

On the calculation of roots of unity in a number field

Pascal Molin

May 2010

Résumé

We review some algorithms for the calculation of roots of unity in a number field, and suggest a hybrid approach which proves to be efficient in average.

1 Introduction

Let $\mathbb{K} = \mathbb{Q}(\alpha)$ be a number field, and assume it is given by a defining polynomial and an integral basis. This paper aims at studying algorithmic approaches to work out the roots of unity contained in \mathbb{K} , that is giving the expression of a primitive root on the integral basis.

We first recall a widely used algorithm based on Kannan's lattice enumeration. Then we suggest a more heuristic approach combining local-global guesses and LLL reduction. Finally, we describe a rigorous algorithm of factorisation of the cyclotomic polynomial, to be used jointly with the preceding heuristics.

Along the way, we introduce a linear programming approach to construct number fields with prescribed ramification.

The algorithm we describe is now part of the PARI/gp software (function `nfrootsOf1`).

Notations

For the following :

- \mathbb{K} is a number field of degree n , $\mathcal{O}_{\mathbb{K}}$ its ring of integers and $\text{disc}_{\mathbb{K}}$ its discriminant. The algebraic norm of an element $x \in \mathbb{K}$ is noted $\text{Norm}(x)$.
- m denotes the number of roots of unity present in \mathbb{K} , or assumed to be. A primitive root is noted ζ_m .
- p is a prime number, \mathfrak{p} an integer ideal dividing it in $\mathcal{O}_{\mathbb{K}}$. Let $\mathbb{k}(\mathfrak{p})$ be its residual field and $\text{Frob}_{\mathfrak{p}}$ the Frobenius automorphism induced in \mathbb{K} , if the extension is Galois.
- for σ an embedding $\mathbb{K} \rightarrow \mathbb{C}$, we note x^σ its action on x .

2 Short vectors : Kannan's algorithm

\mathbb{K} is a separable extension, so one has n embeddings

$$\sigma : \mathbb{K} \hookrightarrow \mathbb{C}.$$

It makes it possible to define a euclidean norm on the \mathbb{Z} -module $\mathcal{O}_{\mathbb{K}}$, putting

$$T_2(x) = \sum_{\sigma} |\sigma(x)|^2.$$

The roots of unity in \mathbb{K} are then the shortest non-zero vectors of the lattice $\mathcal{O}_{\mathbb{K}}$ with the norm T_2 .

Proposition 2.1

For all $x \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$, one has $T_2(x) \geq [\mathbb{K} : \mathbb{Q}]$, with equality if and only if x is a root of unity.

Démonstration : Let $n = [\mathbb{K} : \mathbb{Q}]$, and $x \in \mathcal{O}_{\mathbb{K}}$. The arithmetic-geometric means reads

$$T_2(x) = \sum_{\sigma} |\sigma(x)|^2 \geq n \left(\prod_{\sigma} |\sigma(x)|^2 \right)^{\frac{1}{n}} = n |\text{Norm}(x)|^{\frac{2}{n}}. \quad (1)$$

In particular, if $x \neq 0$, $|\text{Norm}(x)| \geq 1$ which proves the first point.

On the other hand, if x is a vector of norm n , the equality case of the preceding inequality gives $|\sigma(x)| = 1$ for each embedding σ .

One concludes that x is a root of unity with a classical reasoning due to Kummer : since all powers of x have the same property, and since the coefficients of their characteristic polynomials are bounded in the $|\sigma(x^k)|$, these polynomials are finite number, hence their roots. So there exist two exponents $k \neq l$ such that $x^k = x^l$, which proves that $x \neq 0$ is a root of unity. \square

Thus the computation of roots of unity in \mathbb{K} amounts to enumerating vectors in the ellipsoid $T_2(x) \leq n$.

There are two main algorithms performing this task : the first is due to [Fincke and Pohst(1985)], the other to [Kannan(1985)]. These are deterministic algorithms which rely on an initial reduction of the lattice and a exhaustive enumeration of its short vectors. The complexity of this task is in any case exponential, respectively $2^{O(n^2)}$ and $O(n^{\frac{n}{2}})$ binary operations [Hanrot and Stehlé(2007)].

2.1 Results

Dispite its huge theoretic – aka worst-case – complexity, this exhaustive search performs very well in practice in the following settings : low dimension (say $n \leq 50$) ; when there are no nontrivial roots of unity ; or when \mathbb{K} is cyclotomic.

However, one can easily construct number fields for which the enumeration step lasts almost forever. In particular, compositum of small fields which occur frequently in practice.

As an example, the polynomial

$$\begin{aligned}
P = & x^{66} - x^{65} + x^{64} - x^{62} + 2x^{61} - 2x^{60} + x^{59} + x^{58} - 3x^{57} + 4x^{56} - 3x^{55} \\
& + 4x^{53} - 7x^{52} + 7x^{51} - 3x^{50} - 4x^{49} + 11x^{48} - 14x^{47} + 10x^{46} + x^{45} - 15x^{44} \\
& - 20x^{43} + 21x^{42} - 36x^{41} + 16x^{40} + 5x^{39} - 41x^{38} + 57x^{37} - 52x^{36} + 11x^{35} \\
& + 46x^{34} - 98x^{33} + 109x^{32} - 63x^{31} - 35x^{30} + 144x^{29} - 207x^{28} + 172x^{27} \\
& - 28x^{26} - 179x^{25} + 351x^{24} - 379x^{23} + 200x^{22} + 151x^{21} + 114x^{20} + 86x^{19} \\
& + 65x^{18} + 49x^{17} + 37x^{16} + 28x^{15} + 21x^{14} + 16x^{13} + 12x^{12} + 9x^{11} + 7x^{10} \\
& + 5x^9 + 4x^8 + 3x^7 + 2x^6 + 2x^5 + x^4 + x^3 + x^2 + 1
\end{aligned}$$

defines a field containing the forty-sixth roots of unity. The search for roots of unity using Fincke-Pohst algorithm (with the PARI/gp implantation) has been interrupted after four weeks on a dedicated machine.

3 Local-global principle

The local global principle works for roots of unity.

Proposition 3.1

The following statements are equivalent :

- (i) $\mu_m \subset \mathbb{K}$;
- (ii) $\mu_m \subset \mathbb{K}_{\mathfrak{p}}$ for each prime \mathfrak{p} ;
- (iii) for every prime p not dividing m and all prime ideals \mathfrak{p} dividing p , $\text{Norm}(\mathfrak{p}) \equiv 1 \pmod{m}$.

Démonstration : We consider the Galois extension $\mathbb{K}(\mu(n))/\mathbb{K}$. Let us suppose that for each non ramified prime \mathfrak{p} one has $\text{Norm}(\mathfrak{p}) \equiv 1 \pmod{m}$, then the action of $\text{Frob}_{\mathfrak{p}}$ on a m -th root of unity is given by $\zeta \mapsto \zeta^{\text{Norm}(\mathfrak{p})} = \zeta$, so that this Frobenius acts as identity. Čebotarev's density theorem concludes that the Galois group contains only the trivial class of conjugacy, which means that the extension is degree 1. \square

Remark : Čebotarev's theorem allows to replace *every prime p* by *almost all primes*, that is a set of primes of density 1.

For now on, we write $R_{\mathbb{K}}(m, x)$ the fact that the property (iii) holds "up to x "

$$\forall p \leq x, \forall \mathfrak{p} \mid p \mathcal{O}_{\mathbb{K}}, \text{Norm}(\mathfrak{p}) \equiv 1 \pmod{m}. \quad (2)$$

On the contrary, when \mathbb{K} does not contain μ_m , we define the first failure

$$S(\mathbb{K}, m) = \inf \{ p, \exists \mathfrak{p} \mid p \mathcal{O}_{\mathbb{K}} \text{ t.q. } \text{Norm}(\mathfrak{p}) \not\equiv 1 \pmod{m} \}. \quad (3)$$

Using the local-global principle leads to the study of the following :

1. finding values $x_{\mathbb{K}}$ such that $R_{\mathbb{K}}(m, x_{\mathbb{K}}) \Leftrightarrow \mu_m \subset \mathbb{K}$;
2. characterise large (finite) values of $S(\mathbb{K}, m)$.

3.1 Effective Čebotarev's theorems

The first question is solved with the so-called "effective" Čebotarev's density theorems.

Under the generalized Riemann's hypothesis (GRH), [Lagarias and Odlyzko(1977), cor1.2] give the following statement, (where the constant is due to [Serre(1981)]) :

Theorem 3.2

Let \mathbb{L}/\mathbb{K} be a Galois extension, and assume that the Dedekind zeta function of \mathbb{L} does not have any zero of real part greater than $\frac{1}{2}$. Then for every conjugacy class C of $\text{Gal}(\mathbb{L}/\mathbb{K})$, there exists an unramified prime \mathfrak{p} of \mathbb{K} with $\text{Frob}_{\mathfrak{p}} \in C$ and

$$\text{Norm}(\mathfrak{p}) \leq c(\log \text{disc}(\mathbb{L}))^2$$

where c is an absolute constant, which one can take equal to 70.

One applies this theorem to any non trivial class of isomorphisms of $\mathbb{K}(\mu_m)/\mathbb{K}$, which gives

Proposition 3.3

If $\mu_m \notin \mathbb{K}$,

$$S(\mathbb{K}, m) \leq 70 \left(\log \text{disc}(\mathbb{K}(\mu_m)) \right)^2.$$

On the other hand, one can use the majorations of [Serre(1981)] to remove the discriminant and give a criterion depending only on the degree of \mathbb{K} and its ramification.

Proposition 3.4

If $\mu_m \notin \mathbb{K}$,

$$S(\mathbb{K}, m) \leq \sqrt{70} n \varphi(m) \left(\log(n) + \log \varphi(m) + \sum_q \log q \right).$$

3.2 Application : heuristic determination

One can guess the number of roots of unity in \mathbb{K} with the following procedure : "compute the gcd of a number of values $\text{Norm}(\mathfrak{p}) - 1$ until it stabilizes".

This guess can be sharpened considering ramification conditions induced by the inclusion $\mathbb{Q}(\zeta_m) \subset \mathbb{K}$.

Proposition 3.5

If $\mathbb{Q}(\zeta_{p^k}) \subset \mathbb{K}$, one has

- $(p-1) \mid [\mathbb{K} : \mathbb{Q}]$ and $k \leq 1 + v_p([\mathbb{K} : \mathbb{Q}])$;
- $k \leq \frac{v_p(\text{disc}(\mathbb{K}))}{[\mathbb{K} : \mathbb{Q}]} - \frac{1}{p-1}$.

Démonstration : The first point derives from the multiplicativity of degrees

$$[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = (p-1)p^{k-1} \mid [\mathbb{K} : \mathbb{Q}].$$

Moreover, the study of discriminants [Lang(1964)] gives

$$\text{disc}(\mathbb{Q}(\zeta_{p^k})) = \pm p^{p^{k-1}(pk-k-1)}$$

and

$$\text{disc}(\mathbb{K}_1 \mathbb{K}_2) = \text{disc}(\mathbb{K}_1)^{[\mathbb{K}_1 \mathbb{K}_2 : \mathbb{K}_1]} \text{disc}(\mathbb{K}_2)^{[\mathbb{K}_1 \mathbb{K}_2 : \mathbb{K}_2]}.$$

This gives the following criterion :

$$v_p(\text{disc}(\mathbb{K})) \geq \frac{pk-k-1}{p-1} [\mathbb{K} : \mathbb{Q}]. \quad (4)$$

hence the second point of the proposition. □

The guess procedure is then :

Algorithme 1: Heuristic on the number of roots

Input : \mathbb{K} a number field

Output : a multiple m of the number of roots of unity in \mathbb{K} ;

Set $m = 0$ and $p = 2$;

repeat

- set p next prime;
- compute the decomposition of p in $\mathcal{O}_{\mathbb{K}}$;
- compute the gcd f of the inertia degrees;
- set $m = \text{gcd } m, p^f - 1$;

until m stable since the last N loops;

for each divisor $p_i^{k_i}$ of m **do**

- if** $p_i - 1 \nmid [\mathbb{K} : \mathbb{Q}]$ **then**
- $k_i = 0$
- else**
- $k_i = \min(k_i, 1 + v_{p_i}([\mathbb{K} : \mathbb{Q}])$;
- $k_i = \min(k_i, \frac{v_{p_i}(\text{disc}(\mathbb{K}))}{[\mathbb{K} : \mathbb{Q}]} - \frac{1}{p_i-1})$;
- end**

done

return the product of $p_i^{k_i}$

The number output is in any case a multiple of the number of roots of unity in \mathbb{K} , and in most case it matches the true value.

prime l	$S(\mathbb{K}, l)$	prime l	$S(\mathbb{K}, l)$
7	3	18191	29
23	5	31391	31
71	7	366791	43
311	11	4080359	47
479	13	12537719	53
1559	17	30706079	59
5711	19	36415991	61
10559	23	82636319	67

TABLE 1: $S(\mathbb{K}, l)$ for real cyclotomic fields

3.3 Relevance

This heuristic is quite precise in practice. However, one can build number fields \mathbb{K} for which $S(\mathbb{K}, m)$ is large, which means that any sensible implementation of the test 1 (i.e. any reasonable value of N) will output a strict multiple of m .

We sketch such buildings in the next paragraphs.

3.3.1 Example of real cyclotomic fields

One considers the l -th cyclotomic field $\mathbb{Q}(\zeta_l)$, and its totally real subfield $\mathbb{K} = \mathbb{Q}(\zeta_l^+)$, with l such that $S(\mathbb{Q}(\zeta_l^+), l)$ is large.

One has $\text{Norm}(\mathfrak{P}) \equiv 1 \pmod{l}$ for every prime \mathfrak{P} in $\mathbb{Q}(\zeta_l)$, and the inertia degree of \mathfrak{P} is exactly the multiplicative order of p in $(\mathbb{Z}/l\mathbb{Z})^*$.

As a consequence, one still has $\text{Norm}(\mathfrak{p}) \equiv 1 \pmod{l}$ in \mathbb{K} if and only if \mathfrak{p} already has the same inertia degree in \mathbb{K} .

The latter is given by the order of p^2 in the group of squares modulo l . It is equal to the order of p if and only if this order is odd.

A numerical search with this criterion gives interesting values of l , and the first prime p for which $\text{Norm}(\mathfrak{p}) \not\equiv 1 \pmod{l}$. We collected the first values in table 1 : S -values obtained that way are very small.

3.3.2 Example of quadratic compositum

We obtain better situation considering quadratic fields $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. Let us focus on fourth and sixth roots of unity.

μ_4 : We want $\text{Norm}(\mathfrak{p}) \equiv 1 \pmod{4}$, which means that primes congruent to 3 mod 4 are inert, that is $\left(\frac{D}{p}\right) = -1$.

μ_6 : This time, we demand that $\text{Norm}(\mathfrak{p}) \equiv 1 \pmod{3}$, so that the primes $p \equiv 2 \pmod{3}$ (except 2) should be inert ($\left(\frac{D}{p}\right) = -1$).

D	$S(\mathbb{Q}(\sqrt{D}), 4)$	$c \geq$	D	$S(\mathbb{Q}(\sqrt{D}), 6)$	$c \geq$
2	7	2.28e-1	2	17	4.21e-1
3	11	4.45e-1	-5	23	3.43e-1
6	19	3.17e-1	7	29	3.69e-1
21	43	5.48e-1	10	41	4.47e-1
-133	47	2.98e-1	17	47	7.60e-1
-253	67	3.50e-1	-177	71	4.12e-1
1190	71	2.11e-1	1295	89	2.39e-1
-1290	83	2.43e-1	-2033	101	2.47e-1
-4830	107	2.40e-1	-5270	113	2.31e-1
46221	127	2.16e-1	19587	137	2.70e-1
47033	131	2.22e-1	160978	179	1.31e-2
93057	139	2.11e-1			

TABLE 2: $S(\mathbb{K}, 4)$ and $S(\mathbb{K}, 6)$ for quadratic fields

Considering only one field $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ one obtains table 2.

With a compositum of two fields $K = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, we can also mimic the eighth roots of unity when all primes congruent to $3, 5, 7 \pmod{8}$ have a non trivial inertia in at least one quadratic subfield.

As an example $P = x^4 + 1432x^2 + 532900$, which is obtained by composition of $x^2 - 7$ and $x^2 + 723$ passes all tests up to $p = 131$. The heuristic detects wrongly 24th roots of unity.

Focusing on 8th roots, one obtains for example $P = x^4 + 24x^2 + 1156$, which passes all tests up to $p = 127$.

3.3.3 Generalization with linear programming

Larger values of $S(\mathbb{K}, m)$ can be reached with the same idea of composing small fields, in order to distribute inertia degrees among them.

Linear programming can be used to find good combinations with a degree as small as possible. Let $\mathbb{K} = \mathbb{K}_1 \dots \mathbb{K}_n$ be the compositum of the $\mathbb{K}_j = \mathbb{Q}[X]/(Q_j)$.

As before, one demands that for each prime p up to a certain fixed bound, the inertia degree $f_{p/p}$ of $\mathfrak{p} \mid p\mathcal{O}_{\mathbb{K}}$ is a multiple of the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$.

Let us write

$$(\mathbb{Z}/m\mathbb{Z})^\times = \prod_q \prod_i \mathbb{Z}/q^{e_{q,i}}\mathbb{Z},$$

the p -primary decomposition of $(\mathbb{Z}/m\mathbb{Z})^\times$ and

$$o(p) = \prod_q q^{\alpha_{p,q}}$$

the decomposition into prime factors of the order of p modulo m .

m	$\deg(\mathbb{K})$	$\log \text{disc}(\mathbb{K}(\mu_m))$	$S(\mathbb{K}, m)$	$c \geq$
6	8	29.1	131	1.55e-1
6	8	29.9	149	1.67e-1
4	16	137.3	991	5.26e-2
4	32	249.4	2003	3.22e-2
4	32	364.0	2999	2.26e-2
6	32	344.0	2999	2.53e-2
6	32	397.1	3089	1.96e-2

TABLE 3: Fields found with linear programming (using GLPK)

Then define the coefficients

$$\delta(\mathbb{K}_j, p, q^\alpha) = \begin{cases} 1 & \text{if } \forall \mathfrak{p} \mid p \mathcal{O}_{\mathbb{K}_j}, \text{Norm}(\mathfrak{p}) \equiv 1 \pmod{[q^\alpha]} \\ 0 & \text{otherwise.} \end{cases}$$

The property $R(m, x)$ is then coded by the following linear program, where the columns are indexed by a family of polynomials Q_j , and the lines describe the inertia degree with respect to every prime p less than x :

$$\forall p \leq x, \forall q \mid o(p), \sum_j x_j \delta(\mathbb{K}_j, p, q^{\alpha_{p,q}}) \geq 1 \quad (5)$$

We add the following objective function :

$$\text{Minimize } \sum_j x_j \deg(Q_j) - \text{disc}(Q_j)^{-1}$$

in order to minimize the degree of the compositum \mathbb{K} , and to a minor extent its discriminant.

As is, this program would output the m -th cyclotomic extension as a compositum of some of its subfields. Thus we add some low inertia constraints on a prime $p > p_n$ to avoid this situation.

Running this integer linear program, even without reaching the true optimum, yields extensions with interesting extremal ramification properties in the context of effective Čebotarev theorem.

In particular, we tried to obtain large values of the c constant appearing in theorem 3.2.

The table 3 shows some of the constructions obtained this way. The c values are very small compared to the proven value 70, especially when we aim at larger S or m greater than 6.

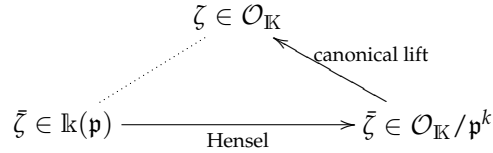
4 Roots lifting

This section is an adaptation to the roots of unity setting of the general algorithm of polynomial factorization in number field, for which we refer to [Belabas(2004)].

4.1 Principle

Once (heuristically) known \mathbb{K} contains the m -th roots of unity, they can be found factoring the cyclotomic polynomial Φ_m , which amounts to :

1. exhibit a root ζ modulo a prime ideal \mathfrak{p} ;
2. lift ζ modulo \mathfrak{p}^k with Hensel's lemma ;
3. take a representative in $\mathcal{O}_{\mathbb{K}}$ as soon as the fundamental domain of the lattice \mathfrak{p}^k is sufficiently large.



The first two steps are straightforward. As for the third, one must make sure that the lift will be a root of unity, if it exists. If it is not, it will contradict the heuristic which will have to be refined.

4.1.1 Lifting in $\mathcal{O}_{\mathbb{K}}$

The lattice \mathfrak{p}^k is represented with a basis (v_1, \dots, v_n) , and the canonical lift $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}^k \rightarrow \mathcal{O}_{\mathbb{K}}$ is the lift belonging to the centered fundamental domain

$$D = \left\{ \sum x_i v_i, x_i \in]-\frac{1}{2}; \frac{1}{2}] \right\}.$$

The proposition 2.1 gives us some information about the locus of roots of unity :

$$\zeta \in B_{T_2}(0, n) = \{x \in \mathcal{O}_{\mathbb{K}}, T_2(x) \leq n\}.$$

As a consequence, one can make sure that the lift will output a root of unity if the ball of radius n is included in the fundamental domain of the lattice \mathfrak{p}^k . The lemma 4.1 below will give such a criterion.

Let us introduce the radius of the maximal ball included in the fundamental domain. It will be bigger if its basis (v_1, \dots, v_n)

- is almost orthogonal ;
- is made of short vectors.

As a consequence, it is desirable to begin with a LLL-reduction of the lattice \mathfrak{p}^k , which amounts to improve the above criteria.

4.2 Detailed algorithm

Let us suppose that we know a multiple m of the number of roots of unity in \mathbb{K} , thanks to heuristic 1.

Algorithm 2: Modular calculation of roots of unity

Input : \mathbb{K} a number field with a basis of $\mathcal{O}_{\mathbb{K}}$, a multiple m of the order of $\mu_{\mathbb{K}}$

Output : the expression of a primitive root in $\mu_{\mathbb{K}}$

begin

- choose a prime p ;
- evaluate the lift exponent k ;
- repeat for** k increasing
 - compute \mathfrak{p}^k and determine a LLL-reduced basis;
 - compute the maximal radius in its fundamental domain D ;
- until** $B_{T_2}(0, n) \subset D$;
- for each** $q = p^l$ dividing m **do**
 - /*look for ζ_q */*
 - repeat for** l decreasing
 - compute a q -th root of unity modulo p ;
 - lift it modulo \mathfrak{p}^k by Hensel ;
 - until** we get a representative ζ_q in $\mathcal{O}_{\mathbb{K}} \cap B$;
- done**
- return** product of ζ_q

end

In the following, we give some details on each step.

4.2.1 Choice of p

Theoretically, every non ramified prime allows to perform the following steps. In practice, one must balance two aspects : a large value of p or a greater inertia degree result in a lattice \mathfrak{p} of larger volume, thus reducing the exponent k . The drawback is however the cost of calculations in $\mathbb{k}(\mathfrak{p})$.

4.2.2 Computations in $\mathbb{k}(\mathfrak{p})$

We use the standard Berlekamp's algorithm to factor the cyclotomic polynomial Φ_m in the finite field $\mathbb{k}(\mathfrak{p}) = \mathbb{F}_p[X]/\bar{P}$.

It has simple roots, and we choose one $\bar{\zeta}$.

4.2.3 Lifting

For every exponent k , powers of \mathfrak{p} are given by

$$\mathfrak{p}^k = \langle p^k, \beta^k \rangle.$$

The value $\zeta \bmod \mathfrak{p}^k$ is lifted via Hensel's lemma.

We then LLL reduce \mathfrak{p}^k to straighten its fundamental domain and improve the following criterion.

4.2.4 Ball inclusion criterion

Lemma 4.1 (Largest inscriptible ball)

Let Λ be a lattice given by a basis (v_1, \dots, v_n) , and put $G = (\langle v_i, v_j \rangle)$ its Gram matrix

The radius of the largest ball included in the fundamental domain of Λ is given by the maximum norm of the columns of the inverse G^{-1} :

$$R_{\max} = \frac{1}{2 \max_j \sqrt{(G^{-1})_{j,j}}}.$$

Démonstration: This radius is the shortest distance of the center of D to its facets.

With a trivial translation, each of these distances is given by

$$d\left(\sum \frac{v_i}{2}, H_j\right) = \frac{1}{2}d(v_j, H_j)$$

where $H_j = \text{Vect}(v_1, \dots, \check{v}_j, \dots, v_n)$ is the hyperplane spanned by the $v_i, i \neq j$.

Let us write \check{v}_j the orthogonal vector to H_j defined by

$$\langle \check{v}_j, v_i \rangle = \delta_{i,j},$$

aka \check{v}_j is solution of the system

$$G\check{v}_j = (\delta_{i,j})_i.$$

It is precisely the j -th column of G^{-1} .

We then obtain $|\langle \check{v}_j, v_j \rangle| = d(v_j, H_j) \|\check{v}_j\| = 1$, hence

$$d(v_j, H_j) = \|\check{v}_j\|^{-1} = \|G_j^{-1}\|^{-1}.$$

It remains to compute the norm

$$\|G_j^{-1}\|^2 = {}^t G_j^{-1} G G_j^{-1} = G_{jj}^{-1},$$

which concludes the proof. \square

For calculations, it is preferable to express \check{v}_i on the orthonormal basis (v_j^*) , that is to replace the Gram matrix G by the Gram-Schmidt orthogonalization matrix

$$K = (\langle v_i^*, v_j \rangle)_{i,j}$$

The inversion step is simpler since this matrix is triangular. The computations have to be adapted only when taking the norm, where the orthogonality give

$$\|K_j^{-1}\|^2 = \sum_i \frac{K_{i,j}^2}{\|v_i^*\|^2}.$$

As a consequence we have the alternative expression

$$R_{\max} = \frac{1}{2} \min_j \sqrt{\sum_i \frac{K_{i,j}^2}{\|v_i^*\|^2}}^{-1}. \quad (6)$$

All in all, the fundamental domain Ainsi, l'on dispose d'un domaine fondamental convenable dès que $R_{\max} \geq n$ pour une base idoine du réseau \mathfrak{p}^k .

4.2.5 Estimates for the exponent k

The most costly part of the algorithm is the LLL reduction of \mathfrak{p}^k , whose complexity is cubic in k . As a consequence, it is crucial to estimate k as precisely as possible so as to make the lifting possible.

A study of the formula (6), taking advantage of the fact that the basis is LLL reduced, gives the following upper bound [Belabas(2004)]

$$R_{\max} \geq \frac{T_2(v_1)}{2\left(\frac{3\sqrt{\gamma}}{2}\right)^{n-1}}.$$

Moreover, the norm of $v_1 \in \mathfrak{p}^k$ is a multiple of $\text{Norm}(\mathfrak{p})^k$ and the arithmetic-geometric means (1) gives

$$T_2(v_1) \geq n \text{Norm}(\mathfrak{p})^{\frac{2k}{n}}.$$

Thus we have :

$$k \leq \frac{n \log\left(2n^{\frac{3}{2}} \left(\frac{3\sqrt{\gamma}}{2}\right)^{n-1}\right)}{2f \log(p)} = O\left(\frac{n^2}{f \log(p)}\right).$$

5 Linear relations between roots

Running the heuristic 1 usually gives a strong confidence that \mathbb{K} contains μ_m , and we can try to output the expression of a primitive root while looking for linear integer dependency between a complex approximation of this root and those of the integer basis elements.

Such relations can be found thanks to LLL in a very classical way. It amounts to reduce the lattice basis given by the columns of the following matrix, where $\sigma : \mathbb{K} \rightarrow \mathbb{C}$ is a fixed embedding.

$$A_\Lambda = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & \ddots & \vdots \\ \vdots & & & 0 \\ 0 & \cdots & 0 & 1 \\ [M\text{Re}(\omega_1^\sigma)] & \cdots & [M\text{Re}(\omega_n^\sigma)] & [Me^{\frac{2i\pi}{m}}] \\ [M\text{Im}(\omega_1^\sigma)] & \cdots & [M\text{Im}(\omega_n^\sigma)] & [Me^{\frac{2i\pi}{m}}] \end{pmatrix} \quad (7)$$

Here M is chosen in such a way that the shortest vector of the lattice must give an equality

$$e^{\frac{2i\pi}{m}} = \sum_{i=1}^n \alpha_i \omega_i^\sigma,$$

that is it must have its last component equal to zero and other components small, while other vectors should be of norm in the greater range given by M .

Rigorously setting up this knapsack strategy demands two estimates : an upper bound for the expected vector norm, and a lower bound for other unwanted vectors. We give such bounds in the proposition 5.2 below.

Then, the properties of LLL-reduced basis (proposition 5.4) allow to choose the constant M to filter exactly the wanted vector.

Notations Every vector Z of Λ is the data of an algebraic integer x given by its coordinates on the basis of \mathcal{O} , and the decimal approximation of a complex number Mz formed of the two last components.

More precisely, for each vector $X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \\ k \end{bmatrix}$, we put $Z = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \\ a \\ b \end{bmatrix}$ the product

$A_\Lambda X \in \Lambda$, and we associate the complex number $z = \sum \alpha_i \omega_i^\sigma + ke^{2i\pi/m}$.

We note $\|X\|_2 = \left(\sum \alpha_i^2\right)^{\frac{1}{2}}$ the usual euclidian norm and $\|X\|_1 = \sum |\alpha_i|$.

Then we have

$$\|Z\|_2^2 = \sum \alpha_i^2 + a^2 + b^2 = \|X\|_2^2 + a^2 + b^2. \quad (8)$$

Lemma 5.1

With the above notations, we have

$$\|X\|_2^2 + \left(M|z| + \sqrt{2}\|X\|_1\right)^2 \geq \|Z\|_2^2 \geq \|X\|_2^2 + \left(M|z| - \sqrt{2}\|X\|_1\right)^2$$

Démonstration : In fact, the definition of integer part implies

$$M\operatorname{Re}(z) - \sum |\alpha_i| \leq a \leq M\operatorname{Re}(z) + \sum |\alpha_i|$$

and the same inequality on imaginary parts, so that when taking the square

$$\begin{aligned} a^2 + b^2 &\geq M^2 |z|^2 - 2M \|X\|_1 (|\operatorname{Re}(z)| + |\operatorname{Im}(z)|) + 2 \|X\|_1^2 \\ &\geq \left(M|z| - \sqrt{2} \|X\|_1 \right)^2. \end{aligned}$$

□

Proposition 5.2

Suppose $\mu_m \subset \mathcal{O}$, and set

$$\zeta_m = \sum \alpha_i \omega_i$$

the root of unity whose image by σ is $e^{\frac{2i\pi}{m}}$. Then

- the vector $Z \in \Lambda$ obtained as image of the vector X of components $(\alpha_1, \dots, \alpha_n, -1)$ satisfies

$$\|Z\|_2^2 \leq 2nC_{\mathcal{O}} + 2 \tag{9}$$

- for all vector Z in Λ whose associated complex number z is non zero, we have

$$\|Z\|_2 \geq \frac{1}{\sqrt{n+1}} \left(\frac{M}{\sqrt{2}\check{C}_{\sigma}} \right)^{\frac{1}{n}} \tag{10}$$

where $C_{\mathcal{O}}$ and \check{C}_{σ} are explicit constants depending on the order \mathcal{O} and defined by the equations (14) and (17) (in appendix).

Démonstration : The vector Z corresponds to the complex $z = 0$, so lemma 5.1 implies $\|Z\|_2^2 \leq \|X\|_2^2 + \|X\|_1^2 = \|\zeta\|_2^2 + \|\zeta\|_1 + 2$. With the trivial upper bound $\|\zeta\|_1 \leq \|\zeta\|_2^2$, the corollary A.2 proves the assertion.

The second part is deduced from lemma 5.1, along with the following lower bound :

Lemma 5.3

Suppose $\zeta_m \in \mathcal{O}$, then keeping current notations, if $z \neq 0$ we have

$$|z| \geq \frac{1}{\check{C}_{\sigma} \|X\|_1^{n-1}}. \tag{11}$$

where \check{C}_{σ} is defined in proposition A.4.

Démonstration : since we supposed $\zeta_m \in \mathcal{O}$, the complex z is the image by σ of the vector $y = \sum \alpha_i \omega_i + k\zeta_m$ of \mathcal{O} , which is assumed nonzero. The triangle inequality gives (suppose $C_{\tau} \geq 1$),

$$|y^{\tau}| \leq |x^{\tau}| + \left| ke^{2i\pi k/m} \right| \leq C_{\tau} \|x\|_{\mathcal{O}} + |k| \leq C_{\tau} \|X\|_1$$

and since $y \in \mathcal{O}$, we obtain the result from $|\operatorname{Norm}(y)| = \prod |y^{\tau}| \geq 1$. □

Let us resume the proof of proposition 5.2. Putting $U = \|X\|_1 \geq 1$, $|z|$ is a solution of the system

$$\begin{cases} \sqrt{n+2} \|Z\|_2 \geq U + |M|z| - \sqrt{2}U \\ |z| \geq \frac{1}{\check{C}_\sigma U^{n-1}} \end{cases}$$

If $M|z| \leq \sqrt{2}U$, then

$$U \geq \left(\frac{M}{\sqrt{2}\check{C}_\sigma} \right)^{\frac{1}{n}} = U_M \quad (12)$$

so that

$$\sqrt{n+2} \|Z\|_2 \geq U_M.$$

On the other hand, if $M|z| \geq \sqrt{2}U$, then

$$\sqrt{n+2} \|Z\|_2 \geq \frac{M}{\check{C}_\sigma U^{n-1}} - (\sqrt{2} - 1)U$$

with a right-hand member which is decreasing in U , hence always greater than its value for U_M , which is U_M . Thus, if $|z| \neq 0$ we have the inequality (10). \square

The theory of LLL reduction gives a quality bound on the short vector output :

Proposition 5.4

Let Λ be a lattice of dimension n , and Z_1 the first vector of a LLL reduced basis. Then for all nonzero vector Z of Λ we have

$$\|Z_1\|_2 \leq 2^n \|Z\|_2.$$

Démonstration : C.f. [von zur Gathen and Gerhard(2003)]. Note that the lattice here has dimension $n + 1$. \square

To make sure that, under hypothesis of proposition 5.2, the short vector output by the LLL reduction is ζ_m , we only need to make impossible the inequality

$$\frac{1}{\sqrt{n+1}} \left(\frac{M}{\sqrt{2}\check{C}_\sigma} \right)^{\frac{1}{n}} \leq 2^n (2nC_{\mathcal{O}} + 2).$$

Therefore we set

$$M > \sqrt{2}2^{n(n+1)} \check{C}_\sigma (\sqrt{n+2}(nC_{\mathcal{O}} + 1))^n. \quad (13)$$

We have thus proved the following

Theorem 5.5

If M satisfies the condition (13) above, the first vector Z_1 of a LLL reduced

basis falls satisfies :

- either its n first components give the expression of a m -th primitive root of unity ζ_m ;
- or \mathcal{O} does not contain the group of m -th roots of unity.

In practice, the size of M would lead to slow computations. However we can decide to run the reduction with a lower value, hoping to obtain a good result, eventually consenting to switch to a guaranteed algorithm to get the root or prove it does not exist in case of failure.

Algorithm 3: Linear dependency

Input : a number field \mathbb{K} with a basis of $\mathcal{O}_{\mathbb{K}}$ and the order m of μ_m

Output : an expression of a m -th primitive root ζ or failure

begin

 choose M to be, say, the n -th root of (13);

 build the matrix (7);

 perform its LLL reduction;

 compute the vector $x \in \mathcal{O}_{\mathbb{K}}$ defined by its first components;

if x is of order m **then**

 | **return** (m, x) ;

else

 | **return** *failure*;

end

end

6 Suggested Algorithm

Collecting previous results, we suggest the following steps, each one making the algorithm stop if it manages to give a definitive answer.

Algorithm 4: Complete strategy

Input : a number field \mathbb{K} with a basis of $\mathcal{O}_{\mathbb{K}}$

Output : the order of μ_m and the expression of a primitive root ζ

```
begin
  guess  $m = \#\mu_{\mathbb{K}}$  with heuristic 1;
  if  $m = 2$  then
    | return ( $m = 2, \zeta = -1$ )
  else
    | try algorithm 3;
    | if we obtain  $\zeta$  of order  $m$  then
    | | return ( $m, \zeta$ )
    | else
    | | run the modular algorithm 2;
    | | return its result ( $m', \zeta$ )
    | end
  end
end
```

7 Timings

The table 4 below gives the results obtained by the different algorithms studied on a panel of polynomials. The factorization algorithm means algorithm 2 run after heuristic 1; and lindep refers to algorithm 3, also after the guess of heuristic 1. A star (\star) indicates that the test had to be interrupted after long calculations.

These results illustrate the strength of the factorisation algorithm : it always give the result in a reasonable time, even in the case we fooled the heuristic step with fields built on purpose (last lines), compelling it to factor more polynomials. The hybrid approach we suggest amounts to take the lindep column, and eventually add factorization column when there is a failure. It manages to solve quickly all simple cases for which Kannan performs very well, and remains polynomial in hard cases.

A Norms on number fields

\mathbb{K} is given by its canonical basis $(1, \alpha, \dots, \alpha^{n-1})$, and the order \mathcal{O} by a basis $(\omega_1, \dots, \omega_n)$. We define M to be the matrix of coordinates of ω_i in the basis (α) , so that

$$(\omega_j) = (\alpha^j)M.$$

For the following, we index with i and j the rows and columns of matrices, so that (x_j) represents the line vector (x_1, \dots, x_n) and (x_i) the corresponding column vector.

Besides algebraic norm, we have to natural norms on \mathbb{K} :

degree	roots m	factorization	Kannan	lindep
<i>small fields</i>				
12	36	20.0ms	0.0ms	20.0ms
32	96	310.0ms	30.0ms	440.0ms
<i>large cyclotomics</i>				
96	194	2mn	690.0ms	5.2s
180	362	1.6h	5.4s	17.4s
<i>compositum of small fields</i>				
54	18	7.7s	* > 3 j	2.3s
66	46	17.4s	* > 4 sem.	1.1s
72	24	15.3s	5h27	<i>fail</i>
<i>fields constructed with linear programming</i>				
24	72	0.2s	0.1s	0.2s
48	24	11s	0.2s	1.7s
54	6	12s	0.2s	2.1s
64	4	18.6s	0.4s	3.3s
64	6	36.4s	0.4s	3.7s

TABLE 4: comparison of all approaches

- the norm $T_2(x) = \sum_{\sigma} |\sigma(x)|^2$ where σ spans $G = \text{Gal}(\mathbb{K}/\mathbb{Q})$
 - the euclidian norm $\|x\| = \|\sum_i x_i \omega_i\| = \sum_i |x_i|^2$.
- We can make the equivalence between these explicit

Proposition A.1

For all $x \in \mathcal{O}$,

$$\|VM\|^{-1} T_2(x) \leq \|x\| \leq \|(VM)^{-1}\| T_2(x)$$

where $V = (\sigma(\alpha^j))_{\sigma,j}$ is the Vandermonde matrix of the conjugates of α and M is the change matrix above.

We note

$$C_{\mathcal{O}} = \|(VM)^{-1}\| \tag{14}$$

the constant on the right.

Démonstration : The conjugates of x are the

$$x^{\sigma} = \left[(\omega_j)(x_i) \right]^{\sigma} = (\alpha_j)^{\sigma} M(x_i) = V_{\sigma} M(x_i) \tag{15}$$

where $V_{\sigma} = ((\alpha^j)^{\sigma})$ is the line of V corresponding to the embedding σ .

Thus we have $(x^{\sigma})_{\sigma} = VM(x_i)$. The T_2 norm being the euclidian norm of the vector $(x^{\sigma})_{\sigma}$, we obtain the two inequalities.

If $x = \zeta$ is a root of unity, we have $T_2(x) = n$ hence the corollary. \square

Corollary A.2

In particular, if ζ is a root of unity in \mathbb{K} , we have

$$\|\zeta\| \leq nC_{\mathcal{O}}. \tag{16}$$

A.1 Estimates on complex embeddings

From the equation (15) we also get

Lemma A.3

For all $x \in \mathcal{O}$,

$$|x^\sigma| \leq \|V_\sigma\| \|M\| \|x\| = C_\sigma \|x\|.$$

This makes it possible to give a lower bound on the modulus of embeddings

Proposition A.4

For all $x \in \mathcal{O} \setminus \{0\}$,

$$|\sigma(x)| \geq \frac{1}{\check{C}_\sigma \|x\|^{n-1}}$$

where

$$\check{C}_\sigma = \|M\|^{n-1} \prod_{\tau \neq \sigma} \|V_\tau\|. \tag{17}$$

Démonstration: Since $|\text{Norm}(x)| = \prod_G |\sigma(x)| \geq 1$, we apply the previous upper bound on all embeddings $\tau \neq \sigma$. \square

Références

[Belabas(2004)] Belabas, K., 2004. A relative van Hoeff algorithm over number fields. J. Symbolic Comput. 37 (5), 641–668.

[Fincke and Pohst(1985)] Fincke, U., Pohst, M., 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math. Comp. 44 (170), 463–471.

[Hanrot and Stehlé(2007)] Hanrot, G., Stehlé, D., 2007. Improved analysis of Kannan’s shortest lattice vector algorithm (extended abstract). In : Advances in cryptology—CRYPTO 2007. Vol. 4622 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 170–186.

- [Kannan(1985)] Kannan, R., 1985. Lattices, basis reduction and the shortest vector problem. In : Theory of algorithms (Pécs, 1984). Vol. 44 of Colloq. Math. Soc. János Bolyai. North-Holland, Amsterdam, pp. 283–311.
- [Lagarias and Odlyzko(1977)] Lagarias, J. C., Odlyzko, A. M., 1977. Effective versions of the Chebotarev density theorem. In : Algebraic number fields : *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975). Academic Press, London, pp. 409–464.
- [Lang(1964)] Lang, S., 1964. Algebraic numbers. Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London.
- [Serre(1981)] Serre, J.-P., 1981. Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. (54), 323–401.
- [von zur Gathen and Gerhard(2003)] von zur Gathen, J., Gerhard, J., 2003. Modern computer algebra, 2nd Edition. Cambridge University Press, Cambridge.