$C(D) = [X_{N-1} D^{N-1} + \cdots + X_r D^r] \bmod g(D) = I(D) \bmod g(D)$

As the check digits are being calculated, the information digits are simultaneously shifted into the encoder and onto the channel. After the last information digit has entered the encoder, the check digits are in the register. The feedback is disabled and the check digits are shifted out to the channel.

c. More Properties of Galois Fields

Consider $GF(q)$ with elements $0, \alpha_1, \cdots, \alpha_{q-1}$. The nonzero elements $\alpha_1, \cdots \alpha_{q-1}$ form an abelian group with $q-1$ elements. The order of each element must divide $q-1$ (Thm 2). Thus $\alpha_i^{q-1} - 1 = 0$, $i = 1, \cdots, q$. Thus the roots of $D^{q-1} - 1$ are $\alpha_1, \cdots \alpha_{q-1}$ so

$$D^{q-1} - 1 = \prod_{i=1}^{q-1} (D - \alpha_i)$$

EX: $GF(5)$

$$D^4 - 1 = (D-1)(D-2)(D-3)(D-4)$$

using $GF(5)$ arithmetic

<u>Def:</u> Primitive Element

a primitive element of $GF(q)$ is one with multiplicative order $q-1$. Thus $\alpha, \alpha^2, \cdots \alpha^{q-1}$ are all the nonzero field elements if α is primitive.

Theorem 8

Every Galois field contains a primitive element.

Proof:

Let m = maximum order of a nonzero field element $\in GF(q)$. From Theorem 3 the order of each nonzero field element divides m so that each is a root of $D^m - 1$. Thus $D^m - 1 = \prod_{i=1}^{q-1} (D - \alpha_i)\ A(D)$ where $\alpha_1, \cdots \alpha_{q-1}$ are the nonzero field elements and $A(D)$ is a polynomial over $GF(q)$. Therefore $m \geq q-1$. Since the order of each element divides $q-1$, $m \leq q-1$.

Q.E.D.

Comment: Theorem 8 implies that the multiplicative group of nonzero elements of a Galois field has a cyclic structure.

Def: A subfield of a field is a field whose elements are a subset of the elements of the original field and whose addition and multiplication rules are the same as for the original field. The original field is called an extension of the subfield.

Theorem 9:

Each Galois field contains a unique subfield with a prime number of elements.

Proof: any subfield contains 0 and 1 and by closure contains $1+1$, $1+1+1$, etc. Denote these elements by $0, 1, 2, 3, \cdots$. These are called the field integers.

The integers must form a cyclic subgroup with say p elements under addition and addition among $0, 1, \cdots, p-1$ must be addition modulo p. From the distributive law, multiplication must also be modulo p since for $k, j \in (0, \cdots, p-1)$ $k \cdot j = k \cdot (\overbrace{1+1+\cdots+1}^{j}) = k + k + \cdots k = (jk) \bmod p$. Thus p must be prime since $(ij) \bmod p \neq 0$ for $i, j \neq 0$. Therefore the integers modulo p is a subfield of every finite field. Any other subfield must contain these integers and the additive group of any subfield contains the integers as a subgroup. Therefore the number of elements in any other subfield is a multiple of p and is not prime. Q.E.D.

<u>Def</u>: Two fields with the same number of elements are said to be <u>isomorphic</u> if they differ only in the labelling of their elements.

<u>Remark</u>: Theorems 8 and 9 imply that any field with a prime number of elements is isomorphic to the integers modulo that number.

<u>Def</u>: The <u>characteristic</u> of a Galois field is the number of elements in it's prime subfield.

<u>Def</u>: If $P(D) = p_0 + p_1 D + \cdots + p_n D^n$ is a polynomial over field E and if F is an extension of E, then $\alpha \in F$ is said to be a <u>root</u> of $P(D)$ if $P(\alpha) = 0$.

