Stark's Conjectures and Hilbert's Twelfth Problem

Xavier-François Roblot

CONTENTS

We give a constructive proof of a theorem of Tate, which states that (under Stark's Conjecture) the field generated over a totally real field K by the Stark units contains the maximal real abelian extension of K. As a direct application of this proof, we show how one can compute explicitly real abelian extensions of K. We give two examples.

In a series of important papers, H. M. Stark [1971; 1975; 1976; 1980] developed a body of conjectures relating the values of Artin L-functions at $s = 1$ (and hence, by the functional equation, their leading terms at $s = 0$) with certain algebraic quantities attached to extensions of number fields. For example, in the case of abelian L-functions with a first-order zero at $s = 0$, the conjectural relation is between the first derivative of the L-functions and the logarithmic embedding of certain units in ray class fields known as Stark units, which are predicted to exist.

The use of these conjectures to provide explicit generators of ray class fields, and thus to answer Hilbert's famous Twelfth Problem was one of the original motivations for their formulation. It has been noticed by several people (including Stark himself [1976]) that they could provide a new way to construct ray class fields of totally real fields.

In particular, if K is a totally real field, the field extension generated over K by the Stark units (see below for details) contains the maximal real abelian extension of K. This result is a direct consequence of [Tate 1984, Chapter IV, Proposition 3.8].

Using the ideas given in [Stark 1976], we give in Section 2 a constructive proof of this result; that is, for each finite real abelian extension L/K we construct explicit generators of L over K using Stark units. This proof has a direct application since we can use it to explicitly compute real class fields of a totally real field. This is discussed in Section 3. Since this construction is based on a conjecture, we

1058-6458/2000 $0.50 per page

also explain in that section how to check the correctness of the result. Finally, we end the paper by giving two examples of such a construction.

1. THE ABELIAN RANK-ONE STARK CONJECTURE

The main reference for Stark's conjectures is [Tate 1984].

Let N/K be an abelian extension of number fields, and let G and $\mathfrak{f}$ denote respectively its Galois group and its conductor.

For $\mathfrak{m}$ an admissible modulus for N/K (that is, $\mathfrak{m}$ is a multiple of $\mathfrak{f}$), we let $I_K(\mathfrak{m})$ be the group of fractional (non-zero) ideals of K coprime to $\mathfrak{m}$, and $P_K(\mathfrak{m})$ the group of fractional (non-zero) principal ideals which have a generator multiplicatively congruent to 1 modulo $\mathfrak{m}$. The ray class group modulo $\mathfrak{m}$ is then given by $\mathrm{Cl}_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_K(\mathfrak{m})$. The norm group of N/K modulo $\mathfrak{m}$ is defined as the subgroup of $I_K(\mathfrak{m})$ generated by the norms from N to K of the fractional ideals of N coprime to $\mathfrak{m}\mathcal{O}_N$ and the group $P_K(\mathfrak{m})$. Let $\mathfrak{N}_{N/K}(\mathfrak{m})$ denote this norm group, it is known from Class Field Theory that $I_K(\mathfrak{m})/\mathfrak{N}_{N/K}(\mathfrak{m}) \cong G$ by the Artin isomorphism. Thus, for a given admissible modulus $\mathfrak{m}$, the norm group $\mathfrak{N}_{N/K}(\mathfrak{m})$ defines N uniquely.

Let S be a fixed finite set of places of K containing the infinite places of K and the finite places ramified in N/K.

To an element $\sigma \in G$, one associates the partial zeta function defined for a complex number s with $\operatorname{Re} s > 1$ by the Dirichlet series

$$\zeta_S(s,\sigma) = \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_\mathfrak{a}=\sigma}} \mathcal{N}\mathfrak{a}^{-s},$$

where $\mathfrak{a}$ runs through the integral ideals of K not divisible by any (finite) prime ideal contained in S and such that the Artin symbol $\sigma_\mathfrak{a}$ is equal to σ.

To a character χ over G, one associates the Artin L-function defined for a complex number s with $\operatorname{Re} s > 1$ by the Euler product

$$L_S(s,\chi) = \prod_{\mathfrak{p}\notin S} (1-\chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1}$$

where $\mathfrak{p}$ runs through the (finite) prime ideals of K not contained in S. (Here and in the sequel, by abuse of notation we consider that the character χ is not only defined on the Galois group G but also on the ray class group $\mathrm{Cl}_K(\mathfrak{f})$ and the group $I_K(\mathfrak{f})$ of the non-zero fractional ideals of K coprime to the finite part of $\mathfrak{f}$.)

These functions can be analytically continued to meromorphic functions on the whole complex plane (L-functions can even be continued to holomorphic functions if the character χ is non-trivial). As is well-known, they are also related to partial zeta functions by the two equivalent identities

$$\zeta_S(s,\sigma) = \frac{1}{[N:K]} \sum_{\chi\in\widehat{G}} L_S(s,\chi)\overline{\chi}(\sigma),$$

$$L_S(s,\chi) = \sum_{\sigma\in G} \zeta_S(s,\sigma)\chi(\sigma).$$

Let χ be a character of G. If χ is the trivial character $\mathbf{1}$ we set $r(\mathbf{1}) = \operatorname{Card} S - 1$, otherwise $r(\chi)$ is the number of places $v \in S$ such that the decomposition group D_v of v in N/K is contained in the kernel of χ, in other words such that $\chi_{|D_v} = \mathbf{1}$. The following result can be found in [Martinet 1977] or [Tate 1984].

