MATHEMATICS OF COMPUTATION
Volume 70, Number 235, Pages 1293–1303
S 0025-5718(00)01255-2
Article electronically published on March 24, 2000

COMPUTING CLASS FIELDS VIA THE ARTIN MAP

CLAUS FIEKER

ABSTRACT. Based on an explicit representation of the Artin map for Kummer extensions, we present a method to compute arbitrary class fields. As in the proofs of the existence theorem, the problem is first reduced to the case where the field contains sufficiently many roots of unity. Using Kummer theory and an explicit version of the Artin reciprocity law we show how to compute class fields in this case. We conclude with several examples.

1. PRELIMINARIES

Let $k/\mathbb{Q}$ be an algebraic number field; we denote its ring of integers by o_k. A *congruence module* $\mathfrak{m}$ formally consists of an integral ideal $\mathfrak{m}_0$ and a formal product $\mathfrak{m}_\infty$ of real places $(.)^{(i)}$ of k viewed as embeddings into $\mathbb{R}$. By $I^{\mathfrak{m}}$ we denote the set of all ideals coprime to $\mathfrak{m}_0$, by $P_{\mathfrak{m}}$ the set of principal ideals generated by elements $\alpha \equiv 1 \bmod^* \mathfrak{m}$ (i.e., $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\alpha^{(i)} > 0$ for all $(.)^{(i)} | \mathfrak{m}_\infty$) and finally by $\mathrm{Cl}_{\mathfrak{m}} := I^{\mathfrak{m}}/P_{\mathfrak{m}}$ the ray class group modulo $\mathfrak{m}$. There are efficient algorithms for computing ray class groups [6, 17] provided we already know the unit and class group of k.

An *ideal group* H (defined $\bmod \mathfrak{m}$) is a subgroup of $I^{\mathfrak{m}}$ containing $P_{\mathfrak{m}}$. For any ideal group H let $\bar{H} := I^{\mathfrak{m}}/H$.

Now, let K/k be a finite extension. By $\mathfrak{d}_{K/k}$ we denote the relative discriminant of K/k as an ideal of o_k.

From now on K/k will always be a finite abelian extension. In this context we denote by $\sigma_{\mathfrak{p}}$ the Frobenius automorphism belonging to the unramified prime ideal $\mathfrak{p}$ of k. We will make extensive use of the Artin map, the multiplicative extension of the function mapping unramified prime ideals to their Frobenius automorphism:

$$(.,K/k) : I^{\mathfrak{d}_{K/k}} \to \mathrm{Gal}(K/k) : \mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \mapsto \prod_{\mathfrak{p}|\mathfrak{a}} \sigma_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where $\sigma_{\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}$ for any $\mathfrak{P}|\mathfrak{p}$ and any $x \in o_K$.

With this in mind we can define class fields:

Definition 1.1. Let $\mathfrak{m}$ be a congruence module, H be an ideal group and K/k be an abelian extension. K is the class field belonging to H iff $\mathrm{Gal}(K/k) \overset{(.,K/k)}{\simeq} I^{\mathfrak{m}}/H$.

Received by the editor April 6, 1999 and, in revised form, August 16, 1999.
2000 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11R37.
Key words and phrases. Computational algebraic number theory, class field theory, Artin reciprocity.

The famous existence theorem of class field theory states that for every ideal group there is a class field and every abelian extension is the class field to a certain ideal group.

The main theorems of class field theory used here can be found in text books treating algebraic number theory, e.g., [11, 15, 16].

Later we will give an algorithm to compute the class field corresponding to H. The algorithm will follow closely the proof of the existence theorem as given in [15, XI §2]. First we reduce the problem to the case when k contains "sufficiently many" roots of unity. In this case we can use Kummer theory and the Artin map to compute the class fields. As a last step we have to compute a certain subfield of this large class field, again using the Artin map and elementary Galois theory.

2. The Artin map

We recall the following properties of the Artin map ([15, X, §1: A2, A4, Thm. 1 – 3]:

Theorem 2.1. *Let K/k be a finite abelian extension.*

1. *Let $K'/K/k$ with abelian K'/k, then*
$$(.,K'/k)|_K = (.,K/k).$$
2. *Let E/k be finite, then*
$$(.,KE/E)|_K = (.,K/k) \circ N_{E/k}\,.$$
3. *If $\mathfrak{m}$ is divisible by all ramified primes, then*
$$(I^{\mathfrak{m}},K/k) = \mathrm{Gal}(K/k).$$
4. *There exists a congruence module $\mathfrak{m}$ such that $P_{\mathfrak{m}} \subseteq \ker(.,K/k)$, any such module $\mathfrak{m}$ is called* admissible.

Later on, it will be important to have an efficient method for actually computing $(\mathfrak{a},K/k)$ for some ideals $\mathfrak{a}$ of k. Let K/k be a finite abelian extension, and $\sigma_1, \ldots, \sigma_n$ be the k-automorphisms of K. For arbitrary (abelian) extensions K/k it is a hard problem to compute the σ_i [1, 13], but for the extensions occurring in our context, we already know the whole Galois group.