EX: R = Field of real numbers
C = " " complex "

Then $C \supset R$ and we frequently find roots of polynomials over R that are in C

Def: Minimal Polynomial

If E is a subfield of Galois field F, then the minimal polynomial $f_\alpha(D)$ over E of $\alpha \in F$ is the monic polynomial over E of lowest degree for which α is a root. (If E is not specified we will assume that it is the subfield with a prime number of elements.)

Theorem 10

For any subfield $E \subset GF(q)$, and each nonzero $\alpha \in GF(q)$, α has a unique minimal polynomial $f_\alpha(D)$ over E and $f_\alpha(D)$ is irreducible over E. Furthermore, for each polynomial $P(D)$ over E, $f_\alpha(D)$ divides $P(D)$ iff α is a root of $P(D)$

Proof:

α is root of $D^{q-1}-1$ which is a polynomial over $GF(q)$ and is also a polynomial over E so that each $\alpha \in GF(q)$ is the root of a polynomial over E. There must be a polynomial $f_\alpha(D)$ over E of lowest degree such that $f_\alpha(\alpha)=0$.

If f_α is reducible then $f_\alpha(\alpha) = g(\alpha)\,h(\alpha) = 0$.

But $g(\alpha)$, $h(\alpha) \in GF(q) \Rightarrow$ either $g(\alpha)$ and/or $h(\alpha) = 0$

contradicting the choice of f_α as having lowest degree. For any $P(D)$ over E

$$P(D) = f_\alpha(D)\, h(D) + r(D).$$

Since $f_\alpha(\alpha) = 0$, $P(\alpha) = r(\alpha)$ and $P(\alpha) = 0$ iff $r(\alpha) = 0$. Since $\deg r(D) < \deg f_\alpha(D)$, $r(\alpha) = 0$ iff $r(D) = 0$. Thus $P(\alpha) = 0$ iff $f_\alpha(D)$ divides $P(D)$.

Assume $\hat{f}_\alpha(D)$ is another minimal polynomial for α over E of the same degree as $f_\alpha(D)$. Then $\hat{f}_\alpha(D) = f_\alpha(D)\, h(D) \Rightarrow h(D) = 1$ so $f_\alpha(D)$ is unique. Q.E.D.

<u>Remark</u> $f_\alpha(D)$ is irreducible over E but considering it as a polynomial over $GF(q)$ $D - \alpha$ is an obvious factor.

<u>Corollary</u>

For a subfield $E \subset GF(q)$ let $f_1(D), \cdots, f_L(D)$ be the distinct minimal polynomials over E for the nonzero elements of $GF(q)$, i.e., $f_{\alpha_1}(D), \cdots, f_{\alpha_{q-1}}(D)$ with repetitions deleted. Then

$$D^{q-1} - 1 = \prod_{i=1}^{L} f_i(D)$$

which factors $D^{q-1} - 1$ into irreducible factors over E. $D^{q-1} - 1$ is known as the <u>cyclotomic</u> polynomial for $GF(q)$

<u>Proof</u>: Since each nonzero element $\in GF(q)$ is a root of $D^{q-1} - 1$, each minimal polynomial divides $D^{q-1} - 1$ by Theorem 10. These polynomials

are irreducible over E and $\prod_{i=1}^{L} f_i(D)$ divides $D^{q-1}-1$. Thus $\deg \prod_{i=1}^{L} f_i(D) \leq q-1$. On the other hand, all the non zero elements of $GF(q)$ are roots of this product so that $\deg \prod_{i=1}^{L} f_i(D) \geq q-1$. Q.E.D.

<u>Theorem 11</u>

Let α be a primitive element in a Galois field $GF(q)$ of characteristic p and let $f(D)$ be the minimal polynomial over $GF(p)$ for α. Then $q = p^n$ if degree of $f(D)$ is n and each element $\beta \in GF(q)$ can be represented as

$$\beta = i_0 + i_1 \alpha + \cdots + i_{n-1} \alpha^{n-1}$$

where $i_0, \cdots, i_{n-1}$ are field integers.

