# Chapter 6: The GF(q) Table

**Chapter Contents**.

**Development History of the Primitive Polynomial**

**Using a Primitive Polynomial as the f(x) in GF(q) = R/I = Polys[ x,GF(p)]/ ( f(x) )**

**Fact**: $f(\alpha) = 0$ for $\alpha + \{x\}$ . { $\alpha$ may or may not be a primitive element of GF(q) }

Construction of the m-tuple *table* for $GF(p^m)$ using powers of $\alpha + \{x\}$

**Question**: Have we by this table construction enumerated all elements of GF(q) - 0 ?

**Fact**: If we choose f(x) to be a *primitive* polynomial of GF(q), then the above table *will* in fact enumerate all non-zero elements of GF(q).

**Fact**: If the Polys[ x,GF(p)]/ ( f(x) ) defining polynomial f(x) of degree m is selected to be p(x), a *primitive polynomial* of GF(q), then the remainder function r(x) = x which belongs to chart row {x}, and which is represented by the m-tuple 010000... , labels a *primitive element* $\alpha$ of GF(q). All other elements of {GF(q) - 0} can therefore be represented as powers of this primitive element $\alpha$.

**Example : The Table for GF(8 = $2^3$)**.

**Question**: Why is this table so useful?

**Sample Minimum Polynomial Calculations**:

## Chapter 6: The GF(q) Table

In Chapter 5 we spent much time developing the notion of a primitive polynomial. In this chapter, we show why primitive polynomials are useful. They let us make a concise table to enumerate all elements of GF(q) as both powers of some $\alpha$, and as m-tuples. From this table, the • and + field operation tables can be immediately derived.

## Development History of the Primitive Polynomial

It is now time for a glance back at the development of the previous chapters.

Chapter 1 provided the underpinning mathematical formalisms, especially the idea of a residue class ring formed as R/I where I is some ideal in a ring R.

In Chapter 2 the connection was made between GF(p) and $Z_p$ , the field of integers modulo p. Once this connection was made, we knew at once how to construct the + and • operation tables for GF(p). However, general facts about GF(q) which applied to GF(p) as a special case were not yet developed.

We knew that the study of $GF(p^m)$ required the use of polynomials, so this was the main topic of Chapter 3. The grand connection was made that

$$GF(p^m) = R/I = Polys[x,GF(p)] / ( f(x) )$$

where f(x) was any irreducible monic polynomial of degree m. We know in retrospect that there are usually many choices for f(x), some of which are primitive polynomials, and some of which are not. We know that changing from one f(x) to another does not change the structure of $GF(p^m)$, it just alters the "basis", which is to say, it alters the way the elements are named. Formally speaking, the different versions of $GF(p^m)$ obtained by changing f(x) are all isomorphic to each other.

Then came Chapter 4 where most of the "facts" about $GF(p^m)$ were painfully extracted and proved. It was like pulling teeth. The m-tuple notation was introduced as a convenient way to label the $p^m$ remainder polynomials which are in effect the elements of $GF(p^m)$. It was noted that in the tuple basis, the + table is trivial to construct, but the • table is painful to construct, requiring many long divisions to find remainder polynomials.

We then considered the cyclic subgroups of GF(q) and were then able to derive many facts about GF(q). For example, each element of GF(q) has some "order" n. We learned that there is always at least one *primitive element* which has order q-1 and whose powers can be used to enumerate the whole field {GF(q) -0}. In other words, we learned that {GF(q)-0,•} is *cyclic*.

This suggested another "basis" for labelling the elements of GF(q), namely, the "powers of $\alpha$" basis, where $\alpha$ is some primitive element. In this basis, we noted that the • table was trivial to write down, but the + table was painful to develop. We compared the two bases for GF(4) toward the end of Chapter 4.

We then learned that the little polynomial $x^{q-1}- 1$ can be exploded into a product of linear factors, each of which contains an element of GF(q). For the first time, this caused us to think about the idea that a polynomial might have roots in GF(q) due to these factors (x-a). Soon, we became comfortable with the idea of a polynomial having some roots in GF(q).

If we look back now at Chapter 3 on polynomials, there was no concept of a polynomial f(x) having an element $\alpha$ of GF(q) as a *root*, which is to say $f(\alpha) = 0$. In Chapter 3, polynomials were what lived in the chart rows of the R/I residue class ring. The rows of this chart *were* the elements of GF(q), but we did not consider to write f(some row) = 0, where "some row" was a root of f. It was not reasonable to think of our defining f(x) as having roots in Chapter 3 because after all, f(x) was supposed to be irreducible over GF(p) which meant you could not factor it, so it seemed there were no roots at all. We later realized that any polynomial f(x) defined over the field GF(p) can be extended to have definition over GF(q), and it is here that an "irreducible in GF(p)" polynomial might have roots. As will be seen below, it is perfectly reasonable to observe that f( {x}) = 0 when f(x) is the defining polynomial, and where {x} is the row containing the polynomial x.

