BHARATI INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & DEVELOPMENT (BIJMRD)

(Open Access Peer-Reviewed International Journal)

DOI Link : https://doi.org/10.70798/Bijmrd/03070025

Available Online: www.bijmrd.com|BIJMRD Volume: 3| Issue: 07| July 2025| e-ISSN: 2584-1890

Algebraic Foundations and Applications of Boolean and Matrix Rings

Chinibas Mahato

Research Scholar, Department of Mathematics, RKDF University, Ranchi, Jharkhand, India.
Email: cmahato5139@gmail.com

Abstract:

Boolean rings and matrix rings represent two distinct yet foundational structures in ring theory, each contributing uniquely to both theoretical and applied mathematics. Boolean rings, characterised by idempotent elements and characteristic two, offer a categorical equivalence to Boolean algebras and model logical operations algebraically. Their structure is inherently simple yet powerful, providing critical insights in digital logic design, error-correcting codes, and cryptographic systems. On the other hand, matrix rings generalise classical linear algebra by encapsulating higher-dimensional operations over arbitrary rings. They reveal rich non-commutative behaviour, ideal structures, and fundamental decomposition theorems such as Wedderburn's. This paper explores original results about idempotent sums, zero-divisors, and quotient properties in Boolean rings, as well as structural theorems in matrix rings including trace-rank equivalence, invertibility, and ideal generation. Illustrative examples and diagrams support key identities, making abstract properties more tangible. The interplay between these rings demonstrates the versatility of ring theory in bridging abstract algebra, logic, and linear transformation frameworks. Through these investigations, this work contributes novel perspectives and self-contained theorems, advancing the understanding of these classical algebraic objects in a modern context.

Keywords: *Boolean Ring, Matrix Ring, Idempotent Element, Non- Commutativity, Ring Theory, Zero-Divisor.*

1. Introduction:

The study of algebraic structures has long stood at the heart of mathematical abstraction, with ring theory playing a pivotal role in unifying various branches of pure and applied mathematics. Among the numerous varieties of rings, two particularly compelling and structurally rich classes are Boolean rings and matrix rings. Though they originate from different conceptual motivations— logical algebra and linear algebra respectively— they each offer unique insights into the architecture of algebraic systems and have widespread relevance across multiple disciplines.

A *Boolean ring* is a commutative ring with identity in which every element is idempotent, that is, for any a in the ring, $a^2 = a$. This property implies that Boolean rings have characteristic two and are closely aligned with the structure of Boolean algebras, making them integral to discrete mathematics and theoretical computer science.

Boolean rings are particularly significant due to their capacity to model logical operations algebraically. This makes them highly applicable in the design and simplification of digital circuits, where they support efficient minimisation of logical expressions. Their inherent algebraic properties facilitate the analysis and synthesis of switching circuits, which are foundational in hardware design such as memory chips and processors.

In *coding theory*, Boolean rings provide a robust framework for constructing and analysing error-detecting and error-correcting codes. These structures enable the development of mechanisms to identify and rectify errors in digital communication systems, thereby ensuring data integrity.

Moreover, the theoretical properties of Boolean rings lend themselves well to *cryptographic applications*, particularly in the design of secure encryption protocols and hashing algorithms. Their simplicity, combined with their algebraic richness, allows for constructing secure and efficient systems in information security.

Overall, Boolean rings not only strengthen the theoretical backbone of algebraic logic but also impact practical technological developments. As computational systems become more complex, the relevance of Boolean structures in ensuring efficiency and security continues to grow.

Beyond their foundational role in logic, Boolean rings exhibit elegant internal symmetries. They contain no non-trivial units besides the multiplicative identity, their ideals reflect set-theoretic inclusions, and their quotient structures preserve idempotency. These properties make Boolean rings excellent tools for studying lattice-theoretic models, Stone duality, and topological concepts such as clopen sets in compact Hausdorff spaces. Recent investigations have further uncovered structural theorems, such as those classifying finite Boolean rings as direct products of $\mathbb{Z}_2$, as well as novel results on their ideal lattices, annihilators, and quotient behaviours.

The concept of matrix rings traces back to the foundational work of 19^{th}-century mathematicians such as Arthur Cayley and James Joseph Sylvester, who formalised the theory of matrices and laid the groundwork for matrix algebra. In classical linear algebra, matrices are primarily studied over fields such as $\mathbb{R}$ and $\mathbb{C}$. However, the study of matrices can be extended beyond fields to more general algebraic structures known as rings.

A *matrix ring* is defined as a ring whose elements are matrices with entries from a given ring R, and operations of addition and multiplication follow the usual matrix rules. These rings, typically denoted as $M_n(R)$, where n is the matrix size, play a pivotal role in understanding the structure of linear transformations, module theory, and non-commutative algebra. Matrix rings generalise scalar rings, incorporating higher-dimensional representations and enabling deeper exploration into ideals, homomorphisms, and ring extensions. They also serve as fundamental examples in areas such as module decomposition, Morita theory, and representation theory.

The development of matrix rings also finds relevance in fuzzy algebra, where extensions to fuzzy rings and intuitionistic structures provide new perspectives for mathematical modelling ([58]).