Proposition 1.1. *The order of vanishing at $s = 0$ of the Artin L-function $L_S(s,\chi)$ is equal to $r(\chi)$.*

We now assume that there exists an infinite place v which is totally split in N/K and we fix w, a place of N dividing v. We also assume that $\operatorname{Card} S \geq 2$. It follows from Proposition 1.1 that $L_S(0,\chi) = 0$ for every character, thus the partial zeta functions ζ_S are all zero at $s = 0$.

Conjecture 1.2 (Stark). *Let m be the number of roots of unity contained in N. There exists an S-unit $\varepsilon \in N$ such that for every $\sigma \in G$*

$$\log|\sigma(\varepsilon)|_w = -m\zeta_S'(0,\sigma),$$

or equivalently

$$L_S'(0,\chi) = -\frac{1}{m}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\varepsilon)|_w$$

for any character χ over G. Furthermore $N(\sqrt[m]{\varepsilon})/K$ is an abelian extension and if $\operatorname{Card} S \geq 3$ then ε is a unit.

Remark 1.3. We denote by $\varepsilon(N/K,S,w)$ the unit ε appearing in the Conjecture if it exists (this is an abuse of language since this unit may not be unique, but in what follows the place w will be a real place and we make $\varepsilon(N/K,S,w)$ unique by assuming that

$w(\varepsilon(N/K,S,w)) > 0)$. When the set S is chosen to be minimal — that is, S is the set of infinite places of K together with the finite places ramified in N/K — we simply write $\varepsilon(N/K,w)$.

2. APPLICATION TO HILBERT'S TWELFTH PROBLEM

Let K be a totally real field distinct from $\mathbb{Q}$ and let v be a fixed infinite place of K. We identify K with its image $v(K)$ in $\mathbb{R}$. *From now on, we assume that Conjecture* 1.2 *is true for any finite abelian extensions N/K in which v is totally split and any choice of the place w of N dividing v.*

Let K^{Stark} be the subfield of $\mathbb{C}$ generated over K by all the units $\varepsilon(N/K,w)$ where N/K runs through the finite abelian extensions of K in which v is totally split, and w runs through the infinite places of N dividing v. Then, we have the following

Theorem 2.1. *The maximal real abelian extension of K is contained in K^{Stark}.*

Equivalently, for any finite real abelian extension L/K, there exist Stark units $\varepsilon_1,\dots,\varepsilon_r$ such that $L\subset K(\varepsilon_1,\dots,\varepsilon_r)$.

Remark 2.2. As mentioned in the introduction, this theorem is a consequence of [Tate 1984, Chapter IV, Proposition 3.8].

We will prove the theorem by proving the second assertion. For that purpose, we will construct the units $\varepsilon_1,\dots,\varepsilon_r$. In fact, we will prove a little more since these units will verify

$$L=\mathbb{Q}(\varepsilon_1+\varepsilon_1^{-1},\dots,\varepsilon_r+\varepsilon_r^{-1}). \tag{2–1}$$

For a prime ideal $\mathfrak{p}$ of K we define an integer $r_\mathfrak{p}$ as follows. If $\mathfrak{p}$ does not divide 2 then $r_\mathfrak{p}=2$, otherwise $r_\mathfrak{p}=n_\mathfrak{p}+2$ where $n_\mathfrak{p}$ is the degree of the local extension $K_\mathfrak{p}/\mathbb{Q}_2$.

Proposition 2.3. *Let L/K be a finite abelian extension of totally real fields. Let v be a infinite place of K and let T be a finite set of prime ideals of K such that for each prime $\mathfrak{p}$ in T, the 2-rank of the decomposition group $D_\mathfrak{p}$ of $\mathfrak{p}$ in L/K is strictly less than $r_\mathfrak{p}$.*

Then there exists a quadratic extension N/L verifying these three conditions:

(A) *The extension N/K is abelian.*

(B) *All the infinite places of K except v become complex in N,*

(C) *The prime ideals of L above T do not split in N/L.*

Remark 2.4. The maximal value for the 2-rank of the decomposition group $D_\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ in any abelian extension of K is $r_\mathfrak{p}$.

Remark 2.5. Conditions (A)–(C) are very important for the construction. Conditions (A) and (B) allow us to apply Conjecture 1.2 to the extension N/K. Condition (C) is necessary to ensure that $L'_S(0,\chi)$ is not going to vanish for too many characters χ, and so make sure that the Stark unit that we obtain is a generator of N (see below).

Proof. Let $\mathfrak{p}$ be a prime ideal in T and fix a prime ideal $\mathfrak{P}$ in L dividing $\mathfrak{p}$. Let $s_\mathfrak{p}$ denote the 2-rank of the decomposition group of $\mathfrak{p}$ in L/K. Then Galois Theory tells us that the number of quadratic extensions of $K_\mathfrak{p}$ contained in $L_\mathfrak{P}$ is $2^{s_\mathfrak{p}}-1$. On the other hand, Kummer Theory tells us that the number of quadratic extensions of $K_\mathfrak{p}$ is $2^{r_\mathfrak{p}}-1$. Since $s_\mathfrak{p}<r_\mathfrak{p}$, there exists (at least) one quadratic extension, say $E_\mathfrak{p}/K_\mathfrak{p}$, such that $E_\mathfrak{p}$ is not contained in $L_\mathfrak{P}$ and thus a $\mathfrak{p}$-adic integer in $K_\mathfrak{p}$, say $\varkappa_\mathfrak{p}$, such that $E_\mathfrak{p}=K_\mathfrak{p}(\sqrt{\varkappa_\mathfrak{p}})$. In particular, $\varkappa_\mathfrak{p}$ is not a square in $L_\mathfrak{P}$.

