TUTORIAL-3
FINITE FIELD

AMAN BHARDWAJ
2019SIY7580

Q1 GIVEN- Ring is commutative with Identity.

TO PROVE- $\mathbb{Q}(\sqrt{3})$ is a field. ie every non zero element of $\mathbb{Q}(\sqrt{3})$ has multiplicative inverse in $\mathbb{Q}(\sqrt{3})$

$x = \mathbb{Q}(\sqrt{3}) = a + b\sqrt{3}$ (Non zero element of $\mathbb{Q}$)

$$x = a + b\sqrt{3} \neq 0 \quad \text{—(i)}$$

$$x^{-1} = \frac{1}{a + b\sqrt{3}}$$

Now Rationalize

$$x^{-1} = \frac{1}{a + b\sqrt{3}} \times \frac{a - b\sqrt{3}}{a - b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} \quad \text{—(ii)}$$

$$=$$

$\therefore\ a + b\sqrt{3} \neq 0$

$\Rightarrow a \neq -b\sqrt{3} \Rightarrow a^2 \neq 3b^2$

$\Rightarrow a^2 - 3b^2 \neq 0$ —(ii)

$$x^{-1} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = a' + b'\sqrt{3} \in \mathbb{Q}(\sqrt{3})$$

$\therefore\ \mathbb{Q}(\sqrt{3})$ satisfies all the Properties of field.

$\Rightarrow \mathbb{Q}(\sqrt{3})$ is a Field.

Hence Proved

Q2. Prove $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Soln- Let $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ and $L = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

To Prove $K = L$

We need to Prove $K \subseteq L$ and $L \subseteq K$

$\because \sqrt{2}, \sqrt{3} \in K \Rightarrow \sqrt{2}+\sqrt{3} \in K$

$\Rightarrow \boxed{L \subseteq K}$ — (I)

Now we need to Prove $\sqrt{2}, \sqrt{3} \in L$

$\Rightarrow$ Prove $\sqrt{2}, \sqrt{3}, \sqrt{2\times3} = \sqrt{6} \in L$

$(\sqrt{2}+\sqrt{3})^2 = 2+3+2\sqrt{6}$

$\Rightarrow \sqrt{6} = \dfrac{(\sqrt{2}+\sqrt{3})^2 - 5}{2} \Rightarrow \boxed{\sqrt{6} \in L}$ — (II)

$\sqrt{2} = \dfrac{2(\sqrt{2}+\sqrt{3}) - \sqrt{6}(\sqrt{2}+\sqrt{3})}{(3-2)}$

$\Rightarrow \boxed{\sqrt{2} \in L}$ — (III)

$\sqrt{3} = \dfrac{3(\sqrt{2}+\sqrt{3}) - \sqrt{6}(\sqrt{2}+\sqrt{3})}{3-2}$

$\Rightarrow \sqrt{3} \in L$ — (IV)

$\because$ from (II), (III), (IV) $\sqrt{2}, \sqrt{3} \in L$

$\Rightarrow \boxed{K \subseteq L}$ — (V)

$\Rightarrow$ from eqn (I) & (V)

$K = L$

$\Rightarrow \boxed{\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})}$

Hence Proved

Q3 Find a basis of $\mathbb{Q}(\sqrt[5]{3})$ over $\mathbb{Q}$.

Soln $x^5 - 3 = 0$ is a polynomial with root $\sqrt[5]{3}$

$$x^5 - 3 = (x - \sqrt[5]{3})(x^4 + (3)^{1/5}x^3 + 3^{2/5}x^2 + 3^{3/5}x + 3^{4/5})$$

$\therefore$ it is irreducible over $\mathbb{Q}$.

$\Rightarrow$ it is monic irreducible over $\mathbb{Q}$.

$$\mathbb{Q}[\sqrt[5]{3}] = \{a_0 + a_1(3)^{1/5} + a_2(3)^{2/5} + a_3(3)^{3/5} + a_4(3)^{4/5} : a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}\}$$

$\therefore$ Basis $[\mathbb{Q}\sqrt[5]{3} : \mathbb{Q}] = \{1, \sqrt[5]{3}, (\sqrt[5]{3})^2, (\sqrt[5]{3})^3, (\sqrt[5]{3})^4\} = 5$

Q4 Prove the ring of Gaussian integers modulo 3 is a field.

