CYCLIC RINGS

1. Introduction

The goal of this work is to explore cyclic rings, derive some results about these structures, and investigate how these results influence ring classification. Some basic facts from abstract algebra will be used without a proof supplied in this work. Also, although the focus of this work is ring theory, some results from number theory are needed, and one of these results will be used without a proof supplied in this work.

Many different definitions are commonly used for a ring. The following will be the working definition for a ring.

Definition. *Let R be a set with well-defined addition and multiplication operations. Then R is a ring if R is an abelian group under addition, the multiplication is associative, and multiplication distributes over addition.*

Note that, by the definition, a ring need not have a multiplicative identity. In some sections of this work, however, alternative definitions of a ring will be considered to see what proven facts would hold true even if a different definition were used for a ring.

If R is a ring, then R^+ will be used to refer to the additive group of R. The order of the additive group of R^+ will be referred to as both $|R|$ and the order of R. Also, 0_R will be used to denote the additive identity of R.

Some basic facts from group theory and number theory will be used in this work without proof. Readers who wish to see proofs of these results can refer to [3].

By the definition of a ring, R^+ must be abelian. The focus of this work will be on rings whose additive groups are cyclic. This is the motivation for the following definition.

Definition. *A ring R is a cyclic ring if R^+ is a cyclic group.*

2. Basic Facts about Cyclic Rings

One reason why the study of cyclic rings is important is that many familiar structures are cyclic rings. Among these are $\mathbb{Z}_n$ and $n\mathbb{Z}$ for any positive integer n. Cyclic rings are relatively easy to study because their additive structure forces them to have certain properties. For instance, if R is an infinite cyclic ring, r is a generator of R^+, and $a, b \in \mathbb{Z}$, then $ar = br$ if and only if $a = b$. If R is a finite cyclic ring of order n, r is a generator of R^+, and $a, b \in \mathbb{Z}$, then $ar = br$ if and only if $a \equiv b \bmod n$. Also, subrings of cyclic rings are cyclic rings. All three of these results follow immediately from elementary results about cyclic groups. Proofs shall be supplied for other basic properties of cyclic rings.

2.1. **Cyclic Rings and the Commutative Property.**

The following fact is well known and is stated in [4].

Lemma 1. *Cyclic rings are commutative under multiplication.*

Proof: Let R be a cyclic ring, r be a generator of R^+, and $s, t \in R$. Then there exist $a, b \in \mathbb{Z}$ with $s = ar$ and $t = br$. Since $st = (ar)(br) = (ab)r^2 = (ba)r^2 = (br)(ar) = ts$, it follows that R is commutative. □

2.2. **Subrings and Ideals of Cyclic Rings.**

The next lemma, which is proven in [2], is analogous to the theorem from group theory which states that every subgroup of an abelian group is normal.

Lemma 2. *Every subring of a cyclic ring is an ideal.*

Proof: Let R be a cyclic ring and r be a generator of R^+. Since R is a ring, then $r^2 \in R$. Let $k \in \mathbb{Z}$ with $r^2 = kr$. Let S be a subring of R. Then S is a cyclic ring. Let s be a generator of S^+. Since S is a subring of R, then $s \in R$. Thus, there exists $z \in \mathbb{Z}$ with $s = zr$.

Let $t \in R$ and $u \in S$. Then there exist $a, b \in \mathbb{Z}$ with $t = ar$ and $u = bs$. Since $tu = (ar)(bs) = (ar)[b(zr)] = (ar)[(bz)r] = (abz)r^2 = (abz)(kr) = (abkz)r = (abk)(zr) = (abz)s \in S$ and multiplication is commutative in R, it follows that S is an ideal of R. □

2.3. **Generators of Cyclic Rings.**

Given a ring R and a generator r of R^+, it is desirable to find all of the generators of R^+ in terms of r. For instance, the next lemma follows immediately from the fact that 1 and -1 are the only generators of $\mathbb{Z}^+$.

Lemma 3. *Let R be an infinite cyclic ring and r be a generator of R^+. Then r and $-r$ are the only generators of R^+.*

The next result immediately follows from the fact that, if $k \in \mathbb{Z}_n$, then k is a generator of $\mathbb{Z}_n^+$ if and only if $\gcd(k, n) = 1$.

Lemma 4. *Let R be a finite cyclic ring of order n, r be a generator of R^+, and $k \in \mathbb{Z}_n$. Then kr is a generator of R^+ if and only if* $\gcd(k, n) = 1$.

