Hints for Project 2 Home Exercise 1.3

Paul Stankovski

Determine whether the polynomial

$$p(x) = x^2 + \alpha^5 x + 1 \tag{1}$$

is primitive, irreducible or reducible over $\mathbb{F}_{2^4}$, where $\alpha^4 + \alpha + 1 = 0$.

Note that α^5, the coefficient of x above, is an element of $\mathbb{F}_{2^4}$. In this exercise we have $q = 2^4$, which is nowhere near being a prime number, so we cannot simply identify $\mathbb{F}_q$ with the integers modulo 16. But we need to know how to calculate with these elements, so what do we do?

Construct the group. Write a multiplication table. The elements of $\mathbb{F}_{2^4}$ can be viewed as polynomials (use variable y) over $\mathbb{F}_2$ taken modulo some irreducible polynomial $\pi(y)$ of degree 4. This is denoted $\mathbb{F}_2[y]/(\pi(y))$. Check your lecture notes for how to write a multiplication table for $\mathbb{F}_{2^4}$.

So, yes, if you are wondering, what you have in Eq. (1) is really a polynomial with polynomial coefficients.

We are given a hint. Letting

$$\pi(y) = y^4 + y + 1,$$

the element α is such that $\pi(\alpha) = 0$ (is π irreducible?). If $\pi(y)$ is primitive, then α generates the multiplicative group $\mathbb{F}_{2^4}^*$, which contains $2^4 - 1 = 15$ elements (all elements of $\mathbb{F}_{2^4}$ except the zero element). In other words, if $\pi(y)$ is primitive, every nonzero element can be written as α^i for $0 \leq i \leq 14$, with $\alpha^0 = \alpha^{15} = 1$.

If $\pi(y)$ primitive? Is it possible to write $p(x) = (x - \alpha^i)(x - \alpha^j)$ for some i and j? Can you show that $p(\alpha^i) = 0$ for some i?