Soln $\mathbb{Z}[i] = a + ib \quad a, b \in \mathbb{Z}$

Addition of $\mathbb{Z}[i]$ =

$= (a+ib) + (c+id) = (a+c) + i(b+d) = a' + ib'$ s.t. $a', b' \in \mathbb{Z}$

Multiplication of $\mathbb{Z}[i]$

$= (a+ib)(c+id) = (ac - bd) + (bc + ad)i = a'' + ib''$ s.t. $a'', b'' \in \mathbb{Z}$.

Multiplication table on next page

$\therefore$ $\mathbb{Z}[i]$ is a Commutative Ring with identity.

Now for $(a+ib) \bmod 3$ for inverse.

$\Rightarrow a, b \in \{0, 1, 2\}$ $\therefore$ 3^2 combinations of (a, b) Possible

$$(a+ib)^{-1} = \frac{1}{a+ib} \times \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = (a^2+b^2)^{-1}(a-ib)$$

$\therefore$ for non zero elements of $\mathbb{Z}[i] \bmod 3$ we need to find that

... on next page

For non zero $a, b \neq 0$ following are the combinations

$a \rightarrow$	0	0	0	1	1	1	2	2	2
$b \rightarrow$	0	1	2	0	1	2	0	1	2
$(a^2+b^2) \bmod 3$	0	1	1	1	2	2	1	2	2
$(a^2+b^2)^{-1}_{\bmod 3}$	–	1	1	1	2	2	1	2	2

∴ for non zero values of $(a+ib) \bmod 3$ the multiplicative inverse of $(a+ib)^{-1} \bmod 3 = (a^2+b^2)^{-1} \cdot (a-ib) \bmod 3$ exists in $Z[i] \bmod 3$

⇒ $Z[i] \bmod 3$ is a field.

Hence Proved.

Find Characteristics of $Z[i] \bmod 3$

Let $x \in Z[i] \bmod 3$

∴ $(x+x+x) \bmod 3 = 3x \bmod 3 = 0$

⇒ characteristic $\text{char}(Z[i] \bmod 3) = 3$ Ans

Multiplication Table With unique inverse → □

⊙	1	2	i	1+i	2+i	2i	1+2i	2+2i
1	[1]	2	i	1+i	2+i	2i	1+2i	2+2i
2	2	[1]	2i	2+2i	1+2i	i	2+i	1+i
i	i	2i	2	2+i	2+2i	[1]	1+i	1+2i
1+i	1+i	2+2i	2+i	2i	[1]	1+2i	2	i
2+i	2+i	1+2i	2+2i	[1]	i	1+i	2i	2
2i	2i	i	[1]	1+2i	1+i	2	2+2i	2+i
1+2i	1+2i	2+i	1+i	2	2i	2+2i	i	[1]
2+2i	2+2i	1+i	1+2i	i	2	2+i	[1]	2i

Q5 Is $\sqrt{2}+\sqrt[3]{7}$ algebraic over $\mathbb{Q}$?

Soln. To be $\sqrt{2}+\sqrt[3]{7}$ algebraic over $\mathbb{Q}$. There exists $f(x)$ such that $f(\sqrt{2}+\sqrt[3]{7})=0$ and coefficients of $f(x) \in \mathbb{Q}$.

Let $\sqrt{2}+\sqrt[3]{7}$ be a root of $f(x)$

$\Rightarrow x = \sqrt{2}+\sqrt[3]{7}$

$\Rightarrow (x-\sqrt{2}) = \sqrt[3]{7}$ (cubing both sides)

$\Rightarrow (x-\sqrt{2})^3 = 7 \Rightarrow x^3+6x-3x^2\sqrt{2}-(\sqrt{2})^3 = 7$

$\Rightarrow x^3+6x-\sqrt{2}(3x^2+2) = 7$

$\Rightarrow x^3+6x-7 = \sqrt{2}(3x^2+2)$

Squaring both sides

$\Rightarrow (x^3+6x-7)^2 = 2(3x^2+2)^2$

$\Rightarrow x^6+36x^2+49+12x^4-84x-14x^3 = 2(9x^4+4+12x^2)$

$\Rightarrow x^6-6x^4-14x^3+12x^2-84x+41 = 0$

This has $\sqrt{2}+\sqrt[3]{7}$ is a root of above Polynomial

$\Rightarrow f(x) = x^6-6x^4-14x^3+12x^2-84x+41$

has root $x = \sqrt{2}+\sqrt[3]{7}$

$\therefore \sqrt{2}+\sqrt[3]{7}$ is algebraic over $\mathbb{Q}$.

