



Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation  
ESA - CNRS 6090

---

# On the Normalization of Numbers and Functions Defined by Radicals

**Marc J. Rybowicz**

Rapport de recherche n° 2002-06

---

Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex  
Tél. 05 55 45 73 23 - Fax. 05 55 45 73 22 - laco@unilim.fr

<http://www.unilim.fr/laco/>



# On the Normalization of Numbers and Functions Defined by Radicals \*

Marc J. Rybowicz  
Laboratoire d'Arithmétique, Calcul Formel et Optimisation  
URA CNRS 1586  
Université de Limoges  
123 Avenue Albert Thomas  
87060 Limoges Cedex  
France  
rybowicz@unilim.fr

January 2, 1996

**Abstract.** We present new results on the degree of algebraic extension fields generated by radicals which extend a classical theorem by Kummer and a more recent publication of M. Kneser. They allow to generalize an algorithm given by R. Zippel for computing a basis for such an extension field. This algorithm may be effectively used by Computer Algebra Systems to handle expressions involving radicals.

---

\* *Mathematical Subject Classification* : 12Y05, 12E05, 11Y40.

This work was partially supported by the Symbolic Computation Group of the University of Waterloo.

# 1 Introduction

Let  $k$  be a field of characteristic 0,  $\beta_1, \dots, \beta_s$  be  $s$  elements of  $k$  and  $n$  be a positive integer. We consider elements  $\alpha_1, \dots, \alpha_s$  of an algebraic closure  $\bar{k}$  of  $k$  such that  $\alpha_i^n = \beta_i$ . In other words, the  $\alpha_i$ 's are  $n$ -th roots of the  $\beta_i$ 's. The problem that we address in this paper is the efficient computation of a basis for  $K = k(\alpha_1, \dots, \alpha_s)$  over  $k$ .

Computer Algebra Systems such as Maple or Mathematica often express solutions to mathematical problems with algebraic numbers and functions defined by radicals. In order to properly manipulate these expressions, the system must be able to decide whether an expression represents zero. This normalization problem clearly reduces to the basis computation mentioned above : if one can decompose the algebraic number (or function) in a basis over some ground field, then the zero recognition problem is solved. Another motivation is the pre-processing of polynomials for factorization, since classical algorithms ([Tra76]) require a basis for the coefficient field. Finally, notice that a mathematical object may be more intelligible when expressed in a basis.

A basis for  $K$  can obviously be determined provided that there is an algorithm for factoring polynomials over finite algebraic extensions of  $k$  : Factor  $x_1^n - \beta_1$  over  $k$  and choose the minimal polynomial  $p_1(x_1)$  of  $\alpha_1$  over  $k$  amongst the irreducible factors of  $x_1^n - \beta_1$ . Then, set  $k_1 = k[x_1]/(p_1)$ , replace  $k$  by  $k_1$ ,  $\beta_1$  by  $\beta_2$  and repeat the process. We eventually obtain a field :

$$k[x_1, x_2, \dots, x_s] / (p_1(x_1), p_2(x_1, x_2), \dots, p_s(x_1, \dots, x_s))$$

which is isomorphic to  $K$ . In the sequel, this algorithm will be referred to as the "brute-force algorithm".

We present in this paper a more efficient method based on extensions of a theorem by Kummer which seem to be interesting in their own right.

Let us introduce some notations :

- we put  $A = \{\alpha_1, \dots, \alpha_s\}$ ,  $B = \{\beta_1, \dots, \beta_s\}$ ,
- $k^*$  is the multiplicative group of non zero elements of  $k$ ,
- $Ak^*$  is the multiplicative group generated by the elements of  $k^*$  and  $A$ ,
- $Bk^{*n}$  is the multiplicative group generated by the  $n$ -th powers of the elements of  $k^*$  and the elements of  $B$ ,
- if  $m$  is an integer, then  $\zeta_m$  denotes a primitive  $m$ -th root of unity. We assume that the equality  $\zeta_{m^d}^d = \zeta_m$  holds for all nonnegative integers  $n$  and  $m$ ,
- if  $l$  is any extension field of  $k$ , then  $\Omega_l$  is the group of  $n$ -th roots of unity contained in  $Al^*$ ,

- $\phi$  is Euler's function.

R. Zippel ([Zip85]) proposed an algorithm based on the following theorem of Kummer (see [Lan65] for an elementary proof). Other related results are quoted in Zippel's paper and ([Sme90]).

**Theorem 1 (Kummer)** *Assume that  $k$  contains  $\zeta_n$ . Then the Galois group of the extension  $K/k$  is isomorphic to the group  $Bk^{*n}/k^{*n}$ . In particular :*

$$[K : k] = (Bk^{*n} : k^{*n}).$$

Unfortunately, Zippel's algorithm requires the introduction of unnecessary roots of unity, and compute a basis for  $k(\zeta_n, A)$  over  $k$ . Adding roots of unity to the ground field can dramatically increase the computation time and Zippel's algorithm is not optimal with this respect.

There has been numerous results along the lines of Kummer's work by Hasse, Siegel, Mordell and others. Several of these theorems are compiled in A. Schinzel's book ([Sch82]). As noted by Schinzel, they are all encompassed by a remarkable result of M. Kneser ([Kne75]) :

**Theorem 2 (M. Kneser)** *Assume that  $K/k$  is a separable extension. Then*

$$[K : k] = (Ak^* : k^*)$$

*if and only if the two following conditions are satisfied :*

1. for all prime  $p$ ,  $\zeta_p \in Ak^* \implies \zeta_p \in k^*$ ,
2.  $1 + \zeta_4 \in Ak^* \implies \zeta_4 \in k^*$ .

Several interesting results derive from this theorem (see for instance [Sch75], [GV81], [AN95]).

In this paper we also build on Kneser's work by relating  $[K : k]$ ,  $(Bk^{*n} : k^{*n})$  and  $[k(\Omega_k) : k]$  when  $n$  is a power of a prime (theorems 4 and 5). Theorems and proofs are gathered in section 2.

Section 3 is devoted to the description of algorithms based on the results of section 2. We give an algorithm which computes a basis for  $K$  over  $k$  using only factorization over fields included in  $k(\Omega)$ .

We assume that there exists algorithms for answering the following questions :

- **Branch choice problem :** Given a radical  $\alpha = \sqrt[n]{\beta}$ , ( $\beta \in k$ ), and a factorization

$$P(x) = x^n - \beta = P_1(x) \dots P_m(x) \tag{1}$$

of the polynomial  $x^n - \beta$ , decide which of the  $P_i$ 's is the actual minimum polynomial for  $\alpha$  over  $k$ . In order to make a branch choice, we need some extra analytical information about  $\alpha$ . If  $\alpha$  is a number, then reliable numerical methods such as interval arithmetic may be used to make a decision. Note that we do not have to prove that a number is zero but only to show that the wrong factors evaluated at  $\alpha$  cannot be zero. If  $\alpha$  is an algebraic function, an evaluation point and the value of  $\alpha$  at this point uniquely determines the branch we are interested in.

- **Perfect n-th power problem :** Given an element  $\beta$  of  $k$ , decide whether there exists  $\gamma$  in  $k$  such that  $\gamma^n = \beta$  and compute  $\gamma$ . It is clear that this problem reduces to the factorization of  $x^n - \beta$  and to the branch choice problem. If  $\beta$  is a number or an algebraic function, the classical algorithms ([Len82]) and ([Tra76]) apply. Since we are only interested in linear factors of  $x^n - \beta$ , several optimizations of these algorithms are possible.

In this paper, we do not address in more detail these two sub-problems. We do not consider neither the question of denesting radicals. (see [Lan92] and [BFHT85]).

## 2 Theoretical foundations

### 2.1 Preliminary results

For the convenience of the reader, we recall a few classical results :

**Theorem 3** *Let  $F$  be a field,  $F_1$  be a finite extension of  $F$  and  $F_2$  a finite Galois extension of  $F$ . Then  $F_1 F_2$  is Galois over  $F_1$ . Moreover, the Galois group of the extension  $(F_1 F_2)/F_1$  is isomorphic to the Galois group of the extension  $F_2/(F_1 \cap F_2)$ .*

**Proof :** See [Lan65]. □

In the next proposition, we use the following notations :

- $p$  is a prime number,
- $e$  and  $m$  are positive integers,
- $a$  is a primitive root mod  $p$ ,
- $\omega = a^{p^{e-1}}$ .

#### Proposition 1

1.  $[Q(\zeta_n) : Q] = \phi(n)$ .
2.  $Q(\zeta_n, \zeta_m) = Q(\zeta_{lcm(m,n)})$ .
3. *If  $p$  is odd, then the Galois group  $G$  of the extension  $Q(\zeta_{p^e})/Q$  is isomorphic to the direct product of a cyclic group  $G_p$  of order  $p-1$  and of a cyclic group  $H_p$  of order  $p^{e-1}$ . The group  $G_p$  is generated by the automorphism  $\sigma$  defined by  $\sigma(\zeta_{p^e}) = \zeta_{p^e}^\omega$ . The group  $H_p$  is generated by the automorphism  $\tau$  defined by  $\tau(\zeta_{p^e}) = \zeta_{p^e}^{(1+p)}$ . For each divisor  $m$  of  $\phi(p^e)$ , there exists a unique subgroup of  $G$  of order  $m$ .*

**Proof:** See [Has80], for instance. □

We then proceed by proving a number of lemmas. We shall make use of the first one without any explicit reference.

**Lemma 1**  $[k(\zeta_n) : k]$  divides  $\phi(n)$ .

**Proof :** Apply theorem 3 to  $F = Q$ ,  $F_1 = k$  and  $F_2 = Q(\zeta_n)$ . The result follows from the fact that  $[Q(\zeta_n) : Q] = \phi(n)$ . □

**Lemma 2** *If  $m = [k(\zeta_{p^e}) : k]$  divides  $p - 1$ , then the Galois group of the extension  $k(\zeta_{p^e})/k$  is generated by the automorphism  $\sigma_m$  defined by :*

$$\sigma_m(\zeta_{p^e}) = \zeta_{p^e}^{\omega^{(p-1)/m}}.$$

**Proof :** Apply again theorem 3 to  $F = Q$ ,  $F_1 = k$  and  $F_2 = Q(\zeta_{p^e})$ . The Galois group of  $k(\zeta_{p^e})/k$  is isomorphic to the Galois group of  $Q(\zeta_{p^e})/(Q(\zeta_{p^e}) \cap k)$ . The latter must be a subgroup of order  $m$  of  $G_p$ . The proposition follows from the fact that  $\sigma_m$  has order  $m$  and  $G$  has a unique subgroup of order  $m$ .  $\square$

**Lemma 3** *Let  $l$  be any extension field of  $k$ . Then,*

$$(Al^* : l^*) = (Bl^{*n} : l^{*n})(\Omega_l l^* : l^*).$$

**Proof:** Let  $\alpha$  be an element of  $Al^*$  and  $\bar{\alpha}$  its class in  $Al^*/l^*$ . We denote by  $\tilde{\beta}$  the class of an element  $\beta$  of  $Bl^{*n}$  in  $Bl^{*n}/l^{*n}$ . Consider the morphism  $\Phi$  below :

$$\begin{array}{ccc} \Phi : Al^*/l^* & \longrightarrow & Bl^{*n}/l^{*n} \\ \bar{\alpha} & \mapsto & \tilde{\alpha}^n \end{array}$$

If  $\bar{\alpha}$  is in the the kernel of  $\Phi$ , then  $\alpha^n = \beta^n$  for some  $\beta$  in  $l^*$ . Thus,  $\alpha = \zeta_n^i \beta$  for some integer  $i$  and  $\alpha \equiv \zeta_n^i \pmod{l^*}$ . Since  $\zeta_n^i \in \Omega_l$ ,  $\alpha \in \Omega_l l^*$  and  $\ker \Phi \subset \Omega_l l^*/l^*$ . Now, if  $\bar{\alpha} \in \Omega_l l^*/l^*$ , then  $\alpha^n \equiv (\zeta_n^i)^n \equiv 1 \pmod{k^{*n}}$  for some integer  $j$ , which proves that  $\Omega_l l^*/l^* \subset \ker \Phi$ .  $\square$

**Example** We choose  $k = Q$ ,  $\alpha_1 = \sqrt[3]{-2}$ ,  $\alpha_2 = \sqrt[3]{3}$ , and  $\alpha_3 = \sqrt[3]{6}$ , where the symbol  $\sqrt[3]{\phantom{x}}$  denotes the principal branch of the cube root function. The set of roots of unity included in  $Ak^*$  is generated by  $\zeta_6 = \sqrt[3]{-1}$  so that  $\Omega_k$  is generated by  $\zeta_3$ . Hence,  $(\Omega_k k^* : k^*) = 3$ . Let us now compute  $(Ak^* : k^*)$ . Consider integers  $e_1, e_2$  and  $e_3$  such that :

$$\alpha_1^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \equiv 1 \pmod{k^*}.$$

Then,

$$\zeta_6^{\pm e_1} \sqrt[3]{2}^{e_1} \alpha_2^{e_2} \alpha_3^{e_3} \equiv 1 \pmod{k^*}.$$

Since  $\alpha_1, \alpha_2$  and  $\sqrt[3]{2}$  are real numbers, we necessarily have  $e_1 \equiv 0 \pmod{3}$ . Hence,  $\alpha_2^{e_2} \alpha_3^{e_3} \equiv 1 \pmod{k^*}$ . It is clear that  $\alpha_1$  and  $\alpha_2$  are multiplicatively independent over  $k^*$ , so that we also have  $e_2 \equiv e_3 \equiv 0 \pmod{3}$ . We conclude that  $(Ak^* : k^*) = 27$ . On the other hand, there is a relation :

$$\beta_1^2 \beta_2^2 \beta_3 \equiv 1 \pmod{k^{*n}}$$

which shows that  $Bk^{*n}/k^{*n} \simeq (Z/3Z)^2$  and  $(Bk^{*n} : k^{*n}) = 9$ .  $\square$

**Lemma 4** *Let  $p$  be a prime number. If  $\zeta_p \in Ak^*$ , then  $\zeta_p \notin k^* \implies p|n$ .*

**Proof:** If  $\zeta_p \in Ak^*$ , then  $\zeta_p^n = \beta \gamma^n$  for some  $\gamma$  and  $\beta$  in  $k^*$ . Writing  $n = pq + r$  with  $0 \leq r < p$ , one obtains immediately that  $\zeta_p^r \in k^*$ . But if  $r \neq 0$  then  $\zeta_p \in k^*$  so that  $\zeta_p \notin k^* \implies r = 0$ .  $\square$

**Lemma 5** *If  $1 + \zeta_4 \in Ak^*$  then  $\zeta_4 \notin k^* \implies 4|n$ .*

**Proof:** If  $1 + \zeta_4 \in Ak^*$ , then  $(1 + \zeta_4)^n \in k^*$ . Writing  $n = 4q + r$  with  $0 \leq r < 4$ , one obtains  $(1 + \zeta_4)^n = (-4)^q b$  where  $b$  is in the set  $\{1, 1 + \zeta_4, 2\zeta_4, 2(\zeta_4 - 1)\}$ . If  $r \neq 0$  then  $\zeta_4 \in k^*$  and the result follows.  $\square$

## 2.2 Power of an odd prime

In this part of the paper,  $p$  denotes an odd prime and we assume that  $n = p^f$ , where  $f$  is a positive integer. We define  $l = k(\zeta_p)$  if  $\zeta_p \in Ak^*$  and  $l = k$  otherwise. Let  $\beta$  be an element of the multiplicative group generated by the elements of  $B$ . We denote by  $\bar{\beta}$  the class of  $\beta$  in  $Bl^{*n}/l^{*n}$  and  $\tilde{\beta}$  the class of  $\beta$  in  $Bk^{*n}/k^{*n}$ . The following sequence of implications :

$$(\tilde{\beta} = \tilde{\gamma}) \implies \beta \gamma^{-1} \in k^{*n} \implies \beta \gamma^{-1} \in l^{*n} \implies (\bar{\beta} = \bar{\gamma})$$

allows to define a morphism  $\Psi$  :

$$\Psi : Bk^{*n}/k^{*n} \longrightarrow Bl^{*n}/l^{*n} \quad (2)$$

$$\tilde{\beta} \longmapsto \bar{\beta}$$

### Proposition 2

1.  $\Psi$  is an isomorphism,

2.

$$(Bl^{*n} : l^{*n}) = (Bk^{*n} : k^{*n}).$$

**Proof :** The second assertion is a trivial consequence of the first one. It remains to prove the first assertion when  $l \neq k$ . The set  $\{\bar{\beta} \mid \beta \in B\}$  is a set of generators for  $Bl^{*n}/l^{*n}$ , so that  $\Psi$  is surjective. We are left to prove that  $\Psi$  is injective. If  $\bar{\beta}$  is an element of the kernel, then there exists an element  $\gamma$  in  $l^*$  such that  $\beta = \gamma^n$ . Let  $\sigma$  denote a generator of the Galois group of  $l/k$ . We have  $\sigma(\gamma^n) = \gamma^n = \sigma(\gamma)^n$  so that  $\sigma(\gamma) = \zeta_n^i \gamma$  for some integer  $i$ . If  $i \equiv 0 \pmod{p^f}$ , then  $\gamma \in k$ ,  $\bar{\beta} = 1$  and we are done. Otherwise, there exists an integer  $j$ , co-prime to  $p$  and a positive integer  $e \leq f$  such that :

$$\zeta_n^i = \zeta_{p^e}^j.$$

Since  $l/k$  is Galois,  $\zeta_n^i$  is in  $l$  and so is  $\zeta_{p^e}$ . Therefore,  $l = k(\zeta_{p^e})$ . The integer  $m = [l : k]$  divides  $\phi(p) = p - 1$ , so that, by lemma 2, we can assume that  $\sigma = \sigma_m$ . If  $t$  is a non negative integer, then we have :

$$\sigma_m(\zeta_{p^e}^t \gamma) = \zeta_{p^e}^{t \omega^{(p-1)/m} + j} \gamma.$$

Now, if we choose  $t$  such that :

$$t \omega^{(p-1)/m} + j \equiv t \pmod{p^e} \quad (3)$$

then  $\gamma_1 = \zeta_{p^e}^t \gamma$  is an element of  $k$  which satisfies  $\gamma_1^n = \beta$ . Hence,  $\bar{\beta} = 1$  and the proof is complete. It remains to prove that equation (3) is always solvable. By Fermat's little theorem,

$$\omega^{(p-1)/m} - 1 = a^{p^{e-1}(p-1)/m} - 1 \equiv a^{(p-1)/m} - 1 \pmod{p}.$$

Since  $a$  is a primitive root modulo  $p$ ,  $a^{(p-1)/m} \not\equiv 1 \pmod{p}$ . Thus,  $\omega^{(p-1)/m} - 1$  is prime to  $p$  and equation (3) has always a solution.  $\square$

**Proposition 3**

$$l(\Omega_l) = k(\Omega_k).$$

**Proof :** Assume that  $l \neq k$ . Then,  $\zeta_p$  is in  $\Omega_k$  and  $l(\Omega_l) = k(\Omega_l)$ . Let  $\zeta$  be an element of  $\Omega_l$ . By definition, there exists  $\alpha \in A$  and  $c \in l$  such that  $\zeta = \alpha c$ . Taking  $n$ -th power in this equality yields  $1 = \beta c^n$  with  $\beta \in B$ . Proposition 2 shows that there exists an element  $d \in k$  such that  $\beta = 1/c^n = 1/d^n$ . Hence,  $c = \zeta_n^j d$  for an appropriate integer  $j$  and it is clear that  $\zeta_n^j$  belongs to  $l$ . Therefore, we have  $\zeta = (\alpha d) \zeta_n^j$ . But  $(\alpha d) \in \Omega_k$  and  $\zeta_n^j \in l = k(\zeta_p) \subset k(\Omega_k)$ . We conclude that  $\zeta \in k(\Omega_k)$  and the proof is complete.  $\square$

**Theorem 4** *Let  $p$  be an odd prime,  $f$  be positive integer and suppose that  $n = p^f$ . Then,*

$$[K : k] = (Bk^{*n} : k^{*n})[k(\Omega_k) : k].$$

**Proof :** The following equalities are trivial :

$$[K : k] = [l(A) : k] = [l(A) : l][l : k].$$

By lemma 4 and lemma 5, the conditions of Kneser's theorem are satisfied for the extension  $l(A)/l$  and we obtain :

$$[K : k] = (Al^* : l^*)[l : k].$$

Lemma 3 implies :

$$[K : k] = (Bl^{*n} : l^{*n})(\Omega_l l^* : l^*)[l : k]$$

Now, applying again Kneser's theorem to the extension  $l(\Omega_l)/l$ , one gets :

$$[K : k] = (Bl^{*n} : l^{*n})[l(\Omega_l) : l][l : k].$$

The theorem follows from propositions 2 and 3.  $\square$

**Example :** We again choose  $k = Q$ ,  $\alpha_1 = \sqrt[3]{-2}$ ,  $\alpha_2 = \sqrt[3]{3}$ , and  $\alpha_3 = \sqrt[3]{6}$ , where the symbol  $\sqrt[3]{\phantom{x}}$  denotes the principal branch of the cubic root function. We have already shown that  $(Bk^{*n} : k^{*n}) = 9$  and that  $\Omega_k$  is generated by  $\zeta_3$ . Hence,  $[Q(\alpha_1, \alpha_2, \alpha_3) : Q] = (Bk^{*n} : k^{*n})[Q(\zeta_3) : Q] = 18$ .  $\square$

## 2.3 Powers of 2

We now consider the case  $n = 2^f$ . It turns out that extra complications occur. For any positive integer  $u$ , we define  $\xi_u = \xi_{2^u} + \xi_{2^u}^{-1}$ . Let  $t$  be the largest integer such that  $\xi_t \in k$  and  $t = \infty$  if no such integer exists. In this section, we denote by  $l$  the field  $k(\zeta_4)$ . Following Schinzel ([Sch77]), we set :

- $a = -1$  if  $t > f$ ,
- $a = (\xi_t + 2)^{2^{f-1}} = \xi_{t+1}^{2^f}$  if  $t < f$ ,
- $a = -(\xi_t + 2)^{2^{f-1}} = -\xi_{t+1}^{2^f}$  if  $t = f$ .

Then, proposition 2 of the previous section is replaced by :

**Proposition 4** *If  $a \in Bk^{*n}$ , then*

$$(Bl^{*n} : l^{*n}) = (Bk^{*n} : \langle k^{*n}, ak^{*n} \rangle),$$

*else*

$$(Bl^{*n} : l^{*n}) = (Bk^{*n} : k^{*n}).$$

**Proof:** We define the morphism  $\Psi$  as in (2). By a lemma of Schinzel ([Sch77][lemma 2]), the kernel of  $\Psi$  is trivial or generated by  $a$ .  $\square$

Let us determine the order of the element  $a$  modulo  $k^{*n}$  :

**Proposition 5** *Assume that  $\zeta_4 \notin k$  and  $n = 2^f > 2$ . Then :*

1.  $-1$  has order 2 modulo  $k^{*n}$ ,
2.  $-(\xi_t + 2)^{2^{f-1}}$  has order 2 modulo  $k^{*n}$  ( $t \neq \infty$ ),
3. the order of  $(\xi_t + 2)^{2^{f-1}}$  is 1 or 2 modulo  $k^{*n}$  ( $t \neq \infty$ ).

**Proof :** It is clear that  $a$  has order at most 2 modulo  $k^{*n}$ . If  $-1 \in k^{*n}$ , then  $\zeta_{2^{f+1}} \in k^*$ . Since  $\zeta_4 \notin k$  this situation cannot happen. If  $-(\xi_t + 2)^{2^{f-1}} \in k^{*n}$ , then  $\zeta_4 (\xi_t + 2)^{2^{f-2}} \in k^*$ . Again, it would imply  $\zeta_4 \in k$ .  $\square$

The order of  $(\xi_t + 2)^{2^{f-1}}$  can actually take the values 1 and 2, as shown by the following examples : We choose  $k = Q(\sqrt{-2})$  and  $A = \{\sqrt[8]{-4}\}$  (we consider principal branches in this example), so that  $t = 2$ ,  $f = 3$  and  $B = \{-4\}$ . It is clear that  $\zeta_4 \notin k$ . We have  $(\xi_2 + 2)^4 = 16 \in Ak^*$  but  $16 = \sqrt{-2}^8$  so we also have  $(\xi_2 + 2)^4 \in k^{*n}$ . If we change the ground field and take  $k = Q$ , then  $(\xi_2 + 2)^4$  has order 2 modulo  $k^{*n}$ .  $\square$

We shall need the lemmas below :

**Lemma 6** For any positive integer  $u$ ,  $k(\xi_u)$  is a Galois extension of  $k$ .

**Proof :** Obvious, since  $k(\xi_u)$  is included in the abelian extension  $k(\zeta_{2^u})$  of  $k$ .  
□

**Lemma 7** Suppose that  $t \neq \infty$ . For any positive integer  $u \geq t$ ,  $\xi_{u+1} \notin k(\xi_u)$ .

**Proof :** We proceed by induction on  $u$  : If  $u = t$ , then the assertion is a trivial consequence of the definition of  $t$ . Let us assume that  $u > t$  and that  $\xi_u$  is not in  $k(\xi_{u-1})$ . If  $\xi_{u+1}$  is in  $k(\xi_u)$ , then we have :

$$\sqrt{2 + \xi_u} = a + b \xi_u,$$

where  $a, b \in k(\xi_{u-1})$ . By squaring this equation and using the induction hypothesis, we obtain the system of equations :

$$\begin{cases} 2 &= a^2 + b^2 (2 + \xi_{u-1}) \\ 1 &= 2 a b \end{cases}$$

Solving for  $a^2$ , one finds that :

$$a^2 = 1 \pm \frac{1}{2} \sqrt{2 - \xi_{u-1}}.$$

Hence, we must have  $\sqrt{2 - \xi_{u-1}} \in k(\xi_{u-1})$ . Since  $\sqrt{2 - \xi_{u-1}}$  is a conjugate of  $\xi_u$  over  $Q$ , by lemma 6, we must have  $\xi_u \in k(\xi_{u-1})$ . This assertion contradicts the induction hypothesis and we conclude that  $\xi_{u+1} \notin k(\xi_u)$ . □

If  $u$  and  $v$  are positive integers ( $u \geq v$ ), we denote by  $N_{u,v}$  the relative norm from  $k(\xi_u)$  to  $k(\xi_v)$ . In particular, if  $t \neq \infty$ , then  $N_{u,t}$  is the norm from  $k(\xi_u)$  to  $k$ .

**Lemma 8** Assume that  $t \neq \infty$ . Then :

1.  $N_{u,t}(\xi_u) = -(2 + \xi_t)$  if  $u = t + 1$ ,
2.  $N_{u,t}(\xi_u) = 2 - \xi_t$  if  $u > t + 1$ .

**Proof :** By lemma 7,  $\xi_{t+1} \notin k$ . The conjugate of  $\xi_{t+1}$  over  $k$  is  $-\xi_{t+1}$  and the first assertion follows. Let  $u$  be an integer satisfying  $u > t + 1$ . By the transitivity of the norm, we have :

$$N_{u,t}(\xi_u) = N_{u-1,t}(N_{u,u-1}(\xi_u)).$$

Repeating the preceding arguments, we find :

$$\begin{aligned}
N_{u,t}(\xi_u) &= N_{u-1,t}(-(2 + \xi_{u-1})) \\
&= N_{u-2,t}(N_{u-1,u-2}(-(2 + \xi_{u-1}))) \\
&= N_{u-2,t}(2 - \xi_{u-2}) \\
&= \dots \\
&= N_{t+1,t}(2 - \xi_{t+1}) = 2 - \xi_t.
\end{aligned}$$

□

Finally, we obtain an extension of ([Sch77][lemma 3]) :

**Lemma 9** *Suppose that  $\zeta_4 \notin k$  and  $t \neq \infty$ . Let  $s$  be an integer such that  $s > t + 1$ . Then  $\zeta_{2^s} \notin k(\zeta_{2^{s-1}})$ .*

**Proof :** We put  $k_1 = k(\xi_{s-1})$ . By lemma 7,  $\xi_s$  does not belong to  $k_1$ . Let  $m$  be the largest integer such that  $\zeta_{2^m}$  belongs to  $k_1(\zeta_4) = k(\zeta_{2^{s-1}})$ . In virtue of ([Sch77][lemma 3]), only two situations can occur : either  $m = s-1$ ,  $\zeta_{2^s} \notin k_1(\zeta_4)$  and we are done, or  $m = s$  and  $\zeta_4 \xi_s = d \in k_1$ . In the latter case, we have  $k(\xi_s) = k(\zeta_{2^s})$ . We now take norms and use lemma 8 :

$$N_{s,t}(\zeta_4 \xi_s) = N_{s,t}(\zeta_4) N_{s,t}(\xi_s) = 2 - \xi_t.$$

On the other hand, since  $d \in k_1$  and  $\xi_s \notin k(\xi_{s-1})$ , we have :

$$N_{s,t}(d) = N_{s-1,t}(N_{s,s-1}(d)) = N_{s-1,t}(d^2) = d_1^2$$

for some  $d_1$  in  $k$ . But if  $2 - \xi_t$  is a square in  $k$ , then  $2 + \xi_t$  is also a square and  $\xi_{t+1}$  belongs to  $k$ . The lemma follows from this contradiction. □

The propositions below are similar to proposition 3 :

**Proposition 6** *Assume that  $\zeta_4 \in \Omega_k$ . If  $a \notin Bk^{*n}$  then  $[l(\Omega_l) : k(\Omega_k)] = 1$ .*

**Proof :** From the assumption,  $l(\Omega_l) = k(\Omega_l)$ . Let  $\zeta$  be an element of  $\Omega_l$ . There exists  $\alpha \in A$  and  $c \in l^*$  such that  $\zeta = \alpha c$ . Raising this equality to the  $n$ -th power yields  $1 = \beta c^n$  with  $\beta \in B$ . By proposition 4 there is an integer  $i$  and an element  $d$  of  $k$  such that  $c = \zeta_n^i d$  and  $\zeta = \alpha d \zeta_n^i$ . Now,  $\alpha d$  is an  $n$ -th root of unity which is in  $Ak^*$  and from the definition, we see that  $\zeta_n^i \in l$ . We conclude that  $\zeta \in k(\Omega_k)$ . □

**Proposition 7** *If  $n > 2$ ,  $t > f$  and  $a = -1 \in Bk^{*n}$  then  $1 + \zeta_4 \in Ak^*$ ,  $\zeta_{2^n} \in k(\Omega_k)$  and  $[l(\Omega_l) : k(\Omega_k)] = 1$ .*

**Proof :** Since

$$-1 = \left( \frac{1 + \zeta_4}{\xi_3} \right)^4 \in Bk^{*n}$$

and  $\xi_3 \in k$ , we also have  $(1 + \zeta_4) \in Ak^*$  and  $\zeta_4 \in Ak^*$ . Hence,  $\zeta_4 \in k(\Omega_k)$  and consequently  $\zeta_{2^t} \in k(\Omega_k)$ . Moreover,  $t > f$  implies that  $\zeta_{2^n} \in k(\Omega_k)$ . Finally, the group  $\Omega_l$ , which contains only  $n$ -th roots of unity, must be included in  $k(\Omega_k)$ .  $\square$

**Proposition 8** *If  $f = t$  and  $a = -\xi_{t+1}^n \in Bk^{*n}$ , then  $1 + \zeta_4 \in Ak^*$ ,  $k(\Omega_k) = k(\zeta_{2^t})$  and  $[l(\Omega_l) : k(\Omega_k)] = 1$ .*

**Proof :** First of all, we treat the case  $f = t = 2$ . Since  $a = -4 \in Bk^{*n}$ ,  $1 + \zeta_4$  belongs to  $Ak^*$ . Consequently,  $\zeta_4 \in \Omega_k$  and  $l(\Omega_l) = k(\Omega_k) = k(\zeta_4)$ . Now, consider the case  $t = f > 2$ . We have :

$$a = \left( \frac{1 + \zeta_4}{\xi_3} \right)^4 (2 + \xi_t)^{n/2}.$$

Since  $f > 2$ , we can extract the fourth root of the right hand side. Therefore, there exists an integer  $j$  such that :

$$\zeta_4^j \left( \frac{1 + \zeta_4}{\xi_3} \right) (2 + \xi_t)^{n/8}$$

is an element of  $Ak^*$ . But  $\xi_3$  and  $(2 + \xi_t)$  are in  $k$  because  $t = f > 2$  : We conclude that  $1 + \zeta_4 \in Ak^*$ . Therefore,  $\zeta_4 \in \Omega_k$  and  $\zeta_n = \zeta_{2^t} \in k(\Omega_k)$ . Again, we must have  $l(\Omega_l) = k(\Omega_k)$ .  $\square$

**Proposition 9** *Assume that  $t < f$ ,  $a = \xi_{t+1}^n \in Bk^{*n}$ . Then :*

1. *If  $a$  has order 1 modulo  $k^{*n}$  and  $\zeta_4 \in \Omega_k$ , then  $[l(\Omega_l) : k(\Omega_k)] = 1$ .*
2. *If  $a$  has order 2 modulo  $k^{*n}$  and  $1 + \zeta_{2^t} \in Ak^*$ , then  $1 + \zeta_4 \in Ak^*$  and  $[l(\Omega_l) : k(\Omega_k)] = 1$ .*
3. *If  $a$  has order 2 modulo  $k^{*n}$ ,  $\zeta_4 \in \Omega_k$  and  $1 + \zeta_{2^t} \notin Ak^*$ , then  $[l(\Omega_l) : k(\Omega_k)] = 2$ .*

**Proof :** If  $a$  has order 1, the argument of the proof of proposition 6 applies.

Now, assume that  $a$  has order 2,  $1 + \zeta_{2^t} \in Ak^*$  and let us prove the second point : If  $t = 2$ , it is clear that  $1 + \zeta_4 \in Ak^*$ . Notice that  $(1 + \zeta_{2^t})^2 = \zeta_{2^t} (2 + \xi_t) \in Ak^*$ . Since  $2 + \xi_t \in k$ , we have  $\zeta_{2^t} \in Ak^*$ . Therefore, if  $t > 3$ , then  $\zeta_8 = (1 + \zeta_4)/\xi_3 \in Ak^*$  and  $1 + \zeta_4$  is in  $Ak^*$ . Let  $\zeta$  denote an  $n$ -th root of

unity in  $\Omega_l$  such that  $\zeta = \alpha c$  with  $\alpha \in A$  and  $c \in l$ . By proposition 4, either the argument used in proposition 6 shows that  $\zeta \in k(\Omega_k)$  or there exists an integer  $j$  and an element  $d$  of  $k$  such that :

$$c = \frac{\zeta_n^j d}{\xi_{t+1}} = \frac{\zeta_n^j \zeta_{2^t+1} d}{1 + \zeta_{2^t}}.$$

In the latter case,  $\zeta_n^j \zeta_{2^t+1}$  is in  $l$ . Our hypothesis implies that the  $n$ -th root of unity  $\alpha d/(1 + \zeta_{2^t})$  belongs to  $Ak^*$ . From :

$$\zeta = \frac{\alpha d}{1 + \zeta_{2^t}} \zeta_n^j \zeta_{2^t+1}, \quad (4)$$

we conclude that  $\zeta \in k(\Omega_k)$ .

Finally, we consider the third situation. Proceeding as in the previous case, we also obtain a relation of the form (4) with  $\zeta_n^j \zeta_{2^t+1}$  in  $l$ . Squaring the latter expression proves that  $\zeta_n^{2j} \in l$ . Notice that we also have :

$$\zeta^2 = \frac{\alpha^2 d^2}{2 + \xi_t} \zeta_n^{2j}$$

Consequently,  $\zeta^2 \in k(\Omega_k)$  and  $[l(\Omega_l) : k(\Omega_k)] \leq 2$ . Since  $a \in Bk^{*n}$ , there exists an integer  $s$  and an odd integer  $i$  such that :

$$\xi_{t+1} = \zeta_{2^t+1} (1 + \zeta_{2^t}) = \zeta_{2^s}^i \alpha d \quad (5)$$

for some  $\alpha \in A$  and  $d \in k$ . We split the problem into three parts : Firstly, we assume that  $s < t + 1$ . Then,  $\zeta_{2^s}$  cannot be in  $\Omega_k$ , otherwise  $1 + \zeta_{2^t}$  would be in  $Ak^*$ . On the other hand, squaring relation (5) shows that  $\zeta_{2^{s-1}}$  is in  $\Omega_k$  : We must have  $\Omega_k = \langle \zeta_{2^{s-1}} \rangle$ . By lemma 9,  $\zeta_{2^s}$  cannot belong to  $k(\Omega_k)$ . But the second equality in 5 shows that  $\zeta_{2^s}$  is an element of  $\Omega_l$ . Therefore, we must have :  $[l(\Omega_l) : k(\Omega_k)] = 2$ .

Secondly, consider the case  $s = t + 1$ . As previously, squaring relation 5, one sees that  $\zeta_{2^{s-1}} = \zeta_{2^t}$  is in  $\Omega_k$ . Relation (5) also yields  $1 + \zeta_{2^t} = \zeta_{2^t}^i \alpha d$  and  $1 + \zeta_{2^t} \in Ak^*$ . The latter inclusion contradicts the hypothesis and we exclude this case.

Then, assume that  $s < t + 1$ . This time, the relation (5) proves that  $\zeta_{2^t+1}$  cannot be in  $\Omega_k$ . However,  $\zeta_{2^t+1}$  belongs to  $\Omega_l$ , so that  $\Omega_k = \langle \zeta_{2^t} \rangle$ . We conclude that  $k(\Omega_k) = k(\zeta_4)$ . If  $\zeta_{2^t+1}$  is in  $k(\Omega_k)$ , a lemma of Schinzel ([Sch77][lemma 3]) shows that  $\zeta_4 \xi_{t+1}$  belongs to  $k$ . But then,  $a$  would have order 1 modulo  $k^{*n}$ . Therefore,  $\zeta_{2^t+1}$  is not in  $k(\Omega_k)$ , and again,  $[l(\Omega_l) : k(\Omega_k)] = 2$ .  $\square$

The following examples show that if  $\zeta_4 \notin k$ ,  $t < f$  and  $1 + \zeta_4 \in Ak^*$ , then we can actually have  $[l(\Omega_l) : k(\Omega_k)] = 1$  or  $[l(\Omega_l) : k(\Omega_k)] = 2$ . In these examples, we consider the principal branch of the radicals involved. We choose  $n = 16$ ,

$k = Q(\sqrt{2})$  so that  $t = 3 < f = 4$ ,  $\xi_t = \sqrt{2}$  and  $\xi_{t+1} = \sqrt{2 + \sqrt{2}}$ . The first example is  $\alpha_1 = \sqrt[3]{-4}$ ,  $\alpha_2 = \zeta_{16} \xi_4$ . Since  $\zeta_8 = \alpha_1^4 / \xi_3$ , we have  $k(\zeta_8) \subset k(\Omega_k)$ . It turns out that  $\zeta_{16}$  is not in  $\Omega_l$ , so that  $\Omega_k = \Omega_l$ . We now replace  $\alpha_2 = \zeta_{16} \xi_4$  by  $\alpha_2 = \xi_4$ . Then we have  $\zeta_{16} \in Al^*$  since  $\zeta_{16} = \xi_4 / (1 + \zeta_8^{-1})$  and  $\zeta_8 \in l$ . Again, one can show that  $\Omega_k = \langle \zeta_8 \rangle$ , but  $\zeta_{16} \notin k(\Omega_k) = Q(\sqrt{2}, \zeta_4)$ .  $\square$

The main result of this section is :

**Theorem 5** *If  $\zeta_4 \notin k$ ,  $f > 2$  and one of the two following conditions is satisfied :*

1.  $t \geq f$  and  $a \in Bk^{*n}$ ,
2.  $t < f$ ,  $a \in Bk^{*n}$ ,  $a$  has order 2 modulo  $k^{*n}$  and  $1 + \zeta_{2^t} \in Ak^*$ ,

then :

$$[K : k] = 1/2(Bk^{*n} : k^{*n}) [k(\Omega_k) : k].$$

In all other cases :

$$[K : k] = (Bk^{*n} : k^{*n}) [k(\Omega_k) : k].$$

**Proof :** Assume for a moment that  $\zeta_4 \in k$  or  $n = 2$  or  $\zeta_4 \notin \Omega_k$ . The latter assumption implies that  $1 + \zeta_4 \notin Ak^*$ . According to Kneser's theorem and lemma 3,

$$[K : k] = (Bk^{*n} : k^{*n})(\Omega_k k^* : k^*).$$

If  $n = 2$ , then  $(\Omega_k k^* : k^*) = [k(\Omega_k) : k] = 1$ . If  $\zeta_4 \in k$ , then we can apply Kneser's theorem to the extension  $k(\Omega_k)/k$  and obtain the result. Finally, if  $1 + \zeta_4 \notin Ak^*$  then  $1 + \zeta_4 \notin \Omega_k k^* \subset Ak^*$  and Kneser's theorem applies again to  $k(\Omega_k)/k$ .

We now assume that  $n > 2$ ,  $\zeta_4 \in \Omega_k$  and  $\zeta_4 \notin k$ . We set  $l = k(\zeta_4)$ . Since  $\zeta_4 \in \Omega_k$ ,  $k(A) = l(A) = K$ . Therefore,

$$[K : k] = [l(A) : l][l : k].$$

The condition of Kneser's theorem are satisfied by the extension  $l(A)/l$ . By Kneser's theorem and lemma 3, we obtain :

$$[K : k] = (Bl^{*n} : l^{*n})(\Omega_l l^* : l)[l : k].$$

We can also apply Kneser's to the extension  $l(\Omega_l)/l$  :

$$[K : k] = (Bl^{*n} : l^{*n})[k(\Omega_l) : k].$$

The theorem is now an immediate consequence of propositions 4 to 9.  $\square$

We close the section by pointing out an important particular case :

**Theorem 6** *If the  $\alpha_i$ 's are real numbers then  $[K : k] = (Bk^{*n} : k^{*n}) [k(\Omega) : k] = (Bk^{*n} : k^{*n})$ .*

**Proof :** Immediate consequence of Kneser's theorem and lemma 3. □

### 3 Algorithms

We present in this section various algorithms for constructing a basis for  $K$  over  $k$ . We have attempted to avoid as far as possible factorization over algebraic extensions of  $k$  and the introduction of spurious roots of unity. The algorithms are inspired by ([Zip85]), but include various improvements based on results of the first section as well as a different presentation. We first treat two important sub-cases :

1. We assume that we know in advance that :

$$[K : k] = (Bk^{*n} : k^{*n})[k(\Omega_k) : k].$$

According to the previous section, such a situation occurs when  $n = p^f$ , with  $p$  odd and prime or  $p = 2$  and  $\zeta_4$  is in  $k$ , for instance. We call this situation *the regular case*.

2. We consider the case where  $n$  is a power of 2. Theorem 5 shows that this case is not always regular.

Finally, we consider the *general case* :  $n$  is supposed to be any composite integer. Following ([CF76]) and ([Sme90]), we also have included an optimization based on the computation of an independent set of multiplicative generators for the  $\beta_i$ 's which allows to skip factorization steps in some cases.

### 3.1 The regular case

We assume that the degree of the extension  $K/k$  is :

$$[K : k] = (Bk^{*n} : k^{*n})[k(\Omega_k) : k]. \quad (6)$$

We describe two algorithms for computing  $(Bk^{*n} : k^{*n})$  which simultaneously provides a set of generator for  $\Omega_k$ . The second one is more efficient, but its scope is limited to certain special cases.

#### 3.1.1 General method

We consider the group  $Bk^{*n}/k^{*n}$  as a group given by generators, namely the  $\beta_i$ 's, and relations. We start with the trivial relations  $\beta_i^n \equiv 1$  and search iteratively for new relations of the form :

$$\prod_{i=1}^s \beta_i^{e_i} = \gamma^n \equiv 1, \quad \gamma \in k, \quad (7)$$

where the  $e_i$ 's are integers satisfying  $0 \leq e_i < n$  and are not all equal to zero. Each time a relation is found, the new relation is added to the others and a minimal set of relations is computed. The problem of determining whether an element of  $k$  is a perfect  $n$ -th power is not addressed in the paper (see the introduction). The minimal set of relations is represented by a matrix  $M$  of exponents in Hermite normal form. More precisely,  $M = (m_{i,j})$  is an  $(s, s)$  matrix of nonnegative integers such that :

1.  $m_{i,j} = 0$  if  $i > j$ ,
2.  $m_{i,i} > 0$ ,
3.  $0 \leq m_{i,j} < m_{j,j}$  if  $i < j$ .

Each line of the matrix represents a relation :

$$\prod_{j=i}^s \beta_j^{m_{i,j}} = \gamma_i^n \equiv 1. \quad (8)$$

The matrix  $M$  is initialized to a diagonal matrix containing  $n$  on the diagonal (the initial trivial relations). When a new relation (7) is found, a  $(s+1, s)$  matrix  $M'$  is formed by adding the line  $(e_1, e_2, \dots, e_s)$  at the bottom of  $M$ . A new Hermite normal form is computed from  $M'$  using row reductions (see [Coh93] for instance) and the last row (containing only zeros) is deleted. If  $T = (t_{i,j})_{\{1 \leq i \leq s+1, 1 \leq j \leq s+1\}}$  is the  $(s+1, s+1)$  left unimodular transformation matrix corresponding to the Hermite reduction, then the new value  $\gamma'_i$  of  $\gamma_i$  is :

$$\gamma'_i = \gamma^{t_{i,s+1}} \prod_{j=1}^s \gamma_j^{t_{i,j}}. \quad (9)$$

The initial values are of course  $\gamma_i = \beta_i$ . After the set of possible exponent vectors has been exhausted, we put  $r_i = m_{i,i}$  and we define :

$$R = \prod_{i=1}^s r_i.$$

Then, we have :

**Proposition 10**

$$(Bk^{*n} : k^{*n}) = R.$$

**Proof :** From the triangular form of the matrix  $M$ , it is clear that every element of  $Bk^{*n}/k^{*n}$  is equivalent to an element of the form  $\beta_1^{e_1}, \dots, \beta_s^{e_s}$  with  $0 \leq e_i \leq r_i - 1$ . On the other hand, if any of these elements was a perfect  $n$ -th power, the relation  $\beta_1^{e_1}, \dots, \beta_s^{e_s} \equiv 1$  would have been found by the exhaustive search. Let  $i$  be the largest integer such that  $e_i$  is nonzero. Then, inspection of the row reduction algorithm shows that we should have  $r_i < e_i$ .  $\square$

For each line  $i$  :

$$\beta_i^{r_i} = \gamma_i^n \prod_{j=i+1}^s \beta_j^{-m_{i,j}} \quad (10)$$

Taking  $n$ -th roots in (10) yields :

$$\alpha_i^{r_i} = \zeta_n^{n_i} \gamma_i \prod_{j=i+1}^s \alpha_j^{-m_{i,j}} \quad (11)$$

for some integer  $n_i$ . Let  $\omega$  be an  $n$ -th root of unity such that :

$$\langle \omega \rangle = \langle \zeta_n^{n_1}, \dots, \zeta_n^{n_s} \rangle.$$

**Proposition 11**  $k(\Omega_k) = k(\omega)$ .

**Proof :** The inclusion  $k(\omega) \subset k(\Omega_k)$  is trivial. Let  $\zeta$  be an  $n$ -th root of unity in  $\Omega_k$ . Using the relations (11), we can write :

$$\zeta = \gamma \omega^j \prod_{i=1}^s \alpha_i^{e_i}$$

where  $\gamma \in k$ ,  $j$  is a well chosen integer and  $0 \leq e_i < r_i$ . Raising this equality to the  $n$ -th power yields :

$$1 = \gamma^n \prod_{i=1}^s \beta_i^{e_i}.$$

If  $e_{i_0}$ 's is different from zero, then  $(Bk^{*n} : k^{*n})$  must be smaller than  $R$  and we obtain a contradiction with proposition 10. Therefore, the  $e_i$ 's are all equal to zero and  $\zeta = \gamma \omega^j$ .  $\square$

Next, for  $1 \leq i \leq s$ , we define :

$$P_i(x) = x^{r_i} - \zeta_n^{n_i} \gamma_i \prod_{j=i+1}^s \alpha_j^{-m_{i,j}} \quad (12)$$

and

$$K_{s+1} = k(\Omega_k) \quad K_i = k(\Omega_k, \alpha_i, \dots, \alpha_s) \quad (13)$$

**Proposition 12** *The polynomial  $P_i(x)$  is the minimal polynomial of  $\alpha_i$  over  $K_{i+1}$ .*

**Proof :** By hypothesis (6), proposition 10 and proposition 11,

$$[K : k] = R[k(\Omega_k) : k] = R[k(\omega) : k].$$

Therefore, none of the  $P_i$ 's splits over  $K_{i+1}$ .  $\square$

It remains to compute  $[k(\Omega_k) : k]$ . It is easy to show that if

$$m = \frac{n}{\gcd(n_1, \dots, n_s)}$$

then we can choose  $\omega = \zeta_m$ . The degree  $v$  of the minimal polynomial of  $\zeta_m$  over  $k$  can be computed by mere factorization over  $k$  of the  $m$ -th cyclotomic polynomial.

**Proposition 13** *The set*

$$\{\zeta_m^{a_0} \alpha_1^{a_1}, \dots, \alpha_s^{a_s} \mid 0 \leq a_0 < v, 0 \leq a_1 < r_1, \dots, 0 \leq a_s < r_s\}$$

*form a basis for  $K$  over  $k$ .*

### Remarks

1. It is clear that we only have to search for new relations of the form (7) for  $e_i$  smaller than the current value of  $m_{i,i}$  since any relation with an  $e_i$  greater or equal to an  $m_{i,i}$  can be reduced using the relations (8).
2. If it has been determined that  $\beta$  is not an  $n$ -th power in  $k$ , then for any integer  $m$  prime to  $n$ ,  $\beta^m$  is not an  $n$ -th power. For, there exists integers  $a$  and  $b$  such that  $am + bn = 1$  and  $\beta^m = \gamma^n \implies \beta^{am} = \beta^{1-bn} = \gamma^n \implies \beta = (\gamma \beta^b)^n$ .

3. Let  $c_n(d)$  denote the cost of factoring a degree  $n$  polynomial over an algebraic extension of degree  $d$  of  $k$ . In the worst case, that is when  $[K : k] = n^s$ , the cost of the brute-force algorithm sketched in the introduction is dominated by the cost of the last step :  $c_n(n^{s-1})$ . In the same condition, taking into account the preceding remark and the computation of  $[k(\Omega_k) : k]$  the cost of our algorithm is  $(n^s/\phi(s)+1) c_n(1)$ . Consider the case of a finite algebraic number field  $k$ . It is reasonable to assume that  $c_n(d) = (nd)^m$  for a positive integer  $m$  (see [Lan85], [Len83] for plausible values of  $m$ ). Then  $c_n(n^{s-1}) = n^{m s}$  and  $n^s/\phi(s) c_n(1) = n^{s+m}/\phi(s)$ . Provided that  $s$  and  $m$  are greater than 1, the exponent  $s+m$  is smaller than  $m s$ . The larger are  $m$  and  $s$ , the greater is the gain that the algorithm achieves.
4. The problem of deciding which roots of unity actually satisfy (11) is a instance of the branch choice problem mentioned in the introduction and is not addressed in this paper.
5. Instead of Hermite normal forms, we could also use Smith normal forms. In that case, the matrix  $M$  is reduced to a diagonal form by applying left and right unimodular transformations. It means that the generators  $\beta_i$ 's are also modified so as to give new generators  $\beta'_i$  such that  $(\beta'_i)^{m_i} \in k^{*n}$ . Using Hermite normal forms yields a basis generated by nested radicals while Smith normal forms produce un-nested radicals. We leave the details to the reader.

Finally, we summarize the method :

**Algorithm Regular-case**( $k, n, B$ )

**Input** :

- $k$ , a field,
- $n$ , an integer,
- $B = \{\beta_1, \dots, \beta_s\}$  a set of  $s$  elements of  $k$ .

**Output** : A set of polynomials  $\{P_0, P_1, \dots, P_s\}$  such that  $P_0$  is a minimal polynomial for a primitive element of  $k(\Omega_k)/k$ , and for  $1 \leq i \leq s$ ,  $P_i$  is the minimal polynomial for  $\sqrt[n]{\beta_i}$  over  $k(\Omega_k, \sqrt[n]{\beta_{i+1}}, \dots, \sqrt[n]{\beta_s})$ .

**Begin**

Initialization.

$S := \{[e_1, \dots, e_s] \mid 0 \leq e_i < n\} - \{[0, \dots, 0]\}$ .

**For**  $i$  **from** 1 **to**  $s$  **do**  $\gamma_i := \beta_i$ .

$M := n * Id_s$ .

Computation of  $(Bk^{*n} : k^{*n})$ .

```

While  $S \langle \rangle \{ \}$  do
  Choose an exponent vector  $v = [e_1, \dots, e_s]$  in  $S$ .
  If  $\beta_1^{e_1} \dots \beta_s^{e_s} = \gamma^n$  for some  $\gamma$  in  $k$  then
     $M, T := \text{Row-reduce}(M, v)$ .
    Update the  $\gamma_i$ 's according to formula (9).
     $S := \text{Update}(S, M)$ .
  else
     $S := \text{Update}(S, v, n)$ .

Computation of the  $P_i$ 's.

Choose the  $n_i$ 's according to (11).
 $m := n/\text{gcd}(n_1, \dots, n_s)$ .
Compute the minimal polynomial  $P_0$  of  $\zeta_m$ .
Define the  $P_i$ 's according to (12).
Return  $\{P_0, P_1, \dots, P_s\}$ .
End.

```

**Algorithm Row-reduce( $M, v$ )**

**Input :**  $M$ , a square matrix of size  $s$  in Hermite normal form,  $v$  a row vector of size  $s$ .

**Output :** a square matrix of size  $s$  in Hermite normal form and the transformation matrix  $T$ .

**Begin**

$M' := \text{stack}(M, v)$ .

$M', T := \text{Hermite}(M')$ .

Delete the line of zeros at the bottom of  $M'$ .

Return  $M'$  and  $T$ .

**End.**

**Algorithm Update( $S, M$ )**

**Input :**  $S$ , a set of  $s$ -uples of nonnegative integers,  $M = (m_{i,j})$  a square matrix of size  $s$  with nonnegative integer entries.

**Output :**  $S$ , a set of  $s$ -uples of nonnegative integers, such that the  $i$ -th coefficient of each  $s$ -uple is smaller than  $m_{i,i}$ .

**Algorithm Update( $S, v, n$ )**

**Input :**  $S$ , a set of  $s$ -uples of nonnegative integers,  $v$ , an  $s$ -uple of nonnegative integers,  $n$ , a positive integer.

**Output :**  $S$ , a set of  $s$ -uples of nonnegative integers, such that there is no  $s$ -uple in  $S$  congruent to  $mv$  modulo  $n$  for any  $m$  co-prime with  $n$ .

**Algorithm** Hermite(P)Input :  $P$ , a matrix with integer entries.Output : The Hermite normal form  $Q$  of  $P$  and the transformation matrix  $T$  such that  $TP = Q$ .**3.1.2 Independent generators**

We shall show in this section, that  $[K : k]$  can sometimes be computed without any factorization of polynomials over  $k$ . This section was motivated by the techniques presented in [CF76]) and [Sme90] for the case  $k = \mathbb{Q}$ .

Let  $\{\delta_i\}_{1 \leq i \leq r}$  be a set of elements of  $k^*$  and denote by  $m_i$  the order of  $\delta_i$  modulo  $k^{*n}$ .

**Definition 1** *The  $\delta_i$ 's are multiplicatively independent modulo  $k^{*n}$  if, for any  $r$ -uple of integers  $(e_1, \dots, e_r)$ , we have :*

$$\prod_{j=1}^r \delta_j^{e_j} \equiv 1 \pmod{k^{*n}} \iff e_j \equiv 0 \pmod{m_j} \quad 1 \leq j \leq r.$$

We assume in this section that there exists a set  $\{\delta_i\}_{1 \leq i \leq r}$  of multiplicatively independent elements of  $k^*$  such that there exists nonnegative integers  $\{p_{i,j}\}_{1 \leq i \leq s, 1 \leq j \leq r}$  satisfying :

$$\beta_i = \prod_{j=1}^r \delta_j^{p_{i,j}}. \quad (14)$$

**Definition 2** *We shall say that the  $\delta_i$ 's form a set of independent generators for the  $\beta_i$ 's.*

**Example :** If  $k = \mathbb{Q}$ , a set of independent generators for the  $\beta_i$ 's can be computed by factorization of the  $\beta_i$ 's or by gcd computations only (see [CF76]). This technique can also be applied when  $k$  is an Euclidean quadratic field with a finite group of units.  $\square$

We now explain how to construct relations of the form (7) from (14). Let  $P$  be the  $(s, r)$  matrix  $P = (p_{i,j})$ . From (7), we get :

$$\prod_{j=1}^r \delta_j^{\sum_{i=1}^s p_{i,j} e_i} = \gamma^n. \quad (15)$$

The independence of the  $\delta_j$ 's gives :

$$\sum_{i=1}^s p_{i,j} e_i \equiv 0 \pmod{m_j} \quad 1 \leq j \leq r. \quad (16)$$

Each of the relation set (16) is a vanishing linear combination of the rows of the  $(r + s, r)$  matrix  $P'$  built by stacking  $P$  and the  $(r, r)$  diagonal matrix  $\text{diag}(m_1, \dots, m_r)$ . Reciprocally, a vanishing linear combination of the rows of  $P'$  yields a relation of type (7). Let  $Q$  be the Hermite normal form of  $P'$  and  $S$  be the unimodular  $(s + r, s + r)$  matrix such that

$$S P' = Q.$$

The matrix  $Q$  is made of an  $(r, r)$  upper triangular matrix with nonzero elements on the diagonal and of a  $(s, r)$  zero block. The  $r$  first rows of  $Q$  are obviously independent over  $Z$ . Hence, the  $s$  last rows of  $S$  generate all the relations of type (16) over  $Z$ .

More precisely, if  $S = (s_{i,j})_{1 \leq i \leq s+r, 1 \leq j \leq s+r}$ , then for  $r + 1 \leq i \leq s + r$ , each line of  $S$  corresponds to the relation :

$$\prod_{j=1}^s \beta_j^{s_{i,j}} = \prod_{j=1}^r \delta_j^{-m_j s_{i,j+s}} = \gamma_i^n \equiv 1 \pmod{k^{*n}} \quad (17)$$

for some  $\gamma_i$  in  $k^*$ . Therefore, we form the square matrix  $M = (m_{i,j})_{1 \leq i \leq s, 1 \leq j \leq s}$  defined by  $m_{i,j} = s_{i,j}$  such that each line of  $M$  corresponds to a relation of type (10) and we triangularize the set of generating relations represented by  $M$  using a Hermite normal form or a Smith normal form, just as in the general case. It is now clear that propositions 10 to 12 hold for the final matrix.

**Algorithm Indep-Gen** $(k, n, B, P, D, m_1, \dots, m_r, E)$

**Input :**

- $k$ , a field,
- $n$ , an integer,
- $B = \{\beta_1, \dots, \beta_s\}$ , a set of  $s$  elements of  $k$ ,
- $P = (p_{i,j})$ , an  $(s, r)$  matrix with integer entries,
- $D = \{\delta_1, \dots, \delta_r\}$ , a set of independent generators for the  $\beta_i$ 's such that  $\beta_i = \prod_{j=1}^r \delta_j^{p_{i,j}}$ ,
- $m_1, \dots, m_r$ , integers such that  $m_i$  is the order of  $\delta_i$  modulo  $k^{*n}$ ,
- $E = \{\varepsilon_1, \dots, \varepsilon_r\}$ , a set of elements of  $k^*$  such that  $\delta_i^{m_i} = \varepsilon_i^n$ .

**Output :** A set of polynomials  $\{P_0, P_1, \dots, P_s\}$  such that  $P_0$  is a minimal polynomial for a primitive element of  $k(\Omega_k)/k$ , and for  $1 \leq i \leq s$ ,  $P_i$  is the minimal polynomial for  $\sqrt[n]{\beta_i}$  over  $k(\Omega_k, \sqrt[n]{\beta_{i+1}}, \dots, \sqrt[n]{\beta_s})$ .

**Begin**

Computation of the relations.

$P' := \text{stack}(P, \text{diag}(m_1, \dots, m_r))$ .

$Q, S := \text{Hermite}(P')$ .

For  $i$  from 1 to  $s$  do

    For  $j$  from 1 to  $s$  do

$m_{i,j} := s_{r+i,j}$ .

$\gamma_i := 1$ .

    For  $j$  from 1 to  $r$  do

$\gamma_i := \gamma_i * \varepsilon_j^{-s_{i,j}+s}$ .

Reduction of the relations.

$M, T := \text{Hermite}(M)$ .

For  $i$  from 1 to  $s$  do

$\gamma_i := \prod_{j=1}^s \gamma_j^{t_{i,j}}$ .

Computation of the  $P_i$ 's.

Proceed as in the general case.

Return  $\{P_0, P_1, \dots, P_s\}$ .

End.

### 3.2 Powers of 2

We assume in this section that  $n > 2$  and  $\zeta_4$  is not in  $k$ , otherwise we are in a regular case. According to theorem 5, the degree of the extension  $K/k$  is  $(Bk^{*n} : k^{*n})[k(\Omega_k) : k]$  or  $1/2(Bk^{*n} : k^{*n})[k(\Omega_k) : k]$ . We recall that :

- $a = -1$  if  $t > f$ ,
- $a = (\xi_t + 2)^{2^{f-1}} = \xi_{t+1}^{2^f}$  if  $t < f$ ,
- $a = -(\xi_t + 2)^{2^{f-1}} = -\xi_{t+1}^{2^f}$  if  $t = f$ .

We assume in the following discussion that  $a$  has order 2 modulo  $k^{*n}$ . If  $a$  has order one, we know from theorem 5 that the situation is regular. We still have to search for relations of the form (7), but we are also looking for relations of the form :

$$\prod_{i=1}^s \beta_i^{f_i} = a \delta^n \equiv 1, \quad \delta \in k, \quad (18)$$

where the  $f_i$ 's are integers, not all equal to zero. We call such a relation an *irregular relation*. As in the regular case, the search for irregular relation reduces to determine whether an element of  $k$  is a perfect  $n$ -th power in  $k$ .

The following properties are immediate :

1.  $a$  is in  $Bk^{*n}$  if and only if there exists an irregular relation (18).
2. Once an irregular relation is found, all irregular relations can be determined by multiplying it by regular relations of type (7).
3. We cannot find a regular relation and an irregular relation for the same exponent vector since  $a$  is supposed to have order 2.
4. If  $v$  is an exponent vector which doesn't provide an irregular relation, then, for any odd integer  $m$ ,  $m v$  cannot yield an irregular relation.

Therefore, we just have to search for one irregular relation : Upon discovering an irregular relation we store it and proceed with the computation of  $(Bk^{*n} : k^{*n})$ . If no such relation has been found, then  $a$  is not in  $Bk^{*n}$  and we are reduced to the regular case. If an irregular relation (18) has been discovered, then we reduce it modulo the relation given by  $M$  so that  $f_i < r_i$  for  $1 \leq i \leq s$ . Let  $v$  denote the largest integer such that  $f_v \neq 0$ . Such an integer exists since  $a$  is supposed to have order 2. Moreover, we must have  $r_v = 2 f_v$ , so that :

$$\beta_v^{r_v/2} = a \delta^n \prod_{j=v+1}^s \beta_j^{-f_j}. \quad (19)$$

We define  $R$ ,  $\omega$ ,  $P_i$  and  $K_i$  ( $1 \leq i \leq s$ ) as before (see (12) and (13)). It is clear that :

**Proposition 14**

$$(Bk^{*n} : \langle k^{*n}, a k^{*n} \rangle) = \frac{1}{2} R.$$

Moreover, since  $\zeta_4 \notin k$ , a small modification of the argument in proposition 11 yields :

**Proposition 15**  $\Omega_k = \langle \omega, -1 \rangle$ .

We consider three different cases :

**Case 1 :**  $t > f$ ,  $a = -1$ .

Extracting  $n$ -roots in (19) gives :

$$\alpha_v^{r_v/2} = \zeta_{2n}^{n_v} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}. \quad (20)$$

for a well chosen integer  $n_v$ . Therefore, we define :

$$Q_v(x) = x^{r_v/2} - \zeta_{2n}^{n_v} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}.$$

**Proposition 16** For  $i \neq v$ ,  $P_i(x)$  is the minimal polynomial of  $\alpha_i$  over  $K_{i+1}$ . Moreover,  $Q_v$  is the minimal polynomial of  $\alpha_v$  over  $K_{v+1}$ .

**Proof :** Proposition 7 says that  $\zeta_{2n} \in k(\Omega_k)$ . From the relations (11) and (20) we get :

$$[K : k] \leq \frac{1}{2} R [k(\zeta_{2n}) : k] \leq \frac{1}{2} R [k(\Omega_k) : k].$$

Finally, theorem 5 and proposition 14 imply that the  $P_i$ 's ( $i \neq v$ ) and  $Q_v$  are irreducible.  $\square$

**Case 2 :**  $t = f > 2$ ,  $a = -\xi_{t+1}^n$ .

Proceeding as in the previous case, we obtain this time :

$$\alpha_v^{r_v/2} = \zeta_{2n}^{n_v} \xi_{t+1} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}. \quad (21)$$

for a well chosen *odd* integer  $n_v$ . We define :

$$Q_v(x) = x^{r_v/2} - \zeta_{2n}^{n_v} \xi_{t+1} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}.$$

**Proposition 17** For  $i \neq v$ ,  $P_i(x)$  is the minimal polynomial of  $\alpha_i$  over  $K_{i+1}$ . Moreover, the polynomial  $Q_v$  is the minimal polynomial of  $\alpha_v$  over  $K_{v+1}$ .

**Proof :** By proposition 8,  $k(\Omega_k) = k(\zeta_{2^t})$ . Since  $n_v$  is odd,  $\zeta_{2^n}^{n_v} \xi_{t+1} = \zeta_{2^t}^{(n_v-1)/2} (1 + \zeta_{2^t})$  is in  $k(\Omega_k)$ . The coefficients of  $Q_v$  are therefore in  $K_{v+1}$ . The proposition now follows from theorem 5 and the relations (11) and (21).  $\square$

**Case 3 :**  $t < f$ ,  $a = \zeta_{t+1}^n$ .

Taking again  $n$ -th root in (19), we get :

$$\alpha_v^{r_v/2} = \zeta_n^{n_v} \xi_{t+1} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}. \quad (22)$$

for a well chosen integer  $n_v$ . So we put :

$$Q_v(x) = x^{r_v/2} - \zeta_n^{n_v} \xi_{t+1} \delta \prod_{j=v+1}^s \alpha_j^{-f_j}.$$

Let  $s$  be the integer such that :

$$\zeta_n^{n_v} = \zeta_{2^s}^j$$

for an odd  $j$  and set  $m = \max\{s, t + 1\}$ .

In the following proposition, we assume that  $\zeta_4$  is in  $\Omega_k$ , otherwise we are in a regular case since  $1 + \zeta_4$  cannot belong to  $Ak^*$ . The condition  $\zeta_4 \in \Omega_k$  can be quickly checked in virtue of proposition 15.

**Proposition 18** *Assume that  $\zeta_4 \in \Omega_k$ . For  $i \neq v$ ,  $P_i(x)$  is the minimal polynomial of  $\alpha_i$  over  $K_{i+1}$ . If  $s = t + 1$  or  $\zeta_{2^m} \in \Omega_k$ , then the minimal polynomial of  $\alpha_v$  over  $K_{v+1}$  is  $Q_v$ . Otherwise, the minimal polynomial of  $\alpha_v$  over  $K_{v+1}$  is  $P_v$ .*

**Proof :** If  $s = t + 1$ , then  $\zeta_{2^s}^j \xi_{t+1} = \zeta_{2^t}^i (1 + \zeta_{2^t})$  is in  $Ak^*$ . Squaring this expression, one sees that  $\zeta_{2^{t-1}}^i \zeta_{2^t} (2 + \xi_t)$  is in  $Ak^*$ . Therefore,  $\zeta_{2^t}$  belongs to  $\Omega_k$  and so does  $(1 + \zeta_{2^t})$ . Theorem 5 completes the proof. Suppose that  $s \neq t + 1$ . Writing  $\xi_{t+1} = \zeta_{2^{t+1}} (1 + \zeta_{2^t})$ , we see that  $1 + \zeta_{2^t}$  is in  $Ak^*$  if and only if  $\zeta_{2^m}$  is in  $Ak^*$ . If  $\zeta_{2^m} \in \Omega_k$ , then the coefficients of  $Q_v$  are in  $K_{v+1}$  and theorem 5 yields the result. If  $\zeta_{2^m}$  is not in  $Ak^*$ , theorem 5 shows that all the  $P_i$ 's are irreducible over their coefficient field.  $\square$

The following algorithm summarizes the method :

**Algorithm Power-of-2( $k, f, B$ )**

**Input :**

- $k$ , a field,

- $f$ , a positive integer,
- $B = \{\beta_1, \dots, \beta_s\}$  a set of  $s$  elements of  $k$ .

**Output :** A set of polynomials  $\{P_0, P_1, \dots, P_s\}$  such that  $P_0$  is a minimal polynomial for a primitive element of  $k(\Omega_k)/k$ , and for  $1 \leq j \leq s$ ,  $P_i$  is the minimal polynomial for  $\sqrt[2^f]{\beta_i}$  over  $k(\Omega_k, \sqrt[2^f]{\beta_{i+1}}, \dots, \sqrt[2^f]{\beta_s})$ .

**Begin**

Initialization and special cases.

If  $f = 1$  or  $\zeta_4 \in k$  then Return Regular-case( $k, 2, B$ ).

$n := 2^f$ .

$t := \text{Max-t}(k)$ .

If  $t < f$  then  $a := \xi_{t+1}^n$

    If  $a \in k^n$  then Return Regular-case( $k, n, B$ ).

elif  $t = f$  then  $a := -\xi_{t+1}^n$

else  $a := -1$ .

$S := \{[e_1, \dots, e_s] \mid 0 \leq e_i < n\} - \{[0, \dots, 0]\}$ .

For  $i$  from 1 to  $s$  do  $\gamma_i := \beta_i$ .

$M := n * Id_s$ .

Is- $a$ -in- $Bk^{*n}$ ? := false.

Computation of the kernel of  $\Psi$ .

While  $S \ll \{\}$  do

    Choose an exponent vector  $v = [e_1, \dots, e_s]$  in  $S$ .

    If  $\beta_1^{e_1} \dots \beta_s^{e_s} = \gamma^n$  for some  $\gamma$  in  $k$  then

$M, T := \text{Row-reduce}(M, v)$ .

        Update the  $\gamma_i$ 's according to formula (9).

$S := \text{Update}(S, M)$ .

    elif not Is- $a$ -in- $Bk^{*n}$ ? then

        If  $\beta_1^{e_1} \dots \beta_s^{e_s} = a \gamma^n$  for some  $\gamma$  in  $k$  then

            Is- $a$ -in- $Bk^{*n}$ ? := true.

$v_a := v$ .

$\gamma_a := \gamma$ .

$S := \text{Update}(S, v, n)$ .

    else  $S := \text{Update}(S, v, n)$ .

Computation of  $k(\Omega_k)$

Determine  $\omega$  from the  $n_i$ 's (see propositions 12 and 15).

Compute the minimal polynomial  $P_0$  of  $\omega$  over  $k$ .

Computation of the  $P_i$ 's.

Define the  $P_i$ 's ( $i > 0$ ) according to (13).

If not Is- $a$ -in- $Bk^{*n}$ ? then

    Return  $\{P_0, P_1, \dots, P_s\}$ .

```

elif  $t > f$  then
    Define  $Q_v$  as in proposition 16.
    Return  $\{P_0, P_1, \dots, P_{v-1}, Q_v, P_{v+1}, P_s\}$ .
elif  $t = f$  then
    Define  $Q_v$  as in proposition 17.
    Return  $\{P_0, P_1, \dots, P_{v-1}, Q_v, P_{v+1}, P_s\}$ .
else
    Define  $s$  and  $m$  as in proposition 18.
    if  $s = t + 1$  or  $\zeta_m \in \langle \omega, -1 \rangle$  then
        Define  $Q_v$  as in proposition 18.
        Return  $\{P_0, P_1, \dots, P_{v-1}, Q_v, P_{v+1}, P_s\}$ .
    else
        Return  $\{P_0, P_1, \dots, P_s\}$ .
End.

```

**Algorithm Max- $\tau(k)$**

Input :  $k$ , a field.

Output : The largest integer  $t$  such that  $\xi_t = \zeta_{2^t} + \zeta_{2^t}^{-1}$  is in  $k$ .

Begin

$t := 2$ .

$\xi := 0$ .

While  $\xi + 2$  is in  $k^2$  do

$\xi := \sqrt{\xi + 2}$ .

$t := t + 1$ .

Return  $t$ .

End.

### 3.3 General case

We assume in this section that  $n$  is not a power of a prime and that the factorization of  $n$  is :

$$n = \prod_{i=1}^m p_i^{e_i}$$

where the  $e_i$ 's are positive integers. For  $1 \leq i \leq m$ , we define :

$$n_i = \frac{n}{p_i^{e_i}}$$

and

$$A_i = \{\alpha_1^{n_i}, \dots, \alpha_s^{n_i}\}.$$

**Proposition 19**  $k(A) = k(A_1, \dots, A_m)$ .

**Proof :** It is obvious that  $k(A_1, \dots, A_m) \subset k(A)$ . Let  $a_1, \dots, a_m$  be integers such that

$$a_1 n_1 + \dots + a_m n_m = 1.$$

Then we have :

$$(\alpha_j^{n_1})^{a_1} \dots (\alpha_j^{n_m})^{a_m} = \alpha_j.$$

Hence,  $k(A) \subset k(A_1, \dots, A_m)$  and the proof is complete.  $\square$

Let us introduce some notations :

- $\Omega_i$  is the group of  $p_i^{e_i}$ -th root of unity contained in  $A_i k^*$ .
- $k_0 = k$ ,  $k_i = k_{i-1}(A_i)$  for  $1 \leq i \leq m$ ,
- $l_0 = k$ ,  $l_i = l_{i-1}(\Omega_i)$  for  $1 \leq i \leq m$ ,
- $h_i = l_i \cap k(A_i)$  for  $1 \leq i \leq m$ .

We shall build recursively the fields  $k_i$  and  $l_i$ , and attempt to keep as low as possible the degree of the field wherein the computations are performed.

We assume in the sequel that  $p_1 > p_2 > \dots > p_m$ .

**Proposition 20** For  $1 \leq i \leq m$ , we have :

1. The prime factors of  $[k_{i-1} : l_{i-1}]$  are in the set  $\{p_1, \dots, p_{i-1}\}$ ,
2.  $[k_{i-1}(\Omega_i) : l_i] = [k_{i-1} : l_{i-1}]$ ,
3.  $[k_i : k_{i-1}(\Omega_i)] = [k(A_i) : h_i]$ .

**Proof :** We begin by proving that 1 implies 2 and 3. Since  $[l_i, l_{i-1}]$  divides  $\phi(p_i^{e_i})$  and  $p_1 > p_2 > \dots > p_{i-1} > p_i$ , no prime factor of  $[k_{i-1} : l_{i-1}]$  can divide  $[l_i, l_{i-1}]$ , so that  $([k_{i-1} : l_{i-1}], [l_i, l_{i-1}]) = 1$ . Hence, equality 2 holds. From theorem 4 and 5,  $[k(A_i) : k(\Omega_i)]$  is a power of  $p_i$  and  $[k(A_i) : h_i]$  must also be a power of  $p_i$ . Since  $l_i/k(\Omega_i)$  is Galois, theorem 3 yields  $[l_i(A_i) : l_i] = [k(A_i) : h_i]$ . But then  $[l_i(A_i) : l_i]$  and  $[k_{i-1}(\Omega_i) : l_i]$  are relatively prime and 3 is true. Finally, we prove 1 by induction on  $i$ . If  $i = 1$ ,  $k_{i-1} = l_{i-1} = k$  and the assertion is trivial. If  $2 \leq i \leq m$ , then assume that assertion 1 is true. We have just shown that :

$$[k_i : l_i] = [k_i : k_{i-1}(\Omega_i)][k_{i-1}(\Omega_i) : l_i] = [k(A_i) : h_i][k_{i-1} : l_{i-1}].$$

Since  $[k(A_i) : l_i \cap k(A_i)]$  is a power of  $p_i$ , the prime factors of  $[k_i : l_i]$  must be in  $\{p_1, \dots, p_{i-1}, p_i\}$ .  $\square$

In order to compute  $k_i/k$ , this proposition shows that we only have to compute the degree of the extensions in dotted lines in the figure 1 below (the letters  $a, b, c$  and  $d$  point out extensions of the same degree). It is clear that this technique is better than the brute-force algorithm and that it totally avoids the introduction of spurious roots of unity.

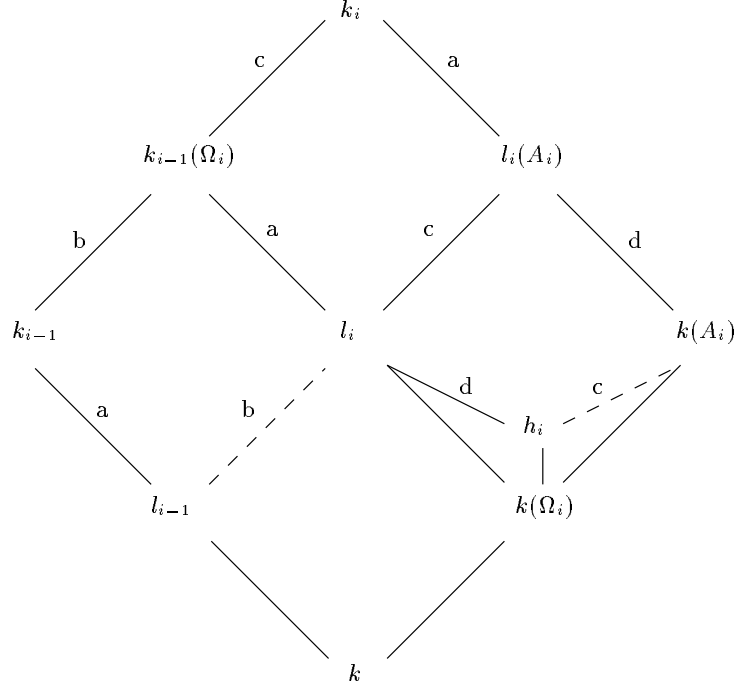


Figure 1

In the case  $k = \mathbb{Q}$ , one can prove a useful proposition :

**Proposition 21** *If  $k = \mathbb{Q}$  and  $(p_1 p_2 \dots p_{i-1}, \beta_1 \dots \beta_s) = 1$  then  $h_i = k(\Omega_i)$ .*

Proof : We have  $h_i = (k(A_i) \cap l_{i-1}) \cup k(\Omega_i)$ . The only primes that ramify in  $l_{i-1}$  are the  $p_j$ 's for  $1 \leq j \leq i-1$  (see [Nar90]). On the other hand, a prime which ramifies in  $k(A_i)$  must divide one of the  $\beta_j$ 's or  $p_i$  by ([Nar90][Prop. 4.13], [Nar90][Prop. 4.12]), and the fact that  $\text{disc}(x^n - a) = (-1)^{n-1} n^n a^{n-1}$ . Hence, if  $(p_1 p_2 \dots p_{i-1}, \beta_1 \dots \beta_s) = 1$ , there is no prime number which ramifies both in  $k(A_i)$  and  $l_{i-1}$ . Since the only unramified extension of  $\mathbb{Q}$  is  $\mathbb{Q}$  ([Nar90][p. 167]), we conclude that  $(k(A_i) \cap l_{i-1}) = \mathbb{Q}$  and we are done.  $\square$

Note that if  $\zeta_j$  is not in  $l_{i-1}$  for some  $j$  ( $1 \leq j \leq i-1$ ), then we can actually skip  $p_j$  in the test.

Prior to presenting our algorithm, we introduce a definition :

**Definition 3** *We shall say that a list of polynomials  $[P_1, \dots, P_r]$  generates a field  $M$  over a field  $L$  if for  $1 \leq i \leq r$ ,  $P_i$  is the minimal polynomial over  $L(\gamma_1, \dots, \gamma_{i-1})$  of an element  $\gamma_i$  of  $M$  and  $L(\gamma_1, \dots, \gamma_r) = M$ .*

**Algorithm General-case( $k, n, B$ )**

Input :

- $k$ , a field,
- $n$ , an integer,
- $B = \{\beta_1, \dots, \beta_s\}$  a set of  $s$  elements of  $k$ .

Output : A list of polynomials  $[P_0, P_1, \dots, P_v]$  such that :

- $P_0$  is the minimal polynomial of a primitive element  $\gamma_0$  of  $l_m/k$ ,
- $P_1, \dots, P_v$  generates  $K$  over  $l_m$ .

Begin

Initialization and special cases.

For  $i$  from 1 to  $s$  do  $\alpha_i := \sqrt[n]{\beta_i}$ .

If the  $\alpha_i$ 's are real numbers or  $\zeta_n \in k$  then

Return Regular-case( $k, n, B$ ).

Factor  $n$  into a product of primes  $n = \prod_{i=1}^m p_i^{e_i}$ .

Sort the  $p_i$ 's by decreasing order.

If  $m = 1$  then Return p-th-power( $k, p_1^{e_1}, B$ ).

Recursion.

$[R_0, \dots, R_r] := \text{General-case}(k, n/p_m^{e_m}, B)$ .

$[S_0, \dots, S_s] := \text{p-th-power}(k, p_m^{e_m}, B)$ .

Computation of  $l_m/k$ .  
 $P_0 := \text{Cyclo}(k, R_0, S_0)$ .  
 Computation of  $l_m(A_m)/l_m$ .  
 If we can prove that  $h_m = k(\Omega_m)$  (see proposition 21) then  
     Return  $[P_0, R_1, \dots, R_r, S_1, \dots, S_r]$   
 else  
      $[T_0, T_1, \dots, T_t] := \text{p-th-power}(l_m, p_m^e, B)$ .  
     Return  $[P_0, R_1, \dots, R_r, T_0, T_1, \dots, T_t]$ .  
 End.

**Algorithm Cyclo**( $k, R_0, S_0$ )

Input :

- $k$ , a field,
- $R_0$ , a cyclotomic polynomial over  $k$ ,
- $S_0$ , a cyclotomic polynomial over  $k$ ,

Output : A cyclotomic polynomial  $P_0$  over  $k$  such that the splitting field of  $P_0$  is the splitting field of  $R_0$  and  $S_0$ .

**Algorithm p-th-power**( $k, p^e, B$ )

Input :

- $k$ , a field,
- $p^e$ , a perfect power of a prime  $p$  ( $e > 0$ ),
- $B = \{\beta_1, \dots, \beta_s\}$  a set of  $s$  elements of  $k$ .

Output : A set of polynomials  $\{P_0, P_1, \dots, P_s\}$  such that  $P_0$  is a minimal polynomial for a primitive element of  $k(\Omega_k)/k$ , and for  $1 \leq j \leq s$ ,  $P_j$  is the minimal polynomial for  $\sqrt[p^e]{\beta_j}$  over  $k(\Omega_k, \sqrt[p^e]{\beta_{j+1}}, \dots, \sqrt[p^e]{\beta_s})$ .

Begin

If  $p$  is odd then  
     Return Regular-case( $k, p^e, B$ )  
 else  
     Return Power-of-2( $k, p^e, B$ )

End.

**Remarks :**

1. In order to simplify the algorithm, we compute the extension  $l_m(A_m)/l_m$  instead of  $k(A_m)/h_m$ . It is the only step which requires factorization of polynomials over an extension of  $k$  (namely, over  $l_m$ ).
2. The following example shows that we may have  $h_m \neq k(\Omega_m)$ : Assume that  $A = \{\sqrt[6]{-1}, \sqrt[6]{-3}\}$ . Then  $A_1 = \{\sqrt[3]{-1}, \sqrt[3]{-3}\}$ ,  $A_2 = \{\sqrt{-1}, \sqrt{-3}\}$ ,  $l_1 = Q(\zeta_3)$ ,  $l_2 = Q(\zeta_3, \zeta_4)$  and  $Q(A_2) = l_2$  so that the intersection  $h_2$  is larger than  $Q(\Omega_2) = Q(\zeta_4)$ . A more general obstruction is the famous theorem of Kronecker-Weber (see [Nar90]): The field  $Q(A_m)$  is included in a cyclotomic extension  $M$  of  $Q$  and if  $l_m$  is large enough to contain  $M$ , then again,  $h_m$  will be equal to  $k(A_m)$ .
3. If we can prove that  $h_m = k(\Omega_m)$ , using degree consideration for instance, or proposition 21, then we have all the information to build  $k_m$  and we can save computation. Otherwise, we proceed with the general method.
4. Although we cannot avoid adding roots of unity to the ground field, the roots that are required are elements of  $k(A)$  and are included in  $k(\zeta_n)$ . There is no introduction of spurious roots of unity.

## 4 Conclusion and acknowledgments

We have described a new algorithm for constructing a basis for

$$K = k(\sqrt[n]{\beta_1}, \dots, \sqrt[n]{\beta_s})$$

over  $k$ . Unlike previously published algorithms, our method avoids the introduction of spurious roots of unity and relies on factorization over  $k$  extended by roots of unity which belong to  $K$ . The algorithm is based on theoretical results extending a classical result of Kummer and a theorem of M. Kneser. The efficiency and correctness of the algorithm depends heavily on the ability to solve what we called the *branch choice problem* and the  *$n$ -th power problem* in the introduction. We have shown that algebraic factorization can be avoided to some extent, provided we can determine *sets of independent generators* for the  $\beta_i$ 's. Determining a larger class of radicals for which this construction is possible would extend the practical range of the algorithm. Finally, obtaining results similar to theorems 4 and 5 when  $n$  is composite would provide an alternative approach for this case.

We would like to thank Michael Monagan for stimulating discussions on this subject. We are also indebted to the Symbolic Computation Group of the University of Waterloo (Ontario) for partially supporting this work. Dominique Duval carefully read a first draft of this paper and several of her comments have been taken into account. Thank you for this useful help.

## References

- [AN95] Toma Albu and Florin Nicolae. Kneser Field Extension with Cogalois Correspondence. *Journal of Number Theory*, 52:299–318, 1995.
- [BFHT85] Allan Borodin, Ronald Fagin, John E. Hopcroft, and Martin Tompa. Decreasing the Nesting Depth of Expressions Involving Square Roots. *JSC*, 1:189–210, 1985.
- [CF76] B.F. Caviness and R. Fateman. Simplification of Radical Expressions. In *Proceedings SYMSAC '76*. ACM, 1976.
- [Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.
- [GV81] David Gay and Yslas Vélez. The Torsion Group of a Radical Extension. *Pacific Journal of Mathematics*, 92.2:317–327, 1981.
- [Has80] H. Hasse. *Number Theory*. Springer-Verlag, 1980.
- [Kne75] Michael Kneser. Lineare Abhängigkeit von Wurzeln. *Acta Arithmetica*, 26:307–308, 1975.
- [Lan65] S. Lang. *Algebra*. Addison-Wesley, 1965.
- [Lan85] Susan Landau. Factoring Polynomials over Algebraic Number Fields. *SIAM J. on Computing*, 14:184–195, 1985.
- [Lan92] Susan Landau. Simplification of Nested Radicals. *SIAM J. on Computing*, 21(1):85–110, 1992.
- [Len82] A. K. Lenstra. Lattices and Factorization of Polynomials over Algebraic Number Fields. In *Proceedings Eurocam '82*, volume 144 of *LNCS*. Springer-Verlag, 1982.
- [Len83] A. K. Lenstra. Factoring Polynomials over Algebraic Number Fields. In *Proceedings Eurocal '83*, volume 162 of *LNCS*. Springer-Verlag, 1983.
- [Nar90] Wladyslaw Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, second edition, 1990.
- [Sch75] Andrzej Schinzel. On Linear Dependence of Roots. *Acta Arithmetica*, 28:161–175, 1975.
- [Sch77] Andrzej Schinzel. Abelian Binomials, Power Residues and Exponential Congruences. *Acta Arithmetica*, 32:245–274, 1977.
- [Sch82] Andrzej Schinzel. *Selected Topics on Polynomials*. University of Michigan Press, 1982.

- [Sme90] Trevor J. Smedley. Detecting Algebraic Dependencies Between Unnested Radicals. In *Proceedings ISSAC '90*. ACM Press, 1990.
- [Tra76] Barry M. Trager. Algebraic Factoring and Rational Function Integration. In *Proceedings SYMSAC '76*, pages 219–226. ACM, 1976.
- [Zip85] Richard Zippel. Simplification of Expressions Involving Radicals. *JSC*, 1:189–210, 1985.