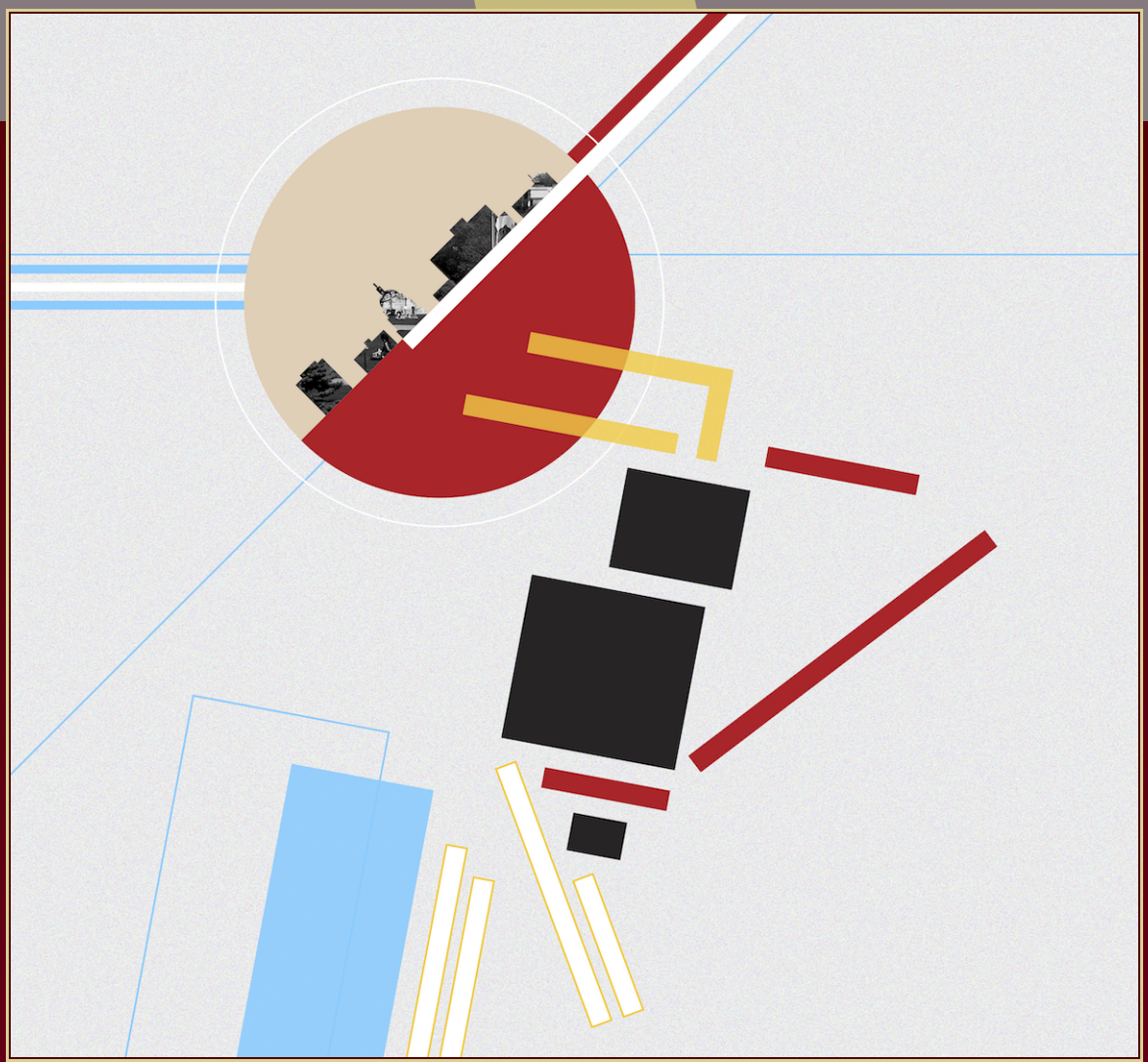
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Explicit computations in Iwasawa theory

Reinier Bröker, David Hubbard, and Lawrence C. Washington



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.137

Explicit computations in Iwasawa theory

Reinier Bröker, David Hubbard, and Lawrence C. Washington

We give two algorithms to compute layers of the anticyclotomic $\mathbb{Z}_3$-extension of an imaginary quadratic field. The first is based on complex multiplication techniques for nonmaximal orders; the second is based on Kummer theory. As an illustration of our results, we use the mirroring principle to derive results on the structure of class groups of nonmaximal orders.

1. Introduction

Let K be an imaginary quadratic field, with fixed algebraic closure $\overline{K}$, and for a fixed odd prime p, let $K^p \subset \overline{K}$ be the compositum of all $\mathbb{Z}_p$-extensions. The Galois group of K^p/K is isomorphic to $\mathbb{Z}_p^2$, and there are two "natural" $\mathbb{Z}_p$-extensions of K inside K^p. The *cyclotomic* $\mathbb{Z}_p$*-extension* K_p^{cycl} is the p-part of the extension $\bigcup_{n\geq 1} K(\zeta_{p^n}) \subset \overline{K}$. The extension $K_p^{\mathrm{cycl}}/\mathbb{Q}$ is procyclic. The *anticyclotomic* $\mathbb{Z}_p$*-extension* K_p^{anti} is implicitly defined by the property that $K_p^{\mathrm{anti}} \subset \overline{K}$ is the unique $\mathbb{Z}_p$-extension of K that is *prodihedral* over $\mathbb{Q}$, meaning that we have

$$\mathrm{Gal}(K_p^{\mathrm{anti}}/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z},$$

where the generator of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ acts by inversion on $\mathbb{Z}_p$.

The fields K_p^{cycl} and K_p^{anti} are linearly disjoint over K, and their compositum equals K^p. Since both have Galois group $\mathbb{Z}_p$, both extensions are unramified outside of p by [16, Proposition 13.2]. This article focuses on *explicitly computing* layers of K_3^{anti} for the case where 3 is ramified in K. By computing, we mean that on input of a positive integer k, we want to compute an irreducible polynomial $f \in K[x]$ of degree 3^k with

$$K_k = K[x]/(f(x)) \subset K_3^{\mathrm{anti}}.$$

The Galois group $\mathrm{Gal}(K_k/K)$ is cyclic of order 3^k.

Although we believe that most of our techniques can be generalized to arbitrary p and arbitrary splitting behavior of p, our restrictions to $p = 3$ and to the case that 3 ramifies in K allow us to highlight the technical considerations that arise in those cases. Furthermore, we can use the *mirror principle* (see Section 5) to obtain a criterion for when the 3-parts of certain class groups are cyclic.

MSC2010: primary 11R23; secondary 14K22.
Keywords: anticyclotomic, Iwasawa theory, nonmaximal order.

The main result of this paper is that we have explicit algorithms to compute K_k. We use complex multiplication (CM) techniques in Sections 2 and 3, and Kummer techniques in Section 6. The CM technique works for any K; the Kummer technique is more restricted.

Previous attempts to compute initial layers of anticyclotomic $\mathbb{Z}_p$-extensions of an imaginary quadratic field include [3; 6; 11; 15]. These papers use a mix of class field theory and decomposition laws of primes.

Perhaps not surprisingly, the *run times* of our algorithms are inherently exponential. Not only are the outputs of the algorithms polynomials of degree 3^k, but the CM approach computes, as intermediate step, a polynomial whose degree and logarithmic height of its coefficients are both $\widetilde{O}(|\mathrm{disc}(K)|^{1/2}3^k)$. For the Kummer approach, we need a polynomial of degree $O(3^k)$ over an auxiliary extension of degree $O(3^k)$; furthermore, the coefficients are themselves symmetric expressions in $O(3^k|\mathrm{disc}(K)|)$ terms.

