Galois New Section 5 (f) PhL 7.1.13

The old section (f) is preserved at the end of this doc under **********
The new section (f) has been installed in Galois doc.

(f) Selecting f(x) for GF(q) = R/(f(x)) and the Classification of Irreducible Polynomials

In Chapter 3 we were able to construct a representation of GF(p^m) by starting with any irreducible polynomial of degree m, q = p^m. We made the identification:

GF(p^m) = R/(f(x)) . // irreducible f(x) is of degree m *(3.17)*

As our GF(2^4) example above shows, even when p=2, there are typically many candidates for f(x), all of which give an equivalent representation of GF(p^m). Moreover, for p>2, every candidate has p-2 shadow candidates which are just scale factor multiples of f(x).

By our definition, a primitive polynomial is monic and so the shadow candidates are eliminated. Since a primitive polynomial of degree m is irreducible, it can serve as an f(x) in the construction of GF(p^m) as the extension field over GF(p). However, it is not necessary to use a primitive polynomial to accomplish the construction. As we shall see in the next chapter, there is a great *advantage* to using a primitive polynomial for this purpose.

We now look into the classification of the irreducible polynomials of GF(q). We start with:

Fact 13: If monic irreducible f(x) is used to construct a representation of GF(q), then f(x) is a minimum polynomial of GF(q) in that representation. Since all representations of GF(q) are equivalent, f(x) is a minimum polynomial of GF(q). (5.33)

Proof: In Fact 1 (6.5) we will show that α = {x} is a root of any degree-m polynomial f(x) used to construct a residue class ring representation of GF(q). Since this α = {x} is an element of GF(q) and is a root of f(x), we can apply Fact 3 (5.6) to conclude that f(x) is a minimum polynomial.

Fact 14:

(a) If monic irreducible f(x) is of degree m, then it is a minimum polynomial for GF(p^m)

(b) If monic irreducible f(x) is not a minimum polynomial for GF(p^m), it must have degree < m.

(5.34)

These are corollaries to Fact 15. If monic irreducible f(x) has degree m, it can be used in GF(q) = R/(f(x)) and it is therefore a minimum polynomial of GF(q). Then (b) is the contrapositive of (a).

Using Fact 14, we can now draw a picture to classify all monic irreducible polynomials of GF(q).

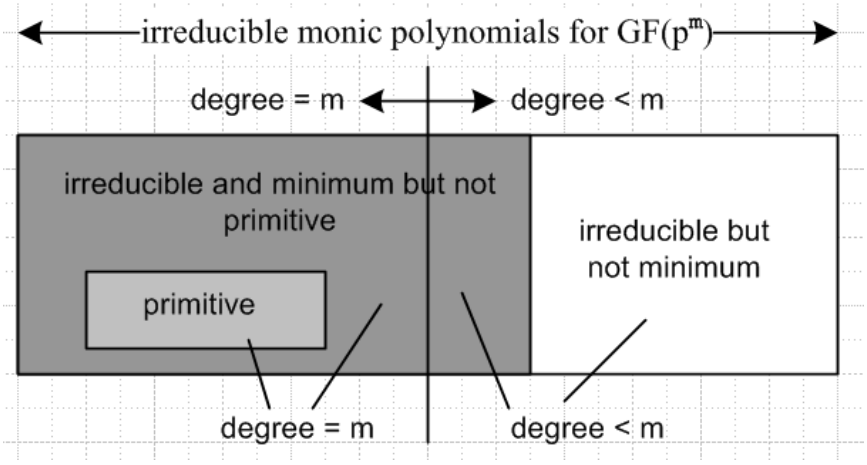

Fig 5.5

Note that minimum polynomials could be in either side of the drawing.

An example for the white region on the right is on the right is $1 + x + x^3$ for GF(2^4)

Non-monic polynomials can always be written as multiples of monic polynomials and can then be classified by the resulting monic polynomial. For example, in GF(5^m) we would have

$(2 + x + 3x^3) = 2(1 + 3x + 4x^3)$ since $2 \bullet 3 = 6 = 1$ and $2 \bullet 4 = 8 = 3$

********** old section 5 (f) **********

(f) Selecting f(x) for construction of GF(p^m) = R/(f(x))

In Chapter 3 we were able to construct a representation of GF(p^m) by starting with any irreducible polynomial of degree m, $q = p^m$. We made the identification:

GF(p^m) = R/(f(x)) // irreducible f(x) is of degree m *(3.17)*

As our GF(2^4) example above shows, even when p=2, there are typically many candidates for f(x), all of which give an equivalent representation of GF(p^m). Moreover, for p>2, every candidate has p-2 shadow candidates which are just scale factor multiples of f(x).

By our definition, a primitive polynomial is monic and so the shadow candidates are eliminated. Since a primitive polynomial of degree m is irreducible, it can serve as an f(x) in the construction of GF(p^m) as the extension field over GF(p). However, it is not necessary to use a primitive polynomial to accomplish the construction. As we shall see in the next chapter, there is a great *advantage* to using a primitive polynomial for this purpose. As a reminder, then:

Fact 13:

- Not all monic irreducible polynomials over GF(p) are primitive polynomials.
- Not all monic irreducible polynomials over GF(p) are minimum polynomials. (5.33)

We saw examples of both these statements in the discussion above following (5.31).

The following two facts are a bit out of order in their appearance here, but we felt they should be stated somewhere. The first is a stronger version of Fact 3 (5.6).

Fact 14: If monic irreducible f(x) is used to construct a representation of GF(q), then f(x) is a minimum polynomial of GF(q) in that representation. (5.34)

Proof: In the next chapter we will show that $\alpha = \{x\}$ is a root of any degree-m polynomial f(x) used to construct a residue class ring representation of GF(q). Since this $\alpha = \{x\}$ is an element of GF(q) and is a root of f(x), we can apply Fact 3 (5.6) to conclude that f(x) is a minimum polynomial.