International Journal of Mathematics and Statistics Invention (IJMSI)
E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759
www.ijmsi.org Volume 1 Issue 1 || August 2013 || PP-44-47

Construction of some Finite Fields of order p^n over GF(p)

Kulvir Singh
Department of Mathematics, Government College, Loharu (India)

ABSTRACT: *Let n be a positive integer and p be a prime such that g.c.d.(n, p)=1. Observe that irreducible polynomials of degree n over GF(p), help us in the construction of finite field GF(p^n). Explicit expression of all162 polynomials of degree 4 over GF(3), all element of field GF(5^2) over GF(5) and all element of field GF(3^3) & GF(3^4) over GF(3) are obtained.*
Keywords: *Irreducible monic polynomial, primitive element, prime field.*

INTRODUCTION:

Let F be a prime field of Char. $p\neq0$, then by [4], o(F)=p. Also we know that if F has finite Characteristic then by[1] it must be prime. If F is a finite field, then by[2] $o(F) = p^n$, for some prime p and an integer n. Let $f(x) \in F[x]$ be an irreducible polynomial of degree 'n' and I=<f(x)>be the ideal generated by f(x). Then K=F[x]/I is a field [3]. Let F=GF(q), q is some prime or prime power, be a finite field containing q elements. Let V(n,q) denotes the vector space over F of all n-tuples $(\alpha_1,\alpha_2,...,\alpha_i,...,\alpha_n)$ $a_i\in R$. Let R bearing with unity. By a polynomial over the ring R we mean a tuple $(a_1,a_2,...,a_i,...)$; $a_i\in R$ and all α_i are zero except some finite term. If n is the largest index for which $a_n\neq0$ then n is called degree of the polynomials $(a_1,a_2,...,a_i,...)$ $a_i\in R$.
In the study of finite fields their reducible factors of x^n-1 where $n=p^m-1$, p, a prime number, playan important role. Every factorization of the polynomial x^q-x, gives us a partition of the elements in GF(q).Further whenever a finite field of order p^m is required then certainly we are in need of some prime polynomial of degree m over GF(p). Thus the study of prime fields also hinges on the factorization of x^n-1, which is the basic object of this paper.

Notations 1.1:(i) A field having finite number of elements known as finite field or Galois field and is denoted by GF(q) .
(ii) R[x] denote the set of polynomial over R
(iii) Polynomial $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ will be represented by $(a_0,a_1,...,a_i,...,a_n)$; $a_i\in R$.

2.1.Expression of all 162 polynomials of degree 4 over GF(3)

00001	00002	00011	00012	00021	00022
00101	00102	00111	00112	00121	00122
00201	00202	00211	00212	00221	00222
01001	01002	01011	01012	01021	01022
01101	01102	01111	01112	01121	01122
01201	01202	01211	01212	01221	01222
02001	02002	02011	02012	02021	02022
02101	02102	02111	02112	02121	02122
02201	02202	02211	02212	02221	02222
10001	10002	10011	10012	10021	10022
10101	10102	**10111**	10112	**10121**	10122
10201	10202	10211	10212	10221	10222
11001	11002	11011	11012	**11021**	11022
11101	11102	**11111**	11112	11121	11122

11201	11202	11211	11212	11221	11222
12001	12002	**12011**	12012	12021	12022
12101	12102	12111	12112	**12121**	12122
12201	12202	12211	12212	12221	12222
20001	20002	**20011**	20012	20021	20022
20101	20102	20111	20112	20121	20122
20201	20202	20211	20212	20221	20222
21001	21002	21011	21012	21021	21022
21101	21102	21111	21112	**21121**	21122
21201	21202	21211	21212	**21221**	21222
22001	22002	22011	22012	22021	22022
22101	22102	**22111**	22112	22121	22122
22201	22202	**22211**	22212	22221	22222

Bold underline expression shows irreducible monic polynomials of degree 4 over GF(3),which are 18 in numbers.
Similarly, irreducible monic polynomials of degree 2 over GF(3),which are 3 in numbers are given by

101 **112** **122**

and irreducible monic polynomials of degree 1over GF(3), which are 3 in numbers are given by
10 **11** **12**

If p is prime then by [3]$x^{p^m}-x$ is a product of all monic irreducible polynomials over GF(p).

Hence, $x^{3^4}-x$ over GF(3) can be written as a product of 24 monic irreducible polynomial as obtained above.

