BULL. AUSTRAL. MATH. SOC. 11R04
VOL. 71 (2005) [167–173]

POWER INTEGRAL BASES FOR REAL CYCLOTOMIC FIELDS

LAUREL MILLER-SIMS AND LEANNE ROBERTSON

We consider the problem of determining all power integral bases for the maximal real subfield $\mathbf{Q}(\zeta+\zeta^{-1})$ of the p-th cyclotomic field $\mathbf{Q}(\zeta)$, where $p \geqslant 5$ is prime and ζ is a primitive p-th root of unity. The ring of integers is $\mathbf{Z}[\zeta+\zeta^{-1}]$ so a power integral basis always exists, and there are further non-obvious generators for the ring. Specifically, we prove that

$$\mathbf{Z}[\alpha] = \mathbf{Z}[\zeta+\zeta^{-1}]$$

if

$$\alpha = \zeta+\zeta^{-1}, 1/(\zeta+\zeta^{-1}), 1/(\zeta+\zeta^{-1}+1), 1/(\zeta+\zeta^{-1}-1), 1/(\zeta+\zeta^{-1}+2),$$

or one of the Galois conjugates of these five algebraic integers. Up to integer translation and multiplication by -1, there are no additional generators for $p \leqslant 11$, and it is plausible that there are no additional generators for $p > 13$ as well. For $p = 13$ there is an additional generator, but we show that it does not generalise to an additional generator for $13 < p < 1000$.

A number field K is said to have a *power integral basis* if its ring of integers $\mathcal{O}_K$ is of the form $\mathbf{Z}[\alpha]$ for some α in the ring. The set of generators is stable under integer translation and multiplication by -1; we call α and α' *equivalent* if $\alpha' = n \pm \alpha$ for some $n \in \mathbf{Z}$. Győry [7] proved that up to equivalence there are only finitely many elements that generate a power basis for any number field K. Most number fields do not have a power integral basis, however, and when one does exist it is usually very difficult to determine all the generators. See Gaál [3] for results on the existence and computation of power integral bases for fields of small degree over $\mathbf{Q}$, and for algorithms for determining power integral bases.

Cyclotomic fields are an interesting case because power integral bases always exist and in some cases we can find all the generators (see Nagell [9], Bremner [1], and Robertson [10, 11]). Real cyclotomic fields (that is, the maximal real subfields of cyclotomic fields) are also interesting because again power integral bases always exist.

Let $p \geqslant 5$ be prime and ζ be a primitive p-th root of unity. Then it is well known that $\mathbf{Z}[\zeta+\zeta^{-1}]$ is the ring of integers of the real cyclotomic field $\mathbf{Q}(\zeta+\zeta^{-1})$. The problem

Received 4th October, 2004

of determining all power integral bases for these fields has not previously been studied, although it has been known since Gras [6] that real cyclotomic fields of prime degree over $\mathbf{Q}$ are the only cyclic extensions of prime degree greater than 3 over $\mathbf{Q}$ that have power integral bases. Here we consider the problem of determining all power integral bases for $\mathbf{Q}(\zeta+\zeta^{-1})$, that is, of finding all α such that $\mathbf{Z}[\alpha]=\mathbf{Z}[\zeta+\zeta^{-1}]$.

If a number field has a power integral basis then the following lemma can be used to find further generators for its ring of integers.

LEMMA 1. *Suppose μ generates a power integral basis for a number field K. If μ is a unit in $\mathcal{O}_K$, then $1/\mu$ also generates a power integral basis for K.*

PROOF: The constant term of the minimal polynomial for μ is equal to ± 1, since μ is a unit. Thus there are $a_i \in \mathbf{Z}$ such that

$$\mu^n + a_{n-1}\mu^{n-1} + \cdots + a_1\mu \pm 1 = 0. \tag{1}$$

Multiply equation (1) by $1/\mu$ to see that $1/\mu \in \mathbf{Z}[\mu]$. Multiply equation (1) by $(1/\mu)^{n-1}$ to see that $\mu \in \mathbf{Z}[1/\mu]$. □

This lemma is important for our work because it provides a strategy for finding new power integral bases for $\mathbf{Q}(\zeta+\zeta^{-1})$ from the known generator $\zeta+\zeta^{-1}$. Namely, for every $n \in \mathbf{Z}$, $\zeta+\zeta^{-1}+n$ is equivalent to $\zeta+\zeta^{-1}$, and so generates a power integral basis. To find further inequivalent generators we look for units of the form $\zeta+\zeta^{-1}+n$, then, by the lemma, $1/(\zeta+\zeta^{-1}+n)$ generates a power integral basis.

