still for better than other known practical coding schemes!

In most practical cases $P_{e,n}$ can be made far smaller than necessary with reasonable values of m. The decoder performance is determined primarily by buffer overflow probability.

→ Viterbi Algorithm : Com Tech Oct ~~Sept.~~ '91 Excellent analysis of conv codes

Jelinek Stack Algorithm

IV. Algebraic Cyclic Block Codes [Ref: Gallager, Ch 6]

A. Review of Algebra

<u>Def:</u> Group

a group, $\mathcal{G}$, is a set of elements $a, b, c, \cdots$ and an operation, $\cdot$, for which

(1) $a \in \mathcal{G}, b \in \mathcal{G} \Rightarrow a \cdot b \in \mathcal{G}$ (closure)

(2) associative law $a, b, c \in \mathcal{G}$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(3) Identity element $e \in \mathcal{G}$

$$a \cdot e = e \cdot a = a \quad \text{for all } a \in \mathcal{G}$$

(4) Inverses: for each $a \in \mathcal{G}$, have inverse a^{-1}

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

<u>Def:</u> Abelian or Comutative Group

$$a \cdot b = b \cdot a$$

<u>Def:</u> Subgroup

a subset $\mathcal{S}$ of $\mathcal{G}$ is a subgroup of $\mathcal{G}$ if the elements of $\mathcal{S}$ satisfy axioms for $\mathcal{G}$

<u>Def:</u> Order of group = number of elements in group

<u>Def:</u> Coset

a right coset of subgroup S of G is set of elements

$$\{ s_1 \cdot a, \; s_2 \cdot a, \; \cdots \}$$

where $s_1, s_2, \cdots$ are all the elements of S and a is an element of G.

a left coset is defined similarly.

<u>Remark:</u> If S has finite order, then each coset has the same number of elements as S

<u>Lemma:</u> If two right (left) cosets of S have element in common, then the cosets are the same.

Proof: Assume one coset generated by "a" and other by "b" and $s_i \cdot a = s_j \cdot b$. Then

$$s_j^{-1} \cdot s_i \cdot a = b$$

so b in coset generated by a. For any $s_k \in S$

$$s_k \cdot b = s_k \cdot s_j^{-1} \cdot s_i \cdot a$$

$\Rightarrow$ all elements in coset generated by b in coset generated by a

EX: Consider (N, K) code over $GF(q)$

$\bullet$ = vector addition, with mod q addition

$e = \vec{0}$

$\vec{x}^{-1} = -\vec{x}$

code words form abelian group. Consider vector $\vec{y}$. Then $\vec{y} + \vec{x}_i$ has same syndrome for all $\vec{x}_i$. Code words $\{\vec{x}_i\}$ are a subgroup of set of N-vectors. $\{\vec{y} + \vec{x}_i\}$ is coset. Thus set of N-vectors with same syndrome form coset.

<u>Max. Likelihood Decoding for BSC</u>

For received $\vec{y}$ assume error $\vec{z}$ to be minimum weight sequence in same coset as $\vec{y}$

Ex: Binary (N, K) Codes

let $\vec{x}_i \times \vec{x}_j = \{x_{i1} \cdot x_{j1}, x_{i2} \cdot x_{j2}, \dots, x_{iN} \cdot x_{jN}\}$

Then

$$W(\vec{x}_i + \vec{x}_j) = W(\vec{x}_i) + W(\vec{x}_j) - 2W(\vec{x}_i \times \vec{x}_j)$$

Notice even weight codewords are subgroup

Odd weight codewords are coset –

assume $\vec{x}_i, \vec{x}_j$ odd weight

Then $W(\vec{x}_i + \vec{x}_j)$ even

$\vec{x}_i + \vec{x}_j = \vec{x}_k$ (even)
$\vec{x}_i = \vec{x}_k + \vec{x}_j \Rightarrow \vec{x}_i$ in coset generated by $\vec{x}_j$ & $\vec{x}_i$ also in coset generated by $\vec{x}_i$ so both cosets must be s

$\Rightarrow$ Either all code words have even weight or 1/2 odd and 1/2 even.

<u>Thm</u>: (Lagrange) 1

The order of a finite group is a multiple of the order of each subgroup.

Proof: G = group order n, A subgroup of G with order m. Assume $n > m$. Form right coset of A with element of G not in A. Then A and

coset contain $2m$ elements. If $n > 2m$ form another coset with unused element of G, etc...
Eventually all elements of G in S or coset
so $n = km$ where $k = 1 +$ no. of cosets.

