ISSN 2959-6157

A Survey on Ring Theory for its Mathematical Foundation and Applications

Huiran Zheng

Abstract:

The origin of the ring theory can be dated to the early 19*th* century. With the rapid development of technology, more and more complex engineering problems and computer problems need to obtain support and results from more basic mathematics theory. Hence, based on this demand, the researcher discovered that ring theory is a very noteworthy math theory for solving the complicated problems above. This paper investigated the ring theory and related articles based on number theory and corresponding applications, which produces and results in a literature review in this particular direction.

Keywords: ring theory, algebra, application

Introduction

A lot of complicated technologies such as artificial intelligence, large complex modelling chip design, and algorithms inside the chip need to use ring theory. For example, Convolutional Neural Network (CNN) is a Deep Learning algorithm designed for working with images and video. Previous research showed that using a residue number system on the hardware implementation of the convolution layer could reduce at most 37.78% cost on hardware compared to complement implementation. (Valueva, Nagornov, Lyakhov, Valuev, and Chervyakov (2020)) For this reason, scholars need to develop theories to satisfy the demands of the development of artificial intelligence. Ring theory can be divided into two parts: commutative and non-commutative. Commutative ring theory began with algebraic number theory, algebraic geometry, and invariant theory. In commutative ring theory, scholars usually focus on rings that have commutative low for multiplication.

Non-commutative ring theory is related to complex numbers and it was started from the theory of hyper-complex number systems. (Kleiner (1998))

We have thoroughly searched most of the related articles and recently published papers on ring theory, but there is not any relatively complete and inclusive literature review that uses ring theory to relate number theory and some of its applications. Due to this reason mentioned above, this paper fills the gap of one of the small directions literature review based on the ring theory. In section 2, this paper will introduce some important basic knowledge about ring theory and number theory, which can establish the relationship between ring theory and number theory, followed by the discussion about some applications of ring theory in number theory such as using ring theory to proving elementary number theory question in Section 3. The final section concludes the main content of the article and proposed potential research and explores the potential research area.

Literature Review

Definition, Origin and Development of Ring Theory

Ring theory can be divided into commutative ring theory and non-commutative ring theory. Commutative ring theory originated in algebraic number theory, algebraic geometry, and invariant theory in the early 19*th* century. Non-commutative ring theory originates from extending the complex numbers to various hypercomplex number systems.

The representation of curves by equations is the basic idea of algebraic geometry.

The key that made algebraic geometry feasible was the solution of equations and the improvement of notation in the 16*th* century by Fermat and Descartes who are the two founders of algebraic geometry (Stillwell and Stillwell (1989)). AW Knapp et al. proposed that number theory had a great advance from 1800 to 1840. Euclid, Diophantus, Fermat, Euler, Lagrange, and Legendre made a lot of contributions in that period. Fermat's Last Theorem, reciprocity laws, and binary quadratic forms occurred in that period which also influenced the kind of algebraic number theory we learn today (Knapp (2007)). An invariant is a property of an object in mathematics that remains unchanged after a certain type of operation or transformation. Israel Kleiner et al. proposed that invariant theory has roots in both number theory and geometry. Between the 1860s and 1880s, invariant theory became a major branch of algebra followed by it becoming an independent field of study in the mid-nineteenth century (Kleiner (1998)). Hamilton (1843) proposed a simple example which is the quaternions. Non-commutative ring theory originated from this simple example.

Rings are algebraic structures closed under addition, subtraction, and multiplication. Malcev (n.d.) who is one of the founders of ring theory is an author of the Levy-Malcev theorem for Lie algebras which made far-reaching contributions to the theory of Lie groups. It is also worth mentioning that his teacher Kolmogorov (1900) began a new branch of mathematics by the locality (compactness) theorem in mathematical logic.

Shirshov (1962) proposed a lot of theories about free Lie algebras, I-algebras, and Jordan and alternative algebras. Those theories had a profound influence on the development of algebra. Harada proposed extension and lifting properties for modules and considered two new classes of Artinian rings which contain QF-rings and Nakayama rings in the early 1980s. His work first considered the extending property for simple submodules and the lifting property for maximal submodules of modules with completely indecomposable decompositions (Harada (1979)).

Israel Kleiner et al. proposed that both commutative and noncommutative rings and their ideals were well-established in the first decade of the 20*th* century (Kleiner (1996)). Fraenkel (1914) gave the first abstract definition of a ring in 1914. Cohn (2012) proposed that ring first just meant a “ring of algebraic integers” before Fraenkel’s work. Noether (1923) discovered the relationship between chains of prime ideal and dimensions of algebraic varieties followed by Noether (n.d.) abstract commutative rings with the ascending chain condition in 1927 and Artin (1927) generalized Wedderburn (1908) structure theorems in 1927. Noether and Artin made the abstract ring concept in the centre of algebra. In 1928, Krull (2020) developed Noether’s idea about the dimension as a powerful tool related to a kind of commutative ring. The rings involved in this definition are known as Noetherian rings and the dimensions of rings are named Krull dimension today. Rowen (2012) proposed that a semi-simple Artinian ring is the Sun of the solar system of ring theory. Jacobson (1956) proposed his density theorem which is the generalization of the essence of the Wedderburn-Artin theory began the structure theory of rings. Every module is a direct sum of simple modules which indicate that scholars can study module in terms of simple modules and Artinian Noetherian modules are the best modules by some of their properties. Hence, simi-simple Artinian rings are important (Rowen (2012)).