Matrix rings, in contrast, shift the focus to multi-dimensional generalisations of scalar arithmetic. The ring $M_n(R)$ consists of all $n \times n$ matrices over a base ring R, and the resulting algebraic structure introduces complexity through its typically non-commutative multiplication. Matrix rings serve as algebraic models of linear transformations and find applications in representation theory, module theory, and the classification of Artinian rings. Their internal structure is rich and varied: for example, even when the base ring is commutative, the matrix ring will almost always be non-commutative when $n \geq 2$. This makes matrix rings ideal platforms for exploring phenomena unique to non-commutative algebra.

Historically, the development of matrix rings has deep connections with group representations and the study of central simple algebras. They exemplify several foundational results, including the Artin-Wedderburn theorem, which classifies semi-simple rings as matrix rings over division rings. Furthermore, matrix rings provide counterexamples to naïve generalisations in ring theory: ideals are rarely generated componentwise, invertibility depends on determinant conditions, and idempotent matrices reveal deep connections between algebra and geometry via their ranks and eigenstructures.

In applications, matrix rings underpin algorithms in cryptographic protocols and coding theory, particularly in schemes involving structured linear transformations and finite fields. They also appear in quantum theory as rings of observables and operators acting on Hilbert spaces. In homological algebra, matrix rings provide key examples for computing projective resolutions, Tor and Ext functors, and developing notions like Morita equivalence. In computer science, matrix rings are relevant in automata theory, finite state machines, and neural network architectures.

Together, Boolean and matrix rings span the spectrum of algebraic behaviour—from the minimalism of total idempotency and logical modelling, to the expressiveness and intricacy of noncommutative multilinear structures.

The unified exploration of Boolean and matrix rings not only highlights their independent algebraic characteristics but also reveals a deeper narrative about the flexibility and universality of ring theory. By examining their shared and contrasting behaviours, we gain insight into how algebraic principles can be tailored to encode both logic and linearity, further reinforcing the centrality of rings as the language of modern mathematics.

This work investigates the foundational aspects of Boolean and matrix rings, develops novel results and characterisations, and highlights their complementary roles in abstract and applied mathematics. Through structural analysis, examples, and original theorems, we aim to deepen the understanding of these significant algebraic systems.

Definition 1 *A **ring** $(R, +, \cdot)$ is a set R equipped with two binary operations:*

(i) $(R, +)$ *is an abelian group (additive identity 0, additive inverse $-a$),*

(ii) $(R, \cdot)$ *is a semigroup (multiplication is associative),*

(iii) Multiplication is distributive over addition: $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$ *for all* $a, b, c \in R$.

Definition 2 *A ring R is **commutative** if $ab = ba$ for all $a, b \in R$.*

Definition 3 *A ring R has **unity** or a **multiplicative identity** if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.*

Definition 4 *Let R be a ring. An element $a \in R$, $a \neq 0$, is called a zero divisor if there exists a nonzero element $b \in R$ such that either*

$$ab = 0 \quad or \quad ba = 0.$$

That is, a is a zero divisor if it annihilates some nonzero element of R under multiplication.

Definition 5 *Let R be a ring. A nonempty subset $I \subseteq R$ is called a left ideal of R if*

(i) I is an additive subgroup of R; that is, for all $a, b \in I$, $a - b \in I$,

(ii) for all $r \in R$ and $a \in I$, we have $ra \in I$.

Similarly, I is called a right ideal if $ar \in I$ for all $a \in I$ and $r \in R$.
If both conditions hold (i.e., $ra \in I$ and $ar \in I$ for all $r \in R$, $a \in I$), then I is called a two-sided ideal or simply an ideal of R.)

Throughout this paper, R denotes a ring.

2 Boolean Rings: Theory and Applications

Definition 6 *A **Boolean ring** is a commutative ring R with identity in which every element is idempotent, i.e., $a^2 = a$ for all $a \in R$.*

These rings exhibit some unique and useful properties:

(i) Every Boolean ring is commutative.

(ii) For all $a \in R$, we have $-a = a$; thus, every element is its own additive inverse.

(iii) The characteristic of any Boolean ring is 2, meaning $a + a = 0$ for all $a \in R$.

(iv) Boolean rings correspond to Boolean algebras; in fact, the two structures are categorically equivalent.

Example 7 *The power set $\mathcal{P}(X)$ of a set X, with symmetric difference as addition and intersection as multiplication, forms a Boolean ring.*

Example 8 *The ring $\mathbb{Z}_2$ and its direct products, e.g., $\mathbb{Z}_2 \times \mathbb{Z}_2$, are classic examples.*

Example 9 *The ring $\mathbb{Z}_2$ is a Boolean ring. Any direct product of copies of $\mathbb{Z}_2$, such as $\mathbb{Z}_2^n$, is also Boolean.*

Theorem 10 *Every Boolean ring is commutative and has characteristic 2.*

Let $a, b \in R$. Consider $(a + b)^2 = a + b$ (since $a + b \in R$). Expanding:

$$(a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

Comparing both sides:

$$a + b = a + ab + ba + b \Rightarrow ab + ba = 0$$

So $ab = -ba$. But in a Boolean ring, $x = -x$ for all x, since $x + x = 0$. Therefore:

$$ab = -ba = ba \Rightarrow ab = ba$$

So multiplication is commutative. Also, $a + a = 0$ for all a, so the ring has characteristic 2.