Hence Proved

Q6 Show F(ω) is a splitting field of ~~[illegible]~~ $f(x) = x^4+x^2+1$

Soln Find roots of $x^4+x^2+1=0$

$\Rightarrow x^4+x^2+1=0$

$\Rightarrow x^4+2x^2+1-x^2=0$

$\Rightarrow (x^2+1)^2-x^2=0$

$\Rightarrow (x^2+x+1)(x^2-x+1)=0$

$\Rightarrow x = \frac{-b \pm \sqrt{D}}{2a}$

$\Rightarrow x = \frac{-1 \pm \sqrt{-3}}{2}, \frac{+1 \pm \sqrt{-3}}{2}$

$\Rightarrow x = \frac{\pm 1 \pm i\sqrt{3}}{2}$ = cube root of unity (ω)

$\Rightarrow$ F(ω) is the splitting field of $f(x)=x^4+x^2+1$ Hence Proved

Find degree over F.

Field $F(\sqrt{-3})$ contains all roots of x^4+x^2+1

∴ Polynomial $\Rightarrow x^2+3$ is irreducible over F

∴ Extension field degree $[F(\sqrt{-3}) : F] = 2$ Ans

Q7 Show $\sqrt{2+\sqrt{3}}$ is algebraic over Q.

Soln. $a = \sqrt{2+\sqrt{3}}$

$\Rightarrow a^2 = 2+\sqrt{3}$

$\Rightarrow (a^2-2) = \sqrt{3}$

$\Rightarrow (a^2-2)^2 = 3$

$\Rightarrow a^4+4-4a^2 = 3$

$\Rightarrow a^4-4a^2+1=0$

$F(x) = x^4-4x^2+1$ has root $x = \sqrt{2+\sqrt{3}}$

∴ $x = \sqrt{2+\sqrt{3}}$ is algebraic over Q. for f(x) whose all coefficients $\in$ Q.

Hence Proved

Q8 $F_3[x]/x^2+1$ is a field.

Soln Consider field $F_3 = \{0, 1, 2\}$.

$$F_3[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_nx^n \ \forall a_n \in F_3\}$$

$$F_3[x]/x^2+1 = \{a_0 + a_1x \text{ s.t } a_0, a_1 \in F_3\}$$

x^2+1 is irreducible in F_3 $\because$ it has no root in F_3.

Consider α which satisfies $f(\alpha)$.

$$\Rightarrow \alpha^2 + 1 = 0 \Rightarrow \boxed{\alpha^2 = -1} \quad \text{—①}$$

Elements of $F_3[x]/x^2+1 = \{0, 1, 2, x, 2x, x+1, 2x+1, x+2, 2x+2\}$

Addition: Consider two elements $(ax+b), (cx+d) \in F_3[x]/x^2+1$

$$(ax+b) + (cx+d) = [(a+c)x + (b+d)] \bmod 3$$

$\therefore (a+c) \bmod 3, (b+d) \bmod 3 \in F_3$ —⑪

★ Addition Table on Next Page

Multiplication Table:- for α satisfies $f(x)$ also from ① $\alpha^2 = -1$

•	0	1	2	α	2α	$\alpha+1$	$\alpha+2$	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$\alpha+1$	$\alpha+2$	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	α	$2\alpha+2$	$2\alpha+1$	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	1	$\alpha+2$	$2\alpha+2$	$\alpha+1$	$2\alpha+1$
2α	0	2α	α	1	2	$2\alpha+1$	$\alpha+1$	$2\alpha+2$	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	$2\alpha+1$	2α	1	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	$\alpha+1$	1	α	2α	2
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	$2\alpha+2$	2	2α	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+2$	$\alpha+2$	α	2	1	2α

