Homework set 14

Hilbert's tenth problem seminar, Fall 2013, due January 14th

By Niels Voorneveld

Exercise 1:
We are in the field $\mathbb{F}_q[Z]$. Remember that $\mathcal{M}$ consists of triples (F, w, s) with s a q-th power, $w \leq s$ and $F = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}$ where d some natural number and all $a_{ij} \epsilon \mathbb{F}_q$.
Remember that $\theta : \mathcal{M} \to \mathbb{F}_q[V, W]$ sends $(\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}, w, s)$ to $\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} V^i W^j$.

Let $(F_1, w, s), (F_2, w, s) \epsilon \mathcal{M}$.
a) Prove that $\theta(F_1, w, s) + \theta(F_2, w, s) = \theta(F_1 + F_2, w, s)$

b) Prove that if $2w \leq s$, $\theta(F_1, w, s) \cdot \theta(F_2, w, s) = \theta(F_1 F_2, 2w, s)$

Exercise 2:
a) Prove that the following function:
$\delta : \mathbb{F}_q[Z] \times \mathbb{F}_q[Z] \to \mathbb{F}_q[Z]$, $(A, B) \mapsto A^p Z + B^p$ is injective.

b) Knowing that any r.e. subset of $\mathbb{F}_q[Z]$ is diophantine in $\mathbb{F}_q[Z]$, prove that any r.e. subset of $\mathbb{F}_q[Z]^k$ for some $k > 1$ is diophantine in $\mathbb{F}_q[Z]$.

Exercise 3:
Take $\mathbb{F}$ to be a recursive infinite algebraic extension of the field $\mathbb{F}_p$, with p some prime. Take q a power of p. Take $X \epsilon \mathbb{F}[Z]$ and assume the following:

$(\exists a, b, u) : X \epsilon \mathcal{A}_u$
$\wedge q^a > u \wedge q^b > u \wedge gcd(a, b) = 1$
$\wedge X^{q^a} \equiv X \pmod{Z^{q^a} - Z}$
$\wedge X^{q^b} \equiv X \pmod{Z^{q^b} - Z}$

Remember from the lecture that if $X \epsilon \mathcal{A}_u$ than $deg(X) \leq u$.

Prove that $X \epsilon \mathbb{F}_q[Z]$
(Hint, remember last week's hand-in exercise).