Chapter 4: The Galois Fields GF(p^m).

Chapter Contents.

GF(p) is a subfield of GF(q)

Fact: Any element of GF(q) can be written in the form **g** = **h**•**g**' where h is an element of GF(p).

Fact: p**g** = **0** for any element **g** of GF(q).

Representing GF(q) Field Elements as Polynomials or as m-tuples.

Extending polynomials from ground field GF(p) to extension field GF(q)

Cyclic Subgroups and GF(q)

Fact 1: The order n of any cyclic subgroup of {GF(q) -0,•} divides q-1.

Fact 2: Many things about a cyclic group, including definition of (α,n,•).

Fact 3: If "g has order n" , then $g^n = 1$ and n is the least integer for which $g^n = 1$.

Fact 4: If $g^k = 1$, the "order of g" divides k. .

Fact 5: If β is any element of (α,n,•), then $\beta^n = 1$.

Fact 6: If β is any element of (α,n,•), then the order of β divides n, the order of α. More specifically, we claim that [order of β] = n/GCD(k,n) where $\beta = \alpha^k$.

Definition: Element a is a *root* of polynomial f(x) means that f(a) = 0.

Fact 7: (The Factor Theorem) Polynomial f(x) can be written as f(x) = (x-a)q(x) for some polynomial q(x) if and only if a is a root of f(x).

Fact 8: The n elements of some cyclic subgroup (α,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.

Fact 9: Consider two cyclic subgroups A = (α,n,•) and B = (β,m,•). If n=km , then A contains B.

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

Corollary : There can be at most one cyclic subgroup of any given order.

Definition: The *exponent* e is the order of the *largest* cyclic subgroup E in {GF(q) - 0}, •}.

Fact 10: The order of any cyclic subgroup of {GF(q)-0,•} divides the exponent e.

Big Theorem 1: The entire group {GF(q) - 0, •} is cyclic.

Fact 11: There exists at least one generator α for {GF(q) - 0, •}. In terms of it, the entire group GF(q) can be enumerated as follows: { 0, 1, α, α^2, α^3 , ... α^{q-2} }, $\alpha^{q-1} = 1$, $\alpha^q = \alpha$

Definition: Any generator of {GF(q) - 0, •} is called a *primitive element* of GF(q).

Fact 12: A power α^k of a primitive element α is a primitive element iff GCD(k,q-1) = 1.

Fact 13: If q-1 is prime, all elements of {GF(q) - 0 - 1} are primitive elements of GF(q).

Examples: GF(4 = 2^2), GF(8 = 2^3), GF(16 = 2^4)

Big Theorem 2: The q elements of GF(q) are the q roots of $f(x) = x^q - x$

Fact 14: All facts above apply to GF(p) since this is a special case of GF(q).

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

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

Fact 15: {GF(p) - 0, •} is a cyclic subgroup, order p-1, of {GF(q) - 0, •} which has order q-1.

Fact 16: If $\alpha^p = \alpha$ for some element α in GF(q), then α is an element of GF(p).

An example of root factorization: GF(4)

Labeling Elements of GF(q), and the + and • Tables

Selected Facts About GF(q)

Fact: $(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$ when **a**,**b** are elements of GF(q).

Fact: $(a + b + c + d + \ldots)^p = a^p + b^p + c^p + d^p + \ldots$ for a,b,c,d... in GF(q).

Appendix 4.1 Proof of Fact 10

Chapter 4: The Galois Fields GF(p^m).

Note: In this chapter, we continue to assume p = a prime number. Also, to avoid writing p^m very many times, we use the shorhand symbol q to stand for p^m . Thus:

$q = p^m$ p = prime number m = positive integer

GF(p) is a subfield of GF(q)

Adding or multiplying two elements in GF(q) means adding or multiplying two rows in the chart built in Chapter 3. This in turn means adding or multiplying two representative remainder polynomials, one from each row. These polynomials have coefficients and variable x in the field GF(p). Thus, addition or multiplication means the + and • operations of GF(p) = Z_p, with the understanding that an improper product polynomial is divided by f(x) to be made proper.

The chart has p rows which correspond to remainder polynomials which are just numbers -- the elements of the base field GF(p). These are the remainder polys of degree 0. If you add or multiply two of *these* rows, you get a remainder which is again just a number. Thus, at the level of the residue class ring where we imagine that the q rows are the elements of GF(q), we can consider the p rows having degree 0 remainders to be the elements of GF(p). Since these rows mix only with themselves under + and •, we see that GF(p) is a subgroup of GF(q) with respect to either operation, with the understanding that 0 is excluded if we use the • operation. Since these things are both fields, we can also say that GF(p) is a subfield of GF(q). This was noted at the end of the last Chapter, here we have tried to firm up the idea.

