円分多項式

定義 1 n 乗して始めて 1 になる数を 1 の**原始 n 乗根 (primitive n-th root)** と呼ぶ.

n が素数の場合は 1 を除く n 乗根は全て原始 n 乗根である．つまり，$z^p = 1$ の解

$$1, \omega, \omega^2, \cdots, \omega^{p-1} \quad \left(\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}\right)$$

から 1 を除いた $p-1$ 個の数がそれにあたる．$\omega = \cos\dfrac{\pi}{4} + i\sin\dfrac{\pi}{4}$ は原始 8 乗根のうちの一つ，$\omega = \cos\dfrac{\pi}{6} + i\sin\dfrac{\pi}{6}$ 原始 12 乗根のうちの一つである．つまり

$$\omega_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

は明らかに 1 の原始 n 乗根の一つである．n が素数の場合は原始 n 乗根の個数は明らかであったが，一般の場合はその個数はいくつであろうか.

定理 1 1 の原始 n 乗根は $\phi(n)$[*1]個ある.

［証明］一般に 1 の n 乗根は ${w_n}^m (m = 0, 1, 2, \cdots, n-1)$ と表せる．これが 1 と等しくなるのは $mx = kn$ となる場合で，m, n が公約数 $d \neq \pm 1$ をもてば，$m'dx = kn'd$ つまり $m'x = kn'$ と表せ，これは 1 の n' 乗根のどれかと等しい．よって m は n と互いに素でなければならず，m は n と互いに素であれば $mx = kn$ を満たす最小の x は n である． ［証明おわり］

定義 2 自然数 n について，1 の原始 n 乗根のみを根とする多項式を**円分多項式**あるいは**円周等分多項式 (Cyclotomic polynomial)** と呼ぶ.

つまり円分多項式は

$$F_n(x) = \prod_{\zeta \text{は 1 の原始 } n \text{ 乗根}} (x - \zeta)$$

と表すことができ，また

$$F_n(x) = \prod_{1 \leq m \leq n-1, (m,n)=1} (x - \omega^m) \quad \left(\text{ただし} \omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)$$

と表すこともできる.

補題 1

$$x^n - 1 = \prod_{d|n} F_d(x)$$

が成り立つ.

［証明］n の全ての約数を $d_0 = 1, d_1, d_2, \cdots, d_k = n$ とする．そのうちの一つを d とする.

$$n = dl$$

[*1] $\phi(n)$ は**オイラー関数**と呼び，n 以下で n と互いに素な自然数の個数を言う.

とすると，

$$\omega^0 = 1, \omega^l, \omega^{2l}, \cdots, \omega^{(d-1)l}$$

はすべて，1 の d 乗根である．このうち，$\omega^{jl}, ((j,d)=1)$ は原始 d 乗根である．このことから 1 の n 乗根全ての集合を A，1 の原始 d 乗根の集合を A_d とすると，

$$A_d \subset A$$

である．また定義 1 から明らかに

$$A_g \cap A_h = \phi \quad (g \neq h)$$

逆を調べてみよう．$1 \leq m \leq n-1$ について $m = m'l, n = dl$ とすると，

$$1, \omega^l, \omega^{2l}, \cdots, \omega^{(d-1)l}$$

は 1 の d 乗根で

$$\omega^m = (\omega^l)^{m'}$$

はこのなかの一つで，かつ $(m', d) = 1$ なので原始 d 乗根である．つまり A の要素であれば A_d のどれかにふくまれる．よって補題は示された． ［証明おわり］

と証明するより具体的な例から感覚的に理解する方がいいであろう，例えば $n = 12$ であれば

$$\begin{aligned}
&x^{12}-1 \\
=&\{x-1\}\left\{x-\omega^6\right\}\left\{(x-\omega^4)(x-\omega^8)\right\} \\
&\qquad\qquad \times\left\{(x-\omega^3)(x-\omega^9)\right\}\left\{(x-\omega^2)(x-\omega^{10})\right\}\left\{(x-\omega)(x-\omega^5)(x-\omega^7)(x-\omega^{11})\right\} \\
=&F_1F_2F_3F_4F_6F_{12}
\end{aligned}$$

定理 2 円分多項式は $\phi(n)$ 次の整数係数の既約多項式である．と書いても同じ意味である．

$\phi(n)$ 次であることはこれまでのことから明らか．また補題 1 より

$$F_n = \frac{x^n - 1}{\prod_{d|n} F_d(x)}$$

であるから $k \leq n-1$ で $F_k \in \mathbb{Q}[x]$ であれば $F_n \in \mathbb{Q}[x]$．またこれは $F_n \in \mathbb{Z}[x]$ であることと同値（「ガウスの補題からアイゼンシュタインの既約判定法」参照）であるから，F_n は整数係数の多項式であることも明らかである．問題はその既約性であるが，これは難しい．ここでその証明するのは可能であるが，非常に長くなるので別稿に譲りたい．

Maxima で計算した結果を示す．最も右側の括弧の中が円分多項式とは限らない

```
(%i1)for n:1 thru 20 do display(&factor(x^n-1))
```

$$
\begin{aligned}
&factor\,(x-1) = x-1\\
&factor\left(x^2-1\right) = (x-1)\,(x+1)\\
&factor\left(x^3-1\right) = (x-1)\left(x^2+x+1\right)\\
&factor\left(x^4-1\right) = (x-1)\,(x+1)\left(x^2+1\right)\\
&factor\left(x^5-1\right) = (x-1)\left(x^4+x^3+x^2+x+1\right)\\
&factor\left(x^6-1\right) = (x-1)\,(x+1)\left(x^2-x+1\right)\left(x^2+x+1\right)\\
&factor\left(x^7-1\right) = (x-1)\left(x^6+x^5+x^4+x^3+x^2+x+1\right)\\
&factor\left(x^8-1\right) = (x-1)\,(x+1)\left(x^2+1\right)\left(x^4+1\right)\\
&factor\left(x^9-1\right) = (x-1)\left(x^2+x+1\right)\left(x^6+x^3+1\right)\\
&factor\left(x^{10}-1\right) = (x-1)\,(x+1)\left(x^4-x^3+x^2-x+1\right)\left(x^4+x^3+x^2+x+1\right)\\
&factor\left(x^{11}-1\right) = (x-1)\left(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)\\
&factor\left(x^{12}-1\right) = (x-1)\,(x+1)\left(x^2+1\right)\left(x^2-x+1\right)\left(x^2+x+1\right)\left(x^4-x^2+1\right)\\
&(\%o1)done
\end{aligned}
$$

円分多項式を眺めているといくつか特徴に気付く．いくつかをピックアップしてみよう．なお証明を記述するのは面倒になったのでやめる．なお円分多項式に関する定理は他にも色々あるが，それらは私には証明できない．

定理 3 F_1 を除いて，円分多項式の係数は左右対称である．

定理 4 F_1 を除く円分多項式の積の多項式の係数は左右対称である．

定理 5 全ての円分多項式の積の多項式の係数は左右対称または符号が入れ替わって左右対称である．

定理 6 $n = 2^k$ を除く円分多項式 F_n の $\dfrac{\phi(n)}{2}$ 次の項の係数は奇数である．

定理 7 $n = 2^k$ を除く円分多項式 $F_{\_}$ の項数は奇数である．

定理 8 $n \leq 104$ の円分多項式 F_n の係数の絶対値は 1 以下である．