3. Constructing Cyclic Rings

A simple method exists for constructing a cyclic ring from a cyclic group. In order to define the multiplication for a cyclic group R, a generator r should be chosen. After that, let r^2 be any element of R. Finally, define multiplication for all elements as follows: If $a, b \in \mathbb{Z}$, then $(ar)(br) = (ab)r^2$. It is routine to check that, for any cyclic group, this procedure defines a multiplication such that the associative property of multiplication and the distributive property hold. Thus, for any cyclic group, this procedure does produce a cyclic ring. This method is demonstrated for $R = \{0_R, r, 2r, 3r\}$, a cyclic group of order four. Following are possible multiplication tables for R.

Before defining r^2:

$\cdot$	0_R	r	$2r$	$3r$
0_R	0_R	0_R	0_R	0_R
r	0_R	r^2	$2r^2$	$3r^2$
$2r$	0_R	$2r^2$	0_R	$2r^2$
$3r$	0_R	$3r^2$	$2r^2$	r^2

$r^2 = 0_R$:

$\cdot$	0_R	r	$2r$	$3r$
0_R	0_R	0_R	0_R	0_R
r	0_R	0_R	0_R	0_R
$2r$	0_R	0_R	0_R	0_R
$3r$	0_R	0_R	0_R	0_R

$r^2 = r$:

$\cdot$	0_R	r	$2r$	$3r$
0_R	0_R	0_R	0_R	0_R
r	0_R	r	$2r$	$3r$
$2r$	0_R	$2r$	0_R	$2r$
$3r$	0_R	$3r$	$2r$	r

$r^2 = 2r$:

$\cdot$	0_R	r	$2r$	$3r$
0_R	0_R	0_R	0_R	0_R
r	0_R	$2r$	0_R	$2r$
$2r$	0_R	0_R	0_R	0_R
$3r$	0_R	$2r$	0_R	$2r$

$r^2 = 3r$:

$\cdot$	0_R	r	$2r$	$3r$
0_R	0_R	0_R	0_R	0_R
r	0_R	$3r$	$2r$	r
$2r$	0_R	$2r$	0_R	$2r$
$3r$	0_R	r	$2r$	$3r$

4. Some Problems

The only other generator of R^+ is $3r$. What if it had been chosen instead of r to determine the multiplicative nature of R? When $r^2 = 0_R = 0r$, $(3r)^2 = 0_R = 0(3r)$, and, when $r^2 = 2r$, $(3r)^2 = 2r = 6r = 2(3r)$. Thus, in these cases, the relationship between a generator and its square is always the same regardless of which generator is chosen to define the multiplication. Unfortunately, this is not always true. For example, when $r^2 = r$, $(3r)^2 = r = 9r = 3(3r)$. Thus, the square of one generator is itself, but the square of the other generator is its triple. In this case, which generator should be chosen to define the multiplication of R? Another question is, given a cyclic group with generator r, which values of r^2 produce isomorphic rings? For the previous example, it can easily be verified that the only two cases that produce isomorphic rings are $r^2 = r$ and $r^2 = 3r$. This may yield a hint of how to determine in general which cyclic rings are isomorphic given a generator r of the additive group and the value of r^2. These problems will be remedied by investigating a certain concept.

5. The Solution: Behavior

5.1. **Definitions.**

Definition. *Let R be an infinite cyclic ring and k be a nonnegative integer. R has behavior k if R^+ has a generator r such that $r^2 = kr$.*

Definition. *Let R be a finite cyclic ring of order n and k be a positive divisor of n. R has behavior k if R^+ has a generator r such that $r^2 = kr$.*

5.2. **Theorems Regarding Existence and Uniqueness of Behavior.** It will be proven that, for any cyclic ring, behavior exists uniquely. Thus, behavior makes the choice of a generator to determine multiplication quite natural.

Theorem 1. *Any infinite cyclic ring has a unique behavior.*

Proof: Let R be an infinite cyclic ring and r be a generator of R^+. Then there exists $z \in \mathbb{Z}$ with $r^2 = zr$. If $z \geq 0$, the z is a behavior of R. If $z < 0$, then $-z > 0$. Note that $-r$ is a generator of R^+. Since $(-r)^2 = (-1)^2r^2 = (-1)^2(zr) = (-z)(-r)$, then $-z$ is a behavior of R. Thus, existence of behavior has been proven.

Let a and b be behaviors of R. Then R^+ has generators s and t such that $s^2 = as$ and $t^2 = bt$. If $s = t$, then $as = s^2 = t^2 = bt = bs$, causing $a = b$. If $s \neq t$, then $t = -s$. In this case, $as = s^2 = (-1)^2s^2 = (-s)^2 = t^2 = bt = b(-s) = -bs$, causing $a = -b$. Since a and b are nonnegative, then $a = b = 0$. Thus, uniqueness of behavior has been proven. □

Theorem 2. *Any finite cyclic ring has a unique behavior.*

Proof: Let R be a cyclic ring of order n and r be a generator of R^+ with $r^2 = ar$ for some $a \in \mathbb{Z}$. Let $k = \gcd(a, n)$ and $b \in \mathbb{Z}$ with $a = bk$. Since $\gcd(b, n) = 1$, then there exists $c \in \mathbb{Z}$ with $bc \equiv 1 \bmod n$. Since $\gcd(c, n) = 1$, then cr is a generator of R^+. Since $(cr)^2 = c^2r^2 = c^2(ar) = c^2(bkr) = c(bc)(kr) = k(cr)$, then k is a behavior of R. Thus, existence of behavior has been proven.

