# 円周等分多項式の有理数体上での既約性

## Irreducibility of the Cyclotomic Polynomial on the Rational Number Field.

新潟歯学部　桜岡　充

Mitsuru SAKURAOKA : The Nippon Dental University, Hamaura-cho 1—8, Niigata 951, Japan

(1998年11月27日　受理)

Abstract

Irreducibility of the cyclotomic polinomial on the rational number field is shown by the method of Artin, which does not need the details of the arithmetics of algebraic number fields. This method is based on the fundamentals of linear algegra.

### §1．はじめに

数体 $K$ の拡大体の要素 $\varepsilon$ が1の $m$ 乗根であるとは $x^m-1$ の根であることであるが $K$ の標数 $p$ が0でないとき，$n=mp$ とするとその係数に $p\times$（整数）があれば0なので $x^n-1=(x^m-1)^p$ であって 1の $n$ 乗根は $m$ 乗根でもある。よって $p\neq 0$ のとき（$K$ の標数）と $n$ が互いに素の場合のみ議論すればすべて尽くされる。

さて，$K$ 内の多項式 $f(x)$ が重根を持つことと $f(x)$ と $f'(x)$ が1次以上の共通因数を持つことと同値であることを念頭におくなら $(x^n-1)'=nx^{n-1}$ で $nx^{n-1}$ の根は0のみであるから $x^n-1$ は分離多項式であることが解る。つまり $K$ 上の $x^n-1$ の分解体 $E$ は $K$ の正規拡大体であり $x^n-1$ のすべての相異なる $n$ 個の根を含むことになる。2個の1の $n$

乗根の積と商はやはり1の $n$ 乗根であるから，この $n$ 個は乗法群をつくる。つまりこの群は $E$ の有限部分群なので巡回群である。よって位数がちょうど $n$ の要素 $\varepsilon$ が存在してこの群は

$$\{1, \varepsilon, \varepsilon^2, \varepsilon^3, \cdots, \varepsilon^{n-1}\} ; \varepsilon^n = 1$$

で与えられる。このεが1の原始 $n$ 乗根である。$n$ と $i$ が互いに素であるとき $\varepsilon^i$ も1の原始 $n$ 乗根であるので 相異なる原始 $n$ 乗根の個数は1，2，…，$n$ のうち $n$ と互いに素なものの個数，つまり Euler 関数 $\varphi(n)$ である。

$d$ が $n$ の約数であるとき $x^d-1$ は $x^n-1$ の約数であることは自明であるので 1の $d$ 乗根は1の $n$ 乗根に含まれる。$\varepsilon^i$の位数つまり $(\varepsilon^i)^d=1$ を満たす最小の数を $d$ とすると $d$ は $n$ の約数である。$n$ と $i$ の最大公約数を（1も含めて）$d_c$とすると，$n=d\cdot d_c$，$i=i'\cdot d_c$（$d$ と $i'$は互いに素）とかけるので

$$(\varepsilon^i)^d=(\varepsilon^{d_c d})^{i'}=1 \quad \text{つまり } \varepsilon^i \text{は1の } d \text{ 乗根,} \tag{1}$$

次に $\varepsilon^i$ が $d$ より小さい位数 $\lambda$ をもつ：$(\varepsilon^i)^\lambda=1$ $(\lambda<d)$ とすると $xi'-yd=1$ なる整数 $x$，$y$ が存在するので $1=\varepsilon^{i\lambda x}=\varepsilon^{\lambda d_c}\cdot\varepsilon^{\lambda y d d_c}=\varepsilon^{\lambda d}$ なので $\varepsilon$ が $n$ より小さい位数をもつことになり $\varepsilon$ が1の原始 $n$ 乗根であることに反する。つまり $\varepsilon^i$の位数は $d$ 以上である。一方（1）でもあるので $\varepsilon^i$の位数は $d$ である。こうして $\varepsilon^i$は1の原始 $d=n/d_c$ 乗根であることが解る。今，$n$ の約数を1，$d_1$，…，$n$ とすれば $i=1$，2，…，$n$ なる $n$ 個の数は

$n$ と互いに素である $i$（この時 $\varepsilon^i$は原始 $n$ 乗根）$\varphi(n)$ 個，
$n$ とのGCMが $d_1$ である $i$（この時 $\varepsilon^i$は原始 $n/d_1$乗根）$\varphi(n/d_1)$ 個，
$n$ とのGCMが $d_2$ である（この時 $\varepsilon^i$は原始 $n/d_2$乗根）$\varphi(n/d_2)$ 個，　(2)
……
$n$ とのGCMが $n$ である
つまり $i=n$（$\varepsilon^i=\varepsilon^n=1$ は原始1乗根）$\varphi(n/n)=1$ 個，

