Exercise 1. Construction of $F_{16}$

1. Let $\alpha$ be a root of $X^4 + X + 1$. Compute all successive powers of $\alpha$. Is $\alpha$ a primitive element in $F_{16}$?
2. Compute $\alpha^7 \times \alpha^{11}$ and $\alpha^7 + \alpha^{11}$ in $F_{16}$.
3. Determine all non-trivial multiplicative subgroups of $F_{16}^*$.
4. Determine the order of each element in $F_{16}$.
5. Compute the minimal polynomials of $\alpha$, of $\alpha^5$, of $\alpha^3$ and of $\alpha^7$.
6. Let $\beta$ be a root of $X^4 + X^3 + X^2 + X + 1$. Is the set $\{1, \beta, \beta^2, \beta^3\}$ a basis of $F_{16}$ over $F_2$?

Exercise 2. Power mappings over $F_{2^m}$

1. Let $s > 0$ be an integer. When does $F_s : x \mapsto x^s$ permute the field $F_{2^m}$?
2. When $F_s$ is a permutation, determine its inverse.
3. When does $F_3 : x \mapsto x^3$ permute $F_{2^m}$?
4. Determine the inverse of $x \mapsto x^{2^m-1}$ on $F_{2^m}$.

Exercise 3. Trace function

Let $q$ be a power of a prime number, and let $m > 0$ be an integer. The Trace mapping from $F_{q^m}$ into $F_q$ is defined by

$$\text{Tr}_{F_{q^m}/F_q}(x) = \sum_{i=0}^{m-1} x^{q^i}, \ x \in F_{q^m}.$$ 

1. Prove that $\text{Tr}_{F_{q^m}/F_q}(x^q) = \text{Tr}_{F_{q^m}/F_q}(x)$ for all $x \in F_{q^m}$.
2. Prove that $\text{Tr}_{F_{q^m}/F_q}$ takes its values in $F_q$.
3. Prove that $\text{Tr}_{F_{q^m}/F_q}$ is a linear function when $F_{q^m}$ is seen as a vector space over $F_q$.
4. Compute $\text{Tr}_{F_{q^m}/F_q}(x)$ when $x \in F_q$. Deduce the value of $\text{Tr}_{F_{2^m}/F_2}(1)$.

Exercise 4. Equations of degree 2 in $F_{2^m}$

1. Determine the number of solutions in $F_{2^m}$ of

$$aX^2 + bX + c = 0,$$

where $a$, $b$ and $c$ are three elements in $F_{2^m}$, $a \neq 0$.

[Hint: When $b \neq 0$, the problem boils down to solving $X^2 + X + d$.]

2. Let $\alpha \in F_{2^m}$ and

$$\theta = c\alpha^2 + (c + c^2)\alpha^4 + \ldots + (c + c^2 + c^4 + \ldots + c^{2^{m-2}})\alpha^{2^{m-1}}.$$ 

Prove that, if $\text{Tr}_{F_{2^m}/F_2}(\alpha) = 1$, then $\theta$ is a root of $X^2 + X + c$.

Deduce a simple expression of the solutions of $X^2 + X + c$ in $F_{2^m}$, when $m$ is odd.
Exercise 5. Polynomials with coefficients in a subfield
Let $K$ be a finite field with characteristic $p$ and $P$ be a polynomial in $K[X]$. Prove that $P(X^p) = (P(X))^p$ if and only if the coefficients of $P$ lie in $F_p$. 