楕

円曲線楕円曲線の定義

楕

円曲線とは,一般的に

$$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in F_q)$$

で与えられる(x, y)に関する方程式のことである.係数a_nが属する体F_qを係数体,変数x, yが属する体を定義体と呼ぶ.このとき、