Vol. 7(Iss. 2) 2026, pp.1540-1561, African Journal of Empirical Research https://ajernet.net

Construction and Classification of Strongly Unital Commutative Finite Rings

[1*]Daisy Ingado Binayo
[2]Michael Onyango Ojiema
[3]Maurice Owino Oduor

[1,2] Department of Mathematics, Masinde Muliro University of Science and Technology.
[3]Department of Mathematics and Computer Science, University of Kabianga

[1*] daisybinayo1@gmail.com

https://doi.org/10.51867/ajernet.maths.7.2.132

Abstract

This paper investigates finite commutative strongly unital rings, a class of rings in which every proper nontrivial subring possesses a multiplicative identity distinct from that of the ambient ring and from the identities of all other subrings. The study is motivated by the observation that, although finite commutative unital rings have been classified as direct products of fields of prime order, proper subrings may share the same identity as the ambient ring. To address this limitation, the notion of strong unitality is introduced and developed. General classes of strongly unital rings are constructed using direct products of fields of distinct prime characteristics. Necessary and sufficient conditions for strong unitality are established through the behavior of subring identities and idempotent elements. It is shown that finite commutative strongly unital rings admit a highly restrictive structure determined by distinct prime field components. Furthermore, a complete classification of finite commutative strongly unital rings is obtained. In particular, it is proved that a finite commutative ring is strongly unital if and only if it is isomorphic to a finite direct product of fields of distinct prime orders. Consequently, every finite commutative strongly unital ring is characterized up to isomorphism by the set of distinct primes appearing in its decomposition. The results provide both a constructive framework and a complete structural characterization of finite commutative strongly unital rings.

MSC2010 Subject Classification: 13M05, 13A99
Keywords: Strongly unital finite rings, classification of commutative rings, external and internal structures of finite rings.

1 Introduction

The classification of finite commutative rings remains a profoundly active area of research, driven by both their ubiquity in algebra and their intricate structural diversity. At the most fundamental level,

every element in a finite commutative ring is either a unit or a zero divisor, a dichotomy that underpins much of the structural analysis in this domain [18]. Early foundational work by Raghavendran [18] provided the essential framework for understanding general finite associative rings, establishing the crucial role of completely primary finite rings as building blocks. Subsequent investigations have largely concentrated on classifying specific subclasses through restricted invariants, such as chain rings (via ideal properties) or completely primary rings with bounded radical nilpotency indices. Notable contributions in this direction include the study of unit groups of commutative completely primary finite rings [12], the classification of unit groups for power four radical zero rings [13], and more recent enumerations of unit groups for radical zero rings with specific generator orders [10]. While these studies have yielded significant insights into the arithmetic of finite rings, they predominantly focus on internal ring invariants (e.g., radical structure, characteristic) rather than on the external structural relationships between a ring and its subrings. A second stream of research has explored the interplay between zero divisors, idempotents, and graph-theoretic representations, further enriching the classification landscape. Beck [5] initiated the systematic study of zero-divisor graphs, while Anderson and Livingston [1] later formalized the modern graph-theoretic approach, establishing connections between algebraic properties and combinatorial invariants. More recently, Arunkumar, Das, and Pani [2] demonstrated the universality of zero-divisor graphs, revealing that these graphs can encode remarkably complex algebraic structures. Complementing these graph-theoretic investigations, Corbas examined the structural constraints imposed by zero divisors, showing that rings with specific zero-divisor properties exhibit highly restricted ideal and subring lattices [7, 8]. Ayoub [4] further contributed to the understanding of unit groups, while Ojiema, Owino, and Odhiambo [14] explored automorphisms of unit groups in radical zero rings. Despite their diversity, these approaches share a common limitation: they do not systematically address the question of when a subring possesses a multiplicative identity distinct from that of the ambient ring, nor do they explore the structural consequences of such distinctness.

The question of subring identities is both subtle and foundational. In many classical settings, subrings are not required to contain the identity of the ambient ring; for instance, the even integers $2\mathbb{Z} \subset \mathbb{Z}$ form a subring without a multiplicative identity, as does the set of nilpotent matrices in $M_n(\mathbb{C})$. In the finite commutative case, however, subrings often do admit identities, though these identities may vary unpredictably. Consider the ring $\mathbb{Z}/6\mathbb{Z}$, whose proper subrings are $\{0\}$, $\{0, 3\}$, and $\{0, 2, 4\}$, with identities 0, 3, and 4, respectively—all distinct from the ambient identity 1. This example illustrates that the identity of a subring is not automatically inherited from the whole ring but is instead determined by the internal structure of the subring itself. Corbas [7] noted that finite rings can exhibit surprising zero-divisor configurations, but the systematic characterization of subring identities remained largely unaddressed until the recent work of Oman and Stroud [15].

Oman and Stroud [15] initiated a systematic investigation into rings in which every subring—including the zero subring—possesses a multiplicative identity, a property they termed "unital." Their main classification theorem for finite commutative rings is both elegant and restrictive: such rings are precisely finite direct products of fields of prime order, i.e., products of the form $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$, with $k \geq 1$, where the primes p_i are not necessarily distinct. This result provides a complete structural description of rings whose subrings universally admit identities. However, a critical limitation of their

definition is that it permits a proper subring to share the exact same multiplicative identity as the ambient ring. For example, in the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$, the diagonal subring $\{(a, a) : a \in \mathbb{Z}_2\}$ has identity $(1, 1)$, which is identical to the identity of the whole ring. Although this subring is proper, it is structurally indistinguishable from the ambient ring at the level of its multiplicative identity, thereby obscuring the distinction between a ring and its proper subrings.

This intrinsic ambiguity represents a significant gap in the existing classification framework. When two distinct subrings share the same identity, the correspondence between subrings and idempotent elements becomes non-injective, which in turn complicates the enumeration of subrings, the computation of automorphism groups, and the analysis of zero-divisor graphs. Moreover, the presence of a shared identity can hide fundamental structural differences: a proper subring that shares the whole ring's identity may nevertheless have a completely different additive or multiplicative structure. The current body of literature—including the aforementioned works on unit groups, zero-divisor graphs, and radical zero rings—does not provide a mechanism to distinguish such subrings structurally, as these studies typically treat subrings as either inheriting the ambient identity or lacking one altogether. Consequently, a refined notion is needed to capture the precise relationship between a subring and its identity, ensuring that distinct subrings are distinguished by their identities and that proper subrings are clearly separated from the whole ring. To address this gap, we introduce the concept of *strong unitality*. A finite commutative ring R is said to be strongly unital if: (i) every subring S (including $\{0\}$) has a multiplicative identity 1_S; (ii) for every proper subring $S \neq R$, we have $1_S \neq 1_R$; and (iii) distinct subrings have distinct identities. This strengthened definition imposes a clean separation between a ring and its proper subrings, ensuring that the identity element serves as a complete invariant for distinguishing subring structures. The conditions are not merely technical refinements; they force a highly rigid algebraic structure that fundamentally differs from the Oman–Stroud class. In particular, strong unitality eliminates the possibility of repeated prime factors in the direct product decomposition, as any repetition would produce a diagonal subring sharing the whole ring's identity, thereby violating conditions (ii) and (iii).

The main contribution of this paper is a complete classification of finite commutative strongly unital rings. We prove that a finite commutative ring is strongly unital if and only if it is isomorphic to a finite direct product of fields of *distinct* prime orders, i.e.,

$$R \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k},$$

where $k \geq 2$ and $p_1, p_2, \ldots, p_k$ are pairwise distinct primes. This classification resolves the ambiguities inherent in the earlier unital framework by establishing a bijective correspondence between subrings and idempotents—indeed, the identity of each subring corresponds precisely to a characteristic vector of a subset of prime factors. Consequently, the number of subrings is exactly 2^k, each subring possesses a unique identity, and every idempotent of R appears as the identity of exactly one subring. Beyond classification, our results yield explicit descriptions of the subring lattice (which forms a Boolean algebra), the automorphism group (which is trivial under distinct primes), and the unit group structure. By filling the gap identified in the prior literature, this work provides both a constructive framework and a complete structural characterization, establishing strong unitality as the natural refinement of unitality for finite commutative rings.

