JP Journal of Algebra, Number Theory and Applications

http://www.pphmj.com
http://dx.doi.org/10.17654/NT040060923
Volume 40, Number 6, 2018, Pages 923-943 **ISSN: 0972-5555**

COMPUTING NORMAL INTEGRAL BASES OF ABELIAN NUMBER FIELDS

Vincenzo Acciaro and Diana Savin

Dipartimento di Economia
Università di Chieti-Pescara
Viale Pindaro 42, 65127, Pescara, Italy

Faculty of Mathematics and Computer Science
Ovidius University
Bd. Mamaia 124, 900527, Constanta, Romania

Abstract

Let L be an abelian number field of degree n with Galois group G. In this paper we study how to compute a normal integral basis for L, if there is at least one, assuming that the group G and an integral basis for L are known. The running time of the algorithm is dominated by the time required to compute the unit group of some cyclotomic fields and test whether some ideals are principal in these fields. When n is a prime power these two tasks can be accomplished quite efficiently thanks to recent results of Biasse, Fieker et al.

1. Introduction

Let L be a Galois number field and let $\mathcal{O}$ denote its ring of algebraic integers. A classical problem of algebraic number theory is to compute a normal integral basis for L over $\mathbb{Q}$, that is a basis of $\mathcal{O}$ as a $\mathbb{Z}$-module

Received: May 26, 2018; Revised: June 26, 2018; Accepted: July 23, 2018
2010 Mathematics Subject Classification: Primary 11R04, Secondary 11R20, 11R33, 11Y40.
Keywords and phrases: normal integral bases, abelian number fields.

which is made up of all the conjugates of a single algebraic integer, assuming that there is at least one.

Although the theoretical aspects of the question are well understood, the effective construction of normal integral basis has been accomplished only in few particular cases.

From a theoretical point of view, the Hilbert-Speiser theorem asserts that an abelian number field L admits a normal integral basis if and only if the conductor of L is square free. In this case such a basis may be constructed by means of Gaussian periods: if we denote the conductor of L by $\mathfrak{f}$, then $Tr_{\mathbb{Q}(\zeta_\mathfrak{f})/L}(\zeta_\mathfrak{f})$ generates a normal integral basis for L (see [16, p. 410]). From a practical point of view, this is quite unsatisfactory, since we need to work in the field $\mathbb{Q}(\zeta_\mathfrak{f})$ whose degree $\varphi(\mathfrak{f})$ may be very large in comparison to $[L:\mathbb{Q}]$. Hence the computation of the relative trace might be very expensive.

In [3] the first author and Fieker devised an algorithm to compute a normal integral basis in cyclic number fields of prime degree, assuming that there is at least one, whose running time is essentially independent of the conductor $\mathfrak{f}$.

In [2] the first author and Cangelmi, using a totally different approach, dealt with abelian number fields of exponent 2, 3, 4 and 6, and obtained a new algorithm whose running time is again independent of the conductor $\mathfrak{f}$.

In this paper we extend the results in [2] to all the abelian number fields of finite degree over $\mathbb{Q}$. The running time of the new algorithm is again independent of the conductor $\mathfrak{f}$.

In Section 2 we fix some notation, give some basic results, and reduce our problem to that of computing a generator of a certain ideal of the group ring $\mathbb{Z}[G]$ of the Galois group G of L.

In Section 3 we construct an explicit homomorphic embedding of this

group ring $\mathbb{Z}[G]$ into the finite product of (possibly multiple copies of) cyclotomic rings of order q, for all the divisors q of n.

In Sections 5 and 6 we describe the main steps of our algorithm.

Sections 7 and 8 are essentially a survey of recent results about the computation of the unit group and the algorithmic solution of the Principal Ideal Problem in cyclotomic fields, which constitute two major ingredients of our algorithm. In particular, if one assumes the Generalized Riemann Hypothesis, the unit group of the cyclotomic fields of order p^n (p prime) can be computed quite efficiently for all p and n such that $\varphi(p^n) < 162$. This result can be applied to speed up our algorithm when our group G is a p-group, since in this case all the cyclotomic fields involved have order a power of p.

Finally, in Section 9, we give some explicit numerical examples obtained by using the computational algebra program Sage [21].

Since the algorithm described in this paper is based upon the theoretical frame-work developed in [2] by the first author and Cangelmi, some overlap with the previous paper is unfortunately unavoidable.

2. Notation and General Framework

From now on, let L be an abelian number field of degree n, let $\mathcal{O}$ be its ring of algebraic integers, and let α be a primitive element for the extension $L/\mathbb{Q}$, so that $L = \mathbb{Q}[\alpha]$. We can assume that $\alpha \in \mathcal{O}$, and we denote the minimal polynomial of α over $\mathbb{Q}$ by $m(x)$, which is therefore a monic polynomial of degree n with integer coefficients.

