AAECC 1, 125–134 (1990)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Canonical Bases for Cyclotomic Fields*

Wieb Bosma

Department of Pure Mathematics, University of Sydney, Sydney, NSW 2006, Australia

Abstract. It is shown how the use of a certain integral basis for cyclotomic fields enables one to perform the basic operations in their ring of integers efficiently. In particular, from the representation with respect to this basis, one obtains immediately the smallest possible cyclotomic field in which a given sum of roots of unity lies. This is of particular interest when computing with the ordinary representations of a finite group.

Keywords: Cyclotomic fields, Roots of unity

1. Introduction

The objective of this paper is to lay the foundations for efficient computation in cyclotomic fields. In particular, we show that the fundamental operations in a cyclotomic field can be performed very efficiently by the use of a certain integral basis.

The need for fast arithmetic in (rings of integers of) cyclotomic number fields arises in the context of the representation theory of finite groups. Extensive calculations in cyclotomic fields occur in applications of character and representation theory, for instance in physics (see [5]), and in the construction of discrete Fourier transforms (see [1–3]).

If G is a finite group with exponent e, then the matrices corresponding to the ordinary (complex) representations of G have their coefficients in $\mathbf{Q}(\zeta_e)$, where ζ_e denotes a primitive e-th root of unity. In practice, a particular representation of G may lie in a small subfield $\mathbf{Q}(\zeta_d)$ of $\mathbf{Q}(\zeta_e)$. As the cost of computing in $\mathbf{Q}(\zeta_d)$ will be directly proportional to d, it is highly desirable to work always in the smallest possible cyclotomic field. Therefore, it is desirable to be able to identify quickly the smallest cyclotomic field in which a given sum of roots of unity lies.

* 1980 Mathematics subject classification (1985): 11R, 11Y

The solution involves constructing an integral basis for $\mathbf{Q}(\zeta_n)$ having the property that it contains an integral basis of $\mathbf{Q}(\zeta_d)$ for every divisor d of n. Given the representation of an element γ with respect to this particular basis, one can immediately recognize the smallest cyclotomic subfield to which it belongs.

It seems that only the problem of recognizing whether γ is rational has been treated explicitly in the literature. For this the choice of a $\mathbf{Q}$-vector space basis, or equivalently, of an integral basis, suffices (see Sect. 4).

Note that our problem is not that of determining the smallest field whatsoever in which a given sum of roots of unity lies; this can be solved by applying some elementary Galois theory: determine the invariant field under the stabilizer in the Galois group of the given element. We are interested in the smallest *cyclotomic* field containing the given element, and an advantage of our approach over the general method is that our special integral basis for the cyclotomic field will solve the problem for *any* of its elements.

Although we do not claim that the results we describe are particularly novel, they do not seem to be generally known. They have been implemented in the character module of the Cayley system for computational algebra.

Section 2 contains basic definitions and results concerning roots of unity. In Sect. 3 we review results about linear relations between roots of unity. These are applied in Sect. 4 in the construction of integral bases consisting of powers of a primitive root of unity. The use of such a basis solves the problem of recognizing rational elements in cyclotomic fields. Finally, in Sect. 5, we construct integral bases that contain a basis for every cyclotomic subfield.

2. Roots of Unity

In this section we quote some basic properties about roots of unity, and we fix the notation. For proofs the reader may consult [8]. Throughout this paper p will denote a prime number.

Let n be a positive integer and let K be a field. An element ζ of K satisfying $\zeta^n=1$ is called an *n-th root of unity*; it is called a *primitive n-th root of unity* if it is not a d-th root of unity for any d smaller than n. The symbol ζ_n will denote a primitive n-th root of unity.

From now on we will assume that K has characteristic 0. The minimal polynomial of ζ_n over $\mathbf{Q}$ is the cyclotomic polynomial Φ_n. The degree of Φ_n is $\phi(n)$, the value of Euler's function ϕ, so that the degree of the cyclotomic field $\mathbf{Q}(\zeta_n)$ is also $\phi(n)$. Over $\mathbf{Z}$ we have

$$X^n-1=\prod_{d|n}\Phi_d(X).$$

The ring of integers of $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$.

