INF 240 - Exercise problems - Structure of finite fields

Nikolay Kaleyski

Exercise 1. *Construct the finite field* $\mathbb{F}_{16}$ *as an extension of* $\mathbb{F}_2$ *by adjoining a root* α *of the irreducible polynomial* $f(x) = x^4+x+1$. *Evaluate* $g(x) = x^3+\alpha x+1$ *at* 1, *at* $\alpha^2+\alpha$, *and at* $\alpha^3+\alpha+1$, *i.e. compute:*

1. $f(1)$;
2. $f(\alpha^2+\alpha)$;
3. $f(\alpha^3+\alpha+1)$.

Exercise 2. *Consider the polynomials* $f(x) = x^2+2$ *and* $g(x) = x^2+4x+2$ *over* $\mathbb{F}_5$. *One of them is primitive, while the other is not; determine which is which.*

Exercise 3. *Consider the polynomial* $f(x) = x^3+6x^2+4$ *over* $\mathbb{F}_7$.

1. *Verify that* f *is irreducible over* $\mathbb{F}_7$;
2. *find all* k *such that* f *remains irreducible over* $\mathbb{F}_{7^k}$;
3. *find all* k *such that* f *has roots in* $\mathbb{F}_{7^k}$.

Exercise 4. *Find all irreducible polynomials of degree* 3 *over* $\mathbb{F}_3$.

Exercise 5. *Consider the finite field* $\mathbb{F}_{2^6}$ *constructed by adjoining a root* α *of* $f(x) = x^6+x^4+x^3+x+1$ *to* $\mathbb{F}_2$. *Compute the absolute trace of the elements* $\alpha+1$, $\alpha^5+\alpha^2+1$ *and* $\alpha^3+\alpha^2+\alpha$.

Exercise 6. *Consider the finite field* $\mathbb{F}_{27}$ *obtained by adjoining a root* α *of the irreducible polynomial* x^3+2x+1 *to* $\mathbb{F}_3$. *Show that the equation*

$$x^2 - x^6 = 2\alpha^2 + 1$$

has no solutions in $\mathbb{F}_{27}$.

Hint: apply the absolute trace to both sides of the equation.

Exercise 7. *Consider the finite field* $\mathbb{F}_q$ *with* $q = 5^{12}$. *Find all subfields of* $\mathbb{F}_q$.

Exercise 8. *Suppose* α *is a primitive element of* $\mathbb{F}_{25}$. *Find all primitive elements of* $\mathbb{F}_{25}$, *i.e. determine all* i *such that* α^i *is a primitive element of* $\mathbb{F}_{25}$.