Since {GF(p) -0} is a subgroup of {GF(q) - 0} under the • operation, we can do the usual coset decomposition as discussed in Chapter 1. So we can make a new chart -- having nothing to do with polynomials -- where we list the p-1 non-zero elements of H = {GF(p) - 0} across the top, and then we fill out the rows ,

$h_1=1$	h_2	h_3	h_4	...	h_{p-1}
g_1	$g_1 \bullet h_2$	$g_1 \bullet h_3$	$g_1 \bullet h_4$	...	$g_1 \bullet h_{p-1}$
g_2	$g_2 \bullet h_2$	$g_2 \bullet h_3$	$g_2 \bullet h_4$	...	$g_2 \bullet h_{p-1}$
more rows like the above					

This decomposition shows that (q-1)/(p-1) = integer. We can express this as:

$$(p^m-1)/(p-1) = 1 + p^2 + p^3 + ... + p^{m-1}$$

So, from the above coset decomposition, we arrive at this fact:

Fact: any non-zero element of GF(q) can be written in the form $\mathbf{g} = \mathbf{h} \bullet \mathbf{g}'$ where h is an element of GF(p). Of course we can now extend this fact to apply to the zero element as well.

We are now in a position to make a claim about GF(q) that is very similar to an earlier claim made about GF(p). Here is is:

Fact: $p\mathbf{g} = \mathbf{0}$ for any element **g** of GF(q).

Proof: Write **g** in the form $\mathbf{g} = \mathbf{h} \bullet \mathbf{g}'$ as noted above. Then

$$p\mathbf{g} = p(\mathbf{h} \bullet \mathbf{g}') = (\mathbf{h} \bullet \mathbf{g}') + (\mathbf{h} \bullet \mathbf{g}') + ... = (\mathbf{h} + \mathbf{h} + \mathbf{h} + ...) \bullet \mathbf{g}' = (p\mathbf{h}) \bullet \mathbf{g}' = 0$$

The last equality comes from Chapter 2 where we showed that $p\mathbf{h} = 0$ for any element h in GF(p).

Representing GF(q) Field Elements as Polynomials or as m-tuples.

Note: in the discussion of this section, we are thinking of polynomial coefficients and of x as being elements of GF(p). That is, we have polynomials over the field F = GF(p). Therefore, the symbols + and • in this section always refer to these operations in GF(p). We know from Chapter 2 that these operations are just the modulo-p + and •.

We do not always write out the + and • operations explicitly. For example, x^3 means x•x•x. Similarly, one might lose sight of the operation + when the summation symbol Σ is used.

We have added this note here only because in a later section we are going to extend the definition of a polynomial to the larger field GF(q). Here, we are only dealing with GF(p).

We have developed the construction of GF(q) = Polys[x, GF(p)] / (f(x),m). In this construction, each element of the field GF(q) is associated with a "row of the chart". Each row of the chart in turn is associated with a remainder polynomial which has degree less than m. An obvious notation for describing each remainder polynomial is an m-tuple which just lists off the coefficients.

By convention, we shall have the leftmost number refer to the coefficient of $x^0 = 1$. This is convenient if you like to write polynomials starting with the *lowest* order, as we shall do below. Some texts use the reverse convention.

Here then is an example for m = 4:

$p(x) = i + jx + kx^3$ f = ij0k

If p = 2, then the only existing non-zero coefficient is 1, so each m-tuple is then a sequence of 1's and 0's:

$p(x) = 1 + x + x^3$ f = 1101

Two elements are of particular interest for arbitrary m:

p(x) = 0 f = 0000.... **0** element of GF(q)

p(x) = 1 f = 0100.... **1** element of GF(q)

Each element if GF(q) is associated with a particular remainder polynomial of degree less than m, and therefore with a particular m-tuple having m digits. We can therefore use these m-tuples to label the GF(q) field elements in a clear, unambiguous fashion.

Now consider two remainder polynomials a(x) and b(x), for some m. M-tuples are also shown.

$a(x) = a_0 + a_1 \bullet x + a_2 \bullet x^2 + a_3 \bullet x^3 + \ldots$ $a = a_0\ a_1\ a_2\ a_3 \ldots$

$b(x) = b_0 + b_1 \bullet x + b_2 \bullet x^2 + b_3 \bullet x^3 + \ldots$ $b = b_0\ b_1\ b_2\ b_3 \ldots$

As noted above, *adding* two GF(q) field elements means adding rows of the chart, and this means adding remainder polynomials. Thus in turn means adding the coefficients. But the coefficients live in the field GF(p), and addition here is just modulo-p addition. Thus, we can add the above remainder polynomials to get the following result:

$c(x) = c_0 + c_1 \bullet x + c_2 \bullet x^2 + c_3 \bullet x^3 + \ldots$ $c = c_0\ c_1\ c_2\ c_3 \ldots$

where

$c_i = a_i + b_i$ where + means addition modulo p

We have just proven this result:

Fact: If the elements of GF(q) are represented as m-tuples, the addition table can be written down immediately with no further ado. One just does a modulo-p addition on each digit position. Knowledge of the defining polynomial f(x) is not even needed.

Example: Here is the addition table for GF(4) = GF(2^2):

+	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

Now what about multiplication?

Following the same line of argument, and writing things out in the obvious manner, one can easily show that the product of two field elements, each represented by some remainder, is a new field element represented by the product of the remainders. However, although each remainder is of degree less than m, it may happen that the product remainder has degree more than m. In this case, as is easily shown, the right thing to do is take this "improper" product remainder, divide it by f(x), and the resulting remainder is the remainder you want.

So we see that some *work* is needed to produce the multiplication table.