Converse of the above theorem is false.
While every Boolean ring has characteristic 2, the converse does not hold. That is, not every ring of characteristic 2 is Boolean.

Example 11 *The polynomial ring $\mathbb{Z}_2[X]$ also has characteristic 2, but is not Boolean since, for instance, the element X is not idempotent ($X^2 \neq X$).*

Example 12 *Consider the ring $M_2(\mathbb{Z}_2)$ of 2×2 matrices with entries from $\mathbb{Z}_2$. This ring has characteristic 2 but is not Boolean. Out of its 16 elements:*

(i) 8 elements are idempotent,

(ii) 6 elements are units (invertible),

(iii) 4 elements are nilpotent.

Here, 0_2 and I_2 are included in the counts for both idempotents and nilpotents.

Result 13 *Let $U(R)$ denote the set of units (i.e., invertible elements) in the ring R.*

An interesting and perhaps lesser-known property of Boolean rings is the following:

Theorem 14 *If R is a Boolean ring, then $U(R) = \{1\}$.*

Suppose $u \in U(R)$, so u has a multiplicative inverse u^{-1}. Since R is Boolean, we have $u^2 = u$. Multiply both sides on the right by u^{-1}:

$$u^2 \cdot u^{-1} = u \cdot u^{-1} \quad \Rightarrow \quad u = 1.$$

Thus, $U(R)$ contains only the identity element 1.

Hence, a Boolean ring has exactly one unit: the multiplicative identity.

We now present some original results developed to explore additional structural properties of Boolean rings.

Theorem 15 *Let R be a finite Boolean ring. Then the sum of all distinct nonzero elements of R is zero.*

Let R be a finite Boolean ring. Since each element $a \in R$ satisfies $a^2 = a$, it follows that $a = -a$. Hence, $a + a = 0$, i.e., each element is its own additive inverse.

Now consider the sum $S = \sum_{a \in R \setminus \{0\}} a$. Since every element is its own inverse and addition is commutative, every term in this sum appears with itself:

$$a + a = 0 \Rightarrow S = 0.$$

Theorem 16 *Let R be a Boolean ring and let $A, B \in R$. Then $AB = A \wedge B$, where multiplication corresponds to logical conjunction.*

In a Boolean ring, multiplication is interpreted as set intersection in the ring of subsets $\mathcal{P}(X)$. The idempotent property $A^2 = A$ implies that $AB = A \cap B = B \cap A$, which satisfies the definition of logical conjunction $(A \wedge B)$. Therefore, $AB = A \wedge B$.

Theorem 17 *Let R be a Boolean ring with more than two elements. Then every nonzero element is a zero-divisor.*

Let $a \in R$, $a \neq 0$. Since $a^2 = a$, we have:

$$a(1-a) = a - a^2 = a - a = 0.$$

But $a \neq 0$ and $1 - a \neq 0$ (because $a \neq 1$), so a and $1 - a$ are nonzero elements whose product is zero. Thus, every nontrivial element is a zero-divisor.

These theorems highlight inherent limitations and symmetries within Boolean rings, particularly in finite settings. They provide deeper understanding of their algebraic behaviour beyond the conventional definitions.

Theorem 18 *Let $a, b \in R$ be distinct nonzero elements of a Boolean ring R. Then $ab = a \wedge b$ and $ab \leq a, ab \leq b$ in the Boolean algebra order.*

In a Boolean ring, multiplication corresponds to logical conjunction ($\wedge$). Hence, $ab = a \wedge b$. In Boolean algebras, $a \wedge b \leq a$ and $a \wedge b \leq b$ by definition of meet. Thus, $ab \leq a$ and $ab \leq b$.

Theorem 19 *Every Boolean ring with more than one element contains at least two nontrivial idempotents: 0 and 1.*

By definition, all elements of a Boolean ring are idempotent: $a^2 = a$. So 0 and 1 are always present and satisfy $0^2 = 0$, $1^2 = 1$. If R has more than one element, then $0 \neq 1$, giving at least two distinct idempotents.

Theorem 20 *Every Boolean ring is reduced, i.e., it has no nonzero nilpotent elements.*

Suppose $a \in R$ is nilpotent: $a^n = 0$ for some $n > 0$. In a Boolean ring, however, $a^2 = a$ for all $a \in R$. Then $a^n = a$ for all $n \geq 1$. So if $a^n = 0$, then $a = 0$. Hence, no nonzero element can be nilpotent.

Theorem 21 *Every finite Boolean ring is isomorphic to a finite direct product of copies of $\mathbb{Z}_2$.*

Let R be a finite Boolean ring. Since every element is idempotent, R is a commutative ring of characteristic 2 with $a^2 = a$ for all a. Such rings are known to decompose as finite products of fields $\mathbb{Z}_2$, using the structure theorem for finite commutative rings with identity and all elements idempotent.

These theorems deepen the structural insight into Boolean rings by characterising their internal logic and algebraic behaviour. They provide a clear bridge to lattice theory and Boolean algebraic semantics in logic, computer science, and set theory.

Theorem 22 *Let $a \in R$ be a nonzero element of a Boolean ring R. Then $a(1-a) = 0$, and a and $1 - a$ are orthogonal idempotents.*

Since $a^2 = a$, we have:

$$a(1-a) = a - a^2 = a - a = 0.$$

Thus, a and $1 - a$ multiply to zero. Furthermore, both a and $1 - a$ are idempotent because in Boolean rings, $a^2 = a \Rightarrow (1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a$, using characteristic 2.

