Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 2, July-2017, ISSN 2230-7540

An Analysis upon Basic Fundamental Application of Ring Theory

Vijay Singh Digamber Gaikwad*

Assistant Professor

Abstract – Ring theory is one of the branches of the abstract algebra that has been broadly used in images. However, ring theory has not been very related with image segmentation. In this paper, we propose a new index of similarity among images using __ rings and the entropy function. This new index was applied as a new stopping criterion to the Mean Shift Iterative Algorithm with the goal to reach a better segmentation. An analysis on the performance of the algorithm with this new stopping criterion is carried out. Whereas ring theory and category theory initially followed different directions it turned out in the 1970s – that the study of functor categories also reveals new aspects for module theory.

In our presentation many of the results obtained this way are achieved by purely module theoretic methods avoiding the detour via abstract category theory.

----------♦----------

INTRODUCTION

In mathematics, a ring is an algebraic structure consisting of a set together with two binary operations usually called addition and multiplication, where the set is an abelian group under addition (called the additive group of the ring) and a monoid under multiplication such that multiplication distributes over addition. In other words the ring axioms require that addition is commutative, addition and multiplication are associative, multiplication distributes over addition, each element in the set has an additive inverse, and there exists an additive identity. One of the most common examples of a ring is the set of integers endowed with its natural operations of addition and multiplication. Certain variations of the definition of a ring are sometimes employed, and these are outlined later in the article.

The branch of mathematics that studies rings is known as ring theory. Ring theorists study properties common to both familiar mathematical structures such as integers and polynomials, and to the many less well-known mathematical structures that also satisfy the axioms of ring theory. The ubiquity of rings makes them a central organizing principle of contemporary mathematics.

Ring theory may be used to understand fundamental physical laws, such as those underlying special relativity and symmetry phenomena in molecular chemistry.

The concept of a ring first arose from attempts to prove Fermat's last theorem, starting with Richard Dedekind in the 1880s. After contributions from other fields, mainly number theory, the ring notion was generalized and firmly established during the 1920s by Emmy Noether and Wolfgang Krull. Modern ring theory—a very active mathematical discipline—studies rings in their own right. To explore rings, mathematicians have devised various notions to break rings into smaller, better-understandable pieces, such as ideals, quotient rings and simple rings. In addition to these abstract properties, ring theorists also make various distinctions between the theory of commutative rings and noncommutative rings—the former belonging to algebraic number theory and algebraic geometry. A particularly rich theory has been developed for a certain special class of commutative rings, known as fields, which lies within the realm of field theory. Likewise, the corresponding theory for noncommutative rings, that of noncommutative division rings, constitutes an active research interest for noncommutative ring theorists. Since the discovery of a mysterious connection between noncommutative ring theory and geometry during the 1980s by Alain Connes, noncommutative geometry has become a particularly active discipline in ring theory.

A ring will be defined as an abstract structure with a commutative addition, and a multiplication which may or may not be commutative. This distinction yields two quite different theories: the theory of respectively commutative or non-commutative rings. These notes are mainly concerned about commutative rings.

Non-commutative rings have been an object of systematic study only quite recently, during the 20th century. Commutative rings on the contrary have appeared though in a hidden way much before, and as many theories, it all goes back to Fermat's Last Theorem.

In 1847, the mathematician Lam´e announced a solution of Fermat's Last Theorem, but Liouville noticed that the proof depended on a unique decomposition into primes, which he thought was unlikely to be true. Though Cauchy supported Lam´e, Kummer was the one who finally published an example in 1844 to show that the uniqueness of prime decompositions failed. Two years later, he restored the uniqueness by introducing what he called "ideal complex numbers" (today, simply "ideals") and used it to prove Fermat's Last Theorem for all n < 100 except n = 37, 59, 67 and 74.

It is Dedekind who extracted the important properties of "ideal numbers", defined an "ideal" by its modern properties: namely that of being a subgroup which is closed under multiplication by any ring element. He further introduced prime ideals as a generalization of prime numbers. Note that today we still use the terminology "Dedekind rings" to describe rings which have in particular a good behavior with respect to factorization of prime ideals. In 1882, an important paper by Dedekind and Weber developed the theory of rings of polynomials.