Since the Artin map is the multiplicative extension of the Frobenius map, we start with the investigation of Frobenius automorphisms. Let $\mathfrak{p}$ be an prime ideal of k which is unramified in K. We have
$$\sigma_{\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}_i$$
for all prime ideals $\mathfrak{P}_i|\mathfrak{p}$, and therefore
$$\sigma_{\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{p}o_K$$
for all $x \in o_K$. Since we assume knowledge of all automorphisms, we simply compute $x^{N(\mathfrak{p})} \bmod \mathfrak{p}o_K$ and compare this to $\sigma(x) \bmod \mathfrak{p}o_K$ for all $\sigma \in \mathrm{Gal}(K/k)$. If we do this for sufficiently many elements we can easily identify $\sigma_{\mathfrak{p}}$.

Later on we are mainly interested in Kummer extensions. In this case we can speed up the computations quite a bit. Let $K := k(y)$ be a Kummer extension with generator $y := \sqrt[n]{\mu}$ (for some $\mu \in k$). Without loss of generality we can assume that

$\sigma_i(y) = \zeta_n^i y$ holds. On the other hand we have $y^{N(\mathfrak{p})} = \mu^q y^r$ for $N(\mathfrak{p}) = qn + r$, $0 \le r < n$. In basis representation w.r.t. the basis $1, y, y^2, \dots, y^{n-1}$ the congruence

$$\sigma_i(y) \equiv y^{N(\mathfrak{p})} \bmod \mathfrak{p}o_K$$

reads:

$$(0, \zeta_n^i, 0, \dots, 0) \equiv (0, \dots, 0, \mu^q, 0, \dots, 0) \bmod \mathfrak{p}o_K$$

(where μ^q is the $(r+1)^{\text{st}}$ component) and therefore neccessarily $r = 1$ holds. Since the determination of i is equivalent to the computation of $\sigma_i = \sigma_{\mathfrak{p}}$, we see that for Kummer extensions the Frobenius automorphism can be computed in the base field.

Note 2.2. For an arbitrary ideal $\mathfrak{a}$ we have two possibilities: either use the definition and factor the ideal, compute the automorphisms corresponding to the prime divisors and compose them; or establish the surjection from the ray class group into the Galois group. The main problem with the first approach is that we frequently need to factor large ideals having norms of more than 1000 digits and large prime factors. For the second approach we need the images of certain ideals generating the ray class group. Numerical experiments show that very few (compared to the group order) small ideals usually suffice to generate the ray class group, as one would expect (see [2]). So it makes sense simply to choose small random prime generators for the ray class group to avoid the factoring and use them to get the surjection.

3. Class fields

In this section we reduce the problem to the case where the field contains sufficiently many roots of unity.

Let $\bar{H}$ be the product of cyclic groups of prime power order: $\bar{H} = \prod_{i=1}^t \bar{H}_i$. Using the Artin map, it follows immediately that $K = \prod_{i=1}^t K_i$ with K_i belonging to H_i.

From now on we assume $\bar{H} \cong C_{p^r}$ for some prime p. Let $E := k(\zeta_{p^r})$, then $F := KE$ is the class field over E belonging to some ideal group H_E. Since $N_{E/k}(P_{\mathfrak{m}o_E}) \subseteq P_{\mathfrak{m}}$ we can define H_E modulo $\mathfrak{m}o_E$. Using

$$\tilde{N}_{E/k} : \mathrm{Cl}_{\mathfrak{m}o_E} \to I^{\mathfrak{m}}/H : \mathfrak{a}P_{\mathfrak{m}o_E} \mapsto N_{E/k}(\mathfrak{a})H,$$

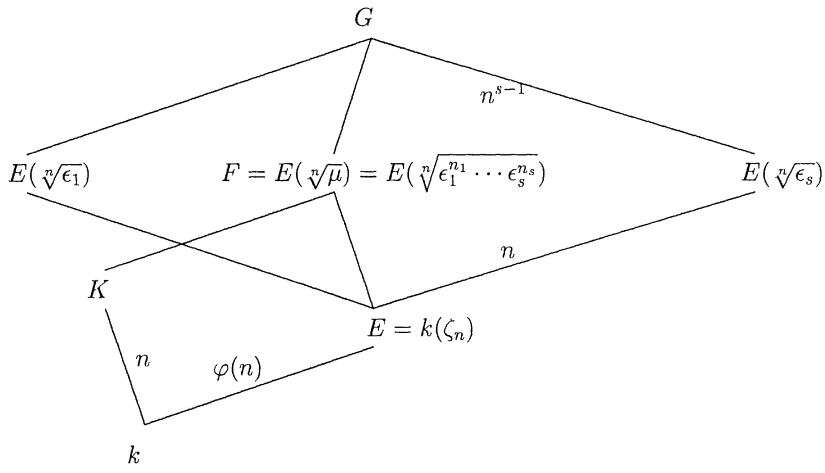
we easily compute $\bar{H}_E = I_E^{\mathfrak{m}}/H_E = P_{\mathfrak{m},E} N_{E/k}^{-1}(\bar{H})$ as a pre-image of a homomorphism between *finite* groups.