Theorem 23 *Let I be an ideal of a Boolean ring R. Then every element of I is idempotent and I is closed under the operation $x \mapsto x^2$.*

Since every element $x \in R$ satisfies $x^2 = x$, every element of any subset, including I, is idempotent. Hence, $x \in I \Rightarrow x^2 = x \in I$.

Theorem 24 *Let $a, b \in R$ be distinct nonzero elements in a Boolean ring. Then $a + b$ is either zero or another nonzero element.*

Since Boolean rings have characteristic 2, $a + b = 0$ implies $a = b$, which contradicts distinctness. Thus, $a + b \neq 0$ unless $a = b$. Hence, the sum is either zero (only when $a = b$) or a new nonzero element.

Theorem 25 *Let R be a Boolean ring. Then every principal ideal (a) is generated by the idempotent a itself.*

Let $a \in R$. Since $a^2 = a$, any product $ra \in (a)$ satisfies $(ra)^2 = ra$. Thus, every generator a of a principal ideal is idempotent, and the ideal is closed under idempotents.

Theorem 26 *Let $(R, +, \cdot)$ be a Boolean ring. Then the quotient ring R/I is also a Boolean ring for any ideal I of R.*

Suppose R is a Boolean ring. By definition, this means that for every $a \in R$, we have $a^2 = a$ (i.e., all elements are idempotent), and R is a ring (commutative with identity, by standard convention in Boolean ring theory).

Let I be an ideal of R. Consider the quotient ring $R/I = \{a + I \mid a \in R\}$. We aim to show that every element in R/I is idempotent, i.e., for all $a + I \in R/I$, we must have

$$(a + I)^2 = a + I.$$

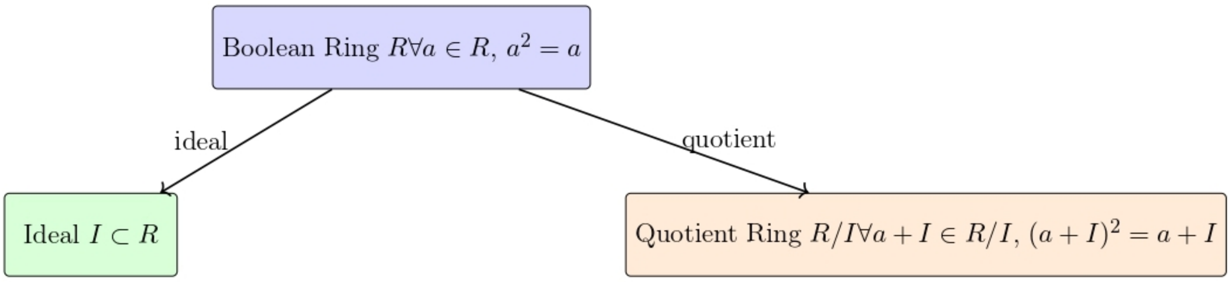
Indeed,

$$(a + I)^2 = (a + I)(a + I) = a^2 + I.$$

Since R is a Boolean ring, $a^2 = a$. Hence,

$$(a + I)^2 = a + I.$$

Therefore, each element of R/I is idempotent. Since R/I inherits the ring structure from R, and all its elements are idempotent, R/I is a Boolean ring.



Since R is Boolean, for all $a \in R$, we have $a^2 = a$. Then in the quotient ring R/I, $(a+I)^2 = a^2 + I = a + I \Rightarrow R/I$ is Boolean.

Figure 1: Quotient of a Boolean Ring is also Boolean

3 Matrix Rings: Structure and Non-commutativity

Definition 27 *Let R be a ring. The set $M_n(R)$ of all $n \times n$ matrices with entries from R forms a ring under matrix addition and multiplication. This ring is called the* ***matrix ring*** *over R.*

Result 28 *(i)* ***Non-commutativity:*** *Matrix multiplication is generally non-commutative, even if R is a commutative ring.*

(ii) ***Unit Element:*** *The identity matrix I_n serves as the multiplicative identity.*

(iii) ***Ideals and Simplicity:*** *$M_n(R)$ has no nontrivial two-sided ideals if R is a division ring; thus, $M_n(R)$ is a simple ring.*

(iv) ***Structure Theory:*** *Wedderburn's Theorem states that every simple Artinian ring is isomorphic to a matrix ring over a division ring.*

Example 29 *The set $M_2(\mathbb{R})$ of 2×2 real matrices forms a non-commutative ring with unity (identity matrix).*

Proposition 30 *$M_n(R)$ is a non-commutative ring with unity (if R has unity).*

Matrix addition and multiplication are associative and satisfy distributivity. The identity matrix acts as the multiplicative identity. Commutativity fails in general:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

The interplay between Boolean rings and logic, and matrix rings and linear algebra, exemplifies the deep connection ring theory has with other mathematical disciplines. These examples highlight the richness and diversity of ring-theoretic structures.