Both approaches have their merits. Indeed, whereas the CM method requires the full class group of K as intermediate step, the Kummer method only looks at the prime 3. If the class group is large, then the Kummer method is better for small n. However, the Kummer method requires working over auxiliary extensions and this makes the method slower for larger n.

We detail various techniques we can use to reduce the size of the generating polynomial for K_k in Section 4. We illustrate our techniques with a variety of examples. All examples were done using the computer algebra package Magma [2] and the CM software package [9].

2. Anticyclotomic extension and ring class fields

Throughout this section, let $K = \mathbb{Q}(\sqrt{D})$ be a fixed imaginary quadratic field of discriminant D in which 3 is ramified. We let $\mathbb{O}$ be the maximal order of K. For any integer $k \geq 1$, the k-th layer K_k of the anticyclotomic $\mathbb{Z}_3$-extension of K is a generalized dihedral extension of $\mathbb{Q}$. Hence, by Bruckner's result (see [5] or [8, Theorem 9.18]), we know that K_k is contained in a *ring class field* for K. Since K_k is unramified outside 3, it follows that K_k is contained in a ring class field for an order $\mathbb{O}_N = \mathbb{Z} + 3^N\mathbb{O}$ of index 3^N for some $N \geq 1$.

In order to bound the exponent, we analyze ring class fields. We let H_N be the ring class field for the order $\mathbb{O}_N$. With this notation, H_0 is the Hilbert class field of K. The extension H_N/K is abelian and unramified outside 3. The Artin map gives an isomorphism $\mathrm{Pic}(\mathbb{O}_N) \xrightarrow{\sim} \mathrm{Gal}(H_N/K)$, with $\mathrm{Pic}(\mathbb{O}_N)$ the *Picard group* of $\mathbb{O}_N$. We have a natural exact sequence

$$1 \to (\mathbb{O}/3^N\mathbb{O})^*/\operatorname{Im}(\mathbb{O}^*)(\mathbb{Z}/3^N\mathbb{Z})^* \to \mathrm{Pic}(\mathbb{O}_N) \to \mathrm{Pic}(\mathbb{O}) \to 1,$$

where the last map is given by $[I] \mapsto [I \cdot \mathbb{O}]$. The kernel of the map $\mathrm{Pic}(\mathbb{O}_N) \to \mathrm{Pic}(\mathbb{O})$ is naturally isomorphic to $\mathrm{Gal}(H_N/H_0)$; the following lemma gives the structure of this group.

Lemma 2.1. *With the notation from the previous paragraph, we have*

$$\mathrm{Gal}(H_N/H_0) \cong \begin{cases} \mathbb{Z}/3^{N-1}\mathbb{Z} & \text{if } D = -3, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^{N-1}\mathbb{Z} & \text{if } D \neq -3 \text{ and } D \equiv -3 \bmod 9, \\ \mathbb{Z}/3^N\mathbb{Z} & \text{if } D \equiv 3 \bmod 9 \end{cases}$$

for $N \geq 1$.

Proof. Let $\mathfrak{p} \mid (3)$ be the ideal of norm 3 in $\mathbb{O}$. We have $(\mathbb{O}/\mathfrak{p}^{2N})^* \cong (A/\mathfrak{p}^{2N})^*$, where A denotes the completion of $\mathbb{O}$ at $\mathfrak{p}$. The ring A is a tamely ramified quadratic extension of $\mathbb{Z}_3$, and it well known that there are only *two* such rings up to isomorphism. For $D \equiv -3 \bmod 9$, we have $A = \mathbb{Z}_3[\sqrt{-3}] = \mathbb{Z}_3[\zeta_3]$, and $A = \mathbb{Z}_3[\sqrt{3}]$ for $D \equiv 3 \bmod 9$. We analyze both cases separately.

The unit group of $A = \mathbb{Z}_3[\zeta_3]$ equals

$$A^* = \langle -\zeta_3 \rangle \times (1 + \mathfrak{p}^2),$$

and $1 + \mathfrak{p}^2$ is torsion free. Hence, $1 + \mathfrak{p}^2$ is a free $\mathbb{Z}_3$-module of rank 2. We get

$$(A/3^N A)^* \cong \langle -\zeta_3 \rangle \times (1 + \mathfrak{p}^2)/(1 + \mathfrak{p}^{2N}) \cong \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/3^{N-1}\mathbb{Z})^2,$$

and hence

$$(A/3^N A)^*/(\mathbb{Z}/3^N\mathbb{Z})^* \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^{N-1}\mathbb{Z}.$$

For $A = \mathbb{Z}_3[\sqrt{3}]$, we have

$$A^* = \langle -1 \rangle \times (1 + \mathfrak{p}),$$

and since ζ_3 is not contained in A, the $\mathbb{Z}_3$-module $1 + \mathfrak{p}$ is torsion free and hence a free rank 2 module. By iteratively applying the "cubing isomorphism" $1 + \mathfrak{p}^k \xrightarrow{\sim} 1 + \mathfrak{p}^{k+2}$ we see that

$$(A/3^N A)^* \cong \langle -1 \rangle \times (1 + \mathfrak{p})/(1 + \mathfrak{p}^{2N}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^N\mathbb{Z} \times \mathbb{Z}/3^{N-1}\mathbb{Z}$$

holds. Since the module $1 + \mathfrak{p}$ is generated over $\mathbb{Z}_3$ by $1 + 3$ and $1 + \sqrt{3}$, we get

$$(A/3^N A)^*/(\mathbb{Z}/3^N\mathbb{Z})^* \cong \mathbb{Z}/3^N\mathbb{Z}.$$

We have $\mathbb{O}^* = \{\pm 1\}$ for $D < -3$, and the only case where the local cube root of unity exists globally is $D = -3$. Quotienting by $\mathrm{Im}(\mathbb{O}^*)$ gives the lemma. □

For $D \equiv -3 \bmod 9$ with $D < -3$, we let $\alpha_N \in \mathbb{O}$ be an element that is congruent to $\zeta_3 \in A$ modulo 3^N. (As in the proof of Lemma 2.1, A denotes the completion of $\mathbb{O}$ at $\mathfrak{p}$.) This element α_N determines an *Artin symbol* $\left(\frac{\alpha_N}{H_N/H_0}\right) \in \mathrm{Gal}(H_N/H_0)$. We let H'_N be the fixed field of the order 3 subgroup $\left\langle \left(\frac{\alpha_N}{H_N/H_0}\right)\right\rangle$ and put

$$H_\infty = \begin{cases} \bigcup_{N \geq 1} H'_N/H_0 & \text{for } D \equiv -3 \bmod 9 \text{ and } D \neq -3, \\ \bigcup_{N \geq 1} H_N/H_0 & \text{otherwise.} \end{cases}$$

Theorem 2.2. *Let K_k be the k-th layer of the anticyclotomic $\mathbb{Z}_3$-extension of K. Then K_k is contained in the ring class field for the order $\mathbb{O}_{k+1} = \mathbb{Z} + 3^{k+1}\mathbb{O}$ of index 3^{k+1}.*

Proof. It is clear that $H_N/\mathbb{Q}$ is generalized dihedral. From Lemma 2.1 and the relation

$$\mathbb{O}_N \subseteq \mathbb{O}_M \implies H_M \subseteq H_N$$

from class field theory, also known as the *Anordnungssatz* for ring class fields, we see that

$$\mathrm{Gal}(H_\infty/H_0) \cong \mathbb{Z}_3.$$

An inspection of the sizes in Lemma 2.1 now gives that the compositum $K_k H_0$ is contained in H_{k+1}. The theorem follows. □

The theory of *complex multiplication* provides us with a means of explicitly computing the extension H_N/K. This theory is usually only developed for *maximal* orders, but it generalizes to nonmaximal orders without too much difficulty. Indeed, by [8, Theorem 11.1] we know that

$$H_N = K[x]/(f_N(x)),$$

with $f_N \in \mathbb{Z}[x]$ the minimal polynomial of the j-invariant of the complex elliptic curve $\mathbb{C}/\mathcal{O}_N$. There are various algorithms to compute f_N; we refer to [1] and the references therein for an overview. However, since the proven upper bound $\widetilde{O}(|\mathrm{disc}(\mathcal{O}_N)^2|)$ (see, e.g., [1, §5]) on the bit size of f_N is believed to be the actual size of f_N, these algorithms are inherently exponential. We will give various practical improvements in Section 4 to this basic approach.