Using the approximation theorem, we see that we can use any multiple of $\mathfrak{m}o_E$ to define H_E.

Let S be a finite set of places of E such that S contains all primes dividing $\mathfrak{m}$ and p and enough primes to generate the (ordinary) class group of E, finally let $s := |S|$. We consider the field $G := E(\sqrt[p^r]{U_S})$, where U_S are the S-Units of E. By the Dirichlet unit theorem we have $G = E(\sqrt[p^r]{\epsilon_1}, \dots, \sqrt[p^r]{\epsilon_s})$, where $\epsilon_1, \dots, \epsilon_{s-1}$ generate a free group and ϵ_s is a generator for the torsion units of o_E; hence G is a Kummer extension of degree $(p^r)^s$ over E with Galois group isomorphic to $C_{p^r}^s$.

Analyzing the proof of the existence theorem presented in [15], we see that G *contains* the class field F over E that we are looking for; we are going to compute F as a subfield of G. To illustrate the relation of the various fields, we have included

the following diagram ($n := p^r$, in the most simple case, i.e., $\mathbb{Q}(\zeta_n)$ and k have no common subfield and $(F : E) = n$):



Since G is abelian over E, there is an admissible module $\tilde{\mathfrak{m}}$ such that $I^{\tilde{\mathfrak{m}}} \to \mathrm{Gal}(G/E) = C_{p^r}^s$ is surjective and $P_{\tilde{\mathfrak{m}}}$ is contained in the kernel, i.e., $\mathrm{Cl}_{\tilde{\mathfrak{m}}} \to \mathrm{Gal}(G/E)$ is a well-defined epimorphism.

Since $\tilde{\mathfrak{m}}$ must be divisible by all ramified primes (and by $\mathfrak{m}$) we need to get their exact powers or at least upper bounds.

Lemma 3.1 (Hasse). *Let G/E be a Kummer extension of exponent n. Then*

$$\tilde{\mathfrak{m}} := \prod_{\substack{\mathfrak{p} \nmid n \\ \mathfrak{p} \mid \mathfrak{d}_{G/E}}} \mathfrak{p} \prod_{\mathfrak{p} \mid n} \mathfrak{p}^{c(\mathfrak{p})}$$

with

$$c(\mathfrak{p}) := \left(v_p(n) + \frac{1}{p-1} \right) e_{E/\mathbb{Q}}(\mathfrak{p}/p) + 1$$

is an admissible module for G/E.

Proof. [10, (166), pages 232–233] □

Note that since G/E is a Kummer extension it is possible to compute the discriminant and the exact conductor of G/E. Although this is (computationally) not difficult, it is more time consuming to compute the conductor than to work with the too large ray class group defined by the estimate of Hasse.

From the properties of the Artin map we see that F is the field fixed by all automorphisms of G/E corresponding to ideal classes of $\mathrm{Cl}_{\tilde{\mathfrak{m}}}$ that become trivial in $\bar{H}_E$. Therefore we need firstly to compute those classes and secondly to compute the field fixed by the corresponding automorphisms. Of course, everything said in 2.2 applies here too.

$\mathrm{Cl}_{\tilde{\mathfrak{m}}}$ is given as a direct product of cyclic groups; hence the natural surjection $\iota : \mathrm{Cl}_{\tilde{\mathfrak{m}}} \to \bar{H}$ can be represented by a matrix M. Since we are only interested in groups of order p^r we can define $M \bmod p^r$. Now the classes we are looking for correspond to the null space of $M \bmod p^r$.

Next we compute the automorphisms belonging to the null space and the field fixed by them. We are looking for a certain Kummer subextension of G of degree dividing p^r, so there is a generator of the form $\mu := \prod_{j=1}^{s} \epsilon_j^{n_j}$ with $0 \le n_j < p^r$. We notice that the group of E-automorphisms of G consists of elements of the form

$$\sigma_{\underline{m}} : \sqrt[p^r]{\epsilon_j} \mapsto \zeta_{p^r}^{m_j} \sqrt[p^r]{\epsilon_j}$$

with $\underline{m} = (m_j)_{1 \le j \le s} \in (\mathbb{Z}/p^r\mathbb{Z})^s$. Using this representation we get

$$\sigma_{\underline{m}}(\sqrt[p^r]{\mu}) = \prod_{j=1}^{s} \zeta_{p^r}^{n_j m_j} \sqrt[p^r]{\mu},$$

so a necessary and sufficient condition for $\sqrt[p^r]{\mu}$ being fixed by $\sigma_{\underline{m}}$ is

$$\sum_{j=1}^{s} n_j m_j \equiv 0 \bmod p^r.$$

Starting with generators for the kernel of ι, we then compute the corresponding $\underline{m}$'s. These $\underline{m}$'s yield a (modular) linear system, whose solutions define μ.