Directions of Research

In theory, ring theory is basic to learning algebraic geometry which is one of the recent popular mathematical areas. Cimprič (2012) et al. proposed the extending of the Artin-Lang theorem and Krivine-Stengle Stellensätze from R to *Mn*(*R*). This theory is not Morita equivalent to classical real algebraic geometry. Lezama and Latorre (2017) proposed the semi-graded rings in 2017, which is a new type of non-commutative rings.

The semi-graded rings extend graded rings and skew Poincaré-Birkhoff-Witt (PBW) extensions. In addition, they prove some elementary properties of the generalized Hilbert series, Hilbert polynomial, and Gelfand-Kirillov dimension. Jason Bell et al. proposed an answer to whether the Poisson Dixmier-Moeglin equivalence holds for any complex affine Poisson algebra in 2017. They gave this answer using techniques from differential-algebraic geometry and model theory (Bell, Launois, Sánchez, and Moosa (2017)). Yunfeng Jiang and Yang Zhang et.al proposed a novel efficient method to count the number of solutions of Bethe ansatz equations based on the Gröbner basis and quotient ring in 2018. Also, they developed an analytical approach which is based on a companion matrix and revisited the completeness problem of Bethe ansatz of the Heisenberg spin chain to show the power of this method (Jiang and Zhang (2018)). Khan et al. proposed the proof of an analogue of the Morel-Voevodsky localization theorem over spectral algebraic spaces in 2019. Also, they deduced a corollary which called “derived nilpotent-invariance” (Khan (2019)). Alain Connes et al. proposed a development in the affine case for general Segal’s Γ-ring in 2021, which unifies two approaches for a geometry under Spec *Z*. To be more specific, the spectrum of an S-algebra is in general a Grothendieck site and it is the natural domain for cyclic homology and for homological algebra (Connes and Consani (2021)). Blechschmidt (2021) et al. proposed the use of the internal language of toposes in algebraic geometry.

This method can give simpler definitions and more conceptual proofs in algebraic geometry. Also, due to the recent development of some abstractions in algebra and the special properties of rings. Ring theory has become popular in cryptography. Vadim Lyubashevsky

et al. proposed an algebraic variant of LWE called ring-LWE and provided that it too enjoys very strong hardness guarantees in 2010. Ring-LWE can be used to resolve an open question which is introducing an algebraic variant of LWE called ring-LWE, and proving that it too enjoys very strong hardness guarantees. Ring-LWE can optimize some applications of LWE to improve efficiency. Hence, the algebraic structure of ring-LWE might be able to lead to new cryptographic applications (Lyubashevsky, Peikert, and Regev (2010)). Areej M. Abduldaim et al. skew π-Armendariz rings which is an algebraic structure and they used these rings to design a neoteric algorithm for zero-knowledge proof in 2017. Also, they considered the security of algebraic cryptography systems which are based on non-commutative rings to ensure that it is impossible to solve the cryptography system in a practical amount of time (Abduldaim and Al-Saidi (2017)) Shahriar Ebrahimi et al. proposed InvRBLWE which is an optimized variant for binary learning with errors over the ring (Ring-LWE) scheme in 2019. InvRBLWE has been proven can be secure against quantum attacks and can improve the efficiency of hardware implementations.

They also proposed two architectures for IneRBLWE which are scalable regarding security levels. Two different ASIC implementations show improvement in speed, area, power, and energy. Moreover, they are the first to implement LWE-based cryptosystems on the ASIC platform (Ebrahimi, Bayat-Sarmadi, and Mosanaei-Boorani (2019)). Shahriar Ebrahimi proposed a masking countermeasure against a differential power analysis (DPA) attack on lightweight implementations of binary Ring-LWE on hardware in 2020. The results show that DPA-secure implementations have lower than 14% performance overhead and still satisfy practical on resource-constrained devices. Besides, the results of experiments of FPGA implementation have more than 99% and 81% improvement in speed and efficiency compared to previous work (Ebrahimi and Bayat-Sarmadi (2020)). Zheng Zhiyong et al.

proposed ϕ-cyclic code in 2021, which may be regarded as a general form of the ordinary cyclic code and applications of extending two public key encryption schemes. One of these is the NtRu public key cryptosystem which is based on polynomial ring theory. Another one is McEliece and Niederriter's cryptosystem which is based on error-correcting theory.

Those results provide a more general construction of NTRU based on ideal matrices and q-ary lattice theory (Zheng, Huang, Xu, and Tian (2021)).