3. Selecting the right subfield

As before, let K be a fixed imaginary quadratic field in which 3 is ramified. We have seen that the k-th layer K_k of the anticyclotomic $\mathbb{Z}_3$-extension of K is contained in the ring class field H_{k+1}. In this section we explain a method to compute K_k as a subfield of H_{k+1}. To keep the sizes of the generating polynomials small, the examples given in this section already use the algorithmic improvements explained in Section 4. The online supplement at http://msp.org/obs/2019/2-1/obs-v2-n1-x09-Examples.txt provides Magma code to compute the examples.

We first assume that K has trivial 3-Hilbert class field. In this case, we have

$$[H_k : K_k] = \#\mathrm{Pic}(\mathcal{O}) \quad \text{for } D \equiv 3 \bmod 9$$

and K_k is the unique subfield of H_k that has degree 3^k over K. For $K = \mathbb{Q}(\sqrt{-3})$, K_k is the unique subfield of degree 3^k of H_{k+1}. For other $D \equiv -3 \bmod 9$, we proceed as follows. As in the discussion preceding Theorem 2.2, we let $\alpha_{k+1} \in \mathcal{O}$ be locally congruent to ζ_3 modulo 3^{k+1}. The fixed field H'_{k+1} of the automorphism $\left(\frac{\alpha_{k+1}}{H_{k+1}/H_0}\right)$ has a unique subfield of degree 3^k over K; this field is the field K_k that we are after.

Example 3.1. The field $K = \mathbb{Q}(\sqrt{-21})$ has class group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The index 4 subfield of the ring class field H_1 is generated by a root of $x^3 - 6x - 12$, but it is *not* part of the anticyclotomic $\mathbb{Z}_3$-extension.

The index 4 subfield $\widetilde{K}_1$ of the ring class field H_2 is obtained by adjoining a root of

$$x^9 + 12x^6 + 81x^5 + 144x^4 + 30x^3 - 324x^2 - 504x - 336$$

to K. The Galois group $\widetilde{K}_1/K$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. To obtain the first layer, we compute that $\alpha_2 = 1 + \sqrt{-21}$ is locally congruent to ζ_3 modulo 9. We take the fixed field of the Artin symbol corresponding to α_2. We find that K_1 is generated by a root of

$$x^3 + 9x - 12$$

over K.

For the general case, we let $H_{0,3}$ be the 3-Hilbert class field of K. The extension H_∞/H_0 naturally defines a $\mathbb{Z}_3$-extension $H_{\infty,3}/H_{0,3}$. The sequence

$$1 \to \mathrm{Gal}(H_{\infty,3}/H_{0,3}) \to \mathrm{Gal}(H_{\infty,3}/K) \to \mathrm{Gal}(H_{0,3}/K) \to 1 \tag{1}$$

need not split in general. If it does split, then $H_{0,3}$ is *not* contained in the anticyclotomic $\mathbb{Z}_3$-extension and finding the layers proceeds as before. Determining whether the sequence splits is often easy. In Section 5, we will give a simple criterion (Theorem 5.1) under which $H_{0,3}$ is not contained in the anticyclotomic $\mathbb{Z}_3$-extension. Furthermore, the following examples show that it is computationally very easy to determine if $H_{0,3}$ lies in the anticyclotomic $\mathbb{Z}_3$-extension or not.

Example 3.2. Fix $K = \mathbb{Q}(\sqrt{-87})$. The class group of $\mathcal{O}$ is cyclic of order 6. The order $\mathcal{O}_1$ of index 3 has cyclic Picard group of order 18. We may replace $H_{\infty,3}$ with $H_{1,3}$ in sequence (1) to obtain the nonsplit sequence

$$1 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to 1.$$

Hence, the 3-part of the Hilbert class field of K is the first layer of the anticyclotomic $\mathbb{Z}_3$-extension. Explicitly, we have

$$K_1 = K[x]/(x^3 - x^2 + 2x + 1).$$

The index 2 subfield of the ring class field for $\mathcal{O}_1$ gives the *second* layer of the anticyclotomic $\mathbb{Z}_3$ extension. It is generated by a root of

$$x^9 + 3x^8 + 6x^7 + 14x^6 + 9x^5 + 21x^4 + 6x^3 + 12x^2 + 3.$$

For $K = \mathbb{Q}(\sqrt{-771})$ we obtain the split sequence

$$1 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to 1$$

and the Hilbert class field is not contained in the anticyclotomic $\mathbb{Z}_3$-extension.

If the 3-part of $\mathrm{Pic}(\mathcal{O})$ is different from $\mathbb{Z}/3\mathbb{Z}$, the situation is slightly more involved. In the remainder of this section we explain how to split the 3-part $\mathrm{Pic}(\mathcal{O})_3$ into a part "inside" and a part "outside" of the anticyclotomic $\mathbb{Z}_3$-extension.

We let $S_{\max} \subseteq \mathrm{Pic}(\mathcal{O})_3$ be the largest subgroup (with respect to inclusion) for which the sequence

$$1 \to \mathrm{Gal}(H_{\infty,3}/H_{0,3}) \to \mathrm{Gal}(H_{\infty,3}/H_{0,3}^{S_{\max}}) \to S_{\max} \to 1$$

splits. Here, $H_{0,3}^{S_{\max}}$ is the fixed field of $H_{0,3}$ for $S_{\max}$. This fixed field is the largest subfield of $H_{0,3}$ that is contained in the anticyclotomic $\mathbb{Z}_3$-extension.

For ease of notation, we restrict to the case $D \equiv 3 \bmod 9$ so $H_{\infty,3}$ is the inverse limit of the 3-parts $\mathrm{Pic}(\mathcal{O}_N)_3$ of the ring class field for $\mathcal{O}_N$. Let $\langle \mathfrak{p} \rangle \subset \mathrm{Pic}(\mathcal{O})_3$ be a subgroup of 3-power order with $\mathfrak{p}$ coprime to 3. The ideal $\mathfrak{p} \cap \mathcal{O}_N$ is an invertible $\mathcal{O}_N$-ideal whose class in $\mathrm{Pic}(\mathcal{O}_N)_3$ maps to the class of $\mathfrak{p}$ in $\mathrm{Pic}(\mathcal{O})_3$. The other preimages are $(\mathfrak{p} \cap \mathcal{O}_N)I$, with I ranging over the kernel of $\mathrm{Pic}(\mathcal{O}_N)_3 \to \mathrm{Pic}(\mathcal{O})_3$. We compute

the order inside $\mathrm{Pic}(\mathcal{O}_N)_3$ for each of the preimages of $\mathfrak{p}$, and check if one of those equals the order of $[\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O})_3$. If it does, the sequence

$$1 \to \mathrm{Gal}(H_{N,3}/H_{0,3}) \to \mathrm{Gal}(H_{N,3}/H_{0,3}^{\langle\mathfrak{p}\rangle}) \to \langle\mathfrak{p}\rangle \to 1$$

splits; otherwise it does not.