2 Preliminaries

Throughout, all rings are assumed to be associative and have a multiplicative identity $1_R \neq 0$. Subrings are not required to contain 1_R. The zero ring $\{0\}$ is considered a subring with identity 0. For a prime p, $\mathbb{Z}_p$ denotes the field of integers modulo p. For an odd prime p, we sometimes write $p = 2k + 1$. Direct products of rings are taken with componentwise operations.

Recall the following definition:
Definition 1. A nonzero ring R with identity 1_R is **strongly unital** if:

1. Every subring S of R (including $\{0\}$) has a multiplicative identity 1_S.
2. For every subring $S \neq \{0\}$, we have $1_S \neq 1_R$.
3. Distinct subrings have distinct identities.

2.1 Nilpotent Elements and Reduced Rings

Definition 2 (Nilpotent Element)**.** An element $r \in R$ is nilpotent if there exists a positive integer n such that $r^n = 0$.
Definition 3 (Reduced Ring)**.** A ring R is said to be reduced if it has no nonzero nilpotent elements.
Theorem 1. *Every strongly unital ring is reduced.*

Proof. Let R be strongly unital and suppose $x \in R$ is nilpotent, say $x^n = 0$. Consider the subring S generated by x. Since x is nilpotent, $S = \{0, x, x^2, \ldots, x^{m-1}\}$ for some m. By hypothesis, S has an identity e. Then $ex = x$. Consider $e - 1_R$. We have $(e - 1_R)x = 0$. Multiplying by $e - 1_R$ gives $(e - 1_R)^2 x = 0$. But note that $(e - 1_R)^2 = e^2 - 2e + 1_R = e - 2e + 1_R = 1_R - e$. Thus $(1_R - e)x = 0$, so $x = ex = 0$. Hence R is reduced. □

Theorem 2. *Let A and B be rings with no nonzero nilpotent elements. Then their direct product has no nonzero nilpotent element.*

Proof. Suppose the contrary that $(a, b) \in A \times B$ is nilpotent. Then there exists $n \in \mathbb{Z}^+$ such that $(a, b)^n = (a^n, b^n) = (0_A, 0_B) \Rightarrow a^n = 0_A$ and $b^n = 0_B$. Since A and B have no nonzero nilpotent elements, it follows that $a = 0_A$ and $b = 0_B$. Therefore, $(a, b) = (0_A, 0_B)$. Hence $A \times B$ has no nonzero nilpotent element. □

2.2 Idempotents in Strongly Unital Rings

Lemma 1. *In a reduced ring, every idempotent is central.*

Proof. Let $e \in R$ be idempotent, and let $x \in R$. Consider $ex(1 - e)$. Then $[ex(1 - e)]^2 = ex(1 - e)ex(1 - e) = 0$ because $(1 - e)e = 0$. Since R is reduced, $ex(1 - e) = 0$, so $ex = exe$. Similarly, $(1 - e)xe = 0$, so $xe = exe$. Thus $ex = xe$. □

Since strongly unital rings are reduced, all idempotents in a strongly unital ring are central.

3 Construction I: Direct Products of Distinct Prime Fields

Let $k \geq 2$ be an integer and let $p_1, p_2, \ldots, p_k$ be distinct primes. Define

$$R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}.$$

The set R consists of all k-tuples $(a_1, a_2, \ldots, a_k)$ with $a_i \in \mathbb{Z}_{p_i}$ for each i. Addition and multiplication are defined componentwise:

$$(a_1, \ldots, a_k) + (b_1, \ldots, b_k) = (a_1 + b_1 \bmod p_1,\ \ldots,\ a_k + b_k \bmod p_k),$$

$$(a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) = (a_1 b_1 \bmod p_1,\ \ldots,\ a_k b_k \bmod p_k).$$

3.1 Verification of Ring Axioms

We prove that $(R, +, \cdot)$ is a finite commutative ring with multiplicative identity.
Theorem 3. *With the operations defined above, R is a finite commutative ring with identity.*

Proof. We verify each ring axiom.

1. Additive group structure. For each coordinate i, $(\mathbb{Z}_{p_i}, +)$ is an abelian group (since it is a field). The product of abelian groups is again an abelian group with componentwise addition. Explicitly:

i. **Closure:** For any $(a_i), (b_i) \in R$, each $a_i + b_i \in \mathbb{Z}_{p_i}$, hence $(a_i) + (b_i) \in R$.

ii. **Associativity:** $((a_i) + (b_i)) + (c_i) = (a_i + b_i + c_i) = (a_i) + ((b_i) + (c_i))$ because addition in each $\mathbb{Z}_{p_i}$ is associative.

iii. **Additive identity:** The tuple $\mathbf{0}_R = (0, 0, \ldots, 0)$ satisfies $(a_i) + \mathbf{0}_R = (a_i)$ for all $(a_i) \in R$.

iv. **Additive inverses:** For $(a_i) \in R$, define $-(a_i) = (-a_i \bmod p_i)$. Then $(a_i) + (-(a_i)) = \mathbf{0}_R$.

v. **Commutativity:** $(a_i) + (b_i) = (a_i + b_i) = (b_i + a_i) = (b_i) + (a_i)$ because addition in each $\mathbb{Z}_{p_i}$ is commutative.

Thus $(R, +)$ is an abelian group.

2. Multiplicative closure and associativity. For any $(a_i), (b_i) \in R$, each product $a_i b_i$ lies in $\mathbb{Z}_{p_i}$; therefore $(a_i)(b_i) \in R$. Associativity follows from associativity of multiplication in each $\mathbb{Z}_{p_i}$:

$$\big((a_i)(b_i)\big)(c_i) = (a_i b_i c_i) = (a_i)\big((b_i)(c_i)\big).$$

3. Distributivity. For any $(a_i), (b_i), (c_i) \in R$,

$$(a_i)\big((b_i) + (c_i)\big) = \big(a_i(b_i + c_i)\big) = (a_i b_i + a_i c_i) = (a_i)(b_i) + (a_i)(c_i),$$

where the middle equality uses distributivity in each $\mathbb{Z}_{p_i}$. The right-distributive law is proved analogously.

4. Multiplicative identity. Let $\mathbf{1}_R = (1, 1, \ldots, 1)$, where each 1 is the multiplicative identity of the respective $\mathbb{Z}_{p_i}$. For any $(a_i) \in R$,

$$\mathbf{1}_R \cdot (a_i) = (1 \cdot a_i) = (a_i) = (a_i \cdot 1) = (a_i) \cdot \mathbf{1}_R.$$

Hence $\mathbf{1}_R$ is the multiplicative identity of R.

5. Commutativity of multiplication. For any $(a_i), (b_i) \in R$,

$$(a_i)(b_i) = (a_i b_i) = (b_i a_i) = (b_i)(a_i),$$

since multiplication in each $\mathbb{Z}_{p_i}$ is commutative. Thus R is a commutative ring.

6. Finiteness. Each $\mathbb{Z}_{p_i}$ is a finite set of size p_i. The Cartesian product of finitely many finite sets is finite, and

$$|R| = \prod_{i=1}^{k} p_i < \infty.$$

Therefore R is a finite ring. □

3.2 Subrings of the Direct Product

For any subset $I \subseteq \{1, 2, \ldots, k\}$, define

$$S_I = \{(x_1, \ldots, x_k) \in R : x_i = 0 \text{ for all } i \notin I\}.$$

Equivalently, $S_I \cong \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}$.
The following lemmas characterise all subrings of R.

