Chin. Ann. of Math.
13B: 2 (1992), 244—250.

CONSTRUCTIONS OF POWER BASES OF CYCLOTOMIC FIELDS

LUO CHENGHUI (罗承辉)*

Abstract

Suppose $\mathbf{Q}(\zeta_m)$ is the m-th cyclotomic number field, where ζ_m is an m-th primitive root of unity, $m>1$ any integer. Let $\alpha_m=\zeta_m+\zeta_m^2+\cdots+\zeta_m^{(m-1)/2}$ if m is odd and let β_m be the product of the integers $1-\zeta_m^j (1<j<m, (j, m)=1)$ if m has at least two distinct prime divisors. It is proved that both α_m and β_m generate power bases of $\mathbf{Q}(\zeta_m)$, i. e., $\mathbf{Z}[\alpha_m]=\mathbf{Z}[\beta_m]+\mathbf{Z}[\zeta_m]$. The author also conjectures that there is no other power basis generator except ζ_m up to equivalence, and proves that this is the case when $m=8$, 9 and 12. The corresponding result for $m=p$ an odd prime was also obtained by A. Bremner with a different method.

§1. Introduction and Main Results

Suppose K is an algebraic number field of degree n, O_K is its algebraic integer ring. An algebraic integer α is said to generate a power basis of K if $\mathbf{Z}[\alpha]=O_K$, i. e., 1, α, α^2, $\cdots\alpha^{n-1}$ form an integral basis of O_K over $\mathbf{Z}$. Let $G=\mathrm{Gal}(K/\mathbf{Q})$ be the Galois group of K/$\mathbf{Q}$. We can easily prove the following

Lemma 1. *If α generates a power basis of K, then so does $k\pm\sigma(\alpha)$ for all $k\in\mathbf{Z}$ and $\sigma\in G$.*

By Lemma 1, we can define an equivalence relation among the generators of power basis of K: α is equivalent to β if $\alpha=k\pm\sigma(\beta)$, $k\in\mathbf{Z}$, $\sigma\in G$.

In 1976, K. Györy [1] proved that there are only finitely many power basis generators in K up to equivalence. In 1988, A. Bremner [2] considered the question of power basis of $\mathbf{Q}(\zeta_p)$, where p is an odd prime. He found one and conjectured that this is the only "non-obvious" power basis generator $\alpha_p=\zeta_p+\zeta_p^2+\cdots+\zeta_p^{(p-1)/2}$. In this paper, we give several power basis generators besides the obvious one ζ_m for cyclotomic fields $\mathbf{Q}(\zeta_m)$, where m is any positve integer, and prove that they are the only ones in $\mathbf{Q}(\zeta_8)$, $\mathbf{Q}(\zeta_9)$ and $\mathbf{Q}(\zeta_{12})$. We may assume $m\not\equiv 2 \pmod 4$ as usual.

Theorem 1. *Suppose $\mathbf{Q}(\zeta_m)$ is the m-th cyclotomic field, where ζ_m is a primitive root of unity.*

Manuscript received June 8, 1990.

* Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China.

(1) *If m is odd, then $\alpha_m=\zeta_m+\zeta_m^2+\cdots+\zeta_m^{(m-1)/2}$ generates a power basis of $\mathbf{Q}(\zeta_m)$.*

(2) *If m has at least two distinct prime divisors, then $\beta_m=\prod_{\substack{1<j<m\\(j,m)=1}}(1-\zeta_m^j)$ generates a power basis of $\mathbf{Q}(\zeta_m)$.*

Theorem 2. *The power basis generators ζ_m, α_m and β_m defined in Theorem 1 are not equivalent to each other when $m\neq 3$.*

Remark 1. We conjecture that ζ_m, α_m and β_m are the only power basis generators up to equivalence, that is to say, we have the following list for all the power basis generators of $\mathbf{Q}(\zeta_m)$ up to equivalence:

ζ_m, if $m=2^k$;

ζ_m, β_m, if $m=2^k m_1$, odd $m_1\neq 1$, $k>1$;

ζ_m, α_m, if $m=p^k$, p is odd prime, $k\geqslant 1$;

ζ_m, α_m, β_m, if m is odd and has at least two distinct prime divisors.

Theorem 3. *Up to equivalence,*

(1) *The only power basis generator of $\mathbf{Q}(\zeta_8)$ is ζ_8.*

(2) *The only power basis generators of $\mathbf{Q}(\zeta_{12})$ are ζ_{12} and β_{12}.*

(3) *The only power basis generators of $\mathbf{Q}(\zeta_9)$ are ζ_9 and α_9.*

§ 2. Proofs of Theorems 1 and 2

Suppose $\sigma_i\in \mathrm{Gal}\ (\mathbf{Q}(\zeta_m)/\mathbf{Q})$ is defined as follows:

$$\sigma_i:\zeta_m\rightarrow\zeta_m^i,\quad (i,\ m)=1.$$

First, we need some lemmas.