The relation between the cyclotomic fields of different degrees is very transparent. If d divides n then $\mathbf{Q}(\zeta_d)\subset\mathbf{Q}(\zeta_n)$; if on the other hand m and n are coprime, then $\mathbf{Q}(\zeta_m)\cap\mathbf{Q}(\zeta_n)=\mathbf{Q}$ and $\mathbf{Q}(\zeta_m,\zeta_n)=\mathbf{Q}(\zeta_{mn})$. As a consequence, $\mathbf{Q}(\zeta_m,\zeta_n)=\mathbf{Q}(\zeta_{\mathrm{lcm}(m,n)})$, and $\mathbf{Q}(\zeta_m)\cap\mathbf{Q}(\zeta_n)=\mathbf{Q}(\zeta_{\mathrm{gcd}(m,n)})$, for arbitrary positive integers m and n. Hence it often suffices to consider the fields $\mathbf{Q}(\zeta_{p^k})$.

One minor complication should be noted: since $\mathbf{Q}$ itself contains the second roots of unity, $\mathbf{Q}(\zeta_{2k})=\mathbf{Q}(\zeta_k)$ for every odd k. Indeed, $-\zeta_k$ is a primitive $2k$-th root of unity. Since $\mathbf{Q}(\zeta_n)=\mathbf{Q}\left(\zeta_{\frac{n}{2}}\right)$ for $n\equiv 2\bmod 4$, we may restrict ourselves to integers $n\not\equiv 2\bmod 4$. As a consequence, 4 rather than 2 will appear to be the "even prime".

2.1. Definitions. A *modified squarefree integer* is an integer m that is

(i) not divisible by the square of an odd prime, and that is

(ii) either odd or congruent to $4 \bmod 8$.

Hence either m is odd, or it is exactly divisible by 2^2 with the odd part of m squarefree.

From now on p^* will denote a *modified prime number*, that is, $p^* = p$ if p is odd and $p^* = 4$ if $p = 2$.

Let $n \not\equiv 2 \bmod 4$. The *modified squarefree part* of n is

$$m = \prod_{p \mid n} p^* .$$

So the modified squarefree part of n is the product of the prime divisors of n in case n is odd, and 4 times the product of the odd prime divisors for even n, with $n \not\equiv 2 \bmod 4$. Also, n is modified squarefree if and only if it equals its modified squarefree part.

2.2. Example. For motivation, we give an example of a cyclotomic integer that is in fact rational. Let $\alpha \in \mathbf{Z}[\zeta_{30}]$ be defined by

$$\alpha = 1 + \zeta_{30} + \zeta_{30}^{7} + \zeta_{30}^{13} + \zeta_{30}^{19} + \zeta_{30}^{20} .$$

We try to rewrite α. First of all, $n = 30 \equiv 2 \bmod 4$, so we reduce to $\mathbf{Z}[\zeta_{15}]$. Using $\zeta_{30} = -\zeta_{15}$, we find

$$\begin{aligned} \alpha &= 1 - \zeta_{15} - \zeta_{15}^{7} - \zeta_{15}^{13} - \zeta_{15}^{19} + \zeta_{15}^{20} \\ &= 1 - \zeta_{15}(1 + \zeta_{15}^{6} + \zeta_{15}^{12} + \zeta_{15}^{3}) + \zeta_{15}^{5} \\ &= 1 - \zeta_{15}(1 + \zeta_{5}^{2} + \zeta_{5}^{4} + \zeta_{5}^{1}) + \zeta_{15}^{5} . \end{aligned}$$

We have also used the fact that ζ_{15}^{3} is a primitive fifth root of unity. As is well known, the sum of all fifth roots of unity equals zero, and the same holds for the third roots of unity (see also Sect. 3 below); hence

$$\alpha = 1 - \zeta_{15}(-\zeta_{5}^{3}) + \zeta_{15}^{5} = 1 + \zeta_{15}^{10} + \zeta_{15}^{5} = 1 + \zeta_{3}^{2} + \zeta_{3} = 0 .$$

This shows that $\alpha = 0$, which is not obvious at first sight. For computational purposes it is obviously highly desirable to recognize this immediately.

2.3. Remark. We have chosen $\zeta_5 = \zeta_{15}^{3}$ and $\zeta_3 = \zeta_{15}^{5}$ in (2.2). One should be aware that this really involves a choice for a particular primitive fifth, respectively third root of unity, and is not due to an intrinsic relation. Sometimes it is convenient to choose primitive fifth and third roots of unity in such a way that $\zeta_{15} = \zeta_3 \zeta_5$; then clearly $\zeta_3 = \zeta_{15}^{10}$ and $\zeta_5 = \zeta_{15}^{6}$. Nowhere in this paper do we assume anything about the embedding of cyclotomic fields in the field of complex numbers.

