MATHEMATICS OF COMPUTATION
Volume 67, Number 222, April 1998, Pages 773–795
S 0025-5718(98)00912-0

COMPUTING RAY CLASS GROUPS, CONDUCTORS AND DISCRIMINANTS

H. COHEN, F. DIAZ Y DIAZ, AND M. OLIVIER

ABSTRACT. We use the algorithmic computation of exact sequences of Abelian groups to compute the complete structure of $(\mathbb{Z}_K/\mathfrak{m})^*$ for an ideal $\mathfrak{m}$ of a number field K, as well as ray class groups of number fields, and conductors and discriminants of the corresponding Abelian extensions. As an application we give several number fields with discriminants less than previously known ones.

The paper is divided as follows. In §1, we give a complete algorithm for computing the groups $(\mathbb{Z}_K/\mathfrak{m})^*$ for a number field K and an arbitrary modulus $\mathfrak{m}$. In §2, we describe the tools necessary for the determination of the ray class group of a number field, and also for solving the corresponding principal ideal problem. In §3, we explain how to compute signatures, conductors and discriminants of the fields associated to subgroups of the ray class group by global class field theory. In principle we can give relative and absolute discriminants of all Abelian extensions of a given base field. Finally in §4, we give some numerical examples obtained by these methods. In particular, we obtain in this way 10 totally complex number fields of degree less than 80 whose discriminants are less than previously known ones.

Using Kummer theory (see e.g. [Da-Po]), we can also obtain a defining equation for these number fields, and we have done this for 9 of the 10 new fields that we have found.

We refer to [Ca-Fr] for notation, definitions and results on global class field theory.

1. COMPUTING THE STRUCTURE OF $(\mathbb{Z}_K/\mathfrak{m})^*$

Let K be a number field, and $\mathfrak{m}$ a modulus in K, in other words $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ is a (formal) product of an integral ideal of K and a subset of the set of real places of K. We denote by $\mathbb{Z}_K$ the ring of integers of K.

In this section, we explain how to compute the group $(\mathbb{Z}_K/\mathfrak{m})^* = (\mathbb{Z}_K/\mathfrak{m}_0)^* \times \mathbb{F}_2^{\mathfrak{m}_\infty}$. The theoretical answer to this question is in principle solved in [Nak]. However this is not suited to algorithmic purposes, and in addition is much more complicated than the solution we present below.

The natural map from the set of elements of $\mathbb{Z}_K$ coprime to $\mathfrak{m}$ to $(\mathbb{Z}_K/\mathfrak{m})^*$ is surjective. Thus, we could represent an element of this set as the class of an element of $\mathbb{Z}_K$ (the so-called one-element representation). However we prefer the following representation which is computationally simpler.

Received by the editor February 19, 1996 and, in revised form, October 30, 1996.
1991 *Mathematics Subject Classification.* Primary 11R37, 11Y40.
Key words and phrases. Ray class groups, conductors, discriminants .

If $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ we represent an element in $(\mathbb{Z}_K/\mathfrak{m})^*$ as a pair $(\overline{\alpha}, v)$ where $\overline{\alpha} \in (\mathbb{Z}_K/\mathfrak{m}_0)^*$ and $v \in \mathbb{F}_2^{\mathfrak{m}_\infty}$ considered as a *column* vector. Note that even when $\mathfrak{m}$ is an ideal (i.e. $\mathfrak{m}_\infty$ is empty), we still consider pairs $(\overline{\alpha}, v)$ where v is the unique vector in 0-dimensional space over $\mathbb{F}_2$. If $(\overline{\alpha}, v) \in (\mathbb{Z}_K/\mathfrak{m})^*$, we will say that $\overline{\alpha}$ is the *finite part*, and v the *infinite part* or the *Archimedean part*. The group law in $(\mathbb{Z}_K/\mathfrak{m})^*$ corresponds to multiplying the finite parts and adding the infinite parts. In all the algorithms that we will present, the above representation is sufficient and simpler than the one-element representation. In some cases, however, it may be desirable to find such a representation. To obtain it, one can do the following: Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus and $(\overline{\alpha}, v)$ a pair representing an element of $(\mathbb{Z}_K/\mathfrak{m})^*$, with $v = (v_j)_{j\in\mathfrak{m}_\infty}$ and call s the sign homomorphism from $\mathbb{Z}_K$ to $\mathbb{F}_2^{\mathfrak{m}_\infty}$. Compute a $\mathbb{Z}$-basis $\gamma_1, \ldots, \gamma_n$ of the ideal $\mathfrak{m}_0$. Considering small linear combinations of the γ_i, find k elements $\beta_1, \ldots, \beta_k$ such that the matrix A over $\mathbb{F}_2$ whose columns are the $s(\beta_j)$ is invertible. Set $w = A^{-1}v$, and let $w = (w_j)$. A suitable element is

$$\beta = \alpha \prod_{\substack{j\in\mathfrak{m}_\infty \\ w_j\neq 0}} \beta_j.$$

Since the final β may be large, we may want to reduce it. This cannot be done too rashly however, since we must now preserve the signature of β. We will discuss this at the end of §2.

To compute the structure of $(\mathbb{Z}_K/\mathfrak{m})^*$, we start by the following lemma, whose non-algorithmic version is trivial.

Lemma 1.1. *Let $\mathfrak{a}$ and $\mathfrak{c}$ be two coprime integral ideals of K.*

(1) *We can algorithmically find elements $a \in \mathfrak{a}$ and $c \in \mathfrak{c}$ such that $a + c = 1$.*

(2) *Set $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. We have a split exact sequence*

$$1 \longrightarrow (\mathbb{Z}_K/\mathfrak{a})^* \xrightarrow{\psi} (\mathbb{Z}_K/\mathfrak{b})^* \xrightarrow{\phi} (\mathbb{Z}_K/\mathfrak{c})^* \longrightarrow 1 \ ,$$

where $\psi(\overline{\alpha}) = \overline{c\alpha + a}$, $\phi(\overline{\beta}) = \overline{\beta}$ and a section σ of ϕ is given by $\sigma(\overline{\gamma}) = \overline{a\gamma + c}$. (Here $\overline{\ }$ denotes the classes in the respective groups, but using the same notation for each will not lead to any confusion as long as we know in which group we are working.)

Proof. (1) By assumption, we have $\mathfrak{a} + \mathfrak{c} = \mathbb{Z}_K$. Thus there exist $a \in \mathfrak{a}$ and $c \in \mathfrak{c}$ such that $a + c = 1$. The algorithm to find them is explained in [Coh2]. For completeness we sketch it here. Let A (resp. C) be the Hermite normal form of $\mathfrak{a}$ and $\mathfrak{c}$ with respect to some fixed integral basis of $\mathbb{Z}_K$. We assume (it is easy to reduce to this case) that the first element of the integral basis is 1. We apply the Hermite normal form algorithm to the matrix $(A|C)$, where here and later, $(A|C)$ denotes the (horizontal) concatenation of the matrices A and C. If U is a unimodular matrix obtained during the HNF, we have $(A|C)U = (0|I)$ where I is the $d \times d$ identity matrix (where $d = [K : \mathbb{Q}]$) since $\mathfrak{a}$ and $\mathfrak{c}$ are coprime. Let X_1 (resp. X_2) be the top (resp. bottom) half of the $(d+1)$st column of U. Then AX_1 and CX_2 represent, with respect to the fixed integral basis, elements a and c satisfying the required conditions.

The proof of (2) is straightforward and tedious, and left to the reader. □

Remark. More generally, if $\mathfrak{a}$ and $\mathfrak{c}$ are two coprime moduli (i.e. $\mathfrak{a}_0 + \mathfrak{c}_0 = \mathbb{Z}_K$ and $\mathfrak{a}_\infty \cap \mathfrak{c}_\infty = \emptyset$) there exist elements a and c such that $a + c = 1$, $a \equiv 1 \pmod{{}^*\mathfrak{c}}$, $c \equiv 1 \pmod{{}^*\mathfrak{a}}$. There is also an exact sequence generalizing (2).

A finitely generated Abelian group $\mathcal{G}$ will be represented by generators and relations, i.e. as a pair (G, D_G) where G is a (finite) set of generators of G given as a row vector, and D_G is a matrix representing a set of relations for G in Smith Normal Form. Since the Abelian groups that we will use are multiplicative, it is to be understood that a product such as GX (where X is a column vector of integers) is to be interpreted in a multiplicative sense, i.e. if $G = (g_i)$ and $X = (x_i)$, then $GX = \prod g_i^{x_i}$.

Thus, let (A, D_A) (resp. (C, D_C)) be the Smith Normal Form of $(\mathbb{Z}_K/\mathfrak{a})^*$ (resp. $(\mathbb{Z}_K/\mathfrak{c})^*$). By Lemma 1.1, it is clear that to obtain the structure of $(\mathbb{Z}_K/\mathfrak{b})^*$ we can simply construct a diagonal matrix using D_A and D_C as diagonal blocks, and then transform this matrix into its Smith Normal Form.

More generally, we will need to perform algorithmically standard operations on Abelian groups such as computing kernels, images, quotients and extensions. Since it is not easy to find explicit descriptions of these algorithms in the literature, and since some details are not completely trivial, we give some explanations for the most important case of group extensions (see [Co-Di-Ol] for complete details).

Let $\mathcal{A} = (A, D_A)$ and $\mathcal{C} = (C, D_C)$ be given in SNF. We assume that we can solve the discrete logarithm problem in $\mathcal{A}$ and $\mathcal{C}$, in other words, that we can express an arbitrary element of the groups as a power product of its generators.

Now assume that we have an exact sequence

$$1 \longrightarrow \mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\phi} \mathcal{C} \longrightarrow 1 \ ,$$

and we want to compute the SNF (B, D_B) of the group $\mathcal{B}$. This is done using the following proposition.

Proposition 1.2. *With the above notation, let B' be such that $\phi(B') = C$, set $S = (B'|\psi(A))$.*

(1) *There exists a matrix P with integer coefficients such that $B'D_C = \psi(A)P$.*
(2) *Set*

$$M = \begin{pmatrix} D_C & 0 \\ -P & D_A \end{pmatrix} \ .$$

Then (S,M) is a system of generators and relations for the group $\mathcal{B}$, and hence we can obtain the SNF (B, D_B) of the group $\mathcal{B}$ by applying the Smith normal form algorithm to (S, M).

Proof. Since ϕ is surjective, we can find B' such that $\phi(B') = C$. Let $\beta \in \mathcal{B}$. We can write $\phi(\beta) = CX = \phi(B')X = \phi(B'X)$, hence $\beta - B'X \in \mathrm{Ker}(\phi)$ so $\beta - B'X = \psi(AY)$ for some integer vector Y. Thus $\beta = B'X + \psi(A)Y = (B'|\psi(A))R$ where $R = \binom{X}{Y}$ is the vertical concatenation of the column vectors X and Y. It follows that $S = (B'|\psi(A))$ forms a generating set for $\mathcal{B}$.

Let us find the relations between these generators. If $R = \binom{X}{Y}$ is such a relation, we have $B'X + \psi(A)Y = 1$. If we apply ϕ to this relation, we obtain $\phi(B')X = CX = 1$, hence $X \in \mathrm{Im}\, D_C$, i.e. $X = D_C X_1$. Thus we have $B'D_C X_1 + \psi(A)Y = 1$.

Set $B'' = B'D_C$. Then $\phi(B'') = \phi(B')D_C = CD_C = \mathbf{1}$. Thus the entries of B'' are in $\mathrm{Ker}(\phi) = \mathrm{Im}(\psi)$, hence since we can solve the discrete logarithm problem in $\mathcal{A}$ we can find a matrix P such that $B'' = \psi(AP) = \psi(A)P$.

