CYCLOTOMIC POLYNOMIALS

KAORU MOTOSE

Abstract. We state fundamental theorems and applications to mathematical items about cyclotomic polynomials.

Key Words on cyclotomic polynomials: prime divisors, orders, factorization over fields and rational primes.

2000 *Mathematics Subject Classification*: Primary 11R09; Secondary 11R18.

The author selects some items from Japanese book [3] with source papers [4], [5] and [6] restricting fundamental theorems and applications to mathematical items about cyclotomic polynomials. There are no new results and no difficult items for understanding. Would you like to use these results in your lecture for your students ?

In this paper, Latin small letters excepting e, x, i in equations or inequalities represent non negative integers. In particular, p is a prime number.

1. Definition and popular theorems

In this section we present definition of cyclotomic polynomials and popular theorems in the text books of algebras and number theory. In this paper, these results are used without references.

Definition. Let Δ_n be the set of primitive nth roots of 1, namely, $\Delta_n := \{\zeta_n^k \mid 1 \leq k \leq n \text{ with } \gcd(k,n) = 1\}$ where $\zeta_n := e^{\frac{2\pi i}{n}}$. The nth (order n) cyclotomic polynomial $\Phi_n(x)$ is defined by $\Phi_n(x) := \prod_{\zeta_n^k \in \Delta_n}(x - \zeta_n^k)$.

Popular theorems. Classifying orders in the set Ω of roots of $x^n - 1$, we have $\Omega = \bigcup_{d|n} \Delta_d$ and $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Thus $\Phi_n(x) \in \mathbb{Z}[x]$ by the induction on n.

$\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)}$ by Möbius inversion formula. Comparing the degrees of both sides of these polynomials, we obtains $n = \sum_{d|n} \varphi(d)$ and $\varphi(n) = \sum_{d|n} \mu(n/d)d$ where $\varphi(n) = |\Delta_n|$. It is easy to see that Galois group $G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to the group $\mathbb{Z}_n^*$ of units of $\mathbb{Z}/n\mathbb{Z}$, namely, $G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_k : \zeta_n \to \zeta_n^k \in \Delta_n\} \cong \mathbb{Z}_n^*$.

2. Prime divisors and the order n of $\Phi_n(a)$

Theorem 1 is the fundamental result on cyclotomic polynomials (see [3, p.46] or [4, first paper, p.38]). This theorem gives a characterization of prime divisors of cyclotomic polynomials. Theorem 1 was used to Theorems 2, 3 and Ap1.

Lemma 1. If $b \equiv 1 \bmod p$ for a prime $p > 2$, then $p \parallel \frac{b^p-1}{b-1}$.

Proof. Set $b := pu + 1$. Then $\frac{b^p-1}{b-1} = \frac{(pu+1)^p-1}{pu} \equiv \binom{p}{2}pu + \binom{p}{1} \equiv p \bmod p^2$.

The paper is in a final form and no version of it will be submitted for publication elsewhere.

Theorem 1. Assume $n \geq 2,\ a \geq 2$, and let $|a|_p$ be the order of a mod p for a prime $p \nmid a$. Then

$$p \mid \Phi_n(a) \text{ if and only if } p \nmid a \text{ and } n = p^r|a|_p \text{ with } r \geq 0.$$
$$\text{In this case, } p \parallel \Phi_n(a) \text{ if } r \geq 1 \text{ and } n \geq 3.$$

Proof. Assume $p \mid \Phi_n(a)$. Then from $a^n - 1 \equiv 0 \bmod p$ and $|a|_p \mid n$, we may set $n = p^r|a|_p \cdot t$ with $r \geq 0$ and $p \nmid t$. We set $s := p^r|a|_p$ and $b := a^s$. Then $n = st, b = a^s \equiv 1 \bmod p$. Since there exists a monic $g(x) \in \mathbb{Z}[x]$ with $\Phi_n(x)g(x) = \frac{x^{st}-1}{x^s-1}$, we have $t > 1$ by $n \geq 2$. A contradiction yields from

$$0 \equiv \Phi_n(a)g(a) = \frac{a^{st}-1}{a^s-1} = \frac{b^t-1}{b-1} = b^{t-1} + \cdots + 1 \equiv t \not\equiv 0 \bmod p.$$

Conversely, we assume $n = p^r|a|_p$. If $p = 2$ then $n = 2^r,\ a$ is odd and $\Phi_{2^r}(a) = a^{2^{r-1}} + 1$ is even and $2 \parallel \Phi_{2^r}(a)$ for $r \geq 2$, namely $n \geq 4$.

We may assume p is odd. In case $r = 0$, it is easy to see $p \mid \Phi_n(a)$. If $r \geq 1$ and set $c = a^{p^{r-1}|a|_p}$. Then we have

$$p \parallel \frac{c^p - 1}{c - 1} = \prod_{d||a|_p} \Phi_{p^r d}(a)$$

since conditions of Lemma 1 are satisfied from assumptions.