THEOREM 1. *The algebraic integer $\zeta+\zeta^{-1}+n$, $n \in \mathbf{Z}$, is a unit in $\mathbf{Z}[\zeta+\zeta^{-1}]$ if and only if $n \in \{0, \pm 1, 2\}$.*

PROOF: Let $g(x) \in \mathbf{Z}[x]$ be the minimal polynomial for $\zeta+\zeta^{-1}$. Then $g(x)$ factors completely in $\mathbf{Z}[\zeta+\zeta^{-1}]$ as

$$g(x) = \prod_{i=1}^{(p-1)/2} (x - \zeta^i - \zeta^{-i}).$$

Let N be the norm from $\mathbf{Q}(\zeta+\zeta^{-1})$ to $\mathbf{Q}$. Then

$$\begin{aligned} \zeta+\zeta^{-1}+n \text{ is a unit} &\iff N(-n-\zeta-\zeta^{-1}) = \pm 1 \\ &\iff \prod_{i=1}^{(p-1)/2} (-n-\zeta^i-\zeta^{-i}) = \pm 1 \\ &\iff g(-n) = \pm 1. \end{aligned}$$

Now, $g(x)$ has $(p-1)/2$ real roots all of which have absolute value is less than 2. Since the degree of $g(x)$ is also $(p-1)/2$, it follows that $g(x)$ is monotonic for $x \leqslant -2$ and $x \geqslant 2$. Thus, to prove the theorem it is sufficient to check that $g(-n) = \pm 1$ for $n = 0, \pm 1, 2$, and that $|g(-n)| > 1$ for $n = -2$.

We consider $n = 0, \pm 1, \pm 2$ separately. Since $\zeta + \zeta^{-1}$ is a unit,

$$g(0) = N(-\zeta - \zeta^{-1}) = \pm 1,$$

as needed. Now,

$$g(-1) = N(-1 - \zeta - \zeta^{-1}) = (-1)^{(p-1)/2} N(1 + \zeta^2 + \zeta^{-2}),$$

since p is odd. But $1 + \zeta^2 + \zeta^{-2} = (\zeta^3 - \zeta^{-3})/(\zeta - \zeta^{-1})$, and so is a unit since $\zeta^3 - \zeta^{-3}$ and $\zeta - \zeta^{-1}$ are associates in $\mathbf{Q}(\zeta)$. Thus $g(-1) = \pm 1$ as well. Similarly,

$$g(1) = N(1 - \zeta - \zeta^{-1}),$$

and

$$1 - \zeta - \zeta^{-1} = (-1 - \zeta^2 - \zeta^{-2})/(1 + \zeta + \zeta^{-1})$$

is a unit. Thus $g(1) = \pm 1$. Also,

$$g(-2) = N(-2 - \zeta - \zeta^{-1}) = (-1)^{(p-1)/2} N(\zeta + \zeta^{-1})^2 = \pm 1,$$

since $\zeta + \zeta^{-1}$ is a unit. Finally, $g(2) = N(2 - \zeta - \zeta^{-1})$. But $2 - \zeta - \zeta^{-1}$ lies over p in $\mathbf{Z}[\zeta + \zeta^{-1}]$. Thus, $g(2) = \pm p$ as needed to complete the proof. □

It is now immediate from Lemma 1 that

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} + 1}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2} \tag{2}$$

and the Galois conjugates of these five elements all generate power integral bases for $\mathbf{Q}(\zeta + \zeta^{-1})$. When $p = 5$ the field $\mathbf{Q}(\zeta + \zeta^{-1}) = \mathbf{Q}\big(\cos(2\pi i/5)\big) = \mathbf{Q}(\sqrt{5})$ is quadratic, so all the generators for $\mathbf{Z}[\zeta + \zeta^{-1}]$, including those in (2), are equivalent to $(1 + \sqrt{5})/2$. When $p = 7$,

$$\frac{1}{\zeta + \zeta^{-1} + 1} = -(\zeta^2 + \zeta^{-2}),$$

so $1/(\zeta + \zeta^{-1} + 1)$ is equivalent to a Galois conjugate of $\zeta + \zeta^{-1}$. When $p \geqslant 11$, however, the following theorem shows that the generators given in (2) and their Galois conjugates are pairwise inequivalent.