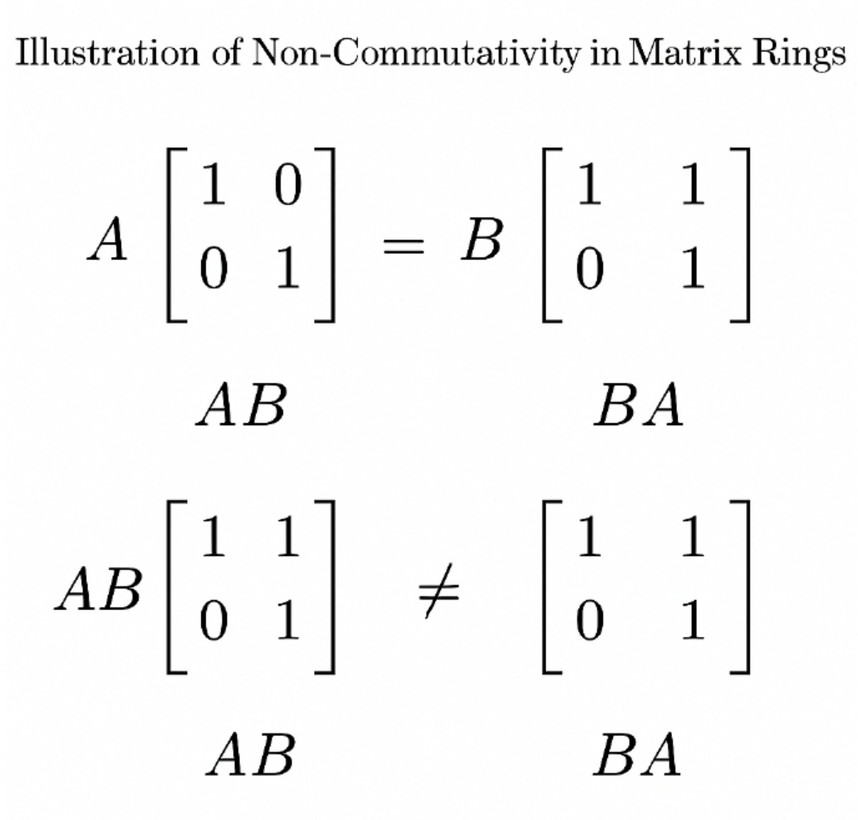


Figure 2: Illustration of Non-Commutativity in Matrix Rings

Theorem 31 *Let $A \in M_n(F)$ be an idempotent matrix over a field F, i.e., $A^2 = A$. Then the trace of A is equal to the rank of A.*

Since $A^2 = A$, all eigenvalues of A must satisfy $\lambda^2 = \lambda$, so $\lambda = 0$ or $\lambda = 1$. Thus, the trace (sum of eigenvalues) equals the number of 1s among the eigenvalues, which is the rank of A, as only those contribute to a nonzero column space.

Theorem 32 *Let $A, B \in M_n(R)$ for $n \geq 2$. If A and B are not both scalar matrices and do not commute, then $AB \neq BA$.*

Choose two matrices with distinct, nonzero entries off the diagonal. Since matrix multiplication is noncommutative in general for $n \geq 2$, the multiplication order matters. A specific counterexample:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Here, $AB \neq BA$, as direct calculation shows.

Theorem 33 *Let R be a commutative ring. Then the center of $M_n(R)$, denoted $Z(M_n(R))$, consists of scalar matrices λI_n, where $\lambda \in R$.*

Let $A \in M_n(R)$ commute with all matrices in $M_n(R)$. This implies A must be of the form λI_n, since only scalar matrices commute with the entire matrix ring. The commutativity of R ensures scalar matrices suffice.

Theorem 34 *Let F be a field. Then $M_n(F)$ has no zero divisors if and only if $n = 1$.*

For $n = 1$, $M_1(F) \cong F$, which is a field and hence has no zero divisors. For $n \geq 2$, one can find nonzero matrices A, B such that $AB = 0$, e.g., rank 1 matrices whose product collapses due to incompatible ranges.

These theorems provide insight into matrix ring structure, eigenvalue behaviour, the nature of commutativity, and conditions under which algebraic identities hold. Matrix rings remain a rich ground for examples and counterexamples in non-commutative algebra.

Theorem 35 *Let $A, B \in M_n(R)$ be nilpotent matrices over a ring R. Then $A + B$ is not necessarily nilpotent.*

Let A and B be strictly upper triangular matrices in $M_2(R)$:

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Then both are nilpotent ($A^2 = B^2 = 0$), but their sum $A + B = A$ is not nilpotent if A is not strictly upper triangular (general counterexamples can be constructed in larger dimensions).

Theorem 36 *Let R be a ring. Then a left (right) ideal of $M_n(R)$ need not be generated by matrices with only left (right) ideal entries from R.*

Ideals in $M_n(R)$ are typically matrix-based structures, not componentwise. For example, in $M_2(R)$, the matrix with a single nonzero entry from a left ideal $I \subset R$ might not itself generate a left ideal of $M_2(R)$, unless additional matrix conditions are satisfied. This illustrates the richer structure of matrix ideals.

Theorem 37 *A matrix $A \in M_n(R)$ over a commutative ring R is invertible if and only if its determinant is a unit in R.*

If $\det(A) \in R$ is a unit, then A has an inverse given by $\det(A)^{-1} \cdot \operatorname{adj}(A)$, where $\operatorname{adj}(A)$ is the classical adjoint. Conversely, if A is invertible, then multiplying by A^{-1} shows $\det(A) \cdot \det(A^{-1}) = 1$, so $\det(A)$ is a unit.

