eta_2}$ lie in $\mathcal{L}$, but not in L, although their squares lie in L. Thus $a_{\tau_1-3} \in L$, since M_1 and M_2 are odd. Again the conditions of Lemma 2 hold and St$(L/F,S)$ is proved in this case.

Acknowledgements

The second author thanks the Mathematics Department of the University of Texas at Austin for its hospitality while much of the work of this paper was being carried out. Thanks also go to Cristian Popescu for several discussions related to this work.

References

[1] G. JANUSZ, *Algebraic number fields.* Academic Press, New York, 1973.

[2] J. W. SANDS, *Galois groups of exponent two and the Brumer-Stark conjecture.* J. Reine Angew. Math. **349** (1984), 129–135.

[3] J. W. SANDS, *Two cases of Stark's conjecture.* Math. Ann. **272** (1985), 349–359.

[4] H. M. STARK, *L-functions at $s = 1$ IV. First derivatives at $s = 0$.* Advances in Math. **35** (1980), 197–235.

[5] J. T. TATE, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$.* Birkhäuser, Boston, 1984.

David S. DUMMIT, Jonathan W. SANDS
Dept. of Math. and Stat.
University of Vermont
Burlington, VT 05401
USA
E-mail : David.Dummit@uvm.edu, Jonathan.Sands@uvm.edu

Brett TANGEDAL
Dept. of Math.
University of Charleston
Charleston, SC 29424
USA
E-mail : tangedal@math.cofc.edu