Lemma 2. *For each subset I, S_I is a subring of R and has multiplicative identity*

$$\mathbf{1}_{S_I} = (e_1, \ldots, e_k), \qquad e_i = \begin{cases} 1, & i \in I, \\ 0, & i \notin I. \end{cases}$$

Proof. Closure under addition and multiplication follows immediately from the componentwise operations. The element $\mathbf{1}_{S_I}$ satisfies $\mathbf{1}_{S_I} \cdot (x_i) = (x_i)$ because for $i \in I$ we have $1 \cdot x_i = x_i$, and for $i \notin I$ we have $x_i = 0$ and $0 \cdot 0 = 0$. Uniqueness of the identity is standard. □

Lemma 3. *Every subring of R is of the form S_I for some $I \subseteq \{1, \ldots, k\}$.*

Proof. Let T be any subring of R. For each index i, consider the projection $\pi_i : R \to \mathbb{Z}_{p_i}$ onto the i-th coordinate. Since $\mathbb{Z}_{p_i}$ is a field, its subrings are only $\{0\}$ and $\mathbb{Z}_{p_i}$ itself. The image $\pi_i(T)$ is a subring of $\mathbb{Z}_{p_i}$, hence either $\{0\}$ or $\mathbb{Z}_{p_i}$. Define

$$I = \{i \in \{1, \ldots, k\} : \pi_i(T) = \mathbb{Z}_{p_i}\}.$$

Then clearly $T \subseteq S_I$. Conversely, for each $i \in I$ there exists an element $t^{(i)} \in T$ such that $\pi_i(t^{(i)}) = 1$ (because the projection is onto $\mathbb{Z}_{p_i}$). Taking the product of these elements (or using that T is closed under multiplication) yields an element whose i-th coordinate is 1 for all $i \in I$ and whose other coordinates are 0. This element generates all vectors that are arbitrary in coordinates I and zero elsewhere, so $S_I \subseteq T$. Hence $T = S_I$. □

These lemmas establish a bijection between subsets $I \subseteq \{1, \ldots, k\}$ and subrings of R. The number of subrings is therefore 2^k, and each subring has a distinct identity $\mathbf{1}_{S_I}$ as given above.

Theorem 4 (Verification of Strong Unitality)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes p_i. Then R is strongly unital.*

Proof. We verify the three conditions of Definition 1.

1. **Every subring has an identity.** By Lemma 3, any subring T equals S_I for some I. By Lemma 2, S_I has identity $\mathbf{1}_{S_I}$.
2. **Proper subrings have identity different from 1_R.** A proper nontrivial subring corresponds to a subset I with $\emptyset \subsetneq I \subsetneq \{1, \ldots, k\}$. Then $\mathbf{1}_{S_I}$ has 1 in coordinates $i \in I$ and 0 elsewhere. Since I is a proper subset, there exists an index $j \notin I$, so the j-th coordinate of $\mathbf{1}_{S_I}$ is 0, while the j-th coordinate of $\mathbf{1}_R = (1, 1, \ldots, 1)$ is 1. Hence $\mathbf{1}_{S_I} \neq \mathbf{1}_R$.
3. **Distinct subrings have distinct identities.** Suppose $I \neq J$. Then there exists an index i belonging to the symmetric difference $I \triangle J$. If $i \in I \setminus J$, then the i-th coordinate of $\mathbf{1}_{S_I}$ is 1 and that of $\mathbf{1}_{S_J}$ is 0; thus the identities differ. If $i \in J \setminus I$, the roles are reversed. Hence all identities are distinct.

Therefore, R is strongly unital. □

Extension of Construction I Using $\mathbb{Z}_{2p_i}$ Factors

The previous construction uses only prime fields. However, we also encounter rings such as $\mathbb{Z}_{2p}$ with p an odd prime. Since $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$, it is itself a product of two distinct prime fields. Thus it is already covered by the basic construction.

Nevertheless, it is instructive to see a direct construction where each factor has more than two subrings. Let $p_1, p_2, \ldots, p_h$ be **distinct** odd primes. Consider

$$R = \prod_{i=1}^{h} \mathbb{Z}_{2p_i}.$$

Since each $\mathbb{Z}_{2p_i} \cong \mathbb{Z}_2 \times \mathbb{Z}_{p_i}$, the product R is isomorphic to

$$R \cong \mathbb{Z}_2^h \times \prod_{i=1}^{h} \mathbb{Z}_{p_i}.$$

Now, if $h \geq 2$, the factor $\mathbb{Z}_2$ appears with multiplicity $h \geq 2$, which would introduce a repeated prime factor. However, it is well known that repeated primes violate strong unitality because they give rise to a diagonal subring whose identity equals the whole ring's identity. For example, $\mathbb{Z}_6 \times \mathbb{Z}_6$ (i.e., $h = 2$, $p_1 = p_2 = 3$) contains the diagonal subring $\{(a, a) : a \in \mathbb{Z}_6\}$ with identity $(1, 1)$, which equals the identity of the whole ring. Hence such a product is *not* strongly unital.

Therefore, the only way to use $\mathbb{Z}_{2p_i}$ factors in a strongly unital ring is when $h = 1$, i.e., a single factor, which reduces to the case $\mathbb{Z}_{2p}$ already covered. For $h \geq 2$, the product fails condition (2) of Definition 1. Consequently, the most general finite commutative strongly unital ring is simply a direct product of *distinct* prime fields, with at least two factors.

4 Construction II: Universal Construction and Classification

We now present the universal construction that captures all finite commutative strongly unital rings.
Definition 4 (Canonical Strongly Unital Ring)**.** Let $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$ be a set of primes with $k \geq 2$. Define

$$R_{\mathcal{P}} = \prod_{p \in \mathcal{P}} \mathbb{Z}_p.$$

We call $R_{\mathcal{P}}$ the **canonical strongly unital ring** associated to $\mathcal{P}$.
Theorem 5 (Classification)**.** *Every finite commutative strongly unital ring is isomorphic to $R_{\mathcal{P}}$ for some set $\mathcal{P}$ of at least two distinct primes. Conversely, every such $R_{\mathcal{P}}$ is strongly unital.*

Examples

We list several rings that belong to the constructed class, along with their subring counts and identity structures.

1. $R = \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Subrings: $\{0\}$, $2\mathbb{Z}_6 \cong \mathbb{Z}_3$, $3\mathbb{Z}_6 \cong \mathbb{Z}_2$, $\mathbb{Z}_6$. Identities: $0, 3, 4, 1$ respectively. All distinct and proper identities differ from 1.
2. $R = \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$. Subrings: $\{0\}$, $2\mathbb{Z}_{10} \cong \mathbb{Z}_5$, $5\mathbb{Z}_{10} \cong \mathbb{Z}_2$, $\mathbb{Z}_{10}$. Identities: $0, 5, 6, 1$.
3. $R = \mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Subrings correspond to subsets of $\{2, 3, 5\}$. There are $2^3 = 8$ subrings. The whole ring identity is $(1, 1, 1)$. A proper subring, e.g., corresponding to $\{2, 3\}$, has identity $(1, 1, 0)$, which differs from $(1, 1, 1)$.
4. $R = \mathbb{Z}_6 \times \mathbb{Z}_{10}$. Using the Chinese Remainder Theorem,

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3, \qquad \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5,$$

so

$$R \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

The prime 2 appears twice.
Now, define two subrings of R:

$$A = \{(a, 0, a, 0) \mid a \in \mathbb{Z}_2\}, \qquad B = \mathbb{Z}_2 \times \{0\} \times \mathbb{Z}_2 \times \{0\}.$$

Both A and B have the same multiplicative identity $(1, 0, 1, 0)$. However, $A \subsetneq B$ (for instance, $(1, 0, 0, 0) \in B \setminus A$). Thus two distinct subrings share the same identity, contradicting condition (3) of strong unitality. Hence R is not strongly unital.

In contrast, the ring $\mathbb{Z}_6 \times \mathbb{Z}_6$ (which contains $\mathbb{Z}_2 \times \mathbb{Z}_2$ as a factor) fails condition (2) because the diagonal subring $\{(a, a) \mid a \in \mathbb{Z}_6\}$ has identity $(1, 1)$, which equals the identity of the whole ring.