For each prime ideal $\mathfrak{p}\in T$, choose such an element $\varkappa_\mathfrak{p}$ and let

$$m_\mathfrak{p}=v_\mathfrak{P}(\varkappa_\mathfrak{p})+v_\mathfrak{P}(2)+1,$$

where $v_\mathfrak{P}$ denotes the valuation associated to $\mathfrak{P}$ (observe that $m_\mathfrak{p}$ does not depend on the choice of $\mathfrak{P}$ since $\varkappa_\mathfrak{p}$ is an element of $K_\mathfrak{p}$). By the Approximation Theorem, one can find an algebraic integer $\varkappa$ in K such that

1. $v(\varkappa)>0$,
2. $v'(\varkappa)<0$ for any infinite place v' of K distinct from v,
3. $\varkappa\equiv\varkappa_\mathfrak{p} \pmod{\mathfrak{p}^{m_\mathfrak{p}}}$ for any prime ideal $\mathfrak{p}\in T$.

Then I claim that $N=L(\sqrt{\varkappa})$ satisfies the properties (A)–(C). First, it is clear that N/K is abelian since it is the compositum of the two abelian extensions L/K and $K(\sqrt{\varkappa})/K$, so (A) is satisfied. Second, since $\sqrt{v'(\varkappa)}$ is a complex number for $v'\neq v$ whereas $\sqrt{v(\varkappa)}$ is real, it follows that v is the only infinite place of K which remains real in N/K and this gives (B). Third, let $\mathfrak{p}$ be a prime ideal in T and suppose that $\mathfrak{p}$ splits in N/L. Denote by $\mathfrak{P}$ and $\tilde{\mathfrak{P}}$ a prime ideal in L and N, respectively, dividing $\mathfrak{p}$ and such that $\tilde{\mathfrak{P}} \mid \mathfrak{P}$. Then the local fields $N_{\tilde{\mathfrak{P}}}$ and $L_{\mathfrak{P}}$ are the same and thus $\varkappa$ is a square in $L_{\mathfrak{P}}$. Now, consider the quadratic polynomial $X^2 - \varkappa_{\mathfrak{p}}$ with coefficients in $L_{\mathfrak{P}}$. This polynomial has a simple root modulo $\mathfrak{P}^{m_{\mathfrak{p}}}$, namely $\sqrt{\varkappa}$, and thus it follows by Hensel's Lemma that it has a root in $L_{\mathfrak{P}}$. But this is impossible since we know that $\varkappa_{\mathfrak{p}}$ is not a square in $L_{\mathfrak{P}}$ and thus $\mathfrak{p}$ cannot split in N/L and (C) is also satisfied. □

We now prove Theorem 2.1. Assume first that L/K is a cyclic extension. We want to construct a quadratic extension N/L satisfying conditions (A)–(C), and such that not too many derivatives of L-functions associated to this extension vanish at $s = 0$ since, otherwise, Conjecture 1.2 would be useless. Looking at the formulae for $r(\chi)$ before Proposition 1.1, one way to do this is to ensure that no prime ideals in S split in N/L. Now, with our choice of S as minimal, the prime ideals in S are exactly the prime ideals that ramify in N/K. Let $\mathfrak{p}$ be such a prime ideal. If $\mathfrak{p}$ is not ramified in L/K, then $\mathfrak{p}$ must be ramified in N/L and thus is not split. If $\mathfrak{p}$ is ramified in L/K, then we want to make sure that it is not going to split in N/L, so we let $\mathfrak{p}$ be an element of T. Hence, we choose T be the set of the prime ideals of K which are ramified in L/K. For each prime ideal $\mathfrak{p}$ in T, the 2-rank of its decomposition group in L/K is equal to 1, so we can apply Proposition 2.3 and obtain a quadratic extension N/L verifying conditions (A)–(C). We fix an infinite place w in N dividing v and let $\varepsilon = \varepsilon(N/K, w)$.

Let τ denote the unique non-trivial automorphism of the quadratic extension N/L, and let $\mathfrak{p}$ be a prime ideal in S. Since $\mathfrak{p}$ does not split in N/L, $D_{\mathfrak{p}}$ contains τ. In particular, if χ is a character of G such that $\chi(\tau) \neq 1$ then $r(\chi) = 1$ and we deduce from Proposition 1.1 that

$$L'_S(0, \chi) \neq 0.$$

Finally, we apply [Stark 1976, Theorem 1], which we restate in our situation with our notations for the sake of completeness.

Theorem 2.6 (Stark). *Assume Conjecture 1.2 is true. Let Γ be the quotient group $G/\{1, \tau\}$, so that Γ is the Galois group of L/K. Assume that for every character ψ of G not induced by a character of Γ one has $L'(0, \psi) \neq 0$. Then, $N = \mathbb{Q}(\varepsilon)$ and*

$$L = \mathbb{Q}(\varepsilon^{-1} + \varepsilon).$$

When L/K is not cyclic, we can split L/K as the compositum of cyclic extensions $L_1/K, \ldots, L_r/K$ and apply to each of these cyclic extensions the above construction to obtain quadratic extensions N_i/L_i and infinite places w_i such that

$$\varepsilon_i = \varepsilon(N_i/K, w_i)$$

satisfies $L_i = K(\varepsilon_i + \varepsilon_i^{-1})$. Assertion (2–1) follows since L is generated over K by the elements $\varepsilon_i + \varepsilon_i^{-1}$, proving the theorem.