<u>Cyclic Subgroups</u>

Let $a \in G$, and order G finite. Define
$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n}$. Consider sequence

$$a, a^2, a^3, \ldots$$

Since group finite, have i and j with $i < j$
for which

$$a^i = a^j = a^i \cdot a^{j-i}$$

and $a^{j-i} = e$

<u>Def</u>: Order of element

Order of $a \in G$ is smallest positive integer m such that $a^m = e$.

<u>Thm 2</u> Let an element, a, of finite group G have order m. Then $a, a^2, \ldots, a^m$ is subgroup of G and m divides order of G.

Proof:

(1) closed under $\cdot$

$$a^i \cdot a^j = a^{i+j}$$

If $i+j \leq m$ $\quad a^{i+j} \in S$

If $i+j > m$ $\quad i+j = qm + r$ with $0 \leq r < m$

$$a^{i+j} = a^{qm} a^r = e \cdot a^r = a^r \in S$$

(2) associative law holds

(3) identity $= a^m$

(4) inverses

$$a^i \cdot a^{m-i} = a^m = e \Rightarrow a^{m-i} = (a^i)^{-1}$$

By Thm 1, m divides order of G

<u>Def:</u> Two positive integers are <u>relatively prime</u> if no positive integer other than 1 is a factor of both

<u>Lemma</u>: Let "a" be an element of order m, b element of order n in <u>abelian</u> group. If m, n relatively prime, then order $a \cdot b$ is mn.

Proof:

$$(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = e$$

Let l = order $a \cdot b$, then $l \leq mn$. also

$$e = (a \cdot b)^{ln} = a^{ln} \cdot (b^n)^l = a^{ln}$$

So l multiple of m since m, n relatively prime

$$e = (a \cdot b)^{lm} = (a^m)^l \cdot b^{lm} = b^{lm}$$

$\Rightarrow$ l multiple of n so $l \geq mn$

Q.E.D.

<u>Thm 3</u>

In finite abelian group, let m be the maximum of order of elements. Then m is a multiple of order of each element $\in G$.

Proof: Let a have maximum order m and let n be order of any other element b.

Let $p_1, p_2, \ldots, p_r$ be all prime numbers that divide m and n. Then

$$m = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}, \quad n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

with $\{m_i\}$ and $\{n_i\}$ nonnegative integers. If m not multiple of n, then $n_i > m_i$ for some $1 \le i \le r$. Let

$$a_j = a^{m/p_j^{m_j}} \Longrightarrow \text{order } a_j = p_j^{m_j}$$

$$b_i = b^{n/p_i^{n_i}} \Longrightarrow \text{order } p_i^{n_i}$$

consider $c = a_1 \cdot a_2 \cdots a_{i-1} \cdot b_i \cdot a_{i+1} \cdots a_r$

By lemma on p.106 order $c = p_1^{m_1} \cdot p_2^{m_2} \cdots p_{i-1}^{m_{i-1}} \cdot p_i^{n_i} \cdot p_{i+1}^{m_{i+1}} \cdots p_r^{m_r}$

$$= m \frac{p_i^{n_i}}{p_i^{m_i}}$$

but $n_i > m_i$ because of assumption and

order $c > m$ = contradiction

QED.

Def. and Lemma: p. 107 a

<u>Def:</u> Field

a field is a set of at least two elements closed under two operations called "addition" (+) and "multiplication" (·), satisfying

(1) abelian group under addition

(2) " " " multiplication if additive identity 0 is deleted

(3) distributive law

$$(a+b)\cdot c = a\cdot c + b\cdot c$$

<u>Def:</u> The <u>greatest</u> <u>common</u> <u>divisor</u> of two integers a and b is the greatest integer that divides both a and b. This will be denoted as $\gcd(a, b)$.

<u>Lemma:</u>

Let b be an element of order n in a finite group. Then the order of b^k is $n / \gcd(n, k)$.