Consider a(x)• b(x) = c(x). If we write out a(x) and b(x) in standard sum notation,

$$a(x)= \sum_{i=0}^{m-1} a_i\ x^i \qquad b(x)= \sum_{i=0}^{m-1} b_i\ x^i$$

then we can write a sum for the (possibly improper) product polynomial as follows:

$$C(x)= \sum_{i=0}^{2m-2} C_i\, x^i \text{ where } C_i = \sum_{j=0}^{i} a_{i-j}\, b_j = \sum_{k=-i/2}^{i/2} a_{(i/2)-k}\, b_{(i/2)+k}$$

As noted earlier, the implied summation and multiplication here is modulo-p.

Once we have found the polynomial C(x), we have to see if it is improper, ie, if it has degree larger than m-1. If so, we have to divide it by the defining polynomial of our construction f(x) and get the remainder. This is then c(x), and the coefficients of c(x) can then be encoded as m-tuples, and these are then put into the multiplication table.

So: if C(x) has degree < m, then c(x) = C(x)
if C(x) has degree ≥m, then C(x) = q(x)f(x) + c(x)

Although "work" is required to get the multiplication table, it is a purely mechanical crank-turning process. No magic is involved. However, for the improper entries, knowledge of f(x) is required so that the division can be done.

From the basic theorem which ends Chapter 3, we know that GF($q = p^m$) is a *field* as long as f(x) is an *irreducible* polynomial of degree m. This just means that f(x) cannot be factored in GF(p).

Let us now search for viable candidate polynomials f(x) of degree 2 that are irreducible and which can therefore serve as the defining function for GF($4 = 2^2$). There are not that many of them to try:

x^2 = (x)(x)
$1 + x^2$ = (1+x)(1+x)
$x + x^2$ = (x)(1+x)
$1 + x + x^2$

There are no more. We have shown that all these choices "factor" in GF(2) except the last one. Therefore, there is exactly one defining polynomial for GF(4), and it is $f(x) = 1 + x + x^2$ = 111 in 3-tuple notation. [In the general case $q = p^m$, there may be more than one possible irreducible f(x)]

Now that we know f(x), we can build the multiplication table for GF(4). Here it is:

•	00	10	01	11

00	00	00	00	00
10	00	10	01	11
01	00	01	11	10
11	00	11	**10**	01

As an example of the precedure described above, we will compute the bolded entry in the table.

$11 \bullet 01 = (1+x)(x) = x + x^2$

This is improper, having degree ≥ 2, so we divide it by $f(x) = 1 + x + x^2$:

$$\begin{array}{r|l} & \underline{\quad 1 \quad .} \\ x^2 + x + 1 & x^2 + x \\ & \underline{x^2 + x + 1} \\ & 1 \end{array}$$

So in this example, $C(x) = x + x^2$, and the remainder is $c(x) = 1 = 10$. Thus, we get **10** in the chart. In just this way we can derive the entire chart.

By the way, notice that the identify **1** = 10 appears in each row (except the first) of the • table, which means that every non-zero element has an inverse. Recall that the modulo-4 tables failed us on this point. GF(4) really is a *field*.

Extending polynomials from ground field GF(p) to extension field GF(q)

Earlier we considered the polynomial $f(x) = 1 + x^2$. Think of the reals as a ground field, and the complex numbers as an extension field. You can start out thinking of the polynomial as having coefficients in the reals, but you can also think of these coefficients as happening to lie on the real axis of the complex number plane. In some sense, then, you are extending the interpretation of your polynomial to a larger world. As noted earlier, a crucial difference is that in the reals, f(x) cannot be factored and is therefore irreducible, but when extended to the complex numbers, suddenly f(x) is no longer irreducible and can be factored into $(x + i)\bullet(x - i)$.

The reason that extending the polynomial from the reals to the complex numbers makes sense is that the reals form a subfield of the field of complex numbers. In similar fashion, GF(p) is a subfield of GF(q). Thus, we can take any polynomial having coefficients in GF(p) and then think of this polynomial as being extended so these coefficients are now elements of the larger field GF(q). The polynomial "looks" the same before and after this extension. However, it may turn out that the polynomial is more factorable in GF(q) than it is in GF(p).

Note that in general you cannot go the other direction. If you have a polynomial with general coefficients in GF(q), how can you write it in terms of only GF(p) elements? For example, the polynomial over the complex number field $f(x) = (x + i)$ cannot be written over the real number field.

Note also: in this extension of the polynomial, we move both the coefficients and the variable x from the ground field to the extension field.

Cyclic Subgroups and GF(q)

Much of the structure of the Galois Field GF(q) can be brought to light by analyzing its cyclic subgroups under the multiplicative operation •. That is the main subject of this section. A *cyclic subgroup* was defined in Chapter 1, and a few facts about it derived there.

Many of the "facts" below apply to cyclic subgroups in general, or in some cases, to commutative groups in general. However, we will be specific and claim our facts only with respect to the field GF(q).

There are many Facts presented in this section, all with proofs. The reader is encouraged to read the proofs, since they serve as checks on the previous material. The main conclusions of this section are presented as Big Theorems 1 and 2.

Notation: In the following set of fact developments, the term "cyclic subgroup" refers exclusively to a cyclic subgroup of the group {GF(q) -0,•}. This means the multiplicative group under • of GF(q) where we have excluded the 0 element. The group {GF(q) -0,•} thus has order q-1.