Remark 2.7. Note that conditions (A)–(C) on the extension N/K of Proposition 2.3 (with T containing the set of prime ideals ramified in L/K) are enough to prove the theorem, and that we may obtain an extension N/L verifying those conditions by other means than those given in the proof of the proposition which constructs N as the compositum of the extension L/K with the quadratic extension $K(\sqrt{\varkappa})/K$ (see last section for such an example).

We end this section with a very useful lemma.

Lemma 2.8. *The Stark unit ε appearing in the above construction is a unit (and not merely an S-unit) and satisfies*

$$|\varepsilon|_{w'} = 1$$

for any infinite place w' of N which does not divide v (that is, for any infinite complex place w' of N).

Proof. To prove the first assertion, it suffices to prove that $\operatorname{Card} S \geq 3$ and the result will follow from Conjecture 1.2. Since S must contain the infinite places of K, the case $\operatorname{Card} S < 3$ can only happen when K is a real quadratic field and N/K is unramified at all the finite places. But this is possible only if N is the Hilbert Class Field or the Narrow Hilbert Class Field of K; in the first case, no infinite places of K are ramified in N/K, in the second the two infinite places of K are ramified in N/K, and neither of these cases apply here since exactly one infinite place must be ramified in N/K.

The proof of the second assertion can be found in [Stark 1976, p. 74] in a slightly different form. □

3. AN OVERVIEW OF THE COMPUTATIONAL ASPECTS

In this section we will briefly describe how one can use the proof of Theorem 2.1 to compute real class fields of a totally real ground field (see [Roblot 1997] for a complete exposition). Similar computations for checking Stark's Conjecture over a real cubic field can be found in [Dummit et al. 1997]. In a more specialized case, namely when K is a real quadratic field and L its Hilbert Class Field, it is possible to obtain a much more powerful algorithm; see [Cohen and Roblot 2000] for details.

Let K be a totally real field of degree $N \geq 2$ and discriminant d_K, let L be a finite real abelian extension of K of conductor $\mathfrak{m}$ (hence $\mathfrak{m}$ is an integral ideal of K). Assume for the sake of simplicity that there exist quadratic extensions N/L verifying conditions (A)–(C) of Proposition 2.3 (e.g., if L/K is cyclic, or more generally if for every prime ideal $\mathfrak{p}$ of K which divides $\mathfrak{m}$, one has $s_\mathfrak{p} < r_\mathfrak{p}$ with the notations of Proposition 2.3).

First, we need to compute a quadratic extension N/L verifying conditions (A)–(C). Of course, the proof of Proposition 2.3 gives us a direct way to do this, but, as quoted in Remark 2.7, we cannot obtain by this method all the quadratic extensions N/L verifying (A)–(C). Furthermore, heuristics and numerical evidences seem to show that the Stark unit tends to grows more or less like the exponential of the square root of the discriminant times the norm of the conductor of N/K and thus we want to lower this norm as much possible. The best way to find N is then to construct explicitly the class group of conductor $\mathfrak{f}_0\mathfrak{f}_\infty$ where $\mathfrak{f}_0 = \mathfrak{a}\mathfrak{m}$ and $\mathfrak{a}$ runs through the integral ideals of K by increasing norm and $\mathfrak{f}_\infty$ contains all the infinite places of K but one, and look for the first one of these class groups which contains a subgroup defining a suitable extension N/L. These computations involve only class groups and can be done using the tools of [Cohen et al. 1998].

Assume we have found such a suitable extension N/L, let $\mathfrak{f}$ be the conductor of N/K, G its Galois group, v the only unramified infinite place, and let $\varepsilon = \varepsilon(N/L, w)$ denote the corresponding Stark unit. We want to compute ε, or more precisely the element $\alpha = \varepsilon + \varepsilon^{-1}$ satisfying $L = K(\alpha)$. Thanks to Lemma 2.8, we know that α is in fact an algebraic integer.

Now, we need to compute the values of $\zeta'_S(0, \sigma)$ for $\sigma \in G$ to high precision. In fact, it is simpler to compute the values of $L'_S(0, \chi)$ and deduce from them the values of $\zeta'_S(0, \sigma)$ using the formulae given in the first section. Let χ be a character of G; using Proposition 1.1, it is easy to prove that $L'_S(0, \chi) = 0$ if $\chi(\tau) = 1$ (recall that τ is a generator of $\mathrm{Gal}(N/L)$) and this term does not contribute to the computation of $\zeta'_S(0, \chi)$. Thus we assume that $\chi(\tau) = -1$. Let $L(s, \chi)$ denote the primitive L-function associated to χ which is defined by

$$L(s, \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1},$$

where $\mathfrak{p}$ runs through all the prime ideals of K and where $\chi(\mathfrak{p})$ is set to be equal to zero whenever $\mathfrak{p}$ divides the conductor $\mathfrak{f}(\chi)$ of χ. We have

$$L'_S(0, \chi) = A(\chi) L'(0, \chi)$$

where

$$A(\chi) = \prod_{\mathfrak{p} \mid \mathfrak{f}} (1 - \chi(\mathfrak{p})).$$

The value of the first derivative of $L(s, \chi)$ at $s = 0$ can be easily determined thanks to the functional equation. Let $\Lambda(s, \chi)$ be the "enlarged" L-function given by

