Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Not Distributive Lattice Over Field of Residue Classes Modulo 5

T. Srinivasarao
Asst.Professor
Dept. Of Math.
University College of Science & Technology
Adikavi Nannaya University
Rajahmundry

Dr. V. Mallipriya
Asst. Professor
Dept. Of Math.
UCS&T
ANUR
Rajahmundry

***Abstract*: The symmetry in algebra usually allows a undirected path between the source and sink in any discussion. So, creating a super algebra in the form of a lattice over a known algebra which does not admit associativity or commutativity or distributivity will help a directed path which has no retreat. Keeping this view point, i have created 3 not distributive lattices over different known fields which can be used in the cryptography techniques of varied approach.**
This is the 4th lattice over somewhat bigger field where the lattice is constructed using the suitable definitions of disjunction and conjunction that allows the failure of distributive property and the lattice is a field extension over the residue classes modulo 5.

CHAPTER 1: INTRODUCTION:

The set of residue classes modulo *p* is a field under addition modulo *p* and multiplication modulo *p*. Let us consider an irreducible polynomial over this field and take the principal ideal generated by the irreducible polynomial. This ideal is the maximal idea in the said field. So, the quotient ring formed is also a field which is the field extension.

Take the extended field as a set on which the disjunction and conjunction operations are defined to verify the distributive property is failed.

CHAPTER 2: CONSTRUCTING A FIELD EXTENSION OVER THE FIELD OF RESIDUE CLASSES MODULO 5

$\mathbb{Z}_5[x]=\{[0],[1],[2],[3],[4]\}$ is the finite field

$f([x])=[2]+[4]x+[3]x^2$ is such that $f([0])=[2],\ f([1])=[4],\ f([2])=[2],\ f([3])=[1],\ f([4])=[1]$

This shows that $f([x])=[2]+[4]x+[3]x^2$ is an irreducible polynomial over $\mathbb{Z}_5[x]$

$\langle f(x)\rangle$ is a principal ideal and maximal ideal in the commutative ring with unity $\mathbb{Z}_5[x]$

So, $\mathbb{Z}_5[x]/\langle f(x)\rangle = \mathbb{Z}_5[x]/M$ is a field.

This field can be visualized in the roaster form as follows.

$\{0+M=2+4x+3x^2, 1+M=3+4x+3x^2, 2+M=4+4x+3x^2, 3+M=4x+3x^2, 4+M=1+4x+3x^2,$

$x+M=2+3x^2, 2x+M=2+x+3x^2, 3x+M=2+2x+3x^2, 4x+M=2+3x+3x^2,$

$x^2+M=2+4x+4x^2, 2x^2+M=2+4x, 3x^2+M=2+4x+x^2, 4x^2+M=2+4x+2x^2,$

$1+x+M=3+3x^2, 2+x+M=4+3x^2, 3+x+M=3x^2, 4+x+M=1+3x^2,$

$1+2x+M=3+x+3x^2, 2+2x+M=4+x+3x^2, 3+2x+M=x+3x^2, 4+2x+M=1+x+3x^2,$

$1+3x+M=3+2x+3x^2, 2+3x+M=4+2x+3x^2, 3+3x+M=2x+3x^2, 4+3x+M=1+2x+3x^2,$

$1+4x+M=3+3x+3x^2, 2+4x+M=4+3x+3x^2, 3+4x+M=3x+3x^2, 4+4x+M=1+3x+3x^2,$

$1+x^2+M=3+4x+4x^2, 2+x^2+M=4+4x+4x^2, 3+x^2+M=4x+4x^2, 4+x^2+M=1+4x+4x^2,$

$1+2x^2+M=3+4x, 2+2x^2+M=4+4x, 3+2x^2+M=4x, 4+2x^2+M=1+4x,$

$1+3x^2+M=3+4x+x^2, 2+3x^2+M=4+4x+x^2, 3+3x^2+M=4x+x^2, 4+3x^2+M=1+4x+x^2,$

$1+4x^2+M=3+4x+2x^2, 2+4x^2+M=4+4x+2x^2, 3+4x^2+M=4x+2x^2, 4+4x^2+M=1+4x+2x^2,$

$x+x^2+M=2+4x^2, 2x+x^2+M=2+x+4x^2, 3x+x^2+M=2+2x+4x^2, 4x+x^2+M=2+3x+4x^2,$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