<u>Proof:</u>

Let order b^k be ℓ. Then $b^{k\ell} = 1$ and $k\ell$ must be a multiple of n, i.e., $k\ell = rn$ for $r \geq 1$. Also $k = c_1 \gcd(k, n)$ and $n = c_2 \gcd(k, n)$ with c_1 and c_2 relatively prime. Thus

$$\ell = r\frac{n}{k} = r\frac{c_2}{c_1}$$

Since c_2 and c_1 are relatively prime, r must be a multiple of c_1 to make the right hand side an integer. The smallest integer value of the right hand side occurs when $r = c_1$ so

$$\ell = c_2 = n / \gcd(n, k) \qquad \text{Q.E.D}$$

Ex. Real no's; integers 0, 1 using modulo 2 arithmetic

Notation: additive identity $= 0$, multiplicative ident. $= 1$
" inverse $= -a$ " inverse $= a^{-1}$

<u>Elementary Properties of Fields</u>

1. $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in \mathcal{F}$

$$a \cdot b = a \cdot (b + 0) = a \cdot b + a \cdot 0$$

$$\Rightarrow \quad a \cdot 0 = 0$$

2. $a \cdot b \neq 0 \quad \forall$ nonzero a and b

nonzero elements form group under $\cdot$

3. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b) \quad \forall a, b$

$$0 = 0 \cdot b = [a + (-a)] \cdot b = a \cdot b + (-a) \cdot b$$

so can use minus sign without parentheses

also

$$(-a) \cdot (-b) = a \cdot b$$

$$0 = (-a) \cdot (-b + b) = (-a) \cdot (-b) + (-a) \cdot b$$

$$= (-a) \cdot (-b) - (a \cdot b)$$

4. $a \cdot b = a \cdot b' \Rightarrow b = b'$ for $a \neq 0$

$$0 = a \cdot b - a \cdot b' = a \cdot (b - b') \Rightarrow b = b'$$

<u>Def</u>: Galois Field is field with finite number of elements

<u>Alternate set of axioms for finite fields</u>

(1) abelian group under addition

$\rightarrow$ (2') multiplication is commutative and associative and $a \cdot b \neq 0$ for a and $b \neq 0$

6.9 Historical digression

It is standard practice to denote a field of order q by $GF(q)$. The initials GF stand for Galois field, after the French mathematician Évariste Galois who died in a duel in 1832 at the age of 20, having invented the theory of finite fields and having made at least two further major contributions to mathematics.

Galois' biography is a cautionary tale for teachers. He was unquestionably one of the great mathematical geniuses, but he failed the exams to enter the École Polytechnique because he refused to write his answers in the form required by the examiners. He did, however, get into the École Préparatoire in 1829. In July 1830 a revolution broke out against the reactionary regime and Galois became an ardent republican. After the suppression of the revolt he wrote an article violently attacking the director of the École Préparatoire for which he was expelled.

He devoted much of his time to republican activities but still continued his research. In July 1831 he was arrested during a demonstration and placed in detention for illegally wearing a uniform and carrying weapons. In March 1832 he was transferred to a nursing home because of the outbreak of a cholera epidemic. Here he had an unhappy love affair. At the end of May after the break-up of the affair he was provoked to a duel by an unknown adversary, believed by some to have been an agent provocateur. On 29 May, believing he would be killed, he wrote desperate letters to his republican friends and a summary of his major results, which he asked his friends to show to Gauss and Jacobi in the event of his death. Nothing seems to have come of this, but the letter was published in the Revue Encyclopédique in September 1832, though it aroused little interest. On 30 May 1832 Galois was admitted to hospital, mortally wounded. He died there on 31 May. His funeral, on 2 June, was the occasion for a republican demonstration heralding the riots in Paris in the following days.

Galois had submitted work to learned journals and the academy from 1829 onwards. His first published major treatise, 'Sur la théorie des nombres' was published in Férussac's *Bulletin des Sciences Mathématiques* in 1830. It defines the so-called 'Galois imaginaries', which are elements of finite fields, and provides the fundamental results on finite fields. A memoir on the solution of equations had earlier been sent to the Academy. Cauchy reviewed it favourably, but advised Galois to rewrite it in the light of the results of the young Danish mathematician Niels Henrik Abel who had just died. The revised memoir was lost on the death of Fourier, who had been assigned to review it, giving rise to the legend that Cauchy had just put Galois' paper in a drawer. In 1831 Galois submitted a new version of his memoir. Cauchy had left France in 1830 and Poisson was assigned to review it. He rejected it, saying that some of the results could be found in Abel's work and the rest were not fully proved. Galois, embittered by this injustice after his earlier misfortune, wrote 'On jugéra' (posterity will judge) in the margin of his copy.