In addition, ring theory also has a high relationship with linear algebra, such as the Laplacian matrix which can provide a computationally tractable solution to the graph partitioning problem. Pirzada, Rather, and Chishti (2021) proposed one method of obtaining the distance Laplacian spectrum of the zero divisor graphs $\Gamma(Zn)$ for different values of n. Finally, it can determine that n for which zero divisor graph $\Gamma(Zn)$ is distance Laplacian integral. Chattopadhyay, Patra, and Sahoo (2020) et al. proved that $\Gamma(Zpt$) is Laplacian integral for every prime p and positive integer $t \geq 2$ in 2020. Pirzada et al.

found the signless Laplacian spectrum of the zero divisor graphs $\Gamma(Zn)$ for various values of n in 2021. Also, they characterize n for which zero divisor graph $\Gamma(Zn)$ are signless Laplacian integral (Pirzada, Rather, Shaban, and Merajuddin (2021)). Sarathy et al. proposed the structure formation of the annihilator monic prime graph of commutative rings and colour-based energy of the annihilator monic prime graph which is called colour distance signless Laplacian energy in 2023. They also provided some applications of

color-based energy (Sarathy and Sankar (2023)). Shouqiang Shen et al. proposed the case that whenever n is an even number or an odd prime power, $G(Zn)$ would be the Laplacian integral in 2023. They also characterize n that algebraic connectivity of $G(Zn)$ coincides with the vertex connectivity (Shen, Liu, and Jin (2023)). Mohd Shariq et al. obtained the Laplacian spectrum of the weakly zero-divisor graph Γ(R) of the ring *Zn* in 2023. Also, they proved that $W\Gamma(Zn)$ in Laplacian integral for arbitrary n (Shariq, Mathil, and Kumar (2023)).

Application of Ring Theory

Due to ring theory occupying the central role in abstract and the rapid development of computer science, there are more and more applications of ring theory in computer vision especially in image segmentation. Garcés, Torres, Pereira, and Rodríguez (2014) et al. proposed that a new index of similarity among images uses *Zn* rings and the entropy function in 2014. The analysis of the performance of the algorithm proved that the new index is a suitable tool for comparing images. Adhami and Brewer (1989) proposed a new ring theory-based algorithm and stopping criterion for image segmentation. This algorithm and stopping criterion using finite cyclic rings and matrices in Ring Theory can perform high-quality image segmentation for images that can be used in computer vision. Aditya, Zulfikar, and Manik (2015) proposed an application program to test division rings and fields. This program can test algebraic structures more than manual ones and has accurate results. Torres, Rodriguez, Garcés, and Pereira (n.d.) et al. proposed a new method for edge detection in obtained images from the Mean Shift iterative algorithm in 2015. They introduced the Mean Shift Gradient Operator which uses ring units for edge detection and explained the importance of ring theory. Adhami and Brewer (1989) proposed a 2 × 3 convolution mask which is a cyclic ring of integers modulo 7. This mask can detect the edges of digital images.

The residue number system is a numeral system representing integers by their values modulo several pairwise coprime integers called the moduli which has a high relationship with ring theory and number theory. Residue number system can be used to improve the system or reduce cost. Cardarilli, Nannarelli, and Re (2007) proposed that the residue number theory (RNS) uses less power than the Two's Complement System (TCS) counterpart. This result indicated that the use of residue number theory can reduce the cost of power consumption. Also, Valueva et al. (2020) proposed the use of RNS in the hardware part of convolutional neural network architecture to implement the convolutional layer of the neural network. The result of this application showed that using RNS can reduce hardware cost by 7.86% to 37.78% compared to the two's complement implementation. Chervyakov proposed a framework of the convolutional neural network constructed with a residue number system for delay minimization. Using this method could accelerate the work of the device by 37.4% as compared to using a binary number system and by 18.5% as compared to using a known residue number system realization (Chervyakov, Lyakhov, and Valueva (2017)).

The applications of ring theory in coding theory and cryptography have grown significantly. Muthuraj and Gandhi (n.d.) proposed an application of HX ring theory in homomorphic encryption which is called HX homomorphic encryption techniques. Using algorithms that run a sequence of mathematical operations can change the value of the numbers in a foreseeable way which can encrypt the information. Galdino, Borges, Ayala-Rincón, et al. (2021) proposed a PVS development of relevant results of the ring theory which provides the required elements to formalize important algebraic theorems.

Hence, the paper proposed the formalization of the general algebraic-theoretical version of the Chinese remainder theorem (CRT) for the theory of rings. Grigoriev proposed a homomorphic public-key cryptosystem over groups and rings. In addition, this homomorphic cryptosystem is designed for the first time over finite commutative rings (Grigoriev and Ponomarenko (2003)).