のどれかの組に分類される。よって

$$\Phi_d(x)=\prod_{\eta=(\text{原始 } d \text{ 乗根})}(x-\eta) \tag{3}$$

と表すことにすると

$$x^n-1=\prod_d \Phi_d(x) \tag{4}$$

とかけることになる。ここに $d$ は $n$ の約数を動く。勿論 $\Phi_1(x)=x-1$ である。そして $\Phi_d(x)$ は最高次係数が1の 体 $K$ の数のみを係数とする多項式である。これは $n=1$ の

ときは自明であり 帰納法の仮定のもとで（2）の並びの逆順をおってゆけば

$$x^d-1=\Phi_d(x)\cdot g(x)$$

において $g(x)$ が最高次係数1の体 $K$ の数のみを係数とするとき 実際の割り算：$(x^d-1)/g(x)$ で $\Phi_d$に $K$ 以外の数が出現しないことよりいえる。（4）の右辺は勿論，$x^n-1$ の $K$ での分解を与えている訳であるが，各因子 $\Phi_d(x)$が $K$ 内で既約であるとは限らない。 然るに $K$ が有理数体 $Q$ のときは $\Phi_n(x)$ は既約であることが示される。これを示すのが小論の目的である。

## §2．($x^n-1$)の分解体 E とその自己同型群

$\varepsilon$ が1の原始 $n$ 乗根の1つであるとき $K$ に $\varepsilon$ を付加して得られる拡大体 $K(\varepsilon)$ は正規拡大体であってすべての1の $n$ 乗根を含むのであるから $x^n-1$ の分解体 $E$ そのものである。 $\Phi_n(\varepsilon)=0$ なので，これは分離多項式 $\Phi_n(x)$ の分解体でもあり，

$$E/K\leqq\varphi(n) \tag{5}$$

が成立する。(等号は $\Phi_n(x)$ が $K$ 内で既約のとき成立する。) いま，$E$ の $K$ 上の自己同型群を $G$ とし その1つの要素を $\sigma$ とかいてみよう。 $\Phi_n(x)$ は $K$ 内にあるのでその根は $K$ 上の群での置換に対して 1の原始 $n$ 乗根は1の原始 $n$ 乗根に写像されるので $i$ と $n$ を互いに素な整数として $\sigma(\varepsilon)=\varepsilon^i$ と表すことができる。このとき

$$\sigma(\varepsilon^j)=(\varepsilon^i)^j=(\varepsilon^j)^i \tag{6}$$

なので $\sigma$ は各 $n$ 乗根を $i$ 乗する写像なのである。これは $i$ が $G$ のどの要素をとったかによって定まり，原始 $n$ 乗根のとり方には無関係であることを示している。そして $i$ は $n$ の倍数を除いて一意であるが $n$ と互いに素な任意の $i$ が自己同型写像を定める訳ではない。例えば $K$ が有理複数体のとき1の4乗根 $\pm1$，$\pm i$ は $K$ に属し $\varepsilon=i$，$\varepsilon^3=-i$ は原始4乗根であるが $E=K(\varepsilon)=K$ であって自己同型群は恒等写像のみからなり，上記の $\sigma(\varepsilon)=\varepsilon^3$ 等の要素をもつことはないのである。

次に $\sigma(\varepsilon)=\varepsilon^i$を与える写像を $\sigma_i$で表すことにすると

$$\sigma_i\sigma_j(\varepsilon)=\sigma_i(\varepsilon^j)=(\varepsilon^j)^i=\varepsilon^{ij}$$

であるので $\sigma_i\sigma_j=\sigma_{ij}$となる。それゆえ各 $\sigma_i$ に $n$ を法とする既約剰余類を一意的に対応ずけることが可能であって，2個の写像の積には各々が対応する剰余類の積が対応する。こ

---

(*) $n$ を法とする既約剰余類を代表する数 $a$，$b$ ($a\neq0$，$b\neq0$) に対して $ab$ も $n$ と素。$ax-by=1$ を満たす $x$，$y$ が存在する。よって $ax=by+1$ なので $a$ の逆要素は常に存在する。つまり既約剰余類は位数 $\varphi(n)$ [Euler 関数] の乗法群をつくる。