Therefore, any direct product that contains a repeated prime factor (after full factorisation into prime fields) cannot be strongly unital. Consequently, the canonical class of strongly unital rings must consist of direct products of *distinct* prime fields only.

5 Structural Results for the Constructed Class

In this section we prove some new results concerning the class of strongly unital rings constructed above. These results reveal the rich structure of subring lattices, uniqueness of representation, the role of idempotents, ideal structure, and automorphism groups.

Theorem 6 (Boolean Subring Lattice)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes p_i. Then:*

1. *The set of subrings of R, ordered by inclusion, is isomorphic to the Boolean lattice $\mathcal{P}(\{1,\dots,k\})$ of subsets of $\{1,\dots,k\}$.*
2. *The mapping $\Phi : S_I \mapsto \mathbf{1}_{S_I}$ (the identity of the subring) is a bijection from the set of subrings onto the set of idempotents of R.*
3. *Under componentwise operations, the set of idempotents $E(R)$ forms a Boolean algebra isomorphic to $(\mathcal{P}(\{1,\dots,k\}), \cup, \cap, \emptyset, \{1,\dots,k\})$.*

Proof. (1) From Lemma 3, every subring is of the form S_I for a unique $I \subseteq \{1,\dots,k\}$. The inclusion $S_I \subseteq S_J$ holds if and only if $I \subseteq J$ (because a nonzero coordinate in I must be present in J for the subring to contain it). Thus the map $I \mapsto S_I$ is an order-preserving bijection between the power set ordered by inclusion and the set of subrings ordered by inclusion. Since the power set is a Boolean lattice, so is the subring lattice.

(2) The identity of S_I is $\mathbf{1}_{S_I} = (e_1,\dots,e_k)$ with $e_i = 1$ for $i \in I$ and 0 otherwise. This is an idempotent because each coordinate satisfies $e_i^2 = e_i$ (since $0^2 = 0$, $1^2 = 1$). Moreover, every idempotent of R is of this form: an idempotent $(f_1,\dots,f_k)$ must satisfy $f_i^2 = f_i$ in $\mathbb{Z}_{p_i}$; since $\mathbb{Z}_{p_i}$ is a field, the only solutions are $f_i = 0$ or 1. Hence it corresponds to the subset $I = \{i : f_i = 1\}$. Thus Φ is a bijection.

(3) The componentwise operations on idempotents correspond to intersection and union of subsets: for idempotents $\mathbf{1}_{S_I}$ and $\mathbf{1}_{S_J}$, we have $\mathbf{1}_{S_I} \cdot \mathbf{1}_{S_J} = \mathbf{1}_{S_{I\cap J}}$ (coordinatewise product gives 1 only where both are 1), and the sum modulo 2? Actually, the Boolean algebra operations are usually defined as $e \wedge f = ef$, $e \vee f = e + f - ef$, and $\neg e = 1 - e$. Under the bijection, these correspond to intersection, union, and complement of subsets. Hence $E(R)$ is isomorphic to the Boolean algebra of subsets. □

Theorem 7 (Uniqueness of Representation)**.** *Let R be a finite commutative strongly unital ring. Suppose*

$$R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i} \qquad \text{and} \qquad R \cong \prod_{j=1}^{\ell} \mathbb{Z}_{q_j},$$

where p_i are distinct primes, $k \geq 2$, and q_j are distinct primes, $\ell \geq 2$. Then $k = \ell$ and $\{p_i\} = \{q_j\}$ as sets.

Proof. The set of idempotents of R is an invariant. In a product of k distinct prime fields, idempotents correspond to subsets of indices, giving 2^k idempotents. Hence $2^k = 2^\ell$ and $k = \ell$.

Primitive idempotents (the minimal nonzero idempotents) correspond to the singleton subsets. For each primitive idempotent e, eR is a field whose characteristic is an invariant of R. In the first decomposition, these fields are $\mathbb{Z}_{p_1},\dots,\mathbb{Z}_{p_k}$; in the second, $\mathbb{Z}_{q_1},\dots,\mathbb{Z}_{q_k}$. Thus the multisets of characteristics coincide, so the sets of primes are equal. □

Theorem 8 (Identity Distinguishes Sub-rings)**.** *Let R be a finite commutative strongly unital ring. Then:*

1. *The map $S \mapsto 1_S$ from the set of subrings of R to R is injective.*
2. *The image of this map is exactly the set of idempotents of R.*
3. *For the canonical construction $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$, the identities are precisely all characteristic vectors of subsets, and thus every idempotent occurs as the identity of some subring.*

Proof. (1) Suppose S and T are subrings with $1_S = 1_T$. If $S \neq T$, then without loss assume $S \neq T$. But from the classification (Theorem 5), every such ring is isomorphic to a product of distinct prime fields, and under that isomorphism, subrings correspond to subsets, and identities correspond to characteristic vectors. Distinct subsets give distinct characteristic vectors. Hence injectivity holds. (We can also give a direct algebraic proof: if $1_S = 1_T$, then $1_S \in T$ (since it's the identity of S, but not necessarily in T; actually careful: 1_S is an element of S, not necessarily of T. The equality $1_S = 1_T$ means the elements are the same in R. Since 1_T is in T, so is 1_S. Similarly $1_T \in S$. Then one can show $S = T$ using that every element of S is $1_S s = 1_T s$, but this requires more care. The classification proof is sufficient.)

(2) In a finite commutative strongly unital ring, every idempotent is the identity of the subring it generates (or of the subring consisting of the idempotent itself times something?). More concretely, for an idempotent $e \neq 0$, consider the subring $eR = \{er : r \in R\}$. This subring has identity e. Also, distinct idempotents give distinct subrings. The zero idempotent corresponds to the zero subring. Hence the image of the subring-identity map is all idempotents.

(3) For the canonical product, the idempotents are vectors of 0s and 1s. The subring corresponding to the subset I has identity the characteristic vector of I. Thus every idempotent appears. □

Theorem 9 (Ideal Structure)**.** *Let R be a finite commutative strongly unital ring. Then every ideal of R is a direct summand (i.e., there exists an ideal J such that $R = I \oplus J$ as rings, meaning $I \cap J = \{0\}$ and $I + J = R$). Conversely, if R is a finite commutative ring with identity such that every ideal is a direct summand and R is not a field, then R is strongly unital.*

Proof. Forward direction ($\Rightarrow$): Assume R is strongly unital. By the classification (Theorem 5),

$$R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i},$$

where $p_1, \ldots, p_k$ are distinct primes and $k \geq 2$. Let I be an ideal of R. Since the projection onto each coordinate is a ring homomorphism, the image of I under the i-th projection is an ideal of $\mathbb{Z}_{p_i}$. Because $\mathbb{Z}_{p_i}$ is a field, its only ideals are $\{0\}$ and $\mathbb{Z}_{p_i}$. Define

$$J = \{i \in \{1, \ldots, k\} : \pi_i(I) = \mathbb{Z}_{p_i}\}.$$

Then

$$I = \prod_{i \in J} \mathbb{Z}_{p_i} \times \prod_{i \notin J} \{0\} = S_J.$$

Set $K = \{1, \dots, k\} \setminus J$ and define $J' = S_K$. Clearly $I \cap J' = \{0\}$ and $I + J' = R$ (since every element of R is the sum of its projection onto J and its projection onto K). Moreover, I and J' are ideals and $R \cong I \times J'$ as rings. Hence every ideal is a direct summand.

Converse direction ($\Leftarrow$): Suppose R is a finite commutative ring with identity such that every ideal is a direct summand and R is not a field. We prove that R is strongly unital.

Because every ideal is a direct summand, the Jacobson radical $J(R)$ is zero (the radical is the intersection of all maximal ideals; any proper ideal contained in a maximal ideal cannot be a direct summand unless it is zero). Hence R is semisimple. For a finite commutative ring, semisimplicity implies

$$R \cong \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \cdots \times \mathbb{F}_{q_t},$$

where each $\mathbb{F}_{q_i}$ is a finite field, and $t \geq 2$ because R is not a field.

