JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

HENRI COHEN

# A survey of computational class field theory

*Journal de Théorie des Nombres de Bordeaux*, tome 11, nº 1 (1999), p. 1-13

<http://www.numdam.org/item?id=JTNB_1999__11_1_1_0>

*Journal de Théorie des Nombres de Bordeaux* **11** (1999), 1–13

# A Survey of Computational Class Field Theory

par HENRI COHEN

RÉSUMÉ. Le but de cet article est de décrire les avancées récentes dans la théorie algorithmique du corps de classes. Nous expliquons comment calculer les groupes de classes de rayon ainsi que les discriminants des corps de classes correspondants. Nous donnons ensuites les trois méthodes principales utilisées pour le calcul des équations des corps de classes : la théorie de Kummer, les unités de Stark et la multiplication complexe. En utilisant ces techniques, nous avons pu construire de nombreux nouveaux corps de nombres intéressants, en particulier ayant un discriminant très proche des bornes d'odlyzko.

ABSTRACT. We give a survey of computational class field theory. We first explain how to compute ray class groups and discriminants of the corresponding ray class fields. We then explain the three main methods in use for computing an equation for the class fields themselves: Kummer theory, Stark units and complex multiplication. Using these techniques we can construct many new number fields, including fields of very small root discriminant.

Let $K$ be a number field and let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a *modulus* in $K$, i.e. $\mathfrak{m}_0$ is an integral ideal and $\mathfrak{m}_\infty$ is a set of real places of $K$. To such a modulus is attached a *ray class group* $Cl_\mathfrak{m}(K)$ which generalizes the notion of ordinary class group. In addition, to each subgroup $\overline{C}$ of $Cl_\mathfrak{m}(K)$ including the trivial subgroups is attached an (isomorphism class of) Abelian extension $L/K$ by class field theory, such that, among other properties, $\mathrm{Gal}(L/K) \simeq Cl_\mathfrak{m}(K)/\overline{C}$.

The main problems of computational class field theory deal with the explicit computations of all these objects. Thus, this paper is divided in three parts. In the first part, we explain the computation of $Cl_\mathfrak{m}(K)$ and its subgroups, and we explain how to compute the discriminant of the corresponding extension $L/K$, which is very easy to do once one has the tools for computing $Cl_\mathfrak{m}(K)$. In the second part, we explain the three known methods for computing an explicit equation for $L/K$. In the last part, we give some applications.

The work described here is essentially work done jointly with F. Diaz y Diaz and M. Olivier, with extra references to work of R. Schertz, X. Roblot, M. Pohst and C. Fieker.

## 1. Computation of Ray Class Groups

We will denote by $\mathbb{Z}_K$ the ring of integers of the number field $K$, by $Cl(K)$ its class group and $U(K)$ its unit group. If $\mathfrak{m}$ is a modulus of $K$, the basic exact sequence involving the ray class group $Cl_{\mathfrak{m}}(K)$ is

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

Thus, to compute $Cl_{\mathfrak{m}}(K)$ and its subgroups, we need to do four things:

- Compute $Cl(K)$ and $U(K)$.
- Deal with exact sequences of Abelian groups (in particular when they are nonsplit).
- Compute $(\mathbb{Z}_K/\mathfrak{m})^*$.
- Compute the subgroups of a given Abelian group.

We consider these problems in turn.

### 1.1. Computation of $Cl(K)$ and $U(K)$.

The computation of $Cl(K)$ and of $U(K)$ has been the subject of intensive work in the past years (Hafner-McCurley, Buchmann et al, Pohst et al, Cohen-Diaz y Diaz-Olivier, see for example [4] and [7]). It is now possible to compute these groups unconditionally for number fields of degree up to 12 to 15 and not too large discriminant, and *under the Generalized Riemann Hypothesis* (GRH) for number fields up to degree 40 and reasonable discriminant.

Together with this computation, one also solves the *principal ideal problem*: express an ideal on the class group generators, and even more importantly find generators of principal ideals.

The main idea to perform this computation is to choose an a priori set of generators $(g_i)_{1\le i\le k}$ for the class group, the so-called *factor base*, and to find sufficiently many relations between these generators by looking for elements of small norm or by reducing ideal products, we refer to loc. cit. for details. The main difference between the conditional and unconditional algorithms comes from the choice of these generators: if we assume GRH, we may take the $g_i$ to be the ideal classes of prime ideals of norm less than equal to $12\log^2(|d(K)|)$ according to a theorem of E. Bach (see [1]). If on the other hand GRH is not assumed, one must take a bound such as the Minkowski bound or a similar bound, which is proportional to $\sqrt{|d(K)|}$, hence very large. Although quite difficult and long to implement, this is now classical, and we will not dwell any longer on this computation.