So finally, the equation for our relation is

$$\psi(A)PX_1 + \psi(A)Y = 1 \iff \psi(A)(PX_1 + Y) = 1 \iff PX_1 + Y \in \operatorname{Im} D_A$$
$$\iff PX_1 + Y = D_A T \quad \text{for some integer vector } T.$$

In other words, R is a relation if and only if we have

$$R = M \begin{pmatrix} X_1 \\ T \end{pmatrix} \quad \text{with} \quad M = \begin{pmatrix} D_C & 0 \\ -P & D_A \end{pmatrix}$$

for some integer vectors X_1 and T. Thus (S, M) is a system of generators and relations for $\mathcal{B}$. Applying the SNF algorithm to (S, M) we obtain two unimodular matrices U and V and the SNF (B, D_B) of the group $\mathcal{B}$ such that $D_B = UMV$ and $B = SU^{-1}$. This finishes the proof of the proposition. □

To solve the discrete logarithm problem in $\mathcal{B}$ is easy. Let $\beta \in \mathcal{B}$. Using the solution to the discrete logarithm in $\mathcal{C}$ we can find X such that $\phi(\beta) = CX = \phi(B')X$, hence $\phi(\beta - B'X) = 1$ so $\beta - B'X \in \operatorname{Im}(\psi)$, and using the solution to the discrete logarithm problem in $\mathcal{A}$ we obtain $\beta - B'X = \psi(A)Y$ for some Y, so $\beta = (B'|\psi(A))\binom{X}{Y}$. Finally, if U is the unimodular matrix obtained in the SNF algorithm above, this gives $\beta = BU\binom{X}{Y}$; hence $U\binom{X}{Y}$ is our desired discrete logarithm.

We can now explain how to compute the structure of $(\mathbb{Z}_K/\mathfrak{a})^*$ for an ideal $\mathfrak{a}$. By Lemma 1.1, it is enough to compute $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ for a prime ideal $\mathfrak{p}$ and a positive integer k, and we now consider this problem.

Definition and Proposition 1.3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be (nonzero) ideals. Assume that $\mathfrak{a} \mid \mathfrak{b} \mid \mathfrak{a}^k$ for some positive integer k. We denote by $(1+\mathfrak{a})/(1+\mathfrak{b})$ the quotient set of $1+\mathfrak{a}$ by the equivalence relation $\mathcal{R}$ defined by $(1+x)\mathcal{R}(1+y) \iff x \equiv y \pmod{\mathfrak{b}}$. Then multiplication in K induces a multiplication in $(1+\mathfrak{a})/(1+\mathfrak{b})$ which makes this set into an Abelian group.*

Proof. It is clear that $\mathcal{R}$ is an equivalence relation. Since $\mathfrak{a}$ is an ideal, $1+\mathfrak{a}$ is stable by multiplication, and since $\mathfrak{b}$ is an ideal, $\mathcal{R}$ is compatible with multiplication. Thus $(1+\mathfrak{a})/(1+\mathfrak{b})$ has a natural commutative multiplication and the class of 1 is the unit element. We only need to show that any element has an inverse. But if $x \in \mathfrak{a}$, then by assumption $x^k \in \mathfrak{b}$. It follows that for any $x \in \mathfrak{a}$ we have

$$(1+x)\left(1 + \sum_{i=1}^{k-1} (-1)^i x^i\right) = 1 + (-1)^{k-1} x^k \ ,$$

hence, if we set $y = \sum_{i=1}^{k-1} (-1)^i x^i$, then $y \in \mathfrak{a}$ and $(1+x)(1+y) - 1 \in \mathfrak{b}$ so the class of $1+y$ is an inverse of the class of $1+x$. Thus $(1+\mathfrak{a})/(1+\mathfrak{b})$ is in a natural way an Abelian group.

Note that it is not difficult to prove that this group is also finite. This will in fact follow from the results proven in the rest of this section. □

Proposition 1.4. *Let $\mathfrak{p}$ be a prime ideal of degree f, and let $q = p^f = |\mathbb{Z}_K/\mathfrak{p}|$. Set $G = (\mathbb{Z}_K/\mathfrak{p}^k)^*$. Let*

$$W = \{x \in G \mid x^{q-1} = 1\} \quad \text{and} \quad G_{\mathfrak{p}} = (1+\mathfrak{p})/(1+\mathfrak{p}^k) \ .$$

Then

(1) $W \simeq (\mathbb{Z}_K/\mathfrak{p})^*$, *and in particular* W *is a cyclic subgroup of order* $q-1$ *of* G. *More precisely, if* $\overline{g_0}$ *is a generator of* $(\mathbb{Z}_K/\mathfrak{p})^*$, *then* $\lceil \log_2(k) \rceil$ *iterations of* $g \leftarrow g - (g^{q-1}-1)/((q-1)g^{q-2}) \bmod \mathfrak{p}^k$ *applied to* g_0 *gives a generator of* W.

(2) $G_{\mathfrak{p}}$ *is a* p*-subgroup of* G *of order* q^{k-1}.

(3) $G = W \times G_{\mathfrak{p}}$.

We leave the (easy) proof to the reader.

Finding a generator $\overline{g_0}$ of the finite field $(\mathbb{Z}_K/\mathfrak{p})^*$ is easily done if $q-1$ is completely factored, simply by trying random elements. Since the probability of finding a generator is $\phi(q-1)/(q-1)$ (where ϕ is Euler's function), this is close enough to 1 in general, so g_0 will be found rapidly.

On the other hand, the converse problem which we also need to solve, of computing discrete logarithms in $(\mathbb{Z}_K/\mathfrak{p})^*$, is a famous difficult problem for which there exists a vast literature. Note, however, that in the context of number fields, q will not be too large in general, hence rather simple-minded techniques such as Shanks's baby-step giant-step method can be used. However, if we deal with inert primes of the order of a few thousands in number fields of degree 20 (this is a reasonable proposition with today's capabilities), then q will have of the order of 70 decimal digits, and the problem starts to become extremely difficult. In this paper, we assume that we deal with numbers of reasonable size.

Once g_0 is found, doing the Hensel iterations explained in Proposition 1.4 (1) is easy. Similarly, once one knows how to compute discrete logarithms in $(\mathbb{Z}_K/\mathfrak{p})^*$, lifting them to W is also easy. In fact, as we will see we do not even need to perform these Hensel liftings.

So the task that remains before us is the computation of the group $G_{\mathfrak{p}} = (1+\mathfrak{p})/(1+\mathfrak{p}^k)$.

An idea that immediately comes to mind is the use of $\mathfrak{p}$-adic logarithms. When the ramification index e of $\mathfrak{p}$ is not too large (more precisely when $e < p-1$), then the $\mathfrak{p}$-adic logarithm series induces an explicit isomorphism between $G_{\mathfrak{p}}$ and the additive group $\mathfrak{p}/\mathfrak{p}^k$, and computing this last group is straightforward. Although simple, this method cannot be applied in all cases, hence we prefer to use the more complicated but general method based on the following ideas.

Proposition 1.5. (1) *Let* $a \le b \le c$ *be integers. We have the exact sequence*

$$1 \longrightarrow (1+\mathfrak{p}^b)/(1+\mathfrak{p}^c) \longrightarrow (1+\mathfrak{p}^a)/(1+\mathfrak{p}^c) \longrightarrow (1+\mathfrak{p}^a)/(1+\mathfrak{p}^b) \longrightarrow 1 \ .$$

(2) *Assume that* $b \le 2a$. *Then the map from the multiplicative group* $(1+\mathfrak{p}^a)/(1+\mathfrak{p}^b)$ *to the additive group* $\mathfrak{p}^a/\mathfrak{p}^b$ *which sends the class of* $1+x$ *modulo* $1+\mathfrak{p}^b$ *to the class of* x *modulo* $\mathfrak{p}^b$ *is well defined and is a group isomorphism.*

Proof. Trivial and left to the reader. Note that in (2) the condition $b \le 2a$ is only needed for the map to be a group homomorphism, otherwise the map is always well defined and is a bijection between the two sets. □

Using this proposition and Proposition 1.2, we will compute successively $(1+\mathfrak{p})/(1+\mathfrak{p}^2)$, $(1+\mathfrak{p})/(1+\mathfrak{p}^4)$, and finally $G_{\mathfrak{p}} = (1+\mathfrak{p})/(1+\mathfrak{p}^k)$.

Thus, the principal steps in the computation of the group $G_{\mathfrak{p}}$ are the following:

Step 1. Computation of $(1+\mathfrak{p}^a)/(1+\mathfrak{p}^b)$ for $a \le b \le 2a$. Using Proposition 1.5 (2), we only need to compute $\mathfrak{p}^a/\mathfrak{p}^b$ and the simplest way is probably as follows. Let $\mathfrak{p} = p\mathbb{Z}_K + \pi\mathbb{Z}_K$ be a two-element representation of $\mathfrak{p}$, where we may assume π chosen so that $v_{\mathfrak{p}}(\pi) = 1$ (if this is not the case, then $v_{\mathfrak{p}}(p) = 1$, i.e. $\mathfrak{p}$ is unramified, and hence we replace π by $\pi + p$).

Then for all m, if $q = \lceil m/e \rceil = \lfloor (m+e-1)/e \rfloor$ where $e = e(\mathfrak{p}/p)$ is the ramification index of $\mathfrak{p}$, we have $\mathfrak{p}^m = p^q\mathbb{Z}_K + \pi^m\mathbb{Z}_K$. Indeed, for any prime ideal $\mathfrak{q}$ different from $\mathfrak{p}$, $\min(v_{\mathfrak{q}}(p), v_{\mathfrak{q}}(\pi)) = 0$, hence $v_{\mathfrak{q}}(p^q\mathbb{Z}_K + \pi^m\mathbb{Z}_K) = 0$, while $v_{\mathfrak{p}}(p^q\mathbb{Z}_K + \pi^m\mathbb{Z}_K) = \min(qv_{\mathfrak{p}}(p), mv_{\mathfrak{p}}(\pi)) = \min(qe, m) = m$.

From this, it is easy to compute the Hermite normal form of $\mathfrak{p}^m$ on some fixed integral basis of $\mathbb{Z}_K$: construct the $n \times 2n$ matrix obtained by concatenating p^q times the identity matrix with the $n \times n$ matrix giving the endomorphism multiplication by π^m on the integral basis, and then apply a Hermite normal form algorithm to obtain the desired HNF.