<u>Proof</u>:

Let $f(D) = f_0 + f_1 D + \cdots + f_{n-1} D^{n-1} + D^n$.

Since $f(\alpha) = 0$, $\alpha^n = -\sum_{i=0}^{n-1} f_i \alpha^i$.

Also $\alpha^{n+1} = -\sum_{i=0}^{n-1} f_i \alpha^{i+1} = -f_{n-1}\left(-\sum_{i=0}^{n-1} f_i \alpha_i\right) - \sum_{i=0}^{n-2} f_i \alpha^{i+1}$

etc, so that all powers of α can be represented as $\sum_{k=0}^{n-1} i_k \alpha^k$.

This representation is unique. Assume that $[i_0, \cdots, i_{n-1}]$ and $[j_0, \cdots, j_{n-1}]$ are two choices to represent β. Then $0 = \sum_{k=0}^{n-1} (i_k - j_k) \alpha^k$

and α is a root of $\Delta(D) = \sum_{k=0}^{n-1} (i_k - j_k) D^k$ but this is

impossible since $\deg \Delta(D) < \deg f(D)$. There are p^n distinct choices for $[i_0, \cdots, i_{n-1}]$ so $q = p^n$.

Q.E.D.

<u>Remark</u>: Since the characteristic of each Galois field is a prime number p, each must have p^n elements for some integer n.

<u>Remark</u>:

Let $f(D)$ be an irreducible polynomial of degree n over $GF(q)$. Then as shown on p.114 the set of polynomials over $GF(q)$ modulo $f(D)$ form a field with q^n elements. If $P(D)$ is a polynomial over $GF(q)$ then $P(D) = f(D)\,h(D) + r(D)$ where $r(D) = P(D) \bmod f(D) = r_0 + r_1 D + \cdots + r_{n-1} D^{n-1}$ with $r_j \in GF(q)$. Also for β a root of $f(D)$ in an extension field of $GF(q)$

$$P(\beta) = \cancelto{0}{f(\beta)}\,h(\beta) + r(\beta) = r_0 + r_1\beta + \cdots + r_{n-1}\beta^{n-1}$$

so elements of the form $r_0 + r_1\beta + \cdots + r_{n-1}\beta^{n-1}$ have a one to one correspondence to the polynomials $r_0 + r_1 D + \cdots + r_{n-1} D^{n-1}$ and are another representation for $GF(q^n)$. In particular for $r_0 = r_2 = \cdots r_{n-1} = 0$ and $r_1 = 1$, $P(\beta) = \beta$ so that $\beta \in GF(q^n)$. These observations are summarized in the following theorem.

<u>Theorem 12</u>

All Galois fields with q^n elements are isomorphic to a field of polynomials over $GF(q)$ modulo an n degree irreducible polynomial over $GF(q)$.

<u>Lemma</u>: The minimal polynomial over $GF(q)$ of any element $\beta \in GF(q^n)$ has degree $\leq n$.

<u>Proof</u>: Let α be a primitive element of $GF(q^n)$ with minimal polynomial $f(D)$ over $GF(q)$ of degree k. Then α^j can be represented as $a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$ with $a_0, \ldots, a_{k-1} \in GF(q)$ using arguments like in Theorem 11. Each element has a unique representation of this form so that k must be n to give q^n elements. Thus the elements $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}$ form a basis for $GF(q^n)$ and it is an n-dimensional vector space with scalars corresponding to the elements $\in GF(q)$. Therefore $1, \beta, \ldots, \beta^n$ cannot be linearly independent and there exists a set of $b \in GF(q)$ such that $b_0 + b_1\beta + \cdots + b_n\beta^n = 0$.

Q.E.D.

<u>Corollary</u>: Every irreducible factor over $GF(q)$ of $D^{q^n-1} - 1$ has degree $\leq n$.