1.2. **Computation on Exact Sequences of Abelian Groups.** Since exact sequences can always be considered as the composition of 3-term exact sequences, we consider only those (although in practice we proceed slightly differently). The problem is simply as follows. Given such a three term exact sequence of Abelian groups

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

with explicitly given maps between the groups (in some well defined sense), given two of the groups, compute the third one.

First, we need to explain how to "give" an Abelian group $\mathcal{A}$. The canonical way is to write it in Smith Normal Form (SNF), i.e. to write

$$\mathcal{A} = \bigoplus_{1 \leq i \leq m} (\mathbb{Z}/a_i\mathbb{Z})\alpha_i$$

where for all $i < m$ we have $a_{i+1} \mid a_i$, $a_i > 1$ for all $i$, and $\alpha_i \in \mathcal{A}$ of order exactly $a_i$. The elementary divisors $a_i$ (not the $\alpha_i$) are unique, and the SNF of an Abelian group $\mathcal{A}$ can easily be obtained from any complete system of generators and relations for $\mathcal{A}$ by using the SNF algorithm (see for example [4], Algorithm 2.4.14). We will set $D_A$ to be the diagonal matrix of the $a_i$, $A$ to be the row vector of the $\alpha_i$, and write simply $\mathcal{A} = (A, D_A)$. Note that, in the above, we have carefully avoided isomorphisms and used explicit equalities. This is essential in all computational work (strictly speaking, the use of $(\mathbb{Z}/a_i\mathbb{Z})$ implies an isomorphism, but it is an extremely convenient shorthand).

An Abelian group is however often not considered as an abstract structure, but as a subgroup of a larger group. In this case, there is another representation which is preferable. To define it, we need another special form of matrices, which is even more essential than that of SNF, the notion of Hermite Normal Form (HNF). We will say that a matrix $H$ is in HNF if it is a square upper triangular matrix $H = (h_{i,j})$ with strictly positive diagonal coefficients $h_{i,i}$, and with the off-diagonal coefficients satisfying $0 \leq h_{i,j} < h_{i,i}$ for $j > i$. The main theorem about the HNF is that given any $k \times m$ matrix $M$ of maximal rank $k$ (so that $m \geq k$), there exist a unique HNF matrix $H$, and a unimodular matrix $U$ such that $MU = (0|H)$. The columns of $H$ form a $\mathbb{Z}$-basis of the module generated by the columns of $M$, and the $m - k$ first columns of $U$ form a $\mathbb{Z}$-basis of the $\mathbb{Z}$-kernel of $M$. In addition, there are efficient algorithms to compute such a decomposition (see for example [4], Algorithm 2.4.8).

Let us come back to the representation of subgroups. Let $\mathcal{B} = (B, D_B)$ be an Abelian group. Then it is easy to show that subgroups of $\mathcal{B}$ are in one to one correspondence with left divisors $H$ of $D_B$ (i.e. integral matrices $H$ such that $H^{-1}D_B$ is also integral) which are in HNF, the columns of $H$ giving the generators of the subgroup in terms of the generators $B$ of the group $\mathcal{B}$. It is not difficult to go back and forth from a subgroup to an SNF representation of a subgroup.

For exact sequences

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

we have three problems to solve: given $\mathcal{A}$ and $\mathcal{B}$, compute $\mathcal{C}$ (computing a quotient), given $\mathcal{B}$ and $\mathcal{C}$, compute $\mathcal{A}$ (computing a kernel), and given $\mathcal{A}$ and $\mathcal{C}$, compute $\mathcal{B}$ (computing an extension). Of course it is essential that the maps $\phi$ and $\psi$ be specified explicitly in some way, otherwise the problem does not make sense.

All these problems can be solved very simply using the HNF and SNF algorithms (see [8] for details). In particular, there is no difficulty in computing group extensions in practice, even when the exact sequence does not split. For the reader's interest, we give the method in that case.