$$\Lambda(s, \chi) = C(\chi)^s \Gamma\left(\tfrac{s}{2}\right) \Gamma\left(\tfrac{s+1}{2}\right)^{N-1} L(s, \chi)$$

where $C(\chi) = \sqrt{\pi^{-N} d_K \mathcal{N}\mathfrak{f}(\chi)}$. Then for any $s \in \mathbb{C}$

$$\Lambda(1 - s, \chi) = W(\chi) \Lambda(s, \bar{\chi}).$$

The constant $W(\chi)$ is a complex number of modulus one, the so-called Artin Root Number (see [Martinet 1977] for a complete exposition of these results in the more general case of Artin L-functions). Letting s tends to zero in this functional equation yields the relation

$$L'_S(0, \chi) = A(\chi) \frac{\Lambda(1, \bar{\chi})}{2\sqrt{\pi^{N-1}} W(\bar{\chi})}$$

where $A(\chi)$ is the constant defined above.

Thus the computation of $L'_S(0, \chi)$ — and hence of $\zeta'_S(0, \sigma)$ — boils down to the computation of three quantities: $A(\chi)$, $W(\bar{\chi})$ and $\Lambda(1, \bar{\chi})$. The computation of $A(\chi)$ is direct using the methods of [Cohen et al. 1998] and one can use explicit formulae to compute $W(\bar{\chi})$; see [Dummit and Tangedal 1998], for example. However, the computation of $\Lambda(1, \bar{\chi})$

requires much more work. We use a result from [Friedman 1988]:

Theorem 3.1 (Friedman). *Let $L(s,\chi)=\sum_{n\geq 1} a_n(\chi)n^{-s}$ be the expression for $L(s,\chi)$ as a Dirichlet series for* $\operatorname{Re} s > 1$. *Then*

$$\Lambda(1,\chi)=\sum_{n\geq 1}\bigl(a_n(\chi)f(C(\chi)/n,1) + W(\chi)a_n(\bar\chi)f(C(\chi)/n,0)\bigr),$$

where

$$f(x,t)=\frac{1}{2i\pi}\int_{\delta-i\infty}^{\delta+i\infty} x^z\frac{\Gamma\left(\frac{z}{2}\right)\Gamma\left(\frac{z+1}{2}\right)^{N-1}}{z-t}\,dz$$

for any real number $\delta > \operatorname{Re} t$.

There exist various methods to compute these integrals. One was developed by E. Tollis [1997]. A quite similar method is used in [Dummit et al. 1997].

One of the most time consuming part of the algorithm is the computation of the coefficients $a_n(\chi)$. We explain briefly how to do this. Assume that the prime ideals of K have been ordered in a sequence $(\mathfrak{p}_i)_{i\geq 1}$ such that $\mathcal{N}\mathfrak{p}_{i+1}\geq \mathcal{N}\mathfrak{p}_i$, and set $\mathfrak{p}_0=\mathcal{O}_K$. Let $I_{n,h}(\chi)$ denote the set of all integral ideals in K of norm n, prime with $\mathfrak{f}(\chi)$ and divisible only by prime ideals $\mathfrak{p}_i$ with $i\leq h$. We set

$$a_{n,h}(\chi)=\sum_{\mathfrak{a}\in I_{n,h}(\chi)}\chi(\mathfrak{a}).$$

Then it is clear that $a_n(\chi)=\lim_{h\to\infty} a_{n,h}(\chi)$, and even more $a_n(\chi)=a_{n,h}(\chi)$ if $\mathcal{N}\mathfrak{p}_h > n$. Now, the coefficients $a_{n,h}(\chi)$ are computed using a sieve and the following lemma.

Lemma 3.2. *We have $a_{1,0}(\chi)=1$ and $a_{n,0}(\chi)=0$ for $n\geq 2$, and for $h\geq 1$*

$$a_{n,h}(\chi)=\sum_{k=0}^{m_{n,h}} a_{n/{q_h}^k,h-1}(\chi)\chi(\mathfrak{p}_h)^k,$$

where $q_h=\mathcal{N}\mathfrak{p}_h$ and $m_{n,h}$ is the largest integer m such that $q_h^m \mid n$.

Proof. This is a direct application of the Euler product formula

$$\sum_{n\geq 1} a_n(\chi)n^{-s}=\prod_{h>1}\left(1-\chi(\mathfrak{p}_h)/\mathcal{N}\mathfrak{p}_h^{-s}\right)^{-1}. \qquad \square$$

Once we have computed the value $\Lambda(1,\chi)$ for all characters χ such that $\chi(\tau)=-1$, we obtain the values of $L'_S(0,\chi)$ and the values of $\zeta'_S(0,\sigma)$ for all $\sigma\in G$. In order to deduce from these values the conjugates of ε, we need to remove the absolute value appearing in Conjecture 1.2. Since we have already assumed that $w(\varepsilon)>0$, it is a direct consequence of the second assertion of the conjecture (namely $N(\sqrt{\varepsilon})/K$ is Galois) that all the others conjugates of ε over K are also positive at w. Hence, we can approximate the irreducible polynomial of α over K by writing

$$\tilde P(X)=\prod_{\sigma}\bigl(X-(e^{-2Z_\sigma}+e^{2Z_\sigma})\bigr),$$

where σ runs through a system of representatives of $G/\langle\tau\rangle$ (which is isomorphic to $\operatorname{Gal}(L/K)$) and Z_σ denotes the approximation of $\zeta'_S(0,\sigma)$ which has been computed (note that $Z_\sigma=-Z_{\tau\sigma}$).

