Commun. Korean Math. Soc. **27** (2012), No. 3, pp. 449–454
http://dx.doi.org/10.4134/CKMS.2012.27.3.449

CYCLOTOMIC POLYNOMIALS OVER CYCLOTOMIC FIELDS

Sung Doo Kim and June Bok Lee

Abstract. In this paper, we find the minimal polynomial of a primitive root of unity over cyclotomic fields. From this, we factorize cyclotomic polynomials over cyclotomic fields and investigate the coefficients of $\Phi_{3n}(x)$ when $3 \nmid n$.

1. Introduction

Throughout this paper, n and m denote two positive integers with the greatest common divisor d of n and m. We define e by $n = de$ and f by $m = df$. Let e' be the largest factor of n such that $\gcd(d, e') = 1$, and $d' = \frac{n}{de'}$.

Let $\zeta_n = e^{2\pi\sqrt{-1}/n}$, which is a primitive nth root of 1, and the Euler ϕ-function $\phi(n)$ is the number of positive integers $\leq n$ that are relatively prime to n. The nth cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{\gcd(l,n)=1 \\ 1\leq l\leq n}} (x - \zeta_n^l).$$

We know that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ but might reducible over an extension field of $\mathbb{Q}$. For each integer k relatively prime to n, if we find the minimal polynomial of ζ_n^k over an extension field of $\mathbb{Q}$, then we can factorize $\Phi_n(x)$ because all roots of $\Phi_n(x)$ are ζ_n^l where $\gcd(l, n) = 1$ and $1 \leq l \leq n$.

In Section 2, we factorize cyclotomic polynomials over cyclotomic fields. In Section 3, we investigate the coefficients of $\Phi_{3n}(x)$ when $3 \nmid n$.

2. A factorization of cyclotomic polynomials over cyclotomic fields

In this section, let k be an integer relatively prime to n, and we find a factorization of $\Phi_n(x)$ over $\mathbb{Q}(\zeta_m)$.

Received February 1, 2011; Revised April 24, 2011.
2010 *Mathematics Subject Classification.* Primary 12D05.
Key words and phrases. factorization, cyclotomic polynomial, cyclotomic field.

2.1. The minimal polynomial of ζ_n^k over cyclotomic fields

Ming-chang Kang ([3]) showed that the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_m)$ is the greatest common divisor of $\Phi_n(x)$ and $x^e - \zeta_d$, which is

$$\prod_{\substack{\gcd(1+hd,n)=1\\ 0\le h\le e-1}} (x-\zeta_n^{1+hd}).$$

However, his expression is difficult to figure out the coefficients. In the following, if we know $\Phi_{e'}(x)$, then we give an easy construction of the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$, which is

$$(\zeta_d^i)^{\phi(e')}\Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}),$$

where i satisfies that $ie' = jd + k$ and $1 \le i \le d$. To prove this, we need some lemmas.

Lemma 2.1. *There exist unique i and j such that $ie' = jd + k$ and $1 \le i \le d$.*

Proof. We can find integers a_0 and b_0 such that $a_0e' - b_0d = k$ because $\gcd(d, e') = 1$. For an integer h, let $i = a_0 + hd$, $j = b_0 + he'$. Then there is a unique h such that $-\frac{a_0}{d} < h \le -\frac{a_0}{d} + 1$, so i is also unique because $0 < i = a_0 + hd \le d$. Therefore, there exist unique i and j such that $ie' - jd = k$ and $1 \le i \le d$. □

Lemma 2.2. *Let a and a' be positive integers such that a is divisible by every prime factor of a'. Then $\phi(a'a) = a'\phi(a)$.*

Proof. Refer to [3]. □

Lemma 2.3. *Let $a \mid b$ and $a \ne b$. Then $\phi(a) = \phi(b)$ if and only if $b = 2a$, where a is odd.*

Proof. If p is a prime number, then $\phi(p^{s+r})/\phi(p^s) = 1$ if and only if either $r = 0$ or $r = 1$, $s = 0$ and $p = 2$. Therefore, $\phi(a) = \phi(b)$ if and only if $b = 2a$, where a is odd. □

Lemma 2.4. $[\mathbb{Q}(\zeta_n^k, \zeta_m) : \mathbb{Q}(\zeta_m)] = [\mathbb{Q}(\zeta_n^k) : \mathbb{Q}(\zeta_d)] = d'\phi(e')$.

