Leftovers from Galois work

This stuff is from Chapter 5, put here on 7.7.

Fact: Consider the process of forming the powers of the conjugate set of α. At some point before the end of the m-element list as shown above, we *might* hit a first power that repeats some earlier element on the list. Once this happens, we claim that all subsequent powers also repeat earlier elements. Thus, you know you are done constructing the distinct conjugate set once you get to the first repeat. If there *is* some repeat point prior to the end of the above list, then let p^k be the power of this first repeat. In this case, the list of distinct conjugates is as follows:

$$\{\ \alpha,\ \alpha^{p}\ ,\ \alpha^{p^2}\ ,\ \alpha^{p^3}\ \ ....\ \ \alpha^{p^{k-1}}\ \ \}\qquad \text{where}\quad \alpha^{p^k}\quad \text{is the first repeater}$$

Proof: Let the first repeat occur when $\alpha^K = \alpha^{K_1}$ where $K = p^k$ and $K_1 = p^{k_1}$. Then we know that $\alpha^{K-K_1} = 1$. Consider then any later element in the series α^N where $N = p^n$, $n > k$. We can expand N in terms of the quotient and remainder you get if you divide N by $K-K_1$:

$$N = Q(K-K_1) + R$$

Clearly $R < K-K_1$ since it is the remainder. What is a lot less clear is that R is a power of p. This fact is proven in the following Lemma, where we find that $R = p^{k'}$ with $k' = \text{Rem}\left[\ \frac{n}{k-k_1}\ \right]$. Thus, we see that $k' < k-k_1$. But because if this fact,

$$\alpha^N = \alpha^{Q(K-K1)}\ \alpha^R = [\alpha^{K-K_1}]^Q\ \alpha^R = [1]^Q\alpha^R = \alpha^R$$

we see that $\alpha^N = \alpha^R$ which is some previous element of the sequence having $R = 2^{k'}$ with $k' < k-k_1$. Thus we are repeating an element which occurred before the first repeat k_1. Since α^N is any power after the first repeat, we see that no new elements will be found after the first repeat occurs, QED.

Lemma needed above: We claim that, for any integer $a>0$ and any integers $b>c>0$, one can write:

$$\text{Rem}\left[\ \frac{x^a}{x^b - x^c}\ \right] = x^d \qquad \text{where}\ \ d = \text{Rem}\left[\ \frac{a}{b-c}\ \right]$$

If we now set $x = p$, $a=n$, $b=k$, $c=k_1$, $d=k'$, we get the result used in the previous proof:

$$\text{Rem}\left[\ \frac{p^n}{p^k - p^{k_1}}\ \right] = p^{k'}\quad \text{where}\ \ k' = \text{Rem}\left[\ \frac{n}{k-k_1}\ \right]$$

Proof of Lemma: We are talking here about a remainder in the division of two polynomials. If $a < b$, the remainder is x^a and there is nothing to do. If $a \geq b$, we do the long division. If you take out a piece of paper and just do the long division process by hand, you see in about 1 minute that at each stage of the division, the subtraction gives just a power of x. The powers of x proceed in a regular pattern. After the

first stage, the power is a - (b-c). After the second stage it is a - 2(b-c), and so on, so that when you are finally done, the remainder is x^d where d = a - N(b-c) for whatever integer N it took to get d down below b. Thus, we can write a = N(b-c) + d, so d = Rem [a/(b-c)].

We now continue to make observations about the sequence of powers of α used to generate the conjugate set of α.

Fact: In constructing the conjugate set of α, if one were to continue building the powers beyond the point of the first repeat, we claim that eventually *all* earlier members of the list are repeated.

Proof: Earlier we assumed that $K = p^k$ was the first repeat point, and we showed that any later power in the sequence has the form $\alpha^N = \alpha^R$ = a repeat of a member prior to k. If we can find an $N = p^n$ such that R = 1, when we will have repeated α itself. Since each element of the set is the preceding one raised to the power p, the next set of powers will repeat the entire conjugate set exactly in the original order.