Thus there exists d with $p \mid \Phi_{p^r d}(a)$ and $0 \equiv a^{p^r d} - 1 \equiv (a^d - 1)^{p^r} \bmod p$. This implies $a^d \equiv 1 \bmod p$ and $|a|_p \mid d$, namely, $d = |a|_p$. Thus $p \parallel \Phi_n(a)$.

3. Factorization of $\Phi_n(x)$ over fields

It is very important to consider the factorization of cyclotomic polynomials over any fields by Theorem 2 (see [3, p.52], [4, V, p.31-32] or [5, VII, p.1]). In particular, factorizations over prime fields $\mathbb{F}_p$ determine the degrees (sizes) of prime ideals (see [1] or [7]) over rational primes in subfields of cyclotomic fields. Cyclotomic fields defined by $\Phi_\ell(x)$ for primes ℓ are the model of class field theory (see [7, Preface and introduction to Chapter 2, p.44]). Moreover the binary Golay code by the factorization of $\Phi_{23}(x)$ mod 2 is rerated to Mathieu group M_{23} and the planetary probe Voyager (see Ap6).

Lemma 2. (a) $\Phi_{np^s}(x) = \Phi_{np}(x^{p^{s-1}})$ for $s \geq 2$. (b) $\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$ for $p \nmid n$.

Proof. (a) It is enough to prove $\Phi_{np} = \Phi_n(x^p)$ for $p \mid n$. We can set $n = n'p$ from $p \mid n$.

$$\Phi_{np}(x) = \prod_{d|np}(x^d - 1)^{\mu(\frac{np}{d})} = \prod_{d|n}(x^{pd} - 1)^{\mu(\frac{n}{d})} \prod_{d|np}(x^d - 1)^{\mu(\frac{n'}{d}p^2)} = \Phi_n(x^p).$$

(b) Let n_0 be the product of distinct primes of n. Then $\Phi_n(x) = \Phi_{n_0}(x^{\frac{n}{n_0}})$ by (a). On the other hand

$$\Phi_{np}(x) = \prod_{d|np}(x^d - 1)^{\mu(\frac{np}{d})} = \frac{\prod_{d|n}(x^{pd} - 1)^{\mu(\frac{n}{d})}}{\prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}} = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

Thus we have the result by the induction on the number r of distinct primes of n.

Theorem 2. A cyclotomic polynomial $\Phi_n(x)$ over a field K has irreducible components of the same degree $[L : K]$, where L is the minimum splitting field of $\Phi_n(x)$ over K.

Proof. Let $f(x) \in K[x]$ be an irreducible component of $\Phi_n(x) \in K[x]$ and let $\alpha \in L$ with the order m be a root of $f(x)$. 'If part' of Theorem 1 holds for $\alpha \in L$ from $\Phi_n(\alpha) = 0$ and assumptions for the characteristic $p \geq 0$ of K. In case $p = 0$, $\Phi_n(x)$ is itself separable. Further in case $p > 0,\ n = p^s m\ (s \geq 0,\ p \nmid m)$, the next equation holds for $p > 0$

$$\Phi_n(x) = \Phi_{pm}(x^{p^{s-1}}) \equiv \left(\frac{\Phi_m(x^p)}{\Phi_m(x)}\right)^{p^{s-1}} \equiv \Phi_m(x)^{p^{s-1}(p-1)} \mod p.$$

Hence L is the minimum splitting field of $\Phi_m(x)$ and $L = K(\alpha)$. Thus $m = [L : K]$ since $f(x) \in K[x]$ is irreducible and has the root $\alpha \in L$.

Examples.

Ex1. $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible. This implies that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ shows the factorization of $x^n - 1$ over $\mathbb{Q}$.

Ex2. $\Phi_n(x) \in \mathbb{R}[x]$ has irreducible factors with degree 2.

$$\Phi_n(x) = \prod_k (x - \zeta_n^k)(x - \zeta_n^{-k}) = \prod_k (x^2 - 2(\cos\frac{2k\pi}{n})x + 1).$$

It shows $\Phi_n(x)$ is strict increasing for $x \geq 1$. This implies $\Phi_n(a) \geq 1$ for $n \geq 2$ and $a \geq 1$ (see the proof of Theorem 3).

Ex3. $\Phi_n(x) \in \mathbb{F}_p[x]$ for a prime p has irreducible factors with the same degree $d = |p|_n$, namely, $\mathbb{F}_{p^d}$ is a minimum splitting field by Frobenius automorphism.

4. **Primes and Cyclotomic polynomials**

Theorem 3 was proved by Theorem 1 and the estimation of $\Phi_n(a)$ (see Ex2). It has applications to Ap1 and Ap3.

Lemma 3. If $p \mid n$ and $p = \Phi_n(a)$, then $n = 6$ and $a = 2$ in case $n \geq 2$ and $a \geq 2$.

