Int. J. Math. And Appl., 7(3)(2019), 123–125
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of *Mathematics And its Applications*

Not Distributive Lattice Over Residue Classes Polynomial Ring

T. Srinivasarao[1,*] and G. Ashok[1]

1 Department of Mathematics, Adikavi Nannaya University, Rajarajanarendranagar, Andhra Pradesh, India.

Abstract: In the era of soft skills and almost every area of physical activity and space, the shied ankle role player is data security. However safe the data may be today by creating the firewall, in few hours or days, those firewalls are pierced through and the data will be hacked/stolen. So, every moment, there is a need for creating new firewalls or new techniques in security systems. Ciphering through algebraic techniques is my view point and taking a lattice based on algebra and failure of distributive property may be considered as a productive approach that enciphers a code and deciphering may be difficult while there is no regularity/balance in the system. The polynomial ring defined over a finite field of residue classes modulo p where p is a prime, is a commutative ring with unity. A principal ideal generated by an irreducible polynomial is a maximal ideal in that ring. So, the theorem 'if R is a commutative ring with unity, M is an ideal of R, then M is maximal if and only if the quotient ring of R by M is a field", helps us to construct a field. Defining the 'join' denoted by '$\vee$' and 'meet' , '$\wedge$' operations on this field using the modulo p operation both on the coefficient and exponent of each monomial of each polynomial will allow the closedness under these operations and thus the formed lattice is a closed algebra. In the present discussion, we restrict our view to the elements of $\mathbb{Z}_5^5[x]$ up to distributive property.

Keywords: Residue classes, polynomial ring, field, join; meet, integration modulo 5, differentiation modulo 5, supremum and infimum, Congruent and Equivalent polynomials, Distributive laws.

1. Introduction

Finite field of residue classes modulo 5 is considered and polynomial ring is defined on it. The lattice in which the distributive property is not assumed is a non distributive lattice and the one in which the distributive property is assumed but failed is a not distributive lattice. The present discussion is about not distributive lattice. We deal with the sets of polynomials in the perspective of Birkhoff [3]. The modulo 5 operation is used on both the coefficient and exponent of each of the monomials of each of the polynomials is defined and so, the formed set denoted by $\mathbb{Z}_5^5[x]$ read as 'multi modulo 5 set of polynomials over integers. The 'multi modulo 5' operation is written as $\left(\int\limits_{\mathbb{Z}_5^5} f(x)\, g(x)\, dx\right) mod\ 5$ and $\left(\frac{d}{dx}\left(f(x)\, g(x)\right)\right) mod\ 5$ according to the operation used.

1.1. Polynomial Ring over a finite field

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

$$\mathbb{Z}_5^5[x] = \left\{0, 1, 2, 3, 4, x, 2x, 3x, 4x, x + x^2, ..., 4 + 4x + 4x^2 + 4x^3 + 4x^4\right\}$$

These are the all polynomials possible by restricting the degree to 4 using the modulo 5 and taking coefficients from the field $\mathbb{Z}_5$.

$$\left|\mathbb{Z}_5^5[x]\right| = 3125$$

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

Definition 1.1. *Let* $f(x), g(x) \in \mathbb{Z}_5^5[x]$, *then*

$$f(x) \vee g(x) = \sup\langle f, g\rangle = \left(\int_{\mathbb{Z}_5^5} f(x)\, g(x)\, dx\right) mod\ 5 \tag{1}$$

Where

$$\left(\int_{\mathbb{Z}_5^5} x^n x^m dx\right) mod\ 5 = \left(mod\left(\frac{x^{n+m+1}}{n+m+1}, 5\right)\right) = (n+m+1)\, mod\ 5 \cdot x^{(n+m+1) mod\ 5} \tag{2}$$

Definition 1.2. *Let* $f(x), g(x) \in \mathbb{Z}_5^5[x]$, *then*

$$f(x) \wedge g(x) = \inf\langle f, g\rangle = \left(\frac{d}{dx}\left(f(x)\, g(x)\right)\right) mod\ 5 \tag{3}$$