Using these ideas, we can give a complete algorithm for computing the class field of E:

Algorithm 3.2. Input: $\mathfrak{m}$, $\bar{H}_E \cong C_{p^r}$, $E \ni \zeta_{p^r}$.
Output: *μ such that $E(\sqrt[p^r]{\mu})$ is the class field belonging to H_E.*

1. *Compute S as described above.*
2. *Compute a basis for the S-units.*
3. *Compute $\tilde{\mathfrak{m}}$ and $\mathrm{Cl}_{\tilde{\mathfrak{m}}}$.*
4. *Compute $\mathfrak{a}_i$ generating the kernel of ι.*
5. *For each such $\mathfrak{a}_i$ compute the corresponding automorphism as a vector $\underline{m}_i \in (\mathbb{Z}/p^r\mathbb{Z})^s$.*
6. *Compute the null space of $(m_{i,j})_{i,j}$ as $\underline{n} \in (\mathbb{Z}/p^r\mathbb{Z})^s$.*
7. *Compute μ.*

Note that by using Theorem 2.1 1, we can compute $m_{i,j}$ independently for each ideal $\mathfrak{a}_i$ and every ϵ_j—we never need to actually generate G.

4. Intersection

In the last section we have seen how to compute class fields when E contains sufficiently many roots of unity. So as a last step we are required to compute a subfield K of E. Different from the situation in the last section, this subfield will not be a Kummer extension, so we have to use a slightly different approach. First we choose $\eta \in F$ such that $F = k(\eta)$, e.g., we can take $\eta = \sqrt[p^r]{\mu} + l\zeta_{p^r}$ for a suitable $l \in N$. Next, we compute the minimal polynomial m_η of η over K. The coefficients $a_0, \ldots, a_t$ of m_η are guaranteed to generate K since $K(\eta) = F$ and

$$\deg(m_\eta)(k(a_0, \ldots, a_t) : k) = (F : k) = \deg(m_\eta)(K : k).$$

Since we are looking for a cyclic extension of k of prime power degree, one coefficient of $a_0, \ldots, a_t$ must be a primitive element for K/k. So it remains to give a procedure to compute m_η.

From [15, XI §1] we know that $KE = F$ is abelian over k and that $p^r o_k \cap N_{E/k}(\tilde{\mathfrak{m}})$ is admissible for this extension. In order to use the Artin map, we have to compute $\mathrm{Gal}(F/k)$.

As in [20, Lemma 1] we extend the automorphisms of E/k to $E(\sqrt[p^r]{\mu}) = F/k$:

Lemma 4.1. *Let $F := k(\zeta_n, \sqrt[n]{\alpha})$, $k(\zeta_n) =: E$ be arbitrary and $\tau : \zeta_n \mapsto \zeta_n^\kappa \in \mathrm{Gal}(F/k)$. Then if F/k is abelian there is an $\alpha_0 \in E$ such that*

$$\tilde{\tau} : F \to F : \left\{ \begin{array}{ccc} \sqrt[n]{\alpha} & \mapsto & \alpha_0 \sqrt[n]{\alpha^\kappa} \\ \zeta_n & \mapsto & \zeta_n^\kappa \end{array} \right\}$$

is an extension of τ.

Proof. Since F/E is normal, $E(\sqrt[n]{\tau(\alpha)}) = F$ and, using [14, page 58], $\sqrt[n]{\tau(\alpha)} = \alpha_0 \sqrt[n]{\alpha^{\kappa'}}$ with $\gcd(\kappa', n) = 1$. It remains to show $\kappa \equiv \kappa' \bmod n$. We define two automorphisms:

$$\tau_1 : F \to F : \left\{ \begin{array}{ccc} \sqrt[n]{\alpha} & \mapsto & \alpha_0 \sqrt[n]{\alpha^{\kappa'}} \\ \zeta_n & \mapsto & \zeta_n^\kappa \end{array} \right\}$$

and

$$\tau_2 : F \to F : \left\{ \begin{array}{ccc} \sqrt[n]{\alpha} & \mapsto & \zeta_n \sqrt[n]{\alpha} \\ \zeta_n & \mapsto & \zeta_n \end{array} \right\}.$$

Since F/k is abelian, we have

$$\zeta_n^\kappa \alpha_0 \sqrt[n]{\alpha^{\kappa'}} = \tau_1 \circ \tau_2(\sqrt[n]{\alpha}) = \tau_2 \circ \tau_1(\sqrt[n]{\alpha}) = \zeta_n^{\kappa'} \alpha_0 \sqrt[n]{\alpha^{\kappa'}}.$$

Finally we get $\kappa \equiv \kappa' \bmod n$. □

Together with the automorphisms of F/E (which are trivial to compute) we have a generating set for the Galois group of F/k.