3. Linear Relations

Linear relations between roots of unity basically all derive from the fact that the sum of all p-th roots of unity is zero:

$$1 + \zeta_p + \ldots + \zeta_p^{p-1} = 0 \tag{3.1}$$

for every prime p. In fact, (3.1) is easily seen to be true for every positive integer p, as we sum over all roots of polynomial $X^p - 1$ (in some algebraic closure of $\mathbf{Q}$).

The symbol W_n will denote the set of all n-th roots of unity, i.e.,

$$W_n = \{\zeta_n^i, 0 \leqq i < n\}.$$

The following theorems have been adapted from [6].

3.2. Theorem. *Let $n \not\equiv 2 \bmod 4$ and let m be the modified squarefree part of n. Then:*

$$\left\{\zeta_m^a \zeta_n^b : 0 \leqq a < m \textit{ and } 0 \leqq b < \frac{n}{m}\right\} = W_n.$$

Furthermore, if $z_{ij} \in \mathbf{Z}$, then:

$$\sum_{j=0}^{\frac{n}{m}-1} \sum_{i=0}^{m-1} z_{ij}\zeta_m^i \zeta_n^j = 0 \Leftrightarrow \sum_{i=0}^{m-1} z_{ij}\zeta_m^i = 0 \quad \textit{for} \quad 0 \leqq j < \frac{n}{m}.$$

Proof. Let $\zeta_n^h \in W_n$; choosing $b \equiv h \bmod \frac{n}{m}$ and a such that $h \equiv a\frac{n}{m} + b \bmod n$, proves the first assertion.

For the second, observe that

$$X^n - 1 = \prod_{i=0}^{m-1} \left(X^{\frac{n}{m}} - \zeta_m^i\right)$$

in $\mathbf{Q}(\zeta_m)$. Now ζ_n is a zero of one of the factors, say $X^{\frac{n}{m}} - \zeta_m^j$; this factor must be irreducible, because its degree is given by

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}(\zeta_m)] = \frac{[\mathbf{Q}(\zeta_n) : \mathbf{Q}]}{[\mathbf{Q}(\zeta_m) : \mathbf{Q}]} = \frac{\phi(n)}{\phi(m)} = \frac{n}{m}.$$

Therefore, if $b_j \in \mathbf{Q}(\zeta_m)$,

$$\sum_{j=0}^{\frac{n}{m}-1} b_j \zeta_n^j = 0 \quad \Rightarrow \quad b_j = 0 \quad \text{for} \quad 0 \leqq j < \frac{n}{m}.$$

That proves (3.2).

3.3. Remarks. Let $n = p^k$ be the power of an odd prime p. The first assertion of (3.2) states that all p^k-th roots of unity can be represented in the form $\zeta_p^a \zeta_{p^k}^b$, with $0 \leqq a < p$ and $0 \leqq b < p^{k-1}$.

If we use this representation, any $\mathbf{Z}$-linear combination of p^k-th roots of unity can be written as an element of $\mathbf{Z}[\zeta_{p^k}]$ with coefficients in $\mathbf{Z}[\zeta_p]$:

$$\sum_{i=0}^{p^{k-1}-1} \left(\sum_{i=0}^{p-1} z_{ij}\zeta_p^i\right) \zeta_{p^k}^j.$$

Now the second part of (3.2) asserts that such a sum is zero if and only if all the coefficients are zero in $\mathbf{Z}[\zeta_p]$.

If $n = 2^k$, with $k \geqq 2$, all n-th roots of unity can be written as $\zeta_4^a \zeta_{2^k}^b$, with $0 \leqq a < 4$ and $0 \leqq b < 2^{k-2}$. A $\mathbf{Z}$-linear combination of 2^k-th roots of unity is zero if and only if its coefficients in $\mathbf{Z}[\zeta_4]$ in the above representation are all zero.

In general, (3.2) reduces the problem of deciding whether a given element of $\mathbf{Z}[\zeta_n]$ is zero, to the same question for elements in $\mathbf{Z}[\zeta_m]$, where m is the modified squarefree part of n. Theorem (3.4) deals with this case.