From last table we can see that the products of all the elements $\in F_3[x]/x^2+1$ — (III)

Multiplicative Inverse :- From multiplication table we can see that all the non-zero elements have their unique multiplicative inverse $\in F_3[x]/x^2+1$ — (IV)

∴ From (II), (III), (IV) we can say that $F_3[x]/x^2+1$ is a field. Hence Proved

It has a total of $3^2 = 9$ elements Ans

* Addition Table :-

+	0	1	2	α	$\alpha+1$	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	2α
0	0	1	2	α	$\alpha+1$	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	2α
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
2	2	0	1	$\alpha+2$	α	$\alpha+1$	2α	$2\alpha+1$	$2\alpha+2$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	1	2	0
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	2	0	1
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	0	1	2
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+2$	α	$\alpha+1$
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	α	$\alpha+1$	$\alpha+2$
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	$\alpha+1$	$\alpha+2$	α

Q9 Prove every non-zero element in $GF(2^n)$ possesses a unique multiplicative inverse.

Soln. Let us consider element

a be a non-zero element of $GF(2^n)$ | fn(x)

Let us Assume that there exist more than 1 multiplicative inverse of a in $GF(2^n)$.

∴ Let $b, c \in GF(2^n)$ be multiplicative inverse of a

$\Rightarrow a \times b = 1 \bmod f_n(x)$

& $a \times c = 1 \bmod f_n(x)$

where $f_n(x)$ be an irreducible polynomial of degree n

$\Rightarrow a \times b = a \times c \bmod f_n(x)$

$\Rightarrow a \times (b-c) = 0 \bmod f_n(x)$

$\Rightarrow$ either $Ka = 0$ or $K'(b-c) = 0$, K & K' are non 0 integers.

but $a \neq$ as a is non zero element

let $b - c = 0 \Rightarrow b = c$ but two elements can not be equal in $GF(2^n)$.

∴ our assumption is incorrect.

∴ By contradiction we can say $GF(2^n)$ Possess a unique multiplicative inverse

Hence Proved

Method II on next page.

Soln Method II 89 Let us consider an element "a" be a non zero element of $GF(2^n) / fn(x)$

Let us assume there exist more than 1 multiplicative inverse of a in $GF(2^n)$. —(I)

∴ Let p & q be the inverses $\in GF(2^n)$ —(II)

$$\therefore \quad a \times p = 1 \mod fn(x) \quad \& \quad a \times q = 1 \mod fn(x) \quad \} \text{ —(III)}$$

Consider $p \mod fn(x)$

$= 1 \cdot p \mod fn(x)$

$= (a \times q) \cdot p \mod fn(x)$ [from (III)]

$= (q \times a) \cdot p \mod fn(x)$ [$\because a \times q = q \times a = 1$]

$= q \cdot (a \times p) \mod fn(x)$ [from (III)]

$= q \cdot (1) \mod fn(x)$

$= q \mod fn(x)$

$\Rightarrow p = q = a^{-1} \mod fn(x)$

∴ our assumption was wrong.

$GF(2^n)$ Posses a unique multiplication Inverse

Hence Proved

Q10 Construct the Field F_{49}.

Soln. F_{49} has 49 elements.

$49 = 7^2$

$F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ Let irreducible Poly $f(x) = x^2 + x + 1$ with root α.

$F_7[x]/_{f(x)} = \{a_0 x + a_1 \text{ s.t. } a_0, a_1 \in F_7\}$ — (1)

$F_7[x]/_{f(x)}$ has 49 elements.

(i) Additive Closure :-

Let two elements be $ax+b$, $cx+d \in F_7[x]$

$\therefore (ax+b) + (cx+d) = [(a+c)x + (b+d)] \bmod 7$

$\in F_7[x]$

(ii) Multiplicative Closure :-

To satisfy this we need an irreducible Polynomial over F_7 which has Order = 2

$\therefore$ let ? be $f(x) = x^2+x+1$ which is irreducible over f_7 as it has no root in F_7.

(iii) Multiplicative Closure -

By Theorem :- Let K be a field and let $f \in K[x]$ be a monic irreducible Polynomial. Then $K[x]/f$ is a field.