Example 3.3. Fix $K = \mathbb{Q}(\sqrt{-6789})$. We have $\mathrm{Pic}(\mathcal{O}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathrm{Pic}(\mathcal{O}_1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. The kernel of the map $\mathrm{Pic}(\mathcal{O}_1) \to \mathrm{Pic}(\mathcal{O})$ is generated by the class of the $\mathcal{O}_1$-ideal

$$I = \mathcal{O}_1(9, 3\sqrt{-6789} - 3)$$

of norm 9. There are four subgroups of $\mathrm{Pic}(\mathcal{O})$ of index 3; elements of order 6 in these subgroups are ideals of norm 5, 7, 11, and 97, respectively. The ideal $\mathfrak{p}_5$ has order 6 in $\mathrm{Pic}(\mathcal{O})$, but $I^k(\mathfrak{p} \cap \mathcal{O}_1)$ has order 18 for $k = 0, 1, 2$ and likewise for $\mathfrak{p}_7$ and $\mathfrak{p}_{97}$. On the other hand, the ideal $(\mathfrak{p}_{11} \cap \mathcal{O}_1)$ has order 6.

The fixed field of H_0 under the subgroup of $\mathrm{Pic}(\mathcal{O})$ generated by $\mathfrak{p}_{11}$ (of order 6), $\mathfrak{p}_5^3$ (of order 2), and $\mathfrak{p}_2 = \mathcal{O}_1(2, 3\sqrt{-6789} + 1)$ (of order 2) equals the first layer K_1 of the anticyclotomic $\mathbb{Z}_3$-extension of K. To find a generating polynomial, we compute the maximal real subfield of H_0 using CM theory and compute its 4 degree 3 subfields $L_1, \ldots, L_4$. We now check whether the Artin symbol corresponding to $\mathfrak{p}_{11}$ acts trivially on KL_i/K. As expected, it does so for a unique field. In the end, we find that a root of

$$x^3 - x^2 + 8x + 124$$

generates K_1/K.

4. Practical improvements

The techniques described yield generating polynomials that are much larger than necessary. The reason for this is that the j-function is *not* the right function to use from a practical perspective to compute a ring class field. For every given discriminant, a suitably chosen *class invariant* can be used instead. The use of class invariants dates back to Weber's days, and modern treatments rely on *Shimura reciprocity*. We refer to [14; 12] for good descriptions and give the main result that we need.

Theorem 4.1. *Let $D < 0$ be a discriminant, and choose a quadratic generator τ for the imaginary order of discriminant D. Then there exists a modular function f of level $n > 1$ such that $f(\tau)$ generates the ring class field; furthermore, the minimal polynomial of $f(\tau)$ over $K = \mathbb{Q}(\sqrt{D})$ can be explicitly computed in time $\widetilde{O}(|D|)$.*

Proof. We refer to [12, Theorem 4; 10, Corollary 3.1] for two classes of functions. □

The size of the generating polynomial for the ring class field depends on the choice of the function f in the theorem. To compute the "reduction factor", we let $\Psi(j, f) = 0$ be the irreducible polynomial relation between j and f and put

$$r(f) = \frac{\deg_f(\Psi(f, j))}{\deg_j(\Psi(f, j))} \in \mathbb{Q}_{>0}.$$

As in [4, §4], we expect the logarithmic height of the coefficients of the minimal polynomial of $f(\tau)$ to be a factor $r(f)$ smaller than the corresponding coefficients for $j(\tau)$. By [4, Theorem 4.1], we have

$$r(f) \leq 800/7 \approx 114.28.$$

If 2 splits in $\mathbb{O}$, then the cube of the Weber-$\mathfrak{f}$ can be used. This function satisfies $(\mathfrak{f}^{24}-16)^3 - j\mathfrak{f}^{24} = 0$ and has reduction factor $72/3 = 24$. If 2 is inert, we can use a suitably chosen *double η-quotient*. The exact reduction factor depends on the choice of the η-quotient; we refer to [10] for details. We can use the CM software package [9] by Enge to compute the necessary ring class fields. This package can select the modular function, so that only the discriminant D is required.

Example 4.2. Let $K = \mathbb{Q}(\sqrt{-3})$. To obtain the first nontrivial layer of the anticyclotomic $\mathbb{Z}_3$-extension, we compute the ring class field for the order $\mathbb{O}_2$. If we use the j-function, we obtain a cubic polynomial with constant term

$$2^{45} \cdot 3 \cdot 5^9 \cdot 11^3 \cdot 23^3.$$

In this case, a suitably chosen *double η-quotient* yields a class invariant. Using the package [9], we obtain the polynomial

$$x^3 - 12x^2 - 6x - 1.$$

We stress that by class invariants, we can only gain a *constant factor* in the size of the coefficients, and that our method is inherently exponential in $\log|D|$. To push the range of examples further, we can employ *lattice basis reduction*. Indeed, if we have computed a polynomial $f(x)$ that generates the ring class field, we can view the order defined by f as a *lattice* in Euclidean space. If the degree and the coefficients of f are not too big, we can compute a short basis for this lattice and obtain a "better" polynomial.

Example 4.3. For $K = \mathbb{Q}(\sqrt{-3})$, the polynomial $f \in \mathbb{Z}[x]$ for $\mathbb{O}_3$ given by Enge's program has coefficients between -24930 and 29559. We view $\mathbb{Z}[x]/(f)$ as a lattice and after lattice basis reduction, we obtain the polynomial

$$x^9 + 9x^6 + 27x^3 + 3.$$

Using the same technique, we find the polynomial

$$x^{27} + 27x^{24} + 324x^{21} + 1980x^{18} + 5022x^{15} - 8262x^{12} - 30348x^9 + 304236x^6 + 1365417x^3 + 3$$

for the third layer of the anticyclotomic $\mathbb{Z}_3$-extension.

5. Mirror principle

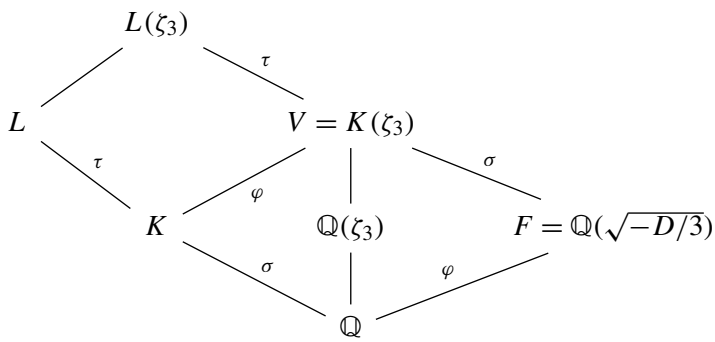
In this section we give an application of the *mirror principle* that relates the class groups of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and the real quadratic field $\mathbb{Q}(\sqrt{-D/3})$. This allows us to prove the following theorem that was alluded to in Example 3.2.

Theorem 5.1. *Let $D \equiv 3 \bmod 9$ be a negative discriminant, and assume that 3 does not divide the class number of the real quadratic field $\mathbb{Q}(\sqrt{-D/3})$. Then the 3-Hilbert class field of $K = \mathbb{Q}(\sqrt{D})$ is contained in the anticyclotomic $\mathbb{Z}_3$-extension of K.*

The proof of the theorem relies on the following lemma. The proof of this lemma is very similar to the proof of Scholz's mirror theorem [13].

