Maple and finite fields PhL 1.23.13

I have just discovered the Maple does in fact know something on this subject, at first I thought it did not.

Consider GF(2^3). We know that $p(x) = x^3 + x + 1$ is a prim poly and there is some primitive element α such that $p(\alpha) = 0$. This α is a root of $x^3 + x + 1$. We can tell Maple this by saying

```
alias(alpha=RootOf(x^3+x+1));
```

$$I, \alpha$$

```
alpha;
```

$$\alpha$$

Now consider the following:

```
Roots(x^7-1,alpha) mod 2;
```

$$[[\alpha^2+\alpha, 1], [\alpha+1, 1], [\alpha, 1], [\alpha^2, 1], [1, 1], [\alpha^2+1, 1], [\alpha^2+\alpha+1, 1]]$$

This command is telling us the 8 roots of x^7-1 in terms of 1 and powers of α. Thus, we have a listing here of all the non-zero elements of GF(2^3) each in terms of α. This is pretty important I think. The second item is just multiplicity, so ignore it. This we have

$\alpha^2+\alpha$	1
$\alpha+1$	α
α	α^2
α^2	$\alpha+1$
1	$\alpha^2+\alpha$
α^2+1	$\alpha^2+\alpha+1$
$\alpha^2+\alpha+1$	α^2+1

I can reorder them as shown on the right, and these are exactly my list in (6.11).

Comment: This give me a quick way to make this list probably for any GF(p^m) field. I know how to do it manually, but this is certainly faster.

Question: Does every GF(2) polynomial have such a set of roots?

I think the answer is no. For example,

```
Roots(x^2+x+1,alpha) mod 2;
```

$$[\,]$$

Although x^2+x+1 has two roots in the complex numbers, I think the above says that it has no roots in GF(8). I would conclude that this could not be a minimum polynomial for GF(8)! So for the first time I seem to have a way to test polynomials. Let's try the two prim polys of GF(8),

```
Roots(x^3+x+1,alpha) mod 2;
```

$$[[\alpha^2+\alpha, 1], [\alpha, 1], [\alpha^2, 1]]$$

```
Roots(x^3+x^2+1,alpha) mod 2;
```

$$[[\alpha+1, 1], [\alpha^2+1, 1], [\alpha^2+\alpha+1, 1]]$$

As expected, each of these prim polys has three roots in GF(8).

Let's advance now to GF(16) which is my interest at the moment. I know a prim poly from my table 6.2 so here we go

```
> restart;
> alias(alpha=RootOf(x^4+x+1)):
> Roots(x^15-1,alpha) mod 2;
```

$$[[\alpha, 1], [\alpha^2+\alpha+1, 1], [\alpha^2+\alpha, 1], [\alpha^3+1, 1], [\alpha^3, 1], [\alpha^3+\alpha+1, 1],$$
$$[\alpha^3+\alpha^2+\alpha, 1], [\alpha^3+\alpha, 1], [1, 1], [\alpha+1, 1], [\alpha^3+\alpha^2+\alpha+1, 1], [\alpha^3+\alpha^2+1, 1],$$
$$[\alpha^3+\alpha^2, 1], [\alpha^2+1, 1], [\alpha^2, 1]]$$

There are your 15 non-zero elements of GF(16), very good. Now try the prim poly itself

```
Roots(x^4+x+1,alpha) mod 2;
```

$$[[\alpha, 1], [\alpha^2+1, 1], [\alpha+1, 1], [\alpha^2, 1]]$$

and as expected there are four roots.

Now we are in a position to test all the 4^{th} degree polys I piled up in (5.31). Here is the first one

$x^4 + x^3 + x^2 + x + 1$

```
Roots(x^4+x^3+x^2+x+1,alpha) mod 2;
```

$$[[\alpha^3+\alpha, 1], [\alpha^3+\alpha^2+\alpha+1, 1], [\alpha^3+\alpha^2, 1], [\alpha^3, 1]]$$

This DOES have four roots! Come back to this one later.

$x^4 + x^3 + x^2 + 1$

```
Roots(x^4+x^3+x^2+1,alpha) mod 2;
```

$$[[1, 1]]$$

I think this is saying that have only one root in GF(16). What exactly does that mean? I think it means this cannot be a min poly because any min poly has all its roots in GF(16) ! Continue on

$x^4 + x^3 + x + 1$

```
Roots(x^4+x^3+x+1,alpha) mod 2;
```

$$[[\alpha^2+\alpha+1, 1], [1, 2], [\alpha^2+\alpha, 1]]$$

If I call the first and last elements a and b, this seems to say

$$x^4 + x^3 + x + 1 = (x-1)^2(x-a)(x-b) = (x+1)[(x+1)(x-a)(x-b)] = (x^3+1)(x+1)$$

Since a root is repeated, this is not a min poly. I can reduce it as shown. I would then claim that the squre bracket shows the roots of $x^3 + 1$ and Maple verifies that fact,

```
Roots(x^3+1,alpha) mod 2;
```

$$[[\alpha^2+\alpha, 1], [\alpha^2+\alpha+1, 1], [1, 1]]$$

Let's keep on truckin' :

$$x^4 + x^2 + x + 1$$

```
Roots(x^4+x^2+x+1,alpha) mod 2;
```

$$[[1, 1]]$$

Again, this is like $x^4 + x^3 + x^2 + 1$ above, it has only 1 root, it cannot be a min poly. Next

```
Roots(x^4+x^2+1,alpha) mod 2;
```

$$[[\alpha^2+\alpha, 2], [\alpha^2+\alpha+1, 2]]$$

This is a surprise to me. There are four roots, this is a min poly. I cannot reduce it in GF(p), it has coefficients in GF(p), it has at least one root in GF(q) so it is a min poly! This must be the third line of (5.27) ! That is what I was looking for!

Question: How can I have Maple evaluate one of those factored min polys from Ch 5? For example, for the GF(2^4) case we have $p_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$