We assume that $\{\beta_1, ..., \beta_n\}$ is a known integral basis of $\mathcal{O}$, that is a basis of $\mathcal{O}$ as a $\mathbb{Z}$-module. We recall that an integral basis can be computed (for example) using the algorithms described in [12] and [18]. Chistov [11] proved that finding the ring of integers of an algebraic number field is polynomial time equivalent to the problem of finding the largest square-free

divisor of a positive integer. No polynomial time algorithm is known for the latter problem, and probably this problem is no easier than the more general problem of factoring integers.

Let G be the Galois group of $L/\mathbb{Q}$. Under the Extended Riemann Hypothesis it is possible to compute efficiently G by using the algorithm described in [4]. Such algorithm gives us explicitly the action of the elements of G on α. So, we let $G = \{g_1, ..., g_n\}$, and put $\alpha_i = g_i(\alpha)$, for $i = 1, ..., n$. Without loss of generality we can assume that the conjugates of α constitute a basis of L as a vector space over $\mathbb{Q}$.

Let $\mathbb{Z}[G]$ and $\mathbb{Q}[G]$ denote respectively the group ring of G over $\mathbb{Z}$ and over $\mathbb{Q}$. The action of G on L can be extended by linearity to an action of $\mathbb{Q}[G]$ (or $\mathbb{Z}[G]$), setting

$$\left(\sum_{g\in G} a_g g\right) x = \sum_{g\in G} a_g g(x),$$

for all a_g in $\mathbb{Q}$ (resp. $\mathbb{Z}$), and all $x \in L$.

We say that L, or $\mathcal{O}$, has a *normal integral basis* when there exists $\theta \in \mathcal{O}$ such that the conjugates of θ constitute a basis of $\mathcal{O}$ as a $\mathbb{Z}$-module. In such a case we call θ a *normal integral basis generator*.

If $\theta \in \mathcal{O}$, then θ is a normal integral basis generator if and only if the discriminant of the set $\{g_1(\theta), ..., g_n(\theta)\}$ equals the discriminant of L. We will need to perform such a check just once, and our algorithm will return θ if such a θ exists, and 'θ does not exist' otherwise.

The fact that the conjugates of α constitute a basis for $L/\mathbb{Q}$ can be rephrased by saying that L is free of rank one as a $\mathbb{Q}[G]$-module. The integer counterpart of this property is given next.

Lemma 2.1. *The field L possesses a normal integral basis if and only if the ring $\mathcal{O}$ is free of rank one as a $\mathbb{Z}[G]$-module.*

Assume now that $\mathcal{O}$ has a normal integral basis and that θ is a normal integral basis generator, so that $\mathcal{O} = \mathbb{Z}[G]\theta$.

Since $\mathcal{O} = \sum_{i=1}^{n} \mathbb{Z}\beta_i$ and L is normal, we also have $\mathcal{O} = \sum_{i=1}^{n} \mathbb{Z}[G]\beta_i$ (where this sum is not direct). In other words, the β_i's form a set of generators of $\mathcal{O}$ as a $\mathbb{Z}[G]$-module. We would like to compute a single free generator of $\mathcal{O}$ from the given set $\{\beta_1, ..., \beta_n\}$.

Let $D \in \mathbb{Z}$ be such that

$$\mathcal{O} \subseteq \mathbb{Z}[G]\frac{\alpha}{D}.$$

For instance, we could take D equal to the discriminant of the set $\{\alpha_1, ..., \alpha_n\}$. For the sake of convenience, we put $\alpha' = \alpha/D$, and $\alpha'_i = g_i(\alpha') = \alpha_i/D$, for $i = 1, ..., n$.

On the one hand, we have $\theta \in \mathbb{Z}[G]\alpha'$, so that $\theta = \sum_{i=1}^{n} t_i\alpha'_i$, for some $t_i \in \mathbb{Z}$. In other words, if we let $t = \sum_{i=1}^{n} t_i g_i$, then we have $\theta = t\alpha'$, where $t \in \mathbb{Z}[G]$.

On the other hand, we can express each element β_j of the known integral basis as a linear combination with integral coefficients of the elements $\alpha'_1, ..., \alpha'_n$. In other words, for $j = 1, ..., n$ we can write

$$\beta_j = \sum_{i=1}^{n} b_{ij}\alpha'_i, \tag{2.1}$$

with $b_{ij} \in \mathbb{Z}$. This is equivalent to say that $\beta_j = b_j\alpha'$, where

$$b_j = \sum_{i=1}^{n} b_{ij}g_i \in \mathbb{Z}[G]. \tag{2.2}$$

Therefore we have

$$\mathcal{O} = \mathbb{Z}[G]t\alpha' = \left(\sum_{j=1}^{n} \mathbb{Z}[G]b_j\right)\alpha',$$

and, since α gives a normal basis for $L/\mathbb{Q}$ and the same is true for α',

$$\mathbb{Z}[G]t = \sum_{j=1}^{n} \mathbb{Z}[G]b_j.$$

In conclusion, we have reduced our problem to the problem of finding a generator of the ideal of $\mathbb{Z}[G]$ generated by the set $\{b_1, ..., b_n\}$. For future reference, let us call this ideal I, that is let us define

$$I = \sum_{j=1}^{n} \mathbb{Z}[G]b_j. \tag{2.3}$$

We complete our arguments and state the main results of this section in the following theorem.