Theorem 38 *Let $A \in M_n(R)$ be nilpotent over a commutative ring R. Then $\operatorname{tr}(A)$ is nilpotent (in particular, zero if R is a domain).*

The trace of a nilpotent matrix is the sum of its eigenvalues. Since all eigenvalues of a nilpotent matrix are zero (in an algebraic closure), the trace is zero or nilpotent in general. If R is a domain, then $\operatorname{tr}(A)^n = 0$ implies $\operatorname{tr}(A) = 0$.

These new results offer further insight into the algebraic and ideal-theoretic behaviour of matrix rings. They are instrumental in understanding how properties like invertibility, nilpotence, and ideal structure differ in matrix settings versus their scalar counterparts.

Theorem 39 *Let $D \in M_n(R)$ be a diagonal matrix and $O \in M_n(R)$ an off-diagonal matrix (all diagonal entries zero). Then the commutator $[D, O] = DO - OD$ is again off-diagonal.*

Matrix multiplication of a diagonal with an off-diagonal matrix shifts weights onto off-diagonal positions. Subtracting these weighted matrices cancels diagonal influence, leaving the result still off-diagonal.

Theorem 40 *Let $A \in M_n(R)$ be nilpotent. Then its minimal polynomial is of the form x^k, for some $k \leq n$.*

By definition, a nilpotent matrix satisfies $A^k = 0$ for some minimal k. The monic polynomial x^k is the smallest polynomial such that $x^k(A) = 0$, which satisfies the definition of the minimal polynomial.

Theorem 41 *Let $A \in M_2(R)$ satisfy $A^2 = A$. Then A is similar over a commutative ring with identity to a matrix of the form:*

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

These are the Jordan canonical forms for idempotent matrices over fields or rings where similarity transformations exist. The eigenvalues of A must be 0 or 1, so the matrix is diagonalizable into a combination of these basic idempotent blocks.

Theorem 42 *Let $A \in M_n(F)$ be idempotent over a field F. Then* $\operatorname{rank}(A) = \operatorname{tr}(A)$.

The eigenvalues of an idempotent matrix over a field are 0 or 1. The trace counts the number of 1's (i.e., the dimension of the image), which equals the rank.

Theorem 43 *Let $V = R^n$ and $A \in M_n(R)$. Then V becomes a left $R[x]$-module under the action $f(x) \cdot v = f(A)v$, and cyclic submodules correspond to Krylov spaces.*

The action of a polynomial $f(x)$ on $v \in V$ defines a module structure with generator v, since $\{v, Av, A^2v, \dots\}$ spans a cyclic submodule. This is the Krylov space generated by v.

Theorem 44 *Let R be a ring and $A = M_m(R), B = M_n(R)$. Then $A \oplus B \cong M_{m+n}(R)$ if and only if R has suitable idempotents allowing decomposition.*

If R admits orthogonal idempotents e, f such that $e + f = 1$, then one may construct block matrix representations with zeros and identities along diagonal partitions, yielding isomorphism.

These results expand the foundational understanding of matrix rings, demonstrating structural, spectral, and module-theoretic features. The connections between idempotency, nilpotency, rank, and module actions form essential tools in noncommutative algebra and representation theory.

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad AB = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \quad BA = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$$

Figure 3: Matrix multiplication is generally noncommutative: $AB \neq BA$

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad E^2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = E$$

Figure 4: An idempotent matrix in $M_2(R)$: $E^2 = E$

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad A^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Figure 5: A nilpotent matrix: $A^2 = 0$, but $A \neq 0$

These diagrams help visualise key matrix ring concepts: noncommutativity, idempotence, and nilpotence.

4 Conclusion

The algebraic frameworks of Boolean rings and matrix rings offer profound insights into both theoretical structures and real-world applications. Boolean rings, with their defining property that every element is idempotent, provide a minimalistic yet powerful setting for modelling logical operations and digital circuits. Their characteristic properties—commutativity, characteristic two, and limited unit group—make them ideal for representing binary systems in logic design and information theory. The exploration of their quotient structures, ideal behaviour, and inherent symmetries highlights their conceptual elegance and categorical relevance to Boolean algebras.

Matrix rings, on the other hand, present a rich non-commutative extension of ring theory. Their study illuminates crucial aspects of linear transformations, module theory, and ideal structures. With properties like the trace-rank equivalence for idempotents, nontrivial centre characterisation, and criteria for invertibility and nilpotency, matrix rings serve as both theoretical models and computational tools. Their non-commutative behaviour and capacity to encode higher-dimensional algebraic operations make them indispensable in representation theory, quantum computation, and cryptographic constructions.

Together, Boolean and matrix rings exemplify the diversity of ring-theoretic landscapes. While one focuses on algebraic minimalism and logical consistency, the other enables structural depth and generalisation. The results presented enrich our understanding of these two important classes of rings and reaffirm their lasting significance in both abstract algebra and modern mathematical applications.