Let A and B be the HNF matrices of $\mathfrak{p}^a$ and $\mathfrak{p}^b$ obtained as above. The columns of A (resp. B) give on the chosen integral basis a $\mathbb{Z}$-basis (α_i) of the ideal $\mathfrak{p}^a$ (resp. (β_i) of $\mathfrak{p}^b$). Since $a \le b$, we have $\mathfrak{p}^b \subset \mathfrak{p}^a$, hence the matrix $A^{-1}B$ which expresses the β_i in terms of the α_i has integer coefficients. If we apply the Smith normal form algorithm to this matrix, we will find unimodular matrices U and V such that $UA^{-1}BV = D_C$ is a diagonal matrix in Smith normal form. If (c_i) are the diagonal entries of D_C and if we set $C = AU^{-1}$, then the columns of C give the coordinates on the chosen integral basis of elements $\gamma_i \in \mathfrak{p}^a$, and we have $\mathfrak{p}^a/\mathfrak{p}^b = \bigoplus(\mathbb{Z}/c_i\mathbb{Z})\overline{\gamma_i}$, where $\overline{\gamma}$ denotes the class of γ modulo $\mathfrak{p}^b$. Because we also have $b \le 2a$, it follows from Proposition 1.5 (2) that

$$(1+\mathfrak{p}^a)/(1+\mathfrak{p}^b) = \bigoplus(\mathbb{Z}/c_i\mathbb{Z})\overline{(1+\gamma_i)} \ .$$

The matrix $U_a = UA^{-1}$ is now used to solve the discrete logarithm problem in this group. Indeed, since $a \le 2b$, Proposition 1.5 tells us that

$$\prod(1+\gamma_{a,i})^{x_i} \equiv 1 + \sum x_i\gamma_{a,i} \pmod{1+\mathfrak{p}^b} \ .$$

Hence if $\overline{\beta} \in (1+\mathfrak{p}^a)/(1+\mathfrak{p}^b)$, we want to solve $\sum x_i\gamma_{a,i} = \beta - 1$, or in matrix terms on the integral basis, $AU^{-1}X = B - 1_K$, where B is the column vector representing β on the integral basis, and 1_K is the column vector representing 1 (i.e. $(1,0,\dots,0)^t$ since we choose an integral basis starting with 1). It follows that $X = UA^{-1}(B - 1_K) = U_a(B - 1_K)$ is the desired discrete logarithm.

Step 2. Computation of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$. Let k be a positive integer. To compute integers d_i and elements δ_i of $\mathbb{Z}_K$ such that $(\mathbb{Z}_K/\mathfrak{p}^k)^* = \bigoplus(\mathbb{Z}/d_i\mathbb{Z})\overline{\delta_i}$ with $d_{i+1} \mid d_i$, we use Step 1 to compute $(1+\mathfrak{p})/(1+\mathfrak{p}^2)$, $(1+\mathfrak{p}^2)/(1+\mathfrak{p}^4)$, $\dots$, $(1+\mathfrak{p}^{2^{m-1}})/(1+\mathfrak{p}^{2^m})$, $(1+\mathfrak{p}^{2^m})/(1+\mathfrak{p}^k)$, where $m = \lfloor \log_2(k-1) \rfloor$. Then using inductively Proposition 1.5 (1) and Proposition 1.2, we obtain successively the structure of $(1+\mathfrak{p})/(1+\mathfrak{p}^2)$, $(1+\mathfrak{p})/(1+\mathfrak{p}^4)$, $\dots$, $(1+\mathfrak{p})/(1+\mathfrak{p}^{2^m})$, $G_{\mathfrak{p}} = (1+\mathfrak{p})/(1+\mathfrak{p}^k)$. Using Proposition 1.4, this gives the structure of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ and also allows us to solve the discrete logarithm problem in $(\mathbb{Z}_K/\mathfrak{p}^k)^*$.

Step 3. Computation of $(\mathbb{Z}_K/\mathfrak{m})^*$. Using Lemma 1.1 recursively on the prime ideal factorization $\mathfrak{m}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m}_0)}$, we obtain the structure of $(\mathbb{Z}_K/\mathfrak{m}_0)^*$, and hence of $(\mathbb{Z}_K/\mathfrak{m})^* = (\mathbb{Z}_K/\mathfrak{m}_0)^* \times \mathbb{F}_2^{\mathfrak{m}_\infty}$.

This concludes the sketch of the algorithm for computing the structure of $(\mathbb{Z}_K/\mathfrak{m})^*$.

It will also be useful to compute discrete logarithms for elements of K^* coprime to $\mathfrak{m}$ which are not necessarily in $\mathbb{Z}_K$. For this, we do the following: Let $\mathfrak{a}$ be a given nonzero integral ideal and an element β of K^* coprime to $\mathfrak{a}$. We assume β given by its components on an integral basis of K and let d be the lowest common multiple of the denominators of the components of β. We assume that $d > 1$, otherwise $\beta \in \mathbb{Z}_K$ and it suffices to use the usual discrete logarithm. Then let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p}}}$ be the prime ideal decomposition of $\mathfrak{a}$. Denote by $e(\mathfrak{p})$ the ramification index of $\mathfrak{p}$. Compute $k \leftarrow \sup_{\mathfrak{p}} \lfloor v_p(d)e(\mathfrak{p})/k_{\mathfrak{p}} \rfloor + 1$, where $v_p(d)$ denotes the ordinary exponent of p in d, where p is the prime number below $\mathfrak{p}$. Using standard ideal operations (cf. [Coh2]), compute the ideal $\mathfrak{d} = d\mathbb{Z}_K + \mathfrak{a}^k$ and the inverse ideal $\mathfrak{d}^{-1}$. Because $d\mathfrak{d}^{-1}$ and $\mathfrak{a}\mathfrak{d}^{-1}$ are coprime integral ideals, we use Lemma 1.1 to compute a and c such that $a \in d\mathfrak{d}^{-1}$, $c \in \mathfrak{a}\mathfrak{d}^{-1}$ and $a + c = 1$. Then a and $a\beta$ are coprime to $\mathfrak{a}$. Now we can compute discrete logarithms for a and $a\beta$ and deduce the discrete logarithm of β.

2. Computing ray class groups

Let $\mathfrak{m}$ be a modulus. Recall the exact sequence

$$U(K) \longrightarrow (\mathbb{Z}_K/\mathfrak{m})^* \longrightarrow Cl_{\mathfrak{m}} \longrightarrow Cl(K) \longrightarrow 1 \ ,$$

where $U(K)$ denotes the unit group of K, $Cl(K)$ the ordinary class group of K, and $Cl_{\mathfrak{m}} = I_{\mathfrak{m}}/P_{\mathfrak{m}}$ the ray class group corresponding to the modulus $\mathfrak{m}$, i.e. the quotient of the group $I_{\mathfrak{m}}$ of nonzero fractional ideals of K coprime to $\mathfrak{m}$ by the subgroup $P_{\mathfrak{m}}$ of principal fractional ideals generated by an element α congruent to 1 mod $^*\mathfrak{m}$. As before, the groups $Cl(K)$ and $U(K)$ must be known by a system of generators and their matrix of relations in SNF. This can be done using either the techniques of [Po-Za] or of [Coh]. Note that [Coh] assumes the GRH, but in fact in practical situations it is rather easy to remove the GRH condition by *certifying* the result unconditionally. We refer to [Zan] and [Di-Ol] for details. Note also that we need to solve the discrete logarithm problem in $Cl(K)$ (in $U(K)$ the problem is ordinary linear algebra). The solution to this is also given in [Coh], where in fact even more information is obtained as part of the *principal ideal problem*: if an ideal is principal, the algorithm also gives a generator. More precisely, if g_i are ideals such that $\overline{g_i}$ are the given generators of $Cl(K)$, then if g is an ideal of K, we can find (v_i) such that $\overline{g} = \prod_i \overline{g_i}^{v_i}$, but the same algorithm gives also $\alpha \in K$ such that $g = \alpha \prod_i g_i^{v_i}$. We will also do this in the context of ray class groups.

The group $(\mathbb{Z}_K/\mathfrak{m})^*$ has been extensively dealt with in §1.

Two remarks on the maps in the above exact sequence above. First, let ψ be the map from $(\mathbb{Z}_K/\mathfrak{m})^*$ to $Cl_{\mathfrak{m}}$. If $\overline{g} \in Cl_{\mathfrak{m}}$ is known to be of the form $\psi(\overline{\alpha})$, we can find $\alpha \in \mathbb{Z}_K$ because in that case g is an ideal of K coprime to $\mathfrak{m}$ which is a principal ideal in the ordinary sense. Thus, by using the solution to the principal ideal problem mentioned above, we can algorithmically find α such that $g = \alpha\mathbb{Z}_K$, and α will be coprime to $\mathfrak{m}$. Using the method described at the end of §1 we can find β and γ such that $\alpha = \beta/\gamma$ with β and γ integral and coprime to $\mathfrak{m}$, hence we can take $\overline{\alpha} = \overline{\beta}/\overline{\gamma}$ in $(\mathbb{Z}_K/\mathfrak{m})^*$.

Second, let ϕ be the map from $Cl_{\mathfrak{m}}$ to $Cl(K)$. Then, if $\overline{g} \in Cl(K) = \mathrm{Im}(\phi)$, we can find an ideal g' coprime to $\mathfrak{m}$ such that $\phi(\overline{g'}) = \overline{g}$. This follows from the following lemma, whose theoretical version is well known.

Lemma 2.1. *Given a fractional ideal g of K and a modulus $\mathfrak{m}$, we can algorithmically find $\alpha \in K^*$ such that αg is an integral ideal coprime to $\mathfrak{m}$.*

We refer to [Coh2] for one method of doing this using the approximation theorem in Dedekind domains, but also mention that a generalization of the *factor refinement* method is better (cf. [B-D-S]).

We now sketch the computation of the ray class group $Cl_{\mathfrak{m}}$ in the usual form $Cl_{\mathfrak{m}} = (\overline{B}, D_B)$ where $\overline{B}$ is a vector of ideal classes $\overline{b_i}$ generating $Cl_{\mathfrak{m}}$ (these classes are represented by ideals b_i, coprime to $\mathfrak{m}$).

We assume already computed $U(K) = (E, D_E)$ with $E = (\epsilon_i)$, $Cl(K) = (C, D_C)$ with $C = (\gamma_i) = (\overline{g_i})$ (by [Po-Za] or [Coh]) and $(\mathbb{Z}_K/\mathfrak{m})^* = (Z, D_Z)$ with $Z = (\zeta_i)$. We denote by ψ the map from $(Z_K/\mathfrak{m})^*$ to $Cl_{\mathfrak{m}}$.

Using the approximation theorem or factor refinement, for each i compute $\alpha_i' \in K^*$ such that $g_i' = \alpha_i' g_i$ is an integral ideal coprime to $\mathfrak{m}$. Let G' be the row vector of the $\overline{g_i'}$, and A' the row vector of the α_i'. The vector A' will be used later to solve the principal ideal problem in ray class groups.

For each ideal g_i, compute $g_i^{c_i}$ (where c_i is the i-th diagonal entry of D_C), and using the solution to the principal ideal problem (see [Coh]), find $\alpha_i \in \mathbb{Z}_K$ such that $g_i^{c_i} = \alpha_i \mathbb{Z}_K$. Here the ${\alpha_i'}^{c_i}\alpha_i$ are elements of $\mathbb{Z}_K$ coprime to $\mathfrak{m}$. Compute the matrix P whose columns are the discrete logarithms of the ${\alpha_i'}^{c_i}\alpha_i$ with respect to the ζ_i and the matrix Q whose columns are the discrete logarithms of the ϵ_i with respect to the ζ_i. Let $B' = (G'|\psi(Z))$ and $H = \begin{pmatrix} D_C & 0 & 0 \\ -P & Q & D_Z \end{pmatrix}$. The reduction of the system of generators and relations (B', H), gives $(\overline{B}, D_B)$ the SNF of $Cl_{\mathfrak{m}}$, unimodular transformation matrices U and V such that $D_B = UHV$ and $\overline{B} = B'U^{-1}$, and thus the structure of $Cl_{\mathfrak{m}}$.

For the corresponding discrete logarithm problem, as in the case of $Cl(K)$ itself, we will in fact solve a stronger problem, the principal ideal problem in ray class groups. Given a fractional ideal h coprime to $\mathfrak{m}$, we compute a solution to the principal ideal problem in $Cl(K)$, in other words we find a column vector W and $\gamma \in K$ such that $h = \gamma G W$ (where G is the row vector of the ideals g_i whose classes are the given generators of $Cl(K)$). Set $\alpha = \gamma/A'W$ (α will be coprime to $\mathfrak{m}$). Using the discrete logarithm algorithm in $(\mathbb{Z}_K/\mathfrak{m})^*$, we compute Y such that $\alpha \equiv ZY \pmod{{}^*\mathfrak{m}}$, and let $\alpha' = ZY$ as an element of $(\mathbb{Z}_K/\mathfrak{m})^*$.