Proof. Refer to [3]. □

Since $\mathbb{Q}(\zeta_d)$ is a subfield of $\mathbb{Q}(\zeta_m)$, if the degree of the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_d)$ is equal to the degree of the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$, then the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_d)$ is equal to the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$.

If u is an algebraic number over a field $\mathbb{F}$, then we will find a monic polynomial whose root is u, and its degree is $[\mathbb{F}(u) : \mathbb{F}]$. If so, it is the minimal polynomial of u over $\mathbb{F}$ because of the uniqueness. We are now ready to prove the following theorem.

Theorem 2.5. *The minimal polynomial of* ζ_n^k *over* $\mathbb{Q}(\zeta_m)$ *is*

$$(\zeta_d^i)^{\phi(e')}\Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}),$$

where i *satisfies that* $ie' = jd + k$ *and* $1 \le i \le d$. *Moreover, all of its roots are* ζ_n^{k+hd} *where* h *is an integer such that* $\gcd(k+hd, n) = 1$ *and* $1 \le k + hd \le n$.

Proof. Since ζ_n^k is a root of $x^e - \zeta_d^k$, the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$ is a factor of $x^e - \zeta_d^k$. By Lemma 2.1, there exist unique i and j such that $ie' = jd + k$ and $1 \le i \le d$, then $(\zeta_d^i)^{e'} = \zeta_d^{jd+k} = \zeta_d^k$. So we get

$$x^e - \zeta_d^k = \zeta_d^k(\frac{x^e}{\zeta_d^k} - 1) = (\zeta_d^i)^{e'}((\frac{x^{d'}}{\zeta_d^i})^{e'} - 1) = \prod_{l|e'}(\zeta_d^i)^{\phi(l)}\Phi_l(\frac{x^{d'}}{\zeta_d^i})$$

because $x^{e'} - 1 = \prod_{l|e'}\Phi_l(x)$ and $e' = \sum_{l|e'}\phi(l)$.

By Lemma 2.3, if $e' \neq 2l$, where l is odd, then there exists the unique factor of the product that has the highest degree $d'\phi(e')$. This is

$$(\zeta_d^i)^{\phi(e')}\Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}).$$

For the remaining case, let $e' = 2a$, where a is odd. Then d and k are odd because e' and n are even. Two polynomials of the highest degree are

$$(\zeta_d^i)^{\phi(2a)}\Phi_{2a}(\frac{x^{d'}}{\zeta_d^i}) \text{ and } (\zeta_d^i)^{\phi(a)}\Phi_a(\frac{x^{d'}}{\zeta_d^i}).$$

Since $x^{2ad'} - \zeta_d^k = (x^{ad'} - \zeta_d^{\frac{d+k}{2}})(x^{ad'} + \zeta_d^{\frac{d+k}{2}})$, ζ_n^k is a root of $x^{ad'} - \zeta_d^{\frac{d+k}{2}}$ or $x^{ad'} + \zeta_d^{\frac{d+k}{2}}$. In fact, $(\zeta_n^k)^{ad'} + \zeta_d^{\frac{d+k}{2}} = \zeta_{2d}^k + \zeta_{2d}^{d+k} = \zeta_{2d}^k - \zeta_{2d}^k = 0$. Therefore, ζ_n^k is a root of $x^{ad'} + \zeta_d^{\frac{d+k}{2}}$. Since $i(2a) - jd = k$ implies $ia - \frac{j-1}{2}d = \frac{d+k}{2}$, we have

$$x^{ad'} - \zeta_d^{\frac{d+k}{2}} = \prod_{l|a}(\zeta_d^i)^{\phi(l)}\Phi_l(\frac{x^{d'}}{\zeta_d^i}).$$