At this stage, both rings of polynomials and rings of numbers (rings appearing in the context of Fermat's Last Theorem, such as what we call now the Gaussian integers) were being studied. But it was separately, and no one made connection between these two topics. Dedekind also introduced the term "field" (K¨orper) for a commutative ring in which every non-zero element has a multiplicative inverse but the word "ring" is due to Hilbert, who, motivated by studying invariant theory, studied ideals in polynomial rings proving his famous "Basis Theorem" in 1893.

It will take another 30 years and the work of Emmy Noether and Krull to see the development of axioms for rings. Emmy Noether, about 1921, is the one who made the important step of bringing the two theories of rings of polynomials and rings of numbers under a single theory of abstract commutative rings.

In contrast to commutative ring theory, which grew from number theory, non-commutative ring theory developed from an idea of Hamilton, who attempted to generalize the complex numbers as a two dimensional algebra over the reals to a three dimensional algebra. Hamilton, who introduced the idea of a vector space, found inspiration in 1843, when he understood that the generalization was not to three dimensions but to four dimensions and that the price to pay was to give up the commutativity of multiplication. The quaternion algebra, as Hamilton called it, launched non-commutative ring theory.

A *ring* is a set A with two binary operations satisfying the rules given below. Usually one binary operation is denoted `+' and called \addition," and the other is denoted by juxtaposition and is called \multiplication." The rules required of these operations are:

1) A is an abelian group under the operation + (identity denoted 0 and inverse of x denoted $-x$);

2) A is a monoid under the operation of multiplication (i.e., multiplication is associative and there is a two-sided identity usually denoted 1);

3) the distributive laws

$(x + y)z = xy + xz$

$x(y + z) = xy + xz$

hold for all x, y, and $z \in A$.

Sometimes one does not require that a ring have a multiplicative identity. The word ring may also be used for a system satisfying just conditions (1) and (3) (i.e., where the associative law for multiplication may fail and for which there is no multiplicative identity.) Lie rings are examples of non-associative rings without identities. Almost all interesting associative rings do have identities.

If 1 = 0, then the ring consists of one element 0; otherwise $1 \neq 0$. In many theorems, it is necessary to specify that rings under consideration are not trivial, i.e. that $1 \neq 0$, but often that hypothesis will not be stated explicitly.

If the multiplicative operation is commutative, we call the ring commutative. *Commutative Algebra* is the study of commutative rings and related structures. It is closely related to algebraic number theory and algebraic geometry.

If A is a ring, an element $x \in A$ is called a *unit* if it has a two-sided inverse y, i.e. $xy = yx = 1$. Clearly the inverse of a unit is also a unit, and it is not hard to see that the product of two units is a unit. Thus, the set $U(A)$ of all units in A is a group under multiplication. ($U(A)$ is also commonly denoted A^*.) If every nonzero element of A is a unit, then A is called a *division ring* (also a skew field.) A commutative division ring is called a field.

Examples:

1. Z is a commutative ring. $U(\mathbf{Z}) = \{1, -1\}$

2. The group $\mathbb{Z}/n\mathbb{Z}$ becomes a commutative ring where multiplication is multiplication mod *n*. $U(\mathbb{Z}/n\mathbb{Z})$ consists of all cosets $i + n\mathbb{Z}$ where *i* is relatively prime to *n*.

3. Let *F* be a field, e.g., *F* = R or C. Let $M_n(F)$ denote the set of *n* by *n* matrices with entries in *F*. Add matrices by adding corresponding entries. Multiply matrices by the usual rule for matrix multiplication. The result is a non-commutative ring. $U(M_n(F)) = Gl(n, F)$ = the group of invertible *n* by *n* matrices.

4. Let *M* be any abelian group, and let End(M) denote the set of endomorphisms of *M* into itself. For $f, g \in \mathrm{End}(M)$, define addition by $(f + g)(m) = f(m) + g(m),$ and define multiplication as composition of functions. (Note: If *M* were not abelian we could still define composition because the composition of two endomorphisms is an endomorphism. However, it would not necessarily be true that the sum of two endomorphisms would be an endomorphism. Check this for yourself.)