Since $R = p^{k'}$, we will get R=1 if k'=0. But we know from the Lemma above that k' = Rem[n/(k-k_1)], so it is easy to find an n that works. Choose n = j(k-k_1) where j is any integer > k/(k-k_1), so that n will be larer than k. Then k' = Rem[n/(k-k_1)] = Rem[j(k-k_1)/(k-k_1)] = Rem[j] = 0.

Thus, we have found an n later in the sequence such that $\alpha^N = \alpha$. The next term will be n = j(k-k_1)+1 which gives k' = 1, and we will get α^R with R = p, we we get α^p. As claimed, the entire sequence will then repeat.

Fact: If you start with *any* element of a conjugate set and use it to form a new conjugate set by computing powers as above, you get the *same* conjugate set. In other words, the conjugate set { α, α^p, α^{pp}, α^{ppp}, ...} contains the same distinct elements as { β, β^p, β^{pp}, β^{ppp}, ...}if you start with some $\beta = \alpha^K$ out of the first set.

Proof: Suppose we do start with some element $\beta = \alpha^K$ somewhere out in the middle of the set. We have just shown that as powers are built up, we eventually get the term α and all subsequent terms after α. So you can start anywhere you like, and you will get the same conjugate set.

Practice Pad:

Lemmas about the cyclic • groups in {GF(q) -0,•}.

Notation: In the following set of fact developments, the term "cyclic subgroup" refers exclusively to a "cyclic subgroup of the group {GF(q) -0,•}. Recall that this larger group has order q - 1.

Fact: Any element α of GF(q) lies in a some cyclic subgroup of some order n, and for all elements β in this subgroup, $\beta^n = \beta$.

Proof: Construct the list of elements {1, α, α^2..}. At some point, you must arrive at some power which we will call n-1 such that $\alpha^{n-1} = 1$. Then as you do higher powers, you repeat the elements of the subgroup, so that $\alpha^n = \alpha$, and so on. If you never arrived at a point where $\alpha^{n-1} = 1$, then you would never

repeat any elements, and then the list would be infinite. But GF(q) is finite. Any other element in the list can be written as $\beta = \alpha^k$ for some integer k. Then $\beta^n = \alpha^{kn} = \alpha^k = \beta$, as claimed.

Fact: The order n of any cyclic subgroup evenly divides the order of the group q-1.

Proof: The coset decomposition of the full group by the subgroup proves this.

Fact: The n elements of a cyclic subgroup of order n are the n roots of the polynomial $1 - x^n$. This polynomial can be fully factored into the n linear factors $(x-a_i)$ where the a_i are the roots.

$$1 - x^n = (x - a_1) \bullet (x - a_2) \bullet (x - a_3) \bullet \ldots (x - a_n)$$

Proof: We know by definition that $a^n = a$ for all elements in the cyclic subgroup. Thus, these n elements are all roots of $f(x) = 1 - x^n$. The term "a is a root of f(x) " means $f(a) = 0$. Since this polynomial has at most n roots and we have found them all, it fully factors as claimed

Fact: Polynomial $1 - x^m$ divides evenly into $1 - x^n$ where n>m are integers . The result is:

$$\left[\frac{1 - x^n}{1 - x^m}\right] = 1 + x^2 + x^3 + \ldots + x^{n-m}$$

Proof: just do the long division. At each level, the remainder has the form $x^{(n-Im)} - 1$. The first remainder has I = 1, then I increases by 1 at each level. At some point, n-Im = m and we are done.

Fact: Given any pair of cyclic subgroups in {GF(q) - 0}, •}, the smaller must be contained within the larger.

Corollary 1: If the orders of two cyclic subgroups are the same, then the subgroups are the same.

Corollary 2: There can be at most one subgroup for any given order.

Proof: Elements of the larger subgroup are the n roots of $1 - x^n$. Elements of the smaller subgroup are the m roots of $1 - x^m$. But from the above fact, we can write:

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

Thus, the m roots of the smaller subgroup must be contained within the the set of roots of the larger subgroup. In other words, if you factored everything in sight into little (x - a) factors, the factors for the smaller subgroup all appear within the factors of the larger subgroup. If the two subgroups have the same order, then the factors are exactly the same on both sides of the above, so the elements of the two subgroups (the set of roots) are identical.