Definition: A *divides* B (sometimes written A|B) means that there is no remainder when A is divided into B. It means that B is a multiple of A.

If A and B are numbers, it means that B= Ak for some integer k = 1,2,3...

If A and B are polynomials, it means B(x) = A(x)q(x) for some polynomial q(x).

Fact 1: The order n of any cyclic subgroup of {GF(q) -0,•} divides q-1.

Proof: The order of any subgroup H divides the order of a group G containing it. This follows from the coset decomposition discussed in Chapter 1.

Fact 2: Start with any α in {GF(q) - 0 ,•}. Start forming a list by taking powers of α:

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

We claim several things:

(a) that there exists an integer n such that α^{n-1} is the *last distinct element* of this list. Thus, the complete list has n distinct elements as follows:

$$\{ 1, \alpha, \alpha^2, ... \alpha^{n-1} \}$$

(b) $\alpha^n = 1$, which repeats the first element of the list (this is the first repeat)

(c) all subsequent powers repeat elements of the list.

(d) **Notation**: The list of n distinct elements forms a *cyclic subgroup* of {GF(q) - 0 ,•} of order n. We can denote this as:

$$(\alpha, n, \bullet) \quad = \quad \{ \text{generator, order , • operation } \}$$

(e) **Definition**: This integer n is called the *order of* α; α is said to be *of order n*.

(f) The fact that α has order n does *not* imply that other elements of the subgroup have order n.
(g) **Definition**: α is called a *generator* of the cyclic subgroup.
(h) Any other list element $\beta = \alpha^k$ which, upon taking powers 0 through n-1, yields the same list as α (with a possible reordering of the elements) is also regarded as a *generator*. Such an alternate generator has order n if α has order n.
(i) If $\beta^n = 1$, it does *not* follow that n is the order of β.
(j) We have shown that *any* element of {GF(q) - 0 ,•} lies in *some* cyclic subgroup of *some* order. For example, α lies in (α, n,•). Another example is that 1 lies in (1,1,•).

Proof: (a),(b) All elements in the list are contained in {GF(q) - 0 ,•} which is a finite set. Therefore, there must be a first power where an element of the sequence repeats some earlier element. Suppose this power is n, so that α^{n-1} is the last distinct item on the list, and suppose $\alpha^n = \alpha^k$, some earlier item on the list. If k > 0, then we would have $\alpha^{n-1} = \alpha^{k-1}$, which says that the previous power also repeated an item on the list, which is a contradiction. Thus, we must have k=0, so $\alpha^n = 1$. (c) As we build subsequent powers, the list repeats: $\alpha^n = 1$, $\alpha^{n+1} = \alpha$, $\alpha^{n+2} = \alpha^2$, and so on. (f) Suppose the order of α is 4 so list is {1, α, α^2, α^3} with $\alpha^4 = 1$. Consider $\beta = \alpha^2$. The order of β is 2, not 4. Notice that 2 divides 4. (h) Such alternate generators may or may not exist; (i) Suppose the order of β is 5, so that $\beta^5 = 1$. It is then certainly true that $\beta^{10} = 1$, but this clearly does not imply that β has order 10.

Fact 3: Let g □ {GF(q) - 0 ,•}. If "g has order n" , then $g^n = 1$ and n is the least integer for which $g^n = 1$.

Proof: This follows from the definition of the order of g. We just want to stress the fact.

Fact 4: Let g □ {GF(q) - 0 ,•}. If $g^k = 1$, the "order of g" divides k. .

Proof: Let n be the order of g. We know from the definition that n is the smallest power of g such that $g^n = 1$. Consider some higher power that is not a multiple of n: k = qn + r where 0 < r < n. Then $g^k = g^{qn}$ $g^r = g^r$. But we know that $g^r \neq 1$ since 0 < r < n. Thus, if k is not a multiple of n, $g^k \neq 1$. Therefore, if $g^k = 1$, then k is a multiple of n, and n divides k.

Fact 5: If β is any element of (α,n,•), then $\beta^n = 1$.

Proof: Since β □ (α,n,•), we know that $\beta = \alpha^k$ for some k, and $\alpha^n = 1$. Thus $\beta^n = \alpha^{nk} = 1^k = 1$.

Fact 6: If β is any element of (α,n,•), then the order of β divides n, the order of α. More specifically, we claim that [order of β] = n/GCD(k,n) where $\beta = \alpha^k$.

Proof: Since β □ (α,n,•), we know that $\beta = \alpha^k$ for some k, and $\alpha^n = 1$ Then as we enumerate the subgroup generated by β, we get { 1, β, β^2, β^3 ... } = { 1, α^k , α^{2k} , α^{3k} ...}. If the order of β is m, then $\beta^m = 1$, and our little cyclic subgroup can be called (β,m,•). This implies that m is the smallest integer such that $\alpha^{mk} = 1$. From Fact 4, mk is therefore a multiple of n, so mk = Nn. From the Lemma below, we conclude that m = n/GCD(k,n). Thus, we find that n/m = GCD(k,n), so that m divides n, QED.

Lemma Problem: Given two two integers a and b, find the smallest integer A such that A(a) = B(b) where B is an integer. That is, find the smallest A so that Aa is a multiple of b.