<u>Proof</u>: Combine the Lemma above, the corollary on page 127 ($D^{q^n-1}-1$ factors into product of minimal polynomials for elements of $GF(q^n)$), and Theorem 15 (p. 137, fields with p^m elements exist for all m and primes p)

<u>Corollary</u>:

Let $f(D)$ be an irreducible polynomial of degree n over $GF(q)$ and let β be a root of $f(D)$ over an extension field. Then $f(D)$ differs from the minimal polynomial for β by at most a factor $\alpha \in GF(q)$.

<u>Proof</u>: The polynomials over $GF(q)$ modulo $f(D)$ form a field with q^n elements as shown on page 114.

This field is isomorphic to the field consisting of elements of the form $b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1}$ with $b_0, b_1, \ldots, b_{n-1} \in GF(q)$ as shown in the second remark on p. 129. Also $\beta \in GF(q^n)$ so that the minimal polynomial for β over $GF(q)$ has degree $\leq n$ according to the Lemma on p. 130. From Theorem 10, p. 126, $f_\beta(D)$ must divide $f(D)$. But $f(D)$ is irreducible over $GF(q)$ so that $f(D) = b\, f_\beta(D)$ where $b \in GF(q)$.

<u>Remark</u>: The above corollary implies that every irreducible polynomial of degree n over $GF(q)$ differs from the minimal polynomial for some element $\in GF(q^n)$ by at most a factor that is an element $\in GF(q)$

<u>Theorem 12 A</u>

If β is an element of an extension field of $GF(q)$, then the order e of β divides $q^k - 1$ but no smaller number of the form $q^n - 1$ where k is the degree of the minimal polynomial over $GF(q)$ for β.

<u>Proof</u>:

Let $f(D)$ be the minimal polynomial over $GF(q)$ for β and have degree k. The polynomial $f(D)$ is irreducible over $GF(q)$

so that the set of polynomials over $GF(q)$ modulo $f(D)$ forms a field with q^k elements. This is isomorphic to the field of elements of the form $\alpha_0 + \alpha_1\beta + \cdots + \alpha_{k-1}\beta^{k-1}$ where $\alpha_0, \ldots, \alpha_{k-1} \in GF(q)$. Thus $\beta \in GF(q^k)$. The set of nonzero elements forms a group of order $q^k - 1$ so the order e of β divides $q^k - 1$. Suppose that e divides $q^n - 1$ for $n \leq k$. Then β is a root of $D^{q^n-1} - 1$ and $f(D)$ must divide $D^{q^n-1} - 1$ by Theorem K. By the first corollary on p. 130 this implies that $\deg f(D) \leq n$ which is a contradiction of $n < k$.

<u>Theorem 13</u>

Let α and β be elements of $GF(q)$ where $q = p^n$ and p is prime. Then for $m \geq 1$

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$$

<u>Proof:</u>

$$(\alpha + \beta)^{p^m} = \sum_{k=0}^{p^m} \binom{p^m}{k} \alpha^k \beta^{p^m - k}$$

for $1 \leq k \leq p^m - 1$

$$\binom{p^m}{k} = p^m \left[\frac{(p^m - 1) \cdots (p^m - k + 1)}{k!} \right] \equiv 0$$

so

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$$

Q.E.D.

<u>Corollary</u>

Let $f(D)$ be a polynomial over $GF(q)$ with $q = p^n$. Then $[f(D)]^{q^m} = f(D^{q^m})$ for $m \geq 1$.