Let $R = \binom{W}{Y}$, the vertical concatenation of the the column vectors W and Y. If U is the unimodular matrix considered above, $L = UR$ is the vector of exponents of the class represented by h in $Cl_{\mathfrak{m}}$ and the element $\beta = \alpha/\alpha'$ is such that $h = \beta H L$ and $\beta \equiv 1 \pmod{{}^*\mathfrak{m}}$.

This finally terminates the algorithmic computation of the ray class group $Cl_{\mathfrak{m}}$ and of the corresponding discrete logarithm problem.

It should be emphasized that the main bottlenecks will be in two places. First, in the computation of discrete logarithms in $(\mathbb{Z}_K/\mathfrak{p})^*$. For this, considering the vast amount of effort which has been spent on the problem, we have nothing more to say.

The second bottleneck will be the size of the generators. Indeed, several times we have to multiply a given set of generators by a unimodular matrix, or multiply

generators by elements to make them coprime to certain ideals. All this makes the coefficients of the generators grow in size. Since this can rapidly make the algorithms completely useless in practice, we should like to give a few brief indications on how to get down to generators of manageable size.

The main place where size reduction is necessary is in the SNF algorithm for Abelian groups. In that algorithm, a set of generators and relations (G, M) is given, and after reducing M to its HNF, which is a harmless process, we use the SNF algorithm to compute unimodular matrices U and V such that $H = UDV$ (and afterwards we remove trivial components). The main problem comes from the fact that the new generators are given essentially by GU^{-1}, and these may be large objects if U^{-1} has large coefficients.

There are several complementary ways to improve this situation, and all should be applied.

(1) The matrix U^{-1} is not unique in general, hence it is worthwhile to find a small such matrix. This can be done using the techniques of [Ha-Ma].

However, in most cases, this just cannot be done, and all possible matrices U^{-1} have large coefficients.

(2) Another idea is to observe that $GM = \mathbf{1}$ in the Abelian group, hence if we add to the columns of U^{-1} any $\mathbb{Z}$-linear combination of the columns of M (or of H), the resulting generators GU^{-1} are unchanged. For doing this reduction, the simplest is probably as follows. Let X be a column vector that we want to reduce modulo the columns of H. Compute first the matrix L obtained from H by applying the LLL algorithm to the columns of H. Then replace X by $X - L\lfloor L^{-1}X \rceil$, where $\lfloor A \rceil$ denotes the result of rounding each entry of a matrix to the nearest integer. This should now be rather small.

(3) We should try to avoid divisions as much as possible. For this, instead of computing a product of the form $\prod_i g_i^{u_i}$ in the naive way, we write

$$\prod_i g_i^{u_i} = \prod_{i,\, u_i>0} g_i^{u_i} / \prod_{i,\, u_i<0} g_i^{-u_i}$$

so that we need to perform only one division. Note that division is in general an expensive operation.

(4) In the (very frequent) case where the group consists of classes of elements of a set modulo some equivalence relation, the elements of the group are usually given by the classes of some representatives, but the latter should be chosen with care. In other words, one should try to reduce modulo the equivalence relation as much as possible.

Let us look in detail at the two cases of importance to us, that of $(\mathbb{Z}_K/\mathfrak{m})^*$ and that of $Cl_{\mathfrak{m}}$.

(4.1) Recall that elements of $(\mathbb{Z}_K/\mathfrak{m})^*$ are represented by pairs $(\overline{\alpha}, v)$ with $\alpha \in \mathbb{Z}_K$ coprime to $\mathfrak{m}_0$ and $v \in \mathbb{F}_2^{\mathfrak{m}_\infty}$. To reduce such a pair, we consider α represented by a column vector X on a fixed integral basis. As in (2), we compute an LLL-reduced basis L of the ideal $\mathfrak{m}_0$, and set $Y \leftarrow X - L\lfloor L^{-1}X \rceil$. This will be a reasonably small vector giving an element β congruent to α modulo $\mathfrak{m}_0$. We can then replace $(\overline{\alpha}, v)$ by $(\overline{\beta}, v)$. This is where the two-element representation is the most useful since we do not have to worry about the signature of β.

(4.2) To reduce an ideal modulo $\mathfrak{m}$ (so that we stay in the same ideal class in $Cl_{\mathfrak{m}}$), we proceed as follows. First, exactly as in the case of $(\mathbb{Z}_K/\mathfrak{m})^*$, instead of representing ideal classes as such, i.e. as classes of ideals coprime to $\mathfrak{m}_0$ modulo

$P_{\mathfrak{m}}$, we will represent them as pairs $(\mathfrak{a}, v)$ where $\mathfrak{a} \in I_{\mathfrak{m}_0}$ is an ideal coprime to $\mathfrak{m}_0$ and $v \in \mathbb{F}_2^{\mathfrak{m}_\infty}$ as usual. The equivalence relation $\mathcal{R}$ on these pairs is defined by $(\mathfrak{a}', v')\mathcal{R}(\mathfrak{a}, v)$ if and only if there exists $\beta \equiv 1 \pmod{{}^*\mathfrak{m}_0}$ such that $v' = v + s(\beta)$. As in the case of $(\mathbb{Z}_K/\mathfrak{m})^*$ this representation will avoid annoying problems due to signatures.

3. Computations in global class field theory

3.1. Algorithmic description of congruence groups. Congruence groups are subgroups of $I_{\mathfrak{m}}$ containing $P_{\mathfrak{m}}$. They naturally correspond to subgroups of $Cl_{\mathfrak{m}}$. We assume that $Cl_{\mathfrak{m}}$ has been computed, so that as usual

$$Cl_{\mathfrak{m}} = \bigoplus_{i=1}^{n} (\mathbb{Z}/c_i\mathbb{Z})\overline{\gamma_i} \ .$$

We have the following result.

Proposition 3.1. *Let c_i and γ_i be as above, let D_C be the diagonal matrix of the c_i, and C the row matrix of the $\overline{\gamma_i}$. There is a one to one correspondence between congruence groups modulo $\mathfrak{m}$ and integral matrices A in Hermite normal form satisfying $A^{-1}D_C \in \mathcal{M}_n(\mathbb{Z})$. The correspondence is as follows.*

(1) *If A is such a matrix, we set $C' = CA$ in the multiplicative sense already used in the preceding sections. Then if $C' = (\overline{\gamma_i'})$, the congruence subgroup H associated to A is the subgroup of $I_{\mathfrak{m}}$ generated by the γ_i' and by $P_{\mathfrak{m}}$.*

(2) *Conversely, if H is a congruence subgroup, let $(\overline{\gamma_i'})_{1\le i\le m}$ be a system of generators of $H/P_{\mathfrak{m}}$, and let C' be the row vector of the $\overline{\gamma_i'}$. We can write $C' = CP$ for an $n \times m$ matrix P. Then A is the Hermite normal form of the matrix $(P|D_C)$.*

(3) *Let A be a matrix in HNF, and let H be the corresponding congruence group. Then $|H/P_{\mathfrak{m}}| = |Cl_{\mathfrak{m}}|/\det(A)$ or equivalently, if $\overline{H} = H/P_{\mathfrak{m}}$, then*

$$h_{\mathfrak{m},H} = |Cl_{\mathfrak{m}}/\overline{H}| = |I_{\mathfrak{m}}/H| = \det(A) \ .$$

Proof. We have $Cl_{\mathfrak{m}} \simeq \mathbb{Z}^n/\Lambda$, where Λ is the lattice $\Lambda = \bigoplus c_i\mathbb{Z}$, so that a $\mathbb{Z}$-basis of Λ is $(c_i\epsilon_i)_{1\le i\le n}$, where the ϵ_i are the canonical basis elements of $\mathbb{Z}^n$. The isomorphism is given explicitly by sending the i-th generator $\overline{\gamma_i}$ of $Cl_{\mathfrak{m}}$ on ϵ_i. Subgroups of $\mathbb{Z}^n/\Lambda$ are of the form Λ'/Λ, where Λ' is a lattice such that $\Lambda \subset \Lambda' \subset \mathbb{Z}^n$. Such a lattice Λ' can be defined in a unique way by a matrix A in Hermite normal form so that the columns of this matrix express a $\mathbb{Z}$-basis of Λ' on the ϵ_i. The condition $\Lambda' \subset \mathbb{Z}^n$ means that A has integer entries, and the condition $\Lambda \subset \Lambda'$ means that $A^{-1}D_C$ also has integer entries, since it is the matrix which expresses the given basis of Λ in terms of that of Λ'. In terms of generators, this correspondence translates into the equality $C' = CA$ of (1).

For (2), we remark that $CD_C = \mathbf{1}$, hence if $C'' = C(P|D_C)$ we have simply added some 1's to the generators of $H/P_{\mathfrak{m}}$. Thus, the group can be defined by the matrix of maximal rank $(P|D_C)$, hence also by the Hermite normal form A of this matrix.

For (3), we know that $A^{-1}D_C$ expresses a basis of Λ in terms of a basis of Λ', hence

$$|H/P_{\mathfrak{m}}| = |\Lambda'/\Lambda| = \det(A^{-1}D_C) = |Cl_{\mathfrak{m}}|/\det(A). \quad \square$$

Thus, finding all congruence groups modulo $\mathfrak{m}$ is equivalent to finding integral HNF matrices A such that $A^{-1}D_C$ also has integer entries. There exist only a finite number of such matrices A, in fact exactly the number of subgroups of $Cl_{\mathfrak{m}}$ or equivalently of $\bigoplus(\mathbb{Z}/c_i\mathbb{Z})$. It is natural to call these matrices the *left divisors* of the matrix D_C.

The question of finding these divisors in an efficient manner does not seem to be easy. However, by the Cohen-Lenstra heuristics generalized to this case, it seems reasonable to assume that $Cl_{\mathfrak{m}}$ will often be cyclic or close to cyclic. Hence, we can proceed as follows. Let n be the number of cyclic components of $Cl_{\mathfrak{m}}$ as above.

If $n = 1$, A divides D_C if and only if $A = (e_1)$ where $e_1 \mid c_1$ and $e_1 \geq 1$, hence we simply look at all (positive) divisors of c_1.

If $n = 2$, then an immediate computation shows that $A = \begin{pmatrix} e_1 & f_1 \\ 0 & e_2 \end{pmatrix}$ divides D_C if and only if for $i = 1$ and $i = 2$, e_i is a positive divisor of c_i, and $f_1 = ke_1/\gcd(e_1, c_2/e_2)$ with $0 \leq k < \gcd(e_1, c_2/e_2)$.

If $n = 3$, we can write an explicit but much more complicated recipe for the coefficients of A, but for general n, it does not seem to be possible. Thus for $n \geq 3$, there does not seem to be any better solution than to try all possible HNF matrices $A = (a_{i,j})$ with $a_{i,i} \mid c_i$ and

$$a_{i,i+1} \equiv 0 \pmod{a_{i,i}/\gcd(a_{i,i}, c_{i+1}/a_{i+1,i+1})} ,$$

which are easily seen to be necessary conditions.

Finally, we consider the question of computing the *image* of a subgroup of $Cl_{\mathfrak{m}}$ by a surjective group homomorphism. The following proposition, given in an abstract situation which does not necessarily refer to ray class groups, answers this question immediately.

