INF 240 - Exercise problems - 8

Nikolay Kaleyski

Recall that if $F = \mathbb{F}_{q^m}$ is an extension field of $K = \mathbb{F}_q$, then for any $a \in F$, its *conjugates with respect to* K are the elements a, a^q, a^{q^2}, $\ldots$, $q^{q^{m-1}}$. The conjugates of an element a behave "similarly" to a in some respects: see 2.14, 2.18, and 2.19 for some properties of the conjugates.

The sum of all the conjugates of an element $a \in F$ with respect to K is the value of the *trace function* $\mathrm{Tr}_{F/K}(a)$. The trace of an element is an important property which has many applications in theory and practice. Here is just one example: showing that some equation $f(x) = g(x)$ has no solution $x \in F$ is usually a difficult problem, especially if the number of elements in F is very large (or unknown); however, sometimes it is possible to show that, say, $\mathrm{Tr}_{F/K}(f(x)) = 0$ for any $x \in F$ but $\mathrm{Tr}_{F/K}(g(x))$ is always non-zero; this then immediately shows that the equation $f(x) = g(x)$ is not solvable. The definition and properties of the trace function are given in 2.22, 2.23, 2.26.

Recall also that an extension $F = \mathbb{F}_{q^m}$ of $K = \mathbb{F}_q$ can be seen as an m-dimensional vector space over K; in other words, every element $a \in F$ can be written as an m-tuple $a = (a_1, a_2, \ldots, a_m)$ of elements $a_i \in K$. Since F is a vector space in this respect, it also has a *basis* $(B_1, B_2, \ldots, B_m)$, i.e. a collection of elements $B_i \in F$ such that any element A of F can be written as a linear combination $A = c_1B_1 + c_2B_2 + \cdots + c_mB_m$ for $c_i \in K$. A vector space (and hence an extension field) can have many different bases in general, and we define three special types of bases: dual and self-dual bases, polynomial bases, and normal bases. See 2.30, 2.32 for more details.

Exercise 1. *Consider the extension field* $\mathbb{F}_{2^3} = \{\alpha^2 + c_1\alpha + c_0 : c_1, c_0 \in \mathbb{F}_2\}$ *where* α *is a root of the irreducible polynomial* $p(x) = x^3 + x + 1$ *in* $\mathbb{F}_2$.

1. *Find the conjugates with respect to* $\mathbb{F}_2$ *of the elements* $a = \alpha^2 + \alpha$, $b = 1$ *and* $c = \alpha + 1$;
2. *Find all primitive elements of* $\mathbb{F}_{2^3}$;
3. *Compute the absolute traces* $\mathrm{Tr}(\alpha^2 + \alpha)$, $\mathrm{Tr}(1)$, *and* $\mathrm{Tr}(\alpha + 1)$;
4. *Using the properties of the trace function in Theorem 2.23, show that for any* $x \in \mathbb{F}_{2^3}$, *we have* $\mathrm{Tr}(x^2 + x) = 0$;
5. *Show that the equation* $x^2 + x + \alpha^2 + 1 = 0$ *has no solution* $x \in \mathbb{F}_{2^3}$.

Exercise 2. *Assume the setting of Example 2.31, i.e. consider* $\mathbb{F}_{2^3}$ *as constructed via the irreducible polynomial* $q(x) = x^3 + x^2 + 1$ *in* $\mathbb{F}_2$. *Verify that* $(\alpha, \alpha^2, 1 + \alpha + \alpha^2)$ *is indeed a self-dual basis of* $\mathbb{F}_{2^3}$ *over* $\mathbb{F}_2$.

Exercise 3. *Consider the polynomial* $f(x) = x^3 + 2x + 1$ *in* $\mathbb{F}_3$.

1. *Is $f(x)$ irreducible in $\mathbb{F}_3$?*

2. *Is $f(x)$ irreducible in $\mathbb{F}_{3^2}$? What about $\mathbb{F}_{3^6}$? What about $\mathbb{F}_{3^8}$?*

3. *What are all natural numbers m for which $f(x)$ is irreducible in $\mathbb{F}_{3^m}$?*

Exercise 4. *Find an irreducible polynomial of degree 3 in $\mathbb{F}_{3^{25}}$.*

Exercise 5. *Show that the absolute trace $\mathrm{Tr} : \mathbb{F}_{3^k} \to \mathbb{F}_3$ satisfies $\mathrm{Tr}(a^9 + b + 2b^3) = \mathrm{Tr}(a)$ for any $a, b \in \mathbb{F}_{3^k}$.*

The following exercises are taken from Lidl & Niederreiter's *Finite fields*.

Exercise 6. *Show that any polynomial of degree 2 in $\mathbb{F}_q[x]$ splits into linear factors over $\mathbb{F}_{q^2}$.*

Exercise 7. *Find all automorphisms of a finite field.*

Exercise 8. *Let F be a finite extension of the finite field K of characteristic p. Show that $\mathrm{Tr}_{F/K}(a^{p^n}) = (\mathrm{Tr}_{F/K}(a))^{p^n}$ for any $a \in F$ and any natural number n.*

Exercise 9. *Show that if $(a_1, \ldots, a_m)$ is a basis of $F = \mathbb{F}_{q^m}$ over $K = \mathbb{F}_q$, then $\mathrm{Tr}_{F/K}(a_i) \neq 0$ for at least one i among $1 \leq i \leq m$.*