Lemma 5.2. *Let $D \equiv 3 \bmod 9$ be a negative discriminant, and assume that 3 does not divide the class number of the real quadratic field $\mathbb{Q}(\sqrt{-D/3})$. Then, there exists exactly one degree 3 extension of $\mathbb{Q}(\sqrt{D})$ that is unramified outside 3 and dihedral over $\mathbb{Q}$.*

Proof. Let $K = \mathbb{Q}(\sqrt{D})$ and let L/K be a degree 3 extension that is unramified outside 3 and dihedral over $\mathbb{Q}$. The field L fits inside



This diagram also defines automorphisms τ, σ, and φ. By abuse of notation, τ denotes both a generator of $\mathrm{Gal}(L/K)$ and its unique lift to $\mathrm{Gal}(L(\zeta_3)/V)$ and likewise for σ and φ. Because $L(\zeta_3)/V$ is a Kummer extension, we can write $L(\zeta_3) = V(\sqrt[3]{\alpha})$ with $\alpha \in V$.

Any such $L(\zeta_3)$ will have φ acting trivially on the corresponding τ as well as have σ acting as -1 on τ. Our proof proceeds by showing that both the field of definition and the norm of α are very restricted.

First we show that α can be taken to lie in the real quadratic field $F = \mathbb{Q}(\sqrt{-D/3})$. The *Kummer pairing*

$$\langle \alpha \rangle / \langle \alpha^3 \rangle \times \langle \tau \rangle \to \mu_3$$

is Galois equivariant, and since σ acts on ζ_3 as -1 and on τ as -1, we see that σ acts as $+1$ on $\alpha \bmod (V^*)^3$. We deduce that $\sigma(\alpha) = \alpha \cdot \beta^3$ for some $\beta \in V^*$, and hence

$$N_{V/F}(\alpha) = \alpha\sigma(\alpha) \equiv \alpha^2 \bmod \text{cubes}.$$

Since α and α^2 generate the same extension, this shows that we may assume that α lies in F.

Since the extension $L(\zeta_3)/V$ is unramified outside 3, we have $(\alpha) = IJ^3$ for ideals I, J with I a product of primes lying over $(3) \subset \mathbb{Z}$. The assumption that 3 does not divide the class number of F now implies that we may assume that α is 3-unit. Furthermore, the assumption $D \equiv 3 \bmod 9$ implies that 3 is inert in $\mathbb{Q}(\sqrt{-D/3})$. We get that α is a unit times 3^a for some a. Since $\varphi(\alpha)$ is congruent to α^{-1} modulo cubes, we must have $a \equiv 0 \bmod 3$. Therefore, we may take $\alpha = \pm\varepsilon$, with ε a fundamental unit of F. $\square$

Proof of Theorem 5.1. Since K has a unique cubic extension that is unramified outside 3 and dihedral over $\mathbb{Q}$, the class group of $\mathbb{O}$ has 3-rank at most 1. We write $\mathrm{Pic}(\mathbb{O})_3 = \mathbb{Z}/3^n\mathbb{Z}$ for some $n \geq 0$. We need to prove that the 3-Hilbert class field $H_3(K)$ coincides with the n-th level K_n.

Suppose that we have $H_3(K) \cap K_n = K_k$ for some $k < n$. The Galois group of the compositum $H_3(K)K_n$ over K then has 3-rank 2. This means that there is more than one cubic extension of K contained in $H_3(K)K_n$. All these extensions are unramified outside 3 and dihedral over $\mathbb{Q}$ however, which is a contradiction. □

Lemma 5.2 allows us to deduce a simple sufficient criterion for when the 3-parts $\mathrm{Pic}(\mathbb{O}_N)_3$ are cyclic.

Theorem 5.3. *Assume that* 3 *does not divide the class number of the real quadratic field* $\mathbb{Q}(\sqrt{-D/3})$. *For* $D \equiv 3 \bmod 9$, *the* 3*-part* $\mathrm{Pic}(\mathbb{O}_N)_3$ *is cyclic for all* $N \geq 0$.

Proof. By Theorem 5.1, the sequence

$$1 \to (\mathbb{O}/3^N\mathbb{O})^*/\operatorname{Im}(\mathbb{O}^*)(\mathbb{Z}/3^N\mathbb{Z})^* \to \mathrm{Pic}(\mathbb{O}_N)_3 \to \mathrm{Pic}(\mathbb{O})_3 \to 1$$

does not split for any N. Since the first and last terms are cyclic, this means that the middle term is cyclic. □

6. Generators via Kummer theory

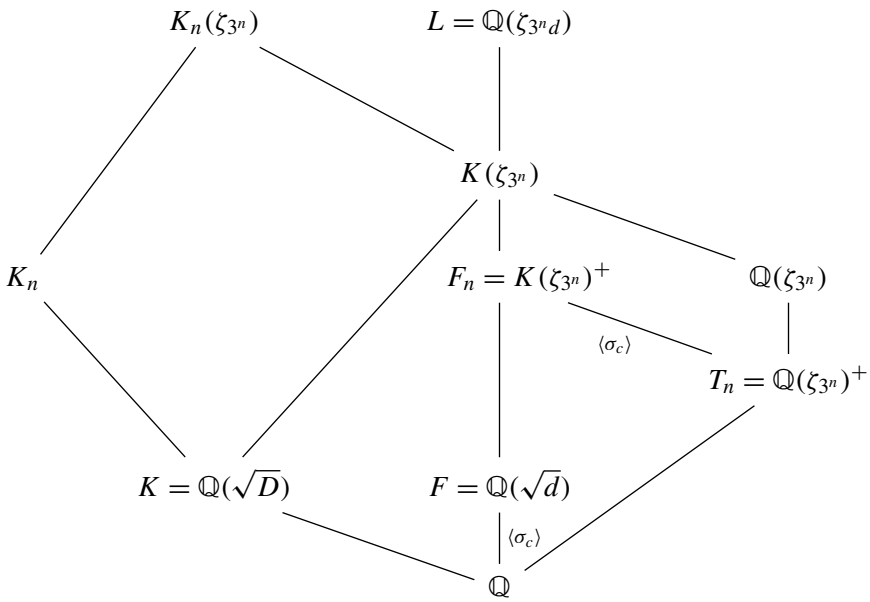
In computational class field theory, the "standard" way to compute an abelian extension of prescribed conductor of a number field K depends on whether K has the appropriate roots of unity. If it does, we can use Kummer theory. If it does not, we adjoin the right root of unity ζ_n to K and compute the right abelian extension of $K(\zeta_n)$ first. Afterwards, we "descend" down to K. We refer to [7] for a detailed description.

If K is imaginary quadratic, we can use complex multiplication techniques instead and bypass the general method. This is the technique we used in Section 2. However, we can make the Kummer theory approach very explicit in our setting. As before, $K = \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field in which 3 ramifies. Throughout this section, we assume 3 does not divide the class number of the real quadratic field $F = \mathbb{Q}(\sqrt{-D/3})$; we also assume that 3 remains inert in F. This last restriction is essential in Lemma 6.4; the split case appears to be much harder.

Theorem 6.1. *Assume that* 3 *ramifies in* $K = \mathbb{Q}(\sqrt{D})$ *and that* 3 *is inert in* $F = \mathbb{Q}(\sqrt{-D/3})$. *If*, *furthermore*, 3 *does not divide the class number of* F, *then the expression for* κ_n *given in Definition 6.7 gives a Kummer generator for* $K_n(\zeta_{3^n})/K(\zeta_{3^n})$ *for* $n \geq 1$.