$\therefore F_{49} = F_7[x]/x^2+x+1 = F_7[\alpha]$ α is a root of x^2+x+1

Elements of $F_{49} = \{a_0\alpha + a_1\}$ Where $a_0, a_1 = \{0, 1, 2, 3, 4, 5, 6\}$

0	α	2α	3α	4α	5α	6α
1	$\alpha+1$	$2\alpha+1$	$3\alpha+1$	$4\alpha+1$	$5\alpha+1$	$6\alpha+1$
2	$\alpha+2$	$2\alpha+2$	$3\alpha+2$	$4\alpha+2$	$5\alpha+2$	$6\alpha+2$
3	$\alpha+3$	$2\alpha+3$	$3\alpha+3$	$4\alpha+3$	$5\alpha+3$	$6\alpha+3$
4	$\alpha+4$	$2\alpha+4$	$3\alpha+4$	$4\alpha+4$	$5\alpha+4$	$6\alpha+4$
5	$\alpha+5$	$2\alpha+5$	$3\alpha+5$	$4\alpha+5$	$5\alpha+5$	$6\alpha+5$
6	$\alpha+6$	$2\alpha+6$	$3\alpha+6$	$4\alpha+6$	$5\alpha+6$	$6\alpha+6$

Q11 Number of monic irreducible polynomials in $F_3[x]$ of degree 12

Soln $N_p(m) = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d}$ —①

$p = 3 \quad d = 1, 2, 3, 4, 6, 12$

$$N_3[12] = \frac{1}{12}\left[\mu(1)3^{12} + \mu(2)3^6 + \mu(3)3^4 + \mu(4)3^3 + \mu(6)3^2 + \mu(12)3^1\right] \text{—②}$$

$\mu(1) = 1 \quad \mu(2) = -1 \quad \mu(3) = -1 \quad \mu(4) = 0 \quad \mu(6) = 1 \quad \mu(12) = 0$

Put values in ②

$$\Rightarrow N_3(12) = \frac{1}{12}\left[3^{12} - 3^6 - 3^4 + 3^2\right]$$

$$= \frac{1}{12}\left[531441 - 729 - 81 + 9\right]$$

$$= 44220$$

∴ Total no. of monic irreducible polynomials in $F_3[x]$ of degree 12 = 44220 Ans

Q12 on next Page

Q12 If a is an algebraic integer and m is an another Integer Polynomial

Prove :-

(a) $a+m$ is an algebraic integer.

(b) am is an algebraic integer.

Sol^n Let $F(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$ be n degree polynomial where $\forall i$ $b_i \in Z$ and $b_n \neq 0$.

$\because$ a is algebraic integer $\therefore$ $f(a) = 0$

$$f(a) = b_n a^n + b_{n-1} a^{n-1} + \dots + b_1 a + b_0 = 0 \quad \text{—— (1)}$$

(a) in eq (1) add and Sub m from a $\therefore F(a+m-m) =$

$$\Rightarrow b_n (a+m-m)^n + b_{n-1} (a+m-m)^{n-1} + \dots + b_1 (a+m-m) + b_0 = 0$$

$$\Rightarrow b_n \sum_{i=0}^{n} {}^nC_i (a+m)(-m)^n + \dots + b_1 [(a+m) - m] + b_0 = 0$$

Now we can separate out coefficients of $(a+m)$ & (m) and merge the coff. of $(-m)^n$ with ^nC_i and b_n. $\therefore$ we get the below form

$$\Rightarrow b_n' (a+m)^n + b_{n-1}' (a+m)^{n-1} + \dots + b_1' (a+m) + b_0' = 0$$

$$\text{—— (11)}$$

$\Rightarrow$ $(a+m)$ also gives • zero , $b_n', b_{n-1}', \dots b_0 \in Z$

$\therefore$ $(a+m)$ is algebraic Integer. Hence Proved

(b) From eq^n (1) multiply and divide m^n $\because f(a) = 0$

$$\Rightarrow \frac{m^n}{m^n} f(a) = 0$$

$$\frac{m^n}{m^n} \left[b_n a^n + b_{n-1} a^{n-1} + \dots + b_1 a + b_0 \right] = 0$$

$$\frac{1}{m^n} \left[b_n (am)^n + b_{n-1} \cdot m \cdot (am)^{n-1} + \dots + b_1 \cdot m^{n-1} (am) + b_0 m^n \right] = 0$$

$$\Rightarrow \frac{1}{m^n} \left[b_n (am)^n + b_{n-1}' (am)^{n-1} + \dots + b_1' (am) + b_0' \right] = 0$$