3.4. Theorem. *Let $n \not\equiv 2 \bmod 4$, and suppose that $n = p^*r$, with p a prime divisor of n and r not divisible by p. Then:*

$$\{\zeta_{p^*}^a \zeta_r^b : 0 \leqq a < p^* \text{ and } 0 \leqq b < r\} = W_n .$$

Furthermore, if $z_{ij} \in \mathbf{Z}$, the following hold. If p is odd:

$$\sum_{j=0}^{p^*-1} \sum_{i=0}^{r-1} z_{ij} \zeta_r^i \zeta_{p^*}^j = 0 \Leftrightarrow \sum_{i=0}^{r-1} z_{ij} \zeta_r^i = \sum_{i=0}^{r-1} z_{i0} \zeta_r^i \quad \text{for} \quad 1 \leqq j < p^* .$$

If $p = 2$, so that $p^* = 4$, then:

$$\sum_{j=0}^{p^*-1} \sum_{i=0}^{r-1} z_{ij} \zeta_r^i \zeta_{p^*}^j = 0 \Leftrightarrow \sum_{i=0}^{r-1} z_{i2} \zeta_r^i = \sum_{i=0}^{r-1} z_{i0} \zeta_r^i \quad \text{and} \quad \sum_{i=0}^{r-1} z_{i3} \zeta_r^i = \sum_{i=0}^{r-1} z_{i1} \zeta_r^i .$$

Proof. The proof is much the same as that of (3.2); this time we use the fact that the p^*-th cyclotomic polynomial Φ_{p^*} is irreducible over $\mathbf{Q}(\zeta_r)$ together with (3.1).

3.5. Remarks. Continuing the discussion of (3.3), suppose now that $n = p$, an odd prime. Then (3.4) merely asserts (with $r = 1$) that a $\mathbf{Z}$-linear combination of p-th roots of unity

$$\sum_{j=0}^{p-1} z_j \zeta_p^j$$

is zero, only when all coefficients z_j are equal. Hence (3.1) is, up to scalar multiplication, the only non-trivial linear relation between p-th roots of unity, and together with the remarks made in (3.3) this determines all linear relations between p^k-th roots of unity.

For $n = 4$ the "primitive relation" over $\mathbf{Z}$ is $\zeta_4^2 + \zeta_4^0 = 0$, from which $\zeta_4^3 + \zeta_4 = 0$ follows.

More generally, (3.4) implies that for a modified squarefree integer m, any $\mathbf{Z}$-linear combination of m-th roots of unity can be written as an element of $\mathbf{Z}[\zeta_{p^*}]$ with coefficients in $\mathbf{Z}\left[\zeta_{\frac{m}{p^*}}\right]$, for any modified prime divisor p^* of m. The second assertion of (3.4) states that such a sum can only be zero if all its coefficients in $\mathbf{Z}\left[\zeta_{\frac{m}{p^*}}\right]$ are equal.

3.6. Corollary. *Let n be a positive integer, $n \not\equiv 2 \bmod 4$, with modified squarefree part m. For every prime p dividing n, let the set A_p consist of p^* integers from distinct residue classes modulo p^*, and let B_n consist of $\frac{n}{m}$ integers from distinct residue classes modulo $\frac{n}{m}$. Then*

$$\left\{\left(\prod_{p|n} \zeta_{p^*}^a\right) \zeta_n^b : a \in A_p, \text{ and } b \in B_n\right\} = W_n .$$

Proof. Immediate from (3.2) and (3.4).

4. Integral Bases

An easy test for equality in $\mathbf{Q}(\zeta_n)$, or any of its cyclotomic subfields, follows immediately from (3.2) and (3.4). However, that does not suffice to solve the problem of determining whether or not a given element is contained in a proper subfield, or even to determine whether or not it is rational. However, it is now easy to describe subsets of W_n that form integral bases for $\mathbf{Q}(\zeta_n)$.

An *integral basis* for $\mathbf{Q}(\zeta_n)$ consists of $\phi(n)$ cyclotomic integers

$$\lambda_1, \lambda_2, \ldots, \lambda_{\phi(n)} \in \mathbf{Z}[\zeta_n]$$

such that every $\alpha \in \mathbf{Z}[\zeta_n]$ can be expressed uniquely in the form

$$\alpha = z_1\lambda_1 + z_2\lambda_2 + \ldots + z_{\phi(n)}\lambda_{\phi(n)}, \quad \text{with} \quad z_1, z_2, \ldots, z_{\phi(n)} \in \mathbf{Z}.$$

We study those integral bases for $\mathbf{Q}(\zeta_n)$ contained in W_n; by (3.2) these are of the form

$$I_A = I_{A(m)} = \left\{\zeta_m^a \zeta_n^b : a \in A(m),\ 0 \leqq b < \frac{n}{m}\right\} \subset W_n; \tag{4.1}$$

where $A(m) \subset \{0, 1, \ldots, m-1\}$, and m is the modified squarefree part of n. We will often simply write A for $A(m)$.