Lemma 2. *If α generates a power basis of K and α is a unit of K, then α^{-1} also generates a power basis of K.*

Proof For any $\beta\in O_K$, we have $\beta\alpha^{n-1}\in O_K$, $n=[K:\mathbf{Q}]$. Since α generates a powerbasis of K, there exist $a_i\in\mathbf{Z}$, $i=0,\ 1,\ \cdots,\ n-1$, such that

$$\beta\alpha^{n-1}=\sum_{i=0}^{n-1}a_i\alpha^i,$$

that is

$$\beta=\sum_{i=0}^{n-1}a_{n-1-i}(\alpha^{-1})^i.$$

Thus α^{-1} generates a power basis of K.

Lemma 3. *ζ_m generates a power basis of $\mathbf{Q}(\zeta_m)$.*

This is well known (see, for example, [3], p. 11).

Lemma 4. *If m is odd, then $1+\zeta_m^{(m-1)/2}$ is a unit of $\mathbf{Q}(\zeta_m)$.*

Proof From

$$\begin{aligned}0&=1+\zeta_m+\zeta_m^2+\cdots+\zeta_m^{m-1}=1+(\zeta_m+\cdots+\zeta_m^{(m-1)/2})+\zeta_m^{(m-1)/2}(\zeta_m+\cdots+\zeta_m^{(m-1)/2})\\&=1+(1+\zeta_m^{(m-1)/2})(\zeta_m+\cdots+\zeta_m^{(m-1)/2}),\end{aligned}$$

we know that

$$(1+\zeta_m^{(m-1)/2})^{-1}=-(\zeta_m+\zeta_m^2+\cdots+\zeta_m^{(m-1)/2})=-\alpha_m$$

is an integer. The lemma follows.

Lemma 5. *If m has at least two prime divisors, then $1-\zeta_m$ is a unit of $\mathbf{Q}(\zeta_m)$. In fact we have* $\prod_{\substack{0<j<m\\(j,m)=1}}(1-\zeta_m^j)=1$.

Proof See [3], p. 12.

Now we can easily obtain Theorem 1 by the lemmas above.

Proof of Theorem 1 (1) If m is odd, then $((m-1)/2, m)=1$. By Lemma 3 and Lemma 1, we know that $1+\zeta_m^{(m-1)/2}=\sigma_{(m-1)/2}(1+\zeta_m)$ is a power basis generator of $\mathbf{Q}(\zeta_m)$. Since $1+\zeta_m^{(m-1)/2}$ is a unit by Lemma 4,

$$\alpha_m=-(\zeta_m^{(m-1)/2})^{-1}=\zeta_m+\zeta_m^2+\cdots+\zeta_m^{(m-1)/2}$$

is a power basis generator of $\mathbf{Q}(\zeta_m)$ by Lemma 2.

(2) If m has at least two distinct prime divisors, then $1-\zeta_m$ is a unit by Lemma 5. By Lemma 3 and Lemma 1, we know that $1-\zeta_m$ is also a power basis generator of $\mathbf{Q}(\zeta_m)$, so by Lemma 2 it follows that

$$\beta_m=(1-\zeta_m)^{-1}=\prod_{\substack{1<j<m\\(j,m)=1}}(1-\zeta_m^j)$$

is also a power basis generator of $\mathbf{Q}(\zeta_m)$.

Proof of Theorem 2 For any $k\in Z$ and $\sigma_j\in\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$, we have

$$k\pm\sigma_j(\zeta_m)+\sigma_{m-1}(k\pm\sigma_j(\zeta_m))$$
$$=2k\pm(\zeta_m^j+\zeta_m^{-j})=2k\pm\cos\frac{2j\pi}{m}\notin\mathbf{Z}(m\neq 3,\ 4).$$

Since

$$\alpha_m+\sigma_{m-1}(\alpha_m)=-1,\ \beta_m+\sigma_{m-1}(\beta_m)=1, \qquad (*)$$

ζ_m is not equivalent to α_m or β_m.

If α_m is equivalent to β_m, then $\alpha_m=k\pm\sigma_j(\beta_m)$ for some $k\in\mathbf{Z}$ and $\sigma_j\in\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$.