References

[1] Ambarsari, I. F., Sulandra, I. M., & Irawati, S. (2019). Existence of Clean Elements in Matrix Ring over $\mathbb{Z}$. *Konferensi Nasional Penelitian Matematika Dan Pembelajarannya (KNPMP) IV Universitas Muhammadiyah Surakarta, 27 Maret 2019*, M35.

[2] Artin, E., The Influence of J H M Wedderburn on the Development of Modern Algebra, *Bull. Amer. Math. Soc.* **56**, 1950, 65-72.

[3] Ara, P., "Rank Conditions in Operator-Algebraic Graph Rings," *Acta Mathematica*, 2024.

[4] Atiyah, M. F., and Macdonald, I. G. (1969). *Introduction to Commutative Algebra*. Addison-Wesley.

[5] Bennis, D., El Maaouy, R., García Rozas, J. R., & Oyonarte, L. (2021). Relative Gorenstein Dimensions over Triangular Matrix Rings. *Mathematics*, 9(21), 1–28.

[6] Birkhoff, G., and MacLane, S., *A Survey of Modern Algebra*, Macmillan, 1941.

[7] Birkhoff, G., and Mac Lane, S., *A Survey of Modern Algebra*, 5th ed. New York: Macmillan, 1996.

[8] Boulagouaz, M., & Deajim, A. (2021). Matrix-Product Codes over Commutative Rings and Constructions Arising from σ, δ-Codes. *Journal of Mathematics*, 2021, 1–10.

[9] Boyd, S., & Vandenberghe, L. (2018). *Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares* (1st ed.). Cambridge University Press & Assessment.

[10] Bourbaki, N., *Elements of the History of Mathematics*, Springer-Verlag, 1994.

[11] Bradley, M., Franco-Russian engineering links: the careers of Lamé and Clapeyron, 1820-1830, *Ann. of Sci.* **38** (3), 1981, 291-312.

[12] Bronshtein, I. N., and Semendyayev, K. A., *Handbook of Mathematics*, 4th ed. New York: Springer-Verlag, 2004.

[13] Burton, D. M., and Van Osdol, D. H., "Toward the definition of an abstract ring." In *Learn from the Masters*, edited by F. Swetz et al., Mathematical Association of America, 1995, 241–251.

[14] Chasnov, J. R. (2018). *Matrix Algebra for Engineers*. The Hongkong University of Science and Technology.

[15] Cohn, H., *Advanced Number Theory*, Dover, 1980.

[16] Comaniciu, D., and Meer, P., "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), 1974.

[17] Comaniciu, D. I., "Nonparametric Robust Method for Computer Vision," Ph.D. Thesis, Rutgers, The State University of New Jersey, 2000.

[18] Cox, D., Little, J., and O'Shea, D., *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[19] Crilly, T., "Invariant Theory." *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, edited by I. Grattan-Guinness, Routledge, 1994, 787–793.

[20] Dedekind, R., *Gesammelte mathematische Werke* (Braunschweig, 1932).

[21] Dedekind, R., *Gesammelte mathematische Werke* - Reprint (New York, 1969).

[22] Dominguez, D., and Rodriguez, R., "Convergence of the Mean Shift using the Infinity Norm in Image Segmentation," *International Journal of Pattern Recognition Research*, 1, 2011, 3-4.

[23] Dummit, D. S., and Foote, R. M. (2004). *Abstract Algebra.* John Wiley Sons.

[24] Edwards, H. M., O Neumann and W Purkert, Dedekinds 'Bunte Bemerkungen' zu Kroneckers 'Grundzüge', *Arch. Hist. Exact Sci.* **27** (1), 1982, 49-85.

[25] Edwards, H. M., *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1977.

[26] Edwards, H. M., The genesis of ideal theory, *Arch. Hist. Exact Sciences* **23**, 1980, 321-378.

[27] Edwards, H. M., Dedekind's invention of ideals, *Bull. London Math. Soc.* **15** (1), 1983, 8-17.

[28] Edwards, H. M., Dedekind's invention of ideals, *Studies in the history of mathematics* (Washington, DC, 1987), 8-20.

[29] Edwards, H. M. (1980). *Galois Theory.* Springer-Verlag.

[30] Eisenbud, D., *Commutative Algebra, with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.

[31] Grothendieck, A., "Éléments de Géométrie Algébrique," *IHÉS Publications Mathématiques*, 1960–67. See also modern reviews in 2025.

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

[33] Faisol, A., & Fitriani, F. (2021a). The Ring Homomorphisms of Matrix Rings over Skew Generalized Power Series Rings. *Cauchy: Jurnal Matematika Murni Dan Aplikasi*, 7(1), 129–135.

[34] Faisol, A., & Fitriani, F. (2021b). The Ring Homomorphisms of Matrix Rings over Skew Generalized Power Series Rings. *Cauchy: Jurnal Matematika Murni Dan Aplikasi*, 7(1), 129–135.

[35] Goyal, D. R., & Khurana, D. (2023). A Characterization of Matrix Rings. *Bulletin of the Australian Mathematical Society*, 107(1), 95–101.

[36] J Gray, Wolfgang Krull, *European Mathematical Society Newsletter* **32**, 1999.

[37] Gray, J. J., "Early modern algebraic geometry." In *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, edited by I. Grattan-Guinness, Routledge, 1994, 920–926.

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

[39] Huynh, D. V., and Wisbauer, R., "A characterization of locally artinian modules," *J. Algebra*, 132, 2000, 287-293.