Lemma Solution: A candidate solution is A = b and B = a, so that we get b(a) = a(b). Let d be the greatest common divisor of a and b, so d = GCD(a,b). Then b/d is an integer and a/d is also an integer, so we get our improved solution [b/d] (a) = [a/d] (b) . By definition of GCD, no larger d works, so there is no smaller solution integer A = b/d, so the answer is A = b/GCD(a,b).

Definition: Element a is a *root* of polynomial f(x) means that f(a) = 0.

Fact 7: (The Factor Theorem) Polynomial f(x) can be written as f(x) = (x-a)q(x) for some polynomial q(x) if and only if a is a root of f(x).

Proof: (1) Assume a is a root of f(x). By the Division Algorithm, we can expand f(x) = (x-a)q(x) + r(x) where the remainder polynomial r(x) has degree less than (x-a), which means it has degree 0, which means r(x) = constant K. Since f(a) = 0, we see that r(x) = K = 0, QED. (2) Assume f(x) = (x-a)q(x). Since q(x) is a polynomial, q(a) is finite, so f(a) = 0.

Fact 8: The n elements of some cyclic subgroup $(\alpha,n,\bullet)$ 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.

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

Proof: We know from Fact 5 that $a^n = 1$ for all n elements in the cyclic subgroup. Thus, these n elements are all roots of $f(x) = 1 - x^n$. According to Fact 7, each such root results in a factor (x-a). Since this polynomial has at most n roots and we have found them all, it fully factors as claimed.

Fact 9: Consider two cyclic subgroups $A = (\alpha,n,\bullet)$ and $B = (\beta,m,\bullet)$. If n=km , then A contains B.

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

Corollary : There can be at most one cyclic subgroup of any given order.

Proof: Let b □ $(\beta,m,\bullet)$. From Fact 5, $b^m = 1$. Raise both sides of this last equation to power k to get $b^{mk} = 1$. If mk=n, we get $b^n = 1$ Thus, b is a root of $f(x) = 1 - x^n$. Since A is a cyclic subgroup of order n, we know by Fact 8 that the n roots of $f(x) = 1 - x^n$ are all elements of A. Since b is a root of f(x), b must equal one of the elements of a. Thus, b is contained in A. Since this is true for any b in B, this means all of B is contained in A. Corollaries follow from k=1.

Definition: The *exponent* e is the order of the *largest* cyclic subgroup E in {GF(q) - 0}, •}.

Fact 10: The order of any cyclic subgroup of {GF(q)-0,•} divides the exponent e.

Proof: This Fact 10 looks innocent enough, but it is the real meat and potatoes of this entire section. We are assuming there is some maximal cyclic subgroup called E of order e. As far as we know at this point in the development, E can be less than all of {GF(q)-0,•}. Thus, if there is some cylic subgroup called G, we do not know that G is contained in E. If we knew that, we would immediately know Fact 10, since the order of any subgroup G divides the order of the containing subgroup E.

So at this point, as far as we know, G may or may not be contained within E. Thus, we need to find a more general proof of Fact 10. Although this proof is very tricky, it uses only Fact 4, Fact 5, and the basic properties of integers. The proof is given in Appendix 4.1 at the end of this Chapter.

Based on Fact 10, we will quickly arrive at Big Theorem 1 below which says that {GF(q) - 0, •} is cyclic. This implies that E must indeed be all of {GF(q) - 0, •}. In retrospect, Fact 10 seems less impressive. But one must remember that the information that E = {GF(q) - 0, •} is not available for the proof of Fact 10.

Big Theorem 1: The entire group {GF(q) - 0, •} is cyclic.

Proof: Consider *any* element α of {GF(q) - 0, •}. From Fact 2(j), it must lie in some cyclic subgroup of some order n. From Fact 5 we know its elements are solutions of $1 = x^n$. From Fact 10 we know that e, the order of the largest cyclic subgroup, must be a multiple of n, we can write e = kn. Raise both sides of $1 = x^n$ to the kth power then to get $1 = x^e$. Thus, we have shown that *any* element α of {GF(q) - 0, •} is a root of $f(x) = 1 - x^e$.

But this f(x) can have at most e roots. Since all q-1 elements of {GF(q) - 0, •} are roots, we know that $q-1 \le e$. On the other hand, it is clear that $e \le q-1$ since e is the order of a cyclic subgroup contained within {GF(q) - 0, •} . 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.

The structure of this proof and Fact 10 were both taken from the reference given in Appendix 4.1.

Fact 11: There exists at least one generator α for {GF(q) - 0, •}. In terms of it, the entire group GF(q) can be enumerated as follows:

$$\{\ 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3, \ldots\ldots\ \alpha^{q-2}\ \} \qquad \alpha^{q-1} = 1\ \alpha^q = \alpha$$

Proof: Since {GF(q) - 0, •} is cyclic and is of order q-1, it must have a generator α. Then we add back the 0 element to get GF(q).

Definition: Any generator of {GF(q) - 0, •} is called a *primitive element* of GF(q). Thus, the α shown above is a primitive element of GF(q).

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

Proof: From Fact 6, the order of α^k is (q-1)/GCD(k,q-1), . If GCD(k,q-1) = 1, the order of α^k is q-1, so α^k is a primitive element of GF(q). If GCD(k,q-1) ≠ 1, then GCD(k,q-1) = N > 1, and order of α^k = (q-1)/M, so in this case α^k is not a primitive element.

