

Solvability by Radicals from an Algorithmic Point of View

Guillaume Hanrot, François Morain

▶ **To cite this version:**

Guillaume Hanrot, François Morain. Solvability by Radicals from an Algorithmic Point of View. [Research Report] RR-4109, INRIA. 2001. inria-00072522

HAL Id: inria-00072522
https://inria.hal.science/inria-00072522

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Solvability by radicals from an algorithmic point of view

G. Hanrot — F. Morain

N° 4109

19th January 2001

THÈME 2



ISSN 0249-6399 ISRN INRIA/RR--4109--FR+ENG

INRIA
LORRAINE

Solvability by radicals from an algorithmic point of view

G. Hanrot* , F. Morain†

Thème 2 — Génie logiciel
et calcul symbolique
Projet SPACES

Rapport de recherche n° 4109 — 19th January 2001 — 18 pages

Abstract: Any textbook on Galois theory contains a proof that a polynomial equation with solvable Galois group can be solved by radicals. From a practical point of view, we need to find suitable representations of the group and the roots of the polynomial. We first reduce the problem to that of cyclic extensions of prime degree and then work out the radicals, using the work of Girstmair. 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.

Key-words: Galois Theory, solvability by radicals

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

* e-mail : Guillaume.Hanrot@loria.fr
† LIX, École polytechnique, F-91128 Palaiseau cedex, e-mail : morain@lix.polytechnique.fr

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy (France)
Téléphone : +33 3 83 59 30 00 — Télécopie : +33 3 83 27 83 19

Résolubilité par radicaux d'un point de vue algorithmique

Résumé : Un des principaux résultats de la théorie de Galois est le fait que toute équation polynomiale dont le groupe de Galois est résoluble peut être résolue par radicaux. D'un point de vue effectif, il est nécessaire d'obtenir une représentation adéquate du groupe et des racines du polynômes. Nous commençons par réduire le problème au cas d'extensions cycliques de degré premier, puis montrons dans ce dernier cas comment exhiber les radicaux, en utilisant le travail de Girstmair. Nous donnons des exemples numériques dans les cas abéliens et non abéliens. Ces résultats sont appliqués à la construction de corps de classes de Hilbert de corps quadratiques imaginaires.

Mots-clés : Théorie de Galois, résolution par radicaux

1 Introduction

The fundamental work of Galois 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 [17], it has been shown that testing solvability can be done in polynomial time. Once we know that an equation is solvable, we may want to compute explicitely the tower of extensions involved, as well as the radicals that enter the game. To these ends, we use a power-conjugate representation of the group that enables us to reduce the problem to that of cyclic extensions, and further to cyclic extensions of prime degree. At this point, we can find the radicals we are looking for.

This approach is well known. For instance, in [12, 14], Huang explains how to solve the n-th cyclotomic equation in polynomial time modulo ERH. In [13, 15], the construction is used to factor polynomials with Abelian Galois groups over finite fields. The present paper can be seen as a self-contained guide to implement the ideas given in these papers, adapting the algebraic-numerical approach of [10] (already followed in [20] and announced as [21] in [3, §8.6]).

After reducing the problem to cyclic cases in a first part of the article, we explain how to solve the resulting equations by radicals. Numerical examples are given of all the phases, using cyclotomic polynomials, but also Hilbert polynomials that define the Hilbert Class Fields of imaginary quadratic fields, and some non-abelian cases as well.

2 From solvable to cyclic extensions

2.1 Group theory

A group G is *polycyclic* if there exist a sequence of subgroups G_0, G_1, ..., G_r such that

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r = 1$$

where for each i, G_i/G_{i+1} is cyclic. If $g_i G_{i+1}$ generates G_i/G_{i+1}, then g_0, ..., g_{r-1} is called a polycyclic generating sequence for G. A group G is polycyclic if and only if G is solvable and all of the subgroups of G are finitely generated. Finding polycyclic generating sequences for a polycyclic group is now routine in the systems handling groups efficiently, as GAP and MAGMA. We refer the reader to [23] for a good introduction on polycyclic groups.

A finite solvable group G is a special case of polycyclic group. If G is the Galois group of some polynomial, and happens to be solvable, then finding the sequences (G_i) or (g_i) is thus easy, also considering that G has generally small cardinality.

Among all solvable groups, an important case is that of Abelian groups. In that case, we can find the structure of G as a product of cyclic groups using SNF techniques (see [4]). Again, this will be an easy task, since the matrices involved are of small size.

As a final result, all elements of G will be represented as

$$g_0^{\alpha_0} g_1^{\alpha_1} \cdots g_{r-1}^{\alpha_{r-1}}$$

where $0 \leq \alpha_i < h_i$ where h_i is the order of G_i/G_{i+1}.

2.2 The main theorems

The main theorem that we will use is the following:

Theorem 2.1 *Let $\mathbb{M}$ be a number field and let $H(X)$ be an irreducible monic degree h polynomial of $\mathbb{M}[X]$ with solvable Galois group G and splitting field L. Write $h = \prod_{i=1}^{n} p_i$, where the p_i are primes not necessarily distinct. There exists a chain of fields:*

$$L = L_0 \supset L_1 \supset \cdots \supset L_n = \mathbb{M}$$

such that L_{i-1}/L_i is cyclic of prime order p_i for $i \geq 1$.

Proof. Start from a polycyclic sequence for G:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r = 1$$

where $G_i/G_{i+1} = g_i G_{i+1}$. By Galois theory, this sequence corresponds to a sequence of subfields

$$L = K_0 \supset K_1 \supset \cdots \supset K_{r-1} \supset K_r = \mathbb{M}$$

such that K_i/K_{i+1} is Galois of cyclic Galois group $< g_i >= G_i/G_{i+1}$. Now, we can peel $< g_i >$ as a product of cyclic groups of prime order to finish the proof. □

2.3 Building the intermediate fields

Let x_1, x_2, ..., x_h be the roots of H and Γ its Galois group. We assume that Γ is isomorphic to the abstract group G and that we know the isomorphism $G \to \Gamma$. We will note γ_i the automorphism corresponding to g_i. More generally, greek letters will denote automorphisms and we will use Γ_i for the subgroup of Γ isomorphic to G_i.

The extension L/K_1 has Galois group $G/G_1 =< g_0 >$. For ξ in G_1, define:

$$f_\xi(X) = \prod_{i=1}^{h_1} (X - \gamma_0^i(\xi(x_0))).$$

By construction, $\gamma_0(f_\xi(X)) = f_\xi(X)$ and therefore $f_\xi(X) \in K_1[X]$. Now, write:

$$f_\xi(X) = X^{h_1} + \sum_{j=0}^{h_1-1} c_{\xi,j} X^j$$

and define

$$g_j(Y) = \prod_{\xi \in G_1} (Y - c_{\xi,j}).$$

The Galois group of g_j is (contained in) G_1 and one of the g_j's is irreducible, say $g_j =: Q_1$ and we have built K_1 as $\mathbb{M}[X]/(Q_1(X))$.

2.4 The cyclic case

We will illustrate the preceding ideas on the basic case of cyclic extensions. This will later be used as a primitive in our code.

Let $f(X)$ be a monic polynomial of degree d with cyclic Galois group $C =< \sigma >$. We let $x_1, \ldots, x_d$ be the roots of f in which $x_k = \sigma^{k-1}(x_1)$. We suppose that d is composite, otherwise, the decomposition is already finished.

Let L be the splitting field of $f(X)$. Let $\psi = \sigma^q$. Let L_1 be the subfield of L fixed by $< \psi >$, and φ be the restriction of σ to L_1. Define

$$f_i(X) = \prod_{k=1}^{p} (X - x_{kq+i})$$

for $1 \leq i \leq q$ and expand it as

$$f_i(X) = \sum_{k=0}^{p} (-1)^{p-k} c_{i,k} X^k.$$

The $c_{i,k}$ are algebraic integers, since they are combinations of the algebraic integers x_j. It is easy to see that f_i is fixed by ψ and therefore $c_{i,k}$ is in L_1 for all i, k. We also introduce

$$g_j(Y) = \prod_{l=0}^{q-1} (Y - c_{l,j})$$

for $0 \leq j < p$. At least one of the g_j is irreducible. We select one of these, say $Q_1 = g_{j_0}$ which defines $L_1/\mathbb{M} = \mathbb{M}[X]/(Q_1(X)) = \mathbb{M}[\alpha]$. Note also that $\varphi(c_{l,j}) = c_{(l+1) \bmod q, j}$, which gives us an ordering on the roots of Q_1.

Let us rewrite the roots of $Q_1(X)$ as α_1, α_2, ..., α_q. Fix a j. Then $c_{0,j}$ is an element of L_1 and therefore there exists a polynomial $A_j(Y) = \sum_{r=0}^{p-1} a_{j,r} Y^r$ with integer coefficients (in $\mathbb{M}$) such that:

$$c_{0,j} = A_j(\alpha_1) = \sum_{r=0}^{p-1} a_{j,r} \alpha_1^r.$$

Applying φ, we get:

$$\varphi^i(c_{0,j}) = c_{i,j} = \sum_{r=0}^{p-1} a_{j,r} (\varphi^i(\alpha_1))^r = \sum_{r=0}^{p-1} a_{j,r} \alpha_i^r.$$

In other words, we have at our disposal the values $(\alpha_i, A_j(\alpha_i) = c_{i,j})_{1 \leq i \leq q}$ which define a polynomial of degree q. The polynomial A_j can be recovered by Newton interpolation. Finally, a factor of $f(X)$ over L_1 is:

$$f_1(X, Y) = \sum_{k=0}^{p} (-1)^{p-k} A_j(Y) X^k.$$

procedure CyclicGalois($f(X)$, $\mathcal{R}$, p, q)

{ $\mathcal{R} = (x_1, x_2, \ldots, x_{pq})$ contains the roots of f ordered in a cyclic way }

1. **for** $i = 1..q$ **do** compute $f_i(X)$.
2. **for** $j = 0..p-1$ **do** compute $g_j(Y)$ and select one which is irreducible $Q_1(X)$.
3. Compute the polynomials $A_j(Y)$ for $0 \leq j < q$ using Newton interpolation.
4. return $Q_1(Y)$, its roots $(c_{l,j_0})_{0 \leq l < q}$ (in this precise order), and $f_1(X, Y)$.

2.5 The final algorithm

One can deduce an algorithm from the proof of 2.1. Using the power-conjugate presentation of G, we can order the roots of H in the following way. For a sequence $A = (a_1, \ldots, a_k)$ of G, and an element a of G, denote by $a \otimes A$ the sequence of elements

$$(aa_1, aa_2, \ldots, aa_k).$$

Starting from the subgroup $A =< g_{r-1} >= (g_{r-1}, g_{r-1}^2, \ldots, g_{r-1}^{h_{r-1}} = 1)$, we re-build G as $g_0 \otimes (g_1 \otimes (\cdots \otimes < g_{r-1} >) \cdots)$. Using this, it is easy to see that

$$G_1 \sim g_1 \otimes (\cdots \otimes < g_{r-1} >).$$

Moreover, this way of representing G enables us to go further. We can peel G_0/G_1 which is cyclic of order h_0, one cyclic group of prime order at a time. We can now describe the final algorithm that uses CyclicGalois as a primitive.

procedure Galois($H(X)$, $\mathcal{R}$, G)

{H is of degree h and solvable Galois group G }

1. [Find structure] obtain a polycyclic generating sequence for G as g_0, g_2, ..., g_{r-1}, where g_i is of order h_i and their corresponding automorphisms γ_i.

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

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 γ in Γ.

4. $k := 0$.

5. [Solve] **for** $i = 0..r-1$ **do**

   { at this point, $\mathcal{R}$ contains the roots of a polynomial of Galois group G_i }

   5.1 factor $h_i = \prod_{j=1}^{s} p_{i,j}$;

   5.2 **for** $j = 1..s-1$ **do**

   { $\mathcal{R}$ contains the roots of a polynomial
   of Galois group $< g_i^{h_i/\prod_{u=j}^{s} p_{i,j}} = 1 >< g_{i+1} > \cdots < g_{r-1} >$ }

   $Q(Y_k), \mathcal{R}, H_k(Y_k, Y_{k-1}) :=$ CyclicGaloisPrime($Q_{k-1}(Y_{k-1})$, $\mathcal{R}$, $p_{i,j}$, $h/p_{i,j}$);

   $h \leftarrow h/p_{i,j}$;

   $k \leftarrow k+1$;

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:*

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

3 Solving by radicals

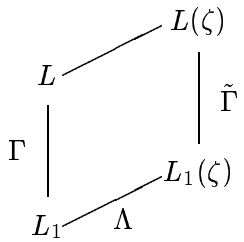
Using the preceding sections, we need concentrate on solving prime degree cyclic equations by radicals. For this, we follow [10], in the continuation of [20]. We give the details so as to make the article self-contained.

Suppose that d is a prime number. Let $f(X)$ be a monic irreducible polynomial of degree d in $K[X]$ 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:

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

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

Let $m = [L_1 : \mathbb{Q}] = m$ and $\{\beta_1, \ldots, \beta_m\}$ be an integral basis of L_1. Let also $\{\rho_1, \ldots, \rho_m\}$ be all embeddings of $L_1 \to \mathbb{C}$. Let ζ be a primitive d-th root of unity (e.g. $\zeta = \exp(2i\pi/d)$). We consider the following diagram of extensions:



The extension $L(\zeta)/L_1(\zeta)$ is Abelian, of Galois group $\tilde{\Gamma}$ isomorphic to Γ, 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 $\Lambda = \{\lambda_1, \ldots, \lambda_d\}$ where $\lambda_k(\zeta) = \zeta^k$. Put:

$$y_k = \sum_{j=1}^{d} x_j \zeta^{-jk}, 1 \leq k \leq d. \tag{2}$$

We can recover the x_j's from the y_k with:

$$x_j = \frac{1}{d} \sum_{k=1}^{d} y_k \zeta^{jk}. \tag{3}$$

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 $y_1 \neq 0$. Put $z^{(k)} = y_1^{d-k} y_k$, $1 \leq k \leq d$. In particular, we get $y_1^d = z^{(1)}$ and

$$\forall k, y_k = \left(\frac{z^{(k)}}{z^{(1)}}\right) y_1^k. \tag{4}$$

We deduce

$$\forall j, dx_j = z^{(d)} + y_1 \zeta^j + \sum_{k=2}^{d-1} \left(\frac{z^{(k)}}{z^{(1)}}\right) (y_1 \zeta^j)^k. \tag{5}$$

Solving $f(x) = 0$ is thus reduced to the computation of the $z^{(k)}$'s. Easy computations show that $z^{(k)} \in L_1(\zeta)$.

A basis of $L(\zeta)/L_1(\zeta)$ is $\{1, \zeta, \ldots, \zeta^{d-1}\}$. We can write: $z^{(k)} = \sum_{j=1}^{d-1} c_j^{(k)} \zeta^{-j}$, where $c_j^{(k)}$ is an element of L_1. The Galois group of $L(\zeta)/L_1$ is the direct product of Γ and Λ. The conjugates of $z^{(k)}$ in $L(\zeta)$ are:

$$z_l^{(k)} = \lambda_l(z^{(k)}) = \sum_{j=1}^{d-1} c_j^{(k)} \zeta^{-jl}, 1 \leq l \leq d. \tag{6}$$

and it is easily seen that the $z_l^{(k)}$'s are in $L_1(\zeta)$. Putting $c_d^{(k)} = 0$ and using the Fourier transform, we get

Proposition 3.1 *For all k, $1 \leq k \leq d$, and all j, $1 \leq j \leq d$, we have*

$$dc_j^{(k)} = \sum_{l=1}^{d} z_l^{(k)} \zeta^{jl}, 1 \leq j < d. \tag{7}$$

Moreover $dc_j^{(k)}$ is an integer of L_1, since it is a combination of algebraic numbers.

We have also: $c_d^{(k)} = 0 = z_1^{(k)} + \cdots + z_d^{(k)}$. If we replace $z_d^{(k)}$ by its values, we find:

Corollary 3.1

$$dc_j^{(k)} = \sum_{l=1}^{d-1} z_l^{(k)} (\zeta^{jl} - 1), 1 \leq j < d. \tag{8}$$

Using the integral basis of $L_1/\mathbb{Q}$, we can write:

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

with $c_{j,i}^{(k)}$ in $\mathbb{Z}$. We write:

$$\begin{array}{ll} \forall i, \rho_i(dc_j^{(k)}) & = \sum_{r=1}^{m} c_{j,r}^{(k)} \rho_i(\beta_r) \\ & = \sum_{l=1}^{d-1} \rho_i(z_l^{(k)})(\zeta^{jl} - 1). \end{array} \tag{9}$$

All we need now are the values of $\rho_i(z_l^{(k)}) = \rho_i(y_l)^{d-k} \rho_i(y_{lk})$ which can be computed from:

$$\rho_i(y_k) = \sum_{j=1}^{d} \rho_i(x_j) \zeta^{-jk}.$$

Using this, $c_{j,r}^{(k)}$ can be computed by means of the resolution of $m \times m$ linear systems, or by precomputing the inverse of the matrix $\mathcal{M} = (\rho_i(z_l^{(k)}))$.

4 Implementation

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 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 [18]) or more subtle methods ([1], [2]).

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.

4.2 Building cyclic extensions

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

$$\max \binom{d}{k} M^k \tag{10}$$

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

The second task is to compute polynomials $A_j(Y) = \sum_{r=0}^{p-1} a_{j,r} Y^r$ such that $A_j(\alpha_i)$ represents an integer of L_1. The coefficients $a_{j,r}$ are rational integers, but they can be written as $b_{j,r}/\delta$ where δ is an integer called the *defect* of the power basis $\{1, \alpha, \ldots, \alpha_q\}$. This number is costly to compute in general, but is known to divide the largest square factor of the discriminant of the defining polynomial $Q_1(Y)$ of α. Once we have a floating point approximation of $a_{j,r}$, then $\delta a_{j,r}$ has to be a rational integer, easy to recognize. This also shows that we might need more accuracy on the integers we use, forcing more precision on the roots of f.

In real life, one chooses an irreducible polynomial $Q_1(X)$ with the smallest possible value of δ. To get more precision, we can refine the roots of the polynomial we are considering via an ordinary Newton iteration if needed.

Finally, we can check our computations by computing the resultant of $Q_1(Y)$ and $f_1(X, Y)$ which must coincide with $f(X)$. 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.

4.3 Solving by radicals

The key point is to be able to find an integral basis of $L_1/\mathbb{M} = \mathbb{M}[\theta]$. It is a relatively easy task for small degree fields, but cumbersome for large ones (see [5]). We prefer using a power basis, paying the price of a possibly huge denominator: each integer γ of L_1 will be written $\gamma = \sum_{j=0}^{m-1} a_j \theta^j$ and its conjugates $\gamma_i = \rho_i(\gamma) = \sum_{j=0}^{m-1} a_j \rho_i(\theta)^j$. The determinant of the matrix $(\rho_i(\theta)^j)$ is an integer (algebraic integer fixed by the ρ_i's). The largest denominator of the a_i's is the largest square dividing this determinant.

The only thing we have to know is the values of the $\rho_i(\theta)$, for instance as floating point numbers. We will see on the numerical examples how this works.

5 Numerical examples

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 $(\mathbb{Z}/m\mathbb{Z})^*$ which is Abelian. The action corresponding to element a of $(\mathbb{Z}/m\mathbb{Z})^*$ sends ζ_m on ζ_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 $< 31 > \times < 11 > \times < 17 >$. We illustrate here the symbolic approach. Letting ζ 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:

$$f_1(X) = (X - \zeta^{17})(X - \zeta^{33}),$$
$$f_2(X) = (X - \zeta^9)(X - \zeta),$$
$$\cdots$$
$$f_8(X) = (X - \zeta^{11})(X - \zeta^{21})$$

yielding:

$$g_1(Y) = Y^8 + 2Y^7 + 3Y^6 + 4Y^5 + 5Y^4 + 4Y^3 + 3Y^2 + 2Y + 1,$$
$$g_2(Y) = Y^8 + 2Y^6 + 4Y^4 + 8Y^2 + 16.$$

We select $g_2(Y)$ since $g_1(Y) = (Y^4 + Y^3 + Y^2 + Y + 1)^2$ is not irreducible. The roots of g_2 in the correct order are:

$$\zeta^{17} + \zeta^{33}, \zeta^9 + \zeta, \ldots, \zeta^{11} + \zeta^{21}.$$

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

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

is computed.

This Galois group is isomorphic to the semidirect product $C(7) \ltimes C(3)$, generated by σ_1 and σ_2, with $\sigma_2\sigma_1 = \sigma_1\sigma_2^2$. If the roots (all real) of T are numbered in increasing order, σ_1 and σ_2 are given as product of cyclic permutations as

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

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

To construct the subfield corresponding to $< \sigma_1 >$, we use a symmetric function of the roots corresponding to an orbit under the action of σ_2. For instance, we look for the minimal polynomial of $\alpha_1 + \alpha_5 + \alpha_6 + \alpha_{11} + \alpha_{14} + \alpha_{16} + \alpha_{17}$, which is $y^3 - 7y^2 + 49$. It remains to compute the root x of T in terms of y. This is done by using the interpolation procedure described at the end of subsection 2.4, and then we are left with the following cyclic equations to solve

$$\begin{aligned} y^3 - 7y^2 + 49 &= 0 \\ x^7 - yx^6 + (3y^2 - 6y - 42)x^5 - (5y^2 - 14y - 63)x^4 & \\ -(7y^2 - 17y - 91)x^3 + (12y^2 - 33y - 147)x^2 - (5y^2 - 15y - 56)x & \\ +4y^2/7 - 2y - 5 &= 0. \end{aligned}$$

We give a second example. A root of the polynomial

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

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 σ_i are given as

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

Since a sequence of subgroups corresponding to G is $G \triangleright < \sigma_1, \sigma_2 > \triangleright < \sigma_1 > \triangleright 1$, we thus compute the minimal polynomial of $\alpha_1 + \alpha_5$ (an orbit under the action of σ_3) and find the irreducible degree 6 polynomial $s(y) = y^6 - 4y^5 - 33y^4 + 33y^3 + 124y^2 + 60y + 8$. The action of σ_2 on the roots of g is given by $(1,6)(3,5)(2,4)$, so that $\beta_1 + \beta_6$ is a root of the polynomial $t(z) = z^3 - 4z^2 - z + 11$. If we compute simultaneously the expressions for y and z in terms of x and y, we end with the following sequence of cyclic equations to solve

$$\begin{aligned} z^3 - 4z^2 - z + 11 &= 0 \\ y^2 - zy - 6z^2 + 4z + 20 &= 0 \\ x^2 - xy + (87y^5 - 374y^4 - 2759y^3 + & \\ 3697y^2 + 9682y + 2324)/12 &= 0. \end{aligned}$$

6 Constructing Hilbert Class fields

This part of the article was the original motivation for our work, before we realized it could be easily extended to the general solvable case. It will serve as an example of Galois extension over a number field which is not $\mathbb{Q}$.

6.1 Theoretical setting

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 [3], where the reader can find more motivation. Constructing cyclic extensions of prime degree of quadratic fields has been the subject of the articles [11, 16, 19]. Here, we are satisfied with an algorithmic approach to the explicit construction of our tower of fields. Ultimately, we will be using this for finding roots of the defining polynomials over finite fields.

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). See the references given above for more details. The Galois group turns out to be isomorphic to the class group $\mathrm{Cl}(-D)$ of $\mathbf{K}$: It is Abelian, and if h is small, computing a 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 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 rational integer δ (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.

6.2 Solving $H_1(X, Y)$ by radical

We assume that $H_1(X, Y)$ is a degree p polynomial in X with coefficients in $L_1(Y) = \mathbf{K}[Y]/(Q_1(Y))$ 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 a cyclic way as usual). Remember that the roots of the polynomials $(f_i(X))_{1\le i\le q}$ 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 manipulation, the roots of H_1, namely the $x_{1,j}$ will be renamed $x_j = x_{1,j}$.

We denote as usual σ 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 τ 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 $(\rho_i(\beta_j))$ 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.

We have to compute the coefficients $c_{j,r}^{(k)}$. We may rewrite system (9) for $1 \le i \le q$ as:

$$\rho_i(dc_j^{(k)}) = \sum_{r=1}^{q} c_{j,r}^{(k)} w_i^{r-1} + \omega \sum_{r=1}^{q} c_{j,r+q}^{(k)} w_i^{r-1} = \sum_{r=1}^{q} (c_{j,r}^{(k)} + \omega c_{j,r+q}^{(k)}) w_i^{r-1}. \tag{11}$$

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

6.2.1 Checking the results

The theory of class fields tells us that rational primes which are 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.

6.3 The complete construction for $D = 239$

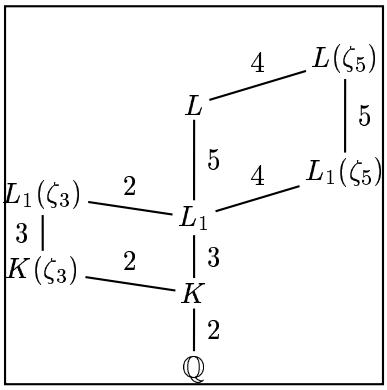
Let us explain how to build the Hilbert Class Field L of $\mathbb{Q}(\sqrt{-239})$. We find that $\mathrm{Cl}(-4 \times 239)$ is cyclic of order 15. The defining polynomial of $\mathbf{K}_H$ is

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

whose roots in cyclic order are:

k	v_k	k	v_k
1	$0.857443485 - 0.622922603i$	9	$-1.063392841 + 0.892292686i$
2	$0.563313291 - 0.634566839i$	10	$-0.722147984 - 0.410736930i$
3	$-0.611580428 - 0.644478138i$	11	$0.531754522 - 0.284231291i$
4	$0.531754522 + 0.284231291i$	12	$-0.611580428 + 0.644478138i$
5	$-0.722147984 + 0.410736930i$	13	$0.563313291 + 0.634566839i$
6	$-1.063392841 - 0.892292686i$	14	$0.857443485 + 0.622922603i$
7	$0.769636684 + 0.114861403i$	15	5.349946540
8	$0.769636684 - 0.114861403i$		

One of the possible tower extensions is:



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

6.3.1 Building L_1

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

j	g_j	$\mathrm{disc}(g_j)/(-239)$	$d(g_j)$
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 $j_0 = 0$. Finally, a factor of $H(X)$ over L_1 is given by

$$H_1(X,Y) = X^5 - 2X^4 + (-Y^2/3 + Y + 4/3)X^3 - 3YX^2 + (-2Y^2/3 + 3Y - 1/3)X - Y.$$

6.3.2 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

$$w_1 = -0.068990 - 0.34369i, w_2 = -0.68990 + 0.34369i, w_3 = 8.1380,$$

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:

i	$\rho_i(\beta_1)$	$\rho_i(\beta_2)$	$\rho_i(\beta_3)$	$\rho_i(\beta_4)$	$\rho_i(\beta_5)$	$\rho_i(\beta_6)$
1	1.	$-0.06899 - 0.3437i$	$-0.1134 + 0.04742i$	$0.5 + 7.730i$	$2.622 - 0.7051i$	$-0.4232 - 0.8526i$
2	1.	8.138	66.23	$0.5 + 7.730i$	$4.069 + 62.91i$	$33.11 + 511.9i$
3	1.	$-0.06899 + 0.3437i$	$-0.1134 - 0.04742i$	$0.5 + 7.730i$	$-2.691 - 0.3614i$	$0.3099 - 0.9000i$
4	1.	$-0.06899 + 0.3437i$	$-0.1134 - 0.04742i$	$0.5 - 7.730i$	$2.622 + 0.7051i$	$-0.4232 + 0.8526i$
5	1.	8.138	66.23	$0.5 - 7.730i$	$4.069 - 62.91i$	$33.11 - 511.9i$
6	1.	$-0.06899 - 0.3437i$	$-0.1134 + 0.04742i$	$0.5 - 7.730i$	$-2.691 + 0.3614i$	$0.3099 + 0.9000i$

which 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 1.

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:

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

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

6.4 A noncyclic group

The group $\mathrm{Cl}(-6052)$ is of type $C(4) \times C(4)$. We can solve

$$H(X) = X^{16} - 18709X^{15} + 15423X^{14} - 58444X^{13} + 91636X^{12} - 135810X^{11}$$
$$+149345X^{10} - 28445X^9 + 52950X^8 - 28445X^7 + 149345X^6$$
$$-135810X^5 + 91636X^4 - 58444X^3 + 15423X^2 - 18709X + 1$$

via:

$$H_3(Y_3) = Y_3^2 - 9504Y_3 + 20736,$$

$$H_2(Y_2, Y_3) = Y_2^2 - \left(\frac{185}{96}\,Y_3 - 3/2\right) Y_2 + Y_3,$$

$$H_1(Y_1, Y_2) = Y_1^2 - \left(-\frac{173}{6884352}\,Y_2^3 + \frac{264113}{573696}\,Y_2^2 - \frac{197537}{47808}\,Y_2 + \frac{13805}{3984}\right) Y_1 + Y_2,$$

$$H_0(Y_0, Y_1) = Y_0^2 - Y_1\,Y_0 - \frac{3880212577117}{22144525053387840}\,Y_1^7 + \frac{14518417424055149}{4428905010677568}\,Y_1^6$$
$$+\frac{17261595060101471}{4428905010677568}\,Y_1^5 + \frac{33006143257103761}{2768065631673480}\,Y_1^4 - \frac{45112147405227119}{2768065631673480}\,Y_1^3$$
$$-\frac{571443627990205}{92268854389116}\,Y_1^2 + \frac{22333117995863}{30756284796372}\,Y_1 + \frac{59520033928081}{12815118665155}.$$

7 Conclusions

We have described 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.

In ECPP [3], we use the explicit construction of class fields to build elliptic curves with complex multiplication by the ring of integers of some imaginary quadratic field $\mathbf{K}$. We then have to find roots of the corresponding polynomials in some possibly large finite field. Following our work, we have to solve intermediate equations of rather small degree compared to the original problem. This accelerates this part of the algorithm and has an impact on the choice of which fields to be used. We will come back on this point in a forthcoming article [22]. In this context, 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.

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 1: Coefficients for $D = 239$.

8 Acknowledgments

It is a pleasure to thank Marcel Martin, who forced the second author to resume this work, undertaken long ago. Thanks also to Allombert who kindly sent us his article [2].

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] H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1993.

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

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

[12] 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.

[13] 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.

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

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

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

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

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

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

[20] 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/`.

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

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

[23] C. C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its applications*. Cambridge University Press, 1994.



Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399