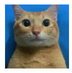

概要

円分多項式に関するあれこれ

1 円分体

定義 1.1. $\zeta^m = 1$ を満たす元 ζ を **1 の** m **乗根**という．1 の m 乗根という．1 の m 乗根 ζ で $1 \leq d < m$ なる整数 d について $\zeta^d \neq 1$ となるものを **1 の原始** m **乗根**という．

補題 1.2. Ω を代数的閉体とするとき次は同値である．

1. 1 の原始 m 乗根が存在する．
2. 1 の m 乗根全体が位数 m の巡回群をなす．
3. Ω の標数を p とするとき p は m と互いに素である．

証明. $2 \Rightarrow 1$：巡回群の生成元が 1 の原始 m 乗根である．$1 \Rightarrow 3$：対偶を示す．$m = pn\,(n \in \mathbb{N})$ と表すことができる．ζ を m 乗根とすると $\zeta^m = \zeta^{pn} = (\zeta^n)^p = 1$ である．$X^p - 1 = (X-1)^p$ であることから $\zeta^n = 1$ となり, 1 の原始 m 乗根は存在しない．$3 \Rightarrow 2$：$f(X) = X^m - 1$ の根を考えるとこれは 1 の m 乗根である．微分 $f'(X) = mX^{m-1}$ は仮定より 0 でない．よって f は分離多項式であり，$f(X)$ の根全体の集合を G とおくと G は位数 m の群である．$d \mid m$ となる整数 d に対して，位数が d の G の部分群 H の個数を考える．このような H が存在すると仮定して，H の任意の元 a はフェルマーの小定理より $a^d = 1$ である．すなわち $g(X) = X^d - 1$ の根である．位数 d の異なる部分群 H' を考えてもやはり $g(X)$ の根となることから H の取り方は高々一通りしかなく，すなわち G は位数 m の巡回群である． □

定理 1.3. F を任意の体，$\overline{F}$ を F の代数的閉包とする．$\zeta_m \in \overline{F}$ を 1 の原始 m 乗根とすれば，$F(\zeta_m)/F$ はアーベル拡大であり，$\mathrm{Gal}(F(\zeta_m)/F) \subset (\mathbb{Z}/m\mathbb{Z})^\times$ が成り立つ．

証明. ζ_m は分離的であることから $F(\zeta_m)/F$ は分離拡大である．ζ_m の最小多項式の根全体が $\langle \zeta_m \rangle$ であることから正規拡大であることもわかり，$F(\zeta_m)/F$ はガロア拡大である． □