Theorem 2.2. *Let L be an abelian number field, and let I be the ideal of $\mathbb{Z}[G]$ defined by* (2.3). *Then, L has a normal integral basis if and only if I is principal. More precisely, if $\alpha' \in L$ is such that $L = \mathbb{Q}[G]\alpha'$ and $\mathcal{O} \subseteq \mathbb{Z}[G]\alpha'$, then we have*:

- *If θ is a normal integral basis generator, and $\theta = t\alpha'$, with $t \in \mathbb{Z}[G]$, then $I = \mathbb{Z}[G]t$.*

- *If I is principal and $t \in \mathbb{Z}[G]$ is a generator of I, then $t\alpha'$ is normal integral basis generator.*

Proof. The above arguments show that if L has a normal integral basis and θ is a normal integral basis generator, then I is principal and is generated by t, which is defined by the relation $\theta = t\alpha'$. Then, it is easily seen that the converse holds true, and that if t is a generator of I, then the element $t\alpha'$ is integral and it is a normal integral basis generator.

3. Decomposition of the Group Ring $\mathbb{Q}G$

We begin by stating a result about rational group rings of finite abelian groups, proved by Perlis and Walker in [17] as well as by Higman [15].

Theorem 3.1 (Perlis, Walker)**.** *Let G be a finite abelian group of order n. Then*

$$\mathbb{Q}G \cong \oplus_{q|n} a_q \mathbb{Q}(\zeta_q),$$

where $a_q\mathbb{Q}(\zeta_q)$ *denotes the direct sum of* a_q *copies of* $\mathbb{Q}(\zeta_q)$*. Moreover,* $a_q = n_q/\varphi(q)$*, with* n_q *equal to the number of elements of order q in G.*

A very enjoyable proof of this result can be found in [19]. However, for our purposes, we are going to construct this isomorphism explicitly, and then we will restrict it to $\mathbb{Z}G$.

Following Higman's approach the idempotent $e_\chi \in \mathbb{C}G$ associated to any character (representation of degree 1) χ is defined as:

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})g.$$

Let $\chi_1, ..., \chi_n$ be the irreducible characters of G, and denote the character group by $\hat{G}$. From now on, we write e_i in place of e_{χ_i}, for short.

Extending the characters linearly to the full group ring, we see that any element h of $\mathbb{C}G$ admits two unique representations:

$$h = \sum_{i=1}^{n} h_i g_i = \sum_{i=1}^{n} c_i e_i,$$

and we have the well known decomposition

$$\mathbb{C}G = \mathbb{C}e_1 \oplus \cdots \oplus \mathbb{C}e_n.$$

If we denote the character matrix $(\chi_i(g_j))_{i,\, j=1,\ldots,n}$ of G by A, then we have

the following equality:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}. \tag{3.1}$$

Conversely, as A is not singular, if the coefficients (c_i) of an element h of $\mathbb{C}G$ are known, we can easily compute the coefficients (h_i) :

$$\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \tag{3.2}$$

Here we can compute directly the inverse of the matrix A, as it is well known [20, Lemma C-2.77] that $(A^{-1})_{ij} = \overline{\chi_j(g_i)}/|G| = \chi_j(g_i^{-1})/|G|$. Hence, we have:

Proposition 3.2. *The map $\mathbb{C}G \to \mathbb{C}^n$ which sends h to $(\chi_1(h), ..., \chi_n(h))$ is a $\mathbb{C}$-algebra isomorphism, and the associated matrix with respect to the bases $(g_1, ..., g_n)$ and $(e_1, ..., e_n)$ is the character matrix A.*

Now, we turn our attention back to the group ring $\mathbb{Q}G$ and to Theorem 3.1. For each irreducible character χ_i, $i = 1, ..., n$, let us denote its order in $\hat{G}$ by q_i. Therefore $\chi_i(g)$ is a root of unity of order q_i for all $g \in G$, and is a primitive root of unity of order q_i for some $g \in G$.

Note that if χ is a character of G with values in some Galois number field K (actually, some $\mathbb{Q}(\zeta)$, for some root of unity ζ) and σ is an automorphism of K, then $\sigma(\chi)$ is another character of G with values in the same field K. We say that χ_i and χ_j, with values in some K, are *algebraically conjugate* if there exists an automorphism σ of K such that $\chi_j = \sigma(\chi_i)$. Thus, χ_i and χ_j are algebraically conjugate if and only if they are equivalent over $\mathbb{Q}$. However, for our purposes, it is better to think in terms of conjugation rather than in terms of equivalence of the associated representations.

Let us select from the set $\{\chi_1, ..., \chi_n\}$ a maximal subset of irreducible characters such that no one of them is algebraically conjugate to some other.

Let us assume that χ_r is an irreducible character of G of order o_r, so that χ_r maps $\mathbb{Q}G$ onto $\mathbb{Q}[\zeta_{o_r}]$. If σ is an automorphism of $\mathbb{Q}[\zeta_{o_r}]$, then σ sends ζ_{o_r} to $\zeta_{o_r}^s$, where o_r and s are coprime, and therefore χ_r to χ_r^s.