3. Construction of some finite fields GF(p^n) over GF(p) (Particular case for p=5 & n=2 and p=3 & n=3, 4).

3.1 Construction of field of order 5^2 over GF(5)

Consider GF(5)=({0,1,2,3,4} $+_5, \times_5$) and $f(x)=x^2+2$ over GF(5). Since deg. f(x)=2 and no element of GF(5) is a root of f(x), therefore f(x) is irreducible over GF(5).Then K=GF(5)[X]/$<X^2+2>$will be a field of order 5^2. We now find all elements of K. We write all possible order pair (a,b) of elements of GF(5), in which first element represent the constant term and second element represent the coefficient of x. Now possible pairs are:

Ordered Pair	Corresponding Polynomials
(0,0)	0
(1,0)	1
(2,0)	2
(3,0)	3
(4,0)	4
(0,1)	x
(1,1)	x+1
(2,1)	x+2
(3,1)	x+3
(4,1)	x+4
(0,2)	2x
(1,2)	2x+1
(2,2)	2x+2
(3,2)	2x+3
(4,2)	2x+4
(0,3)	3x
(1,3)	3x+1
(2,3)	3x+2
(3,3)	3x+3
(4,3)	3x+4
(0,4)	4x

(1,4)	4x+1
(2,4)	4x+2
(3,4)	4x+3
(4,4)	4x+4

Hence, K=({0,1,2,3,4, x, x+1, x+2, x+3, x+4, 2x, 2x+1, 2x+2, 2x+3, 2x+4, 3x, 3x+1, 3x+2, 3x+4, 4x, 4x+1, 4x+2, 4x+3, 4x+4},$+_{f(x)}$,$\times_{f(x)}$).

If we take α=x+4,then we can easily show that α is a primitive element of of K. Other primitive element in K are α^5, α^7,α^{11},α^{13},α^{17},α^{19},α^{23}.

3.2 Construction of field of order 3^3 over GF(3)

Consider GF(3)=({0,1,2}$+_3$,$\times_3$) and $f(x)=x^3+2x+2\in F[x]$ over GF(3). Since $f(\alpha)\neq 0$ for any $\alpha\in$GF(3).Therefore, f(x) is irreducible over GF(3).Then K=GF(3)[X]/$<X^3+2x+2>$ will be a field of order 3^3. To find all 27 elements of field K we write general element of of K which will be $ax^2+bx+c+<x^3+2x+2>$;a,b,c∈GF(3)

We write all possible order 3-tuple (a,b,c) in which first element represent the constant term and second element represent the coefficient of x and third element represent the coefficient of x^2 Now possible pairs are:

Ordered 3-tuples	Corresponding Polynomials
(0,0,0)	0
(1,0,0)	1
(2,0,0)	2
(0,1,0)	x
(1,1,0)	x+1
(2,1,0)	x+2
(0,2,0)	2x
(1,2,0)	2x+1
(2,2,0)	2x+2
(0,0,1)	x^2
(1,0,1)	x^2+1
(2,0,1)	x^2+2
(0,1,1)	x^2+x
(1,1,1)	x^2+x+1
(2,1,1)	x^2+x+2
(0,2,1)	x^2+2x
(1,2,1)	x^2+2x+1
(2,2,1)	x^2+2x+2
(0,0,2)	$2x^2$
(1,0,2)	$2x^2+1$
(2,0,2)	$2x^2+2$
(0,1,2)	$2x^2+x$
(1,1,2)	$2x^2+x+1$
(2,1,2)	$2x^2+x+2$
(0,2,2)	$2x^2+2x$
(1,2,2)	$2x^2+2x+1$
(2,2,2)	$2x^2+2x+2$

Hence, K={0, 1, 2,x, x+1, x+2, 2x, 2x+1, 2x+2, x^2, x^2+1, x^2+2, x^2+X, x^2+X+1, x^2+X+2, x^2+2X, x^2+2X+1, x^2+2X+2, $2x^2$, $2x^2+1$, $2x^2+2$, $2x^2+X$, $2x^2+X+1$, $2x^2+X+2$, $2x^2+2X$, $2x^2+2X+1$, $2x^2+2X+2$}.

Here ($K,+_{f(x)},\times_{f(x)}$) is a field.
Here $\alpha=x^2+1$ is a primitive element of K. Other primitive element in Kare α^5, α^7, α^9, α^{11}, α^{15}, α^{17}, α^{19}, α^{21}, α^{23}, α^{25}.

3.3 Construction of field of order 3^4 over GF(3)

Consider GF(3)=({0,1,2} $+_3$,$\times_3$) and irreducible polynomial $f(x)=x^4+x+2\in F[x]$ of degree 4 over GF(3). Then K=GF(3)[X]/$<X^4+x+2>$ will be a field of order 3^4. To find all 81 elements of field K, we take $\alpha=x^3+1$. Therefore,