Let g and h be behaviors of R. Then g and h are positive divisors of n and R^+ has generators s and t with $s^2 = gs$ and $t^2 = ht$. Since t is a generator of R^+, then there exists $w \in \mathbb{Z}$ with $\gcd(w, n) = 1$ such that $t = ws$. Since $(hw)s = h(ws) = ht = t^2 = (ws)^2 = w^2s^2 = w^2(gs) = (gw^2)s$, then $gw^2 \equiv hw \bmod n$. Since $\gcd(w, n) = 1$, then $gw \equiv h \bmod n$. Since g and h are positive divisors of n and $\gcd(w, n) = 1$, then $g = \gcd(g, n) = \gcd(gw, n) = \gcd(h, n) = h$. Thus, uniqueness of behavior has been proven. □

Within the proof of the previous theorem, the following fact was also proven:

Remark. *If R is a finite cyclic ring of order n and r is a generator of R^+ with $r^2 = ar$ for some $a \in \mathbb{Z}$, then the behavior of R is $\gcd(a, n)$.*

5.3. **Investigation of Behavior.** It is well known that, for any ring, its order determines some of its properties. It turns out that, if a ring is cyclic, then its behavior determines some of its properties also. The next theorem leads to the conclusion that a cyclic ring is uniquely determined by its order and behavior. A similar theorem is proven in [4]; its proof is similar to the one given in this work.

Theorem 3. *Let R and S be cyclic rings. Then R and S are isomorphic if and only if they have the same order and the same behavior.*

Proof: Let R have behavior k and r be a generator of R^+ with $r^2 = kr$.

If R and S have the same order and the same behavior, then S has behavior k. Thus S^+ has a generator s with $s^2 = ks$. It is easy to show that the mapping $\varphi\colon R \to S$ defined by $\varphi(cr) = cs$ for every $c \in \mathbb{Z}$ is an isomorphism.

Conversely, if $R \cong S$, let $\psi\colon R \to S$ be an isomorphism. Then R and S must have the same order. If R is infinite, then S is also infinite, and k is a nonnegative integer. If R is finite, then k divides $|R| = |S|$. Since r is a generator of R^+ and ψ is an isomorphism, then $\psi(r)$ is a generator of S^+. Since $(\psi(r))^2 = \psi(r^2) = \psi(kr) = k\psi(r)$, it follows that S has behavior k. □

Because of the previous theorem, it will suffice to look at exactly one example of a cyclic ring of a given order and behavior. Up to isomorphism, all but one of these can be expressed as a subring of $\mathbb{Z}$ or $\mathbb{Z}_n$ for some suitable n.

Corollary 1. *An infinite cyclic ring with positive behavior k is isomorphic to $k\mathbb{Z}$.*

Proof: It is clear that $k\mathbb{Z}$ is an infinite cyclic ring and k is a generator of $k\mathbb{Z}^+$. Since $k^2 = k(k)$, then $k\mathbb{Z}$ has behavior k. The corollary follows from theorem 3. □

Corollary 2. *A finite cyclic ring of order n with behavior k is isomorphic to $k\mathbb{Z}_{kn}$.*

Proof: It is clear that $k\mathbb{Z}_{kn}$ is a cyclic ring and k is a generator of $k\mathbb{Z}_{kn}^+$. Since $|k\mathbb{Z}_{kn}| = |\langle k\rangle| = |k| = \frac{|1|}{\gcd(k,|1|)} = \frac{kn}{\gcd(k,kn)} = \frac{kn}{k} = n$ and $k^2 = k(k)$, then $k\mathbb{Z}_{kn}$ has order n and behavior k. The corollary follows from theorem 3. □

Up to isomorphism, the only cyclic ring that cannot be described as a subring of $\mathbb{Z}$ or $\mathbb{Z}_n$ is the infinite cyclic with behavior zero. The next definition deals with this case.

Definition. *Let* $\mathbf{B}$ *be the following subset of* $\mathbf{M_{2x2}}(\mathbb{Z})$*:*

$$\mathbf{B} = \left\{ \left(\begin{array}{cc} c & -c \\ c & -c \end{array} \right) \middle| \, \mathbf{c} \in \mathbb{Z} \right\}$$

Corollary 3. *An infinite cyclic ring with behavior zero is isomorphic to* $\mathbf{B}$.

