Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 4

13/03/2012

1. This exercise checks the Leibniz rule for the formal derivative of a polynomial. Let K be a field. The formal derivative of $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ is defined as $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1}$.

   Let now $f(X), g(X) \in K[X]$ and set $h(X) = f(X)g(X)$. Show:

   $$h'(X) = f'(X)g(X) + f(X)g'(X).$$

2. Let K be a finite field with p^n elements.

   (a) Prove $(\alpha + \beta)^p = \alpha^p + \beta^p$ for all $\alpha, \beta \in K$.

   (b) Conclude from (a): $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ for all $d \in \mathbb{N}$.

   (c) Prove that the map

   $$F : K \to K, \quad x \mapsto x^p$$

   defines a field isomorphism, the so-called *Frobenius isomorphism*.

   (d) Compute the order of F.

   (e) Let $1 \leq d \leq n$ and let $F^d = \underbrace{F \circ F \circ \cdots \circ F}_{d \text{ times}}$. Show that the set $K^{\langle F^d \rangle} := \{x \in K \mid F^d(x) = x\}$ is a subfield of K and compute the number of elements of $K^{\langle F^d \rangle}$.