$x+2x^2+M=2,2x+2x^2+M=2+x,3x+2x^2+M=2+2x,4x+2x^2+M=2+3x,$
$x+3x^2+M=2+x^2,2x+3x^2+M=2+x+x^2,3x+3x^2+M=2+2x+x^2,4x+3x^2+M=2+3x+x^2,$
$x+4x^2+M=2+2x^2,2x+4x^2+M=2+x+2x^2,3x+4x^2+M=2+2x+2x^2,4x+4x^2+M=2+3x+2x^2,$
$1+x+x^2+M=3+4x^2,2+x+x^2+M=4+4x^2,3+x+x^2+M=4x^2,4+x+x^2+M=1+4x^2,$
$4+2x+x^2+M=1+x+4x^2,$
$1+2x+x^2+M=3+x+4x^2,2+2x+x^2+M=4+x+4x^2,3+2x+x^2+M=x+4x^2,$
$1+3x+x^2+M=3+2x+4x^2,2+3x+x^2+M=4+2x+4x^2,3+3x+x^2+M=2x+4x^2,$
$4+3x+x^2+M=1+2x+4x^2,$
$1+4x+x^2+M=3+3x+4x^2,2+4x+x^2+M=4+3x+4x^2,3+4x+x^2+M=3x+4x^2,$
$4+4x+x^2+M=1+3x+4x^2,$
$1+x+2x^2+M=3,2+x+2x^2+M=4,3+x+2x^2+M=0+M,4+x+2x^2+M=1,$
$1+2x+2x^2+M=3+x,2+2x+2x^2+M=4+x,3+2x+2x^2+M=x,4+2x+2x^2+M=1+x,$
$1+3x+2x^2+M=3+2x,2+3x+2x^2+M=4+2x,3+3x+2x^2+M=2x,4+3x+2x^2+M=1+2x,$
$1+4x+2x^2+M=3+3x,2+4x+2x^2+M=4+3x,3+4x+2x^2+M=3x,4+4x+2x^2+M=1+3x,$
$1+x+3x^2+M=3+x^2,2+x+3x^2+M=4+x^2,3+x+3x^2+M=x^2,4+x+3x^2+M=1+x^2,$
$1+2x+3x^2+M=3+x+x^2,2+2x+3x^2+M=4+x+x^2,3+2x+3x^2+M=x+x^2,$
$4+2x+3x^2+M=1+x+x^2,$
$1+3x+3x^2+M=3+2x+x^2,2+3x+3x^2+M=4+2x+x^2,3+3x+3x^2+M=2x+x^2,$
$4+3x+3x^2+M=1+2x+x^2,1+4x+3x^2+M=3+3x+x^2,2+4x+3x^2+M=4+3x+x^2,3+4x+3x^2+M=3x+x^2,$
$4+4x+3x^2+M=1+3x+x^2,$
$1+x+4x^2+M=3+2x^2,2+x+4x^2+M=4+2x^2,3+x+4x^2+M=2x^2,4+x+4x^2+M=1+2x^2$
$1+2x+4x^2+M=3+x+2x^2,2+2x+4x^2+M=4+x+2x^2,3+2x+4x^2+M=x+2x^2,$
$4+2x+4x^2+M=1+x+2x^2,$
$1+3x+4x^2+M=3+2x+2x^2,2+3x+4x^2+M=4+2x+2x^2,3+3x+4x^2+M=2x+2x^2,$
$4+3x+4x^2+M=1+2x+2x^2,$
$1+4x+4x^2+M=3+3x+2x^2,2+4x+4x^2+M=4+3x+2x^2,3+4x+4x^2+M=3x+2x^2,$
$4+4x+4x^2+M=1+3x+2x^2\}$

CHAPTER 3: DISJUNCTION AND CONJUNCTION OVER THE FIELD EXTENSION

$$\left|\mathbb{Z}_5[x]/M\right|=125$$

The exponent modulo 2 operation is based on the exponent of the irreducible polynomial which is the cause of the construction of the Galois field.

Definition 1: if *f* and *g* are two members of $\mathbb{Z}_5[x]/M$, then the disjunction is defined by

$$f\vee g=\left\{\left\{\int f(x)g(x)dx\right\}\bmod(5,2)\right\}\bmod 5$$

Note that $\left\{\int cx^n dx\right\}\bmod(5,2)=c\left\{\frac{x^{n+1}}{n+1}\right\}\bmod(5,2)=\left(c\left[5-(n+1)\right]\right)\bmod 5\ x^{(n+1)\bmod 2}$

Definition 2: if f and *g* are the members of $\mathbb{Z}_5[x]/M$, then their conjunction is defined by

$$f\wedge g=\left\{\frac{d}{dx}\left(f(x)g(x)\bmod(5,2)\right)\right\}\bmod 5$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

$$\frac{d}{dx}\left(cx^n\right)\bmod(5,2)=(cn)\bmod 5x^{(n-1)\bmod 2}$$

$$f(x)=1+4x+3x^2, g(x)=4+x, h(x)=3+4x^2$$

$$f\vee g=\left\{\left\{\int\left(1+4x+3x^2\right)(4+x)dx\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left\{\int\left(4+2x+x^2+3x^3\right)dx\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left\{4\frac{x}{1}+\frac{2x^2}{2}+\frac{x^3}{3}+\frac{3x^4}{4}\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left[4(5-2)\right]\bmod 5\ x^{2\bmod 2}+\left[2(5-3)\right]\bmod 5\ x^{3\bmod 2}+\left[5-4\right]\bmod 5\ x^{4\bmod 2}+\left[3(5-5)\right]\bmod 5\ x^{5\bmod 2}$$