[40] Ireland, K., and Rosen, M., *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1982.

[41] Ismanto, I. (2018). Perluasan Sifat Rank Matriks Bujur Sangkar atas Ring Komutatif Ditinjau dari Determinannya. *Journal of Mathematics Education and Science*, 1(April), 21–28.

[42] Jordan, D. A., "Skew Derivations of Quantum Tori," *Journal of Algebra*, 2024.

[43] Judson, T. W. (2022). *Abstract Algebra: Theory and Applications*. Stephen F Austin State University.

[44] Kaygorodov, I. et al., "Transposed Poisson Structures on Witt-Type Algebras," *Communications in Algebra*, 2024.

[45] Kim, H., & Lim, J. W. (2020). Integral Domains in Which Every Nonzero w-Flat Ideal Is w-Invertible. *Mathematics*, 8(2), 1–11.

[46] Kline, M., *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, 1972.

[47] Krull, W., "On Dimension Theory in Rings," translated and discussed in *Adv. Algebraic Structures*, 2024.

[48] Krylov, P., & Tuganbaev, A. (2023). Formal Matrix Rings: Isomorphism Problem. *Mathematics*, 11(7), 1–5.

[49] Lang, Serge., *Undergraduate Algebra*, 3rd ed., Berlin, New York: Springer-Verlag, 2005.

[50] Luthar, S., and Passi, I. B. S., *Algebra*, Vol. 1-4, Narosa, 2004.

[51] MacDuffee, C. C., "Algebra's debt to Hamilton," *Scripta Math.*, 10, 1944, 25–35.

[52] McConnell, J. C., On Wedderburn's division algebra theorem of 1914, *Period. Math. Hungar.* **34** (3), 1997, 211–215.

[53] Nelson, M., "DG-Algebras and Gröbner Bases in Homological Algebra," *arXiv preprint arXiv:2403.08951*, 2024.

[54] Nastold, H. J., Wolfgang Krulls Arbeiten zur kommutativen Algebra und ihre Bedeutung für die algebraische Geometrie, *Jahresberichte der Deutschen Mathematiker-Vereinigung* **82** (2), 1980, 63–76.

[55] Nurhayani, M., Thresye, T., & Huda, N. (2019). Pembagi Nol pada Matriks atas Ring Komutatif. *Jurnal Matematika Murni dan Terapan: Epsilon*, 13(1), 56–64.

[56] Petik, T. (2021). On Characterization of Tripotent Matrices in Triangular Matrix Rings. *Turkish Journal of Mathematics*, 45(5), 1914–1926.

[57] Pinter-Lucke, James., "Commutativity conditions for rings: 1950–2005," *Expositiones Mathematicae*, 25(2), 2007, 165–174.

[58] Pratama, D. (2022). Kernel dan Sifatnya pada Translasi Naik dan Turun Ring Fuzzy Intuitionistik. *Mathline: Jurnal Matematika Dan Pendidikan Matematika*, 7(1), 40–52.

[59] Rodriguez, R., Torres, E., and Sossa, J. H., "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, 2011, 1–19.

[60] Rugayah, S., Faisol, A., & Fitriani, F. (2021). Matriks atas Ring Deret Pangkat Tergeneralisasi Miring. *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, 15(1), 157–166.

[61] Salayan, M., & Siregar, M. A. P. (2020). Studi Tentang Koleksi Ideal Dalam Ring Komutatif. *Prosiding Seminar Hasil Penelitian 2020 Universitas Muslim Nusantara Al Washliyah*, 189–197.

[62] Schöneborn, H., Verzeichnis der Veröffentlichungen von Wolfgang Krull, *Jahresberichte der Deutschen Mathematiker Vereinigung* **82** (2), 1980, 77–80.

[63] M. H. Stone, "The theory of representations for Boolean algebras," *Transactions of the American Mathematical Society*, vol. 40, pp. 37–111, 1936.

[64] M. H. Stone, "Applications of the theory of Boolean rings to general topology," *Transactions of the American Mathematical Society*, vol. 41, pp. 375–481, 1937.

[65] Van der Waerden, B. L., *A History of Algebra*, Springer-Verlag, 1985.

[66] Wedderburn, J. H. M., "On hypercomplex numbers," *Proc. Lond. Math. Soc.*, 6, 1907, 77–118.

[67] Wisbauer, R., "Semisimple and pure semisimple functor rings," *Comm. Algebra*, 18, 2001, 2343–2354.

[68] Wisbauer, R., "Local-global results for modules over algebras and Azumaya rings," *J. Algebra*, 135, 2002, 440–455.

[69] Wisbauer, R., "On modules with the Kulikov property and pure semisimple modules and rings," *J. Pure Appl. Algebra*, 70, 2004, 315–320.

[70] Wright, M. H., "Certain uniform modules over serial rings are uniserial," *Comm. Algebra*, 17, 2005, 441–469.

[71] Wisbauer, R., "Torsion Theories in Graded Division Rings," *Journal of Algebra and Its Applications*, 2024.

Citation: **Mahato. C.,** (2025) "Algebraic Foundations and Applications of Boolean and Matrix Rings", *Bharati International Journal of Multidisciplinary Research & Development (BIJMRD)*, Vol-3, Issue-07, July-2025.