Vice versa, if χ_a and χ_r are two characters of G such that $\chi_a = \chi_r^s$ in $\hat{G}$, with $(r, o_r) = 1$, then $\chi_a = \sigma(\chi_r)$, where σ sends ζ_{o_r} to $\zeta_{o_r}^s$ in $\mathbb{Q}[\zeta_{o_r}]$.

Thus, the computation of a maximal subset of irreducible characters such that no one of them is algebraically conjugate to some other can be done by applying one of the following methods:

- For each character χ, remove all co-prime powers of χ from the list;
- For each character χ, form the orbit of χ under the action of the Galois group of $\mathbb{Q}[\zeta_{o_r}]$, and remove all the conjugates of χ from list.

After rearranging the original set, we can assume that $\{\chi_1, ..., \chi_k\}$ is such a subset, where $1 \le k \le n$.

For further reference, for any character which has not been selected, we keep track of the selected character which is algebraically conjugate to it, and of the automorphism which gives such a relation. Precisely, for any i, where $k < i \le n$, we take note of the (unique) index k_i, with $1 \le k_i \le k$, such that χ_i and χ_{k_i} are algebraically conjugate, and also of the automorphism σ_i such that $\sigma_i(\chi_{k_i}) = \chi_i$.

It is easy to see that, for any divisor q of n, the number of irreducible characters of order q equals $\varphi(q)$ times the number of subgroups of G of order q, and the maximal number of irreducible characters of order q which are not algebraically conjugate equals the number of subgroups of G of order

q. In this way, we recover the same arithmetic conditions stated in Theorem 3.1.

Summarizing, we have:

Proposition 3.3. *Assume that* $\{\chi_1, ..., \chi_k\}$ *is a maximal subset of irreducible characters which are not pairwise algebraically conjugate. Then, the map* $\phi : \mathbb{Q}G \to \mathbb{Q}(\zeta_{q_1}) \oplus \cdots \oplus \mathbb{Q}(\zeta_{q_k})$ *which sends* h *to* $(\chi_1(h), ..., \chi_k(h))$ *is a* $\mathbb{Q}$*-algebra isomorphism. Moreover, if we let B be the matrix made of the first k rows of the character matrix A, then for* $h = \sum_{i=1}^{n} h_i g_i$, *we have* $\phi(h) = (c_1, ..., c_k)$, *where*

$$\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = B \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}. \tag{3.3}$$

Finally, if $(c_1, ..., c_k) \in \mathbb{Q}(\zeta_{q_1}) \oplus \cdots \oplus \mathbb{Q}(\zeta_{q_k})$, *we let* $c_i = \sigma_i(c_{k_i})$ *for all i with* $k < i \le n$, *and we have* $\phi^{-1}((c_1, ..., c_k)) = \sum_{i=1}^{n} h_i g_i$, *where*

$$\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \tag{3.4}$$

At last, we consider the integral case, by restricting the map defined on $\mathbb{Q}G$, and we obtain:

Proposition 3.4. *The restriction of* ϕ *to* $\mathbb{Z}G$ *gives a* $\mathbb{Z}$*-algebra homomorphism*

$$\psi : \mathbb{Z}G \hookrightarrow \mathbb{Z}[\zeta_{q_1}] \oplus \cdots \oplus \mathbb{Z}[\zeta_{q_k}],$$

which is injective. If $h = \sum_{i=1}^{n} h_i g_i$, *then* $\psi(h) = (c_1, ..., c_k)$, *where* $(c_1, ..., c_k)$ *is given by* (3.3). *If* $(c_1, ..., c_k) \in \psi(\mathbb{Z}G)$, *then* $\psi^{-1}((c_1, ..., c_k)) = \sum_{i=1}^{n} h_i g_i$, *where* $(h_1, ..., h_n)$ *is given by* (3.4).

Proof. If χ_j is an irreducible character of G and $a_1, ..., a_n \in \mathbb{Z}$, then

$$\chi_j\left(\sum_{i=1}^{n} a_i g_i\right) = \sum_{i=1}^{n} a_i \chi_j(g_i) \in \mathbb{Z}[\zeta_{q_j}].$$

This shows that the restriction of ϕ to $\mathbb{Z}G$ defines an algebra homomorphism from $\mathbb{Z}G$ into $\mathbb{Z}[\zeta_{q_1}] \oplus \cdots \oplus \mathbb{Z}[\zeta_{q_k}]$. The other claims follow from Proposition 3.3. □

We remark that the homomorphism ψ is not surjective.

4. Ideals in Products of Integral Domains

In the next section we are going to exploit Theorem 2.2 and Proposition 3.4 in order to give an explicit algorithm to find a normal integral basis of L. Here we state some other preliminary results.

Since it is quite difficult to work in $\mathbb{Z}[G]$, we will consider the extension of the ideal I by means of the homomorphism ψ. Then we would like to recover a generator of I starting from a generator of such an extended ideal, whenever they exist.