Then ζ_n^k is not a root of $(\zeta_d^i)^{\phi(a)}\Phi_a(\frac{x^{d'}}{\zeta_d^i})$ but a root of $(\zeta_d^i)^{\phi(2a)}\Phi_{2a}(\frac{x^{d'}}{\zeta_d^i})$. Therefore, the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$ is

$$(\zeta_d^i)^{\phi(e')}\Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}).$$

The minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$ depends on i. Let i_l and j_l satisfy $i_l e' = j_l d + k_l$ and $1 \le i_l \le d$ where l is 1 or 2. If $i_1 = i_2$, then the minimal polynomials of $\zeta_n^{k_1}$ and $\zeta_n^{k_2}$ over $\mathbb{Q}(\zeta_m)$ are the same. Since $i_1 e' = j_1 d + k_1$ and $i_2 e' = j_2 d + k_2$, we get $(j_1 - j_2)d = k_2 - k_1$. So if the minimal polynomials of $\zeta_n^{k_1}$ and $\zeta_n^{k_2}$ over $\mathbb{Q}(\zeta_m)$ are the same, then we have $k_1 \equiv k_2 \pmod{d}$. Conversely, if $k_1 \equiv k_2 \pmod{d}$, then $i_1 = i_2$ because $\gcd(d, e') = 1$ and $1 \le i_1, i_2 \le d$.

Therefore, all roots of the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$ are ζ_n^{k+hd} where h is an integer such that $\gcd(k+hd, n) = 1$ and $1 \le k + hd \le n$. $\square$

For example, the degree of the minimal polynomial of ζ_{30} over $\mathbb{Q}(\zeta_3)$ is $[\mathbb{Q}(\zeta_{30}) : \mathbb{Q}(\zeta_3)] = 4$, and we get

$$x^{10} - \zeta_3 = \zeta_3(\frac{x^{10}}{\zeta_3} - 1) = \zeta_3^{10}((\frac{x}{\zeta_3})^{10} - 1) = \prod_{l|10} \zeta_3^{\phi(l)} \Phi_l(\frac{x}{\zeta_3})$$

$$= \zeta_3^{\phi(1)} \Phi_1(\frac{x}{\zeta_3}) \cdot \zeta_3^{\phi(2)} \Phi_2(\frac{x}{\zeta_3}) \cdot \zeta_3^{\phi(5)} \Phi_5(\frac{x}{\zeta_3}) \cdot \zeta_3^{\phi(10)} \Phi_{10}(\frac{x}{\zeta_3})$$

$$= (x - \zeta_3)(x + \zeta_3)(x^4 + \zeta_3 x^3 + \zeta_3^2 x^2 + \zeta_3^3 x + \zeta_3^4)(x^4 - \zeta_3 x^3 + \zeta_3^2 x^2 - \zeta_3^3 x + \zeta_3^4).$$

So the minimal polynomial of ζ_{30} over $\mathbb{Q}(\zeta_3)$ is $x^4 - \zeta_3 x^3 + \zeta_3^2 x^2 - \zeta_3^3 x + \zeta_3^4$.

2.2. A factorization of cyclotomic polynomials over cyclotomic fields

For each k, we found the minimal polynomial of ζ_n^k over $\mathbb{Q}(\zeta_m)$. So we are ready to factorize $\Phi_n(x)$ over $\mathbb{Q}(\zeta_m)$.

Theorem 2.6. *A factorization of cyclotomic polynomial $\Phi_n(x)$ over $\mathbb{Q}(\zeta_m)$ is*

$$\prod_{\substack{\gcd(i,d)=1 \\ 1 \le i \le d}} (\zeta_d^i)^{\phi(e')} \Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}).$$

Proof. By Theorem 2.5, we know that for all k, the degrees of the minimal polynomials of ζ_n^k over $\mathbb{Q}(\zeta_m)$ are the same. Thus, the number of irreducible factors is $\phi(n)/d'\phi(e') = \phi(d)$. Using Lemma 2.1 and that $\gcd(k, d) = 1$, $\gcd(i, d)$ divides k, so $\gcd(i, d) = 1$. Therefore, $\Phi_n(x)$ is

$$\prod_{\substack{\gcd(i,d)=1 \\ 1 \le i \le d}} (\zeta_d^i)^{\phi(e')} \Phi_{e'}(\frac{x^{d'}}{\zeta_d^i}) \text{ over } \mathbb{Q}(\zeta_m).$$

$\square$

3. The coefficients of $\Phi_{3n}(x)$

In this section, we find the coefficients of $\Phi_{3n}(x)$ and the coefficient of $x^{\phi(pq)}$ of $\Phi_{3pq}(x)$.

