Vedant Milind Athavale

181090071

TY BTech EXTC

Page No.

Date

DCS Class Test

Q1.] Write the elements of GF(32) in power of element α form.

→ $GF(32) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11},$
$\alpha^{12}, \alpha^{13}, \alpha^{14}, \alpha^{15}, \alpha^{16}, \alpha^{17}, \alpha^{18}, \alpha^{19}, \alpha^{20}, \alpha^{21},$
$\alpha^{22}, \alpha^{23}, \alpha^{24}, \alpha^{25}, \alpha^{26}, \alpha^{27}, \alpha^{28}, \alpha^{29}, \alpha^{30}\}$

Primitive polynomial $\Rightarrow$ $x^5 + x^2 + 1$

α is a root

$\therefore \alpha^5 + \alpha^2 + 1 = 0$

$\Rightarrow \alpha^5 = \alpha^2 + 1$

$\alpha^6 = \alpha^3 + \alpha$

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

$\alpha^8 = \alpha^5 + \alpha^3 = 1 + \alpha^2 + \alpha^3$

$\alpha^9 = \alpha + \alpha^3 + \alpha^4$

$\alpha^{10} = \alpha^2 + \alpha^4 + \alpha^5 = \alpha^2 + \alpha^4 + 1 + \alpha^2$

$= 1 + \alpha^4$

$\alpha^{11} = \alpha + 1 + \alpha^2$

$\alpha^{12} = \alpha^2 + \alpha + \alpha^3$

$\alpha^{13} = \alpha^3 + \alpha^2 + \alpha^4$

$\alpha^{14} = \alpha^4 + \alpha^3 + 1 + \alpha^2$

$\alpha^{15} = 1 + \alpha^2 + \alpha^4 + \alpha + \alpha^3$

$\alpha^{16} = \cancel{\alpha + \alpha^3 + 1 + \alpha^2 + \alpha + \alpha^3} = 1 + \alpha + \alpha^3 + \alpha^4$

$\alpha^{17} = 1 + \alpha + \alpha^4$

$\alpha^{18} = \cancel{\alpha^3 + \alpha^2}\ \alpha + 1$

$\alpha^{19} = \alpha + \alpha^2$

$\alpha^{20} = \alpha^2 + \alpha^3$

Scanned with CamScanner

$\alpha^{21} = \alpha^3 + \alpha^4$

$\alpha^{22} = \alpha^4 + 1 + \alpha^2$

$\alpha^{23} = 1 + \alpha^2 + \alpha + \alpha^3$

$\alpha^{24} = \alpha + \alpha^3 + \alpha^2 + \alpha^4$

$\alpha^{25} = 1 + \alpha^3 + \alpha^4$

$\alpha^{26} = 1 + \alpha + \alpha^2 + \alpha^4$

$\alpha^{27} = 1 + \alpha + \alpha^3$

$\alpha^{28} = \alpha + \alpha^2 + \alpha^4$

$\alpha^{29} = 1 + \alpha^3$

$\alpha^{30} = \alpha + \alpha^4$

Page No. ______
Date ______

Q2.] Find the multiplicative inverse of each element of GF(32) in a power of α form.

→ $(1,1)$; (α, α^{30}); (α^2, α^{29}); (α^3, α^{28}); (α^4, α^{27});
(α^5, α^{26}); (α^6, α^{25}); (α^7, α^{24}); (α^8, α^{23});
(α^9, α^{22}); $(\alpha^{10}, \alpha^{21})$; $(\alpha^{11}, \alpha^{20})$; $(\alpha^{12}, \alpha^{19})$;
$(\alpha^{13}, \alpha^{18})$; $(\alpha^{14}, \alpha^{17})$; $(\alpha^{15}, \alpha^{16})$

$\Uparrow$

These are the multiplicative inverse pairs of since $\alpha^{31} = 1$.

Q3] Find the set of conjugacy class of the elements from GF(32)

→ $P(\alpha^2) = 1 + \alpha^4 + \alpha^{10}$
$= 1 + \alpha^4 + 1 + \alpha^4$
$= 0$

$\therefore \alpha^2$ is a primitive element

$\therefore (\alpha^2)^{2^1} = (\alpha^2)^2 = \alpha^4$
$(\alpha^2)^4 = \alpha^8$
$(\alpha^2)^8 = \alpha^{16}$
$(\alpha^2)^{16} = \alpha^{32} = \alpha$
$(\alpha^2)^{32} = \alpha^{64} = \alpha^2 \Rightarrow$ Repetition starts

$\therefore$ Conjugacy class of α^2 is

$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$