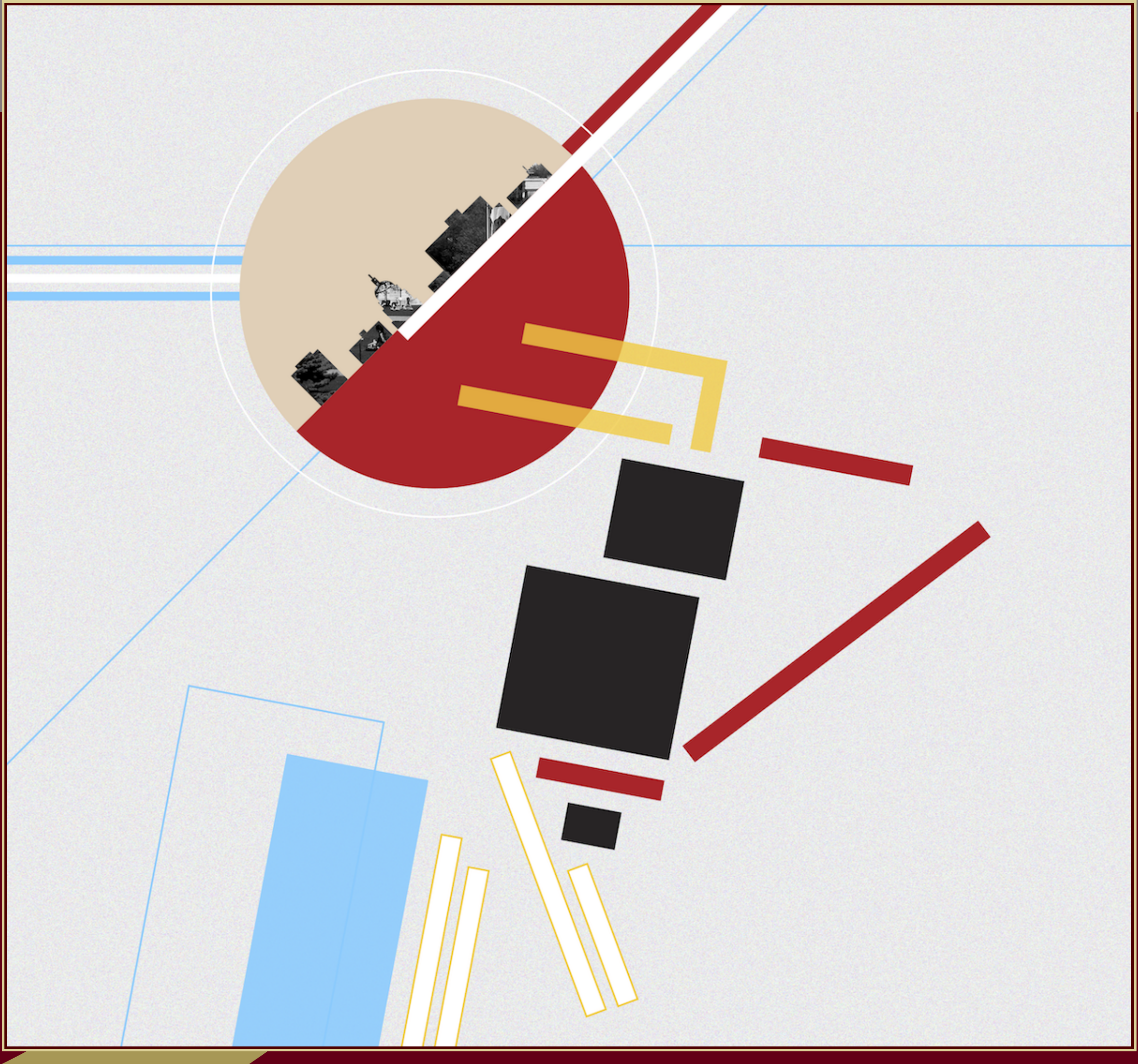
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth
Algorithmic Number Theory Symposium

On the construction of class fields

Claus Fieker, Tommy Hofmann, and Carlo Sircana



msp

THE OPEN BOOK SERIES 2 (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.239

On the construction of class fields

Claus Fieker, Tommy Hofmann, and Carlo Sircana

Class field theory is an important tool in number theory. We discuss improvements to the computation of ray class groups, congruence subgroups and class fields, which are fundamental building blocks of constructive class field theory. As an application and to illustrate the power of our new techniques, we find new fields with minimal discriminant having prescribed Galois group and signature.

1. Introduction

Class field theory of algebraic number fields is one of the main achievements of algebraic number theory from the first half of the 20th century. Building upon Kummer theory, it gives a complete description of abelian extensions of a number field K in terms of objects "inside" K. As a corollary, one obtains a fairly simple parametrization of all abelian extensions of K, similar to the parametrization of abelian extensions of $\mathbb{Q}$ provided by the theorem of Kronecker and Weber. With a growing interest in algorithmic aspects of algebraic number theory and the availability of computational resources, the existence theorem of class field theory was made constructive, resulting in efficient algorithms for working with ray class groups and constructing class fields; see [Has64; DP95; DP98; Poh99; CDyDO96; CDyDO98; Coh99; CS08].

The aim of this paper is to describe new methods for computing class fields with an emphasis on the problem of tabulating extensions of number fields. While the overall strategy is the same as in [CDyDO98] and [DP95], we show how the individual steps can be improved tremendously. The theoretical improvements are accompanied by an efficient implementation allowing computations in situations which were out of reach before. To illustrate this, we have computed new minimal discriminants of number fields with various Galois groups. For a number field K denote by d_K the absolute discriminant of K. If G is a transitive permutation group of degree n and $r \in \mathbb{Z}$, $0 \le r \le n$, we set $d_0(n, r, G)$ to be the smallest value of $|d_K|$, where $[K : \mathbb{Q}] = n$, K has r real embeddings, and if L is the Galois closure of K over $\mathbb{Q}$, then $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ as a permutation group on the embeddings of K in L.

This work was supported by Project II.2 of SFB-TRR 195 "Symbolic Tools in Mathematics and their Application" of the German Research Foundation (DFG).
MSC2010: 11R37, 11Y40.
Keywords: algorithmic number theory, class field theory, class field.

We let C_n denote the cyclic group of order n, D_n denote the dihedral group of order $2n$ and S_n denote the symmetric group on n letters. Using our algorithm we obtain the following minimal discriminants.

Theorem 1. *The following hold*:

(1) $d_0(15, 1, D_{15}) = 239^7$,

(2) $d_0(15, 3, D_5 \times C_3) = 7^{12} \cdot 17^6$,

(3) $d_0(15, 5, S_3 \times C_5) = 2^{10} \cdot 11^{13}$,

(4) $d_0(36, 36, C_9 \rtimes C_4) = 1129^{27}$,

(5) $d_0(36, 0, C_9 \rtimes C_4) = 3^{88} \cdot 29^{27}$.

In all five cases the value of the minimal possible discriminant was not known (see the database of Klüners and Malle [KM01] for the first three cases).

Finally, note that we only consider the problem of computing abelian extensions of arbitrary number fields K, with a focus on normal extensions. For various base fields, there are special methods; for example, complex multiplication for K imaginary quadratic or (conjectural) Stark units for totally real fields.

2. Class field theory and enumeration of abelian extensions

In this section, we briefly recall the main theorem of class field theory and its application to the construction of number fields or complete tables of number fields with specific properties. We refer the reader to [Jan96] or [Lan94] for a detailed description of the topic.

Let K be a number field with ring of integers $\mathcal{O}_K$. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we denote by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation. A *modulus* $\mathfrak{m}$ of K is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ consisting of a nonzero ideal $\mathfrak{m}_0$ of $\mathcal{O}_K$ and a set of real embeddings of K. In this case we also write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ we define $I_\mathfrak{m}$ to be the group of fractional ideals of K generated by the prime ideals not dividing $\mathfrak{m}_0$. Moreover, for $x \in K$ we define $x \equiv 1 \bmod \mathfrak{m}$ if and only if $v_\mathfrak{p}(x-1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{m}_0$ and $\sigma(x) > 0$ for $\sigma \in \mathfrak{m}_\infty$. We define the *ray group* $P_\mathfrak{m} = \{xK \mid x \equiv 1 \bmod \mathfrak{m}\} \subseteq I_\mathfrak{m}$ and call the finite abelian group $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/P_\mathfrak{m}$ the *ray class group* of K modulo $\mathfrak{m}$. A subgroup $P_\mathfrak{m} \subseteq A \subseteq I_\mathfrak{m}$ is called a *congruence subgroup* modulo $\mathfrak{m}$. By abuse of notation, we will also call $\bar{A} = A/P_\mathfrak{m}$ a congruence subgroup. The smallest modulus $\mathfrak{n}$ with $I_\mathfrak{m} \cap P_\mathfrak{n} \subseteq A$ is the *conductor* of A.

