Frobenius morphism

Canonical name	FrobeniusMorphism
Date of creation	2013-03-22 13:51:45
Last modified on	2013-03-22 13:51:45
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	4
Author	alozano (2414)
Entry type	Definition
Classification	msc 14H37
Related topic	FrobeniusAutomorphism
Related topic	FrobeniusMap
Related topic	ArithmeticOfEllipticCurves
Defines	Frobenius morphism

Let K be a field of characteristic $p > 0$ and let $q = p^r$. Let C be a curve defined over K contained in $\mathbb{P}^N$, the projective space of dimension N. Define the homogeneous ideal of C to be (the ideal generated by):

$$I(C) = \{f \in K[X_0, ..., X_N] \mid \forall P \in C, \quad f(P) = 0, \quad f \text{ is homogeneous}\}$$

For $f \in K[X_0, ..., X_N]$, of the form $f = \sum_i a_i X_0^{i_0} ... X_N^{i_N}$ we define $f^{(q)} = \sum_i a_i^q X_0^{i_0} ... X_N^{i_N}$. We define a new curve $C^{(q)}$ as the zero set of the ideal (generated by):

$$I(C^{(q)}) = \{f^{(q)} \mid f \in I(C)\}$$

Definition 1. *The q^{th}-power Frobenius morphism is defined to be:*

$$\phi \colon C \to C^{(q)}$$

$$\phi([x_0, ..., x_N]) = [x_0^q, ... x_N^q]$$

In order to check that the Frobenius morphism is well defined we need to prove that

$$P = [x_0, ..., x_N] \in C \Rightarrow \phi(P) = [x_0^q, ... x_N^q] \in C^{(q)}$$

This is equivalent to proving that for any $g \in I(C^{(q)})$ we have $g(\phi(P)) = 0$. Without loss of generality we can assume that g is a generator of $I(C^{(q)})$, i.e. g is of the form $g = f^{(q)}$ for some $f \in I(C)$. Then:

$$\begin{aligned} g(\phi(P)) = f^{(q)}(\phi(P)) &= f^{(q)}([x_0^q, ..., x_N^q]) \\ &= (f([x_0, ..., x_N]))^q, \quad [a^q + b^q = (a+b)^q \text{in characteristic } p] \\ &= (f(P))^q \\ &= 0, \quad [P \in C, f \in I(C)] \end{aligned}$$

as desired.

Example: Suppose E is an elliptic curve defined over $K = \mathbb{F}_q$, the field of p^r elements. In this case the Frobenius map is an automorphism of K, therefore

$$E = E^{(q)}$$

Hence the Frobenius morphism is an endomorphism (or isogeny) of the elliptic curve.

References

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.