# Solvability by radicals from a practical point of view

G. Hanrot[1] and F. Morain*[2]

[1] *Projet SPACE, INRIA Lorraine, 615, rue du Jardin Botanique, F-54602 Villers-les-Nancy Cedex, France,* hanrot@loria.fr

[2] *LIX École polytechnique, F-91128 Palaiseau CEDEX, FRANCE, morain@lix.polytechnique.fr*

**Abstract**

Any textbook on Galois theory contains a proof that a polynomial equation with solvable Galois group can be solved by radicals. We will use previous works by various authors with the aim of giving practical algorithms. In particular, we will use ingredients from algorithm group theory and algorithmic algebraic number theory. Finding a suitable way of representing algebraic integers will prove crucial. We first reduce the Galois problem to that of cyclic extensions of prime degree and then work out the radicals, using Girstmair's work. We give numerical examples of Abelian and non-Abelian solvable equations and apply the general framework to the construction of Hilbert class fields of imaginary quadratic fields.

## 1. Introduction

Galois's work has given the answer to one of the most difficult problems in algebra: classify all polynomials whose roots can be expressed by radicals. A polynomial has this property if and only if its Galois group is solvable. More recently [28], it has been shown that testing solvability can be done in polynomial time. It is very rare that a random polynomial has an interesting Galois group, let alone a solvable one. On the other hand, families of polynomials with solvable Galois groups are known from a theoretical point of view and we may want to explore them. The cyclotomic polynomials are one example, polynomials defining Hilbert class fields of imaginary quadratic fields are another one. Their use in primality proving in the ECPP algorithm was a motivation for our work (see Section 7).

What would be the ideal approach? Given $P(X)$ over some number field $\mathbb{M}$, compute its Galois group. If it is solvable, solve the equation $P(X) = 0$ by radicals. A lot of work has been done on the computation of Galois groups in the case $\mathbb{M} = \mathbb{Q}$. This task relies on the knowledge of the lattice of transitive subgroups of the symmetric group. All these have

*The second author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

been classified up to degree 15 and are available in systems such as MAGMA, GAP or KANT. Moreover, data bases of polynomials having these groups as Galois groups are also available [23]. The above-mentioned systems provide us not only the Galois group, but also its action on the roots of $P(X)$, without which we cannot do anything.

Assume now that the Galois group is solvable. We want to find representations of the roots of the polynomial by radicals. Let $L$ denote the splitting field of $P$. The overall scheme is to decompose the extension $L/\mathbb{M}$ into cyclic extensions of prime degree and then compute radicals for these extensions. The first part yields an interesting result already: It reduces the computation of the roots of an equation to that of equations of smaller degree.

For our algorithms to succeed, we also need the action of the Galois group on the roots of the polynomial, in such a way that we can perform operations on them, symbolically or numerically. This can be obtained as a byproduct of [28] (however difficult it might seem to implement it), or the classical approach dating back to Stauduhar [34] (see [11] for a recent article on the topic and the whole special issue in which it can be found), or from theoretical results (e.g., cyclotomic polynomials). Classically, floating point representations of the roots were used, but recently, $p$-adic computations were preferred due to their better numerical stability [36, 11].

The algorithms developped for computing with finite solvable groups make use of a powerful representation, called a *power-conjugate* representation. The programs computing Galois groups yield groups as permutation groups, that can be transformed into pc-representations. This representation makes it easy to find the intermediate extensions.

The computation of intermediate cyclic extensions can be viewed as a simplification of the algorithms used to find subfields of a given number field, as in [10, 22, 24], since in our case we know the Galois group and know where the subfields lie. Note also that subfield computations are often used to find information on the Galois group of the polynomial to speed up its computation (see [11]).

The approach we follow is classical. For instance, in [17, 19], Huang explains how to solve the $n$-th cyclotomic equation in polynomial time modulo ERH. In [18, 20], the construction is used to factor polynomials with Abelian Galois groups over finite fields. We can also find connections with the articles dealing with the simplification of nested radicals (see [27], [16]). The present paper can be seen as a self-contained guide to implement the ideas given in these papers (announced as [32] in [3§8.6]), adapting the algebraic-numerical approach of [12] for the radical part. It develops the ideas sketched in [14].

After reducing the problem to cyclic cases in a first part of the article, we explain how to solve the resulting equations by radicals. One of the problems we have to solve is to find a convenient and practical representation of algebraic integers. We will describe two of these: the defect one and the Hecke one which appeared to be superior for reasons that we will explain.

Numerical examples are given of all the phases, using cyclotomic polynomials, but also polynomials that define the Hilbert class fields of imaginary quadratic fields, and some non-abelian cases as well. We also give some benchmarks.

The emphasis of the article will be on practical algorithms that have been implemented and used on a large number of equations.

# 2. From solvable to cyclic extensions

### 2.1. Group theory

Galois theory states that an equation is solvable by radicals if and only if its Galois group is solvable. This means that there exists a sequence of groups $G = G_r \triangleright G_{r-1} \triangleright \ldots \triangleright G_1 \triangleright G_0 = \{1\}$ such that the quotients $G_{i+1}/G_i$ are abelian. In the case of a finite group, the quotients are finitely generated, and we can thus refine the sequence below to get a sequence with *cyclic* quotients of prime order. A group with such a sequence is called *polycyclic*. Any finite solvable group is thus polycyclic.

For all $i \in \{1, \ldots, r\}$, we shall denote by $g_i$ an element of $G_i$ such that $g_i G_{i-1}$ generates $G_i/G_{i-1}$.

Every element of $G$ then has a unique expression as $g_r^{a_r} \ldots g_1^{a_1}$, with $0 \leq a_i < p_i = [G_i : G_{i-1}]$. With these notations, the subgroup $G_i$ is exactly $\{g_i^{a_i} \ldots g_1^{a_1}, 0 \leq a_k < p_k\}$. We further define $\widehat{G}_i$ to be $\{g_r^{a_r} \ldots g_{i+1}^{a_{i+1}}, 0 \leq a_k < p_k\}$, so that $\widehat{G}_i \cdot G_i = G$ and $\widehat{G}_i \cdot < g_i >= \widehat{G}_{i-1}$.

Note also that for $k < i$ we have $g_k g_i = g_i g'$ with $g' \in G_{i-1}$, so that $g'$ can be written as $g_{i-1}^{l(i,k,i-1)} \ldots g_0^{l(i,k,0)}$. A presentation by generators and relations of $G$ is then simply given by the $p_i$ and the $l_{i,k,j}$. Such a presentation is called a *power conjugate presentation*. In the abelian case, we have $l_{i,k,j} = \delta_{k,j}$, and the $p_i$ are obtained from the invariant factors, given for instance by the SNF algorithm [5]. Otherwise, since the limiting step of our algorithm is the determination of the Galois group itself, due to the small size of the groups we have to deal with, it is a matter of routine for systems handling groups efficiently such as GAP or MAGMA to compute a power conjugate presentation of a Galois group given as a permutation group.

Conversely, given $(g_i, p_i, l_{i,k,j})$, we can construct the group $G$ (which is given by generators and relations), the subgroups $G_i$ and the sets $\widehat{G}_i$ just as above.

In the sequel, any solvable group $G$ will be assumed to be given by a power-conjugate presentation $(g_i, p_i, l_{i,k,j})$. We do not need the $l_{i,k,j}$ in the present paper, so we shall omit them.

### 2.2. The main theorems

The main theorem that we shall use is the following:

THEOREM 2.1: *Let $\mathbb{M}$ be a field and let $H(X)$ be an irreducible polynomial with coefficients in $\mathbb{M}$. Suppose $H$ has the solvable Galois group $G = (g_i, p_i)$ and splitting field $\mathbb{M}$. There exists a chain of subfields*

$$L = L_0 \supset L_1 \supset \ldots \supset L_r = \mathbb{M},$$

*with $L_i/L_{i+1}$ cyclic of prime order $p_{i+1}$.*

*Proof:* Put $L_i = L^{G_i}$. The main theorem of Galois theory asserts that we have a chain of inclusions as above, and that $L_i/L_{i+1}$ is Galois with group $G_{i+1}/G_i$. Note also that $L/L_i$ is Galois with group $G_i$, but $L_i/\mathbb{M}$ is Galois iff. $G_i \triangleleft G$, and if this is the case, the Galois group is isomorphic to $G/G_i$, itself isomorphic to $\widehat{G}_i$. Otherwise, $L_i$ comes with conjugate extensions $\xi L_i$. □

### 2.3. Building intermediate fields

Let $H(X)$ be an irreducible polynomial with coefficients in $\mathbb{M}$, and solvable Galois group $G = (g_i, p_i)$, and splitting field $\mathbb{M}(\theta)$.

In this section, we describe how to obtain a polynomial $Q_1 \in \mathbb{M}[Y]$, a root $y$ of which generate the extension $L_1/\mathbb{M}$, together with a factor $H_1(X, y)$ of $H$ over $L_1$, allowing one to get an expression for $\theta$ by solving an equation with cyclic Galois group $\mathbb{Z}/p_1\mathbb{Z}$. We summarize all this in the algorithm CyclicGalois at the end of this section.

Furthermore, at the end of this process, we are left with similar data for the polynomial $Q_1$, allowing one to continue the process until one gets defining polynomials for the full sequence of fields $(L_i)_{0\leq i\leq r}$. This inductive process is made explicit by the algorithm GaloisDecompose.

Let $x_1, \ldots, x_h$ be the roots of $H$, and fix $x$ as one of them. Recall that the subgroup $G_1$ is of order $p_1$, generated by $g_1$. Let $q_1$ be the cardinal of $\widehat{G}_1$.

The set $\widehat{G}_0 = \widehat{G}_1 \cdot < g_1 >$ acts on the set $\{x_1, \ldots, x_h\}$.

For $\xi \in \widehat{G}_1$, define the polynomials

$$U_\xi(X) = \prod_{k=1}^{p_1} (X - \xi g_1^k(x)) = X^{p_1} + \sum_{j=0}^{p_1-1} (-1)^{h-j} c_{\xi,j} X^j.$$

Obviously, we have $U_{\mathrm{id}} \in L[X]$, and $g_1^k U_{\mathrm{id}} = U_{\mathrm{id}}$ for all $k$. As a consequence, $U_{\mathrm{id}} \in L_1[X]$ (recall $L/L_1$ is Galois with group $< g_1 >$; note also that $U_{\mathrm{id}}$ generates $L/L_1$). It follows that $U_\xi \in \xi(L_1)[X]$.

We can now consider the polynomials

$$V_j(Y) = \prod_{\xi \in \widehat{G}_1} (Y - c_{\xi,j}).$$

It is easy to see that if we let $\tau \in G$, $\tau = \lambda g_1^k, \lambda \in \widehat{G}_1$ act on $V_j$, then $\tau$ acts on the $c_{\xi,j}$ as $\lambda$, and this just amounts to permute the terms of the product, hence $\tau V_j = V_j$ for all $\tau \in G$, hence $V_j \in \mathbb{M}[X]$.