Let $\mathcal{A} = (A, D_A)$ and $\mathcal{C} = (C, D_C)$ be given, as well as the maps $\phi$ and $\psi$. Write $A = (\alpha_i)$, $D_A = (a_i)$, $C = (\gamma_i)$ and $D_C = (c_i)$. Since $\psi$ is surjective, we choose arbitrary lifts $\beta'_i$ of $\gamma_i$ to $\mathcal{B}$, i.e. such that $\psi(\beta'_i) = \gamma_i$, and let $B'$ be the row vector of the $\beta'_i$. Then $\psi(\beta'^{c_i}_i) = 1_C$, hence there exists $\alpha'_i \in \mathcal{A}$ such that $\phi(\alpha'_i) = \psi(\beta'^{c_i}_i)$. Let $P$ be the matrix whose columns are the exponents of $\alpha'_i$ on the given generators $\alpha_i$ of $\mathcal{A}$. If $G = (\psi(A)|B')$ and $M = \begin{pmatrix} D_A & -P \\ 0 & D_C \end{pmatrix}$, then $(G, M)$ is a complete system of generators and relations for the group $\mathcal{B}$, from which one computes the SNF $(B, D_B)$ using the SNF algorithm.

1.3. **Computation of $(\mathbb{Z}_K/\mathfrak{m})^*$ and of $Cl_\mathfrak{m}(K)$.** Although a very natural problem, the explicit computation of $(\mathbb{Z}_K/\mathfrak{m})^*$ is not at all easy in theory. There is a paper by Nakagoshi [17] dealing with this problem, but the answer is not at all satisfactory, even for algorithmic purposes. We explain here how the computation can easily be done in practice, although it leaves open a more theoretical answer (which probably does not exist in simple terms).

By the Chinese remainder theorem, we can easily reduce to the case where the modulus $\mathfrak{m}$ is of the form $\mathfrak{p}^k$ for a prime ideal $\mathfrak{p}$. Let $p$ be the prime number below $\mathfrak{p}$.

To compute $(\mathbb{Z}_K/\mathfrak{p}^k)^*$, we first remove the prime to $p$ part, which is isomorphic to $(\mathbb{Z}_K/\mathfrak{p})^* \simeq (\mathbb{Z}/(p^f - 1)\mathbb{Z})$, where $f = f(\mathfrak{p}/p)$ is the residual index of $\mathfrak{p}$ over $p$. This is easy, and of course must be done without using isomorphisms. We are left with the group $G_{\mathfrak{p}^k} = (1 + \mathfrak{p})/(1 + \mathfrak{p}^k)$.

To compute this group, two methods can be used. The first natural one is the use of $\mathfrak{p}$-adic logarithms. Indeed, additive structures are much easier to compute than multiplicative ones, and if $\mathfrak{p}$ is not too ramified, more precisely when $e(\mathfrak{p}/p) < p - 1$, the $\mathfrak{p}$-adic logarithm function gives an explicit isomorphism of the multiplicative group $G_{\mathfrak{p}^k}$ with the additive group $\mathfrak{p}/\mathfrak{p}^k$ which can easily be computed (once again using HNF and SNF techniques).

When this method fails, i.e. when $e(\mathfrak{p}/p) \geq p-1$, we must use another method, which is the computation by induction. Such a method was already used by Hasse and revitalized by Pohst and collaborators, who compute $G_{\mathfrak{p}^k}$ in terms of $G_{\mathfrak{p}^{k-1}}$. To go faster, we prefer doubling the exponent at each step and use induction on the exact sequences

$$1 \longrightarrow \frac{1+\mathfrak{p}^a}{1+\mathfrak{p}^{2a}} \longrightarrow \frac{1+\mathfrak{p}}{1+\mathfrak{p}^{2a}} \longrightarrow \frac{1+\mathfrak{p}}{1+\mathfrak{p}^a} \longrightarrow 1 \ ,$$

together with the trivial isomorphisms

$$\left(\frac{1+\mathfrak{p}^a}{1+\mathfrak{p}^{2a}}, \times\right) \simeq \left(\frac{\mathfrak{p}^a}{\mathfrak{p}^{2a}}, +\right) \ .$$

Of course the above exact sequences are treated using the tools mentioned in the preceding section.

Once $(\mathbb{Z}_K/\mathfrak{m})^*$ has been computed, we use once again the tools developed for computing on exact sequences to compute the ray class group $Cl_{\mathfrak{m}}(K)$. We note that at the same time, it is easy to develop a *principal ideal algorithm* in $Cl_{\mathfrak{m}}(K)$, which not only says if an ideal becomes trivial in the ray class group, but finds a generator multiplicatively congruent to 1 modulo $\mathfrak{m}$ if it is.

1.4. **Computation of the Subgroups of an Abelian Group.** Once $Cl_{\mathfrak{m}}(K)$ is computed, to obtain all Abelian extensions of $K$ of modulus $\mathfrak{m}$ by class field theory, we also need to compute all possible subgroups of the Abelian group $G = Cl_{\mathfrak{m}}(K)$. To do this, we proceed as follows. First write $G \simeq \oplus G_p$, where $G_p$ is the $p$-Sylow subgroup of $G$. Then subgroups $A$ of $G$ are in a unique way of the form $A = \oplus A_p$, where $A_p$ is a subgroup of $G_p$. Thus, we can reduce the problem to finding all subgroups of a $p$-group. Note that in the above description, it is essential to chase though all the implicit isomorphisms using Chinese remainder theorem techniques, and this is a little painful but absolutely necessary.