Besides, ring theory also has several other applications. Awange, Fukuda, Takemoto, and Grafarend (2005) proposed several examples of geodetic problems solved algebraically. Those examples indicate that one of the advantages of algebraic approaches is that they provide exact solutions to problems requiring closed-form approaches. Yichao He et al. proposed two evolution operators which are the global exploration operator and the local development operator and a new algorithm called the Ring Theory-Based Evolutionary Algorithm in 2019. Using those operators and algorithms can solve the combinatorial optimization problem which also indicates using algebraic theory to design evolutionary algorithms is feasible and effective (He, Wang, and Gao (2019)). Ahmed et al. proposed a new hybrid meta-heuristic FS model based on a well-known meta-heuristic Harmony Search (HS) algorithm and a Ring Theory-based Evolutionary Algorithm (RTEA) in 2020, which was named Ring Theory-based Harmony Search (RTHS). Several results have proved the effectiveness of RTHS in solving Feature Selection problems.

Feature Selection is a significant pre-processing step in the fields of machine learning and data mining, which has a major impact on the performance of the corresponding learning models (Ahmed, Ghosh, Singh, Geem, and Sarkar (2020)).

Discussions

Mathematical Foundation

Ring theory has been developed for many applications in various research directions, among which we can selectively have some of them as the proof process as part of our discussion. Here we select one of the most important progress to show our understanding, followed by the practical applications of ring theory. Snake Lemma is a simple and useful tool in homological algebra. It is used to construct long exact sequences and is valid in all Abelian categories (Lemmermeyer (2011)). We went through the whole process as the following (Bosch et al. (2013)).

Let

$$\begin{tikzcd}
(\dagger) & M_1 \arrow[r, "f_1"] \arrow[d, "u_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "u_2"] & M_3 \arrow[d, "u_3"] \\
(\dagger\dagger) & N_1 \arrow[r, "g_1"] & N_2 \arrow[r, "g_2"] & N_3
\end{tikzcd}$$

Figure 1

commutative diagram of R-module homomorphism with exact rows be a commutative diagram of R-module homomorphisms with exact rows. Then the diagram extends uniquely to a commutative diagram

$$\begin{tikzcd}
\ker u_1 \arrow[r, "f'_1"] \arrow[d] & \ker u_2 \arrow[r, "f'_2"] \arrow[d] & \ker u_3 \arrow[d] \\
M_1 \arrow[r, "f_1"] \arrow[d, "u_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "u_2"] & M_3 \arrow[d, "u_3"] \\
N_1 \arrow[r, "g_1"] \arrow[d] & N_2 \arrow[r, "g_2"] \arrow[d] & N_3 \arrow[d] \\
\operatorname{coker} u_1 \arrow[r, "\overline{g}_1"] & \operatorname{coker} u_2 \arrow[r, "\overline{g}_2"] & \operatorname{coker} u_3
\end{tikzcd}$$

Figure 2

extended commutative diagram

where the vertical sequences are just the canonical exact sequences associated with u_1, u_2, u_3. Then we have:

(i) $f'_2 \circ f'_1 = 0$ and $g'_2 \circ g'_1 = 0$

(ii) If g_1 is injective, the top upper row is exact.

(iii) If f_2 is surjective, the bottom lower row is exact.

(iv) Let g_1 be injective and f_2 surjective. Then there exists an R-module homomorphism d: ker $u_3 \longrightarrow$ coker u_1, the so-called morphism, defined as follows:

Starting with $x_3 \in$ ker $u_3 \subset M_3$, choose an f_2-preimage $x_2 \subset M_2$ such that $g_1(y_1) = u_2(x_2)$. Now let d(x_3) be the residue class $\bar{y}_1$ of y_1 in coker u_1.

(v) In the setting of (iv), the exact sequences of (ii) and (iii) yield an exact sequence as follows:

$$\begin{tikzcd}
\ker u_1 \arrow[r, "f'_1"] & \ker u_2 \arrow[r, "f'_2"] & \ker u_3 \arrow[dll, rounded corners, "d"] \\
\operatorname{coker} u_1 \arrow[r, "\overline{g}_1"] & \operatorname{coker} u_2 \arrow[r, "\overline{g}_2"] & \operatorname{coker} u_3
\end{tikzcd}$$

Figure 3

the exact sequence from (ii), (iii) and (iv)

Proof. For any $x_1 \in$ ker u_3, $u_2(f_1(x_1)) = g_1(u_1(x_1))$. Then $f_1(x_1) \in$ ker u_2. Thus, f_1 restricts to an R-morphism f'_1: ker $u_1 \longrightarrow$ ker u_2. Similarly, we can get f'_2 from restriction of f_2. Further more, we have $g_1(u_1(M_1)) = u_2(f_1(M_1))$, so g_1(im u_1) $\subset$ im u_2. In particular, the R-homomorphism $N_1 \xrightarrow{g_1} N_2 \longrightarrow$ coker u_2 has a kernel containing im u_1. Then factorizes uniquely over an R-homomorphism $\bar{g}_1$: coker $u_1 \longrightarrow$ coker u_2. Similarly, we can obtain $\bar{g}_2$. Then we start to prove assertion (i). Since the row (†) and (††) are exact, $f_2 \circ f_1 = 0$ and $g_2 \circ g_1 = 0$. Then we get assertion (i) due to f'_1 and f'_2 are restrictions of f_1 and f_2, and $\bar{g}_1$ and $\bar{g}_2$ is factorized from g_1 and g_2.