4.2. Theorem. *Let n be a positive integer, $n \not\equiv 2 \bmod 4$, with modified squarefree part m. Let $A \subset \{0, 1, \ldots, m-1\}$. If for every modified prime divisor p^* of m we have both*

$$\#\{a \bmod p^* : a \in A\} = \phi(p^*) \quad \text{and} \quad \#\{a \bmod 2 : a \in A\} = 2,$$

then the set I_A, defined by (4.1), *forms an integral basis for* $\mathbf{Q}(\zeta_n)$.

Proof. First note that the set A has the correct cardinality: by the Chinese remainder theorem it consists of

$$\prod_{p \mid m} \phi(p^*) = \phi(m)$$

elements. Therefore I_A has $\phi(m)\frac{n}{m} = \phi(n)$ elements, as required.

To show that there are no linear dependencies between elements of I_A, suppose that for $z_{ij} \in \mathbf{Z}$,

$$\sum_{j=0}^{\frac{n}{m}-1} \sum_{i \in A} z_{ij} \zeta_m^i \zeta_n^j = 0.$$

Then, by (3.2)

$$\sum_{i \in A} z_{ij} \zeta_m^i = 0 \tag{4.3}$$

for $0 \leqq j < \frac{n}{m}$. We claim that the conditions on A imply that all z_{ij} must be zero; to prove this, we apply induction on the number f of (modified) prime divisors of m.

If $f = 1$, then $m = p^*$. When p is an odd prime, it follows from (3.4) that (4.3) can only hold if all the coefficients of $\zeta_{p^*}^i$ are equal; but $\# A = \phi(p^*) = p^* - 1$, so for at least one i this coefficient is zero, hence all z_{ij} must be zero. If $p = 2$, the conditions on A imply that it contains integers in two residue classes modulo 4 that are different modulo 2. By the final assertion in (3.4) again all z_{ij} are zero.

Suppose now $f>1$. Let p^* be a modified prime divisor of m; if we write $\zeta_m = \zeta_{\frac{m}{p^*}}\zeta_{p^*}$, then (4.3) can be written as

$$\sum_{k=0}^{p^*-1}\left(\sum_{i\in A_{p^*}^k} z_{ij}\zeta_{\frac{m}{p^*}}^{i}\right)\zeta_{p^*}^{k}=0$$

where $A_{p^*}^k$ is the set $\{a\in A : a\equiv k \bmod p^*\}$. For at least one k the set $A_{p^*}^k$ is empty, by our hypothesis on A. Theorem (3.4) implies that for every k

$$\sum_{i\in A_{p^*}^k} z_{ij}\zeta_{\frac{m}{p^*}}^{i}=0 .$$

But $A_{p^*}^k$ is a subset of A that also satisfies the hypothesis of the theorem, while $\frac{m}{p^*}$ has $f-1$ prime divisors. By the induction hypothesis, $z_{ij}=0$ for $i\in A_{p^*}^k$. Hence this holds for every k and since A is the union of all $A_{p^*}^k$, each coefficient z_{ij} is zero.

That completes the proof of (4.2).

4.4. Corollary. *Let n be a positive integer, $n\not\equiv 2 \bmod 4$, with modified squarefree part m. For every prime p dividing n let the set A_p^* consist of $\phi(p^*)$ integers from distinct residue classes modulo p, and let B_n consist of $\frac{n}{m}$ integers from distinct residue classes modulo $\frac{n}{m}$. Then*

$$\left\{\left(\prod_{p|n}\zeta_{p^*}^{a}\right)\zeta_n^{b} : a\in A_p^*,\ \textit{and}\ b\in B_n\right\}$$

forms an integral basis for $\mathbf{Q}(\zeta_n)$.

Proof. Immediate.

4.5. Remarks. Theorem (4.2) gives a sufficient condition on A for I_A to be an integral basis, but it is not necessary. For instance, the set

$$\{\zeta_n^0, \zeta_n^1, \ldots, \zeta_n^{\phi(n)-1}\}\subset W_n$$

forms an integral basis for $\mathbf{Q}(\zeta_n)$, for arbitrary n. But $A=\{0,1,\ldots,\phi(n)-1\}$ for squarefree n with $n\not\equiv 2 \bmod 4$, so that this set contains integers in all residue classes modulo every prime divisor of n.