$$=\left\{12\bmod 5\left(x^0\right)+4\bmod 5\left(x^1\right)+1\bmod 5\left(x^0\right)+0\bmod 5\left(x^1\right)\right\}\bmod 5$$

$$=3+4x \qquad \text{..... (3.1)}$$

$$f\vee h=\left\{\left\{\int\left(1+4x+3x^2\right)\left(3+4x^2\right)dx\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left\{\int\left(3+12x+13x^2+16x^3+12x^4\right)dx\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left[3\frac{x}{1}+\frac{12x^2}{2}+\frac{13x^3}{3}+\frac{16x^4}{4}+\frac{12x^5}{5}\right]\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left[3(5-2)\right]\bmod 5x^{2\bmod 2}+\left[12(5-3)\right]\bmod 5x^{3\bmod 2}+\left[13(5-4)\right]\bmod 5x^{4\bmod 2}+\left[16(5-5)\right]\bmod 5x^{5\bmod 2}\right.$$

$$\left.+\left[12(5-6)\right]\bmod 5x^{6\bmod 2}\right\}\bmod 5$$

$$=\left\{4\left(x^0\right)+4\left(x^1\right)+3\left(x^0\right)+0\left(x^1\right)+3\left(x^0\right)+1\left(x^1\right)+3\left(x^0\right)\right\}\bmod 5$$

$$=3 \qquad \text{..... (3.2)}$$

$$(f\vee g)\wedge(f\vee h)=\left\{\frac{d}{dx}\left\{(3+4x)3\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left\{\frac{d}{dx}(9+12x)\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{0\bmod 5+\left[12(1)\right]\bmod 5x^{0\bmod 2}\right\}\bmod 5$$

$$=2 \qquad \text{..... (3.3)}$$

$$g\wedge h=\left\{\frac{d}{dx}\left(g(x)h(x)\right)\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\frac{d}{dx}(4+x)\left(3+4x^2\right)\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\frac{d}{dx}\left(12+3x+16x^2+4x^3\right)\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left(0+3x^0+32x^1+12x^2\right)\bmod(5,2)\right\}\bmod 5$$

$$=\left\{3\left(x^{0\bmod 2}\right)+2\left(x^{1\bmod 2}\right)+2\left(x^{2\bmod 2}\right)\right\}\bmod 5$$

$$=2x \qquad \text{..... (3.4)}$$

$$f\vee(g\wedge h)=\left\{\left\{\int\left(1+4x+3x^2\right)(2x)\right\}\bmod(5,2)\right\}\bmod 5$$

$$=\left\{\left\{\int\left(2x+8x^2+6x^3\right)dx\right\}\bmod(5,2)\right\}\bmod 5$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

$$= \left\{ \left\{ \int \left(2\frac{x^{1+1}}{1+1} + 8\frac{x^{2+1}}{2+1} + 6\frac{x^{3+1}}{3+1} \right) dx \right\} \bmod(5,2) \right\} \bmod 5$$

$$= \left\{ \left\{ 2(5-3)x^2 + 8(5-4)x^3 + 6(5-5)x^4 \right\} \bmod(5,2) \right\} \bmod 5$$

$$= \left\{ 4 \bmod 5 x^{2 \bmod 2} + 8 \bmod 5 x^{3 \bmod 2} + 6(0) \bmod 5 x^{4 \bmod 2} \right\} \bmod 5$$

$$= \left\{ 4x^0 + 3x^1 + 0x^0 \right\} \bmod 5$$

$$= 4 + 3x \qquad \text{..... (3.5)}$$

From (3.3) and (3.5), it follows that the distributivity fails where as other basic properties of a lattice are satisfied.

Inference: $\mathbb{Z}_5[x]/M$ is a lattice in which the distributive property is failed.

Among many such examples given by me, this is the new field which is shown as a ***not distributive lattice***.

REFERENCES:

i. T.Srinivasarao & L.Sujatha, *Residue Matrix and not Distributive Lattice*, IJMTT, 65(8)(2019),1-3
ii. A.J.Kempner, *Polynomials and their residue systems,* Amer.Math.Soc.Trans., 22(1921),240-258
iii. Z.Chen, *On polynomial functions from* $\mathbb{Z}_n$ to $\mathbb{Z}_m$, Discrete Mathematics, 137(1995), 137-145.
iv. T.Srinivasarao & K.Geetha Lakshmi, *Not Distributive Lattice Over a Galois Field,* IJMAA, 7(4)(2019),123-125.