Fact: The cyclic subgroups are fully nested. In other words, given a set of subgroups A,B,C... with orders a,b,c such that a>b>c .. we know that A □ B□ C ...

Corollary 1: There must exist some largest subgroup which contains all the others. Call its order e, the *exponent*. Obviously $e \leq q-1$, the size of the full group $\{GF(q) - 0\}, \bullet\}$.

Corollary 2: The order of any subgroup divides evenly into the exponent e.

Proof: Take the set of subgroups and arrange them by decreasing order. If two or more orders are the same, we know the subgroups are the same, so throw out all but one of any given order. Then a>b implies A □ B according to the fact above, and b>c implies B □ C, and so on. So we have shown the full nesting. There must be some outermost largest subgroup of this nesting, it is the one of order e. According to coset decomposition, the order n of any contained subgroup must evenly divide e.

Big Theorem 1: The group $\{GF(q) - 0, \bullet\}$ is cyclic.

Proof: Consider *any* element α of $\{GF(q) - 0, \bullet\}$. From our first fact, it must lie in some cyclic subgroup of some order n. We know its elements are solutions of $1 = x^n$. Since e, the order of the largest cyclic subgroup, must be a multiple of n, we can write $e = kn$. Raise both sides to the kth power then to get $1 = x^e$. Thus, we have shown the any element α of $\{GF(q) - 0, \bullet\}$ is a root of $f(x) = 1 - x^e$. But this f(x) can have at most e roots. Since all elements of $\{GF(q) - 0, \bullet\}$ are roots, we know that $q-1 \leq e$. On the other hand, it is clear that $e \geq q-1$ since e is the order of a cyclic subgroup contained within $\{GF(q) - 0, \bullet\}$. The only possible solution to this dilemma is $e = q-1$. Thus, the size of the largest cyclic subgroup *equals* the size of the whole group. Thus, the whole group is cyclic. Very impressive.

Big Theorem 2: We shall state this theorem in five equivalant ways:

1) The q-1 elements of $\{GF(q) - 0, \bullet\}$ are the q-1 roots of the polynomial $h(x) = x^{q-1} - 1$
2) The q elements of GF(q) are the q roots of $f(x) = x^q - x$
3) If α is any element of GF(q), then $f(\alpha) = 0$.
4) If α is any element of GF(q) , then $\alpha^q = \alpha$.
5) The polynomial $x^q - x$ can be fully factored into q linear factors of the form $(x - a_i)$. Each factor contains one of the roots of GF(q). There is one factor for each root. Thus:

$$(x^q - x) = (x - a_1)\bullet(x - a_2)\bullet(x - a_3)\bullet(x - a_4)\bullet.....(x - a_q)$$

We might as well pick out the field elements that we know must be present, namely **1** and **0**. Letting these be a_1 and a_q, we can rewrite the above factorization as:

$$(x^q - x) = (x - \mathbf{1})\bullet(x - a_2)\bullet(x - a_3)\bullet(x - a_4)\bullet.....(x - a_{q-1})\bullet (x - \mathbf{0})$$

Proof: These results all trivial once we know that $\{GF(q) - 0, \bullet\}$ is cyclic. Item #1 is true for any cyclic subgroup, we proved it as one of our first facts above. Item #2 is trivial since we have just added a factor of x to account for the 0 element of GF(q). Item#3 and #4 are a restatements of item #2. Item #5 follows because we know that $x^q - x$ has at most q roots, and we have identified all q of them in item #3, so we are just writing them out. Each form of the above theorem stresses a certain point.

Fact: All facts above apply to GF(p) since this is a special case of GF(q).

Corollary: The group $\{GF(p) - 0, \bullet\}$ is cyclic.

Corollary: Big Theorem 2applies to GF(p), replace q with p everywhere.