In Chapter 5 we defined the *minimum polynomial* m(x) of some $\alpha$ in GF(q) to be the smallest set of (x-a) factors which contains the factor $(x-\alpha)$ and which has coefficients in the ground field GF(p). We then noted that m(x) has several roots in GF(q) -- the elements of the conjugate set of $\alpha$. The exact number of roots is not known in general, it is some $k \le m$ where m is the m of $q = p^m$.

Finally, we said that if $\alpha$ is a primitive element of GF(q), then minimum polynomial m(x) gets the special name of being a *primitive polynomial* of GF(q). We noted several facts about such primitive polynomials p(x) : they are monic, irreducible in GF(p), $p(\alpha) = 0$ for some primitive element of GF(q), they are of degree m for $GF(q=p^m)$, they have *period* = q-1.

We considered briefly how one might search for the primitive polynomials for $GF(p^m)$. We know for sure that there is *at least one* primitive polynomial for any choice of p and m, and there is generally more than one. This is simply because there is likely to be more than one cyclic generator of GF(q). One got the impression in Chapter 5 that the process of searching for the p(x) for GF(q) could be automated in some way. To be sure, there exist tables which list at least one primitive polynomial for any choice of p and m. For example, on page 28 Rhee lists (for p=2 only) one primitive polynomial for each power m in the range m=2 through 27.

Having done all this work, the reader must wonder: Why are primitive polynomials useful? Where is the payoff?

## Using a Primitive Polynomial as the f(x) in GF(q) = R/I = Polys[ x,GF(p)]/ ( f(x) )

We have already noted that this is possible, since any primitive polynomial p(x) is irreducible over GF(p) and has degree m. We shall now learn that there is a great advantage in making this selection for f(x). We shall show this by first *not* doing so.

We know that we can represent the elements of GF(q) as m-tuples consisting of m digits, where each digit lies in GF(p). And each such m-tuple is a shorthand notation for a GF(p) remainder polynomial of

degree less than m (relative to the defining polynomial f(x)) which characterizes a row of the R/I chart, that is to say, which characterizes an element of GF(q). For example,

m-tuple = 1ab0... × {r(x)} = {1 + ax+ b $x^2$ + ...} 1,a,b □ GF(p)

Let us now single out one very simple m-tuple and give it a name:

$\alpha$ + {x} = 0100....

Thus, as defined right here, $\alpha$ is the element of GF(q) which corresponds to the R/I chart row {x} which contains the polynomial x. Assume that we use some generic irreducible f(x) to define our R/I chart. We can then start building a table of powers of $\alpha$ as follows: (assume p = 2, m = 4)

| | | |
|---|---|---|
| $\alpha^0$ | {1} | 1000 |
| $\alpha$ | {x} | 0100 |
| $\alpha^2$ | {$x^2$} | 0010 |
| $\alpha^3$ | {$x^3$} | 0001 |
| $\alpha^4$ | {$x^4$} | ???? |

We know that if $\alpha$ is the row containing x, then $\alpha^2$ is the row (in the R/I chart) containing $x^2$, and so on. When we reach the power 4, we have to do a remainder calculation. Assume that f(x) = 1 + $x^2$ + $x^4$, which happens *not* to be a primitive polynomial for GF($2^4$). Then Rem($x^4$/f) = 1 + $x^2$, and this lets us continue with the chart:

| | | |
|---|---|---|
| $\alpha^4$ | {$x^4$} = {1 + $x^2$} | 1010 |

The next row will be $\alpha^5$= $\alpha$ ($\alpha^4$) = {x}•{1+$x^2$} = {x + $x^3$}, so

| | | |
|---|---|---|
| $\alpha^5$ | {$x^5$} = {x + $x^3$} | 0101 |

In this manner, we can build up all powers through $\alpha^{15}$. The job of building the chart is really quite simple and fast. In fact, one does not have to compute any remainders due to the following fact, which may not have been obvious before now:

**Fact**: f($\alpha$) = 0 for $\alpha$ + {x} . { $\alpha$ *may* or may *not* be a primitive element of GF(q) }

**Corollary**: Thus, for our f(x), we have $\alpha^4$ = -$\alpha^2$-1 = $\alpha^2$ + 1, so we can always replace $\alpha^4$ with lower powers of $\alpha$, and in this way build the entire chart without having to do any remainder divisions.