Let L/K be an abelian extension. For every prime ideal $\mathfrak{p}$ of K, which is unramified in L/K, there exists a unique map $\mathrm{Frob}_{\mathfrak{p},L/K} \in \mathrm{Gal}(L/K)$ with $\mathrm{Frob}_{\mathfrak{p},L/K}(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{p}\mathcal{O}_L$ for all $x \in \mathcal{O}_L$. We call $\mathrm{Frob}_{\mathfrak{p},L/K}$ the *Frobenius automorphism* of $\mathfrak{p}$. If $\mathfrak{m}$ is a modulus divisible by the prime ideals ramifying in L/K, there exists a unique morphism $\varphi_{L/K} : I_\mathfrak{m} \to \mathrm{Gal}(L/K)$, called the *Artin map*, such that $\varphi_{L/K}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p},L/K}$ for all nonzero prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}_0$. Any modulus $\mathfrak{f}$ such that $\varphi_{L/K}$ factors through $\mathrm{Cl}_\mathfrak{f}$ is called an *admissible modulus* of L/K. The smallest modulus with this property is called the *conductor* of L/K.

Theorem 2. *If L/K is an abelian extension of conductor $\mathfrak{f}$, then there exists a congruence subgroup $A_{\mathfrak{f}} \subseteq \mathrm{Cl}_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ such that the Artin map induces an isomorphism $\psi_{L/K} : \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \to \mathrm{Gal}(L/K)$. If $A_{\mathfrak{f}}$ is a congruence subgroup of conductor $\mathfrak{f}$, then there exists an abelian extension L/K such that the Artin map induces an isomorphism $\psi_{L/K} : \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \to \mathrm{Gal}(L/K)$.*

Now assume K is a number field, G an abelian group and $X \in \mathbb{R}_{>0}$. We fix an algebraic closure $\overline{K}$ of K. For a finite extension L/K we let $d_{L/K} = \mathrm{N}(\mathfrak{d}_{L/K})$ be the norm of the relative discriminant. To find

$$\{K \subseteq L \subseteq \overline{K} \mid \mathrm{Gal}(L/K) \cong G \text{ and } d_{L/K} \leq X\},$$

we can proceed as follows:

(1) Find a set F containing all possible conductors $\mathfrak{f}$.

(2) For every conductor $\mathfrak{f} \in F$ compute the ray class group $\mathrm{Cl}_{\mathfrak{f}}$ and all subgroups $A \subseteq \mathrm{Cl}_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ with $\mathrm{Cl}_{\mathfrak{f}}/A \cong G$.

(3) Let L be an abelian extension of K corresponding to a pair $(\mathfrak{f}, A)$ of Step (2). If $d_{L/K} \leq X$, compute a defining polynomial for L.

We discuss Step (2) in Section 3 and Step (3) in Section 4. In many applications, one is only interested in field extensions with specific properties. While sieving after Step (3) is always possible, it is not an optimal strategy since the computation of the defining polynomials is usually the most expensive step. Very often, the situation allows one to make improvements already in Steps (2) or (3). For example, since the ramification of L/K is intimately connected to the conductor of this extension, restrictions on the ramification allow us to reduce the set of possible conductors in Step (1). In other common situations, K itself is a normal extension of some subfield K_0 and one is only interested in extensions L/K with Galois group G, such that L/K_0 is also normal. We will address the latter problem in Section 5.

3. Quotients of ray class groups

Let K be an algebraic number field and suppose that we are searching for abelian extensions of K with Galois group of exponent n. As described in Section 2, the fields we are looking for correspond to congruence subgroups H of ray class groups $\mathrm{Cl}_{\mathfrak{m}}$ with conductor $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, such that $\mathrm{Cl}_{\mathfrak{m}}/A$ is of exponent n, that is, to subgroups A with $\mathrm{Cl}_{\mathfrak{m}}^n \subseteq A \subseteq \mathrm{Cl}_{\mathfrak{m}}$. Therefore we do not need the whole group $\mathrm{Cl}_{\mathfrak{m}}$, but only the quotient $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n$.

The standard algorithm (see [CDyDO96]) to compute the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ relies on the exact sequence

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times \to \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl} \to 0, \tag{1}$$

where $\mathcal{O}_K^\times$ are the units of $\mathcal{O}_K$ and Cl is the class group of K. In particular, if $\{u_i\}$, $\{m_i\}$, $\{c_i\}$ are generators of the groups $\mathcal{O}_K^\times$, $(\mathcal{O}_K/\mathfrak{m})^\times$ and Cl, respectively, then we can choose as generators of $\mathrm{Cl}_{\mathfrak{m}}$ the union of the images of the m_i and preimages of the c_i. Computing the relations between the generators of Cl and $(\mathcal{O}_K/\mathfrak{m})^\times$, as well as the generators coming from $\mathcal{O}_K^\times$, requires the computation of generators of principal ideals and of discrete logarithms in $(\mathcal{O}_K/\mathfrak{m})^\times$. Note that the latter problem can be expensive. For every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}_0$, computing the discrete logarithm in $(\mathcal{O}_K/\mathfrak{m})^\times$ requires the computation of a discrete logarithm in the multiplicative group $(\mathcal{O}_K/\mathfrak{p})^\times$ of the residue field. This quickly becomes a bottleneck if $\mathrm{N}(\mathfrak{p})-1$ is hard to factor or divisible by large primes.

To avoid these problems, we show how to directly construct the quotient $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n$ of the ray class group. For clarity of exposition, we will only consider the case when n is a prime power, that is, $n = p^s$ for some prime $p \in \mathbb{Z}_{>0}$. Indeed, if n factors as $n = \prod_{i=1}^r p_i^{e_i}$, we get

$$\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n \cong \prod_{i=1}^r \mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{p_i^{e_i}}.$$

While for finite abelian groups the functor $A \mapsto A/p^sA$ is in general only right exact, we can use the exact sequence (1) together with the following lemma to construct the quotient directly.

Lemma 3. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of finite abelian groups of exponents e_1, e_2 and e_3 respectively. Let $p \in \mathbb{Z}_{>0}$ be a prime number and $k \in \mathbb{Z}_{>0}$ with $k \geq v_p(e_i)$ for $i = 1, 2, 3$. Then the sequence*

$$0 \to A/p^kA \to B/p^kB \to C/p^kC \to 0$$

is exact.

Now let $\tilde{n} = p^{\tilde{s}}$ with $\tilde{s} = v_p(\#(\mathcal{O}_K/\mathfrak{m})^\times) + v_p(\#\mathrm{Cl})$. The lemma shows that we can construct $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$ by working only with $\mathrm{Cl}/\mathrm{Cl}^{\tilde{n}}$ and with $(\mathcal{O}_K/\mathfrak{m})^\times/(\mathcal{O}_K/\mathfrak{m})^{\times\tilde{n}}$ (by applying it to $1 \to (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{O}_K^\times) \to \mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl} \to 1$). In particular, the number of generators of the quotient can be smaller than the number of generators of the entire class group. Since for every generator we have to perform expensive operations, this improves performance.

The lemma also affects the construction of the unit group. Let $\mathfrak{q}$ be a prime ideal divisor of $\mathfrak{m}_0$ and $l = v_\mathfrak{q}(\mathfrak{m}_0)$. Recall that by [Coh00, Proposition 4.2.4] we have

$$(\mathcal{O}_K/\mathfrak{q}^l)^\times \cong (\mathcal{O}_K/\mathfrak{q})^\times \times (1+\mathfrak{q})/(1+\mathfrak{q}^l).$$

We distinguish two cases:

- If $l = 1$, we need to compute a generator of $U/\tilde{n}U$, where $U = (\mathcal{O}_K/\mathfrak{q})^\times$. This is much easier than the computation of a generator of the whole group U, which would require the factorization of $\#U = N(\mathfrak{q}) - 1$. We can assume that $p \mid N(\mathfrak{q}) - 1$, otherwise $\mathfrak{m}$ cannot be the conductor of such an extension ([Coh00, Proposition 3.3.21]). Let $e = v_p(N(\mathfrak{q}) - 1)$. Finding a generator of the group $U/\tilde{n}U$ is equivalent to finding an element of U of order divisible by p^e. Such an element can be found with high probability by picking random elements. Indeed, let g be an element of U and let $s = (N(\mathfrak{q}) - 1)/p^e$. Then g is a generator of $U/\tilde{n}U$ if $g^{sp^{e-1}}$ is not trivial. The probability of finding an element of order divisible by p^e is $\varphi(p^e)/p^e = (p-1)/p$, which is always greater than or equal to $1/2$.