We first state a simple lemma about product of rings. If Γ is any ring, we denote its group of units by $U(\Gamma)$.

Lemma 4.1. *Let Γ be commutative ring which can be expressed as a direct product $\Gamma = \Gamma_1 \times \cdots \times \Gamma_k$ of some rings Γ_i, where $i = 1, ..., k$.*

- *Any ideal J of Γ has the form $J = J_1 \times \cdots \times J_k$, where J_i is an ideal of Γ_i.*

- *An ideal J of Γ is principal if and only if J_i is principal, for all i; in such a case, if $J = a\Gamma$ with $a = (a_1, ..., a_k) \in \Gamma$, then $J_i = a_i\Gamma_i$.*

- *If each Γ_i is an integral domain and $a, b \in \Gamma$, then $a\Gamma = b\Gamma$ if and only if there is a $u \in U(\Gamma)$ such that $a = ub$.*

- $u \in U(\Gamma)$ *if and only if* $u = (u_1, ..., u_k)$, *with* $u_i \in U(\Gamma_i)$.

Now we let $\Gamma = \mathbb{Z}[\zeta_{q_1}] \times \cdots \times \mathbb{Z}[\zeta_{q_k}]$ and $J = \psi(I)\Gamma$, where I is defined by (2.3), and apply the previous lemma to them. The next result explains how we can recover a generator of I, when it exists.

Proposition 4.2. *Let I be a principal ideal of $\mathbb{Z}[G]$, $I = t\mathbb{Z}[G]$, and let $J = \psi(I)\Gamma$. Then J is principal, and if $J = d\Gamma$, then $t = \psi^{-1}(ud)$, for some $u \in U(\Gamma)$.*

Proof. It is obvious that J is principal, since $J = \psi(t)\Gamma$. If $J = \Gamma d$, Lemma 4.1 implies that $\psi(t) = ud$, for some $u \in U(\Gamma)$, whence the result.

□

The proof of the following proposition is easy.

Proposition 4.3. *Let S be a set of coset representatives for $\psi(U(\mathbb{Z}G))$ in $U(\Gamma)$. Let I be a principal ideal of $\mathbb{Z}[G]$, $I = t\mathbb{Z}[G]$, and let $J = \psi(I)\Gamma$. Then J is principal, and if $J = d\Gamma$, then $t = \psi^{-1}(ud)$, for some $u \in S$.*

5. Outline of the Algorithm

Let us assume that L is an abelian number field of degree n with Galois group G, and that L is described by giving the minimal polynomial $m(x)$ of an integral primitive element α, which generates a normal basis for $L/\mathbb{Q}$. We assume that the Galois group G has been computed, that we know the action of its elements on α, and that we have fixed an ordering of them, say $(g_1, ..., g_n)$. We assume also that an integral basis of $\mathcal{O}$ has been computed, and that we have fixed an ordering of its elements, say $(\beta_1, ..., \beta_n)$.

We first compute the discriminant D of the conjugates of α, and determine $\alpha' := \alpha/D$. We then compute the matrix (b_{ij}) defined by (2.1).

Then we fix an ordering of the irreducible characters χ_i of G, take note

of their orders q_i, and compute the character matrix $A := (\chi_i(g_j))$. We reorder the characters and extract the matrix B from A, as it is described in Proposition 3.3.

Next, we compute the ideal $J := \psi(I)R$, which is generated over R by $\psi(b_1), ..., \psi(b_n)$. This is done by applying (3.3). Namely, for $j = 1, ..., n$, if

$$b_j = \sum_{i=1}^{n} b_{ij} q_i, \tag{5.1}$$

then $\psi(b_j) = (c_{1,j}, ..., c_{k,j})$, where

$$\begin{pmatrix} c_{1,j} \\ \vdots \\ c_{k,j} \end{pmatrix} = B \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{n,j} \end{pmatrix}. \tag{5.2}$$

Then, for each $i = 1, ..., k$, we let J_i be the ideal of $\mathbb{Z}[\zeta_{q_i}]$ generated by the set $\{c_{i,1}, ..., c_{i,n}\}$ - in other words, the ideal J_i is generated by the i-th row of the matrix $(b_{ij}) \cdot B$.

Next we must find, for each $i = 1, ..., k$, a generator d_i of the ideal J_i, whenever it exists. For this purpose we can use in Sage - for example - the function *is_principal* [22, p. 241] which returns True if the ideal J_i is principal, followed by the function *gens_reduced* [22, p. 238] which expresses J_i in terms of at most two generators, and one if it is possible.

Now, note that if an irreducible character χ_i maps I into J_i and σ is an automorphism of $\mathbb{Q}(\zeta_{q_i})$, where $i = 1, ..., k$, then:

- $\sigma(\chi_i)$ maps I into $\sigma(J_i)$;
- if d_i is a generator of J_i, then $\sigma(d_i)$ is a generator of $\sigma(J_i)$.