Proof: It is clear that $\mathbf{B}$ is an infinite ring. It is also clear that $U \in \mathbf{B}$ if and only if there exists $u \in \mathbb{Z}$ with $U = \left(\begin{array}{cc} u & -u \\ u & -u \end{array} \right) = u \left(\begin{array}{cc} 1 & -1 \\ 1 & -1 \end{array} \right)$. Thus, $\mathbf{B}$ is a cyclic ring with generator $\left(\begin{array}{cc} 1 & -1 \\ 1 & -1 \end{array} \right)$. Since $\left(\begin{array}{cc} 1 & -1 \\ 1 & -1 \end{array} \right)^2 = \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right)$, the $\mathbf{B}$ has behavior zero. The corollary follows from theorem 3. □

There are cyclic rings whose definitions are similar to that of $\mathbf{B}$ that, by corollary 1 or corollary 2, are isomorphic to $k\mathbb{Z}$ or $k\mathbb{Z}_{kn}$ for some suitable k and n. For every positive integer k, the following subset of $\mathbf{M_{2x2}}(\mathbb{Z})$ is an infinite cyclic ring with behavior k:

$$\left\{ \left(\begin{array}{cc} c & c(k-1) \\ c & c(k-1) \end{array} \right) \middle| \, c \in \mathbb{Z} \right\}$$

For every positive integer n and every positive divisor k of n, the following subset of $\mathbf{M_{2x2}}(\mathbb{Z}_\mathbf{n})$ is a cyclic ring of order n with behavior k:

$$\left\{ \left(\begin{array}{cc} c & c(k-1) \\ c & c(k-1) \end{array} \right) \middle| \, c \in \mathbb{Z}_n \right\}$$

6. Consequences of Behavior

Corollaries 1, 2, and 3 indicate that behavior has a lot of influence over the structure of a cyclic ring and that, if the order and behavior of a cyclic ring are known, virtually all of its properties can be deduced.

6.1. **Zero Divisors of Cyclic Rings.**

It will first be shown that behavior and order determine which elements of a cyclic ring are zero divisors. The next theorem follows immediately from corollaries 1 and 3.

Theorem 4. *An infinite cyclic ring has zero divisors if and only if it has behavior zero.*

The following theorem is a consequence of corollary 2 and the fact that, if $n \in \mathbb{Z}$ with $n > 1$, then an element of $\mathbb{Z}_n$ is either a unit or a zero divisor and cannot be both.

Theorem 5. *Let R be a finite cyclic ring of order n with behavior k and r be a generator of R^+ with $r^2 = kr$. Then the set of zero divisors of R is*

$$D = \{zr | z \in \mathbb{Z} \text{ such that } z < n \text{ and } \gcd(kz, n) > 1\}.$$

Two corollaries follow naturally from this theorem.

Corollary 4. *A finite cyclic ring with composite order has zero divisors.*

Corollary 5. *If a finite cyclic ring R has behavior $k > 1$, then every element of R is a zero divisor.*

6.2. **Nilpotent Elements of Cyclic Rings.** Behavior and order also determine which elements of a cyclic ring a re nilpotent. The next theorem follows immediately from corollaries 1 and 3.

Theorem 6. *An infinite cyclic ring has nonzero nilpotent elements if and only if it has behavior zero.*

The next theorem deals with the finite case. It is also proven in [4] in a similar manner.

Theorem 7. *Let R be a finite cyclic ring of order n with behavior k and r be a generator of R^+ with $r^2 = kr$. Then the set of nilpotent elements of R is*

$$N = \{zr | z \in \mathbb{Z} \textit{ such that every prime divisor of } n \textit{ divides } kz\}.$$

Proof: By corollary 2, $R \cong k\mathbb{Z}_{kn}$. Thus, it will be enough to investigate the statement for rings of this form for any valid k and n..

Let $s \in N \subseteq k\mathbb{Z}_{kn}$. Thus, there exists $z \in \mathbb{Z}$ with $s = kz$. By the definition of N, every prime divisor of n divides kz. Thus, every prime divisor of n divides s. Because of this, it is clear that s is nilpotent.

Let t be a nilpotent element of $k\mathbb{Z}_{kn}$. Then there exists $z \in \mathbb{Z}$ with $t = kz$ and there exists a positive integer m with $t^m = 0$. Since $0 = t^m = (kz)^m$, then n divides $(kz)^m$. Therefore, every prime divisor of n divides kz. Hence, $t \in N$.

It follows that the nilpotent elements of R are exactly the elements of N. □

6.3. **Cyclic Rings in Relation to Integral Domains and Fields.** Behavior and order also determine if a cyclic ring is a field or an integral domain. Before investigating this, it will be useful to determine which cyclic rings have multiplicative identities.

6.3.1. *Cyclic Rings with Multiplicative Identities.* It turns out that behavior is the only aspect of a cyclic ring that determines if it has a multiplicative identity.