If *A* is a ring, a subset *B* of *A* is called a *subring* if it is a subgroup under addition, closed under multiplication, and contains the identity. (If *A* or *B* does not have an identity, the third requirement would be dropped.)

Examples:

1) $\mathbb{Z}$ does not have any proper subrings.

2) The set of all diagonal matrices is a subring of $M_n(F)$.

3) The set of all *n* by *n* matrices which are zero in the last row and the last column is closed under addition and multiplication, and in fact it is a ring in its own right (isomorphic to $M_{n-1}(F)$.) However, it is not a subring since its identity does not agree with the identity of the over ring $M_n(F)$.

A function $f : A \to B$ where *A* and *B* are rings is called a homomorphism of rings if it is a homomorphism of additive groups, it preserves products: $f(xy) = f(x)f(y)$ for all $x, y \in A,$ and finally it preserves the identity: $f(1) = 1.$

Examples: The canonical epimorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism. However, the inclusion of $M_{n-1}(F)$ in $M_n(F)$ as suggested in example 3) above is not a ring homomorphism.

A subset a is called a *left ideal* of *A* if it is an additive subgroup and in addition $ax \in \mathfrak{a}$ whenever $a \in A$ and $x \in \mathfrak{a}.$ If we require instead that $xa \in \mathfrak{a},$ then *a* is called a *right* ideal. Finally, $\mathfrak{a}$ is called a *two-sided* ideal if it is both a left ideal and a right ideal. Of course, for a commutative ring all these notions are the same.

BASIC NOTIONS

A *ring* is defined as a non-empty set *R* with two compositions $+, \cdot : R \times R \to R$ with the properties:

(i) $(R, +)$ is an abelian group (zero element 0);

(ii) $(R, \cdot)$ is a semigroup;

(iii) for all $a, b, c \in R$ the distributivity laws are valid:

$$(a + b)c = ac + bc,\ a(b + c) = ab + ac.$$

The ring *R* is called *commutative* if $(R, \cdot)$ is a commutative semigroup, i.e. if $ab = ba$ for all $a, b \in R.$ In case the composition is not necessarily associative we will talk about a *non-associative* ring.

An element $e \in R$ is a *left unit* if $ea = a$ for all $a \in R.$ Similarly a *right unit* is defined. An element which is both a left and right unit is called a unit (also unity, identity) of R.

In the sequel *R* will always denote a ring. In this chapter we will not generally demand the existence of a unit in *R* but assume $R \neq \{0\}.$

The symbol 0 will also denote the subset $\{0\} \subset R.$

RINGS, IDEALS AND HOMOMORPHISMS

Definition 1. A ring *R* is an abelian group with a multiplication operation $(a, b) \mapsto ab$ which is associative, and satisfies the distributive laws

$$a(b + c) = ab + ab,\ (a + b)c = ac + bc$$

with identity element 1.

There is a group structure with the addition operation, but not necessarily with the multiplication operation. Thus an element of a ring may or may not be invertible with respect to the multiplication operation. Here is the terminology used.

Definition 2. Let a,6 be in a ring *R*. If $a \neq 0$ and $b \neq 0$ but $ab = 0,$ then we say that *a* and *b* are zero divisors. If $ab = ba = 1$, we say that *a* is a unit or that *a* is invertible.

While the addition operation is commutative, it may or not be the case with the multiplication operation.

Definition 3. Let *R* be ring. If $ab = ba$ for any *a, b* in *R*, then *R* is said to be commutative.

Here are the definitions of two particular kinds of rings where the multiplication operation behaves well.

Definition 4. An integral domain is a commutative ring with no zero divisor. A division ring or skew field is a ring in which every non-zero element *a* has an inverse a^{-1}.

Let us give two more definitions and then we will discuss several examples.

Definition 5. The characteristic of a ring *R*, denoted by char#, is the smallest positive integer such that

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n\text{times}} = 0.$$

We can also extract smaller rings from a given ring.