Therefore the remaining elements $d_{k+1}, ..., d_n$ are obtained by applying to each d_i all the non-trivial automorphisms of $\mathbb{Q}(\zeta_{q_i})$, where $i = 1, ..., k$.

Now, Lemma 4.1 tells us that the element $d := (d_1, ..., d_n)$ generates J. We put $t := \psi^{-1}(d)$. In order to recover the standard form of t we just apply (3.4). Hence,

$$t = \sum_{i=1}^{n} t_i g_i, \tag{5.3}$$

where

$$\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = A^{-1} \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}. \tag{5.4}$$

Let us point out that all these computations are done in $\mathbb{Q}(\zeta_r)$, where r is the exponent of G. Now we let $\theta := t\alpha'$, and we compute the discriminant of $\{g_1\theta, ..., g_n\theta\}$.

If $D(g_1\theta, ..., g_n\theta)$ equals the discriminant of L and θ is an algebraic integer, then θ generates a normal integral basis.

Otherwise, we 'adjust' d by multiplying it by a suitable unit $u \in S$, and then we repeat the last matrix multiplication. Precisely, we first multiply the element $(d_1, ..., d_k)$ by a unit $u = (u_1, ..., u_k) \in S$, then we obtain the remaining elements $d_{k+1}, ..., d_n$ by applying to each d_i all the non-trivial automorphisms of $\mathbb{Q}(\zeta_{q_i})$, where $i = 1, ..., k$, and finally we apply again formula (5.4). In this way, we obtain a new θ and we have now to verify whether $D(g_1\theta, ..., g_n\theta)$ equals the discriminant of L and it is an algebraic integer or not.

The process must terminate after a finite number of steps, since the cardinality of S, i.e. the index $|U(\Gamma) : \psi(U(\mathbb{Z}G))|$ is finite, by Theorem 6.1 below. Furthermore, Proposition 4.2 implies that we will surely find a normal basis generator in one of these steps, if it exists.

6. Computation of a Transversal for $\psi(U(\mathbb{Z}G))$ in $U(\Gamma)$

Our next task is to compute efficiently a set S of coset representatives for $\psi(U(\mathbb{Z}G))$ in $U(\Gamma)$.

6.1. Faccin's algorithm

This task could be accomplished, for example, by first computing $U(\Gamma)$ using standard algorithms in algebraic number theory, then computing $U(\mathbb{Z}G)$ by means of the algorithm designed by Faccin [13], and, finally, computing the sought set of coset representatives. However, the computational effort involved by this method is not justified in this context, so we have to revert to a different technique.

6.2. Buchmann's algorithm

Buchmann et al. [10] designed an efficient algorithm allowing one to compute the structure of an unknown finite abelian group X, i.e., its invariant factors, assuming that a set V of generators is given, and that for $a, b \in X$ it is possible to compute their product, it is possible to compute a^{-1}, and it is possible to test the equality $a = b$. Buchmann's algorithm produces a list of positive integers $m_1, ..., m_k$ with $m_1 > 1$ and $m_i \mid m_{i+1}$ $(1 \le i < k)$, and an isomorphism $\phi : G \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ given in terms of the images of the known generators.

Buchmann's algorithm requires $O(|V|\sqrt{|X|})$ group operations and stores $O(\sqrt{|X|})$ group elements.

Once we have expressed X as a direct product of cyclic invariant factors we can list easily all its elements, in $O(|X|)$ time.

In our case $X = U(\Gamma)/\psi(U(\mathbb{Z}G))$. Now, we know a set V of generators of $U(\Gamma)$ (they can be computed in Sage - for example - for each Γ_i using the function *UnitGroup* [22, p. 263]). We define the product of two elements $a, b \in U(\Gamma)$ as their ordinary product in Γ. We define the inverse of an

element $a \in U(\Gamma)$ as its ordinary inverse in Γ. Finally, we decree two elements a and b to be equal whenever they are congruent modulo $\psi(U(\mathbb{Z}G))$. To test if two elements of $U(\Gamma)$ are congruent modulo $\psi(U(\mathbb{Z}G))$ we must divide a by b and the result must be in $\psi(U(\mathbb{Z}G))$; but this is equivalent to say that a/b lies in $\psi(\mathbb{Z}G)$, i.e. that $\psi^{-1}(a/b) \in \mathbb{Z}G$, since both a and b are units of Γ, and thus a/b is a unit of Γ lying in $\psi(\mathbb{Z}G)$.

Buchmann's seminal algorithm was improved (among the others) by Teske [23] and, later on, by Buchmann and Schmidt [9].

6.3. A bound on $|U(\Gamma):\psi(U(\mathbb{Z}G))|$

As far as it concerns $|U(\Gamma) : \psi(U(\mathbb{Z}G))|$, we have the following estimate which the first author proved in [1]:

Theorem 6.1. *Let G be a finite abelian group of order n. If a_q stands for the number of cyclic subgroups of order q of G, then*

$$|U(\Gamma) : \psi(U(\mathbb{Z}G))| < n^n \left(\prod_{q \mid n} \left(\frac{q^{\varphi(q)}}{\prod_{\substack{p \mid q \\ p \text{ prime}}} p^{\varphi(q)/(p-1)}} \right)^{a_q} \right)^{-1}. \qquad (6.1)$$

In particular, in [1] this bound is computed explicitly when G is an elementary abelian p-group, and when G is a cyclic group of order p^n, with p prime.