Eventually Liouville became interested in Galois' work. In 1843, 11 years after Galois' death, he introduced the results to the Academy of Sciences. He announced the publication of the memoir rejected by Poisson for the end of that year (it was actually published in 1846). This memoir can be regarded as the foundation of modern algebra and became the basis for major research efforts over the next 100 years.

From: Oliver Pretzel, Error-Correcting Codes and Finite Fields, Oxford University Press, 1992

(3) Distributive law

(Group axioms (1) closure (2) associative (3) identity (4) inverse)

Proof: Need to show that (2') $\Rightarrow$ (2).

Let $a \neq 0$, then because only have finite number of elements there must be $j > i$ such that $a^i = a^j = a^i \cdot a^{j-i}$ and $e = a^{j-i}$. Also

$$a \cdot a^{j-i-1} = a^{j-i} = e$$

so each element has an inverse.

Q.E.D

The alternate axioms are useful in determining if a finite set of elements is a field.

<u>Example:</u>

Let p be a prime number. Consider the set of elements $\{0, 1, \cdots, p-1\}$. Define addition as addition modulo p, i.e,

$$i + j = (i + j) \bmod p$$

where on the right hand side $+$ is ordinary addition and $a \bmod p$ is the remainder when a is divided by p. Multiplication is multiplication mod p, i.e., $i \cdot j = (i \times j) \bmod p$ where $\times$ is ordinary multiplication.

(1) Abelian group under $+$

(a) closed under $+$

(2) associative law

(3) identity $= 0$

(4) inverses $-j = p - j$

(2) <u>mult. commutative</u>

<u>Mult. associative</u>

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

proof: let $a \times b = q_1 \times p + r_1$

where $r_1 = (a \times b) \bmod p$

and $b \times c = q_2 \times p + r_2$

Then

$$(a \cdot b) \cdot c = [a \times b - q_1 \times p] \times c \bmod p$$

$$= (a \times b \times c) \bmod p$$

by commutative + distributive laws.

By similar argument

$$a \cdot (b \cdot c) = (a \times b \times c) \bmod p$$

<u>$a \cdot b \neq 0$ for $a, b \neq 0$</u>

for $a, b \neq 0$

$a \cdot b = 0$ only if $a \times b$ is multiple of p

since p is prime this is impossible

(3) distributive law

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

let ordinary addition $= +'$

Then $a +' b = q_1 p +' (a + b)$

$$(a + b) \times c = (a +' b - q_1 p) \times c = (a \times c +' b \times c) - q_1 c p$$

$$(a + b) \cdot c = [a \times c +' b \times c] \bmod p$$

also $a \times c = q_2 \times p + (a \cdot c)$

$$b \times c = q_3 \times p + (b \cdot c)$$

$$\Rightarrow (a \cdot c) + (b \cdot c) = [a \times c +' b \times c] \bmod p$$

Polynomials

$$f(D) = f_n D^n + \cdots + f_0$$

is a polynomial over $GF(q)$ of degree n if the coefficients $f_n, \ldots, f_0 \in GF(q)$ and $f_n \neq 0$.

Addition

$$f(D) + g(D) = \sum (f_i + g_i) D^i$$

Multiplication of Polynomials

$$f(D)\, g(D) = \sum_i \left(\sum_{j=0}^{i} f_j g_{i-j} \right) D^i$$

Scalar Multiplication

$$\alpha \in GF(q)$$

$$\alpha f(D) = \sum_i (\alpha \cdot f_i) D^i$$

Thm 4 Euclidean Division Algorithm

Let $f(D)$ and $g(D)$ be polynomials over $GF(q)$ and degree $g \geq 1$. Then there are unique polynomials $h(D)$ and $r(D)$ over $GF(q)$ for which

$$f(D) = g(D)\, h(D) + r(D)$$

and $\deg r < \deg g$

Proof:

Existence: Let $\deg f = n$, $\deg g = m$

If $m > n$ then $h(D) = 0$, $r(D) = f(D)$.