Where

$$\left(\frac{d}{dx}_{\mathbb{Z}_5^5}\left(f(x)\, g(x)\right)\right) mod\ 5 = mod\,(n+m, 5) \cdot x^{(n+m-1) mod\ 5} \tag{4}$$

2. $\left(\mathbb{Z}_5^5[x], \vee, \wedge\right)$ is a Lattice

Every two members of $\mathbb{Z}_5^5[x]$ can be compared using $\vee$ or $\wedge$. So, reflexive, anti-symmetry and transitive properties follow. The uniqueness of integral and that of the derivative confirms that the supremum 'sup' or $\vee$ and infimum 'inf' or $\wedge$ are unique for each pair of members of the set $\mathbb{Z}_5^5[x]$. This establishes the lattice structure of $\mathbb{Z}_5^5[x]$.

Theorem 2.1. $\left(\mathbb{Z}_5^5[x], \vee, \wedge\right)$ *is not a distributive lattice.*

Proof. Consider

$$f(x) = 3x^4 + 2x,$$
$$g(x) = 4x^3 + 2,$$
$$h(x) = x^2 + 2x + 4 \in \mathbb{Z}_5^5[x]$$

Then

$$f(x)\, g(x) = 4x^4 + 2x^2 + 4x$$
$$\left(\int_{\mathbb{Z}_5^5} f(x)\, g(x)\, dx\right) mod\ 5 = \left\{4\left(mod\left(\frac{x^5}{5}, 5\right)\right) + 2\left(mod\left(\frac{x^3}{3}, 5\right)\right) + 4\left(mod\left(\frac{x^2}{2}, 5\right)\right)\right\}$$
$$f \vee g = 4x^3 + 2x^2 \tag{5}$$
$$f(x)\, h(x) = 2x^4 + 2x^3 + 4x^2 + x + 1$$
$$\left(\int_{\mathbb{Z}_5^5} f(x)\, h(x)\, dx\right) mod\ 5 = 2x^4 + 3x^3 + 2x^2 + x$$
$$f \vee h = 2x^4 + 3x^3 + 2x^2 + x \tag{6}$$

Therefore Equations (3), (5) and (6) result in

$$(f \vee g) \wedge (f \vee h) = \left(\frac{d}{dx_{\mathbb{Z}_5^5}}\left(4x^3 + 2x^2\right)\left(2x^4 + 3x^3 + 2x^2 + x\right)\right) mod\ 5$$
$$= 2x^3 + x^2 + x + 1 \tag{7}$$

$$g(x) \wedge h(x) = \left(\frac{d}{dx_{Z_5^5}} \left(4x^3 + 2\right)\left(x^2 + 2x + 4\right) \right) mod\ 5 \tag{8}$$

$$= 2x^3 + 3x^2 + 4x + 4 \tag{9}$$

$$f(x) \vee (g(x) \wedge h(x)) = ?$$

Using (8) in the Definition 1.2,

$$\left(\int_{\mathbb{Z}_5^5} \left(3x^4 + 2x\right)\left(2x^3 + 3x^2 + 4x + 4\right) dx \right) mod\ 5 = x^4 + 3x^3 + x^2 + 2x \tag{10}$$

Equations (7) and (8) confirm that the distributive law fails in the ring of residue polynomials over the field of residues. Therefore $\left(\mathbb{Z}_5^5, \vee, \wedge\right)$ is a lattice in which the distributive property fails. □

3. Conclusions

The set of lattices defined over numerous algebraic structures that failed to admit the distributive property are of the purpose serving towards the information technology where there is the construction of firewalls and keeping the hacking away and maintain the security systems intact. Representing a text or a message with the help of polynomial and applying the not distributive condition, it would be difficult to hack the information.

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* $\mathbb{Z}_n$ *to* $\mathbb{Z}_m$, 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, *Residue Matrix and not Distributive Lattice*, IJMTT, 65(8)(2019), 1-3.