- If $l > 1$, then $p \nmid N(\mathfrak{q}) - 1$ and we can avoid computing the multiplicative group of the residue field altogether, since its order is not divisible by p.

Since in this way we have constructed the quotient $V = \mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$, as a final step we just have to compute V/nV.

4. Ray class fields

Let L/K be an abelian extension of degree n and suppose that we have computed an admissible modulus $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ of L/K divisible only by the ramifying primes, and a congruence subgroup $A_\mathfrak{f}$ such that the Artin map induces an isomorphism $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathrm{Gal}(L/K)$. While various invariants can be computed from only $\mathfrak{f}$ and $A_\mathfrak{f}$, finding explicit defining polynomials for the extension L/K is sometimes relevant, for example when constructing towers of number fields. This problem is usually solved using either Hecke's theorem or the Artin map; see [Coh00, Section 5.5.5] for a comparison of both methods. Here we follow in principle the Artin map approach, but we show how to improve it significantly. We will repeatedly make use of the following key result from [Fie01, Section 3]; see also [Coh00, Section 5.4.1].

Proposition 4. *Assume that K contains the n-th roots of unity and $L = K(\sqrt[n]{\alpha})$ is a Kummer extension. Then, for almost all prime ideals $\mathfrak{p}$ of K, we can efficiently find $k \in \mathbb{Z}$ with $\mathrm{Frob}_\mathfrak{p}(\sqrt[n]{\alpha}) = \zeta_n^k \sqrt[n]{\alpha}$ doing only computations in K.*

4.1. ***Reduction to the prime power case.*** Using the fundamental theorem of finite abelian groups, we may decompose $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$ into a product of cyclic groups of prime power order. Accordingly, L/K is the compositum of linearly disjoint cyclic extensions of K of prime power degree. Thus, from now on we assume that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/\ell^m\mathbb{Z}$ is a cyclic extension of prime power degree $n = \ell^m$ for some prime ℓ. Furthermore we assume that we have computed an explicit isomorphism $\Psi : \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathbb{Z}/\ell^m\mathbb{Z}$.

4.2. ***Using Kummer theory.*** Let $E = K(\zeta_n)$ and $F = LE = L(\zeta_n)$. Then F/E is again an abelian extension and, since $\mathrm{N}_{E/K}(P_{\mathfrak{f}\mathcal{O}_E}) \subseteq P_\mathfrak{f}$, we know that the lift $\mathfrak{f}_E = \mathfrak{f}\mathcal{O}_E$ is an admissible modulus for the abelian extension F/E by [Jan96, Chapter III, Section 3]. Our aim is to find a defining polynomial for the field extension F/E, which is now a Kummer extension. To this end, we compute Cl_E and a finite set S of primes of E containing the infinite primes such that

(1) F/E is unramified outside of S, that is, S contains all primes dividing $\mathfrak{f}_E$,

(2) $\mathrm{Cl}_E/\mathrm{Cl}_E^n$ is generated by the classes of the finite primes in S.

We consider then the group U_S of S-units of E. By Dirichlet's unit theorem it is isomorphic to $\mu_E \times \mathbb{Z}^{\#S-1}$. Let $\varepsilon_0 \in \mathcal{O}_E^\times$ be a torsion unit with $\langle \varepsilon_0 \rangle = \mu_E$. Denoting $r = \#S - 1$, we can compute r elements $\varepsilon_1, \dots, \varepsilon_r \in E$ such that $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$ generate U_S. Since F/E is of exponent n and E contains the n-th roots of unity, by Kummer theory we know that $F = E(\sqrt[n]{W_F})$, where $W_F = E^\times \cap F^{\times n}$. By [CS08, Lemma 5.4], condition (1) implies that $W_F/E^{\times n} \subseteq (U_S \cdot E^{\times n})/E^{\times n}$ and therefore $E \subseteq F \subseteq N$, where $N = E(\sqrt[n]{U_S})$. Since F/E is a cyclic subextension of N/E, Kummer theory asserts that there exists an element $\alpha = \varepsilon_0^{n_0}\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}$ such that $F = E(\sqrt[n]{\alpha})$. Our aim is to determine such an element $\alpha \in U_S$ or, equivalently, suitable exponents $n_0, \dots, n_r \in \mathbb{Z}$.

Let $\mathfrak{f}_N$ be an admissible modulus for N/E and $\mathrm{Cl}_{\mathfrak{f}_N}/A_{\mathfrak{f}_N}$ be the corresponding quotient of the ray class group; the latter is isomorphic to $\mathrm{Gal}(N/E)$ via the Artin map. Since

$$N = E(\sqrt[n]{U_S}) = E(\sqrt[n]{\varepsilon_0}, \dots, \sqrt[n]{\varepsilon_r}),$$

the Galois group $\mathrm{Gal}(N/E)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r+1}$ via

$$\Phi : \sigma \mapsto (\overline{m}_0, \dots, \overline{m}_r), \qquad \text{where } \sigma(\sqrt[n]{\varepsilon_i}) = \zeta_n^{m_i} \cdot \sqrt[n]{\varepsilon_i} \quad \text{for } 0 \le i \le r.$$

We therefore get the following commutative diagram:

$$\begin{tikzcd}
 & I_{\mathfrak{f}_N} \arrow[r] \arrow[rr, bend left, "\varphi_{N/E}"] \arrow[d, "\mathrm{N}_{E/K}"] & \mathrm{Cl}_{\mathfrak{f}_N}/A_{\mathfrak{f}_N} \arrow[r, "\psi_{N/E}"] \arrow[dl, "\mathrm{N}_{E/K}"] & \mathrm{Gal}(N/E) \arrow[r, "\Phi"] \arrow[d, "\pi"] & (\mathbb{Z}/n\mathbb{Z})^{r+1} \arrow[dllll, bend left, "\Xi"] \\
\mathbb{Z}/n\mathbb{Z} & \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \arrow[l, "\Psi"'] \arrow[r, "\psi_{L/K}"'] & \mathrm{Gal}(L/K) & \mathrm{Gal}(F/E) \arrow[l, "\mathrm{res}"'] &
\end{tikzcd}$$

Since F is the fixed field of $\mathrm{Gal}(N/F) \subseteq \mathrm{Gal}(N/E)$, we want to search for elements $v_1, \dots, v_l$ in $(\mathbb{Z}/n\mathbb{Z})^{r+1}$ such that $\langle \Phi^{-1}(v_1), \dots, \Phi^{-1}(v_l)\rangle = \mathrm{Gal}(N/F)$, that is, $\langle v_1, \dots, v_l \rangle = \Phi(\mathrm{Gal}(N/F))$. Through diagram chasing, we see that

$$\begin{aligned}\mathrm{Gal}(N/F) &= \ker(\pi) = \ker(\psi_{L/K}^{-1} \circ \mathrm{res} \circ \pi) \\ &= \ker(\mathrm{N}_{E/K} \circ \psi_{N/E}^{-1}) = \psi_{N/E}(\ker(\mathrm{N}_{E/K})) \\ &= \Phi^{-1}(\ker(\Xi)).\end{aligned}$$

Thus it is sufficient to compute the kernel of the $\mathbb{Z}/n\mathbb{Z}$-linear map Ξ. Once we have generators for the kernel, we can read off exponents $n_0, \dots, n_r$ such that $\alpha = \varepsilon_0^{n_0} \cdots \varepsilon_r^{n_r}$ using linear algebra. The following lemma shows that it is not necessary to directly compute the map Ξ in order to find $\ker(\Xi)$ or $\Phi^{-1}(\ker(\Xi))$.

Lemma 5. *Let T be a finite set of finite primes $\mathfrak{q}$ of E such that $\mathfrak{q}$ does not divide $\mathfrak{f}_N$ and* $(\mathrm{Frob}_{\mathfrak{q}})_{\mathfrak{q} \in T}$ *generates* $\mathrm{Gal}(N/E)$. *For $M = (\Psi(\mathrm{N}_{E/K}([\mathfrak{q}])))_{\mathfrak{q} \in T} \in (\mathbb{Z}/m\mathbb{Z})^{\#T \times 1}$ the following holds: If $v_1, \dots, v_l \in (\mathbb{Z}/n\mathbb{Z})^{\#T}$ generate the right kernel* $\ker(M)$, *then*

$$\sum_{\mathfrak{q} \in T} v_{i,\mathfrak{q}} \cdot \Phi(\mathrm{Frob}_{\mathfrak{q}}), \quad 1 \le i \le l,$$

are generators for $\Phi(\mathrm{Gal}(N/F))$.