7. Computation of the Unit Group of the Cyclotomic Fields $\mathbb{Q}(\zeta_{q_i})$

A crucial and time consuming part of our algorithm consists in the computation of the unit group of the cyclotomic fields $\mathbb{Q}(\zeta_{q_i})$ $(i = 1, ..., k)$. By Dirichlet's unit theorem the unit group of $\mathbb{Q}(\zeta_n)$ is equal to the product

of a free abelian group of rank $\frac{\varphi(n)}{2} - 1$ times the group of n-th roots of unity in the field. Although there are several general purpose algorithms to compute the unit group of an arbitrary number field, they are applicable in practice only to fields $\mathbb{Q}(\zeta_n)$ with $n < 20$.

7.1. The prime power case

When n is a prime power p^m, much more can be said. Let

$$\xi_a = \zeta_n^{\frac{1-a}{2}} \frac{1-\zeta_n^a}{1-\zeta_n},$$

where $1 < a < n/2$ and $\gcd(a, p) = 1$. Let U_n be the group generated by -1, ζ_n and all the ξ_a. Then U_n turns out to be exactly the unit group of $\mathbb{Q}(\zeta_n)$ if $\varphi(n) < 66$, and, moreover, if one assumes the Generalized Riemann Hypothesis, U_n turns out to be exactly the unit group even for all the values of n such that $\varphi(n) < 162$ (refer to [13, Section 2.4.1] for the missing details). In practice when n is a prime power and $\varphi(n) < 162$ a set of generators of the unit group of $\mathbb{Q}(\zeta_n)$ is known.

7.2. The remaining case

When n is not a prime power, Faccin et al. [13, Section 2.4.2] showed that the task can be accomplished with some effort by combining an algorithm of Greither [14] to compute a subgroup E of finite index of the unit group of the maximal real subfield $\mathbb{Q}(\zeta_n)^+$ of $\mathbb{Q}(\zeta_n)$, with an algorithm due to Fieker [7, Section 5.3] to enlarge a subgroup of finite index of the unit group of $\mathbb{Q}(\zeta_n)$ incrementally until the full unit group is obtained. By exploiting these ideas, Faccin et al. [13, Section 2.4.2] where able to compute the generators of the unit group of $\mathbb{Q}(\zeta_n)$ for all $n < 130$; the correctness of their computations depends again upon the assumption of the Generalized Riemann Hypothesis.

8. Principal Ideal Testing in the Cyclotomic Fields $\mathbb{Q}(\zeta_{q_i})$

The other crucial and time consuming part of our algorithm consists in determining whether the ideals J_i of the cyclotomic fields $\mathbb{Q}(\zeta_{q_i})$ $(i = 1, ..., k)$ are principal, and, if this is true, in determining a generator d_i of J_i. This problem, which is known in the literature as the Principal Ideal Problem (PIP), is generally thought to be a quite hard one for arbitrary number fields, and indeed some recent cryptographic schemes rely upon its difficulty. However, in the recent years a lot of progress has been made concerning the algorithmic solution of this problem, especially in the case of the cyclotomic fields, which is of our interest. We state here some recent results.

8.1. The *L*-notation

Let us introduce first the *L*-notation, which is widely used when analyzing the complexity of these algorithms. Given two constants a and c with $a \in [0, 1]$ and $c \geq 0$ we define

$$L_{|\Delta_K|}(a, c) = e^{(c+o(1))(\log|\Delta_K|)^a(\log\log|\Delta_K|)^{1-a}},$$

where $o(1)$ tends to 0 as the discriminant $|\Delta_K|$ of the number field tends to infinity. When the parameter c is superfluous, we denote by $L_{|\Delta_K|}(a)$ the quantity $L_{|\Delta_K|}(a, O(1))$.

8.2. The contribution of Biasse and Fieker

The first sub-exponential time algorithm for computing the class group of a number field of arbitrary degree is due to Biasse and Fieker [6]. By combining this algorithm with Algorithm n. 7 described in [8] one obtains an algorithm to solve the Principal Ideal Problem in sub-exponential time in arbitrary classes of number fields. In particular, for a prime power cyclotomic field K of degree N the Biasse-Fieker algorithm requires time

$L_{|\Delta_K|}(2/3+\varepsilon)$ $(\approx 2^{N^{2/3+o(1)}})$, with $\varepsilon > 0$ arbitrarily small. Here Δ_K denotes the discriminant of K.

8.3. The state of the art

More recently, in [5], Biasse et al. devised an algorithm to solve the Principal Ideal Problem in a prime power cyclotomic field K of degree N in sub-exponential time $L_{|\Delta_K|}(1/2)$ $(\approx 2^{N^{1/2+o(1)}})$. To our knowledge this is the fastest algorithm up to date.