Thus, assume now that $G$ is a $p$-group of SNF $D = (c_i)_{1\leq i\leq m}$. According to the correspondence explained above, finding subgroups of $G$ amounts to finding all the HNF left divisors $H$ of $D$.

If $D$ is of very small size, this is easy. For example, if $m=1$, then $H = (e_1)$ with $e_1 \mid c_1$. If $m=2$, then an immediate calculation shows that $H = \begin{pmatrix} e_1 & f_1 \\ 0 & e_2 \end{pmatrix}$ with $e_i \mid c_i$ for $i=1$ and 2, and $f_1 = ke_1/\gcd(e_1, c_2/e_2)$ with $0 \leq k < \gcd(e_1, c_2/e_2)$.

For larger values of $m$, the answer to this problem has been given completely by G. Birkoff in 1934 [2], and is too complicated to state here. It is however completely algorithmic. I was not aware of this result at the time of my talk, and I am grateful to L. Habsieger and L. Butler for having pointed it out to me. Birkhoff's paper contains many misprints, and I refer to L. Butler's memoir [3] for a detailed statement and improvement of Birkhoff's theorem (K. Belabas has implemented Butler's version of Birkhoff's theorem in Pari, with apparently correct results, and Butler herself has done so, hence presumably there are no misprints in her statement).

## 2. Computation of Ray Class Fields

We now come to the more difficult but more interesting part of the theory: the computation of the class fields themselves.

2.1. **Computation of Conductors and Discriminants.** Using the tools explained in Part 1 that are now at our disposal, we can already perform quite a number of interesting computations, as we now explain. For all the details on these computations, I refer to [9].

First, let $(\mathfrak{m}, C)$ be a congruence subgroup, in other words $C$ is a subgroup of the group $I_{\mathfrak{m}}$ of fractional ideals coprime to $\mathfrak{m}$ containing the group $P_{\mathfrak{m}}$ of principal ideals generated by an element multiplicatively congruent to 1 modulo $\mathfrak{m}$, or equivalently the set $\overline{C}$ of ideal classes is a subgroup of $Cl_{\mathfrak{m}}(K)$. We need to compute the *conductor* of this congruence subgroup, i.e. the smallest modulus $\mathfrak{n}$ for which $C$ can be defined modulo $\mathfrak{n}$. This is now very simple. If $\mathfrak{n} \mid \mathfrak{m}$, denote by $s_{\mathfrak{m},\mathfrak{n}}$ the natural surjection from $Cl_{\mathfrak{m}}(K)$ to $Cl_{\mathfrak{n}}(K)$, and set $h(\mathfrak{m}, C) = |Cl_{\mathfrak{m}}(K)/\overline{C}|$. Then for every place $\mathfrak{p}$ dividing $\mathfrak{m}$ (finite or infinite), compute $h(\mathfrak{m}/\mathfrak{p}, s_{\mathfrak{m},\mathfrak{m}/\mathfrak{p}}(C))$. If for any $\mathfrak{p}$ this is equal to $h(\mathfrak{m}, C)$, replace $\mathfrak{m}$ by $\mathfrak{m}/\mathfrak{p}$ and start again the whole process. We stop when $h(\mathfrak{m}/\mathfrak{p}, s_{\mathfrak{m},\mathfrak{m}/\mathfrak{p}}(C)) < h(\mathfrak{m}, C)$ for all $\mathfrak{p}$, and $(\mathfrak{m}, C)$ is our desired conductor.

Second, let $L/K$ be an Abelian extension (unique up to isomorphism) corresponding to a congruence subgroup $(\mathfrak{m}, C)$ by class field theory. Then even without assuming that $(\mathfrak{m}, C)$ is minimal (i.e. that $\mathfrak{m}$ is the conductor of the extension, or equivalently of the congruence subgroup $(\mathfrak{m}, C)$), we can easily give some information on the field $L$. The signature is easily obtained (in fact it is trivial if $\mathfrak{m}$ is known to be the conductor, since in that case the real places which ramify in $L/K$ are exactly those dividing $\mathfrak{m}$).

