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:

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

Solution. We first prove that $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^n}$ if and only if $s|n$. We have seen that $s|n$ if and only if $q^s - 1|q^n - 1$.

If $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^n}$, then $(\mathbb{F}_{q^s})^* < (\mathbb{F}_{q^n})^*$ so $q^s - 1|q^n - 1$, hence $s|n$.

If $s|n$, then for all $\alpha \in \mathbb{F}_{q^s}$ nonzero, $\alpha^{q^n-1} - 1 = \alpha^{q^s-1} - 1 = 0$. So $\alpha \in \mathbb{F}_{q^n}$.

It is now easy to see that $\mathbb{F}_{q^n} \cap \mathbb{F}_{q^m} = \mathbb{F}_{q^s}$ where s is the largest such that $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^m}$. Therefore $s = \gcd(n, m)$. □

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 $X|Z^{q^{2e}} - Z^{q^e}$.

Solution. (a) We split X in its roots:

$$X = \chi \prod_{i=1}^{n} (X - \alpha_i)^{r_i}$$

where the α_i are all distinct, the $r_i \geq 1$ natural numbers and $\chi \in \mathbb{F}_q$ is some scalar. Now $Y = \prod_{i=1}^{n}(X - \alpha_i)$ is the radical of X, and clearly

$$X|Y^c$$

for $c = \max\{r_1, \ldots, r_n\}$.

(b) Let $\mathbb{F}_{q^d}$ be a field containing all roots of Y. Every element of $\mathbb{F}_{q^d}$ is a root of $Z^{q^d} - Z$, so since Y is square-free:

$$Y = \prod_{i=1}^{n}(Z - \alpha_i)|Z^{q^d} - Z.$$

We had already seen that $d|e$ if and only if $Z^{q^d} - Z|Z^{q^e} - Z$, which shows that for all such e

$$Y|Z^{q^e} - Z$$

over $\mathbb{F}_{q^d}[Z]$.

(c) Let e be such that $d|e$ and $q^e \geq c$. Then:

$$X|Y^c|Y^{q^e}|(Z^{q^e} - Z)^{q^e} = Z^{2q^e} - Z^{q^e}.$$

It follows that $X|Z^{2q^e} - Z^{q^e}$ over $\mathbb{F}_q[Z]$.

□

Exercise 3 In this exercise, we will prove that the irreducible factors of Φ_a in $\mathbb{F}_q[Z]$ have degree $\mathrm{ord}(q \bmod a)$, where $\mathrm{ord}(q \bmod a)$ 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 $\mathbb{F}_q[Z]$,

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

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

Solution. (a) Since ζ_a is a primitive $a-$th root of unity, $\zeta_a^r = 1$ if and only if $a|r$. Hence $\zeta_a \in \mathbb{F}_{q^k}$ if and only if $a|q^k - 1$, which holds if and only if $q^k \equiv 1 \pmod a$.

(b) We know that $\mathbb{F}_q[Z]/(\Psi_a(Z))$ is a vector space over $\mathbb{F}_q$ of dimension $\deg \Psi_a(Z)$, hence

$$\mathbb{F}_q[Z]/(\Psi_a(Z)) \cong \mathbb{F}_{q^{\deg \Psi_a(Z)}}$$

On the other hand, $\zeta_a \in \mathbb{F}_q[Z]/(\Psi_a(Z))$ since $\Psi_a(Z)$ has only primitive roots as zeros. It follows from (a) that $q^{\deg \Psi_a(Z)} \equiv 1 \pmod a$. Since $\Psi_a(Z)$ splits in any field $\mathbb{F}_{q^k}$ for which $\zeta_a \in \mathbb{F}_{q^k}$, the splitting field $\mathbb{F}_q[Z]/(\Psi_a(Z))$ is the smallest such that $\zeta_a \in \mathbb{F}_q[Z]/(\Psi_a(Z))$, so $\deg \Psi_a(Z) = k$ where k is the smallest (nonzero) such that $q^k \equiv 1 \pmod a$, hence $\deg \Psi_a(Z) = \mathrm{ord}(q \bmod a)$.

□