Fact: {GF(p) - 0, •} is a cyclic subgroup (order p-1) of {GF(q) - 0, •} (order q-1).

Proof: If group H is a subset of group G, then H is by definition a subgroup of G. We know that {GF(p) - 0, •} is a group, and we know it is a subset of {GF(q) - 0, •}, so it is a subgroup. We also know that {GF(p) - 0, •} is cyclic, as just stated above. Thus, it is a cyclic subgroup.

Fact: If $\alpha^p = \alpha$ for some element α in GF(q), then α is an element of GF(p).

Proof: If $\alpha = 0$, the result is obvious, since 0 is in GF(p). Otherwise, we know that α is an element of some cyclic subgroup in {GF(q) -0,•} of order p. We know there can only exist one subgroup for a given order. We know that {GF(p) -0,•} is a cyclic subgroup of order p. Thus, α is in GF(p).

Junk Bin

A theorem relating the elements of GF(q) to the polynomial $x^q - x$.

Now we are able to state and then prove the following amazing theorem:

Big Theorem 1: We state this theorem three equivalent ways.

1) The q elements of GF(q) are the roots of the polynomial $f(x) = x^q - x$.
2) If α is an element of GF(q), then $f(\alpha) = \alpha^q - \alpha = 0$.
3) If α is an element of GF(q), then $\alpha^q = \alpha$.

Proof: Let x be a non-zero element of GF(q). Omitting the 0 element, GF(q) is a group under •. We showed in Chapter 1 that every element of a group lies in a cyclic subgroup of some order n, such that $x^n = 1$. We showed that whatever n is, it must divide evenly into q. So assume that q = mn, where m is some integer. Now take $x^n = 1$ and raise both sides to power m. This gives $x^{nm} = x^q = 1$. We have thus shown that any non-zero element of GF(q) satisfies this equation: $x^q - 1 = 0$. So make up a polynomial $h(x) = x^q - 1$. We know that all non-zero elements of GF(q) then satisfy h(x) = 0. Multiply both sides by x, to get $f(x) = x \bullet (x^q - 1)$. Now the zero element of GF(q) trivially satisfies f(x) = 0, and so do all non-zero elements. Multiply the thing out and you get $f(x) = x^q - x$. QED.

Corollary: Since f(x) is a polynomial of degree q, we know generally it can have at most q roots in some field. We have just shown that in the field GF(q) there are *exactly* q roots, and they are *exactly* the elements of GF(q). Thus, in GF(q), we can fully factor the polynomial $(x - x^q)$ in the following manner:

$$(x^q - x) = (x - a_1)\bullet(x - a_2)\bullet(x - a_3)\bullet(x - a_4)\bullet.....(x - a_q)$$

where a_i are the q elements of GF(q). We might as well pick out the field elements that we know must be present, namely **1** and **0**. Letting these be a_1 and a_q, we can rewrite the above factorization as:

$$(x^q - x) = (x - \mathbf{1})\bullet(x - a_2)\bullet(x - a_3)\bullet(x - a_4)\bullet.....(x - a_{q-1})\bullet (x - \mathbf{0})$$

or dividing through by x,

$$(x^{q-1} - 1) = (x - \mathbf{1}) \bullet (x - a_2)\bullet(x - a_3)\bullet(x - a_4)\bullet.....(x - a_{q-1})$$

More Junk

A theorem about GF(q) being cyclic.

More precisely, we are making this claim:

Big Theorem 2: The q-1 non-zero elements of GF(q) form a *cyclic* group under operation •.

Comment on Proof: We intended to prove this here, but have decided against it. The proof can be found in Bobrow and Arbib, *Discrete Mathematics*, Section 8-3, Theorem 8. The proof is rather tricky, but it depends on nothing more than the things we have already shown so far in previous chapters of this report. There is no new magic ingredient. As part of the proof of Big Theorem 2, B&A prove as well the following interesting fact which we will simply state without comment:

Fact: if e is the order of the largest cyclic subgroup of a finite commutative group, then the order of any smaller cyclic subgroup must divide evenly into e. The number e is called the *exponent* of the group.