To verify (ii), assume that g_1 is injective. Due to (i), ker $f'_1 \subset$ im f'_2. Then we only need to show that ker $f'_2 \subset$ im f'_1. For any $x_2 \in$ ker $f'_2 \subset$ ker f_2 due to f'_2 is restriction of f_2. Since ker $f_2 \subset M_2$, $x_2 \in$ M. By the exactness of (†), there exist some $x_1 \in M_1$ such that $f_1(x_1) = x_2$. Then $x_1 \in$ ker u_1. Then $f'_1(x_1) = x_2$ will show x_2, thus ker $f'_2 \subset$ im f'_1. Now $x_2 \in$ ker u_2 implies $g_1(u_1(x_1)) = u_2(f_1(x_1)) = u_2(x_2) = 0$. Since g_1 is injective, we get $u_1(x_1) = 0$. Hence, $x_1 \in$ ker u_1.

Similarly, due to (i), we have im $\bar{g}_1 \subset$ ker $\bar{g}_2$ for the assertion (iii). We only need to prove that ker $\bar{g}_2 \subset$ im $\bar{g}_1$. We choose an element $\bar{y}_2 \in$ ker $\bar{g}_2$, together with a representative $y_2 \in N_2$. Then the image $g_2(y_2)$ is a representative of $\bar{g}_2(\bar{y}_2) = 0$. Thus, $g_2(y_2) \in$ im u_3. We can find a u_3-preimage $x_3 \in M_3$ of $g_2(y_2)$. Since f_2 was surjective, x_3 admits an f_2-preimage $x_2 \in M_2$. Let $y'_2 = y_2 - u_2(x_2)$ is a representative of $\bar{y}_2$. Then, $g_2(y'_2) = g_2(y_2 - u_2(x_2)) = g_2(y_2) - g_2(u_2(x_2)) = g_2(y_2) - u_3(f_2(x_2)) = g_2(y_2) - u_3(x_3) = g_2(y_2) - g_2(y_2) = 0$. But then, using the exactness of row (††), there is a g_1-preimage $y_1 \in N_1$ of y'_2. Writing $\bar{y}_1 \in$ coker u_1 for the associated residue class in coker u_1, we get $\bar{g}_1(\bar{y}_1) = \bar{y}_2$. Therefore, $\bar{y}_2 \in$ im $\bar{g}_1$ and we get that ker $\bar{g}_2 \subset$ im $\bar{g}_1$, as desired.

Now assume the g_1 is injective and f_2 is surjective. We want to show that we can define an R-homomorphism d: ker $u_3 \longrightarrow$ coker u_1, as specified in (iv). To do this, start from an element $x_3 \in$ ker u_3. By the surjectivity of f_2, there exist an f_2-preimage $x_2 \in M_2$.

By the exactness of (†) shown in (ii), the letter is unique up to an additive contribution from im f_1. Then
$g_2(u_2(x_2)) = u_3(f_2(x_2)) = u_3(x_3) = 0$
and, using the exactness of (††), we get $u_2(x_2) \in$ ker $g_2 = g_1$. Thus, $u_2(x_2)$ admits a g_1-preimage $y_1 \in M_1$ where the latter depends uniquely on $u_2(x_2)$, since g_1 is injective. Since x_2, as an f_2-preimage of x_3, is uniquely on x_3 up to an additive contribution form im u_1. In any case, the residue class $\bar{y}_1 \in$ coker u_1, $x_3 \longrightarrow \bar{y}_1$, is well-defined. It is clear that d satisfies the properties of an R-homomorphism, since d has been defined in terms of taking preimages and images with respect to R-homomorphism.

It remains to show that the sequence in (v) is exact at the places ker u_3 and coker u . Let us start with the sequence ker u f'_2 ker $u_3 \xrightarrow{d}$ coker u_1. We prove im $f'_1 \subset$ ker d at 2 first. For any $x_3 \in$ im f'_2 admits an f_2-preimage $x_2 \in$ ker u_2. Then $u_2(x_2) = 0$. In particular, $0 \in N_1$ is a g_1-preimage of $u_2(x_2)$ and, hence, is a representative of $d(x_3)$ so that $d(x_3) = 0$. We get $f'_2 \subset$ ker d. Conversely, suppose $x_3 \in$ ker d. Again, let $x_2 \in M_2$ be an f_2-preimage of x_3 and $y_1 \in N_1$ a g_1-preimage of $u_2(x_2)$. Then, since $x_3 \in$ ker d, we have $y_1 \in$ im u_1 and there exists a u_1-preimage $x_1 \in M_1$ of y_1. Writing

$u_2(f_1(x_1)) = g_1(u_1(x_1)) = g_1(y_1) = u_2(x_2)$
then $u_2(f_1(x_1) - x_2) = u_2(f_1(x_1)) - u_2(x_2) = 0$, hence, $x_2 - f_1(x_1) \in \ker u_2$. Therefore
$x_3 = f_2(x_2) = f_2(x_2) - f_2(f_1(x_1)) = f_2(x_2 - f_1(x_1) \in \operatorname{im} f_2'$
and, hence, $\ker d \subset \operatorname{im} f_2'$. We have proved the sequence $\ker u_2$ f_2' $\ker u_3 \xrightarrow{d}$ coker u_1 is exact.