THEOREM 2. *If α is equivalent to*

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} + 1}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2},$$

or one of the Galois conjugates of these 5 elements then $\mathbf{Z}[\alpha] = \mathbf{Z}[\zeta + \zeta^{-1}]$. Moreover, if $p \geqslant 11$ then these elements are inequivalent, so there are at least $5(p-1)/2$ inequivalent generators for the ring of integers of $\mathbf{Q}(\zeta + \zeta^{-1})$.

https://doi.org/10.1017/S0004972700038119 Published online by Cambridge University Press

PROOF: As discussed above, Lemma 1 and Theorem 1 imply that the $5(p-1)/2$ elements are indeed generators. Suppose that two of these generators are equivalent. Then

$$\frac{1}{\zeta+\zeta^{-1}+a} = n \pm \frac{1}{\zeta^i+\zeta^{-i}+b},$$

for some $a, b \in \{0, \pm 1, 2\}$, $a \neq b$, $1 \leqslant i \leqslant (p-1)/2$, and $n \in \mathbf{Z}$. Getting a common denominator gives that

$$0 = n(\zeta^{i+1}+\zeta^{-i-1}) + (na-1)(\zeta^i+\zeta^{-i}) + n(\zeta^{i-1}+\zeta^{-i+1}) + (nb \pm 1)(\zeta+\zeta^{-1}) + nab - b \pm a,$$

so ζ is a root of

$$g(x) = n(x^{i+1}+x^{p-i-1}) + (na-1)(x^i+x^{p-i}) + n(x^{i-1}+x^{p-i+1}) + (nb \pm 1)(x+x^{p-1}) + nab - b \pm a.$$

Thus, the minimal polynomial for ζ, namely $1+x+x^2+\cdots+x^{p-1}$, divides $g(x)$ since it divides every polynomial satisfied by ζ. This is a contradiction for $p \geqslant 11$, as easily seen by considering the possible degree of $g(x)$ and the number of distinct monomials that occur in $g(x)$ for $1 \leqslant i \leqslant (p-1)/2$ [8]. The theorem follows. □

We now use Lemma 1 again to search for more generators from the generators given in Theorem 2. Let $a \in \{0, \pm 1, 2\}$. If

$$n \pm \frac{1}{\zeta+\zeta^{-1}+a}$$

is a unit for some $n \in \mathbf{Z}$, then, by Lemma 1, its inverse is also a generator. Since the set of units is stable under multiplication by -1, we look for units of the form $n - 1/(\zeta+\zeta^{-1}+a)$, $n \in \mathbf{Z}$. As in the proof of Theorem 1,

$$n - \frac{1}{\zeta+\zeta^{-1}+a} \text{ is a unit} \iff \prod_{i=1}^{(p-1)/2} \left(n - \frac{1}{\zeta^i+\zeta^{-i}+a}\right) = \pm 1$$
$$\iff f_a(n) = \pm 1,$$

where $f_a(x)$ is the minimal polynomial for $1/(\zeta+\zeta^{-1}+a)$. The degree of $f_a(x)$ is $(p-1)/2$ since $1/(\zeta+\zeta^{-1}+a)$ is a generator. The constant term of $f_a(x)$ is ± 1 since $1/(\zeta+\zeta^{-1}+a)$ is a unit. Let k_a denote the coefficient of x in $f_a(x)$. Then

$$f_a(n) = \pm 1 \implies n^{(p-1)/2} + \cdots + k_a n \pm 1 = \pm 1 \tag{3}$$

$$\implies n = \pm 2 \text{ or } n \text{ divides } k_a. \tag{4}$$

Thus, to determine the possible values for n such that $n - 1/(\zeta+\zeta^{-1}+a)$ is a unit, we compute k_a for $a = 0, \pm 1, 2$, and test those n that divide k_a in each case.