Once κ_n is computed, we can use the technique from [7, pp. 514–515] to descend from $K_n(\zeta_{3^n})/K(\zeta_{3^n})$ down to K_n/K.

The following diagram defines the various fields we will work in and explains the inclusion relations between them:



In this diagram, the $+$ notation indicates the maximal real subfield. We write $d = -D/3$, so that $F = \mathbb{Q}$ for $D = -3$ and F is real quadratic otherwise. If F is quadratic, we let χ be the associated quadratic character of conductor d.

All the base fields we consider are subfields of $L = \mathbb{Q}(\zeta_{3^n d})$; we identify $\mathrm{Gal}(L/\mathbb{Q})$ with $(\mathbb{Z}/3^n d\mathbb{Z})^*$ and for an integer b with $\gcd(b, 3d) = 1$, we let σ_b be the automorphism satisfying $\sigma_b(\zeta_{3^n d}) = \zeta_{3^n d}^b$. For $d \neq 1$, we fix an integer $c \equiv -1 \bmod 3^n$ with $\chi(c) = -1$; we identify $\mathrm{Gal}(F_n/T_n) \cong \mathrm{Gal}(F/\mathbb{Q}) \cong \langle\sigma_c\rangle$ in this case. (For $d = 1$, all statements about σ_c play no role and should be ignored.)

Lemma 6.2. *The class number of F_n is coprime to* 3.

Proof. By assumption, 3 remains inert in $F/\mathbb{Q}$. As the extension F_n/F has only one ramified prime and is totally ramified, the lemma follows from [16, Theorem 10.4]. □

The techniques of the proof of Lemma 5.2 show that we may assume that the desired element κ_n lies in F_n. Furthermore, since the class number of F_n is coprime to 3, this proof also shows that κ_n is a 3-unit in F_n.

Furthermore, we claim that we may assume that σ_c inverts κ_n. To see this, note that $K(\zeta_{3^n d})/K$ is disjoint from K_∞/K, and σ_c therefore acts trivially on $\mathrm{Gal}(K_n(\zeta_{3^n})/K(\zeta_{3^n}))$. It also acts by inversion on ζ_{3^n}. Therefore, the Kummer pairing tells us that σ_c acts by inversion on κ_n modulo 3^n-th powers; i.e., we have $\kappa_n^{\sigma_c} = \kappa_n^{-1}\gamma^{3^n}$ for some γ. But then $\kappa_n^{1-\sigma_c} = \kappa_n^2\gamma^{-3^n}$ generates the same extension and is inverted by σ_c since $\sigma_c^2 = 1$ on $K(\zeta_{3^n})$.

Let E_n be the group of 3-units of F_n. Let E_n^- denote the subgroup consisting of elements that are inverted by σ_c, and E_n^+ denote those that are fixed (and hence lie in T_n). We compute a valid κ_n as a

product of suitably chosen 3-units in E_n^-. For $n \geq 1$, we define

$$\xi_n = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^a)^{\chi(a)}.$$

The product is over values of a representing elements of $\mathrm{Gal}(L/T_n)$. We claim that ξ_n lies in F_n. Indeed, for $\sigma_b \in \mathrm{Gal}(L/F_n)$ we have $b \equiv \pm 1 \bmod 3^n$ and $\chi(b) = 1$. The computation

$$\sigma_b(\xi_n) = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^{ab})^{\chi(a)} = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^{a})^{\chi(a/b)} = \xi_n$$

gives $\xi_n \in F_n$.

Lemma 6.3. (a) $\xi_n \in E_n^-$.

(b) *The norm of ξ_n from F_n to F_{n-1} is ξ_{n-1}.*

Proof. For part (a), a simple computation shows that $\sigma_c(\xi_n) = \xi_n^{-1}$. If $d \neq 1$, every factor $1 - \zeta_{3^n d}^a$ is a unit, so ξ_n is a unit. If $d = 1$, then each factor is a 3-unit. Therefore, $\xi_n \in E_n^-$.

For (b), we note that the Galois conjugates of ζ_{3^n} for $L/\mathbb{Q}(\zeta_{3^{n-1}d})$ are $\zeta_{3^n}\zeta_3^i$ for $i = 0, 1, 2$. Therefore, the norm of the factor $(1 - \zeta_{3^n d}^a)$ is

$$\prod_{i=0,1,2} (1 - \zeta_{3^n d}^a \zeta_3^i) = (1 - \zeta_{3^n d}^{3a}) = (1 - \zeta_{3^{n-1} d}^a),$$

and the result follows. □

Lemma 6.4. *The $\sigma_j(\xi_n)$ for $\sigma_j \in Gal(F_n/F)$ are independent 3-units and generate a subgroup of E_n^- of index prime to 3.*

Proof. We need some preliminary work. Since keeping track of powers of 2 is irrelevant for what we do, for numbers a and b we use the notation $a \approx b$ to say that a/b is a power of 2, up to sign. When a, b are groups, $a \approx b$ means that a and b are subgroups of some larger group G with $[G : a]/[G : b]$ equal to a power of 2.

Since $\sigma_c^2 = 1$ on F_n, the identity $x^2 = x^{1-\sigma_c} x^{1+\sigma_c}$ implies

$$E_n \approx E_n^- \oplus E_n^+.$$

Let $\{u_1, \ldots, u_{3^{n-1}}\}$ be a basis for E_n^- and $\{v_1, \ldots, v_{3^{n-1}-1}\}$ be a basis for E_n^+ mod $\{\pm 1\}$. The Galois group of $F_n/\mathbb{Q}$ is given by the elements σ_j and $\sigma_c\sigma_j$, where σ_j runs through $\mathrm{Gal}(F_n/F)$. These can be used to calculate the regulator R_n of F_n, up to powers of 2. Let

$$R_n^- = (\log|\sigma_j(u_i)|_{j,i}) \quad \text{and} \quad R_n^+ = (\log|\sigma_j(v_i)|_{j,i}).$$

Then R_n, up to powers of 2, is the absolute value of the determinant of the matrix

$$\begin{pmatrix} R_n^- & R_n^+ \\ -R_n^- & R_n^+ \end{pmatrix}$$

with the last row deleted. Adding the top rows to the corresponding bottom rows yields a 0-block in the lower left and twice R_n^+ in the lower right. Therefore,

$$R_n \approx \det(R_n^-)\det(R_n^+).$$

Note that $\det(R_n^+)$ is, up to powers of 2, the regulator of T_n.

We define the regulator

$$R_{\xi_n} = |\det(\log|\sigma_j\sigma_i^{-1}\xi_n|)|, \quad i, j \in \mathrm{Gal}(F_n/F),$$

of the $\mathrm{Gal}(F_n/F)$-conjugates of ξ_n. We claim that

$$\det(R_n^-) \approx \frac{h(F_n)R_{\xi_n}}{h(T_n)}$$

holds. (Here, $h(\,\cdot\,)$ denotes the class number.) Since $R_{\xi_n}/\det(R_n^-)$ is the index in E_n^- of the subgroup generated by the conjugates of ξ_n, the lemma then follows from the observation that both T_n and F_n have class number coprime to 3.

The value R_{ξ_n} is a group determinant, and by [16, Lemma 5.26] we have

$$R_{\xi_n} = \pm\prod_{\psi}\sum_{j}\psi(\sigma_j)\log|\sigma_j\xi_n|,$$

where ψ ranges over the Dirichlet characters for $\mathrm{Gal}(F_n/F) \simeq \mathrm{Gal}(T_n/\mathbb{Q})$, and σ_j ranges over $\mathrm{Gal}(F_n/F)$.

