Int. J. Math. And Appl., 7(4)(2019), 123–125
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of *Mathematics And its Applications*

Not Distributive Lattice Over a Galois Field

T. Srinivasarao[1,*] and K. Geetha Lakshmi[1]

1 Department of Mathematics, Adikavi Nannaya University, Rajamahendravaram, East Godavari, Andhra Pradesh, India.

Abstract: A prime element in a Euclidean ring and to an irreducible polynomial in a polynomial ring defined over a field are identical. The irreducible polynomial allows us to construct a prime ideal which in turn leading to a maximal ideal. So, the maximal ideal and the Euclidean ring together form a quotient field in which the zero element is the maximal ideal itself. The quotient field is seen as the extended field over the field referred in the beginning. It is easily seen that the actual irreducible polynomial $f(x)$ is now reducible over the extended field. In the present case, we take a finite field and a polynomial from the polynomial ring over this field and verify the members of the field obey the distributive law or not. The purpose of producing a not distributive lattice is to see that enciphering can be done using the members of such a lattice in which it will be difficult to judge the correct deciphered text. Because, there will be multiple results in the deciphering approach. So, which is the correct decipher among the available cipher texts will be a matter of confusion. The present Galois field is over the field of residue classes modulo 3.

Keywords: Distributive Lattice, Galois Field, Euclidean ring.

1. Introduction

If $(R,+,\bullet)$ is a commutative ring with unity and M is an ideal of R, then M is maximal if and only if R/M is a field. We fit a polynomial ring $F[x]$ in the place of the commutative ring with unity while every polynomial ring defined over a field F is a commutative ring with unity. Also, we replace the maximal ideal M by a principal ideal generated by an irreducible polynomial $\langle p(x)\rangle$ over the ring $F[x]$ leading to $\frac{F[x]}{\langle p(x)\rangle}$ as a field under the addition of cosets defined by $\{\langle p(x)\rangle + f(x)\} \oplus \{\langle p(x)\rangle + g(x)\} = \langle p(x)\rangle + \{f(x) + g(x)\}$ and the multiplication of cosets defined by $\{\langle p(x)\rangle + f(x)\} \odot \{\langle p(x)\rangle + g(x)\} = \langle p(x)\rangle + \{f(x) \bullet g(x)\}$ having the zero element $\langle p(x)\rangle$ and any member of $\frac{F[x]}{\langle p(x)\rangle}$ in the form $\langle p(x)\rangle + f(x)$ is the non zero element if $f(x) \neq p(x)\,g(x)$ for any $g(x)$in $F[x]$.

$$\mathbb{Z}_3 = \{[0],[1],[2]\}$$
$$f(x) = x^2 + 2x + 2$$
$$f([0]) = [2], \quad f([1]) = [2], \quad f([2]) = [1]$$

Observe that $f([x]) \neq [0] \quad \forall \quad 0 \leq x \leq 2$. So, $p(x) = x^2 + 2x + 2$ is irreducible over $\mathbb{Z}_3$. We now make the linear factors of this polynomial that are reducible over the extended fields.

Obviously $\mathbb{Z}_3[x]$ is a polynomial ring under addition modulo 3 and multiplication modulo 3, which is also a commutative ring with unity and $\langle p(x)\rangle = \langle x^2 + 2x + 2\rangle$ is the principal ideal generated by the irreducible polynomial $f(x)$, it is the

* *E-mail: 3848tsrinivasarao@gmail.com*

maximal ideal in $\mathbb{Z}_3[x]$. So, $\frac{\mathbb{Z}_3[x]}{\langle p(x)\rangle} = \mathbb{Z}_3^*[x]$ is a field under the addition of cosets defined by

$$\langle p(x)\rangle + g(x) \oplus \langle p(x)\rangle + h(x) = \langle p(x)\rangle + (g+h)(x)$$

and multiplication of cosets defined by $\langle p(x)\rangle + g(x) \odot \langle p(x)\rangle + h(x) = \langle p(x)\rangle + g(x)h(x)$

$$\frac{\mathbb{Z}_3[x]}{\langle p(x)\rangle} = \{p(x), p(x)+1, p(x)+2, p(x)+x, p(x)+2x, p(x)+1+x, p(x)+2+x, p(x)+1+2x, p(x)+2+2x\}$$

with 9 elements and $f(x)$ is the zero element. We now show that $f(x)$ is reducible over $\mathbb{Z}_3^*[x]$. This field can also conveniently be written as $\mathbb{Z}_3^*[x] = \{0, 1, 2, x, 2x, 1+x, 1+2x, 2+x, 2+2x\}$ by using the zero element x^2+2x+2.
Observe that $\left(x^2+2x+2\right)+1$& $\left(x^2+2x+2\right)+2$ are the non zero elements of $\mathbb{Z}_3^*[x]$. Consider

$$\begin{aligned}\left\{\left(x^2+2x+2\right)+1\right\} \otimes \left\{\left(x^2+2x+2\right)+2\right\} &= \left\{\left(x^2+2x+2\right)+1\right\} \otimes \left\{\left(x^2+2x+2\right)+2\right\} \\ &= \left(x^2+2x+2\right)^2 + 3\left(x^2+2x+2\right) \\ &= \left(x^2+2x+2\right)\left\{x^2+2x+2+3\right\} \\ &= \left(x^2+2x+2\right)\left\{x^2+2x+2\right\} \\ &= \left(x^2+2x+2\right)^2\end{aligned}$$

