Find an irreducible poly that is not a min poly. PhL 6.30.13

This led to my picture and discussion of the classification of irreducible polys of GF(q).
It is now installed in Galois doc near Fig 5.5

(1) I wrote some code to attempt to factor all polynomials for GF(2^4) which have the standard form ending in a 1. Here it is. There are 16 of interest, but the first two are trivial. Here are the possible categories

• factors into all (x-a) factors where in all factors a ≠ 1	irreducible and min poly
• factors in this way, but has at least one (x+1) factor	reducible hence not min poly
• has a single but non-linear in x factor	irreducible and not min poly
• has multiple factors with at least one non-linear	reducible hence not min poly

Search for all irredicible polys for GF(2,4)

```
> restart;
> alias(a = RootOf(z^4+z+1)):
> for n from 1 to 31 by 2 do
    c := convert(n,base,2):
    L := nops(c):
    p := sum(c[i]*x^(i-1),i=1..L):
    f := Factor(p,a) mod 2:
    print(p,"       ",f);
  od:
```

$$1,"\quad",1$$
$$1+x,"\quad",1+x$$
$$1+x^2,"\quad",(1+x)^2$$
$$1+x+x^2,"\quad",(x+a^2+a+1)(x+a^2+a)$$
$$1+x^3,"\quad",(x+a^2+a+1)(x+a^2+a)(1+x)$$
$$1+x+x^3,"\quad",1+x+x^3$$
$$1+x^2+x^3,"\quad",1+x^2+x^3$$
$$1+x+x^2+x^3,"\quad",(1+x)^3$$
$$1+x^4,"\quad",(1+x)^4$$
$$1+x+x^4,"\quad",(x+a)(x+a^2+1)(x+a^2)(x+a+1)$$
$$1+x^2+x^4,"\quad",(x+a^2+a+1)^2\ (x+a^2+a)^2$$
$$1+x+x^2+x^4,"\quad",(1+x^2+x^3)(1+x)$$
$$1+x^3+x^4,"\quad",(x+a^3+1)(x+a^3+a+1)(x+a^3+a^2+a)(x+a^3+a^2+1)$$
$$1+x+x^3+x^4,"\quad",(x+a^2+a)(x+a^2+a+1)(1+x)^2$$
$$1+x^2+x^3+x^4,"\quad",(x^3+1+x)(1+x)$$
$$1+x+x^2+x^3+x^4,"\quad",(x+a^3+a^2)(x+a^3+a^2+a+1)(x+a^3)(x+a^3+a)$$

As I scan down the list, I seem to find certain ones that don't factor. Here they are:

$1 + x + x^3$
$1 + x^2 + x^3$

These two are irreducible in R because they cannot be factored! Since they cannot be factors even in GF(q), they are not min polys.

(2) Here is a list of *all* min polys for GF(2^4).

$$
\begin{aligned}
p_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) && = x^4 + x + 1 \\
p_7(x) &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) && = x^4 + x^3 + 1 \\
m_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) && = x^4 + x^3 + x^2 + x + 1 \\
m_5(x) &= (x - \alpha^5)(x - \alpha^{10}) && = x^2 + x + 1 \qquad (6.21)
\end{aligned}
$$

Therefore, the two polys above are irreducible but they are not min polys! So I now have an example of a polynomial which is irreducible but not a min poly.

(3) **Question**: are all irreducible polys of full degree k also min polys? That was the case in the above example. We can certainly have degree k polys which are reducible, as example above shows. I looked at the case 2^7 and the same seems true. You have to find a single factor containing a poly of degree 7 which is non-linear. Here is the answer:

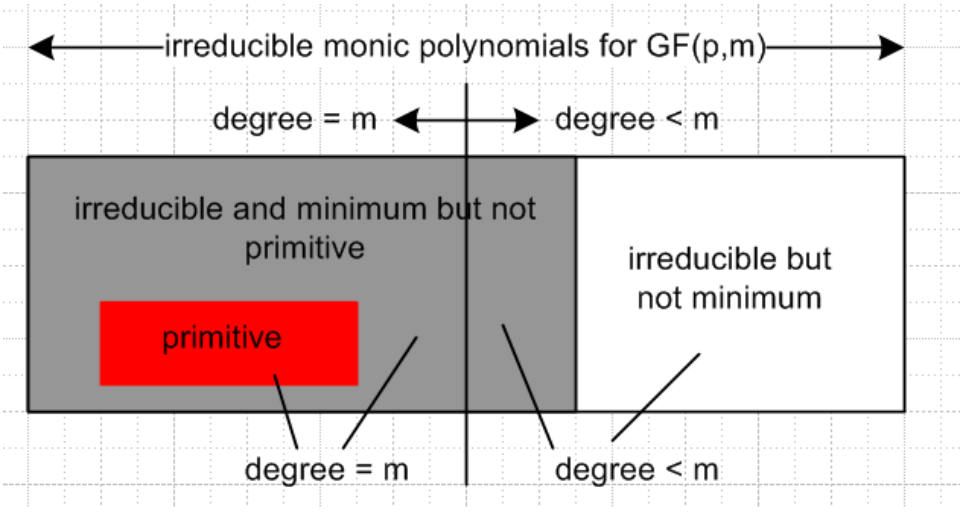
Fact 14: If monic irreducible f(x) is used to construct a representation of GF(q), then f(x) is a minimum polynomial of GF(q) in that representation. (5.34)

To this I could add some Corollaries:

Corollary: If monic irreducible f(x) is of degree m, then it is a minimum polynomial for GF(p^m). (5.34a)

Corollary: If monic irreducible f(x) is not a minimum polynomial for GF(p^m), it must have degree < m. (5.34b)

Here then is the picture I have been waiting for



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

Next question:

How show all those order-reversal things. New doc.