



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. $3 \Rightarrow 2$ □