Theorem 8. *Let R be a cyclic ring. Then R has a multiplicative identity if and only if R has behavior one.*

Proof: Let R have a multiplicative identity. Let u be the multiplicative identity of R, k be the behavior of R, and r be a generator of R^+ with $r^2 = kr$. Let $m \in \mathbb{Z}$ with $u = mr$. Then $r = ur = (mr)r = mr^2 = m(kr) = (km)r$. If R is infinite, then $km = 1$, in which case, since k is nonnegative, then $k = m = 1$. If R is finite, then $km \equiv 1 \bmod |R|$, in which case $\gcd(k, |R|) = 1$. Since k divides $|R|$, then $k = 1$. In any case, R has behavior one.

Conversely, if R has behavior one, then R^+ has a generator s with $s^2 = s$. Let $t \in R$. Then there exists $a \in \mathbb{Z}$ with $t = as$. Since $st = ts = (as)s = as^2 = as = t$, it follows that s is the multiplicative identity of R. □

The previous theorem and the remark following theorem 2 yield that, for any positive integers a and b, the cyclic ring $a\mathbb{Z}_{ab}$ has a multiplicative identity if and only if $\gcd(a, b) = 1$. Also, within the proof of the previous theorem, the following fact was also proven:

Remark. *If a cyclic ring R has a multiplicative identity r, then r is a generator of R^+.*

A result from group theory is that, up to isomorphism, there is exactly one cyclic group of a given order. The following corollary shows that the same fact would hold for cyclic rings if one insists that a ring must have a multiplicative identity. The next corollary is also stated in [4].

Corollary 6. *Up to isomorphism, there is exactly one cyclic ring of a given order that has a multiplicative identity.*

Proof: Let R be a cyclic ring having a multiplicative identity. By the previous theorem, R has behavior one. If R is infinite, then, by corollary 1, $R \cong \mathbb{Z}$, and, if R has order n, then, by corollary 2, $R \cong \mathbb{Z}_n$. □

6.3.2. *Cyclic Rings That Are Fields.*

Theorem 9. *Let R be a cyclic ring. Then R is a field if and only if R has prime order and behavior one.*

Proof: If R is a field, then R has a multiplicative identity. By theorem 8, R has behavior one.

Suppose that the characteristic of R is zero. Then R is infinite. By corollary 1, $R \cong \mathbb{Z}$, which is not a field. Thus, the characteristic of R is not zero. Since R is a field, then the characteristic of R is a prime. Since R is a cyclic ring, then its characteristic and order are equal.

Conversely, if R is a cyclic ring of prime order p having behavior 1, then, by corollary 2, $R \cong \mathbb{Z}_p$, which is a field. □

The reader may determine which cyclic rings are integral domains but are not fields.

6.4. **A Further Investigation of Subrings of Cyclic Rings.** It has already been proven that subrings of cyclic rings are cyclic rings as well as ideals. Some more complex results, which involve the concept of behavior, will be proven in this section.

Given an infinite cyclic ring, it is quite easy to predict the order and behavior of its subrings. The next theorem deals with this topic.

Theorem 10. *Let R be an infinite cyclic ring with behavior k and r be a generator of R^+ with $r^2 = kr$. Then S is a subring of R if and only if there exists a nonnegative integer m such that mr is a generator of S^+. Moreover, if S is an infinite subring of R (that is, $m \neq 0$), then the behavior of S is km.*

The following corollary is an interesting fact about infinite cyclic rings. Its proof is left to the reader.

Corollary 7. *Let R be an infinite cyclic ring. Then R has behavior zero if and only if it is isomorphic to all of its nontrivial subrings.*

The following result, which ties together some of the previous results, shows that infinite cyclic rings of behavior zero are quite different from other infinite cyclic rings.

Theorem 11. *Let R be an infinite cyclic ring. Then the following are equivalent:*
R has behavior zero.
R contains a nonzero element that is a zero divisor.
Every element of R is a zero divisor.
R contains a nonzero nilpotent element.
Every element of R is nilpotent.
R is isomorphic to one of its proper subrings.
R is isomorphic to all of its nontrivial subrings.

Given a finite cyclic ring, it is easy to determine the order of its subrings. It is well known that, for any finite cyclic group and every positive divisor of its order, there exists a unique cyclic subgroup of that order. This fact for cyclic groups carries over to cyclic rings. Moreover, given the order and behavior of a finite cyclic ring R and the order of a subring S of R, the behavior of S can be determined. In [2], the authors prove a result that relates to the following theorem; however, the technique used in their proof is quite different from the following.