Fact 13: If q-1 is prime, all elements of {GF(q) - 0 - 1} are primitive elements of GF(q).

Proof: If q-1 is prime, then *any* k [in the range 0<k<q-1] and q-1 are relatively prime, so GCD(k,q-1) = 1. Thus, from Fact 12, *any* power α^k of a primitive element α with 0<k<q-1 is a primitive element.

Example: GF(4 = 2^2) has q-1 = 3 = prime. The elements are {0,1,α,β}. Either α or β can serve as a generator, they are both primitive elements. Thus, $\beta = \alpha^2$ and $\alpha = \beta^2$. In terms of m-tuple notation and the tables given earlier in this Chapter:

If α = 01, then $\beta = \alpha^2 = 01 \bullet 01 = 11 = \beta$ If β = 11, then $\alpha = \beta^2 = 11 \bullet 11 = 01 = \alpha$

Example: GF(8 = 2^3) has q-1 = 7 = prime:

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

This field has 6 distinct primitive elements. Here they are: $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

Example: GF(16 = 2^4) has q-1 = 15 ≠ prime. If α is a primitive element, then $\beta = \alpha^3$ is not a primitive element. In fact, the order of β's subgroup is 5, not 15: [From Fact 6, 5 = 15/GCD(3,15) = 15/3]

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

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

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

1) The q-1 elements of {GF(q) - 0, •} 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(α) = 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, •} is cyclic. Item #1 is true for any cyclic subgroup, as shown in Fact 8. 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, as argued in Fact 8. Each form of the above theorem stresses a certain point.

Fact 14: All facts above apply to GF(p) since this is a special case of GF(q).

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

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

Fact 15: {GF(p) - 0, •} is a cyclic subgroup, order p-1, of {GF(q) - 0, •} which has 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 16: 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 have $\alpha^{p-1} = 1$, so that α is a root of $x^{p-1}-1$. Since {GF(p) - 0, •} is a a cyclic subgroup of {GF(q) - 0, •} of order p-1, we know from Fact 8 that all p-1 roots of x^{p-1} are elements of {GF(p) - 0, •}. Since α is a root of x^{p-1}, it must be one of the elements of {GF(p) - 0, •}. Thus, whether or not $\alpha=0$, we conclude that $\alpha^p = \alpha$ $\alpha \in$ GF(p).

An example of root factorization: GF(4)

Earlier we displayed the + and • tables for GF(4). Here they are again:

+	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

•	00	10	01	11
00	00	00	00	00
10	00	10	01	11
01	00	01	11	10
11	00	11	10	01

We know that 00 = **0**, and 10 = **1**. According to Big Theorem 2, we should have:

$$(x^4 - x) = (x - a_1)\bullet(x - a_2)\bullet(x - a_3)\bullet(x - a_4)$$

$$= (x - 00)\bullet(x - 10)\bullet(x - 01)\bullet(x - 11)$$

Let's check to see if it works. We can divide out the x to get:

$$(x^3 - 1) = (x - 10)\bullet(x - 01)\bullet(x - 11)$$

But we can factor $(x^3 - 1) = (x - 1)\bullet(x^2 + x + 1)$, so it remains only to show that

$$(x^2 + x + 1) = (x - 01)\bullet(x - 11)$$

Since p = 2 here, we know that $2\mathbf{x} = \mathbf{0}$. That is, x + x = 0, which means that a - b = a - b + 0 = a - b + 2b = a + b. So we rewrite the above as

$$(x^2 + x + 1) = (x + 01)\bullet(x + 11) = x^2 + (01 + 11)\,x + 01\bullet 11$$

Looking up in the tables, we get 01 + 11 = 10 which is the 1 element, and 01•11 = 10 as well. Thus, we have now seen a specific example, GF(4) = GF(2^2), where the polynomial $(x^4 - x)$ fully factors into a product of four linear factors of the form (x-a), one for each element of GF(4).

Notice that $(x^2 + x + 1)$ factors in GF(4) into (x - 01)•(x - 11). However, in GF(2) -- the ground field -- we cannot factor $(x^2 + x + 1)$. In fact, this is f(x), the irreducible polynomial which defines GF(4) .

Labeling Elements of GF(q), and the + and • Tables

In this chapter we have discussed two convenient labeling methods for the elements of GF(q).

One method is to use the m-tuples which consist of m GF(p) "digits", where m is the degree of f(x). Each m-tuple stands for a remainder polynomial in the residue class ring which we identify with GF(q). In this method, the + and • tables all contain m-tuple entries. We saw earlier in this chapter how the + table is trivial to construct in terms of m-tuples -- you just do modulo-p addition on each digit of a pair of m-tuples. However, the • table entry took much more work. You got a convolution of m-tuple digits (since you are multiplying polynomials together), and then you had to take a remainder if the degree was larger than m.

A second labeling method is to find a generator = primitive element α, and list the elements as powers of α. In this method, each + and • table entry is a power of α. In this case, the • table is trivial to construct. You just multiply powers and use the fact that $\alpha^{q-1} = 1$. However, now the + table is non-trivial to construct. Here, you have to convert the powers of α to m-tuples, add, then convert back.