(i) If $\alpha_m=k+\sigma_j(\beta_m)$, from $(*)$ we obtain $k=-1$. So

$$-\frac{1}{1+\zeta_m^{\frac{m-1}{2}}}=-1+\frac{1}{1-\zeta_m^j}=\frac{\zeta_m^j}{1-\zeta_m^j},$$

$$-1-\zeta_m^{\frac{m-1}{2}}=-1+\zeta_m^{-j},$$

$$\zeta_m^{\frac{m-1}{2}}+\zeta_m^{-j}=0,$$

$$\zeta_m^{\frac{m-1}{2}+j}=-1.$$

This is impossible because m is odd.

(ii) If $\alpha_m=k-\sigma_j(\beta_m)$, from $(*)$ we obtain $k=0$. So

$$-\frac{1}{1-\zeta_m^{(m-1)/2}}=-\frac{1}{1-\zeta_m^j},$$

$$\zeta_m^{(m-1)/2}+\zeta_m^j=0,$$

this is impossible, either. So Theorem 2 follows.

§ 3. The Cases $m=8$, 9 and 12

In order to prove Theorem 3, we give a necessary and sufficient condition for α to generate a power basis.

Lemma 6. *A necessary and sufficient condition for an integer α to generate a power basis of $\mathbf{Q}(\zeta_m)$ is that all*

$$q_i(\zeta_m)=\frac{\alpha-\sigma_i(\alpha)}{\zeta_m-\sigma_i(\zeta_m)}$$

are units for $i\in N$, $1<i<m$, $(i, m)=1$ and $\sigma_i\in Gal(\mathbf{Q}(\zeta_m)/\mathbf{Q})$.

Proof See [2].

Besides this, we need the following well known result.

Lemma 7. *Let m be a power of a prime. Then every unit of $\mathbf{Q}(\zeta_m)$ is the product of a real unit and a root of unity.*

Proof of Theorem 3 Let us prove the case $m=12$ first. The degree of $\mathbf{Q}(\zeta_{12})$ over $\mathbf{Q}$ is 4. By the reason of equivalence, we may suppose that $\alpha=b_1\zeta_{12}+b_2\zeta_{11}^2+b_3\zeta_{12}^3$ is a power basis generator of $\mathbf{Q}(\zeta_{12})$, b_1, b_2, $b_3\in\mathbf{Z}$. Then we get

$$q_5(\zeta_{12})=b_1+b_2\zeta_{12}^3\in\mathbf{Q}(\zeta_4),\ q_7(\zeta_{12})=b_1+b_3\zeta_{12}^2\in\mathbf{Q}(\zeta_3).$$

By Lemma 6, they both are units of $\mathbf{Q}(\zeta_{12})$. Hence

$$(b_1,\ b_2,\ b_3)=(0,\ \pm1,\ 1),\ (0,\ 1,\ \pm1),\ (\pm1,\ 0,\ 0),$$

$\alpha=\pm\zeta_{12}$, $\pm(\zeta_{12}^2+\zeta_{12}^3)$, $\pm(\zeta_{12}^2-\zeta_{12}^3)$. But

$$\zeta_{12}^2-\zeta_{12}^3=\sigma_7(\zeta_{12}^2+\zeta_{12}^3),\ \zeta_{12}^2+\zeta_{12}^3=(1-\zeta_{12}^5)(1-\zeta_{12}^7)(1-\zeta_{12}^{11})=\beta_{12},$$

so up to e quivalence all power basis generators of $\mathbf{Q}(\zeta_{12})$ are ζ_{12} and β_{12}.

Now we prove the case $m=8$. Similarily, suppose that $\alpha=b_1\zeta_8+b_2\zeta_8^2+b_3\zeta_8^3$ is a power basis generator of $\mathbf{Q}(\zeta_8)$. Then $q_3(\zeta_8)=(b_1-b_3)+b_2(\zeta_8+\zeta_8^3)$. By Lemma 6 and Lemma 7, there exists $k\in\mathbf{Z}$ such that $\zeta_8^k q_3(\zeta_8)$ is real, that is to say,

$$\zeta_8^k q_3(\zeta_8)=\zeta_8^{-k}q_3(\zeta_8^{-1}).$$

Since $\zeta_8^4=-1$, we may take $k=0$, 1, 2, 3, to obtain the relations among b_i's.

$k=0$ implies $b_2=0$;

$k=1$ implies $b_1=b_3$, $b_2=0$;

$k=2$ implies $b_1=b_3$;

$k=3$ implies $b_1=b_3$, $b_2=0$.