https://doi.org/10.1017/S0004972700038119 Published online by Cambridge University Press

We have

$$f_a(x) = \prod_{i=1}^{(p-1)/2} \Big(x - \frac{1}{\zeta^i + \zeta^{-i} + a}\Big).$$

Thus the constant term of $f_a(x)$ is given by

$$k_a = \pm \sum_{i=1}^{(p-1)/2} \frac{\zeta^i + \zeta^{-i} + a}{N(\zeta + \zeta^{-1} + a)}, \tag{5}$$

where, as above, N is the norm from $\mathbf{Q}(\zeta + \zeta^{-1})$ to $\mathbf{Q}$. Let T denote the trace from $\mathbf{Q}(\zeta + \zeta^{-1})$ to $\mathbf{Q}$. Since $\zeta + \zeta^{-1} + a$ is a unit for $a \in \{0, \pm 1, 2\}$, it follows from (5) that

$$k_a = \pm T(\zeta + \zeta^{-1} + a) = \pm\Big(-1 + \frac{(p-1)a}{2}\Big).$$

Now considering $a = 0, \pm 1, 2$ separately and using (4) yields the following theorem:

THEOREM 3. *Let $n \in \mathbf{Z}$, $n \neq 0$.*

1. *If $n - \big(1/(\zeta + \zeta^{-1})\big)$ is a unit then $n = \pm 1$ or $n = \pm 2$;*
2. *If $n - \big(1/(\zeta + \zeta^{-1} + 1)\big)$ is a unit then n divides $(p-3)/2$ or $n = \pm 2$;*
3. *If $n - \big(1/(\zeta + \zeta^{-1} - 1)\big)$ is a unit then n divides $(p+1)/2$ or $n = \pm 2$;*
4. *If $n - \big(1/(\zeta + \zeta^{-1} + 2)\big)$ is a unit then n divides $p - 2$ or $n = \pm 2$.*

It easily follows from Theorem 1 that $n = 1$ gives a unit in every case in Theorem 3 except when $a = -1$ (Case 3), and $n = -1$ gives a unit in every case except when $a = 2$ (Case 4). For $p < 1000$, we used the computer algebra system Magma to test all of the remaining possibilities for n for units of the form

$$n - \frac{1}{\zeta + \zeta^{-1} + a}, \quad a \in \{0, \pm 1, 2\}.$$

This was done by observing that

$$n - \frac{1}{\zeta + \zeta^{-1} + a} \text{ is a unit} \iff n(\zeta + \zeta^{-1}) + na - 1 \text{ is a unit.}$$

We wrote a computer program that calculated the norms

$$N\Big(n(\zeta + \zeta^{-1}) + na - 1\Big)$$

for $p < 1000$, $a \in \{0, \pm 1, 2\}$, and n as given in Theorem 3. For $p = 11$ and $13 < p < 1000$, all of the norms have absolute value greater than 1, so there are no units of this form. When $p = 13$, however, there is an additional unit, namely, $-2(\zeta + \zeta^{-1}) - 3$ is a unit, which corresponds to $-2 - \big(1/(\zeta + \zeta^{-1} + 1)\big)$ being a unit. Thus we have

THEOREM 4. *Let $a \in \{0, \pm 1, 2\}$, p be prime with $13 < p < 1000$, and ζ be a primitive p-th root of unity. Then $n - \big(1/(\zeta + \zeta^{-1} + a)\big)$ is not a unit in $\mathbf{Z}[\zeta + \zeta^{-1}]$.*

https://doi.org/10.1017/S0004972700038119 Published online by Cambridge University Press

It seems likely that Theorem 4 holds for $p > 1000$ as well.