Theorem 2.2: *We have $L_1 = \mathbb{M}[(c_{\mathrm{id},j})_{0\leq j<p_1}]$, Furthermore, for $\xi \in \widehat{G}_1$, we have $\xi(c_{\mathrm{id},j}) = c_{\xi,j}$.*

*Proof:* Put $L_1' = \mathbb{M}[(c_{\mathrm{id},j})_{0\leq j<p_1}]$. The inclusion $L_1' \subset L_1$ follows from the fact that $U_{\mathrm{id}} \in L_1[X]$.

The splitting field of $U_{\mathrm{id}}(X)$ over $L_1'$ is $L$, hence $[L : L_1'] \leq p_1 = [L : L_1]$, hence $L_1' = L_1$.

The last assertion is trivial. □

It remains to explain how one can find the polynomial $Q_1$ from the generating set $(c_{\mathrm{id},j})_{0\leq j<p_1}$. The easiest case arises when at least one of the $V_j$, say $V_1$, is irreducible over $\mathbb{M}$, since we can take $Q_1 = V_1$, with roots $y_\xi = c_{\xi,1}$.

This might not be the case. As an example, take the field generated over $\mathbb{Q}$ by $\alpha = \sqrt{\ell_1} + \sqrt{\ell_2} + \sqrt{r}$, where $\ell_1, \ell_2, \ell_3$ are e.g. distinct primes. Let $H$ be the minimal polynomial of this algebraic number (a so-called Swinnerton-Dyer polynomial, see e.g. [21]). The field is a degree 8 Galois extension of $\mathbb{Q}$, with group $(\mathbb{Z}/2\mathbb{Z})^3$. Take $\sigma_{\ell_1}$ be the extension of the non-trivial automorphism of $\mathbb{Q}(\sqrt{\ell_1})$ which acts trivially on $\mathbb{Q}(\sqrt{\ell_2}, \sqrt{\ell_3})$, and similarly for $\sigma_{\ell_2}, \sigma_{\ell_3}$. Then we can take as a sequence $G_3 = G \supset < \sigma_{\ell_2}, \sigma_{\ell_2}\sigma_{\ell_3} > = G_2 \supset < \sigma_{\ell_2}\sigma_{\ell_3} > = G_1 \supset 1$.

The computation of the field $L_1$ then involves computing $U_{\mathrm{id}}(X) = X^2 - (\alpha - \sigma_{\ell_2}\sigma_{\ell_3}(\alpha))X - \alpha\sigma_{\ell_2}\sigma_{\ell_3}(\alpha)$. Now $\alpha - \sigma_{\ell_2}\sigma_{\ell_3}(\alpha) = \sqrt{\ell_1}$, and $\alpha\sigma_{\ell_2}\sigma_{\ell_3}(\alpha) = \ell_1 - \ell_2 - \ell_3 - 2\sqrt{\ell_2\ell_3}$. The field we are looking for is $\mathbb{Q}(\sqrt{\ell_1}, \sqrt{\ell_2\ell_3})$, but none of the $c_{\mathrm{id},j}$ generates it by itself.

The group $G$ acts on the set $(c_{\mathrm{id},j})_{0\le j<p_1}$. Denote by $K_j$ the kernel of this action, so that $G_1 \subset K_j$. We have $L_1 \supset L^{K_j} = \mathbb{M}[c_{\mathrm{id},j}]$. A first solution is to find an integer linear combination $C(\lambda_1, \ldots, \lambda_{p_1}) := \sum_{j=0}^{p_1-1} \lambda_j c_{\mathrm{id},j}$ of the $c_{\mathrm{id},j}$ such that the action of $G$ on the $C^{\xi}(\lambda_1, \ldots, \lambda_{n_1})$ has kernel $G_1$. To each subgroup $K_j$ containing $G_1$ we can associate a sub-lattice of $\mathbb{Z}^{p_1}$. The set of invalid linear combinations is then a finite union of strict sublattices. Hence for almost all choices of the $\lambda_1, \ldots, \lambda_{p_1}$ we get a valid linear combination. In practice, if all the $V_j$ are reducible at some point, one can replace the polynomial $H$ by its Tschirnhaus tranform $H(X+1)$. After finitely many such steps (and in practice one should be enough) one comes to the situation where one of the $V_j$ is irreducible.

Assume now that at least one of the $V_j$, say $V_1$, is irreducible. Then, if we put $y = c_{\mathrm{id},1}$, there exists a polynomial $A_j(Y) = \sum_{r=0}^{q_1-1} a_{j,r} Y^r$ with coefficients in $\mathbb{M}$ such that

$$y^{(j)} := c_{\mathrm{id},j} = A_j(y) = \sum_{r=0}^{q_1-1} a_{j,r} y^r.$$

For all $\xi$, we have $c_{\xi,j} = \sum_{r=0}^{q_1-1} a_{j,r} c_{\xi,1}^r$. In other words, we know $A_j(Y)$ by the $q_1$ values it takes on $(c_{\xi,1})_{\xi\in\widehat{G}_1}$, and therefore we can recover its coefficients by Newton interpolation (see section 3 on how to recognize these coefficients as algebraic numbers). Finally, a factor of $H(X)$ over $L_1$ is $H_1(X,Y) := U_{\mathrm{id}}(X,Y) = X^{p_1} + \sum_{j=0}^{p_1-1} (-1)^{p_1-j} A_j(Y) X^j$.

A second solution is to first compute all the values $c_{\xi,j}^{(i)}$ corresponding to the extensions $L_i$ at once. Then, the equations for the $L_i$ are computed upwards. Since $L_i = L_{i+1}[(c_{\mathrm{id},j}^{(i)})_{1\le j\le p_i}]$ and $[L_i : L_{i+1}]$ is prime, for any $j$, either $c_{\mathrm{id},j}^{(i)} = c_{g_{i+1}^k,j}^{(i)}$ for all $k$, or the $c_{g_{i+1}^k,j}^{(i)}$ are pairwise distinct for $k < p_{i+1}$ and $L_{i+1} = L_i[c_{\mathrm{id},j}^{(i)}]$. One then just needs to compute $\tilde{V}_j(Y) = \prod_{k=1}^{p_{i+1}} (Y - c_{g_{i+1}^k,j}^{(i)}) \in L_{i+1}[Y]$, to recognize the coefficients of this polynomial as algebraic integers (see next section) and then the polynomial $Q_i$ defining $L_i$ is obtained as the resultant of $Q_{i+1}$ and $\tilde{V}_j$.

The first solution described above yields the following algorithm:

**procedure** CyclicGalois($f(X)$, $\mathcal{R}$, $p$, $q$)
INPUT: $\mathcal{R} = (x_1, x_2, \ldots, x_{pq})$ the roots of $f(X)$ such that $g_1(x_i) = x_{i+q \bmod pq}$.
OUTPUT: the defining polynomial of $L_1$ with its roots; a factor $U_1(X,Y)$ of $f(X)$ over $L_1$.
0. $T \leftarrow 0$.
1. **for** $i = 1..q$ **do** compute $U_i(X)$.
2. **for** $j = 0..p-1$ **do** compute $V_j(Y)$.
3. **if** all the $V_j(Y)$ are reducible, put $T \leftarrow T+1$ ; $f(X) \leftarrow f(X+T)$, $x_i \leftarrow x_i - T$ for all $i$ and go to 1.

4. Select one of the $V_j(Y)$ which is irreducible, put $Q_1(X) = V_{j_0}(Y)$.

5. Compute the polynomials $A_j(Y)$ for $0 \le j < p$ using Newton interpolation (warning : find the $c_{\xi,j}$ computed during the first iteration, with $T = 0$).

6. return $Q_1(Y)$, its roots $(c_{l,j_0})_{1 \le l \le q}$ (in this precise order), and $U_1(X, Y)$.

### 2.4. The final algorithm

Using the power-conjugate presentation of $G$, we can order $G$ in the following way. For an ordered sequence $A = (a_1, \ldots, a_k)$ of $G$, and an element $a$ of $G$ of order $e$, denote by $a \otimes A$ the ordered sequence of elements

$$(a_1, \ldots, a_k, aa_1, aa_2, \ldots, aa_k, \ldots, a^{e-1}a_1, \ldots, a^{e-1}a_k).$$

Starting from the subgroup $< g_1 >= (1, g_1, g_1^2, \ldots)$, we re-build $G$ as an ordered set as $g_r \otimes (g_{r-1} \otimes (\cdots \otimes < g_1 >) \cdots)$. Using this, it is easy to see that

$$\widehat{G}_1 \sim g_r \otimes (\cdots \otimes < g_2 >).$$

Moreover, this way of representing $G$ enables us to go further, since if the roots in the input of CyclicGalois follow this ordering (which is compatible with the requirement $g_1(x_i) = x_{i+q \bmod pq}$), the roots in the output of CyclicGalois are left in the order corresponding to the action of $\widehat{G}_1$ ordered as above. We can thus peel the cyclic component $< g_2 > \subset \widehat{G}_1$ by using CyclicGalois, and so on. We can now describe the final algorithm that uses CyclicGalois as a primitive.

**procedure** GaloisDecompose($H(X)$, $\mathcal{R}$, $G$)
INPUT: $H(X)$ of degree $h$ and solvable Galois group $G$;
OUTPUT: the cyclic decomposition of $H$ over $\mathbb{M}$ and the corresponding factors and roots.

1. [Find structure] obtain a polycyclic generating sequence for $G$ as $t_1$, $t_2$, …, $t_l$, where $t_i$ is of order $h_i$.

2. [Refine structure] **for** $i = 1..r$ **do**
   2.1 factor $h_i = \prod_{j=1}^{s} p_{i,j}$;
   2.2 replace $(t_i, h_i)$ by $[(t_i^{\prod_{j=1}^{s-1} p_{i,j}}, p_{i,s}), (t_i^{\prod_{j=1}^{s-2} p_{i,j}}, p_{i,s-1}), \ldots, (t_i^{p_{i,1}}, p_{i,2}), (t_i, p_{i,1})]$
   { at this point, we have a polycyclic sequence with cyclic quotients of prime order, say $g_1, \ldots, g_r$ with $g_i^{p_i} \in < g_1, \ldots, g_{i-1} >$.}

2. [Rebuild] $\Gamma := < id >$; **for** $i = r - 1$ **to** $0$ **do** $\Gamma := g_i \otimes \Gamma$.

3. [Build roots of $H(X)$ in the right order] take $x$ in $\mathcal{R}$ and replace $\mathcal{R}$ by the sequence $(\gamma(x))$ for $\gamma$ in $\Gamma$.