Now we will proceed as in the last section. First compute a set of ideals generating the kernel $\tilde{H}$ of $\iota : \mathrm{Cl}_{p^r o_k \cap N_{E/k}(\tilde{\mathfrak{m}})} \to \bar{H}$, then the set T of all conjugates (in F) of η

$$T := \{(\mathfrak{a}, F/k)(\sqrt[p^r]{\mu}) \mid \mathfrak{a} \in \tilde{H}\},$$

and then the minimal polynomial as $m_\eta := \prod_{\gamma \in T}(x - \gamma)$.

5. Complete algorithm

We summarize the complete algorithm:

Algorithm 5.1. Input: *k, $\mathfrak{m}$ and $\bar{H}$.*
Output: *Polynomials $f_i \in k[x]$ generating the class field.*

1. *Compute $\bar{H} = \prod \bar{H}_i$ with $\bar{H}_i \cong C_{p_i^{r_i}} =: C_{n_i}$.*
2. *For each i:*
   (a) *Compute μ_i using Algorithm 3.2.*
   (b) *Compute* $\mathrm{Gal}(k(\zeta_{n_i}, \sqrt[n_i]{\mu_i}))$.
   (c) *Compute η_i and m_{η_i}.*
   (d) *Compute the minimal polynomial for each coefficient of m_{η_i} until one with the appropriate degree is found.*

In the actual implementation the overall structure is slightly different. Since one of the most time consuming parts of the algorithm is the computation of the class group of E (E_i), we group all $\bar{H}_i$'s having the same order together. Another rather surprising bottleneck is the computation of the minimal polynomials in step 2(d), especially if $p_i^{r_i} > 10$, since this involves computations in fields of large degree (up to $\varphi(p_i^{r_i})p_i^{r_i}$) over k.

In order to compute η, we first compute the Galois group of F/k. Depending on the representation of the automorphisms, we either already have a primitive element or the conjugates of $\sqrt[p^r]{\mu}$ and ζ_{p^r}. In the first case we are done; in the second case it is easy to check some small l to detect if $\sqrt[p^r]{\mu} + l\zeta_{p^r}$ is a primitive element.

A last problem is the reduction of the polynomials f_i. The polynomials found using the above procedure are far from being optimal (with respect to the size of the coefficients). Although there are some procedures that heuristically reduce the size of the polynomials ([4, `polred`], [5], [9, p. 69]), there is no known (efficient) algorithm that is known to succeed, i.e., one that will find a smaller polynomial if possible.

6. Examples

We start with a small example illustrating the various steps of the algorithm.

Let $k := Q(\sqrt{10})$ and $\mathfrak{m} := 1o_k$. We take $H := P_{\mathfrak{m}}$ and get $\mathrm{Cl} = \mathrm{Cl}_{\mathfrak{m}} = \langle \mathfrak{p}_2 \rangle \cong C_2$, with $\mathfrak{p}_2 = 2o_k + \sqrt{10}o_k$ being the unique prime ideal over 2.

In the first step we are required to split the group into factor groups of prime power order. Since our group is of order 2, we can skip this step.

We now proceed to compute the class field. Since $\zeta_2 = -1 \in k$, we get $E = k$. The set S now contains the prime ideals $\mathfrak{p}_2$ over 2 and both infinite places. A basis for the S-units consists of the unit $3 + \sqrt{10}$, the torsion unit -1 and the $\mathfrak{p}_2$-unit 2. The estimate from Hasse yields $\tilde{\mathfrak{m}} := \mathfrak{p}_2^5 \mathfrak{p}_\infty^{(1)} \mathfrak{p}_\infty^{(2)}$ as an admissible module for G. The corresponding ray class group now is isomorphic to $C_2^2 \times C_4$ of order 16. As generators we compute $\mathfrak{a}_1 = (1-4\sqrt{10})o_k$, $\mathfrak{a}_2 = (1+4\sqrt{10})o_k$ and $\mathfrak{a}_3 = 5o_k + \sqrt{10}o_k$. Next we compute generators for the kernel of ι. We decompose the basis $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ of $\mathrm{Cl}_{\tilde{\mathfrak{m}}}$ in $\mathrm{Cl}_{\mathfrak{m}}$ and get the following matrix:

$$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix}.$$

We see that the null space mod 2 is generated by $\mathfrak{a}_1$, $\mathfrak{a}_2$. To compute the corresponding Artin automorphism we factor $\mathfrak{a}_i$, $(i = 1, 2)$ and get $\mathfrak{a}_1 = \langle 3, 2+\sqrt{10} \rangle \langle 53, 13+\sqrt{10} \rangle =: \mathfrak{p}_3^{(1)} \mathfrak{p}_{53}^{(1)}$ and $\mathfrak{a}_2 = \langle 3, 4+\sqrt{10} \rangle \langle 53, 40+\sqrt{10} \rangle =: \mathfrak{p}_3^{(2)} \mathfrak{p}_{53}^{(2)}$. Computing $N(\mathfrak{p}_3^{(1)}) = 3$, $(\sqrt{3+\sqrt{10}})^3 = (3+\sqrt{10})\sqrt{3+\sqrt{10}}$ and $(3+\sqrt{10}) - \zeta_2^2 \in \mathfrak{p}_3^{(1)}$, we see that the Frobenius automorphism of $\mathfrak{p}_3^{(1)}$ in $k(\sqrt{3+\sqrt{10}})$ is trivial. Similary we compute the automorphisms of the other pairs of prime ideals and generators. We summarize the results in the following table.