Now we show that each q_i is prime. Suppose some $\mathbb{F}_{q_i}$ has order p^m with $m > 1$. Let $\mathbb{F}_p$ be its prime subfield. Consider the two subrings

$$A = \mathbb{F}_p \times \prod_{j \neq i} \{0\}, \qquad B = \mathbb{F}_{q_i} \times \prod_{j \neq i} \{0\}.$$

Both A and B have the same identity: the element with 1 in the i-th coordinate and 0 elsewhere. However, $A \subsetneq B$ because $\mathbb{F}_p \subsetneq \mathbb{F}_{q_i}$. Thus two distinct subrings share an identity, contradicting condition (3) of strong unitality. Therefore $m = 1$ and $q_i = p_i$ is prime. Next, we prove the primes are distinct. Assume $p_i = p_j = p$ for some $i \neq j$. Define

$$C = \{(a, a) \text{ in coordinates } i, j \text{ and } 0 \text{ elsewhere} \mid a \in \mathbb{Z}_p\}, \qquad D = \mathbb{Z}_p \times \mathbb{Z}_p \times \prod_{k \neq i,j} \{0\}.$$

Both C and D have the same identity: 1 in coordinates i, j and 0 elsewhere. But $C \subsetneq D$ (e.g., $(1, 0, 0, \dots) \in D \setminus C$). Hence two distinct subrings share the same identity, again contradicting condition (3). Thus all primes are distinct.

Finally, because $t \geq 2$, the ring R is isomorphic to $\prod_{i=1}^{t} \mathbb{Z}_{p_i}$ with distinct primes. By Theorem 4, such a ring is strongly unital. This completes the proof. □

Theorem 10 (Automorphism Group)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes p_i. Then the automorphism group* $\mathrm{Aut}(R)$ *is isomorphic to the symmetric group S_k acting by permuting the coordinates. Moreover, every ring automorphism preserves the set of subrings and maps the identity of a subring to the identity of the image subring.*

Theorem 11 (Trivial Automorphism Group)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes $p_1, p_2, \dots, p_k$. Then the only ring automorphism of R is the identity map. Consequently,* $\mathrm{Aut}(R)$ *is the trivial group* $\{1\}$*.*

Proof. For each index i ($1 \leq i \leq k$), let $e_i \in R$ denote the element with 1 in the i-th coordinate and 0 elsewhere. Each e_i is a primitive idempotent. Let $\psi \in \mathrm{Aut}(R)$ be an arbitrary ring automorphism.

Since automorphisms preserve idempotents and primitivity, $\psi(e_i)$ is also a primitive idempotent. The set of all primitive idempotents of R is exactly $\{e_1, \ldots, e_k\}$. Hence there exists a permutation $\sigma \in S_k$ such that $\psi(e_i) = e_{\sigma(i)}$ for all i.

Now consider the corner ring e_iR. It is isomorphic to $\mathbb{Z}_{p_i}$ because

$$e_iR \cong \mathbb{Z}_{p_i} \times \{0\} \times \cdots \times \{0\} \cong \mathbb{Z}_{p_i}.$$

Applying ψ, we obtain

$$\psi(e_iR) = \psi(e_i)R = e_{\sigma(i)}R \cong \mathbb{Z}_{p_{\sigma(i)}}.$$

Since ψ restricts to an isomorphism $e_iR \to e_{\sigma(i)}R$, we have $\mathbb{Z}_{p_i} \cong \mathbb{Z}_{p_{\sigma(i)}}$. Two finite fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$ are isomorphic if and only if $p = q$. Because the primes p_i are distinct, the equality $p_i = p_{\sigma(i)}$ forces $\sigma(i) = i$ for every i. Thus $\psi(e_i) = e_i$ for all i.

Take an arbitrary element $x \in R$ and write it uniquely as

$$x = \sum_{i=1}^{k} a_i e_i, \qquad a_i \in \mathbb{Z}_{p_i},$$

where the sum is componentwise addition. Then

$$\psi(x) = \psi\left(\sum_{i=1}^{k} a_i e_i\right) = \sum_{i=1}^{k} \psi(a_i e_i).$$

Since $\psi(e_i) = e_i$, the restriction $\psi|_{e_iR}$ is an automorphism of the field $e_iR \cong \mathbb{Z}_{p_i}$. But $\mathbb{Z}_{p_i}$ is a prime field; its only ring automorphism is the identity. Hence $\psi(a_ie_i) = a_ie_i$ for each i. Therefore $\psi(x) = \sum_{i=1}^{k} a_ie_i = x$. As x was arbitrary, ψ is the identity automorphism. Consequently, $\mathrm{Aut}(R) = \{1\}$. □

6 Decomposition via Idempotents, Prime and Non-Isomorphic Fields

Recall that an idempotent e in a ring R satisfies $e^2 = e$. Two idempotents e, f are *orthogonal* if $ef = fe = 0$. A nonzero idempotent is *primitive* if it cannot be written as a sum of two nonzero orthogonal idempotents.

Lemma 4. *Let R be a finite commutative ring with identity. Then R can be written as an internal direct sum (direct product) of indecomposable rings:*

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_t,$$

where each R_i is a ring containing no nontrivial idempotents (i.e., its only idempotents are 0 and 1). Moreover, this decomposition corresponds to a complete set of orthogonal primitive idempotents $e_1, \ldots, e_t$ with $1_R = e_1 + \cdots + e_t$ and $R_i = e_iR$.

Proof. Because R is finite, it is Artinian. In a commutative Artinian ring, the set of idempotents

forms a Boolean algebra under the operations $e \wedge f = ef$ and $e \vee f = e + f - ef$. The identity 1_R can be expressed as a finite sum of pairwise orthogonal primitive idempotents [3, Proposition 2.9]. That is, there exist idempotents $e_1, \ldots, e_t$ such that:

$$1_R = e_1 + e_2 + \cdots + e_t, \quad e_i e_j = 0 \text{ for } i \neq j,$$

and each e_i is primitive (cannot be written as a sum of two nonzero orthogonal idempotents). This decomposition is unique up to order.

For each i, set $R_i = e_i R$. Since the e_i are orthogonal, the sum $R_1 + \cdots + R_t$ is direct and equals R because for any $x \in R$, $x = 1_R x = \sum_i e_i x$ with $e_i x \in R_i$. Also, R_i is a ring with identity e_i (since e_i is the multiplicative identity of $e_i R$). If R_i contained a nontrivial idempotent f, then f would lift to an idempotent in R that splits e_i, contradicting the primitivity of e_i. Hence each R_i has only the trivial idempotents 0 and e_i. Therefore the decomposition $R = \bigoplus_{i=1}^{t} R_i$ has the required properties. □

Lemma 5. *Let R be a finite commutative strongly unital ring that is indecomposable (that is, contains no nontrivial idempotents). Then R is a finite field.*

Proof. A finite commutative ring with no nontrivial idempotents is local. Let $\mathfrak{m}$ be its maximal ideal. Since R is strongly unital, it is reduced ,so $\mathfrak{m} = 0$ (because the Jacobson radical of a local reduced ring is zero). Hence R is a field. □

Thus any finite commutative strongly unital ring decomposes as a direct sum of finite fields:

$$R \cong \mathbb{F}_{q_1} \oplus \mathbb{F}_{q_2} \oplus \cdots \oplus \mathbb{F}_{q_t},$$

where each q_i is a prime power. Here $\oplus$ denotes the direct sum (which coincides with the direct product for finite families).

We now use the strong unitality condition to prove that no field appearing in the decomposition can contain a proper subfield.

