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

**Exercise 1** Prove that for all $n, m$:

$$F_{q^n} \cap F_{q^m} = F_{q^\gcd(n,m)}$$

**Solution.** We first prove that $F_{q^n} \subseteq F_{q^m}$ if and only if $s|n$. We have seen that $s|n$ if and only if $q^s - 1|q^n - 1$.

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

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

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

**Exercise 2** Recall that we used the following Diophantine predicate to bound degrees and quantify over $F_q[Z]$ only:

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

which is equivalent to

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

We want to prove that for every $X \in F_q[Z]$, 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 $F_{q^d}$ 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 $\alpha_i$ are all distinct, the $r_i \geq 1$ natural numbers and $\chi \in F_q$ is some scalar. Now $Y = \prod_{i=1}^n (X - \alpha_i)$ is the radical of $X$, and clearly

$$X|Y^c$$

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

1
(b) Let $F_{q^d}$ be a field containing all roots of $Y$. Every element of $F_{q^d}$ 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 $e$

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

over $F_{q^d}[Z]$.

(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 $F_q[Z]$.

Exercise 3 In this exercise, we will prove that the irreducible factors of $\Phi_a$ in $F_q[Z]$ have degree $\text{ord}(q \mod a)$, where $\text{ord}(q \mod a)$ is the order of $q$ in $(\mathbb{Z}/a\mathbb{Z})^\times$. We assume that $a$ is prime to $p$, so that in fact $q \in (\mathbb{Z}/a\mathbb{Z})^\times$. Recall that $\Phi_a(Z) = \prod_{k \in (\mathbb{Z}/a\mathbb{Z})^\times} (Z - \zeta_a^k)$

where $\zeta_a$ 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 $F_q[Z]$.

(a) Show that $\zeta_a \in F_{q^k}$ 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 $F_q[Z]$,

$$F_q[Z]/(\Psi_a(Z)) \cong F_{q^{\text{ord}(q \mod a)}}$$

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

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

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

$$F_q[Z]/(\Psi_a(Z)) \cong F_{q^{\text{deg} \Psi_a(Z)}}$$

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

□