	$3+\sqrt{10}$	-1	2
$\mathfrak{p}_3^{(1)}$	$(-1)^2$	-1	-1
$\mathfrak{p}_3^{(2)}$	-1	-1	-1
$\mathfrak{p}_{53}^{(1)}$	$(-1)^2$	$(-1)^2$	-1
$\mathfrak{p}_{53}^{(2)}$	$(-1)^2$	$(-1)^2$	-1

Now we can compose the automorphisms to get the Artin automorphisms for $\mathfrak{a}_1$ and $\mathfrak{a}_2$:

	$3+\sqrt{10}$	-1	2
$\mathfrak{a}_1$	$(-1)^2$	-1	$(-1)^2$
$\mathfrak{a}_2$	-1	-1	$(-1)^2$

As a matrix over $\mathbb{Z}/2\mathbb{Z}$ this reads as $\left(\begin{smallmatrix}0&1&0\\1&1&0\end{smallmatrix}\right)$ with nullspace generated by $(0,0,1)^t$. We conclude that $k(\sqrt{2})$ is the class field belonging to $\mathfrak{m} = 1o_k$.

To illustrate Algorithm 5.1 we have to choose a different example. We take the same base field, but as $\mathfrak{m}$ we choose $\mathfrak{m} := 9o_k\mathfrak{p}_\infty^{(1)}$ and we get $\mathrm{Cl}_\mathfrak{m} = \langle \mathfrak{p}_2 \rangle \cong C_{12}$. This time have to use a decomposition, $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/\langle \mathfrak{p}_2^3 \rangle \times I^\mathfrak{m}/\langle \mathfrak{p}_2^4 \rangle$. Using the above procedure for $H_1 = \langle \mathfrak{p}_2^3 \rangle P_\mathfrak{m}$, we find that $k(\zeta_3, \sqrt[3]{1+\zeta_3}) =: E(\sqrt[3]{1+\zeta_3}) =: F$. As a module (in E) we used $\tilde{\mathfrak{m}} = 81o_E$.

As stated above, an admissable module for F/k is $po_k \cap N_{E/k}(\tilde{\mathfrak{m}}) = 13122o_k\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$, the corresponding ray class group is ismorphic to $C_2^2 \times C_{8748}$ and may be generated by $\mathfrak{a}_1 := \langle 780765561 - 86099392\sqrt{10} \rangle$, $\mathfrak{a}_2 := \langle 1 + 13122\sqrt{10} \rangle$ and $\mathfrak{a}_3 := \langle -2 + 3\sqrt{10}, 15 - \sqrt{10} \rangle$. We decompose $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ in $\mathrm{Cl}_\mathfrak{m}$ and get $\mathfrak{a}_1 \equiv \mathfrak{p}_2^3 P_\mathfrak{m}$, $\mathfrak{a}_2 \equiv \mathfrak{p}_2^3 P_\mathfrak{m}$ and $\mathfrak{a}_3 \equiv \mathfrak{p}_2 \bmod \mathfrak{p}_2^3 P_\mathfrak{m}$. Therefore the kernel of the embedding ι is generated by $\mathfrak{a}_1$ and $\mathfrak{a}_2$. Next, we have to extend the automorphisms of E/k. Since $\mathrm{Gal}(E/k)$ is cyclic of order two we need to extend $\tau : \zeta_3 \mapsto \zeta_3^2$. As stated in Lemma 4.1 we have to compute $\alpha_0 = \sqrt[3]{\tau(\mu)/\mu^2}$ in E with $\mu = 1+\zeta_3$. Since $\tau(\mu) = -\zeta_3$ and $\mu^2 = \zeta_3$, we can use $\alpha_0 = -1$, $\mathrm{Gal}(F/k) = \langle \tilde{\tau} \rangle \cong C_6$. The automorphisms corresponding to $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are calculated as above: first factorize the ideal into prime ideals, next identify the Frobenius automorphisms corresponding to the prime ideals, and as a last step compose the automorphisms.

The factorization of $\mathfrak{a}_1$ yields

$$\begin{aligned}\mathfrak{a}_1 &= \langle 43, 28+\sqrt{10} \rangle \langle 7232053, 6912383+\sqrt{10} \rangle \langle 1721868839, 1721737619+\sqrt{10} \rangle \\ &=: \mathfrak{p}_{43}^{(1)}\mathfrak{p}_{7232053}^{(1)}\mathfrak{p}_{1721868839}^{(1)}\end{aligned}$$

and $\mathfrak{a}_2 = \langle 1721868839, 131220+\sqrt{10} \rangle =: \mathfrak{p}_{1721868839}^{(2)}$. The corresponding Frobenius automorphisms are as follows.