More Junk

Corollary to Big Theorem 2: There exists at least one generator α in GF(q) such that the elements of the field GF(q) can be listed off as follows:

$$\{\ 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3, ...\ \alpha^{q-1}\ \} \quad \alpha^q = 1$$

Of course 0 is not part of the cyclic group under •, we just list it to show all the elements of GF(q).

In a cyclic group section of Chapter 1, we investigated generators of cyclic groups in some detail. We found that there may or may not be other generators. Things hinge on whether or not q-1 is prime. If q-1 is prime, then all elements (other than 0 or 1 above) of GF(q) are generators. On the other hand, if q-1 is not prime, we found that any $\beta = \alpha^m$ where m divides evenly into q-1 is not a generator.

Definition: A generator of the cyclic group { GF(q) - 0} under • is called a *primitive element* of GF(q).

Example: Consider GF(8) = GF(2^3). We list off the 8 elements

$\{ 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 \}$ $\alpha^7 = 1$

Since q-1 is prime, we know that all elements of GF(8) except 0 and 1 are primitive elements. The reader may find it useful to try a few $\beta = \alpha^m$ and verify that this is so.

Example: Consider GF(16) = GF(2^4) . We have

$\{ 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14} \}$ $\alpha^{15} = 1$

Now q-1 is not prime, so we know that there are some non-generators. Two sure-fire failures will be $\beta = \alpha^5$ and $\beta = \alpha^3$, since 5 and 3 divide into q-1· Try $\beta = \alpha^3$:

$\beta = \alpha^3$
$\beta^2 = \alpha^6$
$\beta^3 = \alpha^9$
$\beta^4 = \alpha^{12}$
$\beta^5 = \alpha^{15} = 1$

The order of this β's cyclic subgroup is 5.

Example: Finally, consider GF(4) since we have its + and • tables above. We should have

$\{ 0, 1, \alpha, \alpha^2 \}$ $\alpha^3 = 1$

Since 3 is prime, either of the two remaining elements in GF(4) is a primitive element. For example:

If $\alpha = 01$, then $\alpha^2 = 01 \bullet 01 = 11$ = the other element.

If $\alpha = 11$, then $\alpha^2 = 11 \bullet 11 = 01$ = the other element.

Item:

Fact: Polynomial $1 - x^m$ divides evenly into $1 - x^n$ iff m divides evenly into n . The result is:

$$\left[\frac{1 - x^n}{1 - x^m} \right] = 1 + x^2 + x^3 + \ldots + x^{n-m}$$

Proof: just do the long division. At each level, the quotient term is x^{n-Im}, and the remainder is x^{n-Im}-1. where integer I = 1,2,3... . If, at some point, n-Im = m, the remainder is $x^m - 1$. The next quotient term will be 1, and the next remainder will be zero and we are done. This requires n = (I+1)m. So things divide evenly only if n is a multiple of m. Otherwise, there is some non-vanishing remainder polynomial.

<u>This put here on 7.16 from Chapter 7:</u>

We now doggedly repeat the above prove in the systematic basis. Apply the above Corollary to f(x) = C(x), a polynomial of degree n-1 corresponding to a legal codeword. Thus,

$x^m C(x) = q(x)(x^n - 1) + C^{(m)}(x)$ $\quad \{ C^{(m)}(x)\} = \{ x^m \} \bullet \{C(x) \}$

Now isolate the term $C^{(m)}(x)$ to one side, and make the replacement

$C(x) = D(x)g(x)$ $\quad \{ C(x)\} = \{ D(x) \} \bullet \{ g(x) \}$

$= \gamma(x) + x^{n-k} d(x)$ $\quad \{ C(x)\} = \{ \gamma(x) \} + \{ x^{n-k} d(x)\}$

to get

$C^{(m)}(x) = x^m D(x)g(x) - q(x)(x^n - 1)$ $\quad \{ C^{(m)}(x)\} = \{ x^m D(x) \} \bullet \{ g(x) \}$