Theorem 12. *Let R be a finite cyclic ring of order n with behavior k. For every positive divisor d of n, there exists a unique subring S of R. Moreover, if a is the integer such that $ad = n$, then the behavior of S is $\gcd(ak, d)$.*

Proof: Let r be a generator of R^+ with $r^2 = kr$ and $a \in \mathbb{Z}$ with $ad = n$. Since d and n are positive, then a is a positive divisor of n. Let S be a subset of R such that ar is a generator of S^+. Then S^+ is a cyclic group under addition. Thus, S is a subring of R. Since $|S| = |\langle ar\rangle| = |ar| = \frac{|r|}{\gcd(a,|r|)} = \frac{n}{\gcd(a,n)} = \frac{ad}{a} = d$, then S has order d. The fact that S is the unique subring of R of order d follows from the discussion preceding the statement of the theorem.

Since ar is a generator of S^+ and $(ar)^2 = a^2r^2 = a^2(kr) = (ak)(ar)$, then, by the remark following theorem 2, S has behavior $\gcd(ak, d)$. □

A result that is useful here and is needed later is a result regarding the τ function. It takes positive integers as input and gives as its output the number of positive divisors of its input. It is proven in [3] that the following rules apply to τ:

1. If p is a prime and x is a nonnegative integer, then $\tau(p^x) = x + 1$.
2. If a and b are positive integers with $\gcd(ab) = 1$, then $\tau(ab) = \tau(a)\tau(b)$.

The τ function makes it easy to count the subrings, and thus the ideals, of a finite cyclic ring.

Corollary 8. *The number of subrings of a finite cyclic ring of order n is exactly $\tau(n)$.*

Proof: Let R be a finite cyclic ring of order n. By Lagrange's theorem, the order of a subring of a finite ring must divide the order of the ring. By the previous theorem, for every positive divisor d of n, there exists a unique subring R of order d. Since there are $\tau(n)$ positive divisors of n, it follows that there are $\tau(n)$ subrings of R. □

6.5. **Cyclic Rings in Relation to Principal Ideal Rings.** Behavior is the only aspect of a cyclic ring that determines if it is a principal ideal ring.

In the next proof, the notation used for principal ideals is the same as that used elsewhere for cyclic groups generated by an element. No confusion should arise, however, since this is the only proof in this work in which the notation refers to ideals.

Theorem 13. *A cyclic ring is a principal ideal ring if and only if it has behavior one.*

Proof: Let R be a cyclic ring with behavior k and r be a generator of R^+ with $r^2 = kr$.

If R has behavior one, then $r^2 = kr = 1r = r$. Let I be an ideal of R. Then I is a cyclic ring. Let i be a generator of I^+. Since I is a subring of R, then $i \in R$. Thus, there exists $b \in \mathbb{Z}$ with $i = br$.

Let $s \in I$. Then there exists $a \in \mathbb{Z}$ with $s = ai$. Since $s = ai = a(br) = (ab)r = (ab)r^2 = (ar)(br) = (ar)i \in \langle i \rangle$, then $I \subseteq \langle i \rangle$.

Let $t \in \langle i \rangle$. Then there exists $v \in R$ with $t = iv$, and there exists $c \in \mathbb{Z}$ with $v = cr$. Since $t = iv = (br)(cr) = (bc)r^2 = (cb)r = c(br) = ci \in I$, then $\langle i \rangle \subseteq I$. Since $I = \langle i \rangle$, then I is principal, and it follows that R is a principal ideal ring.

Conversely, if R is a principal ideal ring, then, since R is an ideal of itself, then R is principal. Let $w \in R$ such that $R = \langle w \rangle$. Since $r \in R = \langle w \rangle$, then there exists $x \in R$ with $r = wx$. Also, there exist $m, n \in \mathbb{Z}$ with $w = mr$ and $x = nr$. Thus, $r = wx = (mr)(nr) = (mn)r^2 = (mn)(kr) = (mnk)r$.

If R is infinite, then $mnk = 1$. Since k is nonnegative, then $k = 1$.

If R is finite, then $mnk \equiv 1 \bmod |R|$. Thus, $\gcd(k, |R|) = 1$. Since k divides $|R|$, then $k = 1$.

Since, in any case $k = 1$, then R has behavior one. □

It may be beneficial to look at some cyclic rings with behavior other than one in order to understand why they are not principal ideal rings. The first example that will be investigated is $2\mathbb{Z}_{12} = \{0, 2, 4, 6, 8, 10\}$. No principal ideal of this ring can contain 2, for example, because, by multiplying any two elements of this ring, a multiple of 4 is obtained. Similarly, in $3\mathbb{Z}$, no principal ideal can contain 3, and the most that a principal ideal of $3\mathbb{Z}$ can contain are the multiples of 9.

The next corollary follows immediately from theorem 8 and theorem 13.

Corollary 9. *Let R be a cyclic ring. Then the following are equivalent:*
R has behavior one.
R has a multiplicative identity.
R is a principal ideal ring.

