Peterson-Weldon Red book Scan **7.13.91**

This is a 1972 book. His chapter 2 is intro to algebra. Not much here , groups and fields and matrices and vector spaces.

Chapter 6: Polynomial Rings and Galois Fields.

This is close to my line of development. Does the big ring ideal business.

His section 6.4 is about the poly residue classes and it just leaves me cold for now. I think they are talking about first restricting to a poly ring / $x^n - 1$, and then within that, further restricting to some g(x). Ie, they are setting up for the basis of coding theory, but I have not needed that stuff, since I am not so much doing codes.

Section 6.5 is titled Galois Fields. Here we open with the result that the chart thing is a field if p(x) is irreducible. Then all of a sudden we gt the same non-sequitor as in Rhee, that $p(\alpha) = 0$. He has not said anything about what p(x) is except it is irreducible. No phrase "prim poly" or anything like that. Just a cold hit. I think Rhee copied the words verbatim.

Good comment about isomorphic: differ only in the way elements are named, same strucutre.

Then we get the expansion theorem and at once we are into the min poly definition. Same porogression as me , nothing I have missed.

They throw in the little $x^n - 1$ divider theorem which I had but took out. I never had to use it.

Theorem 6.13 -- thing about irreducible implies field.
Theorem 6.14 -- little expansion theorem
Theorem 6.15 -- m(x) is irreducible
Theorem 6.16. -- if $p(\alpha) = 0$, then p(x) is multiple of m(x)
Theorem 6.17 -- degree of m(x) is m or less
Theorem 6.18 -- Big Theorem 2 about all the roots
Theorem 6.19 -- the little $x^n - 1$ divide thing I have left out
Theorem 6.20 -- Big Theorem 1, but I could never follow the proof.

I looked at it again. In retrospect, it is not bad. I just dont know how to prove that you have an element α of each prime component as he suggests, though no doubt true. We do know that such orders do divide the big order, but the existence of all these elements is not clear to me. I think this may be where the secret work is hiding.

In any event, he gets a generator in each prime component of q-1, then shows that if you multiply them all together, you get your α. It is induction proof. I like the approach, but I think my time is up on this subject.

Theorem 6.21 -- this is the one that if α is root of a poly, then so is α^p.
Theorem 6.22 -- The roots of $x^q - x$ forma subfield -- so what?!

Theorem 6.23 -- every poly of degree m of GF(p) divides $x^q - x$. I think this is just saying that you only form polys by taking (x-a) factors, and these are a subset of the whole shebang, etc. I agree.

Theorem 6.24 -- Every irreducible factor of $x^q - x$ has degree m or less. But to me, these are just the m(x) things, and I know they are all m or less.

Theorem 6.25 -- If k is degree of m(x) of α, then order of α divides $p^k - 1$ but no smaller. $p^n - 1$. This is one I do not have.

Theorem 6.26 : the idea that the conjugates are all roots of an m(x) type thing.

Theorem 6.27 -- All roots of an irreducible poly have the same order. I did not do this one, but I know it is treu for primitive roots. I did show that somewhere.

They define exponent the way I defined period. Then they have a big rush that looks very compressed, like they ran out of time. Same definition of primitive polynomial as me though, and they tie it to this period thing.

Page 159: I am not happy about writing the x polynomials as powers of α, because then α has two meanings to me. For red book, α is not the prim element, so OK. I will always show powersin x. So his chart page 159 is simply the m-tuple enumeration of elements of GF(16), fine.

Section 6.7.

This is a giant example. Take GF(64). He then forms all the little conjugate sets, just the way I did for GF(16). You find that elements in same set have same order.

He defines $PSI_i(x)$ to be product of all (x-a) factors where elements have some particular order. this is perfectly reasonable, and you will look at GCD(k,q-1) to decide who goes where. Soi the first step is to group the elemental factors in this way. He calls the PSI the cyclotonic polynomials. there are then certain groupings you can make, and you get relations.

Then he writes up the various minimum polys in a good notation. Then the whole thing groups up as shown in the table page 164. This kind of stuff appears in some book by Marsh, tables of these things.

Section 6.8. Off on the subspace kick again, I may come back to this if her refers to it in his linear circuits stuff.

End. So I am happy with this review of the red book on the Galois Math. I don't think I am now missing any major points. Reviews of all my sources are now complete, so the next step finally is to do some applications.