This is the reason why this natural choice for an integral basis of $\mathbf{Q}(\zeta_n)$ is unsuitable for our purposes.

We can always choose the first basis element to be 1 in an integral basis for $\mathbf{Q}(\zeta_n)$. Under this assumption, an element of $\mathbf{Z}[\zeta_n]$ represented with respect to an integral basis will be in $\mathbf{Z}$ if and only if all coefficients other than the first are zero. This solves the problem of recognizing the rational integers in $\mathbf{Z}[\zeta_n]$ (cf. [4, 6, 7]). The following example will elucidate this, and it also shows that the more general question has not yet been answered.

4.6. Example. Let $n=48$, so $m=12$. Let $\alpha,\beta\in\mathbf{Z}[\zeta_{48}]$ be defined by

$$\alpha=1+\zeta_{48}^{3}-\zeta_{48}^{11}+\zeta_{48}^{19}-\zeta_{48}^{23}-\zeta_{48}^{47}, \quad \text{and} \quad \beta=\zeta_{48}^{13}+\zeta_{48}^{29}.$$

First write $\zeta_{48}^i = \zeta_4^r \zeta_3^s \zeta_{48}^t$, for any i, with $0 \leqq r < 4$, $0 \leqq s < 3$, and $0 \leqq t < 4$ $(= n/m)$, as in (3.6). Thus:

$$1 = \zeta_4^0 \zeta_3^0 \zeta_{48}^0,$$

$$\zeta_{48}^3 = \zeta_4^0 \zeta_3^0 \zeta_{48}^3,$$

$$\zeta_{48}^{11} = \zeta_4^2 \zeta_3^2 \zeta_{48}^3,$$

$$\zeta_{48}^{13} = \zeta_4^1 \zeta_3^0 \zeta_{48}^1,$$

$$\zeta_{48}^{19} = \zeta_4^0 \zeta_3^1 \zeta_{48}^3,$$

$$\zeta_{48}^{23} = \zeta_4^3 \zeta_3^2 \zeta_{48}^3,$$

$$\zeta_{48}^{29} = \zeta_4^1 \zeta_3^1 \zeta_{48}^1,$$

and

$$\zeta_{48}^{47} = \zeta_4^1 \zeta_3^2 \zeta_{48}^3.$$

Next we express α and β relative to the integral basis defined by (4.4), taking $A_4^* = \{0, 1\}$, taking $A_3^* = \{0, 1\}$, and taking $B_{48} = \{0, 1, 2, 3\}$. Three elements in the above list are not yet written in terms of this basis, namely ζ_{48}^{11}, ζ_{48}^{23}, and ζ_{48}^{47}. For these, note that $\zeta_4^2 = -\zeta_4^0$, that $\zeta_4^3 = -\zeta_4^1$ and that $\zeta_3^2 = -\zeta_3^0 - \zeta_3^1$. Hence

$$\zeta_{48}^{11} = \zeta_4^0 \zeta_3^0 \zeta_{48}^3 + \zeta_4^0 \zeta_3^1 \zeta_{48}^3 = \zeta_{48}^3 + \zeta_{48}^{19},$$

$$\zeta_{48}^{23} = \zeta_4^1 \zeta_3^0 \zeta_{48}^3 + \zeta_4^1 \zeta_3^1 \zeta_{48}^3,$$

and

$$\zeta_{48}^{47} = -\zeta_4^1 \zeta_3^0 \zeta_{48}^3 - \zeta_4^1 \zeta_3^1 \zeta_{48}^3 = -\zeta_{48}^{23}.$$

From these basis representations we see

$$\alpha = 1,$$

is a rational integer, while

$$\beta = \zeta_{48}^{13} + \zeta_{48}^{29} = \zeta_4 \zeta_{48} + \zeta_4 \zeta_3 \zeta_{48},$$

is not rational.

Thus this basis provides a simple method for determining whether or not a given element is in $\mathbf{Q}$. However, noting that

$$\beta = (1 + \zeta_3)\zeta_4 \zeta_{48} = -\zeta_3^2 \zeta_4 \zeta_{48} = -\zeta_{48}^{45} = -\zeta_{16}^{15}$$

we see that β is contained in the cyclotomic subfield $\mathbf{Q}(\zeta_{16})$, which is not obvious from the above basis representation.