Recall that Theorem 2 provided a list of power bases generators for the ring of integers of $\mathbf{Q}(\zeta + \zeta^{-1})$. For $p = 13$, if we take the inverse of the unit $2 + 1/(\zeta + \zeta^{-1} + 1)$ we get an additional power basis generator for $\mathbf{Z}[\zeta + \zeta^{-1}]$ by Lemma 1. For $p > 13$, we get no additional power bases generators, and our search for generators using Lemma 1 has ended. It is known, however, that there are no additional generators of any form for $p \leqslant 13$. Specifically, Gaál and Schulte [5] computed all power integral bases for a large collection of cubic fields, including the real cyclotomic field for $p = 7$; Gaál and Pohst [4] consider a family of totally real cyclic quintic fields and showed that only one, namely the real cyclotomic field for $p = 11$, admits a power integral basis, and they compute all the generators for this field; Gaál [2] computed all power integral bases for the first five totally real cyclic sextic number fields, which includes the real cyclotomic field for $p = 13$. In the work of Gaál, Pohst, and Schulte the generators are presented in a different form than in our work, but a close examination shows that we found all the generators for $p \leqslant 13$. This is stated in the following theorem.

THEOREM 5. *Let p be prime and ζ be a primitive p-th root of unity. Suppose α generates a power integral basis for $\mathbf{Q}(\zeta + \zeta^{-1})$.*

1. *If $p = 7$ then α is equivalent to*

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2},$$

or one of the Galois conjugates of these 4 elements.

2. *If $p = 11$ then α is equivalent to*

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} + 1}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2},$$

or one of the Galois conjugates of these 5 elements.

3. *If $p = 13$ then α is equivalent to*

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} + 1}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2}, \frac{1}{\left(1/(\zeta + \zeta^{-1} + 1)\right) + 2}$$

or one of the Galois conjugates of these 6 elements.

Similarly, for $p > 13$ it is plausible that there are no generators other than those found by our method and stated in Theorem 2. Thus we conclude with a question.

QUESTION. Let $p > 13$ be prime and ζ be a primitive p-th root of unity. If α generates a power integral basis for $\mathbf{Q}(\zeta + \zeta^{-1})$ then is α necessarily equivalent to

$$\zeta + \zeta^{-1}, \frac{1}{\zeta + \zeta^{-1}}, \frac{1}{\zeta + \zeta^{-1} + 1}, \frac{1}{\zeta + \zeta^{-1} - 1}, \frac{1}{\zeta + \zeta^{-1} + 2},$$

or one of the Galois conjugates of these 5 elements, or do additional generators exist for some prime p?

References

[1] A. Bremner, 'On power bases in cyclotomic number fields', *J. Number Theory* **28** (1988), 288–298.

[2] I. Gaál, 'Computing all power integral bases in orders of totally real cyclic sextic number fields', *Math. Comp.* **65** (1996), 801–822.

[3] I. Gaál, *Diophantine equations and power integral bases. New computational methods* (Birkhäuser, Boston, 2002).

[4] I. Gaál and M. Phost, 'Power integral bases in a parametric family of totally real cyclic quintics', *Math. Comp.* **66** (1997), 1689–1696.

[5] I. Gaál and N. Schulte, 'Computing all power integral bases of cubic fields', *Math. Comp.* **53** (1989), 689–696.

[6] M.–N. Gras, 'Non monogénéité de l'anneau des entiers des extensions cycliques de **Q** de degré premier $l \geqslant 5$', *J. Number Theory* **23** (1986), 347–353.

[7] K. Győry, 'Sur les polynômes à coefficients entiers et de discriminant donné, III', *Publ. Math. Debrecen* **23** (1976), 141–165.

[8] L. Miller-Sims, *Power bases for real cyclotomic fields*, (unpublished honors thesis, Smith College, 2003).

[9] T. Nagell, 'Sur les discriminants des nombres algébriques', *Ark. Mat.* **7** (1967), 265–282.

[10] L. Robertson, 'Power bases for cyclotomic integer rings', *J. Number Theory* **69** (1998), 98–118.

[11] L. Robertson, 'Power bases for 2-power cyclotomic fields', *J. Number Theory* **88** (2001), 196–209.

Department of Mathematics
Smith College
Northampton, MA 01063
United States of America
e-mail: millerlg@math.mcmaster.ca
lroberts@math.smith.edu