The two labeling methods are like having two different bases, or coordinate systems. In the m-tuple basis, addition is easy and multiplication is hard. In the α basis, just the opposite is true.

Here are the GF(4) tables in both bases:

1. Here is the m-tuple basis , where $f(x) = 1 + x + x^2$. The + table can be verified by inspection, but the • table cannot:

+	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10

•	00	10	01	11
00	00	00	00	00
10	00	10	01	11
01	00	01	11	10

11	11	01	10	00

11	00	11	10	01

2. Here is the α basis for $\alpha = 01 = 0x^0 + 1x^1 = 0 + x = x$, and $\alpha^3 = 1$. The $\bullet$ table can be verified by inspection, but the + table cannot. Note in passing that $f(x) = 1 + x + x^2 = 1 + \alpha + \alpha^2$.

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\bullet$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Selected Facts About GF(q)

We try to arrange this list in the same order as the list for GF(p) in Chapter 2.

Fact: The q-1 elements of {GF(q) -0} form a cyclic group under • of order q-1. The generators of this cyclic group are called primitive elements of GF(q) Thus, GF(q) can be enumerated as :

$\{ \mathbf{0}, \mathbf{1}, \alpha, \alpha^2, \alpha^3, \ldots\ldots \alpha^{q-2} \}$ $\alpha^{q-1} = 1$ $\alpha^q = \alpha$

Saying that the group is cyclic implies that at least one primitive element α exists.

Proof: See Big Theorem 1 above.

Fact: For any element $\boldsymbol{\beta}$ of GF(q) , we claim that $\beta^q = \beta$

Proof: See Big Theorem 2 (4) above.

Fact: $p\boldsymbol{\beta} = \mathbf{0}$ for any element $\boldsymbol{\beta}$ of GF(q).

Proof: See first section of this chapter.

Fact: $(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$ when **a**,**b** are elements of GF(q).

Proof: Same as the proof in Chapter 2, except here we say that the binomial coefficients of the cross terms vanish because $p\boldsymbol{\beta} = \mathbf{0}$ for any element $\boldsymbol{\beta}$ of GF(q).

Fact: $(a + b + c + d + \ldots)^p = a^p + b^p + c^p + d^p + \ldots$ for a,b,c,d... in GF(q).

Proof: just apply the above binomial theorem proof a bunch of times.

Appendix 4.1 Proof of Fact 10

Theorem: The order of any cyclic subgroup in {GF(q)-0,•} divides the exponent e.

This proof is a fleshed-out version of a 3-column-inch proof given in Bobrow and Arbib, *Discrete Mathematics*, their Lemma 7 of Chapter 8. We include this proof because it is the essence of the proof that GF(q) is cyclic, which is the single most important fact about GF(q).

Recall that the exponent e is defined to be the order of the largest cyclic subgroup in {GF(q)-0,•}. Let e' be the order of some other subgroup (α,e',•). We want to show that e' divides e.

We will assume that e' does *not* divide e and show that there is a contradiction. The proof has many steps, so they will be numbered.

Step 1. If e' does not divide e, then e and e' can be written as follows:

$e = Rn \qquad R = p^r \qquad s > r \geq 0 \; S>R>1$ r,s,m,n are integers

$e' = Sm \;\; S = p^s$ p = some prime number p does not divide n or m

Proof. Expand both e and e' in terms of powers of primes using the Factorization Theorem of Chapter 1. The p_i are the primes in some standard order, and the exponents are all integers ≥ 0.

$$e = (p_1)^{r_1} (p_2)^{r_2} (p_3)^{r_3} \ldots$$

$$e' = (p_1)^{r_1'} (p_2)^{r_2'} (p_3)^{r_3'} \ldots$$

If e' divides e, then we know that $r_i \geq r_i'$ for all i. In other words, we have to have e' divides e in each prime power component. Therefore, if e' does *not* divide e, there must be at least one prime where this is not true. Thus, let p = this p_i, let $r_i = r$ and $r_i' = s$, so that s > r, and r≥0 since it is an exponent.

$e = (p)^r \bullet$ [all the other primes to their powers] $= p^r n = Rn \qquad s>r \qquad S>R$

$e' = (p)^s \bullet$ [all the other primes to their powers] $= p^s m = Sm$

The bracketed quantities are of course integers which do not contain any powers of the prime p.

Step 2. Consider G = (g,e,•) and G' = (g',e',•). That is, g is a generator of G of order e, and g' is a generator of G' of order e'. Then construct these two elements:

$g_1 = (g)^R$	in G	Claim that order of $g_1 = n$.	$(g_1, n, \bullet) = G_1$
$g_2 = (g')^m$	in G'	Claim that order of $g_2 = S$.	$(g_2, S, \bullet) = G_2$

Proof: Consider these facts:

$$(g_1)^n = (g)^{nR} = (g)^e = 1$$

$(g_2)^S = (g')^{Sm} = (g')^{e'} = 1$

In each line, the last equality is due to fact that e and e' are the orders of the two subgroups G and G'. This is an application of Fact 5. Since $(g_1)^n = 1$, according to Fact 4 we know that the order of g_1 divides n. So we write both:

$(g_1)^n = 1$	(order of g_1) divides n	(order of g_1) = n/d_1
$(g_2)^S = 1$	(order of g_2) divides S	(order of g_2) = S/d_2

We now argue that $d_1 = d_2 = 1$. If this is not so, then for example get:

$(g_1)^{n/d_1} = (g)^{nR/d_1} = (g)^{e/d_1} = 1$
$(g_2)^{S/d_2} = (g')^{Sm/d_2} = (g')^{e'/d_2} = 1$

The top last equality here says (order of g) divides (e/d_1) for d1>1. This implies that (order of g) < e. This is a contradiction since we assumed at the start that (order of g) = e. Thus $d_1 = 1$. Similarly for the lower line. Therefore:

$d_1 = 1$	(order of g_1) = n
$d_2 = 1$	(order of g_2) = S

So now we know the order of our two constructed elements g_1 and g_2.