5. Canonical Integral Bases

Finally, we describe an integral basis for $\mathbf{Q}(\zeta_n)$ contained in W_n that contains a basis for every cyclotomic subfield. To find such a basis, it suffices to choose the set B_n in (4.4) carefully.

5.1. Theorem. *Let n be a positive integer, $n \not\equiv 2 \bmod 4$, with modified squarefree part m. For every prime p dividing n let the set A_p^* consist of $\phi(p^*)$ integers from distinct residue classes modulo p. For every maximal prime power divisor p^k of n, let the set*

$B^*_{p^k}$ consist of $\frac{p^k}{p^*}$ integers from distinct residue classes modulo $\frac{p^k}{p^*}$. Then the set

$$I=\left\{\zeta_n^i=\prod_{p^k\|n}(\zeta_{p^*}^a\zeta_{p^k}^b):a\in A_p^*,\ \textit{and}\ b\in B^*_{p^k}\right\} \tag{5.2}$$

forms a basis for $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$.

Moreover, for every divisor d of n, the set

$$I_d=\{\zeta_n^i\in I:\zeta_n^i\in\mathbf{Q}(\zeta_d)\}$$

forms an integral basis for $\mathbf{Q}(\zeta_d)$.

Proof. The fact that I forms of an integral basis for $\mathbf{Q}(\zeta_n)$ is an immediate consequence of Corollary (4.4).

To see that I contains a basis for every cyclotomic subfield, recall that $\mathbf{Q}(\zeta_d)$ $\cap\mathbf{Q}(\zeta_e)=\mathbf{Q}$ for coprime d and e. Thus it suffices to prove the assertion for the case where n is a prime power p^k. If $n=p^*$, the assertion is trivial. If $n\neq p^*$, note that for every j the set $B^*_{p^{j+1}}$ contains integers pb_i, where the b_i constitute a set of the form $B^*_{p^j}$. Since $\zeta_{p^k}^p\in\mathbf{Q}(\zeta_{p^{k-1}})$, induction completes the proof.

5.3. *Remarks.* We define the *canonical basis* for $\mathbf{Q}(\zeta_n)$ to be the basis I arising from (5.1) by making the obvious choices $A_p^*=\{0,1,\ldots,p-2\}$ and

$$B^*_{p^k}=\left\{0,1,\ldots,\frac{p^k}{p^*}-1\right\}.$$

As an explicit subset of W_n,

$$I=\left\{\zeta_n^i=\left(\prod_{p^k\|n}\zeta_n^{a\frac{n}{p^*}}\right)\zeta_n^b:a\in A_p^*,\ \text{and}\ b\in B_n^*\right\}$$

where we define B_n^* to be the set of $\frac{n}{m}$ integers

$$\sum_{p^k\|n}\frac{n}{p^k}c_p,$$

for all different choices of integers $0\leq c_p<\frac{p^k}{p^*}$.

By writing ζ_n^i in its lowest form, we mean replacing ζ_n^i by

$$\begin{cases}\zeta_k^j,\ \text{with}\ j=\dfrac{i}{\gcd(n,i)}\ \text{and}\ k=\dfrac{n}{\gcd(n,i)} & \text{if this}\ k\neq 2\bmod 4,\\[2ex] -\zeta_k^j,\ \text{with}\ j=\dfrac{i}{\gcd(n,i)}\ \text{and}\ k=\dfrac{n}{2\cdot\gcd(n,i)} & \text{otherwise}.\end{cases}$$

Since $\gcd(j,k)=1$ and $k\neq 2\bmod 4$, the field $\mathbf{Q}(\zeta_k)$ is the smallest cyclotomic field containing ζ_n^i. For example, writing ζ_{48}^6 and ζ_{48}^8 in their lowest form, we get ζ_8 and $-\zeta_3$, respectively.

We can find the smallest subfield containing an element γ of $\mathbf{Q}(\zeta_n)$ as follows.

If we represent the element γ with respect to the basis for $\mathbf{Q}(\zeta_n)$ given in Theorem (5.1), then the smallest cyclotomic field containing γ is the subfield generated by the basis elements which have non-zero coefficients in the representation. This is the field $\mathbf{Q}(\zeta_d)$, where d is the least common multiple of those integers k for which ζ_k^j, written in its lowest form, has non-zero coefficient.

We illustrate this procedure with the example discussed in (4.6).