But there also exists a nice formula for the relative discriminant $\mathfrak{d}(L/K)$ (hence also for the absolute discriminant $d(L) = \pm\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(L/K))d(K)^{[L:K]}$ where the sign is determined by the signature), given as follows. We have

$$\mathfrak{d}(L/K) = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{v_{\mathfrak{p}}}$$

with

$$v_{\mathfrak{p}} = h(\mathfrak{m}, C)v_{\mathfrak{p}}(\mathfrak{m}) - \sum_{1 \le k \le v_{\mathfrak{p}}(\mathfrak{m})} h(\mathfrak{m}/\mathfrak{p}^k, s_{\mathfrak{m},\mathfrak{m}/\mathfrak{p}^k}(C)) \ .$$

Thus, although the field $L$ is in general not uniquely determined by its signature and discriminant, we have pretty good control over it. For example, if we are looking for number fields of reasonably small discriminants (see applications below), one can immediately tell whether a field $L$ will be interesting or not before computing explicitly an equation for it.

Third, we can easily compute the *norm group* of a given Abelian extension $L/K$. Here, we assume that $L/K$ is given explicitly (this will be the case later). We proceed as follows. Let $\mathfrak{m}$ be a known multiple of the conductor of $L/K$, for example the relative discriminant $\mathfrak{d}(L/K)$ together with the real places of $K$ which ramify in $L/K$. Let $(C, D_C)$ be the SNF of the ray class group $Cl_{\mathfrak{m}}(K)$, and denote by $n$ the relative degree $[L : K]$. Initialize a matrix $M$ to the diagonal matrix $D_C$. For each prime ideal $\mathfrak{p}$ of $K$ not dividing $\mathfrak{m}$ do as follows, until the determinant of $M$ is equal to $n$. Compute the factorization of $\mathfrak{p}\mathbb{Z}_L$ into prime ideals $\mathfrak{P}$ of $\mathbb{Z}_L$. Since $L/K$ is Abelian, all the relative residual degrees $f(\mathfrak{P}/\mathfrak{p})$ will be equal, say to $f$. Let $L$ be the column vector of the exponents of $\mathfrak{p}$ on the generators $C$ of $Cl_{\mathfrak{m}}(K)$. Finally, concatenate $M$ with the one column matrix $fL$, and replace $M$ by the HNF of this concatenation. It is easy to show that the determinant of $M$ will always be a multiple of $n$, and that after a small number of steps the matrix $M$ will have determinant exactly equal to $n$. When this happens, $M$ is a left divisor of $D_C$ which gives the norm group $T_{\mathfrak{m}}(L/K)$ (i.e. the kernel of the Artin map) on the given generators $C$ of the class group.

>From this, it is of course trivial to compute the conductor of the Abelian extension $L/K$: set $\mathfrak{m}$ equal to a known multiple of the conductor of $L/K$, say as above the relative discriminant together with the ramified real places. Let $C$ be the norm group for the modulus $\mathfrak{m}$ as computed above. Then the conductor of the congruence subgroup $(\mathfrak{m}, C)$ computed as explained at the beginning of this section is the conductor of the Abelian extension $L/K$.

If desired, it is also easy to compute the conductors of individual characters of the extension $L/K$.

2.2. **Generalities on Class Field Constructions.** We now must deal with the more difficult task of finding an explicit relative or absolute equation for the extension $L/K$, knowing only that it corresponds to a given congruence subgroup $(\mathfrak{m}, C)$ by class field theory.

To my knowledge, there are three methods to do this, which we shall examine in turn (there is a fourth method, used long ago by a distinguished colleague, which is essentially using one's nose, but this does not count as an algorithm).

- **Kummer theory**. This method has the advantage of complete generality, and in fact is also the method used in the theoretical proof of the Takagi existence theorem of class field theory. Its main disadvantage is that it requires sufficiently many roots of unity in the base field, hence in general these have to be adjoined to the base field, so the computations are done in much larger fields than apparently necessary. In addition, it is necessary to have suitable tools to go back down from the larger fields to the fields that we want.

- **The use of Stark's conjectures**. The explicit construction of ray class fields by the use of elements (in fact units) obtained by analytical means was one of the main motivations for Stark's conjectures. The use of these conjectures has now been put in a precise and general algorithmic form by X. Roblot (see [18], [19] and [10]).

This method can be used only when the base field $K$ is totally real (although I have been told that it may be possible to treat also the case where $K$ has a single complex place, i.e. 2 complex conjugate embeddings). The fact that an unproved conjecture is used here is completely unimportant, since once the field $L$ is obtained, it is easy to show that it is the desired ray class field.