Proposition 3.2. *Let $\mathcal{B} = (B, D_B)$ and $\mathcal{C} = (C, D_C)$ be two finite Abelian groups written in Smith normal form, let ϕ be a group homomorphism from $\mathcal{B}$ to $\mathcal{C}$, let H be a subgroup of $\mathcal{B}$ defined by an HNF matrix A_B dividing D_B, and finally, let P be a matrix such that $\phi(B) = CP$ computed using the solution to the discrete logarithm problem in $\mathcal{C}$. Then the Hermite normal form A_C of the matrix $(PA_B|D_C)$ divides D_C and defines the subgroup $\phi(H)$ of $\mathcal{C}$.*

Proof. The generators of H are by definition the entries of BA_B. Hence the generators of $\phi(H)$ are the entries of $\phi(B)A_B = CPA_B$. Since $CD_C = \mathbf{1}$, it follows that the entries of $C(PA_B|D_C)$ also generate $\phi(H)$. But the advantage of this last matrix is that it is of maximal rank (since D_C is), hence if A_C is its HNF, then CA_C generates $\phi(H)$ and A_C is an integral matrix in HNF. Furthermore, since it is obtained as the "matrix GCD" of PA_B and D_C, it divides D_C. Explicitly, let U be the unimodular matrix such that $(PA_B|D_C)U = (0|A_C)$. Write in block matrix form, $U^{-1} = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix}$. Then $(PA_B|D_C) = (0|A_C)U^{-1}$ from which it follows in particular that $A_CU_4 = D_C$, hence $A_C^{-1}D_C = U_4$ has indeed integral coefficients. □

3.2. Computing discriminants, signatures and conductors. Let us now come back to the ray class field situation. Let K be a number field (our base field), let $\mathfrak{m}$ be a modulus, $Cl_{\mathfrak{m}}$ the ray class group, and N the ray class field corresponding to $Cl_{\mathfrak{m}}$. In particular, we have $\mathrm{Gal}(N/K) \simeq Cl_{\mathfrak{m}}$.

For any congruence group H modulo $\mathfrak{m}$, denote by $\overline{H} = H/P_{\mathfrak{m}}$ the subgroup of $Cl_{\mathfrak{m}}$ corresponding to H. We will often identify H and $\overline{H}$.

By Galois theory, subfields L of N are in one to one correspondence with congruence groups H modulo $\mathfrak{m}$ by the maps $H \mapsto L = N^{\overline{H}}$ and $L \mapsto \mathrm{Gal}(N/L)$. We also have $\mathrm{Gal}(L/K) \simeq Cl_{\mathfrak{m}}/\overline{H}$.

Our goal in this section is to compute the signature, relative discriminant and conductor of these subfields L. The result is as follows.

Theorem 3.3. *Set $n = [K : \mathbb{Q}]$, let (r_1, r_2) be the signature of K, so that $r_1 + 2r_2 = n$, and let $d_{K/\mathbb{Q}}$ be its discriminant. For any modulus $\mathfrak{n}$ dividing $\mathfrak{m}$, denote by $s_{\mathfrak{n}}$ the canonical surjection from $Cl_{\mathfrak{m}}$ to $Cl_{\mathfrak{n}}$, and set*

$$h_{\mathfrak{n},H} = |Cl_{\mathfrak{n}}/s_{\mathfrak{n}}(\overline{H})| \ .$$

Let $\mathfrak{m} = \prod_i \mathfrak{p}_i^{e_i}\mathfrak{m}_\infty$ be the prime decomposition of $\mathfrak{m}$.

Then, if L is the extension of K corresponding to the congruence group $(\mathfrak{m}, H)$, we have the following results.

(1) *Let $\delta_{L/K}$ be the relative discriminant of L/K. Then:*

$$\delta_{L/K} = \prod_i \mathfrak{p}_i^{e_i h_{\mathfrak{m},H} - \sum_{1 \le k \le e_i} h_{\mathfrak{m}/\mathfrak{p}_i^k,H}} \ .$$

(Recall also that we have $|d_{L/\mathbb{Q}}| = \mathcal{N}_{K/\mathbb{Q}}(\delta_{L/K})|d_{K/\mathbb{Q}}|^{h_{\mathfrak{m},H}}$.)

(2) *The modulus $\mathfrak{m}$ is the conductor of L if and only if $h_{\mathfrak{m}/\mathfrak{p},H} < h_{\mathfrak{m},H}$ for all $\mathfrak{p} \mid \mathfrak{m}$, including the places at infinity.*

(3) *Let (R_1, R_2) be the signature of L, so that $R_1 + 2R_2 = [L : \mathbb{Q}] = n \cdot h_{\mathfrak{m},H}$. Then we have*

$$R_1 = h_{\mathfrak{m},H}\left(r_1 - |\mathfrak{m}_\infty| + \sum_{v \in \mathfrak{m}_\infty} \delta(h_{\mathfrak{m},H} - h_{\mathfrak{m}/v,H})\right) \ ,$$

where $\delta(x) = 1$ if $x = 0$ and $\delta(x) = 0$ otherwise.

Proof. For (1), we know that

$$\delta_{L/K} = \prod_\chi \mathcal{F}(\chi) \ ,$$

where χ runs through all the characters of $Cl_{\mathfrak{m}}/\overline{H}$ and $\mathcal{F}(\chi)$ is the conductor of χ.

For each $\mathfrak{n} \mid \mathfrak{m}$, denote by $f(\mathfrak{n})$ the number of characters of $Cl_{\mathfrak{m}}/\overline{H}$ of conductor exactly equal to $\mathfrak{n}$. Then since the total number of characters is equal to the order of the group, we have the equation

$$\sum_{\mathfrak{n}|\mathfrak{m}} f(\mathfrak{n}) = |Cl_{\mathfrak{m}}/\overline{H}| = h_{\mathfrak{m},H} \ .$$

By Möbius inversion, it follows that

$$f(\mathfrak{n}) = \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}/\mathfrak{n}) h_{n,H} \ ,$$

where $\mu(\mathfrak{n})$ is defined as in the case of ordinary integers (all this is valid since a modulus can be written as a product of finite or infinite primes in essentially only one way).

Thus, we have

$$\delta_{L/K} = \prod_{\mathfrak{n}|\mathfrak{m}} \prod_{\mathcal{F}(\chi)=\mathfrak{n}} \mathcal{F}(\chi) = \prod_{\mathfrak{n}|\mathfrak{m}} \mathfrak{n}^{f(\mathfrak{n})} = \prod_{\mathfrak{n}|\mathfrak{m}} \mathfrak{n}^{\sum_{\mathfrak{d}|\mathfrak{n}} \mu(\mathfrak{n}/\mathfrak{d}) h_{\mathfrak{d},H}}$$

$$= \prod_{\mathfrak{d}|\mathfrak{m}} \left(\prod_{\mathfrak{c}|(\mathfrak{m}/\mathfrak{d})} (\mathfrak{c}\mathfrak{d})^{\mu(\mathfrak{c})} \right)^{h_{\mathfrak{d},H}} = \prod_{\mathfrak{d}|\mathfrak{m}} (p_1(\mathfrak{d}) p_2(\mathfrak{d}))^{h_{\mathfrak{d},H}} ,$$

where

$$p_1(\mathfrak{d}) = \prod_{\mathfrak{c}|(\mathfrak{m}/\mathfrak{d})} \mathfrak{c}^{\mu(\mathfrak{c})} \quad \text{and} \quad p_2(\mathfrak{d}) = \prod_{\mathfrak{c}|(\mathfrak{m}/\mathfrak{d})} \mathfrak{d}^{\mu(\mathfrak{c})} .$$

The product $p_2(\mathfrak{d})$ is trivial to compute: we have

$$p_2(\mathfrak{d}) = \mathfrak{d}^{\sum_{\mathfrak{c}|(\mathfrak{m}/\mathfrak{d})} \mu(\mathfrak{c})} ,$$

and by definition of the μ function, this exponent is equal to zero unless $\mathfrak{m}/\mathfrak{d} = 1$. Hence $p_2(\mathfrak{d}) = 1$ if $\mathfrak{d} \neq \mathfrak{m}$, and $p_2(\mathfrak{m}) = \mathfrak{m}$.

The product $p_1(\mathfrak{d})$ can be treated as follows. Set $L(\mathfrak{c}) = \mathfrak{p}$ if $\mathfrak{c} = \mathfrak{p}^k$ is a nontrivial prime power (finite or infinite), $L(\mathfrak{c}) = 1$ otherwise. Then $\prod_{\mathfrak{c}|\mathfrak{n}} L(\mathfrak{c}) = \mathfrak{n}$ is a formal equality which only expresses the existence and uniqueness of the decomposition of $\mathfrak{n}$ into prime powers. By multiplicative Möbius inversion, this gives

$$L(\mathfrak{n}) = \prod_{\mathfrak{c}|\mathfrak{n}} (\mathfrak{n}/\mathfrak{c})^{\mu(\mathfrak{c})} = \prod_{\mathfrak{c}|\mathfrak{n}} \mathfrak{n}^{\mu(\mathfrak{c})} / \prod_{\mathfrak{c}|\mathfrak{n}} \mathfrak{c}^{\mu(\mathfrak{c})} .$$

By definition of μ the numerator is equal to 1, hence we obtain the formula

$$\prod_{\mathfrak{c}|\mathfrak{n}} \mathfrak{c}^{\mu(\mathfrak{c})} = 1/L(\mathfrak{n}) .$$

The reader will certainly have recognized that the function $L(\mathfrak{n})$ is the ideal-theoretic analogue of the function $e^{\Lambda(n)}$ of elementary prime number theory.

Replacing in our above formulas, we obtain that $p_1(\mathfrak{d}) = 1/L(\mathfrak{m}/\mathfrak{d})$. Therefore,

$$\delta_{L/K} = \mathfrak{m}^{h_{\mathfrak{m},H}} \prod_{\mathfrak{d}|\mathfrak{m}} L(\mathfrak{m}/\mathfrak{d})^{-h_{\mathfrak{d},H}} = \mathfrak{m}^{h_{\mathfrak{m},H}} \prod_{\mathfrak{p}^k|\mathfrak{m}} \mathfrak{p}^{-h_{\mathfrak{m}/\mathfrak{p}^k,H}}$$

$$= \prod_i \mathfrak{p}_i^{e_i h_{\mathfrak{m},H} - \sum_{1 \leq k \leq e_i} h_{\mathfrak{m}/\mathfrak{p}_i^k,H}} ,$$

thus proving (1).

(2) is simply a restatement of the definition of the conductor of an Abelian extension.

For (3), we note that R_1 will be equal to $[L : K] = h_{\mathfrak{m},H}$ times the number of real places of K unramified in L. By definition of the ray class group, the $r_1 - |\mathfrak{m}_\infty|$ real places not in the modulus $\mathfrak{m}$ must be unramified. Now let $v \in \mathfrak{m}_\infty$. If $h_{\mathfrak{m}/v,H} = h_{\mathfrak{m},H}$, this means that v does not divide the conductor of L, hence that v is unramified in L. On the contrary, if $h_{\mathfrak{m}/v,H} < h_{\mathfrak{m},H}$, then v divides the conductor of L hence v is ramified in L. This gives the formula in (3). □

The explicit computation of relative or absolute discriminants, signatures and conductors, can be done using Proposition 3.2 and Theorem 3.3. To compute the conductor, we recall simply that we replace $\mathfrak{m}$ inductively by $\mathfrak{m}/\mathfrak{p}$ for some

(finite or infinite) place $\mathfrak{p}$ dividing $\mathfrak{m}$, until there does not exist $\mathfrak{p} \mid \mathfrak{m}$ such that $h_{\mathfrak{m}/\mathfrak{p},H} = h_{\mathfrak{m},H}$.