Step 3. Now construct element $g_3 = g_1 g_2$. Let d = (order of g_3) as shorthand, so we have $G_3 = (g_3, d, \bullet)$.

1. $(g_3)^d = 1$
2. d divides nS.

Proof: (1) This follows from Fact 2. (2) Using above facts, find that:

$(g_3)^{nS} = [(g_1)^n]^S [(g_2)^S]^n = 1^S 1^n = 1$

Therefore, from Fact 4, we know that (order of g_3) divides nS, so <u>d divides nS</u>. This result will again be used at the very end of this proof.

Step 4. Define $h = (g_1)^d$. Claim that h lies in both G_1 and G_2 .

Proof: We know that $(g_3)^d = 1$. Therefore, $(g_1^d)\ (g_2^d) = 1$. Therefore $(g_1^d) = (g_2^d)^{-1}$, the inverse element of (g_2^d). But the inverse of any element in G_2 is in G_2 , since it is a group. Thus, $h = (g_1^d)$ lies in G_2. Of course it also lies in G_1 since it is a power of g_1.

Step 5: Now consider the subgroup (h, I, •) generated by h, let I be its order. We claim that

I divides n
I divides S

Proof: Since h is in G_1 , we know from Fact 5 that $h^n = 1$ since n is the order of G_1. Since I is the order of h, we know from Fact 4 that I divides n. Similarly, since h is in G_2, we know from Fact 5 that $h^S = 1$ since S is the order of G_2. Since I is the order of h, we know from Fact 4 that I divides S.

Step 6: Claim the following sequence of results:

1. I = 1
2. h = 1
3. $(g_1^d) = 1$ and $(g_2^d) = 1$.
4. n divides d
4. S divides d

Proof: (1) We know that $S = p^s$ for some prime p, and that n has no powers of p. This means that GCD(n,S) = 1, n and S are "relatively prime". If a number divides into both n and S, that number must be 1. Therefore, from Step 5, I = 1. Thus, our subgroup (h, I, •) has order I = 1; (2) I=1 means that $h^1 = 1$, or simply h = 1. (3) Since (g_1^d) $(g_2^d) = 1$ and $h = (g_1)^d$, the last results follows. (4) Since order of G_1 is n, and since $(g_1^d) = 1$, we know from Fact 5 that n divides d. (5) Since order of G_2 is S, and since $(g_2^d) = 1$, we know from Fact 5 that S divides d.

Step 7: Claim that nS divides d.

Proof: We have already noted that n and S are relatively prime. Thus, if these two numbers both divide into a third number, that third number must be a multiple of nS. From 4 and 5 above, we know that n and S each divide d, and therefore d must be a multiple of nS. Thus, nS divides d.

Step 8: Claim that d = nS.

Proof: From Step 3 above, we learned that d divides nS. From Step 7 we learned that nS divides d. The conclusion is that d = nS.

Step 9: This leads to the contradiction that d > e, and therefore e' divides e.

Proof: Recall that d is the order of field element g_3 in $G_3 = (g_3, d, \bullet)$. We have just shown that d = nS. Since S > R, we know that d > nR. But nR = e, so we have d > e. This is a contradiction because the order of any subgroup is supposed to be less than e -- this was how e was defined.

Recap of the above proof.

The idea is, based on the assumption that e' does not divide e, , to identify some subgroup which has order greater than e, and this is then a contradiction since e is supposed to be the maximal subgroup order. The too-large subgroup is G_3 of order d generated by $g_3 = g_1 g_2$. The proof is really finished at Step 7 where it is found that nS divides d, so that $d \geq nS > nR = e$.

Step 1: Relate (e = order of G) and (e' = order of G') to the four integers R,S,n,m.
Step 2A: Let G = (g,e,•), define $g_1 = g^R$, show order of g_1 = n, so define $G_1 = (g_1 , n, \bullet)$
Step 2B: Let G' = (g',e',•), define $g_2 = g'^m$, show order of g_2 =S, so define $G_2 = (g_2 , S, \bullet)$
Step 3: Consider $G_3 = (g_3, d, \bullet)$, where $g_3 = g_1 g_2$, order d. Since $(g_3)^{nS} = 1$, find that d divides nS.

Step 4: Let $h = g_1^{d,}$ order I. Show that h□ G_1 and h□ G_2
Step 5: I divides n and S
Step 6: I = 1, so $h = g_1^d = 1$; n and S divide d
Step 7: nS divides d

Step 8: d = nS
Step 9: d > e, which is contradiction.
Therefore, e' divides e.