- **The use of complex multiplication**. This method is very efficient, but applies only when the base field is an imaginary quadratic field. The principles behind the method have been known for a century (the use of the values of the elliptic modular invariant $j(\tau)$ at quadratic points), but it is only recently in particular thanks to work of R. Schertz (see [20], [21] and [22]) that the method has become algorithmically useful.

We consider these methods in turn in a little more detail.

2.3. **Kummer Theory.** An easy reduction which can be made (in every method, not simply in Kummer theory), is to reduce to cyclic extensions of prime power degree. The desired extension $L/K$ will simply be the compositum of its cyclic prime power degree subextensions, and the corresponding congruence subgroups are completely under control. This reduction should be made in any case.

>From there, two methods can be used. One is to reduce the cyclic extension of prime power degree to a tower of cyclic extensions of prime degree, in order to apply a theorem of Hecke specific to such extensions describing completely the ramification properties.

The other method is to use directly the Artin map from ideals to the Galois group of the desired extension, and implicitly forget about ramification properties. This method has been introduced by C. Fieker (see [11]) and is certainly much more efficient in the general case. I refer to his paper for details. Here we describe briefly the first method.

Thus, assume that we want to find a cyclic extension $L/K$ of prime degree $\ell$ corresponding to a given congruence subgroup $(\mathfrak{m}, C)$. Thanks to the preceding section, we may assume that $(\mathfrak{m}, C)$ is minimal, i.e. that it is the conductor of the extension $L/K$.

To apply Kummer theory, we need to adjoin to $K$ the $\ell$-th roots of unity, which in general are not all in $K$. Hence, if $\zeta$ is a primitive $\ell$-th root of unity replace $L/K$ by the extension $L_z/K_z = L(\zeta)/K(\zeta)$. Then Kummer theory tells us several things.

- There exists $\alpha \in K_z$ such that $L_z = K_z(\sqrt[\ell]{\alpha})$.
- The number $\alpha$ must satisfy *ramification* conditions coming from a theorem of Hecke which completely describes the ramification properties and the relative discriminant of such a Kummer extension.
- The number $\alpha$ must satisfy *Galois* conditions coming from the fact that the extension $L_z/K$, which is the compositum of the Abelian extensions $L/K$ and $K_z/K$, is Abelian. This is equivalent to the use of *Lagrange resolvents.*

These conditions can be transformed into conditions involving only linear algebra, and we can thus reduce to a small finite set of $\alpha$. There is almost no search in this step.

For each of the tentative $\alpha$, we then compute the norm group using the method explained in the preceding section, and exactly one of the $\alpha$ will give a norm group equal to $C$. Once the correct $\alpha$ is obtained, it is easy to compute the relative equation for $L/K$, and also the absolute equation for $L/\mathbb{Q}$ if desired.

### 2.4. The use of Stark's Conjectures.

For this section, I refer to [18], [19] and [10].

The main inefficiency of the algorithmic use of Kummer theory is the necessity of adjoining an $\ell$-th root of unity $\zeta$, which transforms the base field $K$ into a base field $K_z = K(\zeta)$ of much larger degree.

When $K$ is *totally real*, there exists a completely different method which uses Stark's conjectures and Stark units.

Let $L/K$ be an Abelian extension of $K$, and let $S$ be the set of infinite places of $K$ together with the prime ideals of $K$ which ramify in $L/K$. Let Art be the Artin map from the ideals of $K$ coprime to $S$ to $\mathrm{Gal}(L/K)$.

For $\sigma \in \mathrm{Gal}(L/K)$, define

$$\zeta_{K,S}(s,\sigma) = \sum_{(\mathfrak{a},S)=1,\ \mathrm{Art}(\mathfrak{a})=\sigma} \mathcal{N}(\mathfrak{a})^{-s} .$$

If there exists a unique real embedding $\tau$ of $K$ into $\mathbb{C}$ which is unramified in $L/K$ (i.e. which has only real extensions), then Stark's conjecture asserts that there exists a unit $\varepsilon$ such that for all embeddings $\sigma$ of $L$ extending $\tau$, we have

$$\sigma(\varepsilon) = e^{-2\zeta'_{K,S}(0,\sigma)} .$$

To obtain an extension $L'/K$ satisfying the condition of the conjecture, it is enough to choose $L' = L(\sqrt{\alpha})$ for $\alpha$ satisfying suitable conditions. Once the unit $\varepsilon' \in L'$ is found, one can come down to $L$ by setting $\varepsilon = \varepsilon' + 1/\varepsilon'$, and it can be shown that $L = K(\varepsilon)$.