We have

$$\sum_j \psi(j)\log|\sigma_j\xi_n| = \sum_j \psi(j)\sum_a \chi(a)\log|1-\zeta_{3^n d}^{aj}|,$$

where $1 \le a \le 3^n d$, $(a,d)=1$, and $a \equiv \pm 1 \bmod 3^n$. This equals

$$\sum_{1\le a\le 3^n d,\ (a,3d)=1} \psi(a)\chi(a)\log|1-\zeta_{3^n d}^{a}|.$$

Recall that if ψ has conductor 3^m with $m \ge 1$, then

$$L(1,\overline{\psi\chi}) = -\frac{g(\overline{\psi\chi})}{3^m d}\sum_{1\le a\le 3^m d,\ (a,3d)=1}\psi(a)\chi(a)\log|1-\zeta_{3^m d}^{a}|,$$

where $g(\overline{\psi\chi})$ is a Gauss sum. Since the values of $\psi(a)$ depend only on $a \bmod 3^m$, we have, for fixed a_0 with $3\nmid a_0$,

$$\sum_{\substack{1\le a\le 3^n d\\ a\equiv a_0 \bmod 3^m d}} \psi(a)\log|1-\zeta_{3^n d}^{a}| = \psi(a_0)\log|1-\zeta_{3^m d}^{a_0}|,$$

where we have used the identity $\prod_{\omega^{3^{n-m}}=1}(1-\omega x) = 1 - x^{3^{n-m}}$. Therefore,

$$\sum_j \psi(j)\log|\sigma_j\xi_n| = \frac{3^m d}{g(\overline{\psi\chi})}L(1,\overline{\psi\chi}).$$

If ψ is trivial, then

$$\sum_j \log|\sigma_j\xi_n| = \log|\mathrm{Norm}_{F_n/F_1}\xi_n| = \log|\xi_1|$$

$$= \sum_{\substack{1\le a\le 3d\\(a,3d)=1}} \chi(a)\log|1-\zeta_{3d}^a|.$$

For fixed a_0,

$$\sum_{\substack{a\equiv a_0 \bmod d\\1\le a\le 3d,\ (a,3d)=1}} \log|1-\zeta_{3d}^a| = \log|1-\zeta_{3d}^{3a_0}| - \log|1-\zeta_{3d}^{3a_1}|,$$

where $3a_1 \equiv a_0 \bmod d$ and $1 \le 3a_1 \le 3d$. Therefore,

$$\sum_j \log|\sigma_j\xi_n| = \sum_{\substack{1\le a_0\le d\\(a_0,d)=1}} \chi(a_0)\log|1-\zeta_d^{a_0}| - \sum_{\substack{1\le a_1\le d\\(a_1,d)=1}} \chi(3a_1)\log|1-\zeta_d^{a_1}|$$

$$= (1-\chi(3))\frac{-d}{g(\chi)}L(1,\chi).$$

Using that 3 is inert in $F/\mathbb{Q}$, we compute $1-\chi(3) = 2$.

From the analytic class number formula, we derive

$$\frac{h(F_n)R_n}{\sqrt{\mathrm{disc}(F_n)}}\frac{\sqrt{\mathrm{disc}(R_n)}}{h(T_n)R_n^+} \approx \prod_\psi L(1,\overline{\psi\chi}),$$

where h denotes the class number of the indicated field. By [16, Theorem 3.11 and Corollary 4.6], the Gauss sums, the discriminants, and the conductor $3^m d$ factors cancel, and we obtain

$$\det(R_n^-) \approx \frac{h(F_n)R_{\xi_n}}{h(T_n)}.$$ □

As a byproduct of the calculation with $\psi = 1$, we obtain the following:

Lemma 6.5. *If $d \neq 1$, then $\xi_1 = \epsilon_0^{-4h(F)}$, where $h(F)$ and ϵ_0 are the class number and fundamental unit of F. If $d = 1$, then $\xi_1 = 3$.*

Proof. Up to sign, the case $d \neq 1$ results from keeping track of the factors of 2. In the definition of ξ_1, we can pair the factors for a and $3d-a$ to see that ξ_1 is totally positive. When $d = 1$, the result follows directly from the definition of ξ_1. □

We have almost done all the preparatory work to construct κ_n. Indeed, by Lemma 6.4 we know that κ_n is a product of Galois conjugates of ξ_n. To pin down the product, we need the following standard result.

Lemma 6.6. *Let $m \geq 1$. Let M be a number field, let ζ_m be a primitive m-th root of unity, and let $\alpha \in M(\zeta_m)^\times$. Let $M(\zeta_m, \alpha^{1/m})/M(\zeta_m)$ be a cyclic extension of degree m. Define a map*

$$\omega : \mathrm{Gal}(M(\zeta_m)/M) \to \mathbb{Z}/m\mathbb{Z}$$

by $\tau(\zeta_m) = \zeta_m^{\omega(\tau)}$. Then $F(\zeta_m, \alpha^{1/m})/M$ is Galois with abelian Galois group if and only if

$$\alpha^{\tau - \omega(\tau)} \in (M(\zeta_m)^\times)^m$$

holds for all $\tau \in \mathrm{Gal}(M(\zeta_m)/M)$.

Proof. The proof is a standard calculation with the Kummer pairing. See for instance the proof of [16, Theorem 14.7]. □

Choose $\tau \in \mathrm{Gal}(F_n/F)$ satisfying $\tau(\zeta_{3^n}) = \zeta_{3^n}^4$. We have

$$\kappa_n = \prod_{j=0}^{3^{n-1}-1} \tau^j(\xi_n)^{c_j},$$

for some integers c_j. Therefore, taking indices mod 3^{n-1}, we have

$$\kappa_n^\tau = \prod_{j=1}^{3^{n-1}} \tau^j(\xi_n)^{c_{j-1}}.$$

Lemma 6.6 says that $\kappa_n^{\tau-4}$ is a 3^n-th power, and since the elements $\tau^j(\xi_n)$ are multiplicatively independent, we must have

$$c_{j-1} - 4c_j \equiv 0 \bmod 3^n, \quad 1 \leq j \leq 3^{n-1}.$$

This implies that each c_j is uniquely determined mod 3^n by the value of c_0. Therefore, κ_n is uniquely determined up to an integral power and mod 3^n-th powers. Therefore, if we find $\kappa_n \in F_n$ such that

(1) $\kappa_n^{\tau-4}$ is a 3^nth power and

(2) κ_n is not a cube in F_n,

then we have a Kummer generator for $K_n(\zeta_{3^n})/K(\zeta_{3^n})$.

For $i \geq 1$, define

$$B_i = \prod_{j=1}^{i-1} \left(\frac{1 + 4^{3^{j-1}} + 16^{3^{j-1}}}{3} \right).$$

Let

$$b_i = (1 - B_i)/3,$$

which is an integer for all $i \geq 1$. Finally, for $i \geq 2$, let

$$D_i(x) = \frac{3(b_i(x-1) - 1) - (1 + x^{3^{i-1}} + x^{2 \cdot 3^{i-1}})(b_{i-1}(x-1) - 1)}{x - 4}.$$

Note that the numerator of $D_i(x)$ evaluated at $x=4$ is

$$3(3b_i-1)-(1+4^{3^{i-1}}+16^{3^{i-1}})(3b_{i-1}-1)=3(-B_i)+(1+4^{3^{i-1}}+16^{3^{i-1}})B_{i-1}=0,$$

so D_i has integer coefficients. For example, $D_2(x)=x-1$.