Proof: Let $f(D) = f_0 + f_1 D + \cdots + f_k D^k$

Then $[f(D)]^{q^m} = [f_0 + (f_1 D + \cdots + f_k D^k)]^{q^m}$

$$= \sum_{l=0}^{q^m} \binom{q^m}{l} f_0^{\,l} (f_1 D + \cdots + f_k D^k)^{q^m - l}$$

$$= f_0^{\,q^m} + (f_1 D + \cdots + f_k D^k)^{q^m}$$ by using the reasoning in Theorem 13. Also since $f_0 \in GF(q)$, $f_0^{\,q^m} = f_0$ so

$$[f(D)]^{q^m} = f_0 + (f_1 D + \cdots + f_k D^k)^{q^m}$$

$$\vdots$$

$$[f(D)]^{q^m} = f_0 + f_1 D^{q^m} + \cdots + f_k (D^{q^m})^k$$

$$= f(D^{q^m})$$

Q.E.D.

<u>Corollary</u>:

Let $f(D)$ be a polynomial over $GF(q)$ and let β be a root of $f(D)$ in an extension field. Then β^{q^m} is also a root of $f(D)$ for $m \geq 1$

<u>Proof</u>:

$$0 = [f(\beta)]^{q^m} = f(\beta^{q^m})$$

Q.E.D.

<u>Theorem 13 A</u>

Let $f(D)$ be a polynomial of degree m over $GF(q)$. Let $f(D)$ be irreducible over $GF(q)$

and let β be a root of $f(D)$ in an extension field. Then $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$ are all the roots of $f(D)$.

<u>Proof</u>: By the corollary on p 133 $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$ are roots of $f(D)$. These elements are distinct. To prove this, suppose they are not and $\beta^{q^i} = \beta^{q^j}$ with $j < i$. Then

$$\beta = \beta^{q^m}$$

since $\beta \in GF(q^m)$ as shown in the second remark on p 129. Also

$$\beta = \beta^{q^m} = (\beta^{q^i})^{q^{m-i}} = (\beta^{q^j})^{q^{m-i}} = \beta^{q^{m+j-i}}$$

or

$$1 = \beta^{q^{m+j-i}-1}$$

Thus the order of β divides $q^{m+j-i}-1$. But $f(D)$ differs from the minimal polynomial for β by at most a factor $b \in GF(q)$ as shown in the second corollary on p. 130. Also $m+j-i < m = \deg f(D)$. This contradicts Theorem 12A, p. 131. Since $f(D)$ can have at most m roots $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$ must be these m roots.

Q.E.D.

<u>Theorem 13 B</u> All roots of irreducible polynomial have same order.

<u>Comment</u>:

We have shown that all Galois fields have p^n elements for some integer n and prime number p. It will now be shown that for every integer n and prime p a Galois field

<u>Theorem 13 B</u> all the roots of an irreducible polynomial have the same order.

<u>Proof</u>:

By Theorem 13 A, if β is one root, every other root has the form β^{q^j} for some j. Let e denote the order of β and e' the order of β^{q^j}. Then

$$(\beta^{q^j})^e = \beta^{e q^j} = 1$$

so e' divides e. Similarly

$$\beta^{e'} = (\beta^{q^m})^{e'} = \beta^{q^j q^{m-j} e'} = ((\beta^{q^j})^{e'})^{q^{m-j}} = 1$$

so e divides e' and $e = e'$.

Q.E.D.

with p^n elements exists. Since Galois fields with p^n elements can be generated by taking the polynomials over $GF(p)$ modulo an irreducible polynomial $f(D)$ over $GF(p)$, it is only necessary to prove that irreducible polynomials over $GF(p)$ of degree n exist for all n and prime $p > 1$.