こでいう既約剰余類（＊）とは整数の集合 $\mathbf{Z}$ の $n$ を法とする剰余類のうち $n$ と互いに素の整数からなるもののことである。　従って $E=K(\varepsilon)$ は $x^n-1$ の分解体なのであるから $E$ の $K$ 上の自己同型群 $G$ が原始根のみの置換群として存在し $E/K \leqq \varphi(n)$ なのであるから $G$ は $n$ を法とする既約剰余群のある部分群に同型である。　既約剰余群はもちろん可換群なのであるから $G$ は可換群である。

## §3．$\Phi_n(x)$の有理数体上での既約性

多項式 $f(x)$ を有理数体 $Q$ 上での $x^n-1$ の約数，つまり有理数を係数にもつとする。適当な定数をかけることにより $f(x)$ が整数係数をもつようにできるので これ以後 $f(x)$ は整数係数を持つとして議論をすすめる。 いまある自然数 $k$ に対して $f(x^k)$ を $f(x)$ で割ったときの剰余を $r_k(x)$ とすると $r_k(x)$ は有理係数の多項式であって実際の割り算をやれば商の各次数の係数は $f(x)$ の最高次の係数によってきてその係数の分母の素数因子は有るとしても $f(x)$ の最高次の係数の素因数だけである。 つぎに $f(x^{k+n})-f(x^k)$ については $f(x)$ 中の $ax^m$ なる項からの部分は

$$a(x^{k+n})^m-a(x^k)^m=ax^{mk}(x^{mn}-1)$$

であるが，これは $x^n-1$ で割り切れるので $f(x)$ で割り切れる。つまり $f(x^{k+n})-f(x^k)$ は $f(x)$ で割り切れるので

$$f(x^{k+n})=f(x^k)+f(x)\cdot g(x)\quad[g(x)\text{は多項式}] \tag{7}$$

とかける。よって

$$r_{k+n}(x)=r_k(x) \tag{8}$$

となり $r_k(x)$ は $k$ の $n$ を法とする剰余類に関連ずけることができる。そして $r_k(x)$ のうち相異なるものの数は有限個である。

さて素数 $p$ と $f(x)$ の最高次の係数が互いに素の場合を考える。$p$ が素数のとき $2^p-2=(1+1)^p-(1+1)=\sum_{r=1}^{p-1}{}_pC_r$ なので $2^p-2$ は $p$ で割り切れ，さらに

$$\begin{cases}(n+1)^p-(n+1)=n^p+\sum_{r=1}^{p-1}{}_pC_r\cdot n^r+1-(n+1)=(n^p-n)+\sum_{r=1}^{p-1}{}_pC_r\cdot n^r\\ \qquad\qquad\qquad\qquad=n^p-n+\ [p\text{で割り切れる数}]\end{cases}$$

であるので $n^p-n$ は $p$ で割り切れる。よっていま，

$$f(x)=a_tx^t+a_{t-1}x^{t-1}+\cdots+a_1x+a_0$$

とすると

$$f(x^p)=a_tx^{pt}+a_{t-1}x^{p(t-1)}+\cdots+a_1x+a_0$$

であって$[f(x)]^p$ の中の $x$ に関する各次数の内で $x^{p(t-i)}$の係数以外は二項係数を含み $p$ で割り切れることは自明であり $x^{p(t-i)}$の係数は$(a_{t-i})^p$と二項係数を含む $p$ で割り切れるものの和である。 よって$f(x^p)-[f(x)]^p$の各項のうちで係数が $p$ を explicit に持たないのは$x^{p(t-i)}$の係数であるところの $(a_{t-i})^p-a_{t-i}$のみであることになり これが $p$ の倍数であることから$f(x^p)-[f(x)]^p$の係数はすべて $p$ で割り切れる：

$$f(x^p)-[f(x)]^p=p\cdot h(x) \tag{9}$$

ここに $h(x)$ は整数係数の多項式である。 故に $r_p(x)$ は $h(x)$ を$f(x)$ で割ったときの剰余の $p$ 倍であることになり，$p$ は$f(x)$の最高次係数中にない素数なのであるから $r_p(x)$の分母が $p$ を含まず，分子が $p$ を持つことになって $p$ は $r_p(x)$の係数の分子をすべて割り切っている。