$\alpha^2=x^3+x^2+1$	$\alpha^3=x^3+x^2+x+1$	$\alpha^4=x^3+x^2+x+2$	$\alpha^5=2x^3+x^2+x$
$\alpha^6=2x^2+x+1$	$\alpha^7=x^3+2x+2$	$\alpha^8=2x^3+x^2+1$	$\alpha^9=x^3+2x^2+x+1$
$\alpha^{10}=x^3+x^2+2x+2$	$\alpha^{11}=2x^3+x^2+x+1$	$\alpha^{12}=x^3+2x^2+x+1$	$\alpha^{13}=2x^3+x^2+2x$
$\alpha^{14}=2x^2+x+1$	$\alpha^{15}=2x^3+2x$	$\alpha^{16}=2x^2+2$	$\alpha^{17}=2x^3+2x+2$
$\alpha^{18}=2x^3+2x^2+1$	$\alpha^{19}=x^3+2x^2+2x+1$	$\alpha^{20}=x^3+x^2+2x$	$\alpha^{21}=x^2+x+2$
$\alpha^{22}=2x^3+x$	$\alpha^{23}=2x^2+1$	$\alpha^{24}=x^3+2x+1$	$\alpha^{25}=x^3+x^2$
$\alpha^{26}=x^2+x$	$\alpha^{27}=x+1$	$\alpha^{28}=x^3+2$	$\alpha^{29}=2x^3+x^2+2$
$\alpha^{30}=2x^3+2x^2+x+2$	$\alpha^{31}=2x^3+2x^2+2x$	$\alpha^{32}=2x^2+2x+2$	$\alpha^{33}=x^3+2x+1$
$\alpha^{34}=x^3+2x^2$	$\alpha^{35}=x^3+2x$	$\alpha^{36}=x+2$	$\alpha^{37}=2x^3$
$\alpha^{38}=2x^2$	$\alpha^{39}=2x$	$\alpha^{40}=2$	$\alpha^{41}=2x^3+2$
$\alpha^{42}=2x^3+2x^2+2$	$\alpha^{43}=2x^3+2x^2+2x+2$	$\alpha^{44}=2x^3+2x^2+2x+1$	$\alpha^{45}=x^3+2x^2+2x$
$\alpha^{46}=x^3+2x+2$	$\alpha^{47}=2x^3+x+1$	$\alpha^{48}=x^3+2x^2+2$	$\alpha^{49}=2x^3+x^2+2x+2$
$\alpha^{50}=2x^3+2x^2+x+1$	$\alpha^{51}=x^3+2x^2+2x+2$	$\alpha^{52}=2x^3+x^2+2x+1$	$\alpha^{53}=x^3+2x^2+x$
$\alpha^{54}=x^2+2x+1$	$\alpha^{55}=x^3+x$	$\alpha^{56}=x^2+1$	$\alpha^{57}=x^3+x^2+x+1$
$\alpha^{58}=x^3+x^2+2$	$\alpha^{59}=2x^3+x^2+x+2$	$\alpha^{60}=2x^3+2x^2+x$	$\alpha^{61}=2x^2+2x+1$
$\alpha^{62}=x^3+x$	$\alpha^{63}=x^2+1$	$\alpha^{64}=2x^3+x+2$	$\alpha^{65}=2x^3+2x^2$
$\alpha^{66}=2x^2+2x$	$\alpha^{67}=2x+2$	$\alpha^{68}=2x^3+1$	$\alpha^{69}=x^3+2x^2+1$
$\alpha^{70}=x^3+x^2+2x+1$	$\alpha^{71}=x^3+x^2+x$	$\alpha^{72}=x^2+x+1$	$\alpha^{73}=x^3+x+2$
$\alpha^{74}=2x^3+x^2$	$\alpha^{75}=2x^2+x$	$\alpha^{76}=2x+1$	$\alpha^{77}=x^3$
$\alpha^{78}=x^2$	$\alpha^{79}=x$	$\alpha^{80}=1$	

Hence, $K=(\{0,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{80}\},+_{f(x)},\times_{f(x)})$ is a field of order 81.

Here we also note that total number of primitive elements in K are $\phi(80)=32$, which are as follows: $\alpha,\alpha^3,\alpha^7,\alpha^9,\alpha^{11},\alpha^{13},\alpha^{17},\alpha^{19},\alpha^{21},\alpha^{23},\alpha^{27},\alpha^{29},\alpha^{31},\alpha^{33},\alpha^{37},\alpha^{39},\alpha^{41},\alpha^{43},\alpha^{47},\alpha^{49},\alpha^{51},\alpha^{53},\alpha^{57},\alpha^{59},\alpha^{61},\alpha^{63},\alpha^{67},\alpha^{69},\alpha^{71},\alpha^{73},\alpha^{77},\alpha^{79}$.

REFERENCES

[1]. Herstein, IN(1976), Topics in Algebra, Vikas Publishing House, New Delhi.

[2]. Khanna, Vijay K and Bhambri, S K. (1993),A Course in Abstract Algebra, Vikas Publishing House New Delhi.

[3]. Vermani L.R. (1964), Elements of Algebraic Coding Theory, CHAPMAN &HALL, MATHEMATICS

[4]. Zameerudin Quazi and Surjeet Singh(1975),Modern Algebra,Vikas Publishing House New Delhi.