We need to recognize the coefficients of $\tilde P(X)$ as the v-embedding of algebraic integers of K. For the other embeddings, Lemma 2.8 gives us $|\alpha|_{w'}\leq 2$ for any infinite place w' of N which does not divide v, and thus provides bounds on the embeddings of these coefficients at the others infinite places of K. Now there exist finitely many algebraic integers of a given degree such that all their conjugates are bounded, and thus finitely many algebraic integers in K which are very close to a given real number at the infinite place v and bounded at all the others, and we can list them (in fact, if the precision is sharp enough, we obtain only one candidate for each coefficient). Once we have recognized all the coefficients of $\tilde P$, we obtain a polynomial $P(X)\in\mathcal{O}_K[X]$.

Finally, we need to prove that P is indeed the irreducible polynomial of a generating element of L. It is quite easy to prove that P is irreducible. If so, let $\tilde L$ denote the field it defines. It is also easy to check that the field $\tilde L$ is totally real and to compute the relative discriminant of $\tilde L/K$ (see [Cohen et al. 1996] for algorithms to perform these tasks). Once all these checks have been done, we still need to prove that the extension $\tilde L/K$ is abelian and that its norm group is the same as the one of L/K. Although this can be done quite easily when the degree of the extension is small, it is a difficult task in general and we will not go into details here (see [Roblot 1997]). However, under the Generalized Riemann Hypothesis (GRH), it is possible to find an algorithm which at the same time proves that the extension is abelian and computes its norm group.

We just quote the key result here (which rely on the theorem of Bach and Sorenson [1996]), and we refer the interested reader to [Roblot 1997].

Theorem 3.3. *Assume GRH is true. Let $\tilde{L}/K$ be a finite extension of totally real number fields, and let d, $\mathfrak{d}$ denote respectively the absolute discriminant of $\tilde{L}$, and the relative discriminant of $\tilde{L}/K$. Set*

$$C = \left(4\log d + \tfrac{5}{2}[\tilde{L} : \mathbb{Q}] + 5\right)^2,$$

and let $\mathfrak{S}$ denote the set of prime ideals of K of degree 1, unramified in $\tilde{L}/K$, and of absolute norm smaller than C. Then $\tilde{L}/K$ is an abelian extension if and only if

(i) *all prime ideals $\mathfrak{P}$ in $\tilde{L}$ dividing $\mathfrak{p} \in \mathfrak{S}$ have the same residual degree $f_{\mathfrak{p}}$, and*
(ii) *the group $\mathfrak{N}$ generated by $\mathfrak{p}^{f_{\mathfrak{p}}}$, as $\mathfrak{p}$ ranges through $\mathfrak{S}$, and $P_K(\mathfrak{d})$ has index $[\tilde{L} : K]$ in $I_K(\mathfrak{d})$.*

Furthermore, if these two conditions are satisfied, $\mathfrak{N}$ is the norm group of $\tilde{L}/K$.

4. TWO EXAMPLES

This method has been used to compute the Hilbert Class Field of totally real fields of degrees 2, 3, and 4 and various ray class fields (see [Roblot 1997]) using PARI [Batut et al. 1999]. At the address http://www.math.u-bordeaux.fr/~roblot/resources/hilb.gp one can find a table of the Hilbert Class Field of all real quadratic fields of discriminant less than 10 000, real cubic fields of discriminant less then 150 000 and real quartic fields of discriminant less than 600 000 — a total of 3303 non-principal fields.

We now give two examples of the construction of real abelian extensions of a totally real field using Theorem 2.1. Similar use of Stark's Conjectures to construct class fields can be found in [Cohen and Roblot 2000; Dummit et al. 1997; Stark 1976; 1980]. One can also use Kummer Theory to compute class fields; see for example [Daberkow and Pohst 1995; Fieker 2000].

These two examples where computed with the latest version of GP/PARI (version 2.0.13 alpha) on a DEC Alpha 2100 300MHz with 512Mb of memory. Computation times are provided at the end of each example.

Example 4.1. Let K be the real quadratic field generated over $\mathbb{Q}$ by a square root ω of 82. The discriminant is 328, and $\{1, \omega\}$ forms a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_K$. The field we wish to construct is $L = H_K$, the Hilbert Class Field of K, that is, the maximal abelian extension of K unramified everywhere, which is a cyclic extension of degree 4 of K.

A quadratic extension N/L verifying conditions (A)–(C) and with minimal (norm of) conductor is given by the ray class field modulo $\mathfrak{f} = \mathfrak{p}_3 v_1$ where

$$\mathfrak{p}_3 = 3\mathcal{O}_K + (2\omega - 1)\mathcal{O}_K$$

is a prime ideal dividing 3, and v_1 is the real place sending ω to the negative square root of 82 in $\mathbb{R}$. The extension N/K is a cyclic extension of degree 8, so this extension cannot be constructed using the proof of Proposition 2.3. In fact, the first extension that one can construct using Proposition 2.3 has a conductor of norm 16, and it is certainly more efficient not to use this one but the former (see next remark).