つぎに，すべての $r_k(x)$ および$f(x)$ の最高次の係数すべてにわたって，そこに現れ得る係数の分子をみるとき それらの最大値より大きな整数を $M$ としよう。 $p$ が $M$ より大きな素数であるとき，つまり $p$ が$f(x)$ の最高次の係数も割らないとき，$p$ が $r_p(x)$ の係数の分子を割ることができるのは $r_p(x)=0$ のときだけなので $p\geqq M$ なる素数 $p$ に対しては $r_p(x)=0$ である。(勿論このとき$f(x^p)$ は$f(x)$ で割り切れている。)

また $k$ と $l$ を $r_k(x)=0$，$r_l(x)=0$ を満たすような素数とすると$f(x^k)$ が$f(x)$ で割り切れるので$f(x^{kl})-f(x^l)$ は$f(x^l)$ で割り切れる。そして$f(x^l)$ は$f(x)$ で割り切れるので$f(x^{kl})$ は$f(x)$ で割り切れることになり $r_{kl}(x)=0$ である。すべての素因子が $M$ 以上のときは $r_k(x)=0$ なのである。こうして $M$ より大きな素数自体や素数因子しか持たない合成数 $k$ に対しては $r_k(x)=0$ である。

こんどは $k$ が $n$ と互いに素な数とする。 $k_1=k+n\times$($k$ の素因子でない $M$ より小さい素数全体の積) と書く。 このとき $k_1$は $M$ より小さい素数で割り切れないことは自明でありその素因子は $M$ 以上なので $r_{k1}(x)=0$ である。 ところが $k$ と $k_1$は $n$ を法として同じ剰余類に属しているので(8)より $r_k(x)=r_{k1}(x)=0$ である。つまり $k$ と $n$ が互いに素のとき$f(x^k)$ は$f(x)$で割り切れるという結論に導かれる。($k$ に対して $n$ と互いに素である以外に条件が不必要なのである。) そこで，$f(x)$ に対して これが原始 $n$ 乗根 $\varepsilon$ を根として持つとすると $k$ と $n$が互いに素ならば$f(x^k)=f(x)\cdot q(x)$ となり$f(\varepsilon^k)=0$ である。つまり原始乗根はすべて$f(x)$ の根であり $(f(x)$ の次数$)\geqq\varphi(n)$ が成立する。 それ故全ての原始 $n$ 乗根をもつ円周等分多項式 $\Phi n(x)$ は 次数が $\varphi(n)$ なのであるから $K$ 内で既約でなければならない。($\Phi_n(x)=g(x)\cdot h(x)$；$g(\varepsilon)=0$，$\deg g(x)<\deg\Phi_n(x)=\varphi(n)$ と分解されると再び上記の議論から $g(x)$ が $\varphi(n)$ 個の相異なる原始 $n$ 乗根を持つことになり矛盾である。)

こうして $Q(\varepsilon)/Q=\varphi(n)$ であり $G$ は $\varphi(n)$ 個の要素を持つことになり $n$ と互いに素な任意の $i$ に対して自己同型写像 $\sigma_i$ が定まることが解る。以上より

> 有理数体 $Q$ 内の円周等分多項式 $\Phi_n(x)$ は既約であり $\varepsilon$ を原始 $n$ 乗根の1つとするとき
>
> $$Q(\varepsilon)/Q=\varphi(n)\ ;\ \varphi(n)\ \text{は Euler 関数}$$
>
> である。 $n$ と互いに素な任意の $i$ について，写像 $\sigma_i(\varepsilon)=\varepsilon^i$ は $Q(\varepsilon)$ の $Q$ 上の自己同型群 $G$ に含まれ，$G$ は $n$ を法とする規約剰余類全体のつくる乗法群と同型である。

とくに $n$ が素数 $p$ のとき剰余類はすべて既約剰余類なので群 $G$ は $p$ を法とする既約剰余類のつくる剰法群と同型である。そしてこの既約剰余類群は乗法群なのであるから、位数 $Q(\varepsilon)/Q=\varphi(p)=p-1$ の巡回群である。 さらに

$$x^p-1=\Phi_p(x)\cdot\Phi_1(x)$$

であるので

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

であることも分かる。

## 参考文献


(1) E. Artin : Algebraic nurbers and algebraic function, Lecture notes, Princeton Univ., 1950-51.
Galoissche Theorie, B. G. Teubner Verlag., Leipzig, 1959.

(2) 川久保　勝夫：変換群論，岩波書店，1987.

(3) H. Ohmori : Homomorphic images of Lie group, J. Math. Soc. Japan 18, 1966.

(4) 竹之内　脩・浅野　洋：線形代数学，朝倉書店，1995.