**Proof**: We can certainly write:

{f(x)} = { 1 + $x^2$ + $x^4$ } = {0}

The {0} indicates the chart row which has remainder polynomial 0. This is the top row of the R/I chart, the ideal I. It is to be identified with the 0 element of GF(q). Thus, we can go on to write, using our definition above that $\alpha$ + {x},

$$\{f(x)\} = \{ 1 + x^2 + x^4 \} = \{x\}^0 + \{x\}^2 + \{x\}^4 = f(\{x\})$$
$$= f(\alpha) = \alpha^0 + \alpha^2 + \alpha^4 = 1 + \alpha^2 + \alpha^4 = \{ 0 \} = 0.$$

This is a long winded way of saying that for $\alpha = \{x\}$, we know that $f(\alpha) = 0$, as an equation in GF(q).

So, having build the above table with its 15 entries, we now ask a critical question:

**Question**: Have we in this manner enumerated all elements of GF(q) - 0 ?

**Answer**: No!!! At least there is no guarantee. How do we know that we "hit" all q-1 = 15 distinct m-tuples by this construction? If $\alpha$ as defined above *happens* to be a primitive element of GF(q), then all the m-tuples will be hit, because by definition, $\alpha$ would then be a generator of the full group $\{GF(q) - 0, \bullet\}$. This is our motivation.

**Fact**: If we choose f(x) to be a *primitive* polynomial of GF(q), then the above construction *will* in fact enumerate all non-zero elements of GF(q).

**Proof**: If we had selected f(x) to be some *primitive* polynomial of GF(q), we would know that *all* roots of f(x) are primitive elements of GF(q). This follows from Fact 8(b) and Big Theorem 3 of Chapter 5. We would then look at our construction above where $f(\{x\}) = 0$, and we would conclude that $\alpha = \{x\}$ must therefore be some primitive element of GF(q). Thus, in the above enumeration, we would know that all elements of $\{GF(q) - 0, \bullet\}$ are hit.

Which primitive element of GF(q) is $\alpha = \{x\}$ ? It must be one of the ones in the set of primitive elements which solve $f(\beta) = 0$ for our selected primitive polynomial. Recall that a primitive polynomial is a product of factors of the form (x-a) where the a are the members of the conjugate set of $\beta$. So our $\alpha$ must be some element in this set of primitive elements. We do not care which one it is, we only care that it is a primitive element!

Now there is a point we can make about the meaning of the m-tuple labels. They label the elements of GF(q), but they do so *relative* to the selected defining function f(x). The m-tuple labels are like coordinate system axes used analyze some physical problem. Changing from one defining f(x) to some other f(x) is like changing or rotating the coordinate system to some other set of axes. It is well known that problems are easier to handle in some coordinate systems than in others. For example, a system with cylindrical geometry is very difficult to work with in a cylindrical coordinate system that happens not to line up with the symmetry axis.

In general, there is no reason one would imagine that the (row of the) remainder function r(x) = x and its m-tuple representation 01000.. would be a *primitive* element of GF(q). This would be an amazing coincidence, one would think offhand. It turns out, as shown above, that by using a primitive polynomial as the defining f(x), this is exactly what happens. Using a primitive polynomial is like choosing a smart coordinate system.

We have now proved the following claim, which summarizes the content of this section:

**Fact**: If the Polys[ x,GF(p)]/ ( f(x) ) defining polynomial f(x) of degree m is selected to be p(x), a *primitive polynomial* of GF(q), then the remainder function r(x) = x which belongs to chart row {x}, and which is represented by the m-tuple 010000... , labels a *primitive element* $\alpha$ of GF(q). All other elements of {GF(q) - 0} can therefore be represented as powers of this primitive element $\alpha$.

Now we return to the details of constructing the table. Back to general GF($p^m$), we know that our primitive polynomial p(x) is monic and of degree m, so write it as follows:

$$p(x) = x^m + p_{m-1}x^{m-1} + p_{m-2}x^{m-2} + \ldots + p_3x^3 + p_2x^2 + p_1x + p_0$$

[ $p_0 \neq 0$ because otherwise x could be factored out and p(x) would not be irreducible.] We know that $p(\alpha) = 0$, where $\alpha$ equals {x} *and* $\alpha$ is known to be a primitive element of GF($p^m$). We move the first term to the left and write:

$$\alpha^m = -[\, p_{m-1}\alpha^{m-1} + p_{m-2}\alpha^{m-2} + \ldots + p_3\alpha^3 + p_2\alpha^2 + p_1\alpha + p_0]$$

$$= (p-p_{m-1})\,\alpha^{m-1} + (p-p_{m-2})\,\alpha^{m-2} + \ldots + (p-p_1)\,\alpha + (p-p_0)$$

In the second line we have used the fact that -a + (p-a) for a lying in GF(p). Thus, we are able to replace $\alpha^m$ with a sum of lower powers of $\alpha$. This equation exists in the space GF(q), not GF(p). We are writing the GF(q) element $\alpha^m$ as a sum of other elements of GF(q). The coefficients are still in GF(p).