4. $k := 1$; $Q_0(Y_0) = H(Y_0)$;

5. [Solve] **for** $i = 1..r$ **do**
   { at this point, $\mathcal{R}$ contains the roots of a polynomial on which $\widehat{G}_i$ acts}
   $Q_i(Y_i), \mathcal{R}, H_i(Y_i, Y_{i-1}) :=$
   CyclicGalois($Q_{i-1}(Y_{i-1})$, $\mathcal{R}$, $p_i$, $h/p_i$);

6. [End] return $(H_i(Y_i, Y_{i-1}))_{0 \le i < k}$.

We have in fact proven that:

Proposition 2.1: *All the roots of $H(X)$ over $\mathbb{M}$ are given as solutions of the system of equations:*

$$H_{k-1}(Y_{k-1}) = 0, H_{k-2}(Y_{k-2}, Y_{k-1}) = 0, \ldots, H_0(Y_0, Y_1) = 0.$$

## 3. Representing algebraic integers

Finding integral bases for an algebraic extension is no easy work in general, except in some special cases such as quadratic or cyclotomic number fields. If we are not in such a fortunate case, we can use one of two representations, the power basis one or the Hecke one. We will explain later on the connections with our problem.

We suppose $K/\mathbb{Q}$ is an algebraic extension of degree $q$ defined by a monic irreducible polynomial $Q(Y) = Y^q + \sum_{i=0}^{q-1} q_i Y^i$ with integer coefficients and roots $\alpha = \alpha_1$, $\alpha_2$, ..., $\alpha_q$ (in $\mathbb{C}$). We put $|Q(Y)| = (\sum_i q_i^2)^{1/2}$. We will denote by $\mathcal{O}_K$ the ring of integers of $K$.

We let $\theta$ denote an algebraic integer of $K$ and $\theta_i$ its conjugates. We put $\|\theta\| = \max_{1\leq i\leq q} |\theta_i|$.

### 3.1. Using a power basis

Write $\theta$ as $A(\alpha_1) = \sum_{r=0}^{q-1} a_r\alpha^r$, and the $a_r$'s are elements of $\mathbb{Q}$. It is possible to write them as $b_r/\delta$ where $\delta$ is an integer called the *defect* of the power basis $\{1, \alpha_1, \ldots, \alpha_1^{q-1}\}$. This number is costly to compute in general, but is known to divide the largest square factor of the discriminant of $P(X)$. From this, we conclude that $\delta a_r$ is an integer of $\mathbb{Q}$, that we are able to recognize, if computations are carried out with sufficiently high precision.

In our situation, we want to factor a polynomial $H(X)$ in $\mathcal{O}_K[X]$, and we can find bounds on the coefficients of its factors. If $F(X) = \beta_n X^n + \beta_{n-1}X^{n-1} + \cdots + \beta_0$ and $\beta_i = \sum_{j=0}^{p-1} b_{ij}\alpha^j$, we put $\|F(X)\| = \max_i(\sum_j b_{ij}\alpha^j)^{1/2}$. We find in [35] (see also [26]) the following result.

Theorem 3.1: *Let $H(X) \in \mathcal{O}_K[X]$ and $\beta$ one of its roots. Then $\|\beta\| \leq 1 + \|H(X)\|$.*

*Assume $H(X)$ is monic and $U(X) = \sum_i u_i X^i$ is a factor of $H(X)$ in $\mathcal{O}_K[X]$, where $\delta u_i = \sum_{j=0}^{q-1} u_{i,j}\alpha^j$. Then*

$$|u_{i,j}| \leq \delta \binom{q}{i} \|H(X)\| |Q(Y)|^q (\mathrm{disc}(Q))^{-1/2}.$$

### 3.2. The Hecke representation

When the discriminant of $Q(Y)$ is easily factored, then the defect approach works well. In the other cases, we can use a better representation, which is based on the following Lemma [15].

Lemma 3.1: *Any algebraic integer $\theta$ in $K$ may be written as*

$$\theta = \frac{N(\alpha)}{Q'(\alpha)}$$

*where $N(Y)$ is a polynomial with rational integer coefficients.*

*Proof:* Put

$$N(Y) = \sum_{i=1}^{q} \theta_i \frac{Q(Y)}{Y - \alpha_i}.$$

It is clear that $N(Y)$ has integral coefficients, since $Q(Y)/(Y-\alpha_i)$ has and $\theta_i$ is an integer. Moreover the coefficients are in $\mathbb{Q}$ by Galois theory. Finally $N(\alpha_1) = \theta_1 Q'(\alpha_1)$ as required. $\square$

Note that since $Q$ is irreducible, $Q'(\alpha_i)$ is non-zero. The required precision of the computations is easily seen to depend on $|Q'(\alpha_i)|$ which is in general much smaller than $\mathrm{disc}(Q)$ (remember that $|\mathrm{disc}(Q)| = \prod_i |Q'(\alpha_i)|$).

Note that the polynomial $N$ can be easily computed if we know the values of the $\theta_i$'s since $N(\alpha_i) = \theta_i Q'(\alpha_i)$, so that we can interpolate $N$.

Using elementary arguments, one can show that the size of $N$ is not very much larger than that of $Q$ (recall that classically the bound we get on $g_k$ is $|q_k| \leq \binom{q}{k} \|\alpha\|^k$).

PROPOSITION 3.1: *Write* $N(Y) = \sum_{k=0}^{q-1} n_{q-1-k} Y^k$. *Then*

$$|n_k| \leq q \binom{q}{k} \|\alpha\|^{k+1} \|\theta\|.$$

### 3.3. Back to Galois

Our basic step in GALOISDECOMPOSE is the construction of an intermediate field $K$ defined by a polynomial $Q(Y)$ whose coefficients must be integers in $\mathbb{M}$. The coefficients of $V$ are given as complex floating point numbers. If $\mathbb{M} = \mathbb{Q}$, recognizing integers is easy with enough precision. Otherwise we need all the conjugates of the coefficients that we will recognize as integers over $\mathbb{M}$ using one of the approaches just described. This implies that we need these conjugates in a suitable form, and more precisely, that we dispose of some representation of the embeddings of $\mathbb{M}$ in $\mathbb{C}$, that we will note $(\rho_i)_{1 \leq i \leq m}$ if $m = [\mathbb{M} : \mathbb{Q}]$.

We will give an example later on (see Section 7.3).

## 4. Implementations

### 4.1. Representation of the roots

We need a representation of the roots of $H(X)$ suitable for our computations, meaning that we also require the action of the Galois group on the roots to be computable. The most obvious representation of the roots of $H(X)$ are as floating point numbers to some precision. Alternatively, we can use algebraic (polynomial) expressions for the roots of $H(X)$, coming for example from a list of automorphisms of $L$, obtained in a variety of ways: brute force factorization of $H$ over $L$ (see [29]) or more subtle methods ([1], [2]). One can also use $p$-adic methods, in the continuation of Galois group computations.

The floating point approach is natural in the construction of Hilbert class fields, see below. The algebraic approach might be very costly. The choice of representation depends also on the language the algorithms are to be implemented in.

We have written several implementations of our ideas. Historically, the first program was written in MAPLE, in connection with Hilbert class field computations. There, floating numbers are used. The program is rather slow, but works well in a variety of cases and it is still used for precomputing data for ECPP (see below). We also reprogrammed it in MAGMA using floating point numbers or $p$-adic numbers, since the input of our program is the output of the function `GaloisGroup` which gives us either result. This implementation is almost stand-alone, since we can benefit from the huge effort put in Galois group computation and more generally group handling. Another implementation was done in Pari. In these last two cases, the program are much faster.

### 4.2. Building cyclic extensions

The core of the algorithm is procedure CYCLICGALOIS. In a first step, we have to compute the polynomials $U_i$'s. We can compute a bound on the coefficients of $U_i$ since we know their roots $(x_{kq+i})$. Denoting $\|x\| = \max |x_i|$, it is easy to find the bound

$$\max \binom{d}{k} \|x\|^k \tag{1}$$

for the coefficients $c_{i,k}$ for all $i$ and $k$. Though generally pessimistic, this bound is realistic.

When using the power basis representation, one chooses $V(X)$ with the smallest possible defect. In real life, computing a discriminant may become costly as the degree increases or the base field is not $\mathbb{Q}$. Among all the formulas for computing the discriminant, the most convenient one appeared to be

$$\mathrm{disc}(Q) = (-1)^{q(q-1)/2} \prod_{i=1}^{q} Q'(\alpha_i)$$

which has then to be recognized as an algebraic integer in the base field. To get more precision, we can refine the roots of the polynomial we are considering via an ordinary Newton iteration if needed.

#### *4.2.1. Checking the results*

Finally, we can check our computations by computing the resultant of $Q_1(Y)$ and $U_1(X, Y)$ which must coincide with $f(X)$. In order to speed up this computation, we may as well replace this by a probabilistic version such as checking that

$$\mathrm{Resultant}_Y(U_1(x_0, Y), Q_1(Y)) = f(x_0) \bmod p$$

for several small primes $p$ and integers $x_0$.

Note also that in many cases (cyclotomic, Hilbert class fields), we know how $f(X)$, $Q_1(Y)$ should split modulo primes. This can be used to have another check of the results.

## 5. A first set of numerical examples

In this section, we give numerical examples obtained with GALOISDECOMPOSE.

### 5.1. Cyclotomic extensions

This case is well known, but we give it as an easy example. Our approach recovers the well known Gauss periods of such equations.

Let $m$ be an integer $> 1$ and let $\zeta_m = \exp(2i\pi/m)$ denote an $m$-th root of unity and $\Phi_m(X)$ its minimal polynomial:

$$\Phi_m(X) = \prod_{(a,m)=1} (X - \zeta_m^a).$$

The Galois group of $\Phi_m(X)$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$ which is Abelian. The action corresponding to element $a$ of $(\mathbb{Z}/m\mathbb{Z})^*$ sends $\zeta_m$ on $\zeta_m^a$.

