応用数理概論 (2)・広域数理科学概論 (4)・応用数理特別講義 II
第 4 回 配付資料

2018 年 10 月 25 日

等分多項式

K を標数が 2 でない体，$E\colon y^2 = x^3 + Ax + B$ $(A, B \in K)$ を楕円曲線とする．

定義 4.1. $n \in \mathbb{Z}$ に対して，**等分多項式** (division polynomial) ψ_n を以下で定義する．

$$
\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \quad (n \geq 2),\\
\psi_{2n} &= \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad (n \geq 3),\\
\psi_n &= -\psi_{-n} \quad (n < 0).
\end{aligned}
$$

さらに，ϕ_n, ω_n を以下で定義する．

$$
\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1},\\
\omega_n &= \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).
\end{aligned}
$$

講義で省略する証明については，Washington [2] を参照せよ．また，体の標数が 2 の場合も含む，一般の楕円曲線の等分多項式の定義・性質は Enge [1] を参照せよ．

参考文献

[1] A. Enge, *Elliptic Curves and Their Applications to Cryptography: An Introduction*, Kluwer Academic Publishers, 1999.

[2] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., Chapman & Hall/CRC, 2008.