Let G denote the Galois group of N/K, let σ be a generator of G and let $\tau = \sigma^4$ be the unique element of order 2 (τ generates the Galois group of N/L). It is easy to prove that all characters χ of G such that $\chi(\tau) = -1$ have conductor $\mathfrak{f}$, hence $L_S(s, \chi) = L(s, \chi)$ for any such character. We compute the values of $L'(0, \chi)$ and obtain the values of the derivatives of partial zeta functions, as follows. (The computations have been made with much more precision than given in this paper.)

$$\begin{aligned}
\zeta'_S(0, 1) &= -1.855345769803922\ldots, \\
\zeta'_S(0, \tau) &= -\zeta'_S(0, \sigma), \\
\zeta'_S(0, \sigma) &= -0.811399495928109\ldots, \\
\zeta'_S(0, \tau\sigma) &= -\zeta'_S(0, \sigma), \\
\zeta'_S(0, \sigma^2) &= -1.056128108731457\ldots, \\
\zeta'_S(0, \tau\sigma^2) &= -\zeta'_S(0, \sigma^2), \\
\zeta'_S(0, \sigma^3) &= 0.597654704583391\ldots, \\
\zeta'_S(0, \tau\sigma^3) &= -\zeta'_S(0, \sigma^3).
\end{aligned}$$

Remark 4.2. The logarithmic height of ε (see [Lang 1983] for a definition) is

$$2\left(|\zeta'_S(0,1)| + |\zeta'_S(0,\sigma)| + |\zeta'_S(0,\sigma^2)| + |\zeta'_S(0,\sigma^3)|\right) = 8.64105615809373\ldots$$

(since we know that the other conjugates of ε have an absolute value of 1 by Lemma 2.8). If instead, we had used the class field of conductor 16 for this construction, the logarithmic height of ε would have been $16.985931238837\ldots$, that is to say nearly 2 times larger (the heuristics quoted at the beginning of section 3 give $\sqrt{16/3} \approx 2.3$). This illustrates why we need to find a suitable N with minimal conductor to speed up the computations.

The polynomial $\tilde{P}$ (with the above notation) is

$$\begin{aligned} X^4 &- 58.16615541441224X^3 \\ &+ 799.4369460780463X^2 \\ &- 3980.184730390231X \\ &+ 6515.938649729469, \end{aligned}$$

and we "recognize" this polynomial as the embedding of the following polynomial of $\mathcal{O}_K[X]$:

$$\begin{aligned} P(X) = X^4 - (3\omega + 31)X^3 + (44\omega + 401)X^2 \\ - (220\omega + 1988)X + (360\omega + 3256). \end{aligned}$$

Although the discriminant of this polynomial is far from trivial (its norm is $2^8 3^{12} 73^2$), it nevertheless defines an unramified extension of K of degree 4. Thus, to prove that this extension is indeed the Hilbert Class Field of K, it remains to prove that it is abelian. For that purpose, it suffices to prove that it is Galois since the only Galois groups of order 4 of quartic extensions are abelian groups (namely the cyclic group of order 4 and the Klein group). There are various way to prove this. One way is to compute an absolute (and in this case reduced) polynomial over $\mathbb{Q}$ defining the same field and to compute its Galois group. In our case, we obtain the polynomial

$$\begin{aligned} X^8 - 4X^7 - 14X^6 + 56X^5 + 49X^4 \\ - 196X^3 + 28X^2 + 80X - 25, \end{aligned}$$

whose Galois group is the dihedral group of order 8 which proves that the field it defines is abelian over K and thus is the Hilbert Class Field of $\mathbb{Q}(\sqrt{82})$.

This example was computed in 4 seconds. The computation of the polynomial $P(X)$ took 3 seconds, and the verification (computation of the relative discriminant, and of the Galois group) took less than one second.

Example 4.3. Let K be the field generated over $\mathbb{Q}$ by a root α of the polynomial

$$X^3 - 4X - 1.$$

This is a real cubic field of discriminant 229 and with ring of integers $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $\mathfrak{m}$ denote the prime ideal above 37 defined by

$$\mathfrak{m} = 37\mathcal{O}_K + (8 + \alpha)\mathcal{O}_K;$$

we want to construct the ray class field L of K modulo $\mathfrak{m}$. This is an abelian extension of K of degree three.

Using the proof of Proposition 2.3, one can choose for N the field generated over L by a square root of $\varkappa = \alpha$. This yields an abelian extension of K of degree 6 and conductor $\mathfrak{m} v_1 v_2$ where v_1 and v_2 are the infinite places sending α to $-1.860805\ldots$ and $-0.254101\ldots$, respectively. Here, it is clear that N is of minimal norm. As usual, we denote by G the Galois group of N/K, by τ the non-trivial element of $\mathrm{Gal}(N/L)$ and by σ a generator of G. Let χ denote the character of G such that $\chi(\sigma) = \exp(2i\pi/6)$. This is a generator of the group of characters of G.

The characters of G which are non-trivial on τ are χ, χ^3 and χ^5, since $\chi(\tau) = -1$. For these, we compute the Artin root numbers

$$\begin{aligned} W(\chi) &= -0.367664745\ldots - 0.92995840\ldots i, \\ W(\chi^3) &= 1, \qquad W(\chi^5) = \overline{W(\chi)}, \end{aligned}$$

and the corrective factors

$$A(\chi) = 1, \quad A(\chi^3) = 2, \quad A(\chi^5) = 1.$$

This gives us the following values for the partial zeta functions:

$$\begin{aligned} \zeta'_S(0, 1) &= 1.96011188229224\ldots, \\ \zeta'_S(0, \tau) &= -\zeta'_S(0, 1), \\ \zeta'_S(0, \sigma) &= 1.57294437150264\ldots, \\ \zeta'_S(0, \tau\sigma) &= -\zeta'_S(0, \sigma), \\ \zeta'_S(0, \sigma^2) &= 0.72454531436117\ldots, \\ \zeta'_S(0, \tau\sigma^2) &= -\zeta'_S(0, \sigma^2), \end{aligned}$$

and the polynomial

$$\begin{aligned} X^3 &- 78.20893338606214X^2 \\ &+ 1505.492174458384X \\ &- 5276.952425687298, \end{aligned}$$

which can be seen to be very close to the polynomial

$$\begin{aligned} P(X) = X^3 &- (9\alpha^2 + 17\alpha + 2)X^2 \\ &+ (160\alpha^2 + 338\alpha + 75)X \\ &- (560\alpha^2 + 1185\alpha + 266). \end{aligned}$$