Definition 6. A subring of a ring *R* is a subset 5 of *R* that forms a ring under the operations of addition and multiplication defined in *R.*

Definition 7. Let *R. S* be two rings. A map $f : R \to S$ satisfying

1. $f(a+b) = f(a) + f(b)$ (this is thus a group homomorphism)
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$ for *a,b* G *R* is called ring homomorphism.

The notion of "ideal number" was introduced by the mathematician Kum- mer, as being some special "numbers" (well, nowadays we call them groups) having the property of unique factorization, even when considered over more general rings than $\mathbb{Z}$ (a bit of algebraic number theory would be good to make this more precise). Today only the name "ideal" is left, and here is what it gives in modern terminology:

Definition 8. Let $\mathcal{I}$ be a subset of a ring *R.* Then an additive subgroup of *R* having the property that $ra \in \mathcal{I}$ for $a \in \mathcal{I},\ r \in R$ is called a left ideal of *R.* If instead we have $ar \in \mathcal{I}$ for $a \in \mathcal{I},\ r \in R$

we say that we have a right ideal of *R.* If an ideal happens to be both a right and a left ideal, then we call it a two-sided ideal of #, or simply an ideal of *R.*

Of course, for any ring #, both *R* and $\{0\}$ are ideals. We thus introduce some terminology to precise whether we consider these two trivial ideals.

Definition 9. We say that an ideal $\mathcal{I}$ of *R* is proper if $\mathcal{I} \neq R.$ We say that is it non-trivial if $\mathcal{I} \neq R$ and $\mathcal{I} \neq 0.$

If $f : R \to S$ is a ring homomorphism, we define the kernel of f in the most natural way:

$$\mathrm{Ker} f = \{r \in R,\ f(r) = 0\}.$$

Since a ring homomorphism is in particular a group homomorphism, we already know that f is injective if and only if $\mathrm{Ker} f = \{0\}.$ It is easy to check that $\mathrm{Ker} f$ is a proper two-sided ideal:

- $\mathrm{Ker} f$ is an additive subgroup of *R.*
- Take $a \in \mathrm{Ker} f$ and $r \in R.$ Then $f(ra) = f(r)f(a) = 0$ and $f(ar) = f(a)f(r) = 0$ showing that ra and *ar* are in $\mathrm{Ker} f.$
- Then $\mathrm{Ker} f$ has to be proper (that is, $\mathrm{Ker} f \neq R$), since by definition. $f(1) = 1$

THE CHINESE REMAINDER THEOREM

The multiplication of additive subgroups of *A* satisfies the associative and distributive laws:

$$\begin{aligned} \mathfrak{a}(\mathfrak{bc}) &= (\mathfrak{ab})\mathfrak{c} \\ \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) &= \mathfrak{ac} + \mathfrak{ac} \\ (\mathfrak{a} + \mathfrak{b})\mathfrak{c} &= \mathfrak{ac} + \mathfrak{bc}. \end{aligned}$$

Moreover, it is not hard to see that if **a** is a left ideal then **ab** is also a left ideal. Similarly, if **b** is a right ideal then **ab** is a right ideal. In particular, if **a** is a left ideal and **b** is a right ideal, then **ab** is a two-sided ideal.

Note that in the above formulas, we have used the sum **a + b** of two additive subgroups of A. (Since as additive group, A is abelian, the subgroup **a + b** in fact consists of all sums $x+y$ where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}.$) If **a** and **b** are left (right, two-sided) ideals then **a + b** is a left (right, two-sided) ideal, the smallest such containing *a* and **b.** Similarly, we can form the

intersection $\mathfrak{a} \cap \mathfrak{b}$ of 2 left (right, two-sided) ideals, and the result is again a left (right, two-sided) ideal. More generally, any arbitrary intersection of left (right, two-sided) ideals is again a left (right, two-sided) ideal: in fact the largest left (right, two-sided) ideal contained in all the ideals.