<u>Theorem 14</u>

Let $f(D)$ be a monic irreducible polynomial of degree n over $GF(p)$. Then $f(D)$ divides $D^{p^m-1}-1$ iff n divides m. (p is prime)

<u>Proof:</u>

Consider the field of polynomials over $GF(p)$ modulo $f(D)$. Let α be a root of $f(D)$. Then any element $\in GF(p^n)$ can be represented as

$$\beta = i_0 + i_1\alpha + \cdots + i_{n-1}\alpha^{n-1} \quad \text{where}$$

$i_0, \cdots, i_{n-1}$ are field integers as shown in the second remark on p. 129. Let β be a primitive element of $GF(p^n)$ and

$$B(D) = i_0 + i_1 D + \cdots + i_{n-1} D^{n-1}$$

so that $\beta = B(\alpha)$. Suppose $f(D)$ divides $D^{p^m-1}-1$. Then α is a root of $D^{p^m-1}-1$ and $\alpha^{p^m-1}-1=0$ or $\alpha^{p^m}=\alpha$ so $\beta = B(\alpha) = B(\alpha^{p^m}) = [B(\alpha)]^{p^m} = \beta^{p^m}$. Thus the order of β divides p^m-1 so p^n-1 divides p^m-1. By long division $p^m-1 = (p^n-1)(p^{m-n}+p^{m-2n}+p^{m-3n}+\cdots+1)$ and for no remainder m must be a multiple of n.

Thus if $f(D)$ divides $D^{p^m-1}-1$, n divides m. Conversely if n divides m, p^n-1 divides p^m-1 so that the order of α divides p^m-1 since it must divide p^n-1 and α is a root of $D^{p^m-1}-1$ $\Rightarrow$ $f(D)$ divides $D^{p^m-1}-1$ by Theorem 10.

QED.

<u>Comment</u>: Theorem 14 implies that for $m \geq 1$, the irreducible factors of $D^{p^m-1}-1$ over $GF(p)$ all have degrees that are divisors of m

Lemma: $D^{p^m-1}-1$ has no repeated monic irreducible factors of degree greater than 0 over $GF(p)$.

<u>Proof</u>: Assume $f(D)$ is a monic irreducible factor factor of $D^{p^m-1}-1$ of degree n. Then n divides m and p^n-1 divides p^m-1 so

$$D^{p^m-1}-1 = (D^{p^n-1}-1)\ A(D)$$

where $A(D) = D^{(p^m-1)-(p^n-1)} + D^{(p^m-1)-2(p^n-1)} + \cdots + 1$

$f(D)$ generates a field with p^n elements so $f(D)$ is not a repeated factor of $D^{p^n-1}-1$. $f(D)$ is the minimal polynomial of some element $\alpha \in GF(p^n)$ so that if $f(D)$ divides $A(D)$, α is a root of $A(D)$. Since α has order that divides p^n-1

$$A(\alpha) = 1 + 1 + \cdots + 1 = \frac{p^m-1}{p^n-1} = p^{m-n} + p^{m-2n} + \cdots + 1$$

$$= 1$$

and α cannot be a root of $A(D)$

QE.D.

Theorem 15

For every positive integer m and prime number p, there exist irreducible polynomials over $GF(p)$ of degree m and therefore fields with p^m elements.

Proof:

Let a_i be the number of monic irreducible factors of $D^{p^m-1}-1$ of degree m/i. Therefore

$$p^m - 1 = a_1 m + a_2 m/2 + \cdots + a_m$$

since the degree of a polynomial is the sum of the degrees of its factors. All irreducible factors of degree m/i divide $D^{p^{m/i}-1}-1$ so that

$$a_i \leq \frac{p^{m/i}-1}{m/i}$$

and

$$p^m - 1 \leq a_1 m + \sum_{\substack{i=2 \\ i:\ \frac{m}{i}=\text{integer}}}^{m} [p^{m/i}-1]$$

$$\leq a_1 m + \sum_{j=1}^{\lfloor m/2 \rfloor} [p^j - 1]$$

$$\leq a_1 m + \frac{p^{\lfloor m/2 \rfloor + 1} - p}{p-1} - \left\lfloor \frac{m}{2} \right\rfloor$$

Since $p_m = (p-1)[p^{m-1} + p^{m-2} + \cdots + 1] + 1$, the inequality clearly can only be satisfied for $a_1 > 0$. Therefore irreducible polynomials of degree m over $GF(p)$ exist. Q.E.D.