5.4. Example. According to Theorem (5.1) and Remark (5.3), the elements $\zeta_4^r\zeta_3^s\zeta_{48}^t$ will constitute the canonical basis for $\mathbf{Q}(\zeta_{48})$ if we choose $r \in A_4^* = \{0,1\}$, $s \in A_3^* = \{0,1\}$, and $t \in B_{48}^* = \{0,3,6,9\}$. Then the set $I \subset W_{48}$ is

$$\{\zeta_{48}^0, \zeta_{48}^3, \zeta_{48}^6, \zeta_{48}^9, \zeta_{48}^{12}, \zeta_{48}^{15}, \zeta_{48}^{16}, \zeta_{48}^{18}, \zeta_{48}^{19}, \zeta_{48}^{21}, \zeta_{48}^{22}, \zeta_{48}^{25}, \zeta_{48}^{28}, \zeta_{48}^{31}, \zeta_{48}^{34}, \zeta_{48}^{37}\},$$

which, after rewriting the elements in lowest forms, yields the set

$$\{1, \zeta_{16}, \zeta_8, \zeta_{16}^3, \zeta_4, \zeta_{16}^5, \zeta_3, \zeta_8^3, \zeta_{48}^{19}, \zeta_{16}^7, \zeta_{24}^{11}, \zeta_{48}^{25}, \zeta_{12}^7, \zeta_{48}^{31}, \zeta_{24}^{17}, \zeta_{48}^{37}\}.$$

The lattice of cyclotomic subfields of $\mathbf{Q}(\zeta_{48})$ and that of the corresponding integral bases is displayed in Fig. 1.

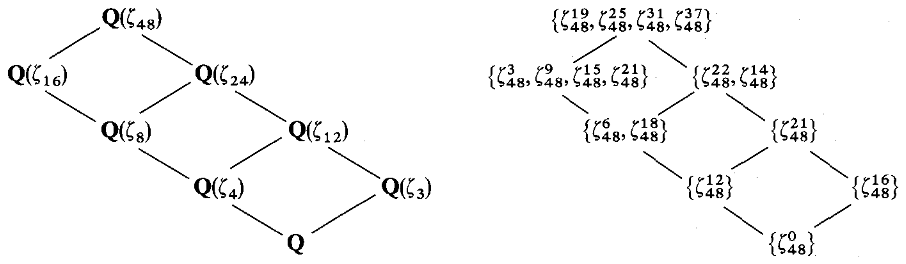

Fig. 1

Looking at the representation of the element $\beta = \zeta_{48}^{13} + \zeta_{48}^{29}$ relative to this basis, and proceeding as before, we find

$$\zeta_{48}^{13} = -\zeta_4^1\zeta_3^1\zeta_{48}^9 = -\zeta_{48}^{37}$$

and

$$\zeta_{48}^{29} = \zeta_4^1\zeta_3^0\zeta_{48}^9 + \zeta_4^1\zeta_3^1\zeta_{48}^9 = \zeta_{48}^{21} + \zeta_{48}^{37};$$

thus $\beta = \zeta_{48}^{13} + \zeta_{48}^{29} = \zeta_{48}^{21} = \zeta_{16}^7 \in \mathbf{Q}(\zeta_{16})$.

Acknowledgement. This research was supported by the Australian Research Council (Grants A68830699 and A68930041).

References

1. Clausen, M.: Fast Fourier transforms for metabelian groups. SIAM J. Comput. (to appear)
2. Clausen, M.: Fast generalized Fourier transforms. Theoret. Comput. Sci. (to appear)
3. Clausen, M., Gollmann, D.: Spectral transforms for symmetric groups – fast algorithms and VLSI architectures. To appear in: Proceedings of the Third International Workshop on Spectral Techniques, Universität Dortmund
4. Conway, J.H., Jones, A.J.: Trigonometric diophantine equations (On vanishing sums of roots of unity). Acta Arith. **30**, 229–240 (1976)
5. Jansen, L., Boon, M.: Theory of finite groups. Applications in physics. Amsterdam: North-Holland 1967
6. Lenstra, H.W., Jr.: Vanishing sums of roots of unity. In: Proc. Bicentennial Congres Wiskundig Genootschap, Part II, Math. Centre Tracts, Vol. 101, Amsterdam: Mathematical Centre 1979
7. Mann, H.B.: On linear relations between roots of unity. Mathematika **12**, 107–117 (1965)
8. Washington, L.: Cyclotomic fields. Berlin, Heidelberg, New York: Springer 1982

Received June 8, 1990; revised version August 16, 1990