Proof. First we have the inequality $(a+1)^{\varphi(n)} > \Phi_n(a) = \prod_k |a - \zeta^k| > (a-1)^{\varphi(n)} \cdots (*)$. If $a \geq 3$, the next inequality yields a contradiction.

$$p = \Phi_n(a) > (a-1)^{\varphi(n)} \geq 2^{p-1} \text{ by } (*).$$

Thus $a = 2$ and p is odd from $2^n \equiv 1 \mod p$. From Theorem 1 $n = p^r m$ and $m = |2|_p > 1$. If $r \geq 2$ then $p = \Phi_n(2) = \Phi_{pm}(2^{p^{r-1}})$ and $2^{p^{r-1}} \geq 4$. This yields the same contradiction as the above. Hence $n = p|2|_p$ and $p > 2$. The next inequality gives $p = 3$ and $n = 3|2|_3 = 6$.

$$p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \left(\frac{2^p - 1}{2 + 1}\right)^{\varphi(m)} \geq \frac{2^p - 1}{3} \text{ by } (*).$$

Theorem 3. There exists a prime p with $n = |a|_p$ satisfying condition $(n, a) \neq (6, 2)$ for $n \geq 3, a \geq 2$ (A. S. Bang et al.).

Proof. $\Phi_n(a) > 1$ since $\Phi_n(x)$ is strict increasing for $x \geq 1$ from Ex2 and $\Phi_n(1) \geq 1$ from Lemma 2 and $n \geq 2$. Thus there exists a prime p with $p \mid \Phi_n(a)$. Theorem 1 implies $n = |a|_p$ in case $p \nmid n$. Thus p is the largest prime divisor since $n = p^r|a|_p, r \geq 1$ and $|a|_p$ is a divisor of $p - 1$ by Fermat little theorem. Further if $q \mid \Phi_n(a)$ with a prime $q \neq p$, then $n = |a|_q$. Hence $\Phi_n(a) = p^s,\ r \geq 1$ and $n = p^r|a|_p \geq 3$. Thus $s = 1$ by Theorem 1 and so $(n, a) = (6, 2)$ by Lemma 3.

5. Some applications of cyclotomic polynomials to the mathematical items

Ap1. Special case of theorem of Dirichlet can be proved: $\{ak \pm 1 \mid k = 1, 2, \cdots\}$ contains infinite many primes using Theorem 3 (see [3, p.40 for $+1$] or [5, VIII for -1]).

Ap2. Gauss sum is closely related to the discriminant of cyclotomic polynomials ([3, p.67] or [4, first paper, p.40]).

Ap3. It follows from Theorem 3 that finite division rings is fields (see [3, p.107] or [5, IV, p.2]). Unfortunately, Hamilton quaternion $\mathbb{H}$ is the only known division ring with the explicit multiplication. We would like to find concrete division rings different from $\mathbb{H}$. Such a try began already on a paper [2, pp.74-83]).

Ap4. For $n > 1$, find $a, m \geq 2$ such that $\gcd(am, n) = 1$ and $a^m \equiv 1 \bmod n$. Then we have $n = \prod_{d|m} \gcd(n, \Phi_d(a))$ (see [3, pp.95-96] or [4, V, p.33]).

Ap5. We can make a cipher as RSA cipher from cyclotomic polynomials because $a^{d-1} \equiv 1 \bmod d$ for $d \mid \Phi_n(a)$ with $\ell \nmid d$ where ℓ is the largest prime divisor of n (see [3, p.83] or [5, IV, pp.1-2]).

Ap6. A code by an irreducible factor with degree 11 of $\Phi_{23}(x) \bmod 2$ was used to a planetary probe Voyager. This code is also related to Mathieu group M_{23} (see [3, p.86] or [4, V, pp.34-35]. In detail, see also binary Golay code in Wikipedia on the internet.

Ap7. Some another applications Ramanujan's sum (see [3, pp.60-64] or [6, pp.65-70]) and others (see [3, chapter 8] or [4] or [5]).

References

[1] K. Ireland and M. Rosen, A classical introduction to modern number theory, GTM **84**, 1982

[2] I. Kikumasa, K. Koike and K. Oshiro, Complex rings, Quaternion rings, Octonion Rings, Proc. 50th symposium on ring theory and representation theory

[3] K. Motose, 円分多項式・有限群の指標 (Cyclotomic Polynomials · characters of finite groups), 弘前大学出版会 (Hirosaki University Press) (2006), in Japanese.

[4] ———, On values of cyclotomic polynomials, Math. J. Okayama Univ., **35**(1993), 35-40; II, **37**(1995), 27-36; III, **38**(1996), 115-122; V, **45**(2003), 29-36.

[5] ———, ———, Bull. Fac. Sci. Tech. Hirosaki Univ., IV, **1**(1998), 1-7; VI, **6**(2004), 1-5; VII, **7**(2004), 1-8; VIII, **9**(2006), 15-27.

[6] ———, Ramanujan's sums and cyclotomic polynomials, Math. J. Okayama Univ.**47**(2005), 65-74.

[7] T. Ono, An introduction to algebraic number theory, 1990, Plenum Press.

Emeritus Professor, Hirosaki University

Toriage 5-13-5, Hirosaki, 036-8171, Japan (home address)

E-mail address: motosekaoru@ka2.so-net.ne.jp, Off-line after 1 July 2019.