3.3. Conductors of characters. The formulas given above (in particular in Theorem 3.3) have the great advantage that we do not need to compute the conductors of individual characters. In this subsection, we explain how to do this if these conductors are really needed.

As before, let

$$Cl_{\mathfrak{m}}(K) = \bigoplus_{1 \le i \le k} (\mathbb{Z}/c_i\mathbb{Z})\overline{\gamma_i}$$

be the SNF of $Cl_{\mathfrak{m}}(K)$. Denote by ζ_n the specific primitive n-th root of unity $\exp(2i\pi/n)$ and let $\zeta = \zeta_{c_1}$ (recall that c_i divides c_1 for all i). Then a character χ is uniquely defined by a vector $(a_1, \ldots, a_k)$ where $a_i \in \mathbb{Z}/c_i\mathbb{Z}$ so that

$$\chi(\prod_i \overline{\gamma_i}^{x_i}) = \prod_i \zeta_{c_i}^{a_i x_i} = \zeta^{\sum_i (c_1/c_i) a_i x_i} \ .$$

By definition, the conductor of χ is equal to the conductor of the congruence group $H = \mathrm{Ker}(\chi)$. Since this is a congruence group, we can use the above methods to compute its conductor. The only problem is to put this group into an algorithmic form, i.e. to compute the corresponding matrix A associated to H by Proposition 3.1.

We have $\chi(\prod_i \overline{\gamma_i}^{x_i}) = 1$ if and only if there exists an integer y such that

$$\sum_i (c_1/c_i) a_i x_i + c_1 y = 0 \ .$$

This is an instance of the integer kernel problem (see [Coh, §2.4.3]). In the present case, it is solved as follows. Set $b_i = (c_1/c_i)a_i$, and let $B = [b_1, \ldots, b_k, c_1]$ considered as a 1 row matrix. Using the Hermite normal form algorithm, we can compute a unimodular matrix U such that $BU = [0, \ldots, 0, d]$ for some d (equal to the GCD of the entries of B). Write in block matrix form

$$U = \begin{pmatrix} E & C \\ R & a \end{pmatrix},$$

where E is a $k \times k$ matrix (and C is a column matrix and R a row matrix). The column vectors $X = (x_i)$ such that there exists a y satisfying our equality above are then exactly the $\mathbb{Z}$-linear combinations of the columns of the matrix E. But this means exactly that the kernel of χ is defined by the matrix E, or if we want it in normalized form, by the HNF of E. We can then compute the conductor as usual.

3.4. Computing defining equations. There seems to be two ways to compute the defining equations of the number fields L defined by a congruence group $(\mathfrak{m}, H)$. One is by Kummer theory. We refer to work of Pohst and collaborators ([Da-Po]) for details on this. The other method, which works only in certain cases, is the use of Stark units (see for example [Rob]). This is the subject of active research.

In this section, we would like to mention the main results which are used in this application of Kummer theory, and specialize to the case of quadratic and cubic extensions.

Let K be a fixed base field. In §3.2, we are given a congruence group $(\mathfrak{m}, H)$, and we compute the relative discriminant and signature of the class field L corresponding to this congruence group. We may of course assume that $\mathfrak{m}$ is the exact conductor of this field (otherwise we can easily reduce to this case). Our goal is to give a defining equation for L/K, here using Kummer theory.

Let us review what we know about the field L. We know its degree (equal to $h_{\mathfrak{m},H}$), its relative discriminant $\delta_{L/K}$, and its signature. We also know exactly the finite and infinite primes of K which ramify in L, i.e. the prime divisors of $\mathfrak{m}$. In fact, the exponents of these primes in $\mathfrak{m}$ give more information. We of course know that L/K is an Abelian extension with Galois group isomorphic to $Cl_{\mathfrak{m}}/H$.

We recall the following simple result, which is the beginning of Kummer theory.

Proposition 3.4. *Let K be a number field and L/K be a cyclic extension of degree p. There exists $\alpha \in K$ such that L is a subfield of degree p of the Abelian extension $N = K(\zeta_p, \sqrt[p]{\alpha})$, where ζ_p is a primitive p-th root of unity.*

If $\zeta_p \in K$ (for example when $p = 2$), then we have $L = N$ and the only problem to solve is to find α. When $\zeta_p \notin K$, we must find α and also find L afterwards.

Assume first that $\zeta_p \in K$. Then $L = K(\sqrt[p]{\alpha})$. The discriminant of the polynomial $x^p - \alpha$ is equal to $\pm p^p \alpha^{p-1}$, hence the only possible ramified prime ideals are those which divide p and those which divide α.

The following theorem gives the main result that we will need.

Theorem 3.5. *Let p be a prime such that $\zeta_p \in K$ and let $L = K(\sqrt[p]{\alpha})$.*

(1) *If $\mathfrak{q}$ is a prime ideal not dividing p, then $\mathfrak{q}$ is unramified in L/K if and only if $v_{\mathfrak{q}}(\alpha) \equiv 0 \pmod{p}$. If $\mathfrak{q}$ is ramified, then $v_{\mathfrak{q}}(\delta_{L/K}) = p - 1$.*

(2) *If $\mathfrak{p}$ is a prime ideal dividing p, assume that $\mathfrak{p} \nmid \alpha$. Set $a = v_{\mathfrak{p}}(1 - \zeta_p) = e(\mathfrak{p}/p)/(p-1)$. Then $\mathfrak{p}$ is unramified in L/K if and only if the congruence*

$$x^p \equiv \alpha \pmod{\mathfrak{p}^{ap}}$$

has a solution in K.

(3) *More precisely, if the congruence above has a solution, but the congruence mod $\mathfrak{p}^{ap+1}$ does not, then $\mathfrak{p}$ stays inert, otherwise $\mathfrak{p}$ is totally split.*

For a proof, see for example [Hec], Theorem 119.

We will make the following simplifying assumptions. First, we assume that $h_{\mathfrak{m},H} = p$ is prime. Then the ramified primes in L/K (i.e. the prime divisors of $\mathfrak{m}$) are totally ramified. Second, we assume that p is coprime to $\mathfrak{m}$, i.e. $\mathfrak{m}$ is not divisible by any prime ideal of K above p.

To choose α, we first look at prime ideals dividing $\mathfrak{m}$, hence not dividing p by assumption. For each such prime ideal, we want $v_{\mathfrak{q}}(\alpha) \not\equiv 0 \pmod{p}$. On the other hand, for any other prime ideal, we want $v_{\mathfrak{q}}(\alpha) \equiv 0 \pmod{p}$. In many cases (but not all), we can even assume that $v_{\mathfrak{q}}(\alpha) = 0$ for these other prime ideals. Assume α thus chosen (there is of course an infinite number of choices). Multiplying α by a unit does not change the above conditions, and we will now use this freedom to deal with the primes above p.

Assume $\mathfrak{p} \mid p$, so that in particular $\mathfrak{p} \nmid \alpha$ and $\mathfrak{p} \nmid \mathfrak{m}$. Thus $\mathfrak{p}$ must be unramified, and by Theorem 3.5 (2), this is equivalent to the congruence $x^p \equiv \alpha \pmod{\mathfrak{p}^{ap}}$ having a solution, and this must be true for all $\mathfrak{p} \mid p$. So if $\mathfrak{c} = \prod_{\mathfrak{p}|p} \mathfrak{p}$, the necessary and sufficient conditions boil down to the solvability of the single congruence

$$x^p \equiv \alpha \pmod{\mathfrak{c}^{ap}} \ .$$

Let α_0 be obtained so that the local conditions at the primes $\mathfrak{q}$ not dividing p are satisfied. We want to find $\alpha = \alpha_0 u$ such that u is a unit and the congruence $x^p \equiv \alpha_0 u \pmod{\mathfrak{c}^{ap}}$ is satisfied. For this, we compute the structure of the group $(\mathbb{Z}_K/\mathfrak{c}^{ap})^*$ as well as the matrix H whose columns are the discrete logarithms of the (known) generating set $\epsilon_0, \ldots, \epsilon_r$ for the units of K in $(\mathbb{Z}_K/\mathfrak{c}^{ap})^*$. Let B be the column vector equal to the discrete logarithm of α_0. Using Gaussian elimination and performing all computations modulo p (i.e. in the field $\mathbb{Z}/p\mathbb{Z}$), check whether the equation $HX \equiv B \pmod{p}$ has a solution or not. If it does not, a unit having the required properties does not exist. In the other case, let $X = (x_0, \ldots, x_r)$ be a lift to $\mathbb{Z}^{r+1}$ (with small coefficients) of a solution of $HX \equiv B \pmod{p}$. The searched unit is $u = \prod \epsilon_j^{-x_j}$.

To continue, we need the following proposition, which is a refinement of Proposition 3.4.

Proposition 3.6. *Assume that K contains the p-th roots of unity. Let g be a primitive root modulo p^2, and assume that there exists an automorphism τ of K extending the automorphism of $\mathbb{Q}(\zeta_p)$ sending ζ_p to ζ_p^g. Let L/K be a cyclic extension of degree p. Then there exists $\beta \in K$ such that if $\alpha = \prod_{a=0}^{p-2} (\tau^a(\beta))^{g^{p-2-a}}$, we have $L = K(\sqrt[p]{\alpha})$.*

Proof. Call σ a generator of the Galois group of L/K. By the normal basis theorem, we can find $\theta \in L$ such that $L = K(\theta)$ and the $\sigma^i(\theta)$ form a basis of L as a K-vector space. Set

$$\gamma = \sum_{i=0}^{p-1} \zeta_p^{-i} \sigma^i(\theta) \ .$$

Since the $\sigma^i(\theta)$ are linearly independent over K, γ is not equal to zero.

We have $\sigma(\gamma) = \zeta_p \gamma$, from which it follows, as in Proposition 3.4, that

$$\gamma^p = (-1)^{p-1} \mathcal{N}_{L/K}(\gamma) \in K \ .$$

Similarly, it is clear that

$$\sigma(\tau^a(\gamma)) = \zeta_p^{g^a} \tau^a(\gamma) \ .$$

We set $\beta = \gamma^g / \tau(\gamma)$. Then $\sigma(\beta) = \beta$, hence by Galois theory we have $\beta \in K$. Furthermore, an immediate calculation shows that

$$\alpha = \prod_{a=0}^{p-2} (\tau^a(\beta))^{g^{p-2-a}} = \gamma^{g^{p-1}-1} = \delta^p$$

with $\delta = \gamma^{(g^{p-1}-1)/p}$. To show that β is as desired, we must show that $L = K(\delta)$ or in other words, since $[L : K]$ is prime, that $\delta \notin K$. But since g is a primitive root modulo p^2, $(g^{p-1} - 1)/p \not\equiv 0 \pmod{p}$, so since $\gamma^p \in K$, if $\delta \in K$ we would have also $\gamma \in K$. But since $\sigma(\gamma) = \zeta_p \gamma$, we would then have $\gamma = 0$, which is absurd. This proves the proposition. □

Corollary 3.7. *Keep the notations of Proposition 3.6. Let $\theta = \sqrt[p]{\alpha}$ such that $L = K(\theta)$. Then if we define*

$$\tau(\theta) = \theta^g / \beta^{(g^{p-1}-1)/p} \ ,$$

and extend τ in a natural way to all of L, this gives an automorphism of L extending the automorphism τ of K. In addition, we have for $0 \le a \le p-2$,

$$\tau^a(\theta) = \theta^{g^a} / \prod_{i=0}^{a-1} (\tau^i(\beta))^{(g^{p-2+a-i}-g^{a-i-1})/p} .$$

Proof. Since $\theta^p = \alpha$, we must have $\tau(\theta)^p = \tau(\alpha)$. Using the definition of α in terms of β, we find that

$$\theta^{gp}/\tau(\theta)^p = \beta^{g^{p-1}-1} ,$$

from which it follows that

$$\theta^g/\tau(\theta) = \zeta_p^k \beta^{(g^{p-1}-1)/p} \quad \text{for some } k .$$

We can choose $k = 0$ (the other choices will give the p different extensions of τ to L), and we obtain the first formula of the corollary. The second is easily proved by induction. □

Assume now that $\zeta_p \notin K$. We set as before $M = K(\zeta_p)$ which is a cyclic extension of K of degree $p-1$. The conditions on α are exactly the same as before, except of course that we must choose $\alpha \in M$ and not in K. Thus, we may assume that N has been obtained. We now want to obtain L itself.

