Seminar Hilbert 10 - Homework 13

Eric Faber

Due January 6

In these exercises, p is a prime and q a power of p.

Exercise 1 Prove that for all n, m:

$$\mathbb{F}_{q^n} \cap \mathbb{F}_{q^m} = \mathbb{F}_{q^{\gcd(n,m)}}$$

Exercise 2 Recall that we used the following Diophantine predicate to bound degrees and quantify over $\mathbb{F}_q[Z]$ only:

$$\beta(X, e) \iff X = 0 \vee (X | Z^{q^{2e}} - Z^{q^e})$$

which is equivalent to

$$\beta(X, e) \iff X^2 | (Z^{q^{2e}} - Z^{q^e})X.$$

We want to prove that for every $X \in \mathbb{F}_q[Z]$, there is e such that $\beta(X, e)$.

Define the *radical* of X to be the biggest square-free divisor of X.

(a) Show that for $X \neq 0$, and Y the radical of X, there exists $c \in \mathbb{N}$ such that

$$X | Y^c.$$

(b) Let $\mathbb{F}_{q^d}$ be the splitting field of Y, for some d. Show that $Y | Z^{q^e} - Z$ for all e such that $d | e$.

(c) Show that there exists e such that $X | Z^{q^{2e}} - Z^{q^e}$.

Exercise 3 In this exercise, we will prove that the irreducible factors of Φ_a in $\mathbb{F}_q[Z]$ have degree $\operatorname{ord}(q \bmod a)$, where $\operatorname{ord}(q \bmod a)$ is the order of q in $(\mathbb{Z}/a\mathbb{Z})^*$. We assume that a is prime to p, so that in fact $q \in (\mathbb{Z}/a\mathbb{Z})^*$. Recall that

$$\Phi_a(Z) = \prod_{k \in (\mathbb{Z}/a\mathbb{Z})^*} (Z - \zeta_a^k)$$

where ζ_a is a primitive $a-$th root of unity, i.e. a generator of the group of $a-$th roots of unity under multiplication.

We know that $\Phi_a(Z)$ has integer coefficients, so we can view it as an element of $\mathbb{F}_q[Z]$.

(a) Show that $\zeta_a \in \mathbb{F}_{q^k}$ if and only if $q^k \equiv 1 \pmod{a}$.

(b) Conclude that for $\Psi_a(Z)$ an irreducible factor of $\Phi_a(Z)$ in $\mathbb{F}_q[Z]$,

$$\mathbb{F}_q[Z]/(\Psi_a(Z)) \cong \mathbb{F}_{q^{\operatorname{ord}(q \bmod a)}}$$

and that therefore $\deg \Psi_a(Z) = \operatorname{ord}(q \bmod a)$.