On the other hand, $q_5(\zeta_8)=b_1+b_3\zeta_8^2\in\mathbf{Q}(\zeta_4)$ is a unit of $\mathbf{Q}(\zeta_8)$, and we have

$$(b_1,\ b_3)=(\pm1,\ 0),\ (0,\ \pm1).$$

Fi nally we get $(b_1,\ b_2,\ b_3)=(\pm1,\ 0,\ 0)$, $(0,\ 0,\ \pm1)$, $\alpha=\pm\zeta_8$ or $\pm\zeta_8^3$. So up to equivalence the power basis generator of $\mathbf{Q}(\zeta_8)$ can only be ζ_8.

Finally, let us deal with the case $m=9$. Let $\alpha=b_1\zeta_9+b_2\zeta_9^2+\cdots+b_5\zeta_9^5$ be the power basis generator. Then

$$q_2(\zeta_9)=(b_1-b_4-b_5)+(b_2-b_5)\zeta_9+(b_2+b_3-b_5)\zeta_9^2+(b_3-b_5)\zeta_9^3$$
$$+(b_3+b_4)\zeta_9^4+b_4\zeta_9^5;$$
$$q_4(\zeta_9)=b_1+(b_2-b_5)\zeta_9+b_4\zeta_9^3+b_2\zeta_9^4.$$

By Lemma 6 and Lemma 7, there exist $k_i\in\mathbf{Z}$ such that $\zeta_9^{k_i}q_i(\zeta_9)$ is real, $i=2,\ 4$, That is to say,

$$\zeta_9^{k_i}q_i(\zeta_9)=\zeta_9^{-k_i}q_i(\zeta_9^{-1}).$$

We can obtain the relations among b_j's from this equation.

If $i=2$, then

$k_2=0$ implies $b_2=b_3=b_5=0$;
$k_2=1$ implies $b_4=b_2+2b_3,\ b_1=0,\ b_5=-b_3$;
$k_2=2$ implies $b_2=0,\ b_4=b_1+b_3,\ b_5=-b_0-2b_3$;
$k_2=3$ implies $b_1=b_3=b_4=0$;
$k_2=4$ implies $b_1=b_4,\ b_3=b_2-b_1,\ b_5=2b_2-b_1$;
$k_2=5$ implies $b_1=b_3,\ b_4=2b_1-b_2,\ b_5=b_2$;
$k_2=6$ implies $b_1=b_2=b_4+b_5$;
$k_2=7$ implies $b_2=b_3,\ b_4=0,\ b_5=b_1-b_2$;
$k_2=8$ implies $b_3=b_1-b_2,\ b_4=b_2-b_1,\ b_5=0$.

If $i=4$, then

$k_4=0$ implies $b_2=b_4=b_5=0$;
$k_4=1$ implies $b_1+b_2=b_4=b_5$;
$k_4=2$ implies $b_1=b_4=b_5=0$;
$k_4=3$ implies $b_1=b_4,\ b_2=b_5=0$;
$k_4=4$ implies $b_2=-b_4,\ b_1=-b_5$;
$k_4=5$ imples $b_1=b_4=0,\ b_2=b_5$;
$k_4=6$ implies $b_1=b_2=b_5=0$;
$k_4=7$ implies $b_1=b_2=b_4+b_5$;
$k_5=8$ implies $b_1=b_2=b_4=0$.

So the only possibilities for $(k_2,\ k_4)$ which result in $\alpha\neq 0,\ \pm\zeta_9,\ \pm\zeta_9^2,\ \pm\zeta_9^4$ or $\pm\zeta_9^5$ are the following:

(i) $(k_2,\ k_4)=(0,\ 3)$ with $b_1=b_4,\ b_2=b_3=b_5=0$. Since $q_4(\zeta_9)=b_1(1+\zeta_9^3)$ must be a unit of $\mathbf{Q}(\zeta_9)$, we see that $b_1=\pm 1,\ \alpha=\pm(\zeta_9+\zeta_9^4)=\mp\zeta_9^7$ is equivalent to ζ_9.

(ii) $(k_2,\ k_4)=(3,\ 5)$ with $b_2=b_5,\ b_1=b_3=b_4=0$. We have $b_2=\pm 1$ since $q_4(\zeta_9)=b_2\zeta_9^4$ must be a unit of $\mathbf{Q}(\zeta_9)$. So $\alpha=\pm(\zeta_9^2+\zeta_9^5)=\mp\zeta_9^8$ is equivalent to ζ_9.