$\mathfrak{p}_{43}^{(1)}$	$\mathfrak{p}_{7232053}^{(1)}$	$\mathfrak{p}_{1721868839}^{(1)}$	$\mathfrak{p}_{1721868839}^{(2)}$
$\tilde{\tau}^4$	$\tilde{\tau}^2$	$\tilde{\tau}^3$	$\tilde{\tau}^3$

And therefore $\mathfrak{a}_1 \mapsto \tilde{\tau}^3$ and $\mathfrak{a}_2 \mapsto \tilde{\tau}^3$. Multipliying $(x - \sqrt[3]{\mu})(x - \tilde{\tau}^3\sqrt[3]{\mu})$ we get $x^2 - (\sqrt[3]{\mu} - \zeta_3\sqrt[3]{\mu^2})x + 1$ as a minimal polynomial for E/K and $x^3 - 3x + 1$ as the minimal polynomial of $-(\sqrt[3]{\mu} - \zeta_3\sqrt[3]{\mu^2})$ over k.

As a second example we take k as the maximal real subfield of $\mathbb{Q}(\zeta_{27})$ and $\mathfrak{m} := 81o_k$. We get $\mathrm{Cl} \cong C_1$, $\mathrm{Cl}_\mathfrak{m} \cong C_{27}$ and K/k is generated by ($\xi := \zeta_{27} + \zeta_{27}^{-1}$):

$$\begin{aligned}&x^{27} - 27x^{25} + 324x^{23} - 2277x^{21} + 10395x^{19} - 32319x^{17} \\ &\quad +69768x^{15} - 104652x^{13} + 107406x^{11} - 72930x^9 + 30888x^7 - 7371x^5 \\ &\quad +819x^3 - 27x - 2 - 7\xi + \xi^2 + 14\xi^3 - 7\xi^5 + \xi^7\end{aligned}$$

Finally, some series computation. Let k be the field generated by a zero ρ of $x^4 + 3x^3 + 2x + 1$. We have $\mathrm{Cl} \cong C_1$, $o_k = \mathbb{Z}[\rho]$, and $\mathfrak{d}_k = -4595$. For all $2 \le i \le 18$

TABLE 1

i	Order	Decomposition	Polynomials
4	2	C_2	$x^2+\rho$
7	3	C_3	$x^3+(2+3\rho^2+\rho^3)x^2-(8-6\rho+10\rho^2+4\rho^3)x-(11-5\rho+10\rho^2+4\rho^3)$
8	8	$C_2\times C_4$	$x^2-2\rho$, $x^4-(2-2\rho+6\rho^2+2\rho^3)x^2+(3-3\rho^2-\rho^3)$
9	9	C_3^2	x^3-3x-1, $x^3-3x-(2-2\rho-7\rho^2-2\rho^3)$
11	5	C_5	$x^5-(11+15\rho^2+5\rho^3)x^4+(44-30\rho+62\rho^2+24\rho^3)x^3-(107-68\rho+94\rho^2+40\rho^3)x^2+(122-34\rho+107\rho^2+41\rho^3)x-(42-10\rho+53\rho^2+19\rho^3)$
12	8	C_2^3	$x^2+\rho$, $x^2-(2+4\rho-2\rho^2-\rho^3)$, $x^2+(2+5\rho-2\rho^2-\rho^3)$
13	12	$C_3\times C_4$	$x^3-(1+3\rho-9\rho^2-3\rho^3)x^2+(2+5\rho-24\rho^2-8\rho^3)x-(6-\rho-13\rho^2-4\rho^3)$, $x^4-(5\rho+2\rho^2)x^3-(8-10\rho-11\rho^2-3\rho^3)x^2+(1+27\rho-34\rho^2-16\rho^3)x-(13+73\rho+15\rho^2-4\rho^3)$
16	32	$C_4\times C_8$	$x^4-(4+4\rho+4\rho^2)x^2+(4+8\rho+6\rho^2-6\rho^3)$, $x^8-(32-12\rho+32\rho+12\rho)x^6+(132-74\rho+144\rho+56\rho)x^4-(16-8\rho+88\rho+28\rho)x^2+(16+51\rho+40\rho+8\rho)$
17	8	C_8	$x^8-x^7-7x^6+6x^5+15x^4-10x^3-10x^2+4x+1$
18	27	C_3^3	$x^3-(2-3\rho+2\rho^2+\rho^3)x^2-(5-3\rho+2\rho^2+\rho^3)x-1$, $x^3+(1+\rho)x^2-(9-2\rho+11\rho^2+4\rho^3)x+(9-5\rho+7\rho^2+3\rho^3)$, $x^3-(3+3\rho)x^2+(3+18\rho+3\rho^2)x+(7+29\rho+57\rho^2+15\rho^3)$

such that the conductor of $\mathrm{Cl}_{(i)}$ is (i) we compute the corresponding ray class fields, i.e., defining equations for the cyclic factors of prime power degree. The corresponding decompositions are summarized in Table 1. Since the polynomials involved are quite large, we only present reduced examples here. The running times vary between seconds for the small examples (C_2, C_3, C_4) up to 10 minutes for the large ones (C_8) plus eventually several hours for a size reduction.