Note that if **a** and **b** are two-sided ideals, then so is **ab** and in addition $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Let *A* and *B* be rings. We can form the additive group $A \times B$, and we can define a multiplication operation on it by

$$(a, b)(a', b') = (aa', bb').$$

It is straightforward to check that $A \times B$ becomes a ring with this operation. It is called the *direct* product ring. Consider the subgroup $A \times \{0\} = \{(a, 0) \mid a \in A\}$. A simple calculation shows that it is closed under either left or right multiplication by arbitrary elements of $A \times B$ so it is a two-sided ideal. In fact, it is the kernel of the map $A \times B \to B$ defined by $(a, b) \mapsto b$. (That map is clearly a ring epimorphism.) Similarly, $\{0\} \times B$ is a two-sided ideal in A, the kernel of the projection $A \times B \to A$. The Chinese Remainder theorem gives us a way of dissecting a ring into a direct product under appropriate circumstances.

THEOREM. *(Chinese Remainder Theorem) Let A be a ring, and suppose* $\mathfrak{a}_i, i = 1, 2, \ldots, n$ *are two-sided ideals in A such that*

$$\mathfrak{a}_i + \mathfrak{a}_j = A \quad \text{for } i \neq j.$$

Then

$$A/\mathfrak{a} \cong \prod_i A/\mathfrak{a}_i \text{ where } \mathfrak{a} = \cap_i \mathfrak{a}_i.$$

Note: The property $\mathfrak{a} + \mathfrak{b} = A$ for two sided ideals is called *comaximality.*

Proof. Let $p_i : A \to A/\mathfrak{a}_i$ be the canonical epimorphism, and define $p : A \to \prod A/\mathfrak{a}_i$ by $p(a) = (p_1(a), \ldots, p_n(a))$. Clearly, p is a ring homomorphism, and $\operatorname{Ker} p = \{a \mid p_i(a) = 0 \text{ for } i = 1, \ldots, n\} = \cap \mathfrak{a}_i$.

The theorem will follow from the first isomorphism theorem if we can show that *p* is an epimorphism. Let d_i be the element $(0, \ldots, 1, \ldots, 0)$ which is 0 at all components except the ith where it is one.

It clearly suffices to show that $d_i = p(a_i)$ for some $a_i \in A$ for each $i = 1, \ldots, n.$ (For, in that case $p(aa_i) = p(a)p(a_i) = p(a)d_i = p_i(a)$ and clearly the direct product is generated by elements of this form.)

RING THEORY IN THE SEGMENTATION OF DIGITAL IMAGES

Many techniques and algorithms have been proposed for digital image segmentation. Traditional segmentation such as thresholding, histograms or other conventional operations are rigid methods. Automation of these classical approximations is difficult due to the complexity in shape and variability within each individual object in the image.

The mean shift is a non-parametric procedure that has demonstrated to be an extremely versatile tool for feature analysis. It can provide reliable solutions for many computer vision tasks. Mean shift method was proposed in 1975 by Fukunaga and Hostetler. It was largely forgotten until Cheng's paper retook interest on it. Segmentation by means of the Mean Shift Method carries out as a first step a smoothing filter before segmentation is performed.

Entropy is an essential function in information theory and this has had a special uses for images data, e.g., restoring images, detecting contours, segmenting images and many other applications. However, in the field of images the range of properties of this function could be increased if the images are defined in $\mathbb{Z}_n$ rings. The inclusion of the ring theory to the spatial analysis is achieved considering images as a matrix in which the elements belong to the cyclic ring $\mathbb{Z}_n$. From this point of view, the images present cyclical properties associated to gray level values.

Ring Theory has been well-used in cryptography and many others computer vision tasks. The inclusion of ring theory to the spatial analysis of digital images, it is achieved considering the image like a matrix in which the elements belong to finite cyclic ring $\mathbb{Z}_n$. The ring theory for the Mean Shift Iterative Algorithm was employed by defining images in a ring $\mathbb{Z}_n$. A good performance of this algorithm was achieved. Therefore, the use of the ring theory could be a good structure when one desire to compare images, due to that the digital images present cyclical properties associated with the pixel values. This property will allow to increase or to diminish the difference among pixels values, and will make possible to find the edges in the analyzed images.