Let

$$\delta_i=\xi_i^{D_i(\tau)} \quad \text{for } i\geq 2, \qquad \beta_i=\xi_i^{b_i(\tau-1)-1} \quad \text{for } i\geq 1.$$

Then $\xi_i,\beta_i,\delta_i\in F_i$, and

$$\delta_i^{\tau-4}=\frac{\beta_i^3}{\beta_{i-1}}$$

for $i\geq 2$. Moreover,

$$\beta_1=\xi_1^{b_1(\tau-1)-1}=\xi_1^{-1}.$$

Definition 6.7. Let $\kappa_1=\xi_1$, and for $n\geq 2$ let

$$\kappa_n=\xi_1\delta_2^3\cdots\delta_n^{3^{n-1}}\in F_n\subset K(\zeta_{3^n}).$$

We have

$$\begin{aligned}\kappa_n^{\tau-4}&=\xi_1^{-3}\frac{\beta_2^9}{\beta_1^3}\frac{\beta_3^{27}}{\beta_2^9}\cdots\frac{\beta_n^{3^n}}{\beta_{n-1}^{3^{n-1}}}\\&=\beta_n^{3^n}.\end{aligned}$$

Lemma 6.8. *κ_n is not a cube in $K(\zeta_{3^n})$.*

Proof. The lemma is equivalent to ξ_1 not being a cube in $\mathbb{Q}(\zeta_{3^n})$. Our assumption $3\nmid h(F)$ implies that $\xi_1=\epsilon_0^{-4h(F)}$ is not a cube in F (when $d\neq 1$; the case $d=1$ is trivial), so $x^3-\xi_1$ generates a non-Galois cubic extension of F that must be disjoint from every abelian extension. Therefore, $\sqrt[3]{\xi_1}\notin K(\zeta_{3^n})$. □

Proof of Theorem 6.1. Lemma 6.8 implies that

$$K(\zeta_{3^n})(\sqrt[3^n]{\kappa_n})/K(\zeta_{3^n})$$

is cyclic of order 3^n. Since $\kappa_n^{\tau-4}$ is a 3^n-th power and κ_n is real, it is the desired Kummer generator for $K_n(\zeta_{3^n})/K(\zeta_{3^n})$. □

Example 6.9. For $K=\mathbb{Q}(\sqrt{-3})$, we have $\kappa_1=3$ and hence $K_1=\mathbb{Q}(\sqrt{-3},3^{1/3})$.

To obtain the second layer, we compute $D_2(x)=x-1$ and

$$\kappa_2=3\left(\frac{(1-\zeta_9^4)(1-\zeta_9^{-4})}{(1-\zeta_9)(1-\zeta_9^{-1})}\right)^3=3\left(\frac{1-\cos(8\pi/9)}{1-\cos(2\pi/9)}\right)^3.$$

We compute that κ_2 is a root of $x^3-1710x^2+513x-27$, and $\kappa_2^{1/9}$ is therefore a root of

$$x^{27}-1710x^{18}+513x^9-27.$$

Having found the extension $K(\zeta_9)(\kappa_2^{1/9})/K(\zeta_9)$, we proceed as in [7, pp. 514–515] to descend to the extension K_2/K. We compute that K_2 is generated over K by a root of

$$x^9 - 59049x^3 + 4251528\sqrt{-3}.$$

Example 6.10. Fix $K = \mathbb{Q}(\sqrt{-87})$. For the first layer, we compute that κ_1 is a root of $x^2 - 727x + 1$. Instead of following the descent procedure from [7], we can also use the following argument to compute K_1/K. We replace x by x^3 and take the compositum with x^2+3 to obtain a degree 12 polynomial defining $K(\zeta_9)(\kappa_1^{1/3})/\mathbb{Q}$. This field has 7 subfields of degree 6. We test these fields pairwise for isomorphism, and compute that there is a unique field that is not isomorphic to another field. Hence, this is the unique field that is Galois over $\mathbb{Q}$ and must equal K_1. Applying lattice basis reduction to the default generator of $K_1/\mathbb{Q}$ gives the polynomial

$$x^6 - 3x^5 + 13x^4 - 21x^3 + 43x^2 - 33x + 9.$$

To obtain K_2, we compute that κ_2 is a root of

$$\begin{aligned} x^6 - 32987530061068308140347 41x^5 + 85914892795986029900161271451168 06x^4 \\ - 28320363968461011184065689777889416199793x^3 \\ + 85914892795986029900161271451168 06x^2 \\ - 32987530061068308140347 41x + 1. \end{aligned}$$

The same technique as for K_1 gives that there are *two* subfields of $K_1(\zeta_9)(\kappa^{1/9})/\mathbb{Q}$ that are Galois over $\mathbb{Q}$. Since one of them is the known field K_1T_1, we select the field K_2 to be the other subfield that is Galois over $\mathbb{Q}$. A generating polynomial is given in Example 3.2.

Acknowledgement

We thank the referees for valuable suggestions on an earlier version of this paper.

References

[1] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter, *Computing Hilbert class polynomials*, Algorithmic number theory (Alfred J. van der Poorten and Andreas Stein, eds.), Lecture Notes Comput. Sci., no. 5011, Springer, 2008, pp. 282–295. MR 2467854

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[3] David Brink, *Prime decomposition in the anti-cyclotomic extension*, Math. Comp. **76** (2007), no. 260, 2127–2138.

[4] Reinier Bröker and Peter Stevenhagen, *Constructing elliptic curves of prime order*, Computational arithmetic geometry (Kristin E. Lauter and Kenneth A. Ribet, eds.), Contemp. Math., no. 463, Amer. Math. Soc., 2008, pp. 17–28. MR 2459986

[5] Gottfried Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32** (1966), 317–326. MR 0217043

[6] J. E. Carroll and H. Kisilevsky, *Initial layers of Z_l-extensions of complex quadratic fields*, Compositio Math. **32** (1976), no. 2, 157–168. MR 0406970

[7] Henri Cohen and Peter Stevenhagen, *Computational class field theory*, Algorithmic number theory: lattices, number fields, curves and cryptography (J. P. Buhler and P. Stevenhagen, eds.), Math. Sci. Res. Inst. Publ., no. 44, Cambridge University, 2008, pp. 497–534. MR 2467555

[8] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Wiley, 2013. MR 3236783

[9] Andreas Enge, *CM: complex multiplication of elliptic curves*, 2016, version 0.3, distributed under GPL V3+.

[10] Andreas Enge and Reinhard Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Théor. Nombres Bordeaux **16** (2004), no. 3, 555–568. MR 2144957

[11] Jae Moon Kim and Jangheon Oh, *Defining polynomial of the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension of imaginary quadratic fields of class number 1*, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 3, 18–19. MR 2046261

[12] Reinhard Schertz, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 325–343. MR 1926005

[13] Arnold Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203. MR 1581309

[14] Peter Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory: its centenary and prospect (Katsuya Miyake, ed.), Adv. Stud. Pure Math., no. 30, Math. Soc. Japan, 2001, pp. 161–176. MR 1846457

[15] Yannick Van Huele, *On T-semisimplicity of Iwasawa modules and some computations with $\mathbb{Z}_3$-extensions*, Ph.D. thesis, University of Washington, 2016. MR 3597700

[16] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts Math., no. 83, Springer, 1997. MR 1421575

Received 19 Feb 2018. Revised 9 Sep 2018.

REINIER BRÖKER: rmbroke@idaccr.org
Center for Communications Research, Princeton, NJ, United States

DAVID HUBBARD: dhubbard@erols.com
Hamilton, NJ, United States

LAWRENCE C. WASHINGTON: lcw@math.umd.edu
Department of Mathematics, University of Maryland, College Park, MD, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine