J. Symbolic Computation (1999) **11**, 1–000

Finding normal integral bases of cyclic number fields of prime degree

VINCENZO ACCIARO AND CLAUS FIEKER

Dipartimento di Informatica, Universita' degli Studi di Bari, via E. Orabona 4, Bari 70125, Italy
Technische Universität Berlin, Fachbereich 3, Sekr. MA 8-1, Straße des 17. Juni 136, 10623 Berlin, Germany

(Received 18 October 1999)

Let L be a cyclic number field of prime degree p. In this paper we study how to compute efficiently a normal integral basis for L, if there is at least one, assuming that an integral basis Γ for L is known. We reduce our problem to the problem of finding the generator of a principal ideal in the p-th cyclotomic field.

1. Introduction

Let us assume that $L = \mathbb{Q}[\alpha]$ is a cyclic number field of prime degree p over $\mathbb{Q}$, given by the minimal polynomial $m_\alpha(x)$ of α over $\mathbb{Q}$, and without loss of generality let us assume that $\alpha \in \mathcal{O}$, the ring of algebraic integers of L.

Let us assume as well that the conjugates of α give a basis for L as a vector space over $\mathbb{Q}$. The problem of finding such an element α is discussed for example in (Schlickewei and Stepanov, 1993)

Let us assume that an integral basis $\alpha_1, \ldots, \alpha_p$ for $\mathcal{O}$ is known. We recall that such an integral basis can be computed using the algorithms described in (Cohen, 1995; Pohst and Zassenhaus, 1989).

Let $G = \langle\sigma\rangle$ be the Galois group of L over $\mathbb{Q}$. If one assumes the Extended Riemann Hypothesis, then it is possible to compute σ in time polynomial in the size of $m_\alpha(x)$, using the algorithm described in (Acciaro and Klüners, 1999).

We say that an element $\theta \in L$ gives a normal integral basis if the ring $\mathcal{O}$ of integers of L is equal to $\sum_{i=1}^{p} \mathbb{Z} \cdot \sigma^i(\theta)$. In this paper we study how to find efficiently such an element θ, if there is at least one.

Assuming the knowledge of the discriminant of L, there is a well known criterion for the existence of normal integral bases for cyclic fields of prime degree: L admits a normal integral basis iff $\sqrt[p-1]{d_L} \in \mathbb{Z}$ is squarefree, i.e. the conductor of L is squarefree (Narkiewicz, 1989, p. 175).

From a theoretical point of view, the existence of an normal integral basis is quite explicit: Let f be the conductor of L. Since $\mathbb{Z}[\zeta_f]$ is integrally closed it is easy to see that ζ_f generates an integral normal basis. Now $\mathrm{Tr}_{\mathbb{Q}(\zeta_f)/L}(\zeta_f)$ generates an normal integral basis for L (Narkiewicz, 1989, p. 174).

From a practical point of view, this is quite unsatisfacory since we need to work in

0747–7171/90/000000 + 00 \$03.00/0

$\mathbb{Q}(\zeta_f)$ of degree $\phi(f)$ which usually is large in comparison to $[L : \mathbb{Q}]$. Therefore the computation of the relative trace will be quite difficult.

The algorithm presented here has the advantage of working only in L and $\mathbb{Q}(\zeta_p)$ avoiding the above mentioned problems. It turns out, that the running time of the algorithm is essentially independend of the conductor. It has been implemented using the number theory package KASH (Daberkow *et al.*, 1997), developed in Berlin by Prof. M. Pohst and his collaborators.

1.1. Modules over Group Rings

Let $\mathbb{Z}[G]$ denote the group ring of G over $\mathbb{Z}$. Observe first that $\mathbb{Z}[G]$ is commutative, and that

$$\mathbb{Z}[G] \cong \mathbb{Z} \oplus \mathbb{Z}\sigma \oplus \cdots \oplus \mathbb{Z}\sigma^{p-1} \cong \mathbb{Z}[x]/(x^p - 1) \tag{1.1}$$

(this follows from the fact, that $\delta : \mathbb{Z}[x] \to \mathbb{Z}[G] : x \mapsto \sigma$ is surjective with kernel generated by $x^p - 1$)

The representation of elements of $\mathbb{Z}[G]$ as polynomials is essentially unique:

Lemma 1.1. *Let $P \in \mathbb{Z}[x]$ then we have:*

$$P(\sigma) = 0 \in \mathbb{Z}[G] \quad \textit{iff} \quad P(1) = 0 \textit{ and } P(\zeta_p) = 0$$

Proof. Let $P \in \mathbb{Z}[x]$ such that $P(\sigma) = 0$. From (1.1) we immediately get $x^p - 1|P(x)$ and therefore $P(1) = P(\zeta_p) = 0$.

On the other hand, suppose $P(1) = P(\zeta_p) = 0$. Then $x - 1|P(x)$ and $x^{p-1} + \cdots 1|P(x)$ and thus $x^p - 1|P(x)$. Initially, the divisibility is only valid in $\mathbb{Q}[x]$, but since the divisors are monic, the divisibility in $\mathbb{Z}[x]$ follows too. □

From now on, let us assume that L is known to have a normal integral basis.

The next lemma gives us a necesary condition for an element $\theta \in \mathcal{O}$ to generate a normal integral basis.

Lemma 1.2. *Let us assume that $L/\mathbb{Q}$ is normal, and that θ generates a normal integral basis. Then $|\operatorname{Tr}(\theta)| = 1$.*

Proof. Let $\theta_1, \ldots, \theta_p$ be the conjugates of θ and $t = \operatorname{Tr}(\theta)$. Then $t = \theta_1 + ... + \theta_p$ and $1 = (1/t)(\theta_1 + ... + \theta_p)$. Since θ generates a normal integral basis it follows that $1/t \in \mathbb{Z}$ and therefore $|t| = 1$. □

Note that if θ gives a normal integral basis, then $-\theta$ gives a normal integral basis as well, hence without loss of generality we can assume that the sought element θ has trace one.

The following lemma is simply another way to state the fact that there exists an element $\theta \in \mathcal{O}$ such that $\mathbb{Z} \cdot \theta + \mathbb{Z} \cdot \sigma(\theta) + \ldots + \mathbb{Z} \cdot \sigma^{p-1}(\theta) = \mathcal{O}$.

Lemma 1.3. *The field L possesses a normal integral basis over $\mathbb{Z}$ if and only if the ring $\mathcal{O}$ is free of rank one as a $\mathbb{Z}[G]$ module.*

Unfortunately, it is quite difficult to deal directly with the ring $\mathbb{Z}[G]$. However, the ring

$\mathbb{Z}[G]$ has a quotient which is a nice Dedekind domain, and we are going now to exhibit it.

Let ζ_p denote a primitive p-th root of unity, and let $\mathcal{R}$ denote the ring of integers of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. Let $s = 1 + \sigma + \cdots + \sigma^{p-1} \in \mathbb{Z}[G]$, and let (s) denote the principal ideal generated by s in $\mathbb{Z}[G]$, that is $s\,\mathbb{Z}[G]$. Then clearly $\mathbb{Z}[G]/(s)$ is a commutative ring.

Let us define a ring homomorphism $\phi : \mathbb{Z}[G] \to \mathcal{R}$, by

$$\phi(\sum_{i=0}^{p-1} a_i\sigma^i) = \sum_{i=0}^{p-1} a_i\zeta_p^i \qquad a_i \in \mathbb{Z}$$

Then we have the following theorem, which is fundamental for the rest of the paper.

THEOREM 1.4. *$\mathbb{Z}[G]/(s) \cong \mathcal{R}$, under the homomorphism ϕ.*

PROOF. See (Curtis and Reiner, 1963, Lemma 74.4, p. 509) □

The following theorem is an easy consequence of Theorem 1.4.

THEOREM 1.5. *If the field L possesses a normal integral basis, then the ring $\mathcal{O}/s\mathcal{O}$ is free of rank one over $\mathbb{Z}[G]/(s)$. Moreover, if θ gives a normal integal basis for L, then $\theta + s\mathcal{O}$ is a free generator for $\mathcal{O}/s\mathcal{O}$ as a $\mathbb{Z}[G]/(s)$ module.*

PROOF. This is a standard result from algebra, see for example (Lang, 1993, p. 136). □

The next thing to notice is that the ideal $s\mathcal{O}$ is just $\mathbb{Z}$, since $s\mathcal{O}$ is just the set of absolute traces from $\mathcal{O}$, and it contains the element 1 by lemma 1.2. Therefore we are led to the following

Problem: *Find a free generator $\beta + \mathbb{Z}$ for $\mathcal{O}/\mathbb{Z}$ as a $\mathbb{Z}[G]/(s)$ module.*

In Section 1.2 we describe our algorithmic solution to this problem.

Let us assume now that we have found a free generator for $\mathcal{O}/\mathbb{Z}$ as a $\mathbb{Z}[G]/(s)$ module. We want to lift this generator to a free generator for $\mathcal{O}$ as a $\mathbb{Z}[G]$ module. Now, lemma 1.2 tells us that in order to find a representative $\theta = \beta + c$ of $\beta + \mathbb{Z}$ we have to require that $\mathrm{Tr}(\beta + c) = \pm 1$. This is easily done, since $\mathrm{Tr}(\beta + c) = \mathrm{Tr}(\beta) + pc$. In particular, note that it is necessary to have $\mathrm{Tr}(\beta) \equiv \pm 1 \pmod{p}$.

1.2. MODULES OVER DEDEKIND DOMAINS

In what follows we denote the action of an element $\sigma^j \in G$ on an element $\alpha \in L$ by $\sigma^j \cdot \alpha$ rather than by $\sigma^j(\alpha)$. Next, we extend this action by linearity on the whole of $\mathbb{Z}[G]$, and we write $g \cdot \alpha$ to denote the action of $g \in \mathbb{Z}[G]$ on $\alpha \in L$.

Let d be arbitrary such that

$$\mathcal{O} \subset \mathcal{M} = \mathbb{Z}[G] \cdot (\alpha/d)$$

e.g. one could take the discriminant of the set $\{\alpha, \sigma(\alpha), \ldots, \sigma^{p-1}(\alpha)\}$, since it is a standard fact from number theory that $\mathcal{O}$ is contained in the free $\mathbb{Z}[G]$ module $\mathcal{M}$ generated by α/d. By hypothesis $\mathcal{O}$ has a normal integral basis generated by θ, and we can write

$$\theta = g \cdot (\alpha/d)$$

for some $g \in \mathbb{Z}[G]$, so we can write

$$\mathbb{Z}[G]\; g \cdot (\alpha/d) = \mathcal{O} \subset \mathcal{M} = \mathbb{Z}[G] \cdot (\alpha/d)$$

Our objective is to find g. Let $\{\alpha_1, \ldots, \alpha_p\}$ be a known integral basis for $\mathcal{O}$. Since by hypothesis

$$\mathcal{O} = \sum_{i=1}^{p} \mathbb{Z}\ \alpha_i$$

(where *the sum is direct*) and L is normal, we must have

$$\mathcal{O} = \sum_{i=1}^{p} \mathbb{Z}[G] \cdot \alpha_i$$

(where *the last sum is not direct*). In other words, the α_i's form a set of generators of $\mathcal{O}$ as a $\mathbb{Z}[G]$ module. We want to compute a single free generator θ from the given set $\{\alpha_1, \ldots, \alpha_p\}$.

Now, using linear algebra computations, we can express each element α_i of the known integral basis as a linear combination with integral coefficients a_{ij} of the elements $\{\alpha/d, \sigma \cdot (\alpha/d), \ldots, \sigma^{p-1} \cdot (\alpha/d)\}$. In other words, for $i = 1, \ldots, p$ we can write

$$\alpha_i = \sum_{j=1}^{p} a_{ij}\ \sigma^{j-1} \cdot (\alpha/d)$$

that is

$$\alpha_i = g_i \cdot (\alpha/d)$$

with

$$g_i = \sum_{j=1}^{p} a_{ij}\ \sigma^{j-1} \in \mathbb{Z}[G]$$

Therefore we can write

$$\mathcal{O} = \left(\sum_{i=1}^{p} \mathbb{Z}[G]\ g_i \right) \cdot (\alpha/d)$$

In particular, this implies that, if we let $\theta = g \cdot (\alpha/d)$ then we must have the following equality of ideals of $\mathbb{Z}[G]$:

$$\mathbb{Z}[G]\ g + \operatorname{ann}(\alpha/d) = \left(\sum_{i=1}^{p} \mathbb{Z}[G]\ g_i \right) + \operatorname{ann}(\alpha/d)$$

where $\operatorname{ann}(\alpha/d)$ is an ideal of $\mathbb{Z}[G]$, defined as follows:

$$\operatorname{ann}(\alpha/d) = \{h \in \mathbb{Z}[G] \mid h \cdot (\alpha/d) = 0\}$$

However, since by hypothesis α gives a normal basis for $L/\mathbb{Q}$, the same is true for α/d, hence $\operatorname{ann}(\alpha/d) = 0$, and we have the following equality of ideals of $\mathbb{Z}[G]$:

$$\mathbb{Z}[G]\, g = \sum_{i=1}^{p} \mathbb{Z}[G]\, g_i$$

Now, under the homomorphism ϕ defined above, the element g_i goes to

$$\gamma_i := \sum_{j=1}^{p} a_{ij}\ \zeta_p^{j-1} \in \mathcal{R}$$

and therefore, under ϕ, the principal ideal $\mathbb{Z}[G]\, g$ of $\mathbb{Z}[G]$ maps to the following integral ideal of $\mathcal{R}$:

$$\mathfrak{I} = \sum_{i=1}^{p} \mathcal{R}\ \gamma_i$$

With Theorem 1.5 in mind, we see that if $\mathcal{O}/s\mathcal{O}$ has a free generator then $\mathfrak{I}$ is a principal ideal.

1.3. Concluding step

It is clear that if g is a generator of $\mathbb{Z}[G]\, g$, then $\phi(g)$ is a generator of $\mathfrak{I} = \phi(\mathbb{Z}[G]\, g)$. However, if γ is a generator of $\mathfrak{I}$, then it may happen that there is no generator of $\mathbb{Z}[G]\, g$ in the set $\phi^{-1}(\gamma)$. This is seen to be equivalent to the following statement: the image of the group of units $\mathbb{Z}[G]^*$ of $\mathbb{Z}[G]$ is contained properly in the group of units $\phi(\mathbb{Z}[G])^*$ of $\phi(\mathbb{Z}[G])$. Therefore we continue with a closer examination of the the unit groups. In order do do this we introduce some more notation. Let $\pi := \zeta_p - 1$ be a generator for the unique prime ideal of $\mathcal{R}$ lying above p. Since p is totally ramified, we have a canonical isomorphism

$$\mathbb{Z}/p\mathbb{Z} \to \mathcal{R}/(\pi) : k + p\mathbb{Z} \mapsto k + (\pi) \tag{1.2}$$

of residue rings. As immediately consequences we note:

$$j \equiv k \pmod{\pi} \quad\Longleftrightarrow\quad j \equiv k \pmod{p} \tag{1.3}$$

$j,\, k \in \mathbb{Z}$ and for any $P \in \mathbb{Z}[t]$

$$P(\zeta_p) \equiv P(1) \pmod{\pi} \tag{1.4}$$

since $\zeta_p \equiv 1 \pmod{\pi}$.

Theorem 1.6.

$$\phi(\mathbb{Z}[G]^*) = \{\epsilon \in \mathcal{R}^* \mid \epsilon \equiv \pm 1 \pmod{\pi}\}$$

Proof. Let $h = P(\sigma) \in \mathbb{Z}[G]^*$ be a unit ($P \in \mathbb{Z}[t]$). Then there is an $Q(\sigma) \in \mathbb{Z}[G]^*$ such that $P(\sigma)Q(\sigma) = 1$. Therefore we also have $P(\zeta_p)Q(\zeta_p) = 1$ and $P(1)Q(1) = 1$ which implies $P(1) = \pm 1$ and $\epsilon := \phi(h) = P(\zeta_p) \in \mathcal{R}^*$. Using (1.3) and (1.4) we see $\epsilon \equiv \pm 1 \pmod{\pi}$.

Now, let us suppose $\epsilon \in \mathcal{R}^*$, $e \in \{\pm 1\}$ s.th.

$$\epsilon \equiv e \pmod{\pi}. \tag{1.5}$$

$\epsilon \in \mathcal{R}^*$ implies the existenc of $P,\ Q \in \mathbb{Z}[t]$ s.th. $\epsilon = P(\zeta_p)$ and $P(\zeta_p)Q(\zeta_p) = 1$. Using

(1.4) we get $P(1)Q(1) = 1 \pmod{\pi}$. Using (1.5) and (1.3) we see $P(1) \equiv e \equiv Q(1) \pmod{p}$. Let $P(1) = e + kp$ and $Q(1) = e + lp$ and define $P' := P - k\Phi_p$, $Q' := Q - l\Phi_p$ where $\Phi_p := (t^p - 1)/(t-1)$. Since $\Phi_p(1) = p$ we get $P'(1) = e = Q'(1)$. Similarily, $\Phi_p(\zeta_p) = 0$ implies $P'(\zeta_p) = Q'(\zeta_p)$. Finally this yields

$$P'(\sigma)Q'(\sigma) = 1$$

as desired, therefore ϵ is a unit in $\mathbb{Z}[G]$. □

Using circular units we get:

THEOREM 1.7. *$\phi(\mathbb{Z}[G]^*)$ is of finite index in $\mathcal{R}^*$, more precisely: the circular units $u_k := (1-\zeta_p^k)/(1-\zeta_p)$, $1 \le k \le (p-1)/2$ are a complete set of representatives for $\mathcal{R}^*/\phi(\mathbb{Z}[G]^*)$. The index is $(p-1)/2$.*

PROOF. Since $u_k = 1+\zeta_p+\ldots+\zeta_p^{k-1}$ we get (using (1.4)) $u_k \equiv k \pmod{\pi}$. We conclude $u_k \equiv u_j \pmod{\phi}(\mathbb{Z}[G]^*)$ if and only if $k = j$.

Let $u \in \mathcal{R}^*$ be an arbitrary unit. Then $u \equiv \pm k \pmod{\pi}$ with $1 \le k \le (p-1)/2$ by (1.2), therefore $u \equiv \pm u_k \pmod{\pi}$, $u/u_k \equiv \pm 1 \pmod{\pi}$ implying $u \equiv \pm u_k \pmod{\phi}(\mathbb{Z}[G]^*)$ using theorem 1.6. □

Using either standard algorithms (Pohst and Zassenhaus, 1989) or Buchmann's subexponential class group algorithm we can effectively find an element $\gamma \in \mathcal{R}$ such that $\mathfrak{I} = \gamma\mathcal{R}$. Representing γ as $\sum_{j=1}^{p-1} a_j \zeta_p^{j-1}$ we can compute a representative g' in $\mathbb{Z}[G]$ of the preimage of γ:

$$g' := \sum_{j=1}^{p-1} a_j \sigma^{j-1} \in \mathbb{Z}[G]$$

so that

$$\theta \in (g' + \mathbb{Z}[G]\, s) \cdot (\alpha/d) = g' \cdot (\alpha/d) + \mathbb{Z}[G]\, s \cdot (\alpha/d) = g' \cdot (\alpha/d) + \mathbb{Z}\,\mathrm{Tr}(\alpha/d)$$

Since we assumed the existence of a normal integral basis, theorem 1.5 guarantees the existence of $\tilde{\theta} \in L$ s.th. $\mathbb{Z}[G]\tilde{\theta} = \mathcal{O}$, $\tilde{\theta} = g \cdot (\alpha/d)$ and $(\phi(g)) = \mathfrak{I} = (\gamma)$. Therefore $\phi(g) = \gamma\epsilon$. Obviously, if $g \cdot (\alpha/d)$ generates $\mathcal{O}$, so does $(eg) \cdot (\alpha/d)$ for any $e \in \mathbb{Z}[G]^*$. Therefore theorem 1.7 implies that there is a unit u_k in $\mathcal{R}$ and $e \in \mathbb{Z}[G]^*$ s.th. $\phi(eg) = \gamma u_k$.

If $\mathrm{Tr}(g' \cdot (\alpha/d)) \not\equiv \pm 1 \pmod{p}$ it is not possible to adjust g' in order to have $\mathrm{Tr}(\theta) = \pm 1$. This means that we have selected a wrong generator for our ideal. By the above considerations, if we exchange γ with γu_k we must get a generator after at most $(p-1)/2$ trials.

2. Example

To illustrate our algorithm, consider the field $L = \mathbb{Q}(\alpha)$, where α is a root of the polynomial

$$m_\alpha(x) \quad = \quad x^5 - 1210x^3 + 18755x^2 - 53240x - 145079$$

this field has discriminant $14641 = 11^4$. (Note that in this case we know a normal integral basis, $\zeta_{11} + \bar{\zeta}_{11}$ is a generator since L is the maximal real subfield of $\mathbb{Q}(\zeta_{11})$.)

First, we observe that the conjugates of $\alpha - 1$ yield a normal basis for the field. We compute an integral basis for L, obtaining:

$$\begin{aligned}
\alpha_1 &= 1 \\
\alpha_2 &= (1+\alpha)/5 \\
\alpha_3 &= (121 + 22\alpha + \alpha^2)/275 \\
\alpha_4 &= (1001 + 253\alpha + 3\alpha^2 + \alpha^3)/1375 \\
\alpha_5 &= (38841 + 8349\alpha + 176\alpha^2 + 44\alpha^3 + 1\alpha^4)/75625
\end{aligned}$$

Now we express the elements of the computed integral basis as a linear combination of the elements of the normal basis and we get:

$$\begin{aligned}
(\alpha_1, \ldots, \alpha_5) &= (\alpha - 1, \sigma(\alpha - 1), \ldots, \sigma^4(\alpha - 1)) \cdot \\
& \begin{pmatrix} -1/5 & 3/25 & -122/275 & 589/275 & -144/275 \\ -1/5 & -2/25 & -12/25 & 29/25 & -229/275 \\ -1/5 & -2/25 & -117/275 & 284/275 & -189/275 \\ -1/5 & -2/25 & -122/275 & 314/275 & -189/275 \\ -1/5 & -2/25 & -112/275 & 254/275 & -184/275 \end{pmatrix}
\end{aligned}$$

We immediately see that we can take $d = 275$ as the denominator. Next, we compute the elements g_i as $g_1 = -(275/5)\sum_{i=0}^{4} \sigma^i, \ldots$. After applying ϕ to the elements g_i we get

$$\begin{aligned}
\gamma_1 &= 0 \\
\gamma_2 &= 55 \\
\gamma_3 &= -10 - 20\zeta_5 - 5\zeta_5^2 - 10\zeta_5^3 \\
\gamma_4 &= 335 + 65\zeta_5 + 30\zeta_5^2 + 60\zeta_5^3 \\
\gamma_5 &= 40 - 45\zeta_5 - 5\zeta_5^2 - 5\zeta_5^3
\end{aligned}$$

We find out (computationally) that the ideal $\mathcal{I} = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5 \rangle$ is generated by γ_3. As a preimage for γ_3 we can take α_3. Since $\mathrm{Tr}(\alpha_3) = 11 \equiv 1 \pmod 5$, we see that $\alpha_3 - 2$ has trace one, and it generates indeed a normal integral basis.

The above example took approximately 1.5 sec on a SPARC 5 running SunOS 5.5.1 and KASH 1.9. In this particular example about 60% of the time was spent to compute a generator for the ideal $\mathcal{I}$.

If we apply our algorithm to different cyclic number fields of the same degree p the execution time can be reduced to a large extent, since the computation of the class group of $\mathbb{Q}(\zeta_p)$ (needed for the computation of a generator of $\mathcal{I}$) must be performed only once. In our example, if we ignore the time spent to compute the class group of $\mathbb{Q}(\zeta_5)$, the computation time reduces to 0.3 sec.

Next we consider the family L_n of fields generated by a root ρ_n of the polynomial

$$\begin{aligned}
x^5 &+ n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 \\
&+ (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1.
\end{aligned}$$

These fields have been investigated by several people (Lehmer, 1988; Schoof and Washington, 1989; Darmon, 1991; Gaál and Pohst, 1997). There are explicit formulas for the conductor, for a set of fundamental units and for an integral basis. We computed integral normal bases for L_n, $1 \leq n < 1000$. The maximal conductor was $1001006006011 = 11 \cdot 71 \cdot 2621 \cdot 489011$, obtained for $n = 999$. The maximal $\phi(f)$ was 997008993010 for $n = 998$. The complete series was done in 2 minutes.

In almost all cases (766 out of the 800 tamely ramified fields) the generator for the integral normal bases was of the shape $a + \rho_n$ for some $a \in \mathbb{Z}$.

Our experiments show that for larger examples ($p = 11, 13, 17$) the running time of the algorithm is dominated by the integral basis computation.

3. Acknowledgement

We would like to thank an anonymous referee for his useful suggestions. In particular, theorem 1.7 and the elegant phrasing of theorem 1.6 are due to him.

References

Acciaro, V., Klüners, J. (1999). Computing automorphisms of abelian number fields. *Math. Comp.*, **68**:1179 – 1186.

Cohen, H. (1995). *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 2nd edition.

Curtis, C. W., Reiner, I. (1963). *Representation Theory of Finite Groups and Associative Algebras*. John Wiley and Sons.

Daberkow, M., Fieker, C., Klüners, J., Pohst, M. E., Roegner, K., Schoörnig, M., Wildanger, K. (1997). KANT V4. *J. Symb. Comput.*, **24**:267–283.

Darmon, H. (1991). Note on a polynomial of Emma Lehmer. *Math. Comp.*, **56**:795 – 800.

Gaál, I., Pohst, M. (1997). Power integral bases in a parametric family of totally real cyclic quinitcs. *Math. Comp.*, **66**:1689 – 1696.

Lang, S. (1993). *Algebra*. Addison-Wesley, 3rd edition.

Lehmer, E. (1988). Connection between Gaussian periods and cyclic units. *Math. Comp.*, **50**.

Narkiewicz, W. (1989). *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 2nd edition.

Pohst, M. E., Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory*. Encyclopaedia of mathematics and its applications. Cambridge University Press.

Schlickewei, H. P., Stepanov, S. A. (1993). Algorithms to construct normal bases of cyclic number fields. *J. Number Theory*, **44**:30–40.

Schoof, R., Washington, L. (1989). Quintic polynomials and real cyclotomic fields with large class numbers. *Math. Comp.*, **50**:543 – 556.