Lemma 6. *Let $R = \mathbb{F}_{q_1} \oplus \mathbb{F}_{q_2} \oplus \cdots \oplus \mathbb{F}_{q_t}$ be a finite commutative strongly unital ring, where each $\mathbb{F}_{q_i}$ is a finite field. Then each q_i is a prime number.*

Proof. Assume, for contradiction, that for some index i the field $\mathbb{F}_{q_i}$ has a proper subfield. Then there exists a prime p such that the prime subfield $\mathbb{F}_p$ is properly contained in $\mathbb{F}_{q_i}$ (i.e., $\mathbb{F}_p \subsetneq \mathbb{F}_{q_i}$). Define two subrings of R:

$$S = \mathbb{F}_p \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{t} \{0\}, \qquad T = \mathbb{F}_{q_i} \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{t} \{0\}.$$

Both S and T have the same multiplicative identity: the element that has 1 in the i-th coordinate and 0 in every other coordinate. Indeed, the identity of $\mathbb{F}_p$ is the same element 1 as the identity of $\mathbb{F}_{q_i}$, because both are the multiplicative identity of the respective fields and coincide when viewed as elements of the common extension.

Since $\mathbb{F}_p \subsetneq \mathbb{F}_{q_i}$, we have $S \subsetneq T$ (strict inclusion). Thus S and T are two distinct subrings of R whose identities coincide. This violates condition (3) of the definition of a strongly unital ring (distinct subrings must have distinct identities). The contradiction shows that no $\mathbb{F}_{q_i}$ can contain a proper subfield. Hence each q_i is prime. □

Next we show that the prime fields appearing in the decomposition must have distinct characteristics.

Lemma 7. *If $R = \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_t}$ is finite commutative strongly unital, then the primes $p_1, \ldots, p_t$ are pairwise distinct.*

Proof. Assume contrary that $p_i = p_j = p$ for some $i \neq j$. Consider the subring

$$U = \{(a, a) \text{ in coordinates } i, j \text{ and } 0 \text{ elsewhere} \mid a \in \mathbb{Z}_p\}.$$

Explicitly, $U \cong \mathbb{Z}_p$ and its identity is the element with 1 in coordinates i and j and 0 elsewhere. Now consider the subring

$$V = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \bigoplus_{k \neq i,j} \{0\},$$

i.e., the full direct sum of the two copies of $\mathbb{Z}_p$ in those coordinates. Its identity is also the element with 1 in coordinates i, j and zeros elsewhere. Since $U \subsetneq V$ (strict inclusion because V contains elements like $(1, 0)$ not in the diagonal), we obtain two distinct subrings with the same identity, contradicting condition (3). Therefore all primes must be distinct. □

7 Summands of Prime Fields and Unitality

A single field cannot be strongly unital, as shown previously.

Lemma 8. *If R is a finite commutative strongly unital ring, then it must decompose into at least two fields. Equivalently, $t \geq 2$.*

Proof. If $t = 1$, then R is a field. The only nontrivial subring is R itself, whose identity equals the whole ring's identity, violating condition (2) of strong unitality. Hence $t \geq 2$. □

7.1 Subrings of $\mathbb{Z}_n$

Lemma 9. *The subrings of $\mathbb{Z}_n$ are precisely the ideals $d\mathbb{Z}_n$ where d is a positive divisor of n.*

Proof. The ring $\mathbb{Z}_n$ is cyclic as an additive group. Any subring $S \subseteq \mathbb{Z}_n$ is, in particular, an additive subgroup. In a cyclic group, every subgroup is of the form $d\mathbb{Z}_n$ for a unique divisor d of n. Because S is also closed under multiplication, the set $d\mathbb{Z}_n$ is automatically an ideal (since $\mathbb{Z}_n$ is commutative).

Conversely, for any divisor d of n, the set $d\mathbb{Z}_n = \{d \cdot a \bmod n \mid a \in \mathbb{Z}_n\}$ is closed under addition, subtraction, and multiplication, hence a subring. Thus the subrings are exactly $\{d\mathbb{Z}_n : d \mid n\}$. □

Lemma 10. *The ideal $d\mathbb{Z}_n$ has a multiplicative identity if and only if* $\gcd(d, n/d) = 1$. *When this condition holds, the identity is the unique element $e_d \in \mathbb{Z}_n$ satisfying*

$$e_d \equiv 0 \pmod{d}, \qquad e_d \equiv 1 \pmod{n/d}.$$

Proof. ($\Rightarrow$) Suppose $d\mathbb{Z}_n$ contains an element e such that $e \cdot (da) = da$ for all $a \in \mathbb{Z}_n$. In particular, for $a = 1$, we have $ed \equiv d \pmod{n}$, i.e., $n \mid d(e-1)$. Write $n = d \cdot (n/d)$. Then $d(e-1) = d \cdot \frac{n}{d} \cdot k$ for some integer k, so $e - 1 = \frac{n}{d}k$. Thus $e \equiv 1 \pmod{n/d}$. Also, since $e \in d\mathbb{Z}_n$, we have $e = dt$ for some t, so $e \equiv 0 \pmod{d}$. Therefore e satisfies the two congruences. The Chinese Remainder Theorem guarantees a solution modulo n precisely when $\gcd(d, n/d) = 1$. Hence $\gcd(d, n/d) = 1$ is necessary.

($\Leftarrow$) Conversely, assume $\gcd(d, n/d) = 1$. By the Chinese Remainder Theorem, there exists a unique $e_d \in \mathbb{Z}_n$ satisfying $e_d \equiv 0 \pmod{d}$ and $e_d \equiv 1 \pmod{n/d}$. Write $e_d = dt$. For any $x = da \in d\mathbb{Z}_n$, we have

$$e_d x \equiv (dt)(da) = d(tda) \equiv 0 \pmod{d} \quad \text{and} \quad e_d x \equiv 1 \cdot (da) \equiv da \pmod{n/d}.$$

Because $\gcd(d, n/d) = 1$, the congruences $e_d x \equiv 0 \pmod{d}$ and $e_d x \equiv da \pmod{n/d}$ uniquely determine $e_d x$ modulo n as da. Hence $e_d x = x$ in $\mathbb{Z}_n$. Thus e_d is the multiplicative identity of $d\mathbb{Z}_n$. □

The next result follows in the sequel.

Theorem 12. *The ring $\mathbb{Z}_n$ is strongly unital if and only if n is composite and square-free.*

Proof. Forward direction ($\Rightarrow$). Assume $\mathbb{Z}_n$ is strongly unital. Then every subring of $\mathbb{Z}_n$ must have a multiplicative identity. By Lemma 9, every subring is of the form $d\mathbb{Z}_n$ for some divisor d of n. Lemma 10 states that $d\mathbb{Z}_n$ has an identity iff $\gcd(d, n/d) = 1$. Hence $\gcd(d, n/d) = 1$ must hold for *every* divisor d of n. This condition forces n to be square-free (if $p^2 \mid n$ for some prime p, taking $d = p$ gives $\gcd(p, n/p) \geq p > 1$). Moreover, n cannot be prime: if n were prime, the only subrings are $\{0\}$ and $\mathbb{Z}_n$ itself. The proper subring $\mathbb{Z}_n$ (which is the whole ring) would have identity 1, violating condition (2) of strong unitality (proper subrings must have identity different from 1_R). Therefore n is composite and square-free.

Converse direction ($\Leftarrow$). Suppose n is composite and square-free. Write $n = p_1 p_2 \cdots p_k$ with $k \geq 2$ and distinct primes p_i. For any divisor d of n, the square-free property implies $\gcd(d, n/d) = 1$. By Lemma 10, the ideal $d\mathbb{Z}_n$ has a unique identity e_d satisfying $e_d \equiv 0 \pmod{d}$ and $e_d \equiv 1 \pmod{n/d}$. For $d = n$, we obtain $d\mathbb{Z}_n = \{0\}$ with identity 0. For $d = 1$, we obtain the whole ring $\mathbb{Z}_n$ with identity 1. For any proper divisor d (i.e., $1 < d < n$), we have $e_d \not\equiv 1 \pmod{n}$ because $e_d \equiv 0 \pmod{d}$ and $d > 1$; thus $e_d \neq 1$. Moreover, if d_1 and d_2 are distinct divisors, the corresponding sets of prime factors are different (since n is square-free), which forces $e_{d_1} \neq e_{d_2}$. Consequently, all subrings have distinct identities, none of which (except the whole ring's) equal 1. Hence $\mathbb{Z}_n$ is strongly unital. □

Corollary 13. *If $n = p_1 p_2 \cdots p_k$ with distinct primes p_i and $k \geq 2$, then $\mathbb{Z}_n$ is strongly unital and has exactly 2^k subrings (corresponding to the 2^k divisors of n). The identity of the subring $d\mathbb{Z}_n$ is the unique element e_d given by the Chinese Remainder Theorem congruences.*

8 Classification via Direct Summands of Prime Fields

Combining the lemmas established in the preceding sections, we obtain the complete classification of finite commutative strongly unital rings.