3.1. The coefficients of $\Phi_{3n}(x)$

We already know that $\Phi_{2n}(x) = \Phi_n(-x)$ when $2 \nmid n$. By Theorem 2.6, $\Phi_{3n}(x)$ has only two irreducible factors, so we can easily expand them. Now using the coefficients of $\Phi_n(x)$, we find the coefficients of $\Phi_{3n}(x)$ when $3 \nmid n$.

Theorem 3.1. *Let $\Phi_n(x) = \sum_{l=0}^{\phi(n)} a_l x^l$ and $\Phi_{3n}(x) = \sum_{l=0}^{2\phi(n)} c_l x^l$ when $3 \nmid n$. Then*

$$c_l = c_{2\phi(n)-l} = \frac{1}{2} \sum_{m=0}^{l} k_m a_m a_{l-m},$$

where $0 \le l \le \phi(n)$ *and*

$$k_m = \begin{cases} 2 & \text{if } m + l \equiv 0 \pmod 3 \\ -1 & \text{if } m + l \not\equiv 0 \pmod 3. \end{cases}$$

Proof. By Theorem 2.6, we know that $\Phi_{3n}(x)$ is

$$(\zeta_3)^{\phi(n)}\Phi_n(\frac{x}{\zeta_3}) \cdot (\zeta_3^2)^{\phi(n)}\Phi_n(\frac{x}{\zeta_3^2}) \text{ over } \mathbb{Q}(\zeta_3).$$

Then $c_l = c_{2\phi(n)-l} = a_0(\zeta_3)^{\phi(n)}a_l(\zeta_3^2)^{\phi(n)-l} + \cdots + a_l(\zeta_3)^{\phi(n)-l}a_0(\zeta_3^2)^{\phi(n)}$ where $0 \le l \le \phi(n)$. So we get

$$\begin{aligned} c_l &= \sum_{m=0}^{l} a_m a_{l-m}\zeta_3^{\phi(n)-m}\zeta_3^{2(\phi(n)-(l-m))} \\ &= \sum_{m=0}^{l} a_m a_{l-m}\zeta_3^{l+m} = \sum_{m=0}^{l} a_{l-m}a_m\zeta_3^{2(l+m)} \end{aligned}$$

and

$$2c_l = \sum_{m=0}^{l} a_m a_{l-m}(\zeta_3^{l+m} + \zeta_3^{2(l+m)}).$$

Moreover, $\zeta_3^{3h+1} + \zeta_3^{2(3h+1)} = -1$, $\zeta_3^{3h+2} + \zeta_3^{2(3h+2)} = -1$ and $\zeta_3^{3h} + \zeta_3^{2(3h)} = 2$ for $h \in \mathbb{Z}$. Let $k_m = \zeta_3^{l+m} + \zeta_3^{2(l+m)}$. Then

$$c_l = c_{2\phi(n)-l} = \frac{1}{2}\sum_{m=0}^{l} k_m a_m a_{l-m},$$

where $0 \le l \le \phi(n)$ and

$$k_m = \begin{cases} 2 & \text{if } m + l \equiv 0 \pmod 3 \\ -1 & \text{if } m + l \not\equiv 0 \pmod 3. \end{cases} \qquad \square$$

Let $\Phi_{35}(x) = \sum a_n x^n$. Then we know that $a_0 = 1$, $a_1 = -1$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 1$, $a_6 = -1$ and $a_7 = 1$. So the coefficient of x^7 of $\Phi_{105}(x)$ is $\frac{1}{2}(-a_0a_7 - a_1a_6 + 2a_2a_5 - a_3a_4 - a_4a_3 + 2a_5a_2 - a_6a_1 - a_7a_0) = \frac{1}{2}(-1 - 1 + 0 + 0 + 0 + 0 - 1 - 1) = -2$.