If $n \geq m$ divide g into f as in ordinary polynomial division except using $GF(q)$ arithmetic.

$$
\begin{array}{r|l}
 & g_m^{-1} \cdot f_n D^{n-m} + \cdots \\
\hline
g_m D^m + g_{m-1} D^{m-1} + \cdots + g_0 & f_n D^n + f_{n-1} D^{n-1} + \cdots + f_0 \\
 & \underline{f_n D^n + g_{n-1} \cdot g_m^{-1} \cdot f_n D^{n-1}} \\
 & \cdots \\
 & \text{etc} \\
\hline
 & r(D)
\end{array}
$$

<u>Uniqueness:</u> assume two solutions h, r ; h', r' then

$$f(D) = hg + r = h'g + r'$$

or $$g[h - h'] = r' - r$$

Deg $r' - r < \deg g \Rightarrow h - h' = 0 \Rightarrow h = h' \Rightarrow$ and $r' - r = 0 \Rightarrow r = r'$

QED.

<u>Def:</u> $f(D) \bmod g(D)$ = remainder when f is divided by $g(D)$.

<u>Def:</u> $g(D)$ is a factor of $f(D)$ if $f(D) = g(D)h(D)$

<u>Def:</u> A polynomial is <u>reducible</u> if it has at least two factors of degree 1 or more. Otherwise it is <u>irreducible</u>.

<u>Def:</u> <u>Monic</u> polynomial has coefficient of highest power of D equal to 1.

<u>Theorem 5 (Unique Factorization)</u>

A polynomial $f(D)$ over a given field has a unique factorization into a field element times a product of monic irreducible polynomials over

Def. Polynomial ideal

Any subset C of polynomials over a field F which contains the sum and difference of any two, and all multiples of any one of its members is called a polynomial ideal.

→ Theorem A

A polynomial ideal consists of either (i) 0 alone or (ii) the set of multiples of any non-zero member $a(D)$ of least degree.

Proof:

Case (i) is trivial

Assume case (ii). Then there must be a polynomial $a(D)$ of least degree. Let $b(D)$ be any polynomial in C. Then

$$b(D) = q(D)\,a(D) + r(D)$$

or $\quad r(D) = b(D) - q(D)\,a(D)$ with $\deg r(D) < \deg a(D)$

But $\quad r(D) \in C$, $\Rightarrow r(D) = 0$, $b(D) = q(D)\,a(D)$.

Q.E.D.

Theorem B

Any two polynomials $x(D)$ and $y(D)$ have a greatest common divisor $c(D)$ satisfying (i) $c \mid x$ and $c \mid y$, (i') $p \mid x$ and $p \mid y$ implies $p \mid c$. Moreover, (ii) c is a linear combination of x and y, i.e., $c(D) = s(D)\,x(D) + t(D)\,y(D)$.

Proof: Let x and y be any two polynomials and consider the set $C = \{ s(D)\,x(D) + t(D)\,y(D) : s$ and t are any polynomials $\}$. Then C contains any sum,

difference, or multiples of its members since

$$(sx + ty) \pm (s'x + t'y) = (s \pm s')x + (t \pm t')y$$

and $q(sx+ty) = (qs)x + (qt)y$

Thus C is an ideal and each member is a multiple of some least degree polynomial $a(D)$. This polynomial $a(D)$ divides $x(D) = 1 \cdot x(D) + 0 \cdot y(D)$ and $y(D) = 0 \cdot x(D) + 1 \cdot y(D)$ and will be divisible by any common divisor of x and y, since $a(D) = s_0(D)\,x(D) + t_0(D)\,y(D)$.

QED.

<u>Def:</u> Relatively Prime

$a(D)$ and $b(D)$ are relatively prime if their greatest common divisor is a constant

<u>Theorem C</u>

If $p(D)$ is irreducible, then $p(D) \mid a(D)\,b(D)$ implies $p(D) \mid a(D)$ or $p(D) \mid b(D)$.

<u>Proof:</u>

Assume $p(D)$ is monic. Then g.c.d. of $p(D)$ and $a(D)$ is either $p(D)$ or 1. In former case $p(D) \mid a(D)$; in latter case we can write

$$1 = s(D)\,p(D) + t(D)\,a(D)$$

so $$b(D) = 1 \cdot b(D) = s(D)\,p(D)\,b(D) + t(D)\,[a(D)\,b(D)]$$

Since $p(D)$ divides $a(D)\,b(D)$, it divides right-hand side and consequently $b(D)$.

Q.E.D.

Theorem D Unique Factorization

Any non-constant polynomial $a(D)$ can be expressed as a constant c times a product of monic irreducible polynomials. This expression is unique except for order of factors.

