Coding and Cryptography Fall 2016
Worksheet on finite fields

Katherine E. Stange

October 24, 2016

We will study the set $\mathbb{F}_4$ of polynomials in X with coefficients modulo 2, considered modulo $X^2 + X + 1$.

1. For example, in this world,
$$X^2 = X + 1.$$
Explain why.

2. List all the elements of $\mathbb{F}_4$.

3. Determine the full addition and multiplication tables of $\mathbb{F}_4$.

4. Write a substraction and division table for $\mathbb{F}_4$. You can put "not defined" when division is not possible.

5. By looking at the tables you've created, verify whether or not the following properties hold:
   (a) There is an element e_A which satisfies $a + e_A = a$ for all a. What is it?
   (b) There is an element e_M which satsifies $ae_M = a$ for all a. What is it?
   (c) The elements e_A and e_M are distinct.
   (d) For each a, there is an element a'_A satisfying $a + a'_A = e_A$. Explain.
   (e) For each non-zero a, there is an element a'_M satisfying $aa'_M = e_M$. Explain.
   (f) Addition is associative (give an example of this property).
   (g) Multiplication is associative (give an example of this property).
   (h) Addition is commutative (give an example of this property).
   (i) Multiplication is commutative (give an example of this property).
   (j) Multiplication distributes over addition (give an example of this property).

6. The fact that $\mathbb{F}_4$ satisfies the above axioms shows it is a field. It is a field of four elements. Can you construct a field of 9 elements? What sizes are possible by this method?