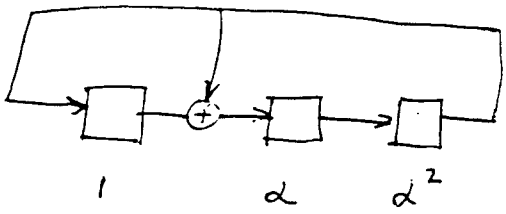
Calculation of Minimal Polynomials

First, a specific representation for $GF(2^3)$ will be presented to illustrate the Galois field concepts discussed previously and also to provide specific examples for the calculation of minimal polynomials.

Representation for $GF(2^3)$

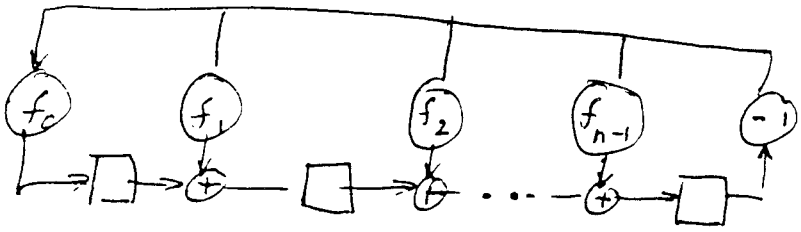
Let $f(D) = D^3 + D + 1$. Since $f(1) = f(0) = 1$, D and $D+1$ are not factors of $f(D)$ over $GF(2)$. If $f(D)$ is reducible over $GF(2)$ it must be the product of three first degree polynomials over $GF(2)$ or a first degree polynomial over $GF(2)$ and an irreducible second degree polynomial over $GF(2)$. Neither can be true since D and $D+1$ are not factors of $f(D)$ over $GF(2)$. Thus $f(D)$ is irreducible over $GF(2)$. The field of polynomials modulo $f(D)$ is a representation for $GF(2^3)$. The set of elements of the form $i_0 + i_1\alpha + i_2\alpha^2$ where $i_0, i_1, i_2 \in GF(2)$ and α is a root of $f(D)$ is isomorphic to the field of polynomials modulo $f(D)$. The elements $1, \alpha, \alpha^2, \cdots, \alpha^k, \cdots$ have a one to one correspondence to the elements $1, D, D^2, \cdots, D^k \bmod f(D), \cdots$. Since $f(\alpha) = 0$, $\alpha^3 = 1 + \alpha$, $\alpha^4 = \alpha + \alpha^2$, $\alpha^5 = \alpha^2 + \alpha^3 = \alpha^2 + (1+\alpha)$, $\alpha^6 = \alpha + \alpha^2 + \alpha^3 = \alpha + \alpha^2 + (1+\alpha) = 1 + \alpha^2$, $\alpha^7 = \alpha + \alpha^3 = \alpha + (1+\alpha) = 1$, etc. A circuit for

calculating successive powers of α is shown below. The contents of the register are the coefficients of $1, \alpha, \alpha^2$ or equivalently $1, D, D^2$. Notice that the powers of α generate all the non zero elements $\in GF(2^3)$ so that α or equivalently D is a primitive element of $GF(2^3)$. If the contents of the register are not initially $(0,0,0)$ they can never become $\vec{0}$ and will repeat only after all the 7 nonzero field elements have been generated in the register.



Circuit to Generate Powers of α

For an arbitrary polynomial $f(D) = f_0 + f_1 D + \cdots + D^n$ over $GF(q)$ a circuit for calculating successive powers of a root of $f(D)$ or equivalently $D^k \bmod f(D)$ has the form shown below.



Circuit to Generate $D^k \bmod f(D)$

The representations for the $GF(2^3)$ field elements are summarized in the table below. Minimal polynomials over $GF(2)$ are given for each element. Methods for calculating them will be presented below.