Corollary 3.8. *Keep the notations of Proposition 3.6 and Corollary 3.7, applied to the extension N/M instead of L/K. Set*

$$\lambda = \sum_{a=0}^{p-2} \tau^a(\theta)$$

as defined in Corollary 3.7. Then $L = K(\lambda)$.

Proof. We have $\lambda \in N$ and $\tau(\lambda) = \lambda$, hence by Galois theory $\lambda \in L$. Since $[L : K]$ is prime, to show that $L = K(\lambda)$ we need only to show that $\lambda \notin K$. Assume the contrary. Thus, $\sum_{a=0}^{p-2} \tau^a(\theta) = \lambda \in K$. Recall that N, as the compositum of the two Abelian extensions L/K and M/K, is Abelian, hence τ and σ commute. Applying σ^i to the above equality, and using $\sigma(\theta) = \zeta_p\theta$ and $\tau(\zeta_p) = \zeta_p^g$, we obtain for each i

$$\sum_{a=0}^{p-2} \zeta_p^{ig^a} \tau^a(\theta) = \lambda .$$

Using these equalities only for $0 \le i \le p-2$, we thus obtain a system of $p-1$ equations in $p-1$ unknowns, whose determinant is that of the Vandermonde matrix $\zeta_p^{ig^a}$. Since the $\zeta_p^{g^a}$ are distinct for $0 \le a \le p-2$, this determinant is nonzero, hence we obtain $\theta \in M$, which is absurd. Hence $\lambda \notin K$ and $L = K(\lambda)$ as claimed. □

4. Numerical results

4.1. Two examples of Kummer theory. To illustrate the results of §3, we give two examples coming from the numerical results given in §4.2. The first example is that of a quadratic extension, for which it is not necessary to adjoin roots of unity. The second example is that of a cubic extension.

In the first example, the base field K is defined by a root z of the polynomial $x^6 - x^5 + 2x^3 - 2x^2 + 1$. In this field, the prime number 41 splits as the product of three prime ideals of degree 1, and one prime ideal of degree 3. One of the prime

ideals of degree 1 is equal to $\mathfrak{P}_{41} = 41\mathbb{Z}_K + (z+4)\mathbb{Z}_K$. The number field K has two real places v_1 and v_2. We take as modulus $\mathfrak{m} = \mathfrak{P}_{41}v_1v_2$ and $H = P_{\mathfrak{m}}$ as congruence group. Using the methods of the preceding sections, we find that the ray class group is of order 2, that $\mathfrak{m}$ is a conductor, hence that there exists a quadratic extension L of K ramified exactly at primes above $\mathfrak{m}$, hence totally complex and ramified only at the finite prime $\mathfrak{P}_{41}$, and we compute its relative discriminant to be equal to $\mathfrak{P}_{41}$ itself (in the present case, this is trivial). We now want a defining equation for L/K.

Since L/K is quadratic, we have $L = K(\sqrt{\alpha})$ for some $\alpha \in \mathbb{Z}_K$. We first want this extension to be unramified outside 2 and $\mathfrak{P}_{41}$. For this, using the principal ideal problem in K, we compute that $\mathfrak{P}_{41} = \alpha_0\mathbb{Z}_K$ with $\alpha_0 = z^5 + 2z^2 - 2z$. Since we want L/K to be ramified above $\mathfrak{P}_{41}$ and no other prime ideals, from Theorem 3.5 and the fact that K is principal, we see that we must choose $\alpha = \alpha_0 u$ for u a unit of $\mathbb{Z}_K$. We now use the methods described before Proposition 3.6 to remove ramification above 2. We check that 2 is inert in K, hence $a = v_{\mathfrak{p}}(1-\zeta_2) = 1$. Thus $\mathfrak{c}^{ap} = 4\mathbb{Z}_K$ and we find that

$$(\mathbb{Z}_K/4\mathbb{Z}_K)^* \simeq (\mathbb{Z}/126\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^5$$

with generators $-2z^5 + z - 2$, -1 and $-2z^i + 1$ for $1 \le i \le 4$.

We can choose as generators of units $\epsilon_0 = -1$, $\epsilon_1 = z$, $\epsilon_2 = z^3 + 1$, $\epsilon_3 = z^4 - z^3 + z^2 + z - 1$. The matrix H of discrete logarithms of the units is

$$H = \begin{pmatrix} 0 & 64 & 97 & 11 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} ,$$

while the column vector B of the discrete logarithm of α_0 is equal to $B = [68, 0, 1, 1, 0, 0]^t$. By Gaussian elimination in $\mathbb{Z}/2\mathbb{Z}$, we see that the column vector $X = [0, 0, 1, 1]^t$ is the unique solution modulo 2 to $HX \equiv B \pmod 2$. Thus if we set

$$\alpha = \alpha_0\epsilon_2^{-1}\epsilon_3^{-1} = -z^5 + 2z^4 - 3z^2 + 3z \ ,$$

the ramification conditions at all the finite primes will be satisfied. The only freedom that we still have is to multiply by a square of a unit. In particular this does not change the signature, i.e. the ramification at infinity. One checks that indeed the real places are ramified, so L is a totally complex field.

Thus L can be defined over K by the equation

$$x^2 - (-z^5 + 2z^4 - 3z^2 + 3z) = 0 \ .$$

To get the absolute defining equation of L over $\mathbb{Q}$, we simply compute the resultant with respect to z of $x^2 - (-z^5 + 2z^4 - 3z^2 + 3z)$ with the defining polynomial $z^6 - z^5 + 2z^3 - 2z^2 + 1$, and we obtain

$$x^{12} - x^{10} + 2x^8 + 28x^6 - 23x^4 - 47x^2 + 41$$

as defining equation for our number field L.

Using polynomial reduction techniques (see [Coh] and [Co-Di]), we finally obtain the equation

$$x^{12} - 2x^{11} + 2x^{10} - x^9 + 2x^8 - 5x^7 + 8x^6 - 7x^5 + 4x^4 - 3x^3 + 4x^2 - 3x + 1$$

given below.

As a second example, we will take the case of a cubic extension. Here the base field K is defined by a root of the polynomial $x^6 - 2x^5 + 3x^4 + x^2 + 3x + 1$. This is a totally complex number field in which 2 is inert, and we choose as modulus $\mathfrak{m}$ the prime ideal $2\mathbb{Z}_K$ alone, and $H = P_{\mathfrak{m}}$. Using the algorithms of §3, we find that the ray class group is of order 3, hence that there exists a cubic extension L of K ramified only at 2, and we compute its relative discriminant ideal to be equal to $4\mathbb{Z}_K = 2^2\mathbb{Z}_K$. We now want a defining equation for L/K. Since $\zeta_3 \notin K$, we must start by adjoining ζ_3 to K. Thus we set $M = K(\zeta_3)$ and $N = L(\zeta_3)$. A straightforward computation, followed by polynomial reduction, shows that M can be defined by a root of the polynomial

$$P = x^{12} - 2x^{11} + x^{10} - 6x^9 + 8x^8 + 7x^7 + 5x^6 - 20x^5 - 2x^4 + 3x^3 + 8x^2 + 3x + 1.$$

Applying Proposition 3.6 to the extension N/M, we see that there exists $\beta \in M$ such that $N = M(\sqrt[3]{\alpha})$ with $\alpha = \beta^2\tau(\beta)$. In M, the prime 2 splits as the product of two prime ideals of degree 6, and since M is principal, they are generated by elements β_0 and $\beta_1 = \tau(\beta_0)$ respectively which can be found using the principal ideal problem (note that we must choose $\beta_1 = \tau(\beta_0)$ here and not any other generator). Since we do not want any ramification outside 2, we must choose β equal to some product of powers of β_0 and β_1 such that the corresponding $\alpha = \beta^2\tau(\beta)$ satisfies the conditions of Theorem 3.5. It is easily checked that any choice of such a β will lead to the same field. Thus, we can choose $\beta = \beta_0$, and we will have the correct ramification outside from 3.

To get rid of the ramification at 3, we look for a unit u such that $\alpha = \alpha_0 u$ is such that the congruence $x^3 \equiv \alpha \pmod{\mathfrak{c}^{3a}}$ has a solution, with $\alpha_0 = \beta_0^2\tau(\beta_0)$. In our field M, we have $3\mathbb{Z}_M = \mathfrak{p}^2\mathfrak{p}'^2$ for prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of degree 3, and hence $(1-\zeta_3)\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$. Thus $a = 1$, $\mathfrak{c} = \mathfrak{p}\mathfrak{p}'$, and so we must solve the congruence

$$x^3 \equiv \alpha_0 u \pmod{\mathfrak{p}^3\mathfrak{p}'^3} .$$

We compute that

$$(\mathbb{Z}_M/(\mathfrak{p}^3\mathfrak{p}'^3))^* \simeq (\mathbb{Z}/78\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^{10}$$

and the corresponding SNF generators. Then, we can easily find a desired unit u, which will be defined up to cubes of units.

However, to be able to get down to L, we will need to write u in the form $u = \epsilon^2\tau(\epsilon)$ for some unit ϵ. To do this, we must do two things. First, we must find the action of τ on the generators $\epsilon_0, \ldots, \epsilon_5$ of the units of M. If we have kept track of how the field $M = K(\zeta_3)$ was constructed, this is trivially done. If not, we can apply one of the techniques for the field isomorphism problem to get explicitly the action of τ.

In any case, in this way, we obtain a 6×6 matrix U such that the columns of U give (multiplicatively) the components of $\tau(\epsilon_j)$ on the ϵ_i. Let X be the column vector giving the components of our unit u on the ϵ_j. Then $(2X - UX)/3$ will be

the components of the desired unit ϵ on the ϵ_i. Note that this is a good check of the correctness of many computations, since these components must be integers.

So finally, we choose $\beta = \beta_0\epsilon$ and $\alpha = \beta^2\tau(\beta)$. To find L, we apply Corollaries 3.7 and 3.8 which tell us that $L = K(y)$ with $y = \theta + \theta^2/\beta$, where θ is a root of $x^3 - \alpha = 0$. It is now easy to find a relative equation for L/K, and hence an absolute equation, which we can then reduce. This is how the degree 18 example below was computed.

We have not given explicit values for the different numbers which are involved (the units, α_0, β, etc...) because they are not canonical and depend on the way the algorithms are programmed, so the reader will certainly have different values than ours. Only the final reduced equation given below should be similar.

4.2. Small discriminants. Using the algorithms described in this paper, we have computed a very large number of Abelian field extensions corresponding to congruence groups $(\mathfrak{m}, H)$. Here, to compute such an extension means to compute its degree, signature, absolute or relative discriminant, but not a defining equation.