One can check that the field extension L generated by a root of this polynomial is a totally real field of degree 9 and that its relative discriminant is $\mathfrak{m}^2$. Since this is a square and since L/K is a cubic extension, it follows from Galois Theory that it is an abelian extension (Galois group of cubic extensions are S_3 or $A_3 \simeq C_3$, and the latter occurs if and only if the discriminant is a square). Since L/K is an abelian extension of prime degree $l = 3$, the Führerdiskriminantenproduktformel tells us that its discriminant is equal to its conductor raised to the power $l - 1 = 2$. Thus, $\mathfrak{m}$ is the conductor of L/K, and that finishes the proof that this is indeed the field L that we wanted. For completeness, we give a reduced polynomial that defines L over $\mathbb{Q}$:

$$X^9 + 2X^8 - 9X^7 - 11X^6 + 28X^5 + 18X^4 - 34X^3 - 8X^2 + 13X - 1.$$

This example was computed in 24 seconds. The computation of the polynomial $P(X)$ took 23 seconds, and the verification (computation of the relative discriminant) took less than one second.

ACKNOWLEDGEMENT

I thank David Solomon for his careful reading of the original manuscript and for his comments.

REFERENCES

[Bach and Sorenson 1996] E. Bach and J. Sorenson, "Explicit bounds for primes in residue classes", *Math. Comp.* **65**:216 (1996), 1717–1735.

[Batut et al. 1999] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, "Pari-GP, version 2.0", software, 1999. See ftp://megrez.math.u-bordeaux.fr/pub/pari.

[Cohen and Roblot 2000] H. Cohen and X.-F. Roblot, "Computing the Hilbert class field of a real quadratic field", *Math. Comp.* **69** (2000), 1229–1244. See http://www.math.u-bordeaux.fr/~cohen/.

[Cohen et al. 1996] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Algorithmic techniques for relative extensions of number fields", preprint, 1996.

[Cohen et al. 1998] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Computing ray class groups, conductors and discriminants", *Math. Comp.* **67**:222 (1998), 773–795.

[Daberkow and Pohst 1995] M. Daberkow and M. Pohst, "Computations with relative extensions of number fields with an application to the construction of Hilbert class fields", pp. 68–76 in *Proc. ISSAC'95*, ACM Press, New York, 1995.

[Dummit and Tangedal 1998] D. Dummit and B. Tangedal, "Computing the leading term of an abelian L-function", pp. 400–411 in *Algorithmic number theory: third international symposium, ANTS-III* (Portland, OR), edited by J. P. Buhler, Lecture Notes in Comp. Sci. **1423**, Springer, Berlin, 1998.

[Dummit et al. 1997] D. S. Dummit, J. W. Sands, and B. A. Tangedal, "Computing Stark units for totally real cubic fields", *Math. Comp.* **66**:219 (1997), 1239–1267.

[Fieker 2000] C. Fieker, "Computing class fields via the Artin map", to appear in *Math. Comp.* (2000). PII S0025-5718(00)01255-2.

[Friedman 1988] E. Friedman, "Hecke's integral formula", Exp. No. 5, 23 in *Séminaire de Théorie des Nombres,* 1987–1988, Univ. Bordeaux I, Talence, 1988.

[Lang 1983] S. Lang, *Fundamentals of Diophantine geometry*, Springer, New York, 1983.

[Martinet 1977] J. Martinet, "Character theory and Artin L-functions", pp. 1–87 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977.

[Roblot 1997] X.-F. Roblot, *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon*, Thèse, Université Bordeaux I, Talence, 1997.

[Stark 1971] H. M. Stark, "Values of L-functions at $s = 1$, I: L-functions for quadratic forms", *Advances in Math.* **7** (1971), 301–343 (1971).

[Stark 1975] H. M. Stark, "L-functions at $s = 1$, II: Artin L-functions with rational characters", *Advances in Math.* **17**:1 (1975), 60–92.

[Stark 1976] H. M. Stark, "L-functions at $s = 1$, III: Totally real fields and Hilbert's twelfth problem", *Advances in Math.* **22**:1 (1976), 64–84.

[Stark 1980] H. M. Stark, "L-functions at $s = 1$, IV: First derivatives at $s = 0$", *Adv. in Math.* **35**:3 (1980), 197–235.

[Tate 1984] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, Birkhäuser, Boston, 1984.

[Tollis 1997] E. Tollis, "Zeros of Dedekind zeta functions in the critical strip", *Math. Comp.* **66**:219 (1997), 1295–1321.

Xavier-François Roblot, Department of Computer Science, Concordia University, 1445 de Maisonneuve Blvd. West, Montreal, Quebec H3G 1M8, Canada (roblot@cs.concordia.ca)

Received October 10, 1998; accepted in revised from May 10, 1999