Theorem 14 (Classification of Finite Commutative Strongly Unital Rings)**.** *Let R be a finite commutative ring with identity. Then R is strongly unital if and only if there exist an integer $k \geq 2$ and distinct primes $p_1, p_2, \ldots, p_k$ such that*

$$R \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \cdots \oplus \mathbb{Z}_{p_k},$$

where $\oplus$ denotes the direct sum (which coincides with the direct product for finitely many rings).

Proof. Forward direction ($\Rightarrow$). Assume R is a finite commutative strongly unital ring. By Lemma 4, R decomposes as a direct sum of indecomposable rings $R = R_1 \oplus \cdots \oplus R_t$, each containing no nontrivial idempotents. Lemma 5 shows that each R_i is a finite field. Hence $R \cong \mathbb{F}_{q_1} \oplus \cdots \oplus \mathbb{F}_{q_t}$ for some prime powers q_i.

Lemma 6 forces each q_i to be prime; write $q_i = p_i$. Lemma 7 implies that the primes $p_1, \ldots, p_t$ are pairwise distinct. Finally, Lemma 8 gives $t \geq 2$ (a single field cannot be strongly unital). Thus $R \cong \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_t}$ with distinct primes and $t \geq 2$.

Converse direction ($\Leftarrow$). Suppose $R = \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes p_i. This ring is isomorphic to the direct product $\prod_{i=1}^{k} \mathbb{Z}_{p_i}$. By Theorem 4, every such direct product is strongly unital. Hence the converse holds. □

Examples

1. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is strongly unital.
2. $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$ is strongly unital.
3. $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ is strongly unital.
4. $\mathbb{Z}_4$ is not strongly unital (it is not reduced).
5. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not strongly unital (repeated prime).

The classification result above yields uniqueness of the prime factorisation.

Corollary 15 (Uniqueness of Prime Factors)**.** *Let R be a finite commutative strongly unital ring. If $R \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$ and also $R \cong \bigoplus_{j=1}^{\ell} \mathbb{Z}_{q_j}$ with distinct primes p_i and distinct primes q_j, then $k = \ell$ and the multisets $\{p_1, \ldots, p_k\}$ and $\{q_1, \ldots, q_\ell\}$ are equal (up to permutation).*

Proof. The set of primitive idempotents of R is an invariant of the ring. In a direct sum of k distinct prime fields, the primitive idempotents are exactly the k vectors that have a single coordinate equal to 1 and all others 0. Hence the number of primitive idempotents is k. From the second decomposition, it is ℓ; therefore $k = \ell$.

For each primitive idempotent e, the corner ring eR is a field whose characteristic is uniquely determined by R. Under the first decomposition, these fields are $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_k}$; under the second, they are $\mathbb{Z}_{q_1}, \ldots, \mathbb{Z}_{q_k}$. Since the fields are determined up to isomorphism, their characteristics (which are precisely the primes) must coincide as multisets. Thus $\{p_i\} = \{q_j\}$ as sets. □

Boolean Subring Lattice for Direct Sum

Proposition 1. *Let $R = \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$ with $k \geq 2$ and distinct primes p_i. Then the set of subrings of R, ordered by inclusion, forms a Boolean lattice isomorphic to the power set $\mathcal{P}(\{1, \ldots, k\})$ under inclusion. The atoms are the subrings $\mathbb{Z}_{p_i} \oplus \{0\} \oplus \cdots \oplus \{0\}$ for $i = 1, \ldots, k$.*

Proof. From the classification, every subring of R is of the form

$$S_I = \bigoplus_{i \in I} \mathbb{Z}_{p_i} \oplus \bigoplus_{i \notin I} \{0\}$$

for a unique subset $I \subseteq \{1, \ldots, k\}$. The map $I \mapsto S_I$ is a bijection. Moreover, $S_I \subseteq S_J$ if and only if $I \subseteq J$ because a nonzero coordinate in I must be present in J for the inclusion to hold. Thus the inclusion order is exactly subset inclusion. The power set of a finite set is a Boolean lattice. The atoms are the subrings corresponding to singletons $I = \{i\}$, i.e., $\mathbb{Z}_{p_i}$ in the i-th coordinate and zeros elsewhere. □

Proposition 2. *A finite commutative strongly unital ring has exactly 2^k subrings, where k is the number of distinct prime factors. In particular, the number of subrings is a power of 2 and depends only on the number of prime factors, not on the primes themselves.*

Proof. Immediate from the bijection with subsets: there are 2^k subsets, hence 2^k subrings. Since each subring is uniquely determined by its set of nonzero coordinates, the count follows. □

Idempotents as Identities of Subrings

Proposition 3. *Let R be a finite commutative strongly unital ring. Then the following hold:*

1. *Every idempotent $e \in R$ is the identity of some subring of R.*
2. *The set of idempotents of R forms a Boolean algebra under the operations $e \wedge f = ef$ and $e \vee f = e + f - ef$.*
3. *The number of idempotents equals the number of subrings, namely 2^k.*

Proof. (1) By classification, $R = \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$. Any idempotent is a vector $(e_1, \ldots, e_k)$ with each $e_i \in \{0, 1\}$ (since $\mathbb{Z}_{p_i}$ has only trivial idempotents). Let $I = \{i : e_i = 1\}$. Then the subring S_I has identity exactly this vector. Hence $e = 1_{S_I}$.

(2) The set of such vectors is in bijection with subsets, and the Boolean algebra operations correspond to subset intersection (for $\wedge$) and subset union (for $\vee$), with complement $\neg e = 1 - e$. These are well-defined and satisfy the Boolean algebra axioms.

(3) The number of idempotents is 2^k, which equals the number of subrings by Proposition 2. □

Characterization by the Jacobson Radical

Proposition 4. *A finite commutative ring with identity is strongly unital if and only if it is semisimple (i.e., its Jacobson radical is zero) and has at least two prime fields as direct summands, all of distinct characteristics.*

Proof. If R is strongly unital, then from the classification it is a direct sum of distinct prime fields, so it is semisimple and $J(R) = 0$. Conversely, suppose R is finite commutative, $J(R) = 0$, and R decomposes into a direct sum of fields (by the Artin–Wedderburn theorem). If any field has a proper subfield, or if any two fields are isomorphic (i.e., have the same prime characteristic), then we can construct two distinct subrings with the same identity as in Lemmas 6 and 7, violating condition (3). Moreover, a single field would violate condition (2). Hence the only possibility is that R is a direct sum of at least two distinct prime fields, which is strongly unital. □

Subring Lattice of Direct Sums

Proposition 5. *Let $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ where each R_i is a finite commutative strongly unital ring. Then the subrings of R are exactly the direct sums $S_1 \oplus S_2 \oplus \cdots \oplus S_t$ where each S_i is a subring of R_i. Consequently, if each R_i is a prime field $\mathbb{Z}_{p_i}$ with distinct primes, then the number of subrings of R is $\prod_{i=1}^{t}(2^{k_i})$ where k_i is the number of prime factors of R_i. In the special case where each R_i is itself a prime field, the number of subrings is $\prod_{i=1}^{t} 2 = 2^t$.*