3.2. The coefficient of $x^{\phi(pq)}$ of $\Phi_{3pq}(x)$

If p and q are distinct prime numbers, then the coefficient of $x^{\phi(pq)/2}$ of $\Phi_{pq}(x)$ is $(-1)^r$, where r and s satisfy $(p-1)(q-1) = rp + sq$, $0 \le r \le q-2$ and $0 \le s \le p-2$ (see [4]). This time, we find the coefficient of $x^{\phi(pq)}$ of $\Phi_{3pq}(x)$.

Theorem 3.2. *Let p and q be odd primes where $3 \nmid p < q$. Then the coefficient of $x^{\phi(pq)}$ of $\Phi_{3pq}(x)$ is*

$$\begin{cases} -1 & \text{if } r \equiv 2 \pmod 3 \text{ or } s \equiv 2 \pmod 3, \\ 1 & \text{otherwise,} \end{cases}$$

where r and s satisfy $(p-1)(q-1) = rp + sq$, $0 \le r \le q-2$ and $0 \le s \le p-2$.

Proof. Let $\Phi_{pq}(x) = \sum_{l=0}^{\phi(pq)} a_l x^l$ and $\Phi_{3pq}(x) = \sum_{l=0}^{2\phi(pq)} c_l x^l$. Then by Theorem 3.1, we have

$$c_{\phi(pq)} = \frac{1}{2}\sum_{m=0}^{\phi(pq)} k_m a_m a_{\phi(pq)-m} \quad \text{where} \quad k_m = \begin{cases} 2 & \text{if } m + \phi(pq) \equiv 0 \pmod 3 \\ -1 & \text{if } m + \phi(pq) \not\equiv 0 \pmod 3. \end{cases}$$

Since $\Phi_{pq}(x)$ is symmetric, $a_m = a_{\phi(pq)-m}$. So

$$c_{\phi(pq)} = \frac{1}{2}\sum_{m=0}^{\phi(pq)} k_m a_m^2.$$

By [4], the coefficients of $\Phi_{pq}(x)$ are -1, 0 or 1, and the number of l such that $a_l = \pm 1$ is $2(r+1)(s+1) - 1$. By [1] and [2], we have $| \, c_{\phi(pq)} \, | \le 2$ and $c_{\phi(pq)}$ is odd. Therefore, $c_{\phi(pq)} = -1$ or 1. Let h be the number of m such that $k_m a_m^2 = 2$. Then the number of $k_m a_m^2 = -1$ is $2(r+1)(s+1) - 1 - h$. So

$$\sum_{m=0}^{\phi(pq)} k_m a_m^2 = 3h - 2(r+1)(s+1) + 1 = -2 \ \text{ or } \ 2.$$

Therefore, $3h$ is $2(r+1)(s+1) - 3$ or $2(r+1)(s+1) + 1$. So the coefficient of $x^{\phi(pq)}$ of $\Phi_{3pq}(x)$ is

$$\begin{cases} -1 & \text{if } r \equiv 2 \pmod 3 \text{ or } s \equiv 2 \pmod 3 \\ 1 & \text{otherwise.} \end{cases}$$

□

References

[1] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}*, Amer. Math. Monthly **75** (1968), 370–372.

[2] G. P. Dresden, *On the middle coefficient of a cyclotomic polynomial*, Amer. Math. Monthly **111** (2004), 531–533.

[3] M.-C. Kang, *Minimal polynomials over cyclotomic fields*, Amer. Math. Monthly **104** (1997), no. 3, 258–260.

[4] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial $\Phi_{pq}(X)$*, Amer. Math. Monthly **103** (1996), no. 7, 562–564.

Sung Doo Kim
Department of Mathematics
Yonsei University
Seoul 120-749, Korea
E-mail address: ksd93@hanmail.net

June Bok Lee
Department of Mathematics
Yonsei University
Seoul 120-749, Korea
E-mail address: leejb@yonsei.ac.kr