BCH questions PhL 1.21.13

All this material has been incorporated into Galois doc, Chapter 5 (g)

Consider the set of roots of g(x) { α, α^2 , α^3, ...α^N }. Each of these powers has a minimum polynomial $m_i(x)$.

Question #1: Can the same root "a" appear in two different minimum polynomials? For example

$m_1(x) = (x-a)(x-b)$
$m_2(x) = (x-a)(x-c)(x-d)$

Answer: We know exactly the roots in for any min poly from our formula. They are the distinct members of this set of m elements.

$$\{ \alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, ... \alpha^{p^{m-1}} \}$$

This we know that the number of elements in the conjugate set of α is $\leq$ m. If α is primitive, then the number of distinct elements is exactly m by (5.15). We do have α = primitive. The general min poly formula is for any α is

$$m(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \quad . \qquad (5.17)$$

where $k \leq m$. How do you compute k ? I do know that any α has some order n. We can see from the above that

$$\alpha^{p^k - 1} = 1$$

Therefore I think this is true

n = order of α = $p^k - 1$ since then $\alpha^n = 1$ and this is the smallest power that does it.

Therefore, for α = primitive, the then we have the full list

$$m(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{m-1}}) \qquad \alpha^{p^m} = \alpha \quad . \qquad (5.17)$$

In this case, there are m distinct roots of m(x), and the order of α is $p^m - 1 = q$, all this fits together.

Subquestion. If α is primitive, is α^i also primitive? Recall

Fact 12: A power α^k of a known primitive element α of GF(q) is itself a primitive element if and only if GCD(k,q-1) = 1. (4.32)

So I guess in general I don't know whether or not α^i is also a primitive element! So I don't now the order of the min poly of α^i right now.

All I really know is this:

The order of α^i is some number $n_i = p^{ki} - 1$ for some $k_i \leq m$.
Thus, if we write out the product

Back to Question 1. Suppose two different min polys have the same root a.

$$m(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \quad . \qquad (5.17)$$

$$n(x) = (x - \beta) \bullet (x - \beta^p) \bullet (x - \beta^{p^2}) \bullet (x - \beta^{p^3}) \ldots .... (x - \beta^{p^{k'-1}}) \qquad \beta^{p^{k'}} = \beta \quad . \qquad (5.17)$$

Suppose in the first poly we have

$$\alpha^{p^i} = a$$

and in the second poly we have

$$\beta^{p^j} = a$$

Then we have (assume for now that $i \geq j$)

$$\alpha^{p^i} = \beta^{p^j}$$

$$\beta = \alpha^{[p^i/p^j]} = \alpha^{p^{i-j}}$$

Since $i-j \geq 0$, we have $\beta = \alpha$ or α^p or α^{p^2} etc. Therefore, β must be in m(x).

Pause: I suspect you can take any element in (5.17) and write it as the first element. For example

$$m(x) = (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \bullet (x - \alpha)$$

or

$$m(x) = (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \bullet (x - \alpha) \bullet (x - \alpha^p)$$

You get the same polynomial in either case. This last version can be written

$$m(x) = (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \bullet (x - \alpha^{p^k}) \bullet (x - \alpha^{p^{k+1}}) \qquad \alpha^{p^k} = \alpha$$

$$m(x) = (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \bullet (x - \alpha^{p^k}) \bullet (x - \alpha^{p^{k-1+2}}) \qquad \alpha^{p^k} = \alpha$$

In general we could I think write

$$m(x) = (x - \alpha^{p^r}) \bullet (x - \alpha^{p^{r+1}}) \ldots \ldots \ldots \bullet (x - \alpha^{p^{r+k-1}}) \qquad \alpha^{p^k} = \alpha$$

The idea is that you can pick any r you want to start the expression for m(x).

Resume: Back to m(x) and n(x) having the same root a. We found that $\beta = \alpha^{p^r}$ with r = i-j. This I think means that m(x) and n(x) are the same polynomial! That would be a major fact. Can I get verification?

Lectures on Finite Fields and Galois Rings
By Zhe-Xian Wan

google books

4.19 Prove that any two distinct monic irreducible polynomials over a field F can
not have a common root in any extension field of F. 4.20 Let F be any field

There it is! Assuming this is true, then here is what I know. If we take

$$g_N(x) = \text{LCM}[\, m_1(x)m_2(x)m_3(x)m_4(x) \ldots m_N(x)] \;=\; m_a(x)m_b(x)m_c(x)$$

Then since the min polys have no overlapping roots, we know that the order of the resulting product is less than q-1 !!

Fact 16: Any root of a minimal polynomial can be written as the first root.

Proof: Consider this generic minimum polynomial of α shown in (5.17), where k ≤ m,

$$m(x) = (x - \alpha) \bullet (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \qquad (*)$$

We can move the leftmost root to the right end and write α as α^{p^k} to get

$$m(x) = (x - \alpha^p) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \bullet (x - \alpha^{p^k})$$

Now take the left element above and move *it* to the right end

$$m(x) = (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots \ldots (x - \alpha^{p^{k-1}}) \bullet (x - \alpha^{p^k}) \bullet (x - \alpha^{p^{k+1}})$$

Since we can do this any number of times, we conclude that m(x) can be written as

$$m(x) = (x - \alpha^{p^r}) \bullet (x - \alpha^{p^{r+1}}) \ldots \ldots \ldots \bullet (x - \alpha^{p^{r+k-1}})$$

for any integer r such that α^{p^r} is in the original set of roots. This is what we mean by saying that any element of (*) can be written as the first root.

Fact 17: Two distinct minimum polynomials can have no roots in common. In other words, the elements of two distinct conjugate sets have no common elements.

Proof: Let m(x) and n(x) be two distinct minimum polynomials

$$m(x) = (x - \alpha) \bullet (x - \alpha^{p}) \bullet (x - \alpha^{p^2}) \bullet (x - \alpha^{p^3}) \ldots .... (x - \alpha^{p^{k-1}}) \qquad \alpha^{p^k} = \alpha \quad .$$

$$n(x) = (x - \beta) \bullet (x - \beta^{p}) \bullet (x - \beta^{p^2}) \bullet (x - \beta^{p^3}) \ldots .... (x - \beta^{p^{k'-1}}) \qquad \beta^{p^{k'}} = \beta \quad .$$

Our formula above for the minimal polynomial of some GF(q) field element α was,

$$\{ \alpha, \alpha^{p}, \alpha^{p^2}, \alpha^{p^3}, ... \alpha^{p^{k-1}} \} \qquad \alpha^{p^k} = \alpha \qquad \text{k conjugates} \qquad k \leq m \qquad (5.16)$$

Question: is the conjugate set a cyclic subgroup of something? This is just not obvious to me. It is not a list of sequential powers as I am used to.