In this paper, a new similarity index among images is defined, and some interesting properties based on this index are proposed. We compare also the instability of the iterative mean shift algorithm (MSHi) by using this new stopping criterion . Furthermore, we make an extension, and we expand the theoretical aspects by studying in depth the cyclical properties of rings applied to images. For this purpose, some issues are pointed out below:

- Revision of the mean shift theory.
- Important elements of the ring $G_{k\times m}(\mathbb{Z}_n)(+,\cdot)$ are given: neutral, unitary, and inverse. In particular, the inverse element was used so much to the theoretical proofs as well as practical aspects.
- Explanation of strong equivalent images by using histograms.
- Definition of equivalence classes.
- Quotient space. Definition and existence.
- Natural Entropy Distance (NED) definition.
- Configuration of the algorithm MSHi with the NED distance.

REFERENCES

Berrick, A. J. and Keating, M. E. (2000). An Introduction to Rings and Modules with K-Theory in View. Cambridge, England: Cambridge University Press.

D. Comaniciu, P. Meer (1974). “Mean Shift: A Robust Approach toward Feature Space Analysis”, IEEE Trans. on Pattern Analysis and Machine Intelligence Ph. D. Thesis, New York University, 24 (5).

D. Dominguez and R. Rodriguez (2011). “Convergence of the Mean Shift using the Infinity Norm in Image Segmentation”, International Journal of Pattern Recognition Research, 1, pp. 3-4.

D. I. Comaniciu (2000). “Nonparametric Robust Method for Computer Vision”, Ph. D. Thesis, Rutgers, The State University of New Jersey.

D. S. Dummit and R. M. Foote (2009). Abstract Algebra, Wiley.

Huynh, D.V., Wisbauer, R. (2000). A characterization of locally artinian modules, J.Algebra 132, pp. 287-293.

K. Fukunaga and L. D. Hostetler (1975). “The Estimation of the Gradient of a Density Function”, IEEE Trans. on Information Theory, IT-21(1) pp. 32-40.

Lang, Serge (2002). *Algebra*, Graduate Texts in Mathematics, 211 (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556

Lang, Serge (2005). *Undergraduate Algebra* (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-22025-3.

M. Artin (2002). Algebra, Prentice Hall of India.

Pinter-Lucke, James (2007). "Commutativity conditions for rings: 1950–2005", *Expositiones Mathematicae* 25 (2): pp. 165–174 doi:10.1016/j.exmath.2006.07.001, ISSN 0723-0869

R. Rodriguez, E. Torres, and J. H. Sossa (2011). “Image Segmentation based on an Iterative Computation of the Mean Shift Filtering for different values of window sizes”, International Journal of Imaging and Robotics, 6, pp. 1-19.

S. Luthar and I. B. S. Passi (2004). Algebra, Vol 1-4, Narosa, 1997-2004.

T. Grenier, C. Revol-Muller, F. Davignon, and G. Gimenez (2006). “Hybrid Approach for Multiparametric Mean Shift Filtering”, IEEE Image Processing, International Conference, Atlanta, GA, 17(8), pp. 8-11.

Wisbauer, R. (2001). Semisimple and pure semisimple functor rings, Comm.Algebra 18, pp. 2343-2354.

Wisbauer, R. (2002). Local-global results for modules over algebras and Azumaya rings, J.Algebra, pp. 135, pp. 440–455.

Wisbauer, R. (2004). On modules with the Kulikov property and pure semisimple modules and rings, J.Pure Appl.Algebra 70, pp. 315-320.

Wright, M. H. (2005). Certain uniform modules over serial rings are uniserial, Comm. Algebra 17, pp. 441-469.

Y. Cheng (1995). “Mean Shift, Mode Seeking, and Clustering”, iEEE Trans. On Pattern Analysis and Machine Intelligence, Ph. D. Thesis, New York University, 17 (8), pp. 790-799.

Y. Garcés, E. Torres, O. Pereira, C. Perez, R. Rodriguez (2013). Stopping Criterion for the Mean Shift Iterative Algorithm, Springer,

Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, Lecture Notes in Computer Science, Vol. 8258, pp. 383 390.

Corresponding Author

Vijay Singh Digamber Gaikwad*

Assistant Professor

E-Mail – **vijaysinghgaikwad0@gmail.com**