9. Some Worked Out Examples

We computed the following examples with the aid of the public domain computer algebra system SAGE [21].

Example 9.1. Consider the polynomial $x^{12} + 8 * x^{11} - 837 * x^{10} - 98016 * x^9 - 9093374 * x^8 + 971323080 * x^7 + 88039800038 * x^6 + 3042444275430 * x^5 + 67073014243125 * x^4 - 3252703653719588 * x^3 - 94326521098073965 * x^2 + 3079043710339656342 * x + 7564167843561531059$. The discriminant of its splitting field L is 205924456521. A generator of a normal integral basis exists in this case, and its minimal polynomial is $x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$, which 'resembles' the 13-th cyclotomic polynomial $x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Example 9.2. Consider the polynomial $x^8 + 20 * x^7 + 800 * x^6 + 12485 * x^5 + 235045 * x^4 + 2387800 * x^3 + 24032600 * x^2 - 34407800 * x + 62712400$. The discriminant of its splitting field L is 1265625. A generator of a normal integral basis exists in this case, and its minimal polynomial is $x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$, which 'resembles' the 15-th cyclotomic polynomial $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.

Acknowledgement

The authors thank the anonymous referees for their valuable suggestions which led to the improvement of the manuscript.

References

[1] V. Acciaro, On the index of the group of units of the integral group ring of finite abelian groups, JP Journal of Algebra, Number Theory and Applications 36(3) (2015), 201-213.

[2] V. Acciaro and L. Cangelmi, A simple algorithm to find normal integral bases of abelian number fields of exponent 2, 3, 4 and 6, JP Journal of Algebra, Number Theory and Applications 18(1) (2010), 49-65.

[3] V. Acciaro and C. Fieker, Finding normal integral bases of cyclic number fields of prime degree, J. Symbolic Comput. 30(2) (2000), 129-136.

[4] V. Acciaro and J. Klüners, Computing automorphisms of abelian number fields, Math. Comp. 68(227) (1999), 1179-1186.

[5] J. F. Biasse, T. Espitau, P. A. Fouque, A. Gelin and P. Kirchner, Computing generator in cyclotomic integer rings, EUROCRYPT 2017, Springer-Verlag, 2017, pp. 60-88.

[6] J. F. Biasse and C. Fieker, Subexponential class group and unit group computation in large degree number fields, LMS Journal of Computation and Mathematics 17(A) (2014), 385-403.

[7] J. F. Biasse and C. Fieker, Improved techniques for computing the ideal class group and a system of fundamental units in number fields, Proceedings of ANTS, 2012.

[8] J. F. Biasse, Subexponential time relations in the class group of large degree number fields, Advances in Mathematics of Communications 8(4) (2014), 407-425.

[9] J. Buchmann and A. Schmidt, Computing the structure of a finite abelian group, Math. Comp. 74(252) (2005), 2017-2026.

[10] J. Buchmann, M. J. Jacobson, Jr. and E. Teske, On some computational problems in finite abelian groups, Math. Comp. 66(220) (1997), 1663-1687.

[11] A. L. Chistov, The complexity of constructing the ring of integers of a global field, Soviet Math. Dokl. (English translation) (1989), 597-600.

[12] H. Cohen, A course in computational algebraic number theory, Graduate Texts in Mathematics 138, 3rd corr. print., Springer, Berlin, 1996.

[13] P. Faccin, W. A. De Graaf and W. Plesken, Computing generators of the unit group of an integral abelian group ring, J. of Algebra 373 (2013), 441-452.

[14] C. Greither, Improving Ramachandra's and Levesque's unit index, CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 111-120.

[15] G. Higman, The units of group rings, Proceedings of the London Mathematical Society (2) 46 (1940), 231-248.

[16] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd ed., Springer, Berlin, 2004.

[17] S. Perlis and G. Walker, Abelian group algebras of finite order, Trans. Amer. Math. Soc. 68 (1950), 420-426.

[18] M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory, Encyclopedia of Mathematics and its Applications, 30, Cambridge University Press, Cambridge, 1989.

[19] C. Polcino Milies and S. K. Sehgal, An introduction to group rings, Algebras and Applications, Vol. I, Kluwer Academic Publisher, Dordrecht, 2002.

[20] J. J. Rotman, Advanced modern algebra, 3rd ed., Part II, Graduate Studies in Mathematics 180, AMS, 2017.

[21] W. A. Stein et al., Sage Mathematics Software (Version 8.2), The Sage Development Team, 2018, http://www.sagemath.org.

[22] W. A. Stein et al., Sage Reference Manual: Algebraic Numbers and Number Fields, Release 8.2, The Sage Development Team, 2018. http://doc.sagemath.org/pdf/en/reference/number fields/number fields.pdf.

[23] E. Teske, A space efficient algorithm for group structure computation, Math. Comp. 67(224) (1998), 1637-1663.

Vincenzo Acciaro: v.acciaro@unich.it

Diana Savin: savin.diana@univ-ovidius.ro
dianet72@yahoo.com