Finally, let us discuss this the sequence $\ker u_3 \xrightarrow{d}$
coker u_1
$\bar{g}_1$
$\longrightarrow$
coker u_2. First, we
show $\operatorname{im} d \subset \ker \bar{g}_1$. To do this, choose an element $x_3 \in \ker u_3$ and let $x_2 \in M_2$ be an
f_2-preimage of x_3, as well as $y_1 \in N_1$ a g_1-preimage of $u_2(x_2)$. Then y_1 is a representative of $d(x_3)$ and $g_1(y_1) = u_2(x_2) \in \operatorname{im} u_2$ a representative of $\bar{g}_1(d(x_3))$. But then $\bar{g}_1(d(x_3)) = 0$ and we have $\operatorname{im} d \subset \ker \bar{g}_1$. Conversely, consider an element $\bar{y}_1 \in \ker \bar{g}_1$, together with a representative $y_1 \in N_1$. Then we have $g_1(y_1) \in \operatorname{im} u_2$ and there is a u_2-preimage $x_2 \in M_2$ of $g_1(y_1)$. Observing the equation $u_3(f_2(x_2)) = g_2(u_2(x_2)) = g_2(g_1(y_1)) = 0$, where we use
that $g_2 \circ g_1 = 0$ due to the exactness of (††), we conclude $x_3 := f_2(x_2) \in \ker u_3$ and see from the construction of x_3 taht $d(x_3) = \bar{y}_1$. Therefore $\bar{y}_1 \in \operatorname{im} d$ and, hence, $\ker \bar{g}_1 \subset \operatorname{im} d$.

We finished the proof of the exactness of the sequence ker $u_3 \xrightarrow{d}$
Hence, we have proved assertion (v).
coker u_1
$\bar{g}_1$
$\longrightarrow$
coker u_2.

As shown in the proof above, we have successfully proved Snake Lemma. Based on this we can also discuss the related application side of this mathematical tool.

Applications of Ring Theory

Unlike those fancy names such as artificial intelligence or quantum computing, ring theory is not often mentioned in many literature and algorithms. However, as the foundation of many related sub-algorithms or mathematical operators. Many algorithms already have ring theory embedded within them. This study would like to start with the most commonly and widely used applications, followed by more complicated algorithms in related areas.

- Filter Design

Filter as an engineering concept is often used everywhere. However, it has a broader definition in mathematics. A filter in a broad sense can be considered as a function mapping. Also, this mapping can be an arbitrary function that includes simple mathematical operators and also more complex such as convolution, integration, partial differentiation, or even more complicated algorithms, including Fourier

transform, Laplacian transform, etc. The development of information processing, data mining, data cleaning, data extraction, and so on have corresponding complex algorithms but also need a lot of calculations. Hence, this study discovers that ring theory is more or less used in these algorithms due to all of these algorithms including linear calculations of the matrix. From this perspective, it can explore the mathematical, geometric, and algebraic implications of these algorithms.

- Matrix Factorization

Firstly, scholars will come across a lot of places where they need to do complex matrix factorization. For example, when doing segmentation of time-series data, scholars usually construct a self-similarity matrix (SSM) at first. For example, if 10321 is an original signal in which there are 5 numbers, the corresponding
self-similarity matrix will be a 5 × 5 matrix. Since the first number of signals is 1, the final row is 1 × 1 1 × 0 1 × 3 1 × 2 1 × 1 which is equal to 1 0 3 2 1 Similarly, the 4*th* row, 3*th* row, 2*nd* row and 1*st* row are got. Hence, people get the

$$\begin{matrix} 1 & 0 & 3 & 2 & 1 \\ 2 & 0 & 6 & 4 & 2 \\ 3 & 0 & 9 & 6 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 2 & 1 \end{matrix}$$

be factorized. There are many ways to do matrix factorization. Hence, based on math foundation and ring theory, Laplacian Structural Decomposition (LSD) is one of the methods which has been used more and is relatively effective recently. From this, corresponding eigenvectors and eigenvalues are obtained, and scholars can use them to do clustering to complete the final segmentation task.

- Chinese Remainder Theorem

When having a very large number needed to calculate, people usually can calculate directly. However, the ways of computer to calculate is different from people's.
Researchers discovered that if using a computer to calculate a lot of large numbers, the rate of calculating may decrease. Hence, people can use the Chinese Remainder Theorem to develop an algorithm that is similar to the residue number system.

Based on ring theory, people can use a better way to change complex number to simple number (in remainder form), which lead to us getting relatively complex results from calculating the simple number.