We have proceeded as follows. Using tables of number fields K of degree less or equal to 7 available by anonymous ftp at the URL

`ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`

we have computed a list of moduli $\mathfrak{m}$ of norm less than or equal to a certain bound. For each of these $(K, \mathfrak{m})$ we have obtained the ray class group $Cl_{\mathfrak{m}}$ using the above algorithms, and then for each subgroup $\overline{H}$ of $Cl_{\mathfrak{m}}$, we have computed the signature and discriminant of the field L corresponding to the congruence group $(\mathfrak{m}, H)$. The subgroups $\overline{H}$ can be obtained as explained in §3.1.

In the course of this computation, if we find that $\mathfrak{m}$ is not the conductor of L (i.e. that $h_{\mathfrak{m},H} = h_{\mathfrak{m}/v,H}$ for some $v \mid \mathfrak{m}$), then we stop the computation and go to the next. Otherwise, we keep only those L which give an absolute degree $[L : \mathbb{Q}] = h_{\mathfrak{m},H} \cdot [K : \mathbb{Q}]$ less than or equal to 100. Finally, among those, we keep only those whose root discriminant is close compared to the GRH bounds (for example less than 1.2 times these bounds, see [Odl]).

To run these programs, we have recomputed these GRH bounds so as to have a complete list for all signatures (R_1, R_2) and degree up to 100. These are available as a text file readable by GP/Pari at the same URL given above.

Now the question arises of where to stop the search, both for the base fields, and, for a given base field, for the moduli.

We use the following criterion. Let C be the maximum of the allowable root discriminants. For example, we can take $C = 1.2B$ where B is the upper bound of the Odlyzko bounds for all degrees considered with a given signature.

Set $n = [K : \mathbb{Q}]$ and $N = [L : \mathbb{Q}]$. Then by Theorem 3.3, we have

$$|d_{L/\mathbb{Q}}|^{1/h_{\mathfrak{m},H}} = \frac{\mathcal{N}(\mathfrak{m})}{\prod_{\mathfrak{p}\mid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{\sum_{1\le k\le e_i} h_{\mathfrak{m}/\mathfrak{p}^k,H}/h_{\mathfrak{m},H}}} |d_{K/\mathbb{Q}}| \ .$$

However, since $\mathfrak{m}$ is assumed to be the conductor, we have $h_{\mathfrak{m}/\mathfrak{p}^k,H} < h_{\mathfrak{m},H}$ for $k \ge 1$. Call $\tau(a)$ the smallest prime divisor of an integer a. Thus $h_{\mathfrak{m}/\mathfrak{p}^k,H} \le$

$h_{\mathfrak{m},H}/\tau(h_{\mathfrak{m},H})$. From this and the above formula giving $d_{L/\mathbb{Q}}$, an immediate computation shows that

$$\mathcal{N}(\mathfrak{m}) \leq \left(|d_{L/\mathbb{Q}}|^{1/N}/|d_{K/\mathbb{Q}}|^{1/n}\right)^{n\tau/(\tau-1)} ,$$

with $\tau = \tau(h_{\mathfrak{m},H})$. Since we want the root discriminant to be less than C, and since $\tau/(\tau-1)$ is at most equal to 2, this implies

$$\mathcal{N}(\mathfrak{m}) \leq C^{2n}/|d_{K/\mathbb{Q}}|^2 .$$

Now this is of course a very pessimistic upper bound, but it shows several things. First, the number of moduli to consider for a given base field is finite (assuming of course that we limit the degree and the discriminant).

Second, the number of base fields to consider is also finite. More precisely, as $|d_{K/\mathbb{Q}}|$ increases, the number of possible moduli will decrease rather quickly, hence interesting fields will become rather rare.

Furthermore, note that the result does not depend on $h_{\mathfrak{m},H}$ and in particular not on the group H. For a given degree, the bound can be considerably improved (for example if the relative degree is odd, then $\tau/(\tau-1) \leq 3/2$, which gives much better bounds). Furthermore, for a given modulus satisfying the bounds, usually only a small number of H will be able to satisfy the simple condition on the degree of the field.

Of course all these observations are well known, but it is useful to put them on a quantitative footing.

One can then ask if it is plausible to find completely all the Abelian extensions of number fields of degree less than or equal to 7 (we do not have reasonably large tables in higher degrees) satisfying the limitations of degree and discriminant given above (degree up to 100 and root discriminant up to 1.2 times the GRH bound). While not absolutely impossible, it seems like a huge amount of computation.

To compare with previous results, we had at our disposal two sources. First the computations of [Mar] which were done 15 years ago in exactly the same spirit as this paper, but without the computer power. It is all the more remarkable that we have not been able to beat many of his records.

Second the papers [Leu] and [Le-Ni] which deal with Euclidean fields, most of which are not obtained as Abelian extensions of subfields, and only in small degree (less than or equal to 11).

We give below a list of 10 totally complex number fields obtained by the ray class field method. These fields all seem to be new and give the smallest known discriminant corresponding to their signature. In each case, the congruence group is trivial, and $\mathfrak{m}_\infty$ is the set of all real places of the base field K (if this was not the case, either L would not be totally complex or $\mathfrak{m}$ would not be its conductor). Thus we list the absolute degree $[L : \mathbb{Q}]$, the base field K, the finite part $\mathfrak{m}_0$ of the modulus $\mathfrak{m}$ as a product of prime ideals (written $\mathfrak{P}_p$ to indicate a prime ideal of degree 1 above p and $\mathfrak{p}_p$ a prime ideal of degree 2 above p), the discriminant in factored form, the root discriminant, and the percentage above the Odlyzko bound that we have computed (note that the bounds that we use are slightly better than those used by [Mar], hence when comparing the papers one should compare the

root discriminant and not the percentage).

N	K	$\mathfrak{m}_0$	$d_{L/\mathbb{Q}}$	$\lvert d_{L/\mathbb{Q}}\rvert^{1/N}$	GRH
12	$x^6-x^5+2x^3-2x^2+1$	$\mathfrak{P}_{41}$	$37^2\cdot 41\cdot 857^2$	7.666	0.843%
16	x^4-x-1	$\mathfrak{P}_{17}\mathfrak{P}_{37}$	$17^2\cdot 37^2\cdot 283^4$	9.179	1.164%
18	$x^6-2x^5+3x^4+x^2+3x+1$	(2)	$-2^{12}\cdot 23^6\cdot 107^3$	9.836	1.378%
28	x^4+2x^2-2x+1	$\mathfrak{P}_{71}$	$2^{28}\cdot 37^7\cdot 71^6$	12.296	1.135%
32	x^4-x^3+2x+1	$\mathfrak{P}_3\mathfrak{p}_{13}$	$3^{28}\cdot 7^8\cdot 13^{14}$	13.065	1.135%
36	$x^4-x^3+31x^2-24x+252$	(1)	$3^{18}\cdot 4057^9$	13.823	1.709%
40	x^2+2	$\mathfrak{P}_3\mathfrak{P}_3'\mathfrak{P}_{11}$	$2^{60}\cdot 3^{20}\cdot 11^{18}$	14.412	1.543%
48	$x^4-x^3+4x^2+3x+9$	$\mathfrak{p}_2\mathfrak{p}_5$	$2^{16}\cdot 3^{24}\cdot 5^{20}\cdot 13^{24}$	15.386	1.006%
52	$x^4-2x^3+21x^2-20x+68$	(1)	$2^{78}\cdot 1009^{13}$	15.941	1.626%
56	x^4-x^3-2x+8	$\mathfrak{P}_2^3$	$2^{49}\cdot 3^{42}\cdot 241^{14}$	16.472	2.283%

Using Kummer theory as explained in §3, we have computed relative and absolute defining equations for all of these fields with the exception of the one in degree 52. The absolute equations of the first three are:

$$x^{12}-2x^{11}+2x^{10}-x^9+2x^8-5x^7+8x^6-7x^5+4x^4-3x^3+4x^2-3x+1,$$

$$x^{16}+2x^{14}-x^{13}+3x^{12}-4x^{11}+4x^{10}-7x^9+5x^8-7x^7+4x^6 - 4x^5+3x^4-x^3+2x^2+1,$$

$$x^{18}-x^{17}+3x^{16}+2x^{15}-x^{14}+11x^{13}+3x^{12}+3x^{11}+28x^{10} - 18x^9+47x^8-27x^7+45x^6-23x^5+27x^4-11x^3+9x^2-2x+1.$$

In addition to these fields, we have also computed the first few thousand octic fields containing a quartic subfield in every possible signature. Finally, we have also found a large number of fields with small discriminants and of various degrees and signatures. These computations will be described in a forthcoming paper. Many of these fields have large discriminants compared to the Odlyzko bounds. This may be expected, since there is no reason, especially in large degrees, that small discriminants will correspond to Abelian extensions of subfields. On the contrary, it is plausible that the Galois group of such fields will tend to be the complete symmetric group S_n, which prevents the fields from having nontrivial subfields.

References

[B-D-S] E. Bach, J. Driscoll and J. Shallit, *Factor refinement*, J. Algorithms **15** (1993), 199–222. MR **94m:**11148

[Ca-Fr] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London, 1967. MR **35:**6500

[Coh] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer-Verlag, Berlin, Heidelberg, New York, 1993. MR **94i:**11105

[Coh2] H. Cohen, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), 1681–1699. MR **97e:**11159

[Co-Di] H. Cohen and F. Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Th. des Nombres Bordeaux (série 2) **3** (1991), 351–360. MR **93a:**11107

[Co-Di-Ol] H. Cohen, F. Diaz y Diaz and M. Olivier, *Algorithmic methods for finitely generated Abelian groups*, submitted to J. of Symbolic Computation 1996.

[Da-Po] M. Daberkow and M. Pohst, *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields*, Proc. ISAAC'95 (1995) (to appear).

[Di-Ol] F. Diaz y Diaz and M. Olivier, *Algorithmique Algébrique dans les Corps de Nombres*, Etat de la Recherche en Algorithmique Arithmétique, Laboratoire A2X, Bordeaux, 1995.

[Ha-Ma] G. Havas and B. Majewski, *Hermite normal form computation for integer matrices*, Congr. Numer. **105** (1994), 87–96. MR **96k:**15004

[Hec] E. Hecke, *Lectures on the theory of algebraic numbers*, GTM 77, Springer-Verlag, Berlin, Heidelberg, New York, 1981. MR **83m:**12001

[Leu] A. Leutbecher, *Euclidean fields having a large Lenstra constant*, Ann. Inst. Fourier **35,2** (1985), 83–106. MR **86j:**11107

[Le-Ni] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, Lecture Notes in Math., vol. 1380, Springer, New York, 1989. MR **90i:**11123

[Mar] J. Martinet, *Petits discriminants des corps de nombres*, Journées arithmétiques 1980 (J.V. Armitage, Ed.), London Math. Soc. Lecture Notes Ser. 56 (1982), 151–193. MR **84g:**12009

[Nak] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo* $\wp^{N+1}$, Nagoya Math. J. **73** (1979), 41– 60. MR **80c:**12010

[Odl] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Th. des Nombres Bordeaux (série 2) **2** (1990), 119–141. MR **91i:**11154

[Po-Za] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Math. and its Applications, Cambridge University Press, Cambridge, 1989. MR **92b:**11074

[Rob] X.-F. Roblot, *Unités de Stark et corps de classes de Hilbert*, C. R. Acad. Sci. Paris **323** (1996), 1165–1168.

[Zan] H. Zantema, Class numbers and units; Computational methods in number theory II (Math. Centrum, ed.), Math. Centre Tracts 155, Amsterdam, 1982, pp. 213–234. MR **85g:**11118a

Laboratoire A2X, Université Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France

E-mail address: cohen@math.u-bordeaux.fr

E-mail address: diaz@math.u-bordeaux.fr

E-mail address: olivier@math.u-bordeaux.fr