The reader may determine which cyclic rings are principal ideal domains.

6.6. **Prime Ideals of Cyclic Rings.** One result that will eventually be proven here is that every prime ideal of a cyclic ring with finite index is maximal. Before proving this result, the forms of prime ideals of cyclic rings must be known. Some other interesting results involving prime ideals of cyclic rings will be proven along the way.

Because the trivial ideal is the only finite ideal of an infinite cyclic ring, then it must be considered separately. The following lemma indicates if the trivial ideal of an infinite cyclic ring is prime.

Lemma 5. *Let R be an infinite cyclic ring. Then $\{0_R\}$ is a prime ideal of R if and only if R has positive behavior.*

Proof: This follows immediately from the fact that R has nontrivial zero divisors if and only if R has behavior zero. □

Theorem 14. *Let R be cyclic ring with behavior k and I be an ideal of R such that $[R : I]$ is finite. Then I is prime if and only if there exists a prime p with $\gcd(k, p) = 1$ such that $[R : I] = p$.*

Proof: Let r be a generator of R^+ with $r^2 = kr$. Since I is a subring of R, then I is a cyclic ring.

If R is infinite, then, by theorem 10, there exists a nonnegative integer i such that ir is a generator of I^+. Since $[R : I]$ is finite, then I is infinite. Thus, $ir \neq 0_R$. Therefore, $i \neq 0$. By theorem 10, I has behavior ik.

If R is finite, then, in any case, $[R : I]$ is finite. Let n be the order of R and i be the smallest positive integer such that ir is a generator of I^+. Since $nr = 0_r \in I$, then $\gcd(i, n)r \in I$. Since $\gcd(i, n) \leq i$, then, by choice of i, i is a divisor of n. Since $|I| = |\langle ir\rangle| = |ir| = \frac{|r|}{\gcd(i,n)} = \frac{n}{i}$, it follows that $[R : I] = \frac{|R|}{|I|} = i$.

Suppose in either case that i is composite. Let $a, b \in \mathbb{Z}$ with $1 < a \leq b < i$ such that $ab = i$. Thus, ar and br are not elements of I. Since $(ar)(br) = (ab)r^2 = i(kr) = k(ir) \in I$, then I is not prime.

Suppose in either case that i is prime and that $\gcd(k, i) \neq 1$. Then $\gcd(k, i) = i$. Thus, i divides k. Let $z \in \mathbb{Z}$ with $k = iz$. Since $i \neq 1$, then $r \notin I$. Since $r^2 = kr = (iz)r = z(ir) \in I$, then I is not prime. It follows that, if I is prime, then i is a prime such that $\gcd(k, i) = 1$.

Suppose that R is infinite and that $k = 0$. If I is prime, then $1 = \gcd(k, i) = \gcd(0, i) = i$, contradicting that i is prime.

If R is infinite and I is prime, then, by corollary 1, $R \cong k\mathbb{Z}$, $I \cong ik\mathbb{Z}$, and it follows that $[R : I] = i$. Hence, in either case, if I is prime, then i is a prime such that $\gcd(k, i) = 1$ and $[R : I] = i$.

Conversely, if p is a prime with $\gcd(k, p) = 1$ such that $[R : I] = p$, then $k \neq 0$. Since $[R : I] = i$, then $i = p$. Thus, pr is a generator of I.

Let $c, d \in R$ with $cd \in I$. Then there exist $f, g, h \in \mathbb{Z}$ with $c = fr$, $d = gr$, and $cd = h(pr)$. Thus, $(hp)r = h(pr) = cd = (fr)(gr) = (fg)r^2 = (fg)(kr) = (fgk)r$. If R is infinite, then $hp = fgk$. If R is finite, then $hp \equiv fgk \bmod |R|$. In either case, p divides fgk. Since $\gcd(k, p) = 1$, then p divides fg. Since p is prime, then it can be assumed without loss of generality that p divides f. Since $c = fr \in I$, it follows that I is prime. □

The following theorem is useful for determining how many prime ideals an arbitrary finite cyclic ring has.

Theorem 15. *Let $p_1, \ldots, p_m$ be distinct primes, $a_1, \ldots, a_m$ be positive integers, $c_1, \ldots c_m \in \mathbb{Z}$ with $0 \leq c_j \leq a_j$ for every integer j with $1 \leq j \leq m$, z be the number of c_j that are equal to zero, $n = \prod_{j=1}^{m} p_j^{a_j}$, and $k = \prod_{j=1}^{m} p_j^{a_j}$. If R is a finite cyclic ring with order n and behavior k, then R has exactly z prime ideals.*

Proof: Let P be the set of all p_j such that $c_j = 0$, S be the set of all prime ideals of R, and I_x denote the element of S such that $|R| = x|I_x|$. Define $\varphi\colon P \to S$ by $\varphi(p_j) = I_{p_j}$. By theorems 12 and 14, φ is well defined.

