Finite Fields

Andrew Lin

12/8/15

1 Existence and Construction

A finite field is defined as a field with a finite number of elements. The *order* of the field is the number of elements it contains. We denote F_n as a field with order n.

To determine the order of a field, let us consider the subfield generated by 1, the multiplicative identity. Since the field has finite order, this subfield must have finite order, and it is isomorphic to Z/nZ. However, since this is a field and every non-zero element has a multiplicative inverse, it must be isomorphic to Z/pZ. To extend this to higher powers, we can use linear algebra, but that will be omitted here.

There are two ways to construct a field with order $n = p^m$. The first is to use polynomials with coefficients in Z/pZ, modulo an irreducible polynomial of degree m. Alternatively, adjoin a root of this irreducible polynomial to Z/pZ.

For example, a field of order $8 = 2^3$, written as F_8 can be represented in two ways:

1) quadratic polynomials with coefficients of 0 or 1, mod an irreducible cubic (for example, $x^3 + x + 1$)

2) $Z/2Z(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$.

2 Structure

2.1 Multiplicative group

The multiplicative group is $F^* = F - (0)$, which has $n-1$ elements (because there are n elements in the field).

Consider the element with the largest order in the group, m. Then consider the polynomial $x^m - x$. Since $x^m = x$ for all elements, there are $n - 1$ roots of the polynomial. Since there is unique factorization, the number of roots must be less than the degree of the polynomial, so $n - 1 \leq m$. However, the order of an element can't be more than the number of elements in the group, so $m \leq n - 1$, and they are equal. Therefore, the multiplicative group is cyclic!

An example of this would be $Z/13Z$. There must be a primitive element with order 12; in this case, 2 is one of them.

In other words, the multiplicative group of F_n is isomorphic to $Z/(n-1)Z$. This also tells us that F_n is a splitting field of $x^n - x$.

2.2 Subfields and Isomorphism

We have just proved that all fields of the same size are splitting fields of the same polynomial. Therefore, all fields of the same order are isomorphic to each other! This is basically because the polynomial keeps the structure of the field structured enough: the cyclic nature, characteristic p, etc.

Therefore, we can find an easy way to describe subfields: F_{p^m} is a subfield of F_{p^n} if $x^{(p^m)} - x | x^{(p^n)} - x$. Algebraically, this means $p^m - 1$ divides $p^n - 1$. This only happens when m divides n (because of factoring).