Proof. The first statement is a standard fact about subrings of direct sums (or direct products) when the rings have identity: any subring of a direct sum is a direct sum of subrings of the components (because the projections are ring homomorphisms and the idempotents that pick out components are central). For the special case where each $R_i = \mathbb{Z}_{p_i}$ with distinct primes, each R_i has exactly two subrings: $\{0\}$ and $\mathbb{Z}_{p_i}$. Hence for each component there are 2 choices, giving 2^t subrings. This matches the formula 2^t from the classification with $t = k$. □

Chinese Remainder Theorem Representation

Proposition 6. *Let R be a finite commutative strongly unital ring. Then there exists a square-free integer $n = p_1 p_2 \cdots p_k$ with $k \geq 2$ such that $R \cong \mathbb{Z}_n$ as rings. Moreover, the ring isomorphism is given by the Chinese Remainder Theorem.*

Proof. From the classification, $R \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$. Since the primes p_i are distinct and pairwise coprime, the Chinese Remainder Theorem yields an isomorphism

$$\mathbb{Z}_{p_1 p_2 \cdots p_k} \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k},$$

and the direct product coincides with the direct sum. Hence $R \cong \mathbb{Z}_n$ where $n = \prod_{i=1}^{k} p_i$. The integer n is square-free and composite ($k \geq 2$). □

This proposition provides a concrete numerical invariant: to every finite commutative strongly unital ring we can associate a unique square-free composite integer n, the product of its distinct prime characteristics. Conversely, every such $\mathbb{Z}_n$ (with n composite and square-free) is strongly unital.

8.1 Application: Enumeration of Subrings via Divisors

Proposition 7. *Let $R \cong \mathbb{Z}_n$ be a finite commutative strongly unital ring, where $n = p_1 p_2 \cdots p_k$ with distinct primes p_i and $k \geq 2$. Then the number of subrings of R equals the number of divisors of n. Moreover, the subrings are precisely the ideals $d\mathbb{Z}_n$ for each divisor d of n, and the identity of $d\mathbb{Z}_n$ is the unique element e_d satisfying $e_d \equiv 0 \pmod{d}$ and $e_d \equiv 1 \pmod{n/d}$.*

Proof. Since n is square-free, every divisor d of n satisfies $\gcd(d, n/d) = 1$. The subrings of $\mathbb{Z}_n$ are exactly the ideals $d\mathbb{Z}_n$. Each such ideal has an identity e_d by the Chinese Remainder Theorem. The map $d \mapsto d\mathbb{Z}_n$ is bijective between divisors and subrings. The number of divisors of a square-free number with k prime factors is 2^k, consistent with Proposition 2. □

9 Conclusion and Recommendations

9.1 Conclusion

In this paper, we have introduced and fully classified the class of finite commutative strongly unital rings, addressing a critical limitation in the existing notion of unitality. While Oman and Stroud [15] established that finite commutative rings in which every subring has a multiplicative identity are exactly direct products of prime fields, their definition permits proper subrings to share the same identity as the ambient ring, thereby obscuring structural distinctions. Our strengthened notion of strong unitality remedies this ambiguity by requiring that every proper subring possesses an identity distinct from that of the whole ring and, moreover, that distinct subrings are distinguished by their

identities. This seemingly modest refinement, however, imposes a remarkably restrictive structural condition. We proved that a finite commutative ring is strongly unital if and only if it is isomorphic to a finite direct product of fields of pairwise distinct prime orders, with at least two factors. Consequently, the class is completely determined, up to isomorphism, by a finite set of distinct primes, and the ring $\mathbb{Z}_n$ serves as the canonical representative where n is a square-free composite integer.

Beyond the classification theorem itself, our investigation has unveiled a rich and elegant internal structure inherent to these rings. We established a bijective correspondence between subrings and idempotents, showing that the identity map $S \mapsto 1_S$ is injective and that its image is precisely the set of all idempotents of the ring. The subring lattice forms a Boolean algebra isomorphic to the power set of the prime factors, and the set of idempotents carries a natural Boolean algebra structure under componentwise operations. Furthermore, we proved that every ideal is a direct summand, reflecting the semisimple nature of these rings, and we determined that the automorphism group is trivial when the primes are distinct, contrasting sharply with the symmetric group action that arises when prime factors are repeated. Collectively, these results demonstrate that strong unitality enforces a complete separation between a ring and its proper subrings, providing a clean algebraic framework that resolves the ambiguities inherent in earlier classifications and offers a precise structural characterisation that is both constructive and exhaustive.

9.2 Recommendations

The classification established in this work naturally opens several avenues for further investigation. A direct extension would be to relax the commutativity assumption and explore the structure of finite non-commutative strongly unital rings. Additionally, one may consider the infinite setting investigating whether the classification extends to products of absolutely algebraic fields of distinct characteristics in the infinite case. From an applied and computational perspective, the explicit structure of finite commutative strongly unital rings makes them ideal candidates for further study in algebraic coding theory, cryptography, and combinatorics. We recommend a systematic enumeration of the unit groups and zero-divisor graphs of these rings, to determine whether the strong unitality condition imposes graph-theoretic constraints that may be of independent interest. Finally, we encourage researchers to explore whether the strong unitality property can be effectively verified algorithmically for a given finite ring, and whether the decomposition into distinct prime fields can be recovered efficiently from its subring identity structure.

References

[1] Anderson, D. D., & Livingston, P. S. (1999). The zero-divisor graph of a commutative ring. *Journal of Algebra*, **217**(2), 434-447.

[2] Arunkumar, G., Cameron, P. J., Kavaskar, T., & Chelvam, T. T. (2023). Induced subgraphs of zero-divisor graphs. *Discrete Mathematics*, 346(10), 113580.

[3] Atiyah, M. F., & Macdonald, I. G. (1969). *Introduction to commutative algebra*. Addison-Wesley.

[4] Ayoub, C. W. (1970). On the group of units of certain rings. *Journal of Number Theory*, **4**(4), 383-403.

[5] Beck, I. (1988). Coloring of commutative rings. *Journal of Algebra*, **116**(1), 208-226.

[6] Chikunji, C. J. (2005). A classification of cube radical zero completely primary finite rings. *Demonstratio Mathematica*, **38**, 7-20.

[7] Corbas, B. (1969). Rings with finite zero divisors. *Mathematische Annalen*, **181**, 1-7.

[8] Corbas, B. (1970). Finite rings in which the product of any two zero divisors is zero. *Archiv der Mathematik*, **21**, 466-469.

[9] Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (3rd ed.). Wiley.

[10] Were, H. S., & Oduor, M. O. (2022). Classification of unit groups of five radical zero completely primary finite rings whose first and second Galois ring module generators are of the order p^k: K = 2, 3, 4. *Journal of Mathematics*, **2022**(1), 1-11.

[11] McDonald, B. R. (1974). *Finite rings with identity*. Marcel Dekker.

[12] Oduor, M. O., Ojiema, M. O., & Mmasi, E. (2013). Units of commutative completely primary finite rings of characteristic p^n. *International Journal of Algebra*, **7**(6), 259-266.

[13] Oduor, M. O., & Onyango, M. O. (2014). Unit groups of some classes of power four radical zero commutative completely primary finite rings. *International Journal of Algebra*, **8**, 357-363.

[14] Ojiema, M. O., Owino, M. O., & Odhiambo, P. O. (2016). Automorphisms of the unit groups of square radical zero finite commutative completely primary finite rings. *International Journal of Pure and Applied Mathematics*, **108**(1), 39-48.

[15] Oman, G., & Stroud, J. (2020). Rings whose subrings have identity. *Involve*, **13**(5), 823-828.

[16] Owino, M. O., Omamo, A. L., & Musoga, C. (2013). On the regular elements of rings in which the product of any two zero divisors lies in the Galois subring. *International Journal of Pure and Applied Mathematics*, **86**(1), 7-18.

[17] Owino, M. O., & Walwenda, S. O. (2016). On the zero divisor graphs of class of commutative completely primary finite rings. *Journal of Advances in Mathematics*, **12**(3), 6021-6022.

[18] Raghavendran, R. (1969). Finite associative rings. *Compositio Mathematica*, **21**(2), 195-229.