Let $I_y \in S$. By theorem 14, y is a prime with $\gcd(k, y) = 1$ such that $n = |R| = y|I_y|$. Since y is a prime that divides n, then $y = p_t$ for some integer t with $1 \leq t \leq m$. Since $\gcd(k, p_t) = 1$, then p_t does not divide k. Thus, $c_t = 0$. Therefore, $p_t \in P$. Since $\varphi(p_t) = I_{p_t} = I_y$, then φ is surjective.

Let $p_g, p_h \in P$ with $\varphi(p_g) = \varphi(p_h)$. Then $I_{p_g} = i_{p_h}$. Since $p_g|I_{p_g}| = |R| = p_h|I_{p_h}| = p_h|I_{p_g}|$, then $p_g = p_h$. Therefore, φ is injective. Hence, φ is a bijection.

Since P contains z elements and a bijection exists between P and S, then S has z elements. It follows that R has exactly z prime ideals. □

6.7. **Maximal Ideals of Cyclic Rings.** In order to prove the promised results regarding prime and maximal ideals of cyclic rings, the forms of maximal ideals of cyclic rings must be known. Since every cyclic ring is isomorphic to either **B**, some subring of $\mathbb{Z}$, or some subring of $\mathbb{Z}_n$ for suitable n, then the next theorem follows from the properties that maximal ideals of these rings must have.

Theorem 16. *Let R be a cyclic ring and I be an ideal of R. Then I is maximal if and only if there exists a prime p such that $[R : I] = p$.*

Following is a result promised earlier.

Theorem 17. *Let R be a cyclic ring and P be a prime ideal of R such that $[R : P]$ is finite. Then P is a maximal ideal of R.*

Proof: Let R have behavior k. By theorem 14, there exists a prime p such that $\gcd(k, p) = 1$ and $[R : P] = p$. By theorem 16, P is a maximal ideal of R. □

The following theorem is useful for determining how many maximal ideals an arbitrary finite cyclic ring has.

Theorem 18. *Let n be a positive integer with m distinct prime divisors. If R is a finite cyclic ring of order n, then R has exactly m maximal ideals.*

Proof: Let P be the set of all prime divisors of n, S be the set of all maximal ideals of R, and I_x denote the element of S such that $|R| = x|I_x|$. Define $\varphi\colon P \to S$ by $\varphi(p) = I_p$. By theorems 12 and 16, φ is well defined.

Let $I_y \in S$. Then y is a prime such that $n = |R| = y|I_y|$. Since y is a prime divisor of n, then $y \in P$. Since $\varphi(y) = I_y$, then φ is surjective.

Let $a, b \in P$ with $\varphi(a) = \varphi(b)$. Then $I_a = I_b$. Since $a|I_a| = |R| = b|I_b| = b|I_a|$, then $a = b$. Therefore, φ is injective. Hence, φ is a bijection.

Since P contains m elements and a bijection exists between P and S, then S contains m elements. It follows that R has exactly m maximal ideals. □

7. Classification of Cyclic Rings

7.1. **A Specific Case: Zero Rings.** It is clear that, up to isomorphism, the only infinite cyclic ring that is a zero ring is **B**. It is also clear that, up to isomorphism, all finite cyclic rings that are zero rings are of the form $n\mathbb{Z}_{n^2}$ for some positive integer n.

Some obvious properties of zero rings are that all of their subrings are ideals and that they have no prime ideals. Also, two zero rings are isomorphic if and only if their additive groups are isomorphic. This has some obvious yet interesting consequences with respect to finite zero rings. The first is that every finite zero ring can be written as a product of cyclic rings. The second is that, for every positive integer n, up to isomorphism, the number of zero rings of order n is equal to the number of abelian groups of order n.

7.2. **The General Case.** Some additional results from group theory and number theory are needed in order to deal with the general case effectively.

7.2.1. *Preliminaries.*

Definition. *Let n be a positive integer. Then n is squarefree if, for every prime p, p^2 does not divide n.*

It is clear that a positive integer n is squarefree if and only if either $n = 1$ or there are distinct primes $p_1, \ldots, p_m$ such that $n = \prod_{j=1}^{m} p_j$.

The following lemma is well known.

Lemma 6. *Let G be a finite group with squarefree order. Then G is cyclic if and only if G is abelian.*

Proof: It is clear that G is cyclic implies that G is abelian.

If G has order one, then G is clearly cyclic. Thus, for the remainder of the proof, it will be assumed that G has more than one element.

Let G be an abelian group. Let $p_1, \ldots, p_m$ be distinct primes with $|G| = \prod_{j=1}^{m} p_j$. Let $g_1, \ldots, g_m \in G$ such that $|g_j