Proof

The constant c is the coefficient of the highest order term in $a(D)$. Assume two "prime" factorizations

$$a(D) = c\, p_1(D) \cdots p_m(D) = c\, q_1(D) \cdots q_n(D)$$

Since $p_1(D)$ divides $a(D) = c\, q_1(D) \cdots q_n(D)$, by Theorem C it must divide some factor $q_i(D)$; since $q_i(D)$ is irreducible, $q_i(D)/p_i(D)$ must be a constant; since both are monic, the constant is 1. Thus $p_1(D) = q_i(D)$. Continuing process completes the proof.

QED.

Euclidean algorithm for Finding GCD

Assume $\deg r(D) < \deg s(D)$

$$s(D) = q_1(D)\, r(D) + r_1(D) \quad ; \deg r_1 < \deg r$$

$$r(D) = q_2(D)\, r_1(D) + r_2(D)$$

$$\vdots$$

$$r_{n-2}(D) = q_n(D)\, r_{n-1}(D) + r_n(D)$$

$$r_{n-1}(D) = q_{n+1}(D)\, r_n(D)$$

Last nonzero remainder, $r_n(D)$, is $\gcd(r, s)$

the field, each of degree ≥ 1.

Proof: $f(D) = f_n D^n + \cdots + f_0 = f_n (D^n + \cdots + f_n^{-1} \cdot f_0)$

so field element must be f_n. Assume two factorizations $a_1(D)\, a_2(D) \cdots a_k(D) = b_1(D) \cdots b_j(D)$ with a's, b's monic and irreducible for monic polynomial $f_n^{-1} f(D)$. If $a_\ell(D) = b_m(D)$ we could factor this out of f and consider factoring a lower degree polynomial. Therefore assume $a_\ell(D) \neq b_m(D)$ for all ℓ and m. Let $\deg b_1 \leq \deg a_1$. Then $a_1(D) = b_1(D)\, h(D) + r(D)$ and

$$[b_1(D)\, h(D) + r(D)]\, a_2(D) \cdots a_k(D) = b_1(D) \cdots b_j(D)$$

or $$r(D)\, a_2(D) \cdots a_k(D) = b_1(D)[b_2(D) \cdots b_j(D) - h(D)\, a_2(D) \cdots a_k(D)$$

Since $\deg r < \deg b_1$, $b_1(D)$ cannot be a factor of left hand side $\Rightarrow$ no equality and $a_1(D) = b_1(D)$.

Q.E.D.

<u>Def</u>: $\alpha \in$ field $\mathcal{F}$ is a root of $f(D)$ over $\mathcal{F}$ if $f(\alpha) = 0$.

<u>Theorem 6</u>

An element α of field $\mathcal{F}$ is a root of a nonzero polynomial $f(D)$ over $\mathcal{F}$ iff $D - \alpha$ is a factor of f. If $\deg f = n$, then at most n field elements are roots of f.

Proof:

If $f(D) = (D - \alpha)\, h(D)$ then $f(\alpha) = 0$

If $f(D) = (D - \alpha)\, h(D) + r(D)$, the $\deg r = 0$ so that $r(D) = r_0$, a field element. If $f(\alpha) = 0$ then $r_0 = 0$ and $D - \alpha$ is factor of f.

If f is factored, the deg f is the sum of the degrees of the factors. Thus there can be at most n roots in the field.

<u>Second Example of Finite Field</u>

Let $f(D)$ be an irreducible polynomial of degree n over $GF(q)$. Let the field elements be polynomials of degree $< n$ over $GF(q)$. Define $+$ as polynomial addition modulo q and $*$ as $g_1(D) * g_2(D) = [g_1(D) \times g_2(D)] \bmod f(D)$.

(1) abelian group under $+$

(3) Distributive law

(2') If $g_1(D) * g_2(D) = 0$ then $g_1(D) g_2(D) = f(D) h(D)$

Since deg g_1 and deg $g_2 \leq n-1$, f can not be a factor of $g_1(D) g_2(D) \Rightarrow g_1$ and/or $g_2 = 0$

We will call this the field of polynomials over $GF(q)$ modulo $f(D)$. Has q^n elements

Note: $f(D)$ must be irreducible otherwise the product of two field elements will equal $f(D)$

<u>Ex.</u> $f(D) = D^2 + D + 1$, $GF(2)$

$f(0) = f(1) = 1$

	0	1	D	D+1
0	0	1	D	D+1
1	1	0	D+1	D
D	D	D+1	0	1
D+1	D+1	D	1	0

Addition Table