Field Element	1	D	D^2	Minimal
	1	α	α^2	Polynomials
1	1	0	0	$D+1$
α or D	0	1	0	D^3+D+1
α^2 or D^2	0	0	1	D^3+D+1
α^3 or $D^3 \bmod f(D)$	1	1	0	D^3+D^2+1
α^4 or $D^4 \bmod f(D)$	0	1	1	D^3+D+1
α^5 or $D^5 \bmod f(D)$	1	1	1	D^3+D^2+1
α^6 or $D^6 \bmod f(D)$	1	0	1	D^3+D^2+1
α^7 or $D^7 \bmod f(D)$	1	0	0	

Two methods for calculating minimal polynomials are described below.

<u>Method 1</u>

Let $f_\alpha(D)$ be the minimal polynomial for α over $GF(q)$. Then the roots of $f_\alpha(D)$ must be $\alpha, \alpha^q, \alpha^{q^2}, \cdots$ and according to Theorem 13A the m distinct elements of this sequence must be all the roots of $f_\alpha(D)$. Thus

$$f_\alpha(D) = (D-\alpha)(D-\alpha^q)\cdots(D-\alpha^{q^{m-1}})$$

<u>Example</u> Consider the field $GF(2^3)$ on p. 140.

The minimal polynomial over $GF(2)$ for α is desired. Since $f(D)$ is irreducible and monic, $f_\alpha(D)$ must be $f(D)$. The roots of $f_\alpha(D)$ are

$$\alpha, \alpha^2, \alpha^4, \alpha^8 = \alpha^7 \cdot \alpha = \alpha$$

so

$$f_\alpha(D) = (D-\alpha)(D-\alpha^2)(D-\alpha^4)$$

$$= D^3 + (\alpha+\alpha^2+\alpha^4)D^2 + (\alpha^3+\alpha^5+\alpha^6)D - \alpha^7$$

$$= D^3 + D + 1 = f(D)$$

since according to the table

$$\alpha + \alpha^2 + \alpha^4 = (010) + (001) + (011) = (000)$$

$$\alpha^3 + \alpha^5 + \alpha^6 = (110) + (111) + (101) = (100)$$

<u>Method 2</u>

The degree of $f_\beta(D)$ can be found by applying Theorem 13A. If $\deg f_\beta(D) = n$ then assume $f_\beta(D) = b_0 + b_1 D + \cdots + b_{n-1} D^{n-1} + D^n$. Let $D = \beta$ and solve the set of n equations for the field elements $b_0, b_1, \ldots, b_{n-1} \in GF(q)$.

<u>Example</u>: Consider $GF(2^3)$ on p 140

The minimal polynomial over $GF(2)$ for $\beta = \alpha^3$ is desired. The roots of $f_{\alpha^3}(D)$ must be

$$\beta = \alpha^3, \beta^2 = \alpha^6, \beta^4 = \alpha^{12} = \alpha^7 \cdot \alpha^5 = \alpha^5, \beta^8 = \alpha^{10} = \alpha^3 = \beta$$

Thus $\deg f_{\alpha^3}(D) = 3$

So $f_\beta(D) = b_0 + b_1 D + b_2 D^2 + D^3$

and

$$f_\beta(\beta) = [0,0,0] = b_0 \underbrace{[1,0,0]}_{1} + b_1 \underbrace{[1\,1\,0]}_{\beta=\alpha^3} + b_2 \underbrace{[1\,0\,1]}_{\beta^2=\alpha^6} + \underbrace{[0\,0\,1}_{\beta^3=\alpha^9=}$$

so

$$\begin{aligned} b_0 + b_1 + b_2 &= 0 \\ b_1 &= 0 \\ b_2 + 1 &= 0 \end{aligned} \implies b_0 = 1, \quad b_1 = 0, \quad b_2 = 1$$

So $\quad f_{\alpha^3}(D) = 1 + D^2 + D^3$