So now the construction of a complete table for GF($p^m$) is a straightforward and fast mechanical procedure once some primitive polynomial p(x) is specified. There are no remainder division computations needed, one just keeps re-using the $p(\alpha) = 0$ equation to reduce things to degree less than m.

**Example GF(8 = $2^3$)**. From the primitive polynomial lookup table in Rhee we find that $p(x) = 1 + x + x^3$. Therefore, setting $p(\alpha) = 0$ we get this reduction rule: $\alpha^3 = 1 + \alpha$. So we can build the entire table in 2 minutes:

| | | | | |
|---|---|---|---|---|
| 0 | | 000 | 0 | |
| $\alpha^0 = 1$ | 100 | 4 | | |
| $\alpha^1 = \alpha$ | 010 | 2 | | |
| $\alpha^2$ | | 001 | 1 | |
| $\alpha^3 = 1 + \alpha$ | | 110 | 6 | |
| $\alpha^4 = \alpha + \alpha^2$ | | 011 | 3 | $\alpha^4 = \alpha\,\alpha^3 = \alpha(1 + \alpha) = \alpha + \alpha^2$ |
| $\alpha^5 = 1 + \alpha + \alpha^2$ | 111 | 7 | | $\alpha^5 = \alpha\,\alpha^4 = \alpha^2 + \alpha^3 = \alpha^2 + \alpha + 1$ |
| $\alpha^6 = 1 + \alpha^2$ | | 101 | 5 | $\alpha^6 = (\alpha^3)^2 = (1+\alpha)^2 = 1 + \alpha^2$ |

Notice that all 3-tuples are "hit", as claimed above. We have added some octal/hex numbers to make this fact more obvious. Also we know that $\alpha^7 = 1$, since the non-zero elements of GF(8) form a cyclic group under •. This fact was not needed to build that above table, but it is needed to construct the • table.

**Question**: Why is this construction so useful?

**Answer**: The reason is that it provides an immediate + addition table. Recall from our earlier discussion that in the powers-of-α basis, the • table was trivial , but the + table was difficult to compute. With the above construction, the • table is still trivial, but the + table is now almost as trivial! Here are some sample computations:

• table: $\alpha^5 \bullet \alpha^6 = \alpha^{11} = \alpha^4$ and so on, not much more to say, since $\alpha^7 = 1$

+ table:
$\alpha^5 + \alpha^6 = (1 + \alpha + \alpha^2) + (1 + \alpha^2) = \alpha$
$\alpha^5 + \alpha^4 = (1 + \alpha + \alpha^2) + (\alpha + \alpha^2) = 1$
$\alpha^5 + \alpha^3 = (1 + \alpha + \alpha^2) + (1 + \alpha) = \alpha^2$
$\alpha^5 + \alpha^2 = (1 + \alpha + \alpha^2) + ( \alpha^2) = 1 + \alpha = \alpha^3$
etc.

So by choosing a primitive polynomial to develop the extension field,

$$GF(p^m) = Polys[x,GF(p)] / ( p(x) ),$$

We can construct the above m-tuple table for any p and any m, and we then know how to add and multiply group elements with ease.

**Sample Minimum Polynomial Calculation**: Suppose we want to compute all minimum polynomials m(x) for α elements in GF(8). We start off with α, and pick up 3 of our 6 non-trivial field elements:

$$m_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$$

The subscript on m is conventionally used to denote the lowest power of α in the grouping. Now we have a way to multiply this out to get a reasonable polynomial. Using the above table we get:

coeff of $x^3 = 1$
coeff of $x^2 = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + ( \alpha + \alpha^2) = 0$
coeff of $x^1 = \alpha^3 + \alpha^5 + \alpha^6 = (1 + \alpha) + (1 + \alpha + \alpha^2) + (1 + \alpha^2) = 1$
coeff of $x^0 = \alpha^7 = 1$

Thus, we find

$$m_1(x) = 1 + x + x^3.$$

As expected, $m_1(x)$ for α is exactly p(x) used above. Here is a more interesting computation, which picks up the three remaining non-trivial field elements.

$$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$$

Since every element in GF(8) is known to be a primitive element, we are not surprised to find m = 3 factors in this grouping as well. The reader may verify that:

$m_3(x) = 1 + x^2 + x^3$ .

Since $\alpha^3$ is a primitive element, this must be another acceptible primitive polynomial. We could use it to develop another version of the above table. [ We already knew this was an acceptible p(x) from Fact 12 of Chapter 5, which says you can reverse the coefficients on a p(x) to get another p(x). ]