$b_n, b_{n-1}', \dots b_0' \in Z$

$\therefore$ (am) is algebraic integer. Hence Proved

Q13 (a) Let α be a root of $x^2+1=0$ and K be the field $F_3[\alpha]$. write down basis for K, Consider a vector space over F_3. write out the elements of F_1 explicitely.

Soln α is a root of x^2+1

$\Rightarrow \alpha^2+1=0 \Rightarrow \alpha^2 = -1 = 2 \bmod 3$.

K be field over $F_3[\alpha]$

$F_3 = \{0,1,2\}$ $\quad F_3[x] = \{a_0 + a_1 x + \cdots + a_n x^n \ \forall\ a_i \in F_3\}$

$\Rightarrow F_3[x]/x^2+1 = \{a_0 \alpha + a_1 \alpha : a_0, a_1 \in F_3\}$

∴ Elements of $F_3[\alpha]$ α is a root of x^2+1.

0	α	2α
1	$\alpha+1$	$2\alpha+1$
2	$\alpha+2$	$2\alpha+2$

Basis of $K = \{1, \alpha\}$ Ans

Element of $F_1 = \{0\}$ Ans

Q13(b) Deduce that if you repeat the construction of (a) with different irreducible polynomial then it will result in same finite field.

Proof ~~Consider F_1 and F_3~~

Consider two fields $K = F_3[\alpha] \mid m_1(x)$ & $L = F_3[\alpha] \mid m_2(x)$

where $m_1(x)$ and $m_2(x)$ are two irreducible poly. of degree $d = 2$

∴ Both K & L have $3^2 = 9$ elements.

Now we need to show K & L are isomorphic.

~~using~~

Continued on Next Page

13(b) Continued - - -

Using Proposition :- Let F be a finite field with p^d elements where p is prime and $d \geq 1$, and let

$$x^{p^d} - x = m_1(x)\, m_2(x) \cdots m_n(x)$$

be irreducible polynomial into $Z_p[x]$. Then:

(a) The minimal poly. for each element of F is one of poly $m_i(x)$ $\forall i \{1, \ldots n\}$

(b) for $\forall i$ the no. of elements of F with minimal poly. $m_i(x)$ is equal to the degree of $m_i(x)$

By above Proposition $m_1(x)$ & $m_2(x)$ are factors of $(x^{3^2} - x)$ in $F_3[x]$.

There must exist a, b in K & L respectively with degree $d = 2$ which are generators of K & L and are root of $m_1(x)$ & $m_2(x)$ respectively

$\Rightarrow$ By Proposition

$$F_3[x]/m_1(x) \simeq F_3[x]/m_2(x)$$

$\Rightarrow$ Finite field K and L are isomorphic to $F_3[x]/m_i(x)$

$\Rightarrow$ Hence we can say different irreducible Polynomials Produce same field $K = L$

Hence Proved

Where $K = L =$ Subfield of $F_3[x]$ and are isomorphic

Q14 Find all the Primitive Elements of $GF(3^2) = GF(3)/x^2+x+2$

Soln $GF[3] =$

$F_3 = \{0, 1, 2\}$

$GF(3^2) = \{ax+b : a, b \in F_3\}$

	0	1	2
0	0	x	$2x$
1	1	$1+x$	$1+2x$
2	2	$2+x$	$2+2x$

Let α be generator $GF(3) \mid x^2+x+2$

$\therefore \Rightarrow \alpha^2+\alpha+2 = 0 \Rightarrow \alpha^2 = -(\alpha+2) = 2\alpha+1$ — (1)