Let us give a non-trivial example. Take $(\mathbb{Z}/40\mathbb{Z})^*$ which has structure $C(2) \times C(2) \times C(4)$ and is equal to $< 31 > \times < 11 > \times < 17 >$. Letting $\zeta$ denote a primitive 40-th root of unity, the roots of $\Phi_{40}(X)$ correctly ordered are:

$$[\zeta^{17}, \zeta^9, \zeta^{33}, \zeta, \zeta^{27}, \zeta^{19}, \zeta^3, \zeta^{11}, \zeta^7, \zeta^{39}, \zeta^{23}, \zeta^{31}, \zeta^{37}, \zeta^{29}, \zeta^{13}, \zeta^{21}].$$

We will decompose $\mathbb{Q}(\zeta)$ as a tower of four degree 2 extensions. We begin with:

$$U_1(X) = (X - \zeta^{17})(X - \zeta^7),$$

$$U_2(X) = (X - \zeta^9)(X - \zeta^{39}),$$

$$\ldots$$

$$U_8(X) = (X - \zeta^{11})(X - \zeta^{21})$$

yielding:

$$V_1(Y) = Y^8 + 2Y^7 + 3Y^6 + 4Y^5 + 5Y^4 + 4Y^3 + 3Y^2 + 2Y + 1,$$
$$V_2(Y) = Y^8 + 2Y^6 + 4Y^4 + 8Y^2 + 16.$$

We select $Q_1 := V_2(Y)$ since $V_1(Y) = (Y^4 + Y^3 + Y^2 + Y + 1)^2$ is not irreducible. The roots of $V_2$ in the correct order are:

$$\zeta^{17} + \zeta^7, \zeta^9 + \zeta^{39}, \ldots, \zeta^{11} + \zeta^{21}.$$

Continuing this way, we finally find:

$$H_3 = Y_3^2 - 2Y_3 - 4, H_2 = Y_2^2 - Y_3Y_2 + 4,$$

$$H_1 = Y_1^2 + Y_2, H_0 = Y_0^2 - Y_1Y_0 + 1/2Y_1^2.$$

### 5.2. Non Abelian cases

Our first example comes from Allombert's paper [2], in which the Galois group of the polynomial

$$\begin{aligned} H(x) &= x^{21} - 7x^{20} - 21x^{19} + 238x^{18} - 245x^{17} - 1848x^{16} \\ &\quad +4732x^{15} + 1861x^{14} - 18536x^{13} + 16856x^{12} + \\ &\quad 14819x^{11} - 32431x^{10} + 8897x^{9} + 16660x^{8} \\ &\quad -13533x^{7} + 392x^{6} + 3514x^{5} - 1547x^{4} \\ &\quad +161x^{3} + 49x^{2} - 14x + 1. \end{aligned}$$

is computed.

This Galois group is isomorphic to the semidirect product $C(7) \ltimes C(3)$, generated by $\sigma_1$ and $\sigma_2$, with $\sigma_2\sigma_1 = \sigma_1\sigma_2^2$. If the roots (all real) of $T$ are numbered in increasing order, $\sigma_1$ and $\sigma_2$ are given as product of cyclic permutations as

$$\begin{aligned} \sigma_1 &= (1,10,2)(3,11,7)(4,8,6)(5,15,21) \\ &\quad (9,13,14)(12,17,20)(16,19,18), \\ \sigma_2 &= (1,6,14,5,17,11,16) \\ &\quad (2,13,12,18,8,21,3) \\ &\quad (4,7,9,19,15,10,20). \end{aligned}$$

The right sequence of subgroups for $G$ is $G \triangleright < \sigma_2 > \triangleright 1$, since $< \sigma_1 >$ is not a normal subgroup of $G$.

Hence we have

$$\begin{aligned} U_{\mathrm{id}}(X) &= (X-\alpha_1)(X-\alpha_5)(X-\alpha_6)(X-\alpha_{11})(X-\alpha_{14})(X-\alpha_{16})(X-\alpha_{17}) \\ U_{\sigma_1}(X) &= (X-\alpha_2)(X-\alpha_3)(X-\alpha_8)(X-\alpha_{12})(X-\alpha_{13})(X-\alpha_{18})(X-\alpha_{21}) \\ U_{\sigma_1^2}(X) &= (X-\alpha_4)(X-\alpha_7)(X-\alpha_9)(X-\alpha_{10})(X-\alpha_{15})(X-\alpha_{19})(X-\alpha_{20}). \end{aligned}$$

All the corresponding polynomials $V_j$ happen to be irreducible, so we can take e.g. $H_1 := V_1(Y_1) = Y_1^3 - 7Y_1^2 + 49$, and we obtain

$$\begin{aligned} H_0(Y_0, Y_1) = \; Y_0^7 \; & -Y_1Y_0^6 + (3Y_1^2 - 6Y_1 - 42)Y_0^5 - (5Y_1^2 - 14Y_1 - 63)Y_0^4 \\ & -(7Y_1^2 - 17Y_1 - 91)Y_0^3 + (12Y_1^2 - 33Y_1 - 147)Y_0^2 \\ & -(5Y_1^2 - 15Y_1 - 56)Y_0 + 4Y_1^2/7 - 2Y_1 - 5. \end{aligned}$$

We give a second example. A root of the polynomial

$$\begin{aligned} S(x) &= x^{12} - 4x^{11} - 32x^{10} + 131x^{9} + 313x^{8} \\ &\quad -1395x^{7} - 949x^{6} + 5344x^{5} + 575x^{4} - 5817x^{3} \\ &\quad -1300x^{2} + 288x + 64 \end{aligned}$$

defines the Galois closure of the field generated by a root of $x^4 - 17x^2 - 31x + 13$. $S$ has Galois group $A_4$, and is generated by $\sigma_1, \sigma_2, \sigma_3$ of order 3, 2 and 2, with the relations $\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_3$, $\sigma_3\sigma_1 = \sigma_1\sigma_2$, $\sigma_3\sigma_2 = \sigma_2\sigma_3$. Again, if we order the (all real) roots of $S$ increasingly, the $\sigma_i$ are given as

$$\begin{aligned}
\sigma_1 &= (1,2,4)(3,12,11)(5,7,8)(6,10,9),\\
\sigma_2 &= (1,10)(2,7)(3,4)(5,12)(6,8)(9,11),\\
\sigma_3 &= (1,5)(2,11)(3,8)(4,6)(7,9)(10,12).
\end{aligned}$$

A polycyclic corresponding to $G$ is $G \rhd <\sigma_2, \sigma_3> \rhd <\sigma_3> \rhd 1$.

We get for instance $U_{\mathrm{id}}(X) = (X - \alpha_1)(X - \alpha_5)$, and the $V_i$ are

$$\begin{aligned}
V_1(Y_1) &= Y_1^6 - 4Y_1^5 - 33Y_1^4 + 33Y_1^3 + 124Y_1^2 + 60Y_1 + 8,\\
V_2(Y_1) &= Y_1^6 - Y_1^5 - 150Y_1^4 - 315Y_1^3 + 892Y_1^2 - 480Y_1 + 64.
\end{aligned}$$

Take $Q_1 = V_1(Y_1)$. We get

$$H_0(Y_0, Y_1) = Y_0^2 - Y_1Y_0 + (87Y_1^5 - 374Y_1^4 - 2759Y_1^3 + 3697Y_1^2 + 9682Y_1 + 2324)/12.$$

During the next step, we get again two irreducible $V_i'$, with

$$\begin{aligned}
V_1' &= Y_2^3 - 4Y_2^2 - Y_2 + 11\\
V_2' &= Y_2^3 + 32Y_2^2 + 12Y_2 - 8,
\end{aligned}$$

both irreducible. Take $H_2 = V_2'$, we obtain $H_1(Y_1, Y_2) = Y_1^2 - Y_2Y_1 - 6Y_2^2 + 4Y_2 + 20$.

## 6. Solving by radicals

Using the preceding sections, we need to concentrate on solving prime degree cyclic equations by radicals. For this, we follow [12], in the continuation of [31]. We give the details so as to make the article self-contained.

Suppose that $d$ is a prime number. Let $f(X)$ be a monic irreducible polynomial of degree $d$ in $L_1[X]$ of cyclic Galois group $\Gamma = <\phi>$, and splitting field $L$. We suppose that the roots of $f$ are $x_1, \ldots, x_d$, ordered in a cyclic way:

$$\phi(x_j) = x_{j+1} \text{ if } j < d \text{ and } \phi(x_d) = x_1. \tag{2}$$

We make the conventions that $x_i = x_j$ whenever $i \equiv j \bmod d$ and that $0 \bmod d = d$.

Let $\zeta$ be a primitive $d$-th root of unity (e.g. $\zeta = \exp(2i\pi/d)$). We consider the following diagram of extensions:

$$\begin{tikzcd}
 & L(\zeta) \arrow[d, dash, "\tilde{\Gamma}"] \\
L \arrow[ur, dash] \arrow[d, dash, "\Gamma"'] & L_1(\zeta) \\
L_1 \arrow[ur, dash, "\Lambda"'] &
\end{tikzcd}$$

We shall assume that $\mathbb{Q}(\zeta)$ and $L_1$ are linearly disjoint, so that $[L_1(\zeta) : L_1] = d - 1$. See at the end of the section for modifications if this is not the case.

Let $m = [L_1 : \mathbb{Q}]$ and $\{\beta_1, \ldots, \beta_m\}$ be an integral basis of $L_1$. Furthermore, let $\{\rho_1, \ldots, \rho_m\}$ be all embeddings of $L_1 \to \mathbb{C}$.

Together with $f$, it is necessary to consider also the polynomials $\rho_i(f)$, with roots $x_1^{(i)}, \ldots, x_d^{(i)}$, the $x^{(i)}$ being ordered so that $\phi(x_k^{(i)}) = x_{k+1}^{(i)}$, $k < d$, and $\phi(x_d^{(i)}) = x_1^{(i)}$. We can then extend $\rho_i$ to an embedding $\tilde{\rho}_i$ of $L(\zeta)$ into $\mathbb{C}$ by $\tilde{\rho}_i(x_j) = x_j^{(i)}$, $\tilde{\rho}_i(\zeta) = \zeta$.

The extension $L(\zeta)/L_1(\zeta)$ is Abelian, of Galois group $\tilde{\Gamma}$ isomorphic to $\Gamma$, with generator $\tilde{\phi}$ given by $\tilde{\phi}(x_j) = \phi(x_j)$ and $\tilde{\phi}(\zeta) = \zeta$. The extension $L_1(\zeta)/L_1$ is also Abelian and its Galois group is $\Lambda = \{\lambda_1, \ldots, \lambda_{d-1}\}$ where $\lambda_k(\zeta) = \zeta^k$.