When people use ring theory to calculate, regardless of any mathematical operator, they will need to use addition and multiplication. Hence, researchers will focus on those two particular tasks to design the connection of the logic circuit gate in designing and developing the chip, just like the filter operation from the previous section.

Conclusion

This paper summarizes previous results that are related to ring theory and its application to fill the gap in this area. Besides, it is deeply discussed the mathematical foundation and the corresponding applications of ring theory in discussion. Corresponding further studies are proposed below.

However, there are also some limitations of this paper. Firstly, ring theory originated from algebra. Therefore, when the researcher looked for articles, she may more or less use some articles related to algebra, but not only introduce ring theory. In addition, there will be slightly fewer articles in the field of mathematics. Hence, when the researcher searched for articles, she found more articles about the applications and some areas that are related to ring theory. These articles may not be so closely related to ring theory.

There are some further studies. Ring theory can be applied in many areas, including information encoding based on information theory (encryption), also in the communication area, and information flow across devices. Another potential research area could be the evaluation function or the loss function when evaluating the machine learning models or

simply the pre-processing data before feeding into the model, like the sound processing in the natural language processing area.

References

Abduldaim, A. M., & Al-Saidi, N. M. (2017). Generalized π-armendariz authentication cryptosystem. *International Journal of Mathematical and Computational Sciences*, *11* (9), 422–427.

Adhami, R. R., & Brewer, V. E. (1989). Edge detection using a cyclic ring of integers modulo 7. In *1989 the twenty-first southeastern symposium on system theory* (pp. 145–146).

Aditya, R., Zulfikar, M. T., & Manik, N. I. (2015). Testing division rings and fields using a computer program. *Procedia Computer Science*, *59* , 540–549.

Ahmed, S., Ghosh, K. K., Singh, P. K., Geem, Z. W., & Sarkar, R. (2020). Hybrid of

harmony search algorithm and ring theory-based evolutionary algorithm for feature selection. *IEEE Access*, *8* , 102629–102645.

Artin, E. (1927). Zur theorie der hyperkomplexen zahlen. In *Abhandlungen aus dem*

mathematischen seminar der universität hamburg (Vol. 5, pp. 251–260).

Awange, J. L., Fukuda, Y., Takemoto, S., & Grafarend, E. W. (2005). Role of algebra in modern day geodesy. In *A window on the future of geodesy: Proceedings of the international association of geodesy iag general assembly sapporo, japan june 30–july 11, 2003* (pp. 524–529).

Bell, J., Launois, S., Sánchez, O. L., & Moosa, R. (2017). Poisson algebras via model theory and differential-algebraic geometry. *Journal of the European Mathematical Society*, *19* (7), 2019–2049.

Blechschmidt, I. (2021). Using the internal language of toposes in algebraic geometry.

arXiv preprint arXiv:2111.03685 .

Bosch, S., et al. (2013). *Algebraic geometry and commutative algebra*. Springer.

Cardarilli, G. C., Nannarelli, A., & Re, M. (2007). Residue number system for low-power dsp applications. In *2007 conference record of the forty-first asilomar conference on signals, systems and computers* (pp. 1412–1416).

Chattopadhyay, S., Patra, K. L., & Sahoo, B. K. (2020). Laplacian eigenvalues of the zero divisor graph of the ring zn. *Linear Algebra and its applications*, *584* , 267–286.

Chervyakov, N., Lyakhov, P., & Valueva, M. (2017). Increasing of convolutional neural

network performance using residue number system. In *2017 international*

multi-conference on engineering, computer and information sciences (sibircon) (pp. 135–140).

Cimprič, J. (2012). Real algebraic geometry for matrices over commutative rings. *Journal of Algebra*, *359* , 89–103.

Cohn, P. M. (2012). *Introduction to ring theory*. Springer Science & Business Media. Connes, A., & Consani, C. (2021). On absolute algebraic geometry the affine case.

Advances in Mathematics, *390* , 107909.

Ebrahimi, S., & Bayat-Sarmadi, S. (2020). Lightweight and dpa-resistant post-quantum cryptoprocessor based on binary ring-lwe. In *2020 20th international symposium on computer architecture and digital systems (cads)* (pp. 1–6).

Ebrahimi, S., Bayat-Sarmadi, S., & Mosanaei-Boorani, H. (2019). Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in iot. *IEEE Internet of Things Journal*, *6* (3), 5500–5507.

Fraenkel, E. (1914). Über die beziehungen der leukämie zu geschwulstbildenden prozessen des hämatopoetischen apparates. *Virchows Archiv für pathologische Anatomie und Physiologie und für klinische Medizin*, *216* (3), 340–354.

Galdino, A. L., Borges, A. A., Ayala-Rincón, M., et al. (2021). Formalization of ring theory in pvs. *Journal of Automated Reasoning*, *65* (8), 1231–1263.

Garcés, Y., Torres, E., Pereira, O., & Rodríguez, R. (2014). Application of the ring theory
in the segmentation of digital images. *arXiv preprint arXiv:1402.4069* .