$\alpha^0 = 1$

$\alpha^1 = \alpha$

$\alpha^2 = 2\alpha+1$

$\alpha^3 = 2\alpha^2+\alpha = 4\alpha+2+\alpha = 2\alpha+2$

$\alpha^4 = 2\alpha^2+2\alpha = 6\alpha+2 = 2$

$\alpha^5 = 2\alpha$

$\alpha^6 = 2\alpha^2 = 4\alpha+2 = \alpha+2$

$\alpha^7 = 2\alpha^2+2\alpha = 4\alpha+1 = \alpha+1$

$\alpha^8 = \alpha^2+\alpha = 3\alpha+1 = 1$

$\therefore$ we are able to generate all the elements of $GF(3^2)$

$\therefore \alpha$ is the Primitive element which is a root of x^2+x+2

Now we will check for others :- (Check Powers of other elements)

(a) $\beta = \alpha^0 = 1$

$\beta^0 = 1$ $\therefore$ $\beta = 1$ is not generator (Primitive element)

(b) $\beta = \alpha^2 = 2\alpha+1$

$\beta^0 = 1 \quad \beta^1 = 2\alpha+1 \quad \beta^2 = \alpha^4 = 2 \quad \beta^3 = \alpha^6 = \alpha+2$

$\beta^4 = \alpha^8 = 1 \quad \beta^5 = \beta$ $\therefore$ is not primitive element

(c) $\beta = (2\alpha+2) = \alpha^3$

$\Rightarrow \beta^0 = 1 \quad \beta^1 = 2\alpha+2 \quad \beta^2 = \alpha^6 = \alpha+2 \quad \beta^3 = (\alpha+2)(2\alpha+2)$

$= 2\alpha^2 + 6\alpha + 4$

$= 4\alpha + 2 + 6\alpha + 4$

$= 10\alpha + 6 = \alpha$

$\beta^4 = \alpha(2\alpha+2) = 2\alpha^2 + 2\alpha = 2$

$\beta^5 = 2(2\alpha+2) = \alpha+1$

$\beta^6 = (2\alpha+2)(\alpha+1) = 2\alpha^2 + 4\alpha + 2 = 8\alpha + 4 = 2\alpha+1$

$\beta^7 = \beta^3 \cdot \beta^4 = 2\alpha \quad \beta^8 = 2\alpha(2\alpha+2) = 4\alpha^2 + 4\alpha = 12\alpha + 4 = 1$

$\therefore (2\alpha+2)$ is a Primitive Root

(d) $\beta = (\alpha^4) = 2$

$\beta^0 = 1 \quad \beta^1 = 2 \quad \beta^2 = 1 \Rightarrow$ Not a Primitive element

(e) $\beta = \alpha^5 = 2\alpha$

$\beta^0 = 1 \quad \beta^1 = 2\alpha \quad \beta^2 = 2\alpha \times 2\alpha = 4\alpha^2 = 8\alpha + 4 = 2\alpha + 1$

$\beta^3 = 4\alpha^2 + 2\alpha = 10\alpha + 4 = \alpha + 1$

$\beta^4 = 2\alpha^2 + 2\alpha = 6\alpha + 2 = 2$

$\beta^5 = 2 \cdot 2\alpha = \alpha \quad \beta^6 = 2\alpha^2 = \alpha + 2$

$\beta^7 = \beta^3 \cdot \beta^4 = 2\alpha + 2$

$\beta^8 = 1$ $\therefore$ 2α is a primitive element

(f) $\beta = \alpha^6 = \alpha+2$

$\beta^0 = 1, \quad \beta^1 = \alpha+2 \quad \beta^2 = \alpha^2 + 4\alpha + 2 = 6\alpha + 3 = 0$

$\therefore$ $\alpha+2$ is not a primitive element

(g) $\beta = \alpha^7 = \alpha+1 \Rightarrow \beta^0 = 0 \quad \beta^1 = \alpha+1 \quad \beta^2 = \alpha^2 + 2\alpha + 1 = \alpha+2$

$\beta^3 = \alpha^2 + 3\alpha + 2 = 2\alpha \quad \beta^4 = 2\alpha^2 + 2\alpha = 2 \quad \beta^5 = 2\alpha+2$

$\beta^6 = 8\alpha + 4 = 2\alpha + 1 \quad \beta^7 = 2 \cdot 2\alpha = \alpha \quad \beta^8 = 1$ $\therefore$ A Primitive Element

All Primitive Elements $\{\alpha, 2\alpha, \alpha+1, 2\alpha+2\}$ Ans