and this is a multiple of $p(x) \in \langle p(x)\rangle$ the zero element of $\mathbb{Z}_3^*[x]$. So, $x^2+2x+2+1 = x^2+2x$ and $x^2+2x+2+2 = x^2+2x+1$ are the factors of $p(x) = x^2+2x+2$ in the extension field. So, $\mathbb{Z}_3^*[x]$ is an extension field or a Galois field defined over the field $\mathbb{Z}_3$ with the irreducible polynomial $p(x) = x^2+2x+2$.

Remark 1.1. *See that the degree of the factor polynomials $p(x)$ is equal to the degree of the polynomial $p(x)$. The reason for this is, the field over which $p(x)$ irreducible is already a finite field.*

Definition 1.2. $p(x) \vee_{mod\ 3} q(x) = \left\{\int p(x)\, q(x)\, dx\right\} mod\ 3$,

$$\left\{\int x^n dx\right\} mod\ 3 = \left\{\frac{x^{n+1}}{n+1}\right\} mod\ 3 = (3-(n+1)\ mod\ 3)\, x^{(n+1) mod\ 3}$$

Definition 1.3. $p(x) \wedge_{mod\ 3} q(x) = \left\{\frac{d}{dx}(p(x)\, q(x))\right\} mod\ 3$,

$$\frac{d}{dx}(x^n) = (n\ mod\ 3)\, x^{n-1\ mod\ 3}$$

$\vee_{mod3}$	0	1	2	x	$2x$	$1+x$	$2+x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	x	$2x$	x^2	x^2	$x+x^2$	$2x+x^2$	$x+x^2$	$2x+x^2$
2	0	$2x$	x	x^2	x^2	$2x+x^2$	$x+x^2$	$2x+x^2$	$x+x^2$
x	0	x^2	x^2	0	0	x^2	x^2	x^2	x^2
$2x$	0	x^2	x^2	0	0	x^2	x^2	x^2	x^2
$1+x$	0	$x+x^2$	$2x+x^2$	x^2	x^2	$x+x^2$	$2x$	x	$2x+x^2$
$2+x$	0	$2x+x^2$	$x+x^2$	x^2	x^2	$2x$	$x+x^2$	$2x+x^2$	x
$1+2x$	0	$x+x^2$	$2x+x^2$	x^2	x^2	x	$2x+x^2$	$x+x^2$	$2x$
$2+2x$	0	$2x+x^2$	$x+x^2$	x^2	x^2	$2x+x^2$	x	$2x$	$x+x^2$

$\wedge_{mod3}$	0	1	2	x	$2x$	$1+x$	$1+2x$	$2+x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	2	1	2	1	2
2	0	0	1	2	1	2	1	2	1
x	0	1	2	$2x$	x	$1+2x$	$1+x$	$2+2x$	$2+x$
$2x$	0	2	1	x	$2x$	$2+x$	$2+2x$	$1+x$	$1+2x$
$1+x$	0	1	2	$1+2x$	$2+x$	$2+2x$	x	$2x$	$1+x$
$1+2x$	0	2	1	$1+x$	$2+2x$	x	$1+2x$	$2+x$	$2x$
$2+x$	0	1	2	$2+2x$	$1+x$	$2x$	$2+x$	$1+2x$	x
$2+2x$	0	2	1	$2+x$	$1+2x$	$1+x$	$2x$	x	$2+2x$

$$\langle p(x)\rangle + (1+2x) \wedge_{mod\ 3} \{\langle p(x)\rangle + (2+x) \vee_{mod\ 3} \langle p(x)\rangle + (1+x)\} = \langle p(x)\rangle + 2 + 2x \quad (1)$$

$$\{\langle p(x)\rangle + (1+2x) \wedge_{mod\ 3} \langle p(x)\rangle + (2+x)\} \vee_{mod\ 3} \{\langle p(x)\rangle + (1+2x) \wedge_{mod\ 3} \langle p(x)\rangle + (1+x)\} = \langle p(x)\rangle + (2+x) \vee_{mod\ 3} (x)$$
$$= \langle p(x)\rangle + x^2 \quad (2)$$

(1) & (2) confirm that the lattice is not distributive.

References

[1] A.J.Kempner, *Polynomials and their residue systems* , Amer. Math. Soc. Trans., 22(1921), 240-288.

[2] Z. Chen, *On polynomial functions from Z_n to Z_m*, Discrete Mathematics, 137(1995), 137-145.

[3] G. Birkhoff and O. Frink, *Representations of lattices by sets*, Transactions of American Mathematical Society, 64(2)(1948), 299-316.

[4] T. Srinivasarao and L. Sujatha, *title?*, IJMTT, 65(8)(2019), pp ?

[5] T. Srinivasarao and G. Ashok, *title?*, IJMAA, Vol. ?, Issue ?, Year ?, Page ?