(iii) $(k_2,\ k_4)=(6,\ 7)$ with $b_1=b_2=b_4+b_4$. Then

$$\zeta_9^6q_2(\zeta_9)=(b_3-b_5)+(b_3+b_4)(\zeta_9+\zeta_9^8)+b_4(\zeta_9^2+\zeta_9^7),$$
$$\zeta_9^7q_4(\zeta_9)=b_4(\zeta_9+\zeta_9^8)+(b_4+b_5)(\zeta_9^2+\zeta_9^7),$$

$$q_8(\zeta_9)=(b_3+2\,b_5)+2b_4(\zeta_9+\zeta_9^8)+b_3(\zeta_9^2+\zeta_9^7).$$

Let $\mathbf{Q}(\zeta_9)^+=\mathbf{Q}(\zeta_9+\zeta_9^8)$ be the maximal real subfield of $\mathbf{Q}(\zeta_9)$, $N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}$ is the norm of $\mathbf{Q}(\zeta_9)^+/\mathbf{Q}$. Obviously, we have

$$(N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}(\alpha))^2=N_{\mathbf{Q}(\zeta_9)/\mathbf{Q}}(\alpha).$$

Since

$$N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}[a+b(\zeta_9+\zeta_9^8)+c(\zeta_9^2+\zeta_9^7)]$$
$$N=a^3-3a(b^2-bc+c^2)-(b^3-6\,b^2c+3\,bc^2+c^3),$$

we have

$$N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}[\zeta_9^6q_2(\zeta_9)]=(b_3-b_5)^3-3(b_3-b_5)(b_3^2+b_3b_4+b_4^2)$$
$$-(b_3^3-3b_3^2b_4-6b_3b_4^2); \tag{1}$$
$$N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}[\zeta_9^7q_4(\zeta_9)]=b_4^3-3b_4^2b_5-6b_4b_5^2-b_5^3; \tag{2}$$
$$N_{\mathbf{Q}(\zeta_9)^+/\mathbf{Q}}[q_8(\zeta_9)]=(b_3+2\,b_5)^3-3(b_3+2\,b_5)(b_3^2-2\,b_3b_4+4\,b_4^2)$$
$$-(b_3^3+6b_3^2b_4-24b_3b_4^2+8b_4^3). \tag{3}$$

These three expressions are congruent to b_4-b_5 modulo 3, so without loss of generality we can equate the three expressions above to $+1$.

Substracting (1) from (3) gives

$$b_3(b_4^2+b_4b_5+b_5^2)=b_4^3+3b_4b_5-b_5^3.$$

By (2), b_4, b_5 can not be zero simultaneously and $(b_4,\ b_5)=1$, so

$$b_4^2+b_4b_5+b_5^2\neq 0,\ b_3=\frac{b_4^3+3\,b_4^2b_5-b_5^3}{b_4^2+b_4b_5+b_5^2}=(b_4-b_5)+\frac{3\,b_4b_5}{b_4^2+b_4b_5+b_5^2}\,b_4.$$

So we obtain

$$\frac{3\,b_4b_5}{b_4^2+b_4b_5+b_5^2}\in\mathbf{Z} \tag{4}$$

since $b_3\in\mathbf{Z}$ and $(b_4,\ b_4^2+b_4b_5+b_5^2)=1$. It is easy to see that

$$-3\leqslant\frac{3\,b_4b_5}{b_4^2+b_4b_5+b_5^2}\leqslant 3. \tag{5}$$

Hence we obtain the solutions of (1), (2), (3) by (2), (4) and (5):

$(b_3,\ b_4,\ b_5)=(1,\ 1,\ 0)$ implies $\alpha=\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4=\alpha_9$;

$(b_3,\ b_4,\ b_5)=(1,\ 0,\ -1)$ implies $\alpha=-\zeta_9-\zeta_9^2+\zeta_9^3-\zeta_9^5=\sigma_4(\alpha_9)$;

$(b_3,\ b_4,\ b_5)=(1,\ -1,\ 1)$ implies $\alpha=\zeta_9^3-\zeta_9^4+\zeta_9^5=\sigma_7(\alpha_9)$.

So, up to equivalence, the only power basis generators are ζ_9 and α_9. This completes the proof of Theorem 3.

Remark 2. A. Bremner [2] also proved the case $m=p$, an odd prime of Theorem 1 (1) by a different method. The conjecture in Remark 1 for the case $m=5$ and 7 has been verified by T. Nagell[4] and A. Bremner[2]; and it is obviously true when $m=3$ and 4.

I would like to thank my teachers Feng Keqin and Zhang Xianke for their much help and many suggestions.

Refrences

[1] Győry, K. Sru les polynômes à coefficients entier et de discriminant donné, III, *Publ. Math. Debrecen*, **23** (1976), 141—165.

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

[3] Washington, L. C., Introduction to cycloto mic fields, Springer-Verlag, New York, 1982.

[4] Nagell, T. Sur les discriminants des nombers algébriques, *Ark. Mat.* **19**:7 (1967), 265—282.