Now make the further replacement

$(x^n - 1) = h(x)g(x).$ $\quad \{ 0\} = \{ h(x) \} \bullet \{ g(x) \}$

to get

$= [\ x^m D(x) - q(x)h(x)\ ]\ g(x)$

Since g(x) has degree n-k, and since $C^{(m)}(x)$ has degree n-1, the item in brackets [ ] must have degree k-1. It is just some data polynomial $D_m(x)$ of degree k-1. Thus,

$C^{(m)}(x) = D_m(x)\ g(x)$ $\quad \{ C^{(m)}(x)\} = \{ D_m(x) \} \bullet \{ g(x) \}$

where $D_m(x)$ is some polynomial of degree k-1. Using the Division Algorithm, we can expand the product on the RHS relative to the polynomial x^{n-k} as follows:

$D_m(x)\ g(x) = x^{n-k} q(x) + r(x)$

Because q(x) and r(x) are unique

$x^{n-k} d_m(x) = D_m(x)\ g(x) + r(x)$

We can now think of expanding $x^{n-k}\ d_m(x)$ over g(x) using the Division Algorithm. Since there is a unique quotient and remainder, it must be that the quotient is $D_m(x)$, and the remainder is $\gamma_m(x)$. Thus, there exists some data polynomial $d_m(x)$ which produces $D_m(x)$ as the quotient, and this in turn produces $C^{(m)}(x)$ as a code word. Since $d_m(x)$ is a data word, $C^{(m)}(x)$ must be a legal codeword.

Old Contents for Chapter 4: (7.21.91)

• Recall that the elaborate construction of Chapter 3 resulted in the following identification:

$$GF(q) = Polys[x, GF(p)] / (f(x),m) \qquad q = p^m$$

where f(x) is some irreducible (not factorable in GF(p)) polynomial of degree m. The mess on the right is the residue class ring formed by taking as an "ideal" the set of polynomials which are multiples of f(x). We built "the chart" and each row was identified with a particular remainder polynomial, and also as an element of GF(q).

• It is shown that GF(q) contains GF(p) as a subfield, and that because of this, any element of GF(q) can be written in the form $\mathbf{g} = \mathbf{h} \bullet \mathbf{g}'$, where h is in GF(p).

• This leads to a generalization from GF(p) to GF(q) of this fact: $p\mathbf{g} = \mathbf{0}$ for any $\mathbf{g}$ in GF(q).

• It is next shown that the elements of GF(q) can be represented by m-tuples which serve as a shorthand notation for the remainder polynomials which represent the elements (chart rows) of GF(q) according to the construction $GF(q) = Polys[x, GF(p)] / (f(x),m)$.

• If the elements of GF(q) are labelled as m-tuples, it is shown that the + table for the field GF(q) can be instantly constructed by modulo-p arithmetic, without knowledge of the defining polynomial f(x).

• For a particular irreducible f(x) of degree m, we can also construct the • table for GF(q), although it requires a bit of work.

• It is next shown that a polynomial over field GF(p) can be extended to the larger field GF(q) . It "looks" the same. It is normal for the polynomial to be "more factorable" in GF(q) than it is in GF(p).

• Next we get Big Theorem 1 which says that the polynomial $x^q - x$ factors completely in GF(q) and the q roots are the q elements of GF(q). This means that $g^q = g$ for any element in GF(q).

• Then comes Big Theorem 2 which says that the q-1 non-zero elements of GF(q) form a cyclic group under multiplication •. This means that all non-zero elements can be written as powers of at least one generator element, called by definition a *primitive element*.

• It is noted (in passing) that the order of any cyclic group of any finite commutative group must divide evenly into the order of the *largest* such cyclic group. This largest order is called the *exponent*.

• A comparison is made between two methods of labelling GF(q) elements and makint the + and • tables. One method is the m-tuples, where + is simple. The other is the cyclic basis as powers of a primitive element, where • is simple.

• A list of facts about GF(q) is given, and should be compared to the GF(2) list in Chapter 2.