Put:

$$y_k = \sum_{j=1}^{d} x_j \zeta^{-jk}, 1 \leq k \leq d. \tag{3}$$

We can recover the $x_j$'s from the $y_k$ via:

$$x_j = \frac{1}{d} \sum_{k=1}^{d} y_k \zeta^{jk}. \tag{4}$$

From their definition, we see that the $y_k$'s are algebraic numbers of $L(\zeta)$. The $y_k$'s for $k < d$ cannot be all zero, since otherwise, we would have: $x_1 = \cdots = x_d = y_d/d$. Suppose that $y_1 \neq 0$ (If $y_k \neq 0$, we can replace $\zeta$ by $\zeta^k$). Put $z_k = y_1^{d-k} y_k$, $1 \leq k \leq d$. In particular, we get $y_1^d = z_1$ and

$$\forall k, y_k = \left(\frac{z_k}{z_1}\right) y_1^k. \tag{5}$$

We deduce

$$\forall j, dx_j = z_d + y_1\zeta^j + \sum_{k=2}^{d-1} \left(\frac{z_k}{z_1}\right) (y_1\zeta^j)^k. \tag{6}$$

Solving $f(x) = 0$ is thus reduced to the computation of the $z_k$'s. Using the fact that $\tilde{\phi}(y_k) = \zeta^{-k} y_k$, one proves that $z_k$ lives in $L_1(\zeta)$. Moreover, writing $z_k = \sum_{j=1}^{d} c_{kj} \zeta^{-j}$, where $c_{kj}$ is an element of $L_1$, the conjugates of $z_k$ in $L_1(\zeta)$ are:

$$\lambda_l(z_k) = \sum_{j=1}^{d} c_{kj} \zeta^{-jl}, 1 \leq l \leq d. \tag{7}$$

Putting $c_k d = 0$ and solving for the $c_{kj}$, we get

Proposition 6.1: *For all $k$, $1 \leq k \leq d$, and all $j$, $1 \leq j \leq d$, we have*

$$dc_{kj} = \sum_{l=1}^{d} \lambda_l(z_k) \zeta^{jl}, 1 \leq j < d. \tag{8}$$

*Moreover $dc_{kj}$ is an algebraic integer of $L_1$, since it is a combination of algebraic integers.*

We have also: $c_{kd} = 0 = \sum_{i=1}^{d} \lambda_k(z_i)$, hence:

$$dc_{kj} = \sum_{l=1}^{d-1} \lambda_l(z_k)(\zeta^{jl} - 1), 1 \leq j < d. \tag{9}$$

At this point, we have to recognize the $dc_{kj}$ as algebraic integers of $L_1$, a task we already encountered. Using the integral basis of $L_1/\mathbb{Q}$, we can write:

$$\forall k, dc_{kj} = c_{kj}^{(1)}\beta_1 + \cdots + c_{kj}^{(m)}\beta_m,$$

with $c_{kj}^{(i)}$ in $\mathbb{Z}$. Applying $\tilde{\rho}_i$ to (9), we get the linear systems (one for each of the $c_{kj}$) of equations

$$\begin{aligned}\forall i, \textstyle\sum_{r=1}^{m} c_{kj}^{(r)} \rho_i(\beta_r) &= \rho_i(dc_{kj}) \\ &= \textstyle\sum_{l=1}^{d-1} \tilde{\rho}_i(\lambda_l(z_k))(\zeta^{jl} - 1).\end{aligned} \tag{10}$$

Note that the $\tilde{\rho}_i(\lambda_l(z_k))$ can easily be evaluated since

$$\tilde{\rho}_i(\lambda_l(y_k)) = \sum_{j=1}^{d} x_j^{(i)} \zeta^{-jkl}.$$

Finding the expression for $z_k$ boils down to solving $d^2$ linear systems of size $m \times m$, with the same matrix, whose inverse can be computed once and for all.

**Remark.** If $[L_1(\zeta) : L_1] := t \neq d - 1$, there is one major difficulty: we need to know the conjugates of $\zeta$ over $L_1$, i.e., $\lambda_l(\zeta)$. But since $d$ is prime, $(\mathbb{Z}/d\mathbb{Z})^*$ is cyclic, and hence there is only one subgroup $\{1 = \ell_1, \ell_2, \ldots, \ell_t\}$ of order $t$, and the conjugates of $\zeta$ over $L_1$ are $\zeta, \zeta^{\ell_2}, \ldots, \zeta^{\ell_t}$. We can then replace $z_k = \sum_{j=1}^{d} c_{kj}\zeta^{-j}$ by $z_k = \sum_{j=1}^{t} c_{kj}\zeta^{-\ell_j}$, The argument then runs smoothly, and we only have to solve $dt$ systems of size $m \times m$.

## 7. Hilbert class fields

This part of the article was the original motivation for our work, before we realized it could be extended to the general solvable case. This section will give examples of Galois extension over number fields which are not simply $\mathbb{Q}$.

The theory of Hilbert class fields is very rich and we cannot give details here. We refer the reader to [7, 8, 9, 5] for more details. Our interest in constructing such objects is related to primality proving (see [3]), where the reader can find more motivation. Basically, we will compute a generating polynomial for a Hilbert class field and then solve the equation by radicals, which can be seen as a top-down computation. Note that a bottom-up computation would be to construct cyclic extensions of prime degree of quadratic fields: It has been the subject of the articles [13, 25, 30].

### 7.1. Theoretical setting

The only thing we need to know is that we are given a polynomial $H_D(X)$ corresponding to the imaginary quadratic field $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$ and class number $h =$

$h(-D)$. This polynomial defines a Galois extension called the *Hilbert class field* $\mathbf{K}_H$ of $\mathbf{K}$, it is the maximal unramified Abelian extension of $\mathbf{K}$. We can also compute the roots of $H_D(X)$ as floating point numbers and we know the action of the Galois group on the roots (see [3] for more details). The Galois group is isomorphic to the class group $\mathrm{Cl}(-D)$ of $\mathbf{K}$: It is Abelian, and if $h$ is small, computing an SNF is easy, and very often it is cyclic (following the Cohen-Lenstra heuristics [6]). The cases where it is not is mostly dominated by the case where $D$ has a large number of prime factors, forcing a large 2-Sylow subgroup. This case corresponds to a large number of genera in the class group and yields a large number of intermediate quadratic fields leading to the genus field of $\mathbb{Q}(\sqrt{-D})$. In this case, an algorithm has already been explained in [3§7.3]. We will give later on an example of decomposition using the (real) genus field as the base field instead of $\mathbb{Q}$.

We are now ready to apply the machinery developped in the preceding sections to this case. Note that since $\mathbf{K}_H/\mathbf{K}$ is unramified, for any intermediate field $\mathbf{K}_H \supset L \supset \mathbf{K}$, the discriminant of $L$ is $\Delta(L) = (-D)^{[L:\mathbf{K}]}$ and that all defining polynomials $Q_1(X)$ of $L$ have discriminant $\delta^2\Delta(L)$ for some rational integer $\delta$ (we can be more precise by studying the prime factors of $D$).

Remember that we will first decompose our Galois group as cyclic extensions of prime degree. Then, we will find roots of our polynomials by radicals.

### 7.2. Solving $H_1(X, Y)$ by radicals

We content ourselves with the case where $\mathrm{Cl}(-D)$ is cyclic of composite order.

We assume that $H_1(X, Y)$ is a degree $p$ polynomial in $X$ with coefficients in the field $L_1(Y) = \mathbf{K}[Y]/(Q_1(Y))$ where $Q_1(Y)$ is a degree $q$ (not necessarily prime) polynomial with rational integer coefficients. The polynomial $H_1$ is a factor of our polynomial $H(X)$ of degree $pq$ and roots $v_1, \ldots, v_{pq}$ (ordered in the usual way). Remember that the roots of the polynomials $(U_i(X))_{1\le i\le q}$ are $x_{i,1}, \ldots, x_{i,p}$ where $x_{i,j} = v_{i+(j-1)q}$ for $1 \le j \le p$. The roots of $Q_1$ are $w_1, \ldots, w_q$ where $w_i = \mathcal{S}(x_{i,1}, \ldots, x_{i,p})$, in which $\mathcal{S}$ designates a symmetrical function of the input. For ease of notation, the roots of $H_1$, namely the $x_{1,j}$ will be renamed $x_j = x_{1,j}$.

We denote as usual $\sigma$ the Galois action $v_1 \mapsto v_2 \mapsto \cdots \mapsto v_{pq} \mapsto v_1$. The automorphism $\psi = \sigma$ generates $\mathrm{Gal}(L_1/\mathbf{K})$. We compute $\psi(w_i) = w_{i+1}$ since $\psi(w_i) = \mathcal{S}(\psi(x_{i,1}), \ldots)$ and $\psi(v_i) = \sigma(v_i) = v_{i+1}$.

Remember that an integral basis of $\mathbf{K}$ is $\{1, \omega\}$ where $\omega = (1 + \sqrt{-D})/2$ if $D$ is odd and $\omega = \sqrt{-D/4}$ otherwise. Denote by $\tau$ the ordinary complex conjugation that sends $\sqrt{-D}$ onto $-\sqrt{-D}$. The extension $L_1/\mathbb{Q}$ is generalized dihedral and has Galois group the semi-direct product of $< \tau >$ and $< \psi >$.

We will take as integral basis for $L_1/\mathbb{Q}$ the numbers

$$\beta_i = \begin{cases} w_1^{i-1} & \text{for } 1 \le i \le q, \\ \omega w_1^{i-1} & \text{for } q+1 \le i \le 2q. \end{cases}$$

The embeddings from $L_1$ to $\mathbb{C}$ are taken to be

$$\rho_i = \begin{cases} \psi^{i-1} & \text{for } 1 \le i \le q, \\ \tau\psi^{i-1} & \text{for } q+1 \le i \le 2q. \end{cases}$$

Since the extension $L/L_1$ is unramified, the determinant of the matrix $\mathcal{M} = (\rho_i(\beta_j))$ must be equal to $(-D)^q \mathrm{disc}(Q_1)^2$, a quantity that we can compute using integer arithmetic. The defect is then easy to determine.

In the notations of Section 6, we have to compute the coefficients $c_{j,r}^{(k)}$. We may rewrite system (10) for $1 \leq i \leq q$ as:

$$\begin{aligned}\rho_i(dc_{kj}) &= \sum_{r=1}^{q} c_{j,r}^{(k)} w_i^{r-1} + \omega \sum_{r=1}^{q} c_{j,r+q}^{(k)} w_i^{r-1} \\ &= \sum_{r=1}^{q} (c_{j,r}^{(k)} + \omega c_{j,r+q}^{(k)}) w_i^{r-1}.\end{aligned}$$

We first solve the interpolation problem $W(w_i) = \rho_i(dc_{kj})$ and then we recover the $c_{j,r}^{(k)}$ using real and imaginary part.

*7.2.1. Checking the results*

The theory of class fields tells us that rational primes which are a norm in $\mathbb{Q}(\sqrt{-D})$ split completely in $\mathbf{K}_H$. In practical terms, this means that for primes of the form $P = (x^2+Dy^2)/4$ for rational integers $x$ and $y$, the polynomial $H_D(X)$ has $h$ roots in $\mathbb{F}_P$. It does also mean that all intermediate polynomials in our tower of extension split modulo $P$. Checking the result is then easy by trying a small number of these splitting primes.

### 7.3. An example using the genus field

In this section, we explain by an example what has to be done when the base field is not $\mathbb{Q}$, but we know an easy to handle integral basis.

We use the notations of [3§7.3]. Let $-D = -1015 = (5)(29)(-7)$ of class number $h = 16$ and genus number $g = 4$. The genus field of $\mathbb{Q}(\sqrt{-D})$ is $\mathbb{Q}(\sqrt{5}, \sqrt{29}, \sqrt{-7})$. The real genus field is $\mathbf{K}_G^+ = \mathbb{Q}(\sqrt{5}, \sqrt{29})$. A convenient invariant is $\mathfrak{f}(-D)/\sqrt{2}$ and its minimal polynomial is

$$\begin{aligned}H(X) = H_{-4\times 1015}[\mathfrak{f}/\sqrt{2}](X) &= X^{16} - 44\,X^{15} - 81\,X^{14} - 16\,X^{13} + 66\,X^{12} + 172\,X^{11} + 126\,X^{10} \\ &+65\,X^9 - 50\,X^8 - 97\,X^7 - 69\,X^6 - 32\,X^5 + 12\,X^4 + 11\,X^3 + 12\,X^2 + 4\,X + 1\end{aligned}$$

of Galois group isomorphic to $C(2) \times C(8)$. The algebraic graph of extensions is depicted in Figure 1. We note $(u_i)_{1 \leq i \leq 16}$ the roots of $H(X)$.

Every integer $\theta$ of $\mathbf{K}_G^+$ can be written as (see [4]):

$$\frac{1}{4} \sum_{i=0}^{3} P_i \alpha_i$$

where $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \{1, \sqrt{5}, \sqrt{29}, \sqrt{145}\}$ and $P_i$ are rational integers. The conjugates of $\theta$ are given by:

$$\begin{pmatrix} \varphi_0(\theta) \\ \varphi_1(\theta) \\ \varphi_2(\theta) \\ \varphi_3(\theta) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} P_0/4 \\ P_1\sqrt{5}/4 \\ P_2\sqrt{29}/4 \\ P_3\sqrt{145}/4 \end{pmatrix}$$

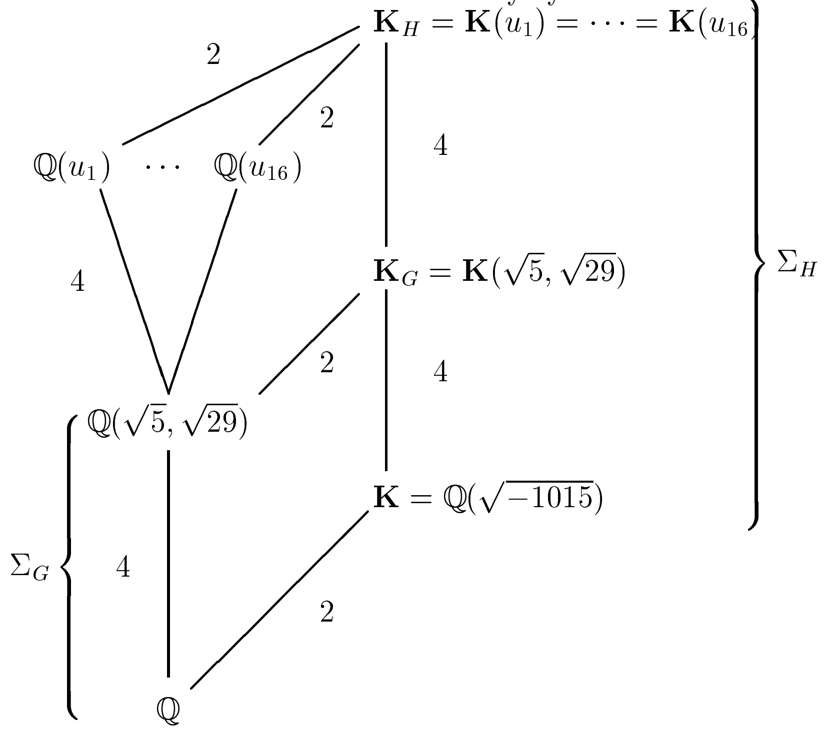


**Figure 1:** The graph of extensions.

Using the techniques described in [3§7.3], we can find the factorization of $H(X)$ as a product of four factors over $\mathbf{K}_G^+$, together with their roots. Note that the first factor is associated with the principal genus $G_0$ that is a (cyclic – in that case) subgroup of $\mathcal{H}(-D)$ and that gives us the ordering on the roots of *all* polynomials. In Table 1, we give for each genus the corresponding polynomial and its roots in the correct order.

Now we will launch our algorithm on $H[G_0]$, and parallel the operations on the conjugate polynomials $H[G_i]$ as well. The corresponding polynomials are given in Table 1 as well. (We have numbered the conjugates with a superscript.) The $V_j^{(r)}$'s have coefficients in $\mathbf{K}_G^+$. For instance, we must solve:

$$\begin{pmatrix} 38.209 \\ 1.1396 \\ 1.2981 \\ 0.35387 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1\sqrt{5} \\ a_2\sqrt{29} \\ a_3\sqrt{145} \end{pmatrix}$$

whose solution is $a_0 = 10.25$, $a_1 = 4.25$, $a_2 = 1.75$, $a_3 = 0.75$. Proceeding in the same way for all coefficients, we can recover:

$$V_0^{(0)} = Y^2 + (41/4 + 17/4\sqrt{5} + 7/4\sqrt{29} + 3/4\sqrt{145})Y - 15/4 - 5/4\sqrt{5} - 3/4\sqrt{29} - 1/4\sqrt{145},$$

$$V_1^{(0)} = Y^2 + (-11 - 5\sqrt{5} - 2\sqrt{29} - \sqrt{145})Y + 3/2 + 1/2\sqrt{5}.$$

Using $V_1^{(0)}$ as a defining polynomial for $L_1$, we end up with the decomposition of $H[G_0]$ as:

$$P_1(Y) = Y^2 + (41/4 + 17/4\sqrt{5} + 7/4\sqrt{29} + 3/4\sqrt{145})Y - 15/4 - 5/4\sqrt{5} - 3/4\sqrt{29} - 1/4\sqrt{145}$$

| $i$ | $\varphi_i$ | $G_i$ | $H[G_i]$ |
|---|---|---|---|
| 0 | $(+,+)$ | $(+,+,+)$ | $X^4 + \left(-11 - 5\sqrt{5} - 2\sqrt{29} - \sqrt{145}\right) X^3$ |
| | | | $+ \left(-\frac{35}{4} - \frac{15}{4}\sqrt{5} - 7/4\sqrt{29} - 3/4\sqrt{145}\right) X^2$ |
| | | | $+ \left(-\frac{15}{4} - 5/4\sqrt{5} - 3/4\sqrt{29} - 1/4\sqrt{145}\right) X$ |
| | | | $-\frac{15}{4} - 5/4\sqrt{5} - 3/4\sqrt{29} - 1/4\sqrt{145}$ |
| | | | $X^4 - 44.992X^3 - 35.590X^2 - 13.594X - 13.594$ |
| | | | $0.029132 - 0.59304i, -0.84238, 0.029132 + 0.59304i, 45.776$ |
| 1 | $(-,+)$ | $(-,+,-)$ | $X^4 + \left(-11 + 5\sqrt{5} - 2\sqrt{29} + \sqrt{145}\right) X^3$ |
| | | | $+ \left(-\frac{35}{4} + \frac{15}{4}\sqrt{5} - 7/4\sqrt{29} + 3/4\sqrt{145}\right) X^2$ |
| | | | $+ \left(-\frac{15}{4} + 5/4\sqrt{5} - 3/4\sqrt{29} + 1/4\sqrt{145}\right) X$ |
| | | | $-\frac{15}{4} + 5/4\sqrt{5} - 3/4\sqrt{29} + 1/4\sqrt{145}$ |
| | | | $X^4 + 1.4516X^3 - 0.75759X^2 - 1.9834X - 1.9834$ |
| | | | $-1.6282, -0.55318 + 0.80215i, 1.2830, -0.55318 - 0.80215i$ |
| 2 | $(+,-)$ | $(+,-,-)$ | $X^4 + \left(-11 - 5\sqrt{5} + 2\sqrt{29} + \sqrt{145}\right) X^3$ |
| | | | $+ \left(-\frac{35}{4} - \frac{15}{4}\sqrt{5} + 7/4\sqrt{29} + 3/4\sqrt{145}\right) X^2$ |
| | | | $+ \left(-\frac{15}{4} - 5/4\sqrt{5} + 3/4\sqrt{29} + 1/4\sqrt{145}\right) X$ |
| | | | $-\frac{15}{4} - 5/4\sqrt{5} + 3/4\sqrt{29} + 1/4\sqrt{145}$ |
| | | | $X^4 + 0.63158X^3 + 1.3200X^2 + 0.50419X + 0.50419$ |
| | | | $-0.38422 - 0.71074i, -0.38422 + 0.71074i, 0.068431 - 0.87618i, 0.068431 + 0.87618i$ |
| 3 | $(-,-)$ | $(-,-,+)$ | $X^4 + \left(-11 + 5\sqrt{5} + 2\sqrt{29} - \sqrt{145}\right) X^3$ |
| | | | $+ \left(-\frac{35}{4} + \frac{15}{4}\sqrt{5} + 7/4\sqrt{29} - 3/4\sqrt{145}\right) X^2$ |
| | | | $+ \left(-\frac{15}{4} + 5/4\sqrt{5} + 3/4\sqrt{29} - 1/4\sqrt{145}\right) X$ |
| | | | $-\frac{15}{4} + 5/4\sqrt{5} + 3/4\sqrt{29} - 1/4\sqrt{145}$ |
| | | | $X^4 - 1.0909X^3 + 0.028097X^2 + 0.073560X + 0.073560$ |
| | | | $0.76911 + 0.018061i, 0.76911 - 0.018061i, -0.22365 + 0.27252i, -0.22365 - 0.27252i$ |

| $r$ | $U_1^{(r)}$ | $U_2^{(r)}$ |
|---|---|---|
| 0 | $X^2 - 0.058264X + 0.35254$ | $X^2 - 44.934X - 38.561$ |
| 1 | $X^2 + 0.34525X - 2.0890$ | $X^2 + 1.1064X + 0.94945$ |
| 2 | $X^2 + (0.31579 + 1.5869i)X - 0.64903 + 0.28801i$ | $X^2 + (0.31579 - 1.5869i)X - 0.64903 - 0.28801i$ |
| 3 | $X^2 + (-0.54546 - 0.29058i)X - 0.17693 + 0.20556i$ | $X^2 + (-0.54546 + 0.29058i)X - 0.17693 - 0.20556i$ |

| $r$ | $V_0^{(0)}$ | $V_1^{(r)}$ |
|---|---|---|
| 0 | $Y^2 + 38.209Y - 13.594$ | $Y^2 - 44.992Y + 2.6180$ |
| 1 | $Y^2 + 1.1396Y - 1.9834$ | $Y^2 + 1.4516Y + 0.38197$ |
| 2 | $Y^2 + 1.2981Y + 0.50419$ | $Y^2 + 0.63158Y + 2.6180$ |
| 3 | $Y^2 + 0.35387Y + 0.073560$ | $Y^2 - 1.0909Y + 0.38197$ |

**Table 1:** Data for the genus field example.

$P_2(X,Y) = X^2-((-11/8-7/8\sqrt{5}+1/8\sqrt{29}+1/8\sqrt{145})Y-7/8-3/8\sqrt{5}+1/8\sqrt{29}+1/8\sqrt{145})X+Y.$

### 7.4. The complete construction for $D = 239$

Let us explain how to build the Hilbert class field $\mathbf{K}_H$ of $\mathbb{Q}(\sqrt{-239})$. We find that $\mathrm{Cl}(-4 \times 239)$ is cyclic of order 15. The defining polynomial of $\mathbf{K}_H$ is

$$H(X) = X^{15} - 6X^{14} + 2X^{13} + 8X^{12} + 4X^{11} - 27X^{10} + 13X^9$$
$$+15X^8 - 4X^7 - 20X^6 + 13X^5 + 5X^4 - 4X^3 - 4X^2 + 4X - 1$$

whose roots in cyclic order are:

| $k$ | $v_k$ | $k$ | $v_k$ |
|---|---|---|---|
| 1 | $0.857443 - 0.622922i$ | 9 | $-1.063392 + 0.892292i$ |
| 2 | $0.563313 - 0.634566i$ | 10 | $-0.722147 - 0.410736i$ |
| 3 | $-0.611580 - 0.644478i$ | 11 | $0.531754 - 0.284231i$ |
| 4 | $0.531754 + 0.284231i$ | 12 | $-0.611580 + 0.644478i$ |
| 5 | $-0.722147 + 0.410736i$ | 13 | $0.563313 + 0.634566i$ |
| 6 | $-1.063392 - 0.892292i$ | 14 | $0.857443 + 0.622922i$ |
| 7 | $0.769636 + 0.114861i$ | 15 | $5.349946$ |
| 8 | $0.769636 - 0.114861i$ | | |

One of the possible extensions tower is:

$$\begin{tikzcd}
 & & L(\zeta_5) \arrow[dd, dash, "5"] \\
 & L \arrow[ur, dash, "4"] \arrow[dd, dash, "5"] & \\
L_1(\zeta_3) \arrow[dr, dash, "2"] \arrow[dd, dash, "3"'] & & L_1(\zeta_5) \\
 & L_1 \arrow[ur, dash, "4"'] \arrow[dd, dash, "3"] & \\
K(\zeta_3) \arrow[dr, dash, "2"] & & \\
 & K \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

We first find the intermediate fields and then solve each equation by radicals.

#### *7.4.1. Building $L_1$*

To find the polynomials $V_j$, one uses the floating point values given above. Using the algorithms of the preceding sections, we find that:

| $j$ | $V_j$ | $\mathrm{disc}(V_j)/(-239)$ | $d(V_j)$ |
|---|---|---|---|
| 0 | $Y^3 - 8Y^2 - Y - 1$ | $3^2$ | 3 |
| 1 | $Y^3 + 21Y^2 + 20Y + 27$ | $53^2$ | 53 |
| 2 | $Y^3 - 24Y^2 - 9Y - 27$ | $3^8$ | 81 |
| 3 | $Y^3 + 10Y^2 - 31Y + 23$ | $3^4$ | 9 |
| 4 | $(Y-2)^3$ | 0 | $--$ |

We select $j_0 = 0$ and give in Table 2 the coefficients of $H_1(X,Y)X^5 + \sum_{i=0}^{4} C_i(Y)X^i$, both with the defect representation and the Hecke one. For the Hecke representation, we compute the derivative of $V_0$ and its values on its roots:

| $i$ | $\alpha_i$ | $V_0'(\alpha_i)$ |
|---|---|---|
| 1 | $-0.06899 - 0.34369i$ | $-0.23624 + 5.6413i$ |
| 2 | $-0.06899 + 0.34369i$ | $-0.23624 - 5.6413i$ |
| 3 | $8.1379802576468891$ | $67.472$ |

For instance, we find that

$$V_0'(\alpha_1)C_0(Y) = -(8.0000000000000010Y^2 + 2.0000000000000010Y + 3.0000000000000004)$$

which yields $C_0(Y) = -(8Y^2 + 2Y + 3)/V_0'(Y)$.

| $i$ | $3C_i(Y)$ | $V_0'(Y)C_i(Y)$ |
|---|---|---|
| 4 | $-6$ | $-(6Y^2 - 32Y - 2)$ |
| 3 | $-Y^2 + 3Y + 4$ | $-(10Y^2 + 23Y + 1)$ |
| 2 | $-9Y$ | $-(24Y^2 + 6Y + 9)$ |
| 1 | $-2Y^2 + 9Y - 1$ | $-21Y^2 + 4Y + 4$ |
| 0 | $-3Y$ | $-(8Y^2 + 2Y + 3)$ |

**Table 2:** Coefficients of $H_1(X,Y)$.

*7.4.2. Using radicals*

We have $L_1 = K(w_1)$ where $w_1$ is a root of $Q_1(Y) = Y^3 - 8Y^2 - Y - 1$. The roots of $Q_1$ are

$$w_1 = -0.0689 - 0.3436i, w_2 = -0.689 + 0.3436i, w_3 = 8.138,$$

obtained from the roots of $H$ as:

$$w_1 = v_1 \cdot v_4 \cdot v_7 \cdot v_{10} \cdot v_{13},$$

$$w_2 = v_2 \cdot v_5 \cdot v_8 \cdot v_{11} \cdot v_{14},$$

$$w_3 = v_3 \cdot v_6 \cdot v_9 \cdot v_{12} \cdot v_{15}.$$

The matrix $\mathcal{M}$ is given in Table 3 (remember that $\beta_1 = 1$ and therefore $\rho_i(\beta_1) = 1$ for all $i$). It has determinant $(3^2 \times 239)^2(-239)^3$, so that $(3^2 \times 239)c_{j,r}^{(k)} \in 5\mathbb{Z}$. The coefficients $c_{j,r}^{(k)}$ are given in Table 4.

Now that we have completed the work for $L/L_1$, we can do the same for $L_1/K$. A root $u$ of $Q_1(Y)$ is computed via:

$$y^3 = -9\zeta_3^2\omega - 557\zeta_3^2 + 9\zeta_3\omega - 566\zeta_3,$$

$$u = \frac{1}{3}\,\frac{\left(-134\,{\zeta_3}^2 - 134\,\zeta_3\right)y^2}{\left(-1114 - 18\,\omega\right){\zeta_3}^2 + \left(-1132 + 18\,\omega\right)\zeta_3} + \frac{1}{3}\,y + \frac{8}{3}.$$

| $i$ | $\rho_i(\beta_2)$ | $\rho_i(\beta_3)$ | $\rho_i(\beta_4)$ | $\rho_i(\beta_5)$ | $\rho_i(\beta_6)$ |
|---|---|---|---|---|---|
| 1 | $-0.06899 - 0.3437i$ | $-0.1134 + 0.04742i$ | $0.5 + 7.730i$ | $2.622 - 0.7051i$ | $-0.4232 - 0.8526i$ |
| 2 | $8.138$ | $66.23$ | $0.5 + 7.730i$ | $4.069 + 62.91i$ | $33.11 + 511.9i$ |
| 3 | $-0.06899 + 0.3437i$ | $-0.1134 - 0.04742i$ | $0.5 + 7.730i$ | $-2.691 - 0.3614i$ | $0.3099 - 0.9000i$ |
| 4 | $-0.06899 + 0.3437i$ | $-0.1134 - 0.04742i$ | $0.5 - 7.730i$ | $2.622 + 0.7051i$ | $-0.4232 + 0.8526i$ |
| 5 | $8.138$ | $66.23$ | $0.5 - 7.730i$ | $4.069 - 62.91i$ | $33.11 - 511.9i$ |
| 6 | $-0.06899 - 0.3437i$ | $-0.1134 + 0.04742i$ | $0.5 - 7.730i$ | $-2.691 + 0.3614i$ | $0.3099 + 0.9000i$ |

**Table 3:** The matrix $\mathcal{M}$.

| $k$ | $j$ | $r$ | $c_{j,r}^{(k)}/5$ | $k$ | $j$ | $r$ | $c_{j,r}^{(k)}/5$ | $k$ | $j$ | $r$ | $c_{j,r}^{(k)}/5$ | $k$ | $j$ | $r$ | $c_{j,r}^{(k)}/5$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | $-74054/717$ | 2 | 1 | 1 | $-1147/717$ | 3 | 1 | 1 | $446/239$ | 4 | 1 | 1 | $0$ |
| | 1 | 2 | $-27905/239$ | | 1 | 2 | $9000/239$ | | 1 | 2 | $-3182/239$ | | 1 | 2 | $4$ |
| | 1 | 3 | $-130495/717$ | | 1 | 3 | $-21113/717$ | | 1 | 3 | $-424/239$ | | 1 | 3 | $-1$ |
| | 1 | 4 | $-4135/717$ | | 1 | 4 | $-32/239$ | | 1 | 4 | $-47/717$ | | 1 | 4 | $0$ |
| | 1 | 5 | $-1550/239$ | | 1 | 5 | $403/239$ | | 1 | 5 | $-89/239$ | | 1 | 5 | $0$ |
| | 1 | 6 | $-12665/717$ | | 1 | 6 | $-185/239$ | | 1 | 6 | $-85/717$ | | 1 | 6 | $0$ |
| | 2 | 1 | $-51719/717$ | | 2 | 1 | $-3673/717$ | | 2 | 1 | $1633/717$ | | 2 | 1 | $-4/3$ |
| | 2 | 2 | $-19605/239$ | | 2 | 2 | $4293/239$ | | 2 | 2 | $-2242/239$ | | 2 | 2 | $1$ |
| | 2 | 3 | $-242350/717$ | | 2 | 3 | $-21242/717$ | | 2 | 3 | $-2203/717$ | | 2 | 3 | $-2/3$ |
| | 2 | 4 | $860/239$ | | 2 | 4 | $-302/717$ | | 2 | 4 | $-53/239$ | | 2 | 4 | $0$ |
| | 2 | 5 | $970/239$ | | 2 | 5 | $-699/239$ | | 2 | 5 | $182/239$ | | 2 | 5 | $0$ |
| | 2 | 6 | $-4140/239$ | | 2 | 6 | $-775/717$ | | 2 | 6 | $-45/239$ | | 2 | 6 | $0$ |
| | 3 | 1 | $-49139/717$ | | 3 | 1 | $-1325/239$ | | 3 | 1 | $1474/717$ | | 3 | 1 | $-4/3$ |
| | 3 | 2 | $-18635/239$ | | 3 | 2 | $3594/239$ | | 3 | 2 | $-2060/239$ | | 3 | 2 | $1$ |
| | 3 | 3 | $-254770/717$ | | 3 | 3 | $-7339/239$ | | 3 | 3 | $-2338/717$ | | 3 | 3 | $-2/3$ |
| | 3 | 4 | $-860/239$ | | 3 | 4 | $302/717$ | | 3 | 4 | $53/239$ | | 3 | 4 | $0$ |
| | 3 | 5 | $-970/239$ | | 3 | 5 | $699/239$ | | 3 | 5 | $-182/239$ | | 3 | 5 | $0$ |
| | 3 | 6 | $4140/239$ | | 3 | 6 | $775/717$ | | 3 | 6 | $45/239$ | | 3 | 6 | $0$ |
| | 4 | 1 | $-26063/239$ | | 4 | 1 | $-1243/717$ | | 4 | 1 | $1291/717$ | | 4 | 1 | $0$ |
| | 4 | 2 | $-29455/239$ | | 4 | 2 | $9403/239$ | | 4 | 2 | $-3271/239$ | | 4 | 2 | $4$ |
| | 4 | 3 | $-47720/239$ | | 4 | 3 | $-21668/717$ | | 4 | 3 | $-1357/717$ | | 4 | 3 | $-1$ |
| | 4 | 4 | $4135/717$ | | 4 | 4 | $32/239$ | | 4 | 4 | $47/717$ | | 4 | 4 | $0$ |
| | 4 | 5 | $1550/239$ | | 4 | 5 | $-403/239$ | | 4 | 5 | $89/239$ | | 4 | 5 | $0$ |
| | 4 | 6 | $12665/717$ | | 4 | 6 | $185/239$ | | 4 | 6 | $85/717$ | | 4 | 6 | $0$ |

**Table 4:** Coefficients for $D = 239$.

### 7.5. Application to ECPP

We did a lot of computations with our algorithms, including the computation of Galois decomposition for all known $D$'s with class number $h \leq 64$ and all possible type of groups. Although the defects are theoretically known, they tend to be huge and we encountered many precision problems, so that the Hecke representation turned out to be much superior to the defect one.

The decompositions are stored for future use in ECPP. In the program, we use such equations to build elliptic curves over $\mathbb{F}_P$ having complex multiplication modulo $P$. The equations are solved one by one modulo $P$, which takes much less time than solving directly a degree $h$ equation. Another point worth noting is that in the Hecke representation, the denominators that occur are always non-zero modulo $P$, since $H'(X)$ cannot be zero. It it were, then $H$ would have a double root, and this is not possible since $P$ has degree one in $\mathbf{K}$. The defect representation sometimes involve small primes that split in $\mathbf{K}_H$, and therefore the denominator are not invertible modulo $P$.

We do not use radicals usually, since for this to be faster than other methods such as Cantor-Zassenhaus's, we might want roots of unity defined in our field, which cannot be assured at all.

The present work makes it possible to use larger degree extensions than previously foreseen, which has an impact on the size of primes that can be certified. We will come back on this point in a forthcoming article [33].

We also noticed a useful trick in that case, that can be used in all cases where the Galois group is Abelian. We can decompose our group $G =< g_r > \otimes(< g_{r-1} > \otimes(\cdots \otimes < g_1 >)\cdots)$ in such a way that if the order of $g_i$ is $p_i$, then the $g_i$'s are sorted w.r.t. the smallest $p_i$. This is coherent with Theorem 3.1: The smaller the degree of the extension field $K/\mathbb{Q}$, the better.

## 8. Benchmarks

All timings are given in seconds on a Pentium III-450 MHz. We give two types of benchmarks. The first type concerns Hilbert class fields of degrees $2^n$ for $3 \leq n \leq 7$: We use our Maple program (version 5.5) to compare the defect approach and the Hecke one. In each of the sub-columns, we give the precision required together with the size (`size` function of Maple) of the result and the CPU time needed.

| $n$ | $D$ | Height($H_D$) | defect | | | Hecke | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 95 | 1.3 | 13 | 103 | 0.140 | 13 | 269 | 0.299 |
| 4 | 407 | 2.5 | 17 | 216 | 0.359 | 17 | 598 | 0.909 |
| 5 | 791 | 4.5 | 100 | 801 | 7.8 | 25 | 1313 | 2.970 |
| 6 | 2519 | 7.8 | 672 | 3420 | 268. | 42 | 3172 | 10.590 |
| 7 | 28664 | 37.3 | 7168 | 48567 | 11703. | 1792 | 15257 | 2608.860 |

The reason for choosing a power of 2 as extension degree is that it is the most difficult case, having to cut into two pieces at each time.

The second type of results concerns our Magma program (version 2.8-1) and compares the floating point approach and the $p$-adic approach on the computation of the extension tower of $(X^{257}-1)/(X-1)$ – an example giving the way to construct a regular 257-gone using ruler and compass. For the complex approach, we need 80 digits of precision and it takes 25 seconds. For the $p$-adic way, we use $p = 1543$ and precision 32. We get the answer in Hecke form after 21 seconds.

## 9. Conclusions

We have described practical algorithms to compute the roots of solvable equations by radicals. Even the first part, replacing an equation of large degree by the solution of intermediate equations of small degree is already useful. The interesting reader will find a stand-alone implementation of the algorithms on our web pages.

We have not explained how to use $p$-adic numbers in place of complex floating point numbers. In the case where the base field is $\mathbb{Q}$, there is little to change. The only point is in recognizing integers from their $p$-adic expression, but this is a well-known problem. When the base field is not $\mathbb{Q}$, we need to use unramified $p$-adic extensions of $\mathbb{Q}_p$ and though possible in theory, we have still to work out all the details. The floating point approach seems better as for now.

## 10. Acknowledgements

We thank M. Martin, who forced the second author to resume this work, undertaken long ago. Thanks also to B. Allombert who kindly sent us his article [2]; A. Enge for his careful reading; C. Fieker for comments on a previous version of this paper; P. Gaudry who communicated us his knowledge of $p$-adic numbers in Magma.

## References

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

[2] B. Allombert. A new algorithm for the computation of Galois automorphisms. Submitted for publication, May 2000.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[4] D. Chatelain. Bases normales de l'anneau des entiers de certaines extensions abéliennes de Q. *C. R. Acad. Sci. Paris Sér. I Math.*, 270:557–560, March 1970. Ser. A.

[5] H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1996. Third printing.

[6] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In H. Jager, editor, *Number Theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer-Verlag, 1984. Proc. of the Journées Arithmétiques 1983, July 11–15.

[7] H. Cohn. *A classical invitation to algebraic numbers and class fields.* Universitext. Springer-Verlag, 1978.

[8] H. Cohn. *Introduction to the construction of class fields.* Number 6 in Cambridge studies in advanced mathematics. Cambridge University Press, 1985.

[9] D. A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons, 1989.

[10] J. D. Dixon. Computing subfields in algebraic number fields. *J. Austral. Math. Soc. Ser. A*, 49:434–448, 1990.

[11] K. Geissler and J. Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30:675–716, 2000.

[12] K. Girstmair. Über die praktische Auflösung von Gleichungen höheren Grades. *Mathematische Semesterberichte*, Band XXXIV/1987(Heft 2):213–245, 1987.

[13] G. Gras. Extensions abéliennes non ramifiées de degré premier d'un corps quadratique. *Bull. Soc. Math. France*, 100:12–193, 1972.

[14] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In B. Mourrain, editor, *Symbolic and algebraic computation*, pages 175–182. ACM, 2001. Proceedings ISSAC'2001, London, Ontario.

[15] E. Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen.* Chelsea Publishing Company, 2 edition, 1970.

[16] G. Horng and M.-D. Huang. Solving polynomials by radicals with roots of unity in minimum depth. *Math. Comp.*, 68(226):881–885, April 1999.

[17] M.-D. A. Huang. Factorization of polynomials over finite fields and factorization of primes in algebraic number fields. In *Proc. 16th ACM STOC*, pages 175–182. ACM, 1984. Washington, apr. 30 – may 2.

[18] M.-D. A. Huang. Riemann hypothesis and finding roots over finite fields. In *Proc. 17th ACM STOC*, pages 121–130. ACM, 1985. Providence, Rhode Island, May 6–8.

[19] M.-D. A. Huang. Factorization of polynomials over finite fields and decomposition of primes in algebraic numbers fields. *J. Algorithms*, 12:482–489, 1991.

[20] M.-D. A. Huang. Generalized Riemann hypothesis and factoring polynomials over finite fields. *J. Algorithms*, 12:464–481, 1991.

[21] E. Kaltofen, David R. Musser, and B. David Saunders. A generalized class of polynomials that are hard to factor. *SIAM J. Comput.*, 12(3):473–483, August 1983.

[22] J. Klüners. On computing subfields. A detailed description of the algorithm. *J. Théor. Nombres Bordeaux*, 10:243–271, 1998.

[23] J. Klüners and G. Malle. Explicit Galois realization of transitive groups of degree up to 15. *J. Symbolic Comput.*, 30:675–716, 2000.

[24] J. Klüners and M. Pohst. On computing subfields. *J. Symbolic Comput.*, 24:385–397, 1997.

[25] S.-H. Kwon and J. Martinet. Sur les corps résolubles de degré premier. *J. Reine Angew. Math.*, 375/376:12–23, 1987.

[26] S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1):184–195, February 1985.

[27] S. Landau. Simplification of nested radicals. *SIAM J. Comput.*, 21(1):85–110, 1992.

[28] S. Landau and G. Miller. Solvability by radicals is in polynomial time. *J. Comput. System Sci.*, 30:179–208, 1985.

[29] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc.*, 26:211–244, 1992.

[30] D. Martinais and L. Schneps. Polynômes à groupe de Galois diédral. *Sém. Théor. Nombres Bordeaux*, 4:141–153, 1992.

[31] F. Morain. Construction of Hilbert class fields of imaginary quadratic fields and dihedral equations modulo $p$. Rapport de Recherche 1087, INRIA, September 1989. Available at `http://www.lix.polytechnique.fr/Labo/Francois.Morain/`.

[32] F. Morain. Solving generalized dihedral equations. Manuscript, August 1990.

[33] F. Morain. Three methods for computing Hilbert polynomials. Draft, January 2001.

[34] R. P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

[35] P. J. Weinberger and L. P. Rotschild. Factoring polynomials over algebraic number fields. *ACM Trans. Math. Software*, 2(4):335–350, 1976.

[36] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118:617–636, 1997.