Several non-trivial technical details must be solved, in particular the numerical computation of $\zeta'_{K,S}(0,\sigma)$, but this leads to a reasonably efficient method. The generating polynomials which are obtained usually have large coefficients and must be reduced using well known polynomial reduction methods such as the Polred algorithm of Pari (see [6]). When applicable (i.e. when the base field $K$ is totally real), this method performs much faster than the method using Kummer theory, except when $K$ already contains all the necessary roots of unity (for example when $[L : K] = 2$ or more generally when $\mathrm{Gal}(L/K)$ is an elementary 2-group). Only in that case is it preferable to use Kummer theory or genus theory when applicable.

2.5. **The use of Complex Multiplication.** For this section, I refer to [20], [21] and [22] (see also [23] and [12]).

Let $K$ be an imaginary quadratic fields. If $j(\tau)$ denotes the usual modular function, the modular invariance implies that one can define $j(\mathfrak{a})$ for an ideal $\mathfrak{a}$, and the polynomial

$$P(X) = \prod_{\bar{\mathfrak{a}} \in Cl(K)} (X - j(\mathfrak{a})) \in \mathbb{Z}[X]$$

is an irreducible polynomial which defines the Hilbert class field of $K$, i.e. the ray class field corresponding to the trivial modulus $\mathfrak{m} = \mathbb{Z}_K$.

Modifications of this construction using the Weierstraß $\wp$ function gives also ray class fields.

The problem with this method is that the size of the coefficients of the polynomials obtained in this way is very large (10 or 20 digits even for small discriminants).

The use of other functions such as Weber's functions is well known to improve dramatically the situation (see [23], [12]). The problem with these functions is that they do not work in all cases (one often has to assume that the discriminant of the quadratic field is prime to 3, or in given congruence classes modulo 8). In the worst cases, they give polynomials with coefficients which are again too large to be practical.

A systematic treatment of this algorithmic problem using a quotient of a product of two $\eta$ functions has been given in the 1980's by R. Schertz, together with non-trivial generalizations to the case of ray class fields. This method is extremely efficient and allows to compute Hilbert and ray class fields of imaginary quadratic fields in very little time. This method always gives polynomials having relatively small coefficients (although necessarily still exponentially growing with the size of the discriminant, as will all methods based on modular functions), although the coefficients are a little larger than the ones obtained with the Weber functions in the special cases where these functions give good results.

For instance, we have the following theorem of Schertz. Note that condition (2) was forgotten in his papers.

**Theorem 1.** *Let* $(\mathfrak{a}_i)_{1\le i\le h(K)}$ *be a system of representatives of the ideal classes of* $K = \mathbb{Q}(\sqrt{D})$, *chosen to be primitive. Let* $\mathfrak{p}$ *and* $\mathfrak{q}$ *be ideals of* $K$ *of norm* $p$ *and* $q$ *respectively. Assume that:*

1. *The ideals* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are primitive ideals which are non-principal.*
2. *If both the classes of* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are of order 2 in the class group, these classes are equal.*
3. *For all* $i$, $\mathfrak{p}\mathfrak{q}\mathfrak{a}_i$ *is a primitive ideal.*
4. $e$ *is a positive integer chosen such that* $24 \mid e(p-1)(q-1)$.

*Set*

$$P(X) = \prod_{1\le i\le h(K)} \left( X - \left( \frac{\eta(\tau_i/p)\eta(\tau_i/q)}{\eta(\tau_i/pq)\eta(\tau_i)} \right)^e \right)$$

*where* $\mathfrak{a}_i\mathfrak{p}\mathfrak{q} = a_i(pq\mathbb{Z} + \tau_i\mathbb{Z})$.

*Then* $P(X) \in \mathbb{Z}[X]$, *it is irreducible in* $\mathbb{Z}[X]$ *and also in* $K[X]$, *its constant term is equal to* $\pm 1$, *and the field obtained by adjoining to* $K$ *a root of* $P$ *is the Hilbert class field of* $K$.

For similar results leading to the construction of ray class fields, see [21] and [22].

## 3. Applications and Software

3.1. **Applications.** Apart from the intrinsic interest of computing ray class fields, the main application of the above algorithms is the construction of new number fields, in particular number fields of small discriminant, or large tables of number fields having given Galois group. As already mentioned, all the implementations and the applicationss are joint work with F. Diaz y Diaz and M. Olivier.

- **Small discriminants**. We have found many number fields having smaller discriminants than previously known ones, and very close to the GRH bounds (often less than 1%). For example, in the totally complex case, J. Martinet in [16] gives a table of the best known fields for degree up to 80 (using similar methods, but more adapted to hand computation). We have obtained better fields for 10 cases ranging from degree 12 to degree 56 (we had in fact also obtained a better field in degree 10, but it was first found by Leutbecher and Niklash in [15] while searching for small Euclidean fields). For example, in degree 12, the totally complex field of smallest known discriminant is generated by the polynomial

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

whose root discriminant is only 0.843% above the GRH bound. I refer to [9] for the other examples and details.