The complete algorithm is part of the current KASH release [12] and is available via anonymous ftp from the following URL:

`ftp://ftp.math.tu-berlin.de:/pub/algebra/Kant/Kash`

7. COMPARISON

There are some other methods known for computing class fields. For ray class fields of imaginary quadratic fields there is the classical approach using complex multiplication [19] that is very fast and applicable even if the ray class group has cyclic factors of a large prime power order. A drawback of this method is that one is not able to compute arbitrary class fields. In practice this limits the method to

ray class groups of order not larger than 300, since the polynomials become quite large.

There are efforts to use similar (i.e., analytical) methods for other base fields by using Stark units. One obstacle here is that it is not proven that this method actually works. However, if one gets results, it is possible to verify them unconditionally. Currently those methods work for small (degree ≤ 4, discriminant < 600000) totally real fields [3, 8, 18]. However, if these methods are applicable, they are usually quite fast, especially for large cyclic factor grops.

For Hilbert class fields (i.e., $\mathfrak{m} = o_k$) there is an algorithm due to Daberkow and Pohst [7] using a classical result of Hecke about ramification in Kummer extensions. This approach has two disadvantages: firstly, the authors get a large number (exponential in the group order) of candidates for F and have to use sieving techniques to find the correct one; and secondly, it is not possible to deal directly with groups having cyclic factors of order p^r with $r > 1$.

There is a recent algorithm due to Cohen [5] that generalizes the approach of Daberkow and Pohst to arbitrary class fields. He can limit the number of possible generators in an efficient way, but still has difficulties for $r > 1$.

Common to all algebraic approaches is that they require the knowledge of the class group of E. The calculation of Cl_E can be time consuming.

8. Acknowledgments

I would like to thank the anonymous referee for numerous suggestions which improved the paper. In addition I have to thank Soun-Hi Kwon who discovered a number of mistakes in a preprint.

References

[1] V. Acciaro and J. Klüners. Computing automorphisms of abelian number fields. *Math. Comp.*, 68(227):1179–1186, 1999. MR **99i:**11099

[2] E. Bach and J. Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.*, 65(216):1717 – 1735, 1996. MR **97a:**11143

[3] H. Bauer. Zur Berechnung von Hilbertschen Klassenkörpern mit Hilfe von Stark-Einheiten. Diploma thesis, Technische Universität Berlin, 1998.

[4] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 1 edition, 1993. MR **94i:**11105

[5] H. Cohen. Advanced topics in computational number theory, Volume 193 of *Graduate Texts in Mathematics*. Springer, 1 edition, 1999. CMP 2000:05

[6] H. Cohen, F. Diaz y Diaz, and M. Olivier. Computing ray class groups, conductors and discriminants. *Math. Comp.*, 67(222):773–795, 1998. MR **98g:**11128

[7] M. Daberkow and M. E. Pohst. On the computation of Hilbert class fields. *J. Number Theory*, 69:213–230, 1998. MR **99h:**11130

[8] D. S. Dummit, J. W. Sands, and B. A. Tangedal. Computing Stark units for totally real cubic fields. *Math. Comp.*, 66(219):1239–1267, 1997. MR **97i:**11110

[9] C. Fieker. *Über relative Normgleichungen in algebraischen Zahlkörpern*. PhD thesis, Technische Universität Berlin, 1997.

[10] H. Hasse. *Vorlesungen über Klassenkörpertheorie*. Physika Verlag, Würzburg, 1967. MR **36:**3752

[11] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate studies in Mathematics*. AMS, 1996. MR **96j:**11137

[12] KANT Group. KANT V4. *J. Symb. Comp.*, 24:267–283, 1997.

[13] J. Klüners. *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*. PhD thesis, Technische Universität Berlin, 1997.

[14] H. Koch. *Number Theory II*, volume 62 of *Encyclopaedia of Mathematical Sciences*. Springer, Berlin, 1992.

[15] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 1994. MR **95f:**11085

[16] J. Neukirch. *Algebraische Zahlentheorie*. Springer, 1992. MR **92a:**01057

[17] S. Pauli. Zur Berechnung von Strahlklassengruppen. Diploma thesis, Technische Universität Berlin, 1996.

[18] X.-F. Roblot. *Algorithmes de factorisation dans les corps de nombres et applications de la conjecture de Stark à la construction des corps de classes de rayon*. PhD thesis, Université Bordeaux I, 1997.

[19] R. Schertz. Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern. *J. Number Theory*, 34:41–53, 1990. MR **91e:**11134

[20] I. R. Shafarevich. A new proof of the Kronecker-Weber theorem. In *Collected mathematical papers*, pages 54–58. Springer, 1989.

FACHBEREICH 3, MATHEMATIK MA 8–1, TECHNISCHE UNIVERSITÄT BERLIN, STRASSE DES 17. JUNI 136, D-10623 BERLIN, F.R.G.

E-mail address: fieker@math.tu-berlin.de