Vedant Milind Athavale
181090071

TY BTECH EXTC

Page No
Date 03/09/2020

DCS Tutorial - I

Q1.] (•) Vector spaces: A vector space is a collection of object called vectors, which may be added together and multiplied by numbers, called scalars

Eg :- Linear equations :- systems of homogeneous linear equations are closely tied to vector spaces. For eg:-
the solution of $a + 3b + c = 0$
$4a + 2b + 2c = 0$

where, $a = a$, $b = a/2$, $c = -5a/2$ (Triples)

• They form a vector space: sums and scalar multiples of such triples still satisfy the same ratios of the three variables

(•) Groups: A group is a set of finite element where a binary operation * on G is a rule that assigns to each pair of elements a and b, third element $c = a * b$

Eg :- $G(5) = \{0, 1, 2, 3, 4\}$
$* \Rightarrow$ mod 5 additions

(•) Fields: A set of element F on which two binary operation ('+') and (·) are defined is called a field if:

$\Rightarrow$ F is commutative under +
$\Rightarrow$ There exist additive and multiplicative identity
$\Rightarrow$ Multiplication is distributive over addition
i.e., $a \cdot (b + c) = a \cdot b + a \cdot c$

Eg: $GF(2) = \{0, 1\}$

Page No
Date

(•) <u>Vector Subspaces:</u> a subset S of vector V is a subspace if: -

⇒ For any two vectors u & V in S, u+V is also in S.

⇒ for any element a in F & V in S, a·V is also a vector in S, e.g., S = {0, 1}

(•) <u>Vector Basis :-</u> The set of linearly independent vectors that span the space is called the basis of the vector space.

Eg: (10000, 01000, 00100, 00010, 00001)
for V = {0, 1, 2, 3, 4}

(•) <u>Spanning Vectors :-</u> They are the linear combination of the basis vectors
e.g. (10000, 01000, 00100, 00010, 00001)

Page No. ______
Date ______

Q2.] Irreducible polynomial :-

A polynomial $f(X)$ over $GF(2)$ of degree 'm' is said to be irreducible over $p(x)$ if it is not divisible by any Polynomial over $GF(2)$ of degree less than 'm' but greater than zero

Eg : $1 + X + X^3$, degree 3
$1 + X + X^4$, degree 4
$1 + X^2 + X^5$, degree 5

Q3.] Primitive ~~pot~~ elements :- They are elements by taking powers of which, all the elements in the set can be obtained, except zero element.

Primitive polynomial :- An irreducible polynomial $P(x)$ of degree 'm' is said to be primitive if the smallest positive integer 'n' for which $p(X)$ divides $X^n + 1$ where $n = 2^m - 1$

E.g. $P(X) = X^3 + X + 1$ divides $1 + X^7$.

Scanned with CamScanner

Page No.
Date

Q5.] Given polynomial $F = X^5 + X^2 + 1$ over GF(2)

$GF(2) = \{0, 1\}$

$F(0) = 0 + 0 + 1 \neq 0$
$P(1) = 1 + 1 + 1 = 3 \neq 0$

Thus, F(X) does not satisfy either 0 or 1. Hence, the given polynomial is irreducible over GF(2).

Q4.] $G = \{0, 1, 2, 3, 4, 5, 6\}$

Considering element 2

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 1$ (mod-7)
$2^4 = 16 = 1$ (repeat), $2^5 = 32 = 4$ (mod-7),
$2^6 = 64 = 1$ (repeat)

Since only 1, 2, 4 are received, hence, 2 is not primitive.

Similarly, considering 3:

$3^1 = 3$, $3^2 = 9$, $3^3 = 27 = 6$, $3^4 = 81 = 4$ and
so, on gives us all elements of set

Similar results for 5.

$\therefore$ 3 & 5 are primitive elements.

Scanned with CamScanner

Q6.] $P(x) = 1 + x + x^4$

$GF(2^4) = GF(16)$

Taking,

$\alpha = 2$

$\alpha^3 = \alpha + 1$

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

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

$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = 1 + \alpha^2$

$\alpha^7 = \alpha^3 + \alpha = 1 + \alpha + \alpha = 1$

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

$\alpha^9 = \alpha + \alpha^3 = \alpha + \alpha + 1 = 1$

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

$\alpha^{11} = \alpha^3 + \alpha^5 = 1 + \alpha + 1 + \alpha + \alpha^2 = \alpha^2$

$\alpha^{12} = \alpha^3 = 1 + \alpha$

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

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

Page No.
Date

$GF(16) = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots\ldots, \alpha^{2^m - 2 = 14}\}$

$= \{0, 1, 2, 4, 3, 7, 5, 1, 5, 1, 2, 4, 3, 6, 7\}$

Q7] Conjugacy class -

I Let α be root of polynomial, its roots are

α^{2^l}, $l = 1 \Rightarrow \alpha^2$

similarly considering $l = 2, 3, 4$

$\alpha^2, \alpha^4, \alpha^8, \alpha^{16} = \alpha$ since $\alpha^{15} = 1$

$\therefore$ Conjugacy class $= \{\alpha, \alpha^2, \alpha^4, \alpha^8\}$
for root α

II Let α^3 be root of polynomial its other roots are -

$(\alpha^3)^{2^l}$

Taking $l = 1, 2, 3, 4$ we get

$\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^8, \alpha^{48} = \alpha^3$ (respectively)

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$(\alpha^3)^{2^1} \quad (\alpha^3)^{2^2} \quad (\alpha^3)^{2^3} \quad (\alpha^3)^{2^4}$

$\therefore$ Conjugacy class for α^3 is $= \{\alpha^3, \alpha^6, \alpha^8, \alpha^{12}\}$

Page No.
Date

III Let α^5 be the root of polynomial its other roots are -

$$(\alpha^5)^{2^l}$$

Taking $l = 1, 2$ we get,

$$\underset{(\alpha^5)^2}{\alpha^{10}}, \underset{(\alpha^5)^{2^2}}{\alpha^{20}} = \alpha^5 \text{ (repeating)}$$

$\therefore$ Conjugacy class for α^5 is $= \{\alpha^5, \alpha^{10}\}$

IV Let α^7 be root of polynomial its other roots are -

$$(\alpha^7)^{2^l}$$

Taking, $l = 1, 2, 3$ we get,

$$\underset{(\alpha^7)^2}{\alpha^{14}}, \underset{(\alpha^7)^{2^2}}{\alpha^{28}} = \alpha^{13}, \underset{(\alpha^7)^{2^3}}{\alpha^{56}} = \alpha^{11}, \underset{(\alpha^7)^{2^4}}{\alpha^{112}} = \alpha^7$$

(repeating)

$\therefore$ Conjugacy class is $= \{\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}\}$