Grigoriev, D., & Ponomarenko, I. (2003). Homomorphic public-key cryptosystems over groups and rings. *arXiv preprint cs/0309010* .

Hamilton, W. R. (1843). On quaternions; or on a new system of imaginaries in algebra
(letter to john t. graves, dated october 17, 1843). *Philos. Magazine*, *25* , 489–495.

Harada, M. (1979). Non-small modules and non-cosmall modules. In *Ring theory, proceedings of 1978 antwerp conference*.

He, Y., Wang, X., & Gao, S. (2019). Ring theory-based evolutionary algorithm and its
application to d {0-1} kp. *Applied Soft Computing*, *77* , 714–722.

Jacobson, N. (1956). *Structure of rings* (Vol. 37). American Mathematical Soc.

Jiang, Y., & Zhang, Y. (2018). Algebraic geometry and bethe ansatz. part i. the quotient ring for bae. *Journal of High Energy Physics*, *2018* (3), 1–40.

Khan, A. (2019). The morel–voevodsky localization theorem in spectral algebraic
geometry. *Geometry & Topology*, *23* (7), 3647–3685.

Kleiner, I. (1996). The genesis of the abstract ring concept. *The American mathematical monthly*, *103* (5), 417–424.

Kleiner, I. (1998). From numbers to rings: The early history of ring theory. *Elemente der Mathematik*, *53* , 18–35.

Knapp, A. W. (2007). *Advanced algebra*. Springer Science & Business Media.

Kolmogorov, A. N. (1900). Kolmogorov 1903–1987. In *Proc. 3rd ieee conference on structure in* (pp. 80–101).

Krull, W. (2020). *Primidealketten in allgemeinen ringbereichen*. Walter de Gruyter GmbH & Co KG.

Lemmermeyer, F. (2011). The snake lemma. *arXiv preprint arXiv:1108.5684* .

Lezama, O., & Latorre, E. (2017). Non-commutative algebraic geometry of semi-graded rings. *International Journal of Algebra and Computation*, *27* (04), 361–389.

Lyubashevsky, V., Peikert, C., & Regev, O. (2010). On ideal lattices and learning with
errors over rings. In *Advances in cryptology–eurocrypt 2010: 29th annual international conference on the theory and applications of cryptographic techniques, french riviera, may 30–june 3, 2010. proceedings 29* (pp. 1–23).

Malcev, A. I. (n.d.). 1909–1967.

Muthuraj, R., & Gandhi, N. R. (n.d.). Application of hx ring theory in homomorphic encryption.

Noether, E. (n.d.). Ideal theory in rings (idealtheorie in ringbereichen), translated by daniel berlyne. *arXiv preprint arXiv:1401.2577* .

Noether, E. (1923). Eliminationstheorie und allgemeine idealtheorie. *Mathematische
Annalen*, *90* (3-4), 229–261.

Pirzada, S., Rather, B., Shaban, R. U., & Merajuddin, S. (2021). On signless laplacian spectrum of the zero divisor graphs of the ring zn. *Korean Journal of Mathematics*, *29* (1), 13–24.

Pirzada, S., Rather, B. A., & Chishti, T. (2021). On distance laplacian spectrum of zero divisor graphs of the ring zn. *Carpathian Mathematical Publications*, *13* (1), 48–57.

Rowen, L. H. (2012). *Ring theory, 83*. Academic Press.

Sarathy, R., & Sankar, J. R. (2023). Applications on color (distance) signless laplacian energy of annihilator monic prime graph of commutative rings. *Ain Shams Engineering Journal*, 102469.

Shariq, M., Mathil, P., & Kumar, J. (2023). Laplacian spectrum of weakly zero-divisor graph of the ring zn. *arXiv preprint arXiv:2307.12757* .

Shen, S., Liu, W., & Jin, W. (2023). Laplacian eigenvalues of the unit graph of the ring zn.
Applied Mathematics and Computation, *459* , 128268.

Shirshov, A. I. (1962). On the bases of a free lie algebra. *Algebra i Logika*, *1* (1), 14–19. Stillwell, J., & Stillwell, J. (1989). *Mathematics and its history* (Vol. 3). Springer.

Torres, E., Rodriguez, R., Garcés, Y., & Pereira, O. (n.d.). Edge detection in segmented images through mean shift iterative gradient using ring.

Valueva, M. V., Nagornov, N., Lyakhov, P. A., Valuev, G. V., & Chervyakov, N. I. (2020).
Application of the residue number system to reduce hardware costs of the convolutional neural network implementation. *Mathematics and computers in simulation*, *177* , 232–243.

Wedderburn, J. M. (1908). On hypercomplex numbers. *Proceedings of the London Mathematical Society*, *2* (1), 77–118.

Zheng, Z., Huang, W., Xu, J., & Tian, K. (2021). A generalization of cyclic code and applications to public key cryptosystems. *arXiv preprint arXiv:21*