- **Tables of octic fields.** We have made extensive systematic tables of all octic fields containing a quartic subfield, with more than 10000 fields per signature. In addition, we have computed *all* the minimum discriminants for the possible pairs Galois group, signature, for such fields. Some were missing from the tables obtained from the main computation, hence we extended the tables as needed, using the specific properties of the Galois group we were looking for.

In particular, we found a large number of nonisomorphic arithmetically equivalent fields (i.e. having the same Dedekind zeta function) corresponding to exactly 2 specific Galois groups in degree 8, and we also found many sets of nonisomorphic number fields having the same discriminant, the largest having 11 elements.

3.2. **Software.** Two packages can be used freely for the above computations:

The **KANT/KASH** package from Berlin, under the supervision of M. Pohst. This is available from:

`ftp.math.tu-berlin.de`

The **PARI/GP** package from Bordeaux, under my supervision (and now under the supervision of K. Belabas). This is available from:

`megrez.math.u-bordeaux.fr`

Mention should be also made of the much larger software package **MAGMA** which contains KANT and a part of PARI, under the supervision of J. Cannon in Sidney. Number theory is only a minor part of this package, which also contains functionalities for many other algebraic subjects, Although non-commercial, this package is not free, however.

Finally, the C++ software library **LiDIA** from Darmstadt under the supervision of J. Buchmann is also a remarkable package, and will soon contain functions for class field theory.

## References

[1] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), p. 355–380.

[2] G. Birkhoff, *Subgroups of Abelian groups*, Proc. Lond. Math. Soc. (2) **38** (1934-5), p. 385–401.

[3] L. Butler, *Subgroup Lattices and Symmetric Functions*, Memoirs of the A.M.S. **539** (1994).

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer-Verlag, Berlin, Heidelberg, New-York (1993).

[5] H. Cohen, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), p. 1681–1699.

[6] H. Cohen and F. Diaz y Diaz *A polynomial reduction algorithm*, Sém. Th. des Nombres Bordeaux (série 2), **3** (1991), p. 351–360.

[7] H. Cohen, F. Diaz y Diaz and M. Olivier, *Subexponential algorithms for class and unit group computations*, J. Symb. Comp. **24** (1997), p. 433–441.

[8] H. Cohen, F. Diaz y Diaz and M. Olivier, *Algorithmic methods for finitely generated Abelian groups*, J. Symb. Comp., to appear.

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

[10] H. Cohen and X. Roblot, *Computing the Hilbert class field of real quadratic fields*, Math. Comp., to appear.

[11] C. Fieker, *Computing class fields via the Artin map*, J. Symb. Comput., to appear.

[12] A. Gee, *Class invariants by Shimura's reciprocity law*, J. Théor. Nombres Bordeaux **11** (1999), 45–72.

[13] E. Hecke, *Lectures on the theory of algebraic numbers* GTM **77**, Springer-Verlag, Berlin, Heidelberg, New York (1981).

[14] A. Leutbecher, *Euclidean fields having a large Lenstra constant*, Ann. Inst. Fourier **35**, 2 (1985), p. 83–106.

[15] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, TUM Math. Inst. preprint **M8705** (1987).

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

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

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

[19] X.-F. Roblot, *Stark's Conjectures and Hilbert's Twelfth Problem*, J. Number Theory, submitted, and *Algorithmes de Factorisation dans les Extensions Relatives et Applications de la Conjecture de Stark à la Construction des Corps de Classes de Rayon*, Thesis, Université Bordeaux I (1997).

[20] R. Schertz, *Zur expliciten Berechnung von Ganzheitbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper*, J. Number Theory **34** (1990), p. 41–53.

[21] R. Schertz, *Problèmes de Construction en Multiplication Complexe*, Sém. Th. des Nombres Bordeaux (Séries 2), **4** (1992), p. 239–262.

[22] R. Schertz, *Construction of ray class fields by elliptic units*, J. Th. des Nombres Bordeaux **9** (1997), p. 383–394.

[23] N. Yui and D. Zagier, *On the singular values of Weber modular functions*, Math. Comp. **66** (1997), p. 1645–1662.

Henri Cohen
Laboratoire A2X
Institut Mathématiques Bordeaux
351 cours de la Libération
F-33405 Talence Cedex
*E-mail* : cohen@math.u-bordeaux.fr