Remark 6. This is quite different from the original approach in [Fie01, Section 3]. There, an admissible modulus $\mathfrak{f}_N$ was explicitly constructed using bounds due to Hasse [Has67]. This was then followed by the computation of a generating set for the kernel $\ker(\mathrm{N}_{E/K}) \subseteq \mathrm{Cl}_{\mathfrak{f}_N}$ and the application of $\psi_{N/E} \circ \Phi$. Since the valuations of $\mathfrak{f}_N$ obtained by Hasse can be very large, the necessary discrete logarithms in the ray class group $\mathrm{Cl}_{\mathfrak{f}_N}$ tended to be quite costly. We circumvent this by avoiding any computation with $\mathrm{Cl}_{\mathfrak{f}_N}$.

4.3. ***Descent to L/K.*** Suppose now that we have found $\alpha \in E$ such that $F = E(\sqrt[n]{\alpha})$. We aim to find a defining polynomial for L/K. As a first step, we compute $\mu \in F$ such that $F = K(\mu)$. Since $E(\sqrt[n]{\alpha}) = K(\zeta_n, \sqrt[n]{\alpha})$, we can find μ as $\mu = \sqrt[n]{\alpha} + k\zeta_n$ for a suitable $k \in \mathbb{Z}$. Note that k can be found by trying small elements in $\mathbb{Z}$. As the coefficients of the minimal polynomial f_L^{μ} of μ over L generate the cyclic extension L/K, it is sufficient to determine

$$f_L^{\mu} = \prod_{\sigma \in \mathrm{Gal}(F/L)} (X - \sigma(\mu)) \in L[X].$$

Hence the problem of finding a defining polynomial is reduced to the problem of computing an explicit description of $\mathrm{Gal}(F/L)$ on $\sqrt[n]{\alpha}$ and ζ_n. Since F/K is the compositum of E and L, it is abelian with admissible modulus $\mathfrak{f}_F = n\mathcal{O}_K \cap \mathfrak{f}_N$. Denote by $A_{\mathfrak{f}_F}$ the corresponding congruence subgroup of $\mathrm{Cl}_{\mathfrak{f}_F}$. We have the following commutative diagram:

$$\begin{tikzcd}
I_{\mathfrak{f}_F} \arrow[r] \arrow[rr, bend left, "\varphi_{F/K}"] \arrow[dr] & \mathrm{Cl}_{\mathfrak{f}_F}/A_{\mathfrak{f}_F} \arrow[r, "\psi_{F/K}"] \arrow[d] & \mathrm{Gal}(F/K) \arrow[d, "\mathrm{res}"] \\
\mathbb{Z}/n\mathbb{Z} & \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \arrow[l, "\Psi"'] \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

First, note that we can easily compute a generating set for $\mathrm{Gal}(F/K)$. As the group $\mathrm{Gal}(E/K) = \mathrm{Gal}(K(\zeta_n)/K)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and n is a prime power, we can find $r, s \in \mathbb{Z}$ such that $\mathrm{Gal}(E/K)$ is generated by $\zeta_n \mapsto \zeta_n^r$ and $\zeta_n \mapsto \zeta_n^s$. Using [Fie01, Lemma 4.1], we can determine extensions $f, g : F \to F$ of both morphisms, which together with $F \to F$, $\sqrt[n]{\alpha} \mapsto \zeta_n \sqrt[n]{\alpha}$, generate $\mathrm{Gal}(F/K)$. We now need to find $\mathrm{Gal}(F/L) = \ker(\mathrm{res} : \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K))$.

Lemma 7. *Let T be a finite set of finite primes $\mathfrak{q}$ of K such that $\mathfrak{q}$ does not divide $\mathfrak{f}_F$ and $(\mathrm{Frob}_{\mathfrak{q}})_{\mathfrak{q} \in T}$ generates $\mathrm{Gal}(F/K)$. Let $M = (\Psi([\mathfrak{q}]))_{\mathfrak{q} \in T} \in (\mathbb{Z}/n\mathbb{Z})^{\#T \times 1}$. If $v_1, \ldots, v_l \in (\mathbb{Z}/m\mathbb{Z})^{\#T}$ generate the right kernel $\ker(M)$, then*

$$\prod_{\mathfrak{q} \in T} (\mathrm{Frob}_{\mathfrak{q}})^{v_{i,\mathfrak{q}}}, \quad 1 \le i \le l,$$

are generators for $\mathrm{Gal}(F/L)$.

To compute $\mathrm{Frob}_{\mathfrak{q}}$ in F/K, we can proceed as follows. Since we already know $\mathrm{Gal}(F/K)$, if we pick a prime $\mathfrak{p}$ of F lying over $\mathfrak{q}$, we can find $\mathrm{Frob}_{\mathfrak{q}}$ as the unique $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(\zeta_n) \equiv \zeta_n^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$ and $\sigma(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$.

Remark 8. If $n = \ell$ is prime, even fewer steps are necessary. Since $[K(\zeta_n) : K]$ is a divisor of $\ell - 1$, it is coprime to ℓ and thus $\mathrm{Gal}(F/L)$ is the unique subgroup of $\mathrm{Gal}(F/K)$ of order ℓ. If f is the lift of a generator of $\mathrm{Gal}(K(\zeta_n)/K)$ to $\mathrm{Gal}(F/K)$, then f^ℓ will be a generator of $\mathrm{Gal}(F/L)$.

Remark 9. In [Fie01, Section 4], the set $\mathrm{Gal}(F/L)$ is also computed as the kernel of the restriction map $\mathrm{res} : \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$. More precisely, $\mathrm{Gal}(F/L)$ is computed as the image of $\ker(\iota : \mathrm{Cl}_{\mathfrak{f}_F} \to \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}))$

under $\psi_{F/K}$. This is a costly operation due to discrete logarithms in ray class groups. In our approach this is circumvented by the use of the Artin map on sufficiently many prime ideals.

4.4. ***Reduction of generators.*** In the computation of a defining polynomial of the class field, we find a generator of a Kummer extension. Depending on the situation, this is either the final result or this computation is followed by the descent. To improve the overall performance, it is beneficial to find a "small" generator for the Kummer extension. More precisely, let K be an algebraic number field; given $\alpha \in K^\times$, we want to find a "small" representative for $\alpha \cdot K^{\times n}$, that is, we want to find $\beta \in K^\times$ such that $\beta^n \cdot \alpha$ is "small". To this end, we will describe how to compute a so-called compact representation

$$\alpha = \alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}$$

with small elements $\alpha_i \in \mathcal{O}_K$. Once we have found this, α_0 will be a small representative in the coset of α modulo $K^{\times n}$.

Note that the notion of compact representations was used in [Thi95] in connection with the computation of units and principal ideal generators; see also [BF14]. Here we give a different algorithm, which uses a similar approach to [BF14], but which also works for elements which are not units. As the value of the presented algorithms comes from the practicality, we will refrain from giving precise statements about the size of the objects. Note that it is possible to obtain rigorous estimates using Remarks 11 and 13.

The first step of a compact representation is a reduction at the finite places. We let

$$\alpha\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{p}_i^{n_i}$$

be the prime ideal factorization of $\alpha\mathcal{O}_K$ and set $N = \max_i n_i$.

Algorithm 10. Let $k = \lfloor \log_n(N) \rfloor$. The following steps return small (with respect to the T_2-norm) elements $\alpha_0, \dots, \alpha_k$ and $\mathfrak{a}$ of small norm with

$$\alpha\mathcal{O}_K = (\alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}) \cdot \mathfrak{a}.$$

(1) Define $\mathfrak{a}_{k+1} = 1$.

(2) For $j = k, \dots, 0$ define $\mathfrak{b}_j = \prod_{i=1}^{l} \mathfrak{p}_i^{\lfloor (n_i \bmod n^{j+1})/n^j \rfloor}$.

(3) For $j = k, \dots, 0$ find $\alpha_j \in (\mathfrak{a}_{j+1}^n \mathfrak{b}_j)^{-1}$ such that the ideal $\mathfrak{a}_j := \alpha_j^{-1} \mathfrak{a}_{j+1}^n \mathfrak{b}_j$ has small norm.

(4) Return $\alpha_0, \dots, \alpha_k$ and $\mathfrak{a} = \mathfrak{a}_0$.

Remark 11. Finding α_j in Steps (1) and (3) is the well known problem of finding small representatives in ideal classes. The solution involves computing a small basis of the inverse ideal using a lattice reduction. If one uses LLL reduction ([LLL82]), the ideals $\mathfrak{a}_j$ will have a small norm bounded by $O(2^{d^2}\sqrt{|d_K|})$ (see also [BFH17, 4.3]).

We now assume that we have an element $\alpha \in \mathcal{O}_K$ such that $|\mathrm{N}(\alpha)|$ is small and for which we want to compute a compact representation. To do so, we need the following notion. Let $\mathfrak{b}$ be a nonzero integral ideal of $\mathcal{O}_K$. We define

$$\lfloor \sqrt[n]{\mathfrak{b}} \rfloor = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor v_{\mathfrak{p}}(\mathfrak{b})/n \rfloor},$$

to be the n-th root of $\mathfrak{b}$. Here the product runs over all nonzero prime ideals of $\mathcal{O}_K$. Note that $\lfloor \sqrt[n]{\mathfrak{b}} \rfloor$ is an integral ideal such that $\lfloor \sqrt[n]{\mathfrak{b}} \rfloor^n$ divides $\mathfrak{b}$.

Let $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ be the complex embeddings of K. For an element $v = (v_i)_{1 \le i \le d} \in \mathbb{R}^d$ we denote $\max_{1 \le i \le d} |v_i|$ by $\|v\|_\infty$. Recall that the $T_{2,v}$-norm is defined to be $T_{2,v}(\beta) = \sum_{i=1}^d v_i^2 |\sigma_i(\beta)|^2$ for $\beta \in K$.

Algorithm 12 (compact representation for elements of small norm). Let $\alpha \in \mathcal{O}_K$ with $|\mathrm{N}(\alpha)|$ small. The following steps return small elements $\alpha_0, \ldots, \alpha_k$ such that

$$\alpha = \alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}.$$

(1) Define $v = (v_j)_{1 \le j \le d} = (\log(|\sigma_j(\alpha)|))_{1 \le j \le d} \in \mathbb{R}^d$ and $k = \lfloor \log_n(\|v\|_\infty) \rfloor$ so that $n^k \le \|v\|_\infty \le n^{k+1}$. We set $\tilde{\alpha}_{k+1} = \alpha$.

(2) For $i = k, \ldots, 1$, we set $w = (\exp(n^{-i} v_j))_{1 \le j \le d}$ and then compute $\mathfrak{b}_i = \left\lfloor \sqrt[n^i]{\tilde{\alpha}_{i+1} \mathcal{O}_K} \right\rfloor$. Next, use lattice reduction to find an element $\gamma_i \in \mathfrak{b}_i^{-1}$ which is small with respect to $T_{2,w}$, and set $\alpha_i = \gamma_i^{-1}$ and $\tilde{\alpha}_i = \tilde{\alpha}_{i+1} \cdot \gamma_i^{n^i}$.

(3) Define $\alpha_0 = \tilde{\alpha}_1$ and return $\alpha_0, \ldots, \alpha_k$.

Remark 13. The size of the elements $\gamma_1, \ldots, \gamma_k$ of the algorithm is bounded in T_2-norm in terms of n and $\sqrt{d_{K/\mathbb{Q}}}$. Assume that we are in the i-th iteration of the algorithm; using the same notation as in Algorithm 12, the element $\gamma_i \in \mathfrak{b}_i^{-1}$ obtained by the LLL-algorithm has small $T_{2,w}$-norm:

$$T_{2,w}(\gamma_i) \le C \left(d_{K/\mathbb{Q}}^{1/2} N(\mathfrak{b}_i)^{-1} \prod_{j=1}^d w_j \right)^{2/d} \le C \left(d_{K/\mathbb{Q}}^{1/2} N(\alpha)^{1/n^i} \right)^{2/d},$$

where C is the explicit constant of the reduction algorithm and the last inequality comes from the fact that $\left(N(\mathfrak{b}_i)^{-1} \prod_{j=1}^d w_j\right)^{n^i} = N(\alpha) N(\mathfrak{b}_i)^{-n^i}$ is integral, hence bounded by $N(\alpha)$. Clearly, $\alpha \gamma_i^{n^i} \in \mathcal{O}_K$ and we have the following bound on its size:

$$\begin{aligned} T_2(\alpha \gamma_i^{n^i}) &= \sum_{s=1}^d (w_s^{-2n^i} |\sigma_s(\alpha)|^2)(w_s^{2n^i} |\sigma_s(\gamma_i^{n^i})|^2) = \sum_{s=1}^d w_s^{2n^i} |\sigma_s(\gamma_i^{n^i})^2| \\ &\le \left(\sum_{s=1}^d w_s^2 |\sigma_s(\gamma_i)|^2 \right)^{n^i} = T_{2,w}(\gamma_i)^{n^i} \le C^{n^i} N(\alpha)^{2/d} d_{K/\mathbb{Q}}^{n^i/d}. \end{aligned}$$

Thus

$$\|v\|_\infty \le \log T_2(\alpha \gamma_i^{n^i}) \le n^i \log\left(C N(\alpha)^{2/d} d_{K/\mathbb{Q}}^{1/d}\right).$$

Now, $w_i^{-1} = \exp(-n^{-i} v_i) \leq \exp(n^{-i}\|v\|_\infty) \leq CN(\alpha)^{2/l} d_{K/\mathbb{Q}}^{1/d}$ and

$$T_2(\gamma_i) = \sum_{s=1}^{d} w_s^{-2} w_s^2 |\sigma_s(\gamma_i)|^2 \leq \|w^{-1}\|_2^2 T_{2,w}(\gamma_k) \leq dC^3 d_{K/\mathbb{Q}}^{3/d} N(\alpha)^{4/d+2/(dn^i)}$$

is bounded as well.

Summarizing, to reduce an element $\alpha \in K$ modulo $K^{\times n}$, we first apply Algorithm 10 to obtain $\alpha_0, \dots, \alpha_k \in K$ and an ideal $\mathfrak{a}$ of bounded norm such that $\alpha\mathcal{O}_K = (\alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}) \cdot \mathfrak{a}$. Thus the element $\tilde{\alpha}$ defined by

$$\tilde{\alpha} = \alpha(\alpha_0^{-1}\alpha_1^{-n} \cdots \alpha_k^{-n^k})$$

is an element of small norm. This is followed by an application of Algorithm 12 to $\tilde{\alpha}$, which yields $\tilde{\alpha}_0, \dots, \tilde{\alpha}_l$ with

$$\tilde{\alpha} = \tilde{\alpha}_0 \tilde{\alpha}_1^n \cdots \tilde{\alpha}_k^{n^k}.$$

Since

$$\alpha = \prod_{i=0}^{\max(k,l)} (\alpha_i \tilde{\alpha}_i)^{n^i},$$

(where we set $\alpha_i = 1$ and $\tilde{\alpha}_i = 1$ for $i > k$ and $i > l$, respectively), we see that $\alpha \equiv \alpha_0\tilde{\alpha}_0 \bmod K^{\times n}$. By construction, $\alpha_0\tilde{\alpha}_0$ is a small element.

4.5. *Computation of Galois groups.* Let L/K be an abelian extension of degree n, for which we have computed a polynomial $f \in K[X]$ with $L \cong K[X]/(f)$. Denote by $\gamma \in L$ a root of f in L. Our aim is to show how to compute $\mathrm{Gal}(L/K)$ using the objects which showed up during the computation of the defining polynomial f. By computing $\mathrm{Gal}(L/K)$, we mean the computation of the image of γ under the elements of $\mathrm{Gal}(L/K)$. As in Section 4 we may assume that L/K is cyclic. Recall that $F = L(\zeta_n) = K(\zeta_n)(\sqrt[n]{\beta}) = E(\sqrt[n]{\beta})$. Assume first that L and $K(\zeta_n)$ are linearly disjoint. Then the restriction $\mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$ is an isomorphism and, since F/E is a Kummer extension with generator $\sqrt[n]{\beta}$, we have

$$\mathrm{Gal}(F/E) = \langle \sigma : F \to F : \sqrt[n]{\beta} \mapsto \zeta_n \sqrt[n]{\beta} \rangle.$$

In particular, $\sigma|_L$ is a generator of $\mathrm{Gal}(L/K)$ and $a_0, \dots, a_{n-1} \in K$ with

$$\sigma|_L(\gamma) = \sigma(\gamma) = \sum_{i=0}^{n-1} a_i \gamma^i$$

can be found using linear algebra.

In the general case, the restriction map $\mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$ is not surjective. But as the restriction map $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ is always surjective, we can solve the problem by restricting generators of $\mathrm{Gal}(F/K)$ to $\mathrm{Gal}(L/K)$. This can be done using linear algebra as above. Since we have already constructed $\mathrm{Gal}(F/K)$ in the descent step, we do not need to recompute the automorphisms of this extension.

Assume that K/K_0 and L/K_0 are normal extensions; this occurs frequently when constructing towers of normal extensions with more than two layers. In this case, it makes sense to compute the "absolute" Galois group $\mathrm{Gal}(L/K_0)$. The naive way of computing $\mathrm{Gal}(L/K_0)$ would be to write L/K_0 as a simple extension and to find the roots of the defining polynomial. While this works well for small degrees, it quickly becomes unfeasible.

Alternatively, note that $\mathrm{Gal}(L/K_0) = \langle \sigma_1, \dots, \sigma_r, \mathrm{Gal}(L/K)\rangle$, where $\sigma_1, \dots, \sigma_r$ are extensions of generators of $\mathrm{Gal}(K/K_0)$ to L. By the first part, we know how to compute generators of $\mathrm{Gal}(L/K)$, thus it is sufficient to show how to extend an automorphism $\sigma \in \mathrm{Gal}(K/K_0)$ to an element of $\mathrm{Gal}(L/K_0)$. Let ℓ be a prime dividing $[L : K]$ and denote by L_ℓ/K the largest subextension such that $[L : L_\ell]$ is coprime to ℓ. As $\mathrm{Gal}(L_\ell/K)$ is isomorphic to the ℓ-Sylow subgroup of $\mathrm{Gal}(L/K)$, L_ℓ/K_0 is also normal. Since L/K is the compositum of the linearly disjoint L_ℓ/K, where ℓ divides $[L : K]$, we may assume that $L = L_\ell$ is an abelian ℓ-extension of K. In particular, L itself is the compositum of linearly disjoint cyclic extensions $L_i = K(\gamma_i)$ of prime power degree ℓ^{m_i}. Recall that we have constructed the extension L_i/K by passing to the Kummer extension $L_i(\zeta_{\ell^{m_i}})/K(\zeta_{\ell^{m_i}})$, for which we computed an element $\beta_i \in K(\zeta_{\ell^{m_i}})$ with $L_i(\zeta_{\ell^{m_i}}) = K(\zeta_{\ell^{m_i}}, \sqrt[m_i]{\beta_i})$. For simplicity we assume that $m_i = m$ for all $i = 1, \dots, r$ and set $n = \ell^m$, $E = K(\zeta_n)$. We have the following lattices of number fields:

$$\begin{tikzcd}
& K(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & K_0(\zeta_n) \arrow[dl, dash] \\
& K \cap K_0(\zeta_n) &
\end{tikzcd}
\qquad
\begin{tikzcd}
& E(\sqrt[m]{\beta_1}, \dots, \sqrt[m]{\beta_r}) = M \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & E = K(\zeta_n) \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

The idea is to extend $\sigma \in \mathrm{Gal}(K/K_0)$ to an automorphism of

$$M = E(\sqrt[n]{\beta_1}, \dots, \sqrt[n]{\beta_r})$$

and then to restrict this to L. As the first step, we extend σ to $K(\zeta_n)$. Denote by K_1 the intersection $K_0(\zeta_n) \cap K$. Then $K(\zeta_n)/K_1$ is the compositum of the linearly disjoint extensions K/K_1 and $K_0(\zeta_n)/K_1$. Thus it is straightforward to extend σ to an automorphism of $K(\zeta_n)$, which we also denote by σ.

In the next step, we extend σ to an automorphism $\hat{\sigma}$ of M by determining $\hat{\sigma}(\sqrt[n]{\beta_i})$ for all $i = 1, \dots, r$, using the Frobenius automorphisms. We now fix $i \in \{1, \dots, r\}$. Since M/E is a Kummer extension, there exist unique $1 \le n_j \le n$ and $\mu \in K(\zeta_n)$ such that

$$\hat{\sigma}(\sqrt[n]{\beta_i}) = \mu \cdot (\sqrt[n]{\beta_1})^{n_1} (\sqrt[n]{\beta_2})^{n_2} \cdots (\sqrt[n]{\beta_r})^{n_r}. \tag{2}$$

Our aim is to determine the n_j as well as μ. As $\hat{\sigma}$ extends σ, we may assume that $\hat{\sigma}(\sqrt[n]{\beta_i}) = \sqrt[n]{\sigma(\beta_i)}$. For a finite prime $\mathfrak{p}$ of E, unramified in M/E, there exist $e_\mathfrak{p}$, $e_{\mathfrak{p},1}, \dots, e_{\mathfrak{p},r} \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\begin{aligned}
\mathrm{Frob}_{\mathfrak{p},M/E}(\sqrt[n]{\beta_j}) &= \mathrm{Frob}_{\mathfrak{p},E(\sqrt[n]{\beta_j})/E}\big(\zeta_n^{e_{\mathfrak{p},j}} \sqrt[n]{\beta_j}\big), \\
\mathrm{Frob}_{\mathfrak{p},M/E}\big(\sqrt[n]{\sigma(\beta_i)}\big) &= \mathrm{Frob}_{\mathfrak{p},E(\sqrt[n]{\sigma(\beta_i)})/E}\big(\sqrt[n]{\sigma(\beta_i)}\big) = \zeta_n^{e_\mathfrak{p}} \sqrt[n]{\sigma(\beta_i)}.
\end{aligned}$$

Since $\mathrm{Frob}_{\mathfrak{p},M/E}(\mu)=\mu$, applying $\mathrm{Frob}_{\mathfrak{p},M/E}$ to (2) yields

$$\zeta_n^{e_\mathfrak{p}}=\zeta_n^{n_1e_{\mathfrak{p},1}}\cdots\zeta_n^{n_re_{\mathfrak{p},r}},\quad\text{that is,}\quad 0=e_\mathfrak{p}-\sum_{i=1}^r n_ie_{\mathfrak{p},i}\ \text{in}\ \mathbb{Z}/n\mathbb{Z}.$$

Thus, for each prime we get a linear equation over $\mathbb{Z}/n\mathbb{Z}$ of which $n_1,\dots,n_r$ is a solution. Since $\mathrm{Gal}(M/E)$ is generated by $\mathrm{Frob}_{\mathfrak{p},M/E}$, $\mathfrak{p}$ a finite prime of K, we know that using sufficiently many primes $(n_1,\dots,n_r)$ will be the unique solution of the simultaneous equations. Hence we can use Proposition 4 to compute $n_1,\dots,n_r$. Once this is done, we can recover μ by extracting an n-th root of

$$\frac{\sigma(\beta_i)}{\beta_1^{n_1}\cdots\beta_r^{n_r}}=\mu^n.$$

5. Invariant subgroups

5.1. ***Normal extensions.*** Let K be a number field which is normal over the base field K_0 with Galois group $G=\mathrm{Gal}(K/K_0)$. In this section we describe how to compute abelian extensions of K, which are also normal over K_0.

The action of G on K extends to an action on the places of K and, in particular, on the set of moduli of K. Let $\mathfrak{m}$ be a modulus which is invariant under the action of G, that is, $\sigma(\mathfrak{m})=\mathfrak{m}$ for every $\sigma\in G$. In this case G acts on the ray class group $\mathrm{Cl}_\mathfrak{m}$ by sending $[I]$ to $[\sigma(I)]$.

Remark 14. Let L be an abelian extension of K with conductor $\mathfrak{m}$ and let $\sigma: L\to\bar{\mathbb{Q}}$ be an embedding. Then $\sigma(\mathfrak{m})$ is the conductor of $\sigma(L)$ over $\sigma(K)$. To see this it is enough to consider the compositum of the Artin map with σ.

Proposition 15. *Let $\mathfrak{m}$ be a modulus of K which is invariant under the action of G. Every subgroup H of $\mathrm{Cl}_\mathfrak{m}$ which is invariant under the action of G corresponds to an abelian extension L/K, such that L/K_0 is normal. Conversely, let L be an abelian extension of K which is normal over K_0. Then the conductor $\mathfrak{f}$ of L/K as well as the corresponding congruence subgroup are invariant under the action of G.*

Proof. Firstly, we prove that if $\mathfrak{m}$ is an invariant modulus, the statement is true for $H=\{1\}$ and the corresponding extension L. Let σ be an embedding of L into $\bar{\mathbb{Q}}$ such that $\sigma|_{K_0}=\mathrm{id}$. Then $\sigma(K)=K$ since K is normal over K_0 and $\sigma(L)$ is an abelian extension of K with admissible modulus $\sigma(\mathfrak{m})$. As $\sigma(\mathfrak{m})=\mathfrak{m}$, we get $\sigma(L)\subseteq L$ and thus L/K_0 is normal.

Now, let H be an invariant subgroup of $\mathrm{Cl}_\mathfrak{m}$ corresponding to an extension L and let F be the ray class field corresponding to $\{1\}<\mathrm{Cl}_\mathfrak{m}$. We want to show that L is normal over K_0, or, equivalently, that $\mathrm{Gal}(F/L)$ is normal in $\mathrm{Gal}(F/K_0)$. In this setting, we have the exact sequence

$$1\to\mathrm{Gal}(F/K)\to\mathrm{Gal}(F/K_0)\to\mathrm{Gal}(K/K_0)\to 1.$$

In particular, $\mathrm{Gal}(F/K_0)$ is generated by a set of generators of $\mathrm{Gal}(F/K)$ and preimages of generators of $\mathrm{Gal}(K/K_0)$. Obviously, $\mathrm{Gal}(F/L)$ is invariant under conjugation by elements of $\mathrm{Gal}(F/K)$ in $\mathrm{Gal}(F/K_0)$ since F/K is abelian. By the properties of the Artin map, $\mathrm{Cl}_\mathfrak{m}\simeq\mathrm{Gal}(F/K)$ and the action of G on $\mathrm{Cl}_{\mathfrak{m}}$ corresponds to conjugation in the group $\mathrm{Gal}(F/K_0)$. Since H is invariant, this means that $\mathrm{Gal}(F/L)$ is invariant under conjugation by generators of $\mathrm{Gal}(K/K_0)$ and therefore it is a normal subgroup.

On the other hand, let L be an abelian extension of K which is normal over K_0. The conductor being invariant follows from the observation above. Furthermore, we know that the field L corresponding to $\{1\} < \mathrm{Cl}_{\mathfrak{f}}$ is normal over K_0. Since L is normal, it corresponds to a normal subgroup of $\mathrm{Gal}(F/K_0)$, so it is invariant under conjugation by elements of this group. By the properties of the Artin map, the action of $\mathrm{Gal}(K/K_0)$ on $\mathrm{Gal}(F/K)$ is given by conjugation in $\mathrm{Gal}(F/K_0)$. Since L is normal, the corresponding subgroup is invariant. □

Consequently, if we are searching for abelian extensions of K which are also normal over K_0, we can restrict to invariant subgroups of the ray class groups.

5.2. *Computing invariant subgroups.* Let M be a finite abelian group of exponent n and G a finite group acting on M. We now describe how to compute the set of all G-invariant subgroups of M. While one could of course first compute the set of all subgroups of M using a theorem of Butler [But94], the following example shows that this is in general not a useful approach.

Example 16. We consider the abelian group $M = (\mathbb{Z}/25\mathbb{Z})^{11}$ with the symmetric group $G = S_{11}$ acting via $\sigma(a_1, \dots, a_{11}) = (a_{\sigma(1)}, \dots, a_{\sigma(11)})$ for $\sigma \in S_{11}$ and $(a_1, \dots, a_{11}) \in M$. Then the number of subgroups of M with quotient isomorphic to $\mathbb{Z}/25\mathbb{Z}$ is 119209287109375, and only one of these subgroups is invariant.

Denote by $\mathbb{Z}[G]$ the integral group ring of G. Since G-invariant subgroups of M are the same as $\mathbb{Z}[G]$-submodules of M and $n\mathbb{Z}$ acts trivially on M, it is sufficient to determine the $(\mathbb{Z}/n\mathbb{Z})[G]$-submodules of M.

By induction, it is enough to find all the irreducible $(\mathbb{Z}/n\mathbb{Z})[G]$-submodules of M. Since this task can be easily solved in case the exponent n of M is a prime number using the meat-axe (see [Par84] and [HEO05, Section 7.4]), we will focus on the nonprime case. As usual we can assume that the exponent n is a prime power: indeed, for every prime number q dividing the order of M, the q-Sylow subgroup of M is invariant and they generate the whole group M. This means that every simple $(\mathbb{Z}/n\mathbb{Z})[G]$-submodule of M must be contained in one of the Sylow subgroups of M. As the q-Sylow subgroup of M is naturally a $(\mathbb{Z}/q^{v_q(n)}\mathbb{Z})[G]$-module, we may assume that $n = p^s$ is a prime power.

Proposition 17. *Let N be a simple $(\mathbb{Z}/p^s\mathbb{Z})[G]$-module. Then the exponent of N is p.*

Thus all minimal submodules are contained in the submodule $M_p = \{m \in M \mid pm = 0\}$, which is naturally an $\mathbb{F}_p[G]$-module. Thus to find the $(\mathbb{Z}/p^s\mathbb{Z})[G]$-submodules, we just have to apply the method for the prime case and iterate. In particular, we have an efficient algorithm to determine the G-invariant subgroups of an abelian group M.

Remark 18. Assume we want to compute only G-invariant subgroups N of M such that the quotient M/N has exponent m. As mM itself is G-invariant, the group G also acts on M/mM and the G-invariant subgroups of M with quotient of exponent m correspond to the G-invariant subgroups of M/mM. In the situation where $M = \mathrm{Cl}_{\mathfrak{m}}$ is the ray class group, this implies that again it is sufficient to only compute the quotient $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^m$ instead of the whole ray class group.

5.3. ***Duality.*** While the previous section provides a solution to the problem of finding G-invariant subgroups of M, it can be very inefficient if we are looking only for subgroups N with small index in M, since it can be necessary to repeat the procedure for finding minimal submodules multiple times.

In this case, we can use duality to translate the problem of finding submodules of small index into the one of finding submodules of small order. Recall that the dual group M^* of M is the group $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}/p^s\mathbb{Z})$, which is isomorphic to M. In practice, an isomorphism can be written explicitly after a choice of a basis. In our case, we assume that M has exponent p^s and is given in Smith normal form, that is, $M = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_w}\mathbb{Z}$ with $1 \le n_1 \le \cdots \le n_w = s$. Let $e_1, \dots, e_w$ be the canonical generators of M. Then we define elements of the dual

$$e_i^* : M \to \mathbb{Z}/p^s\mathbb{Z}, \qquad e_j \mapsto \delta_{ij} \frac{p^s}{\mathrm{ord}(e_i)},$$

where δ_{ij} is the Kronecker delta and $\mathrm{ord}(e_i)$ denotes the order of e_i. The dual is again in Smith normal form with respect to this generating set.

Every endomorphism φ of M induces a dual morphism

$$\varphi^* : M^* \to M^*, \qquad f \mapsto f \circ \varphi.$$

In particular every element $g \in G$ acts on M^*, endowing M^* with the structure of a $(\mathbb{Z}/p^s\mathbb{Z})[G]$-module. The action of G on the dual group just defined preserves the inclusion-reversing correspondence existing between subgroups of M and subgroups of M^*. Given a subgroup H of M, define the orthogonal complement of H as

$$H^\perp = \{\varphi \in M^* \mid H \subseteq \ker(\varphi)\}.$$

Proposition 19. *There is an inclusion-reversing bijection between submodules of M and M^*:*

$$\{(\mathbb{Z}/p^s\mathbb{Z})[G]\text{-submodules of } M\} \to \{(\mathbb{Z}/p^s\mathbb{Z})[G]\text{-submodules of } M^*\},$$
$$H \mapsto H^\perp.$$

Furthermore, for every submodule H of M, we have $H^\perp \simeq G/H$.

Thus if we want to search for submodules of small index, we can instead search for submodules of the dual module of small order and then use duality. In order to make this computationally effective, we need to understand how to obtain the action on the dual group M^* given the one on the group M. As above, we assume that M is given in Smith normal form with generators e_i and we consider the corresponding element of the dual e_i^*. Let $\varphi \in \mathrm{Aut}(M)$ be the automorphism of M induced by $g \in G$. We want to compute the matrix $A = (a_{ij})$ associated to φ^* with respect to the basis e_i^*. Note that by definition, $\varphi^*(e_i^*) = e_i^* \circ \varphi$. Let B be the matrix representing φ with respect to the elements e_i and let d_i

be the valuation of the order of e_i at p. Then

$$\varphi^*(e_i^*)(e_j) = e_i^*(\varphi(e_j)) = e_i^*\left(\sum_k b_{jk}e_k\right) = b_{ji}e_i^*(e_i) = b_{ji}p^{s-d_i}.$$

On the other hand,

$$\varphi^*(e_i^*)(e_j) = \left(\sum_k a_{ik}e_k^*\right)(e_j) = a_{ij}e_j^*(e_j) = a_{ij}p^{s-d_j}.$$

Therefore, it is enough to choose a_{ij} satisfying the relation $a_{ij}p^{s-d_j} = b_{ji}p^{s-d_i}$.

6. Application: fields with minimal discriminant

The algorithms outlined in the previous sections have been implemented in the number theory package Hecke [FHHJ17].[1] As an application, we used our implementation to find number fields K having Galois closure L over $\mathbb{Q}$ with prescribed Galois group and such that K has minimal discriminant among all fields with this property. We chose to consider the following cases:

- K of degree 15 with $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_{15}$ and signature $(1, 7)$.
- K of degree 15 with $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_5 \times C_3$ and signature $(3, 6)$.
- K of degree 15 with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3 \times C_5$ and signature $(5, 5)$.
- K of degree 36 with $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_9 \rtimes C_4$ and signatures $(36, 0)$, $(0, 18)$.

All together the computations took 12 hours on an Intel i7-4790 with 3.6 GHz. The results of the computation are given in Theorem 1.

6.1. ***Nonnormal extensions of degree* 15.** In this section, we consider number fields K of degree 15 over $\mathbb{Q}$ having Galois closure L over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong G \in \{D_{15}, D_5 \times C_3, S_3 \times C_5\}$. Our strategy is to compute the normal closure L (of degree 30) of K and then use the trace and norm to find the corresponding field K (as in Section 4.3). Since G has a normal cyclic subgroup of degree 15, we can construct L as a relative cyclic extension of degree 15 over a quadratic field F_2. A crucial point is the choice for the bound on the discriminant of the Galois closure L given a bound on the field K of degree 15. Since L is the compositum of F_2 and K we have $d_{L/\mathbb{Q}} \leq d_{F_2/\mathbb{Q}}^{15} \cdot d_{K/\mathbb{Q}}^2$. Thus, we need to find a bound for the field F_2 given the one on K. For this, we have to distinguish the cases corresponding to the different groups.

- If $G = D_{15}$, we can apply [Coh00, Theorem 9.2.6] to obtain the bound $d_{F_2/\mathbb{Q}} \leq d_{K/\mathbb{Q}}^{1/7}$.
- If $G = D_5 \times C_3$, then K has an intermediate subfield K_1 of degree 5 and $d_{K_1/\mathbb{Q}} \leq d_{K/\mathbb{Q}}^{1/3}$ by the behavior of the discriminant in towers of extensions. Now, the Galois closure of K_1 has Galois group D_5 and so we apply again [Coh00, Theorem 9.2.6] to obtain $d_{F_2/\mathbb{Q}} \leq d_{K_1/\mathbb{Q}}^{1/2} \leq d_{K/\mathbb{Q}}^{1/6}$.

[1] Available at https://github.com/thofma/Hecke.jl

- If $G = S_3 \times C_5$, we use the same strategy as in the case of $D_5 \times C_3$. Here K has an intermediate subfield K_1 of degree 3 whose Galois closure is an S_3-extension of $\mathbb{Q}$ and $d_{K_1/\mathbb{Q}} \leq d_{K/\mathbb{Q}}^{1/5}$. Therefore $d_{F_2/\mathbb{Q}} \leq d_{K_1/\mathbb{Q}} \leq d_{K/\mathbb{Q}}^{1/5}$.

Thus, we need to list the imaginary quadratic fields up to these bounds, since we are searching for fields K with nonreal embeddings. By Proposition 15, the possible conductors are invariant under the action of the Galois group of F_2. For every possible conductor $\mathfrak{m}$, we need to search for invariant subgroups of index 15 in the group $R = \mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{15}$. Before computing the defining polynomial, we check that the action of G on the quotient by any subgroup corresponds to the correct group extension. More precisely, let H be a congruence subgroup of $\mathrm{Cl}_\mathfrak{m}$ and let σ be the generator of $\mathrm{Gal}(F_2/\mathbb{Q})$. Then:

- For the D_{15}-extensions, σ must send every element of $\mathrm{Cl}_\mathfrak{m}/H$ to its inverse.
- For the $D_5 \times C_3$-extensions, σ must fix the 3-Sylow subgroup of $\mathrm{Cl}_\mathfrak{m}/H$ and act on the 5-Sylow by sending every element to its inverse.
- For the $S_3 \times C_5$-extensions, σ must fix the 5-Sylow subgroup of $\mathrm{Cl}_\mathfrak{m}/H$ and act on the 3-Sylow by sending every element to its inverse.

6.2. ***Extensions of degree* 36.** For $G = C_9 \rtimes C_4$, we construct these fields as a tower of a normal field of degree 4 and a field of degree 9 on top of it. In this example, the tools we developed in the previous sections are fundamental, since we are dealing with extensions having nonsquarefree degree.

References

[BF14] Jean-François Biasse and Claus Fieker, *Subexponential class group and unit group computation in large degree number fields*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 385–403. MR 3240816

[BFH17] Jean-François Biasse, Claus Fieker, and Tommy Hofmann, *On the computation of the HNF of a module over the ring of integers of a number field*, J. Symbolic Comput. **80** (2017), no. part 3, 581–615. MR 3574529

[But94] Lynne M. Butler, *Subgroup lattices and symmetric functions*, Mem. Amer. Math. Soc., no. 539, Amer. Math. Soc., Providence, RI, 1994. MR 1223236

[CDyDO96] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Computing ray class groups, conductors and discriminants*, Algorithmic number theory, Lecture Notes in Comput. Sci., no. 1122, Springer, 1996, pp. 49–57. MR 1446497

[CDyDO98] ———, *Computing ray class groups, conductors and discriminants*, Math. Comp. **67** (1998), no. 222, 773–795. MR 1443117

[Coh99] Henri Cohen, *A survey of computational class field theory*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 1–13. MR 1730429

[Coh00] ———, *Advanced topics in computational number theory*, Graduate Texts in Math., no. 193, Springer, 2000. MR 1728313

[CS08] Henri Cohen and Peter Stevenhagen, *Computational class field theory*, Algorithmic number theory: Lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., no. 44, Cambridge Univ. Press, 2008, pp. 497–534. MR 2467555

[DP95] M. Daberkow and M. Pohst, *Computations with relative extensions of number fields with an application to the construction of hilbert class fields*, Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 1995, pp. 68–76.

[DP98] ———, *On the computation of Hilbert class fields*, J. Number Theory **69** (1998), no. 2, 213–230. MR 1617325

[FHHJ17] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson, *Nemo/Hecke: computer algebra and number theory packages for the Julia programming language*, Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2017, pp. 157–164. MR 3703682

[Fie01] Claus Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303. MR 1826583

[Has64] H. Hasse, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante −47*, Acta Arith. **9** (1964), 419–434. MR 0172866

[Has67] ———, *Vorlesungen über Klassenkörpertheorie*, Thesaurus Mathematicae, no. 6, Physica-Verlag, Würzburg, 1967. MR 0220700

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Chapman & Hall/CRC, Boca Raton, FL, 2005. MR 2129747

[Jan96] Gerald J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Math., no. 7, Amer. Math. Soc., 1996. MR 1362545

[KM01] Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196. MR 1901356

[Lan94] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Math., no. 110, Springer, 1994. MR 1282723

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR 682664

[Par84] R. A. Parker, *The computer calculation of modular characters (the meat-axe)*, Computational group theory, Academic Press, London, 1984, pp. 267–274. MR 760660

[Poh99] Michael E. Pohst, *From class groups to class fields*, Algorithmic algebra and number theory, Springer, 1999, pp. 103–119. MR 1672109

[Thi95] Christoph Thiel, *On the complexity of some problems in algorithmic algebraic number theory*, Ph.D. thesis, Universität des Saarlandes, 1995.

Received 2 Mar 2018. Revised 28 Aug 2018.

CLAUS FIEKER: fieker@mathematik.uni-kl.de
Fachbereich Mathematik, Technische Universität Kaiserslautern, Kaiserslautern, Germany

TOMMY HOFMANN: thofmann@mathematik.uni-kl.de
Fachbereich Mathematik, Technische Universität Kaiserslautern, Kaiserslautern, Germany

CARLO SIRCANA: sircana@mathematik.uni-kl.de
Fachbereich Mathematik, Technische Universität Kaiserslautern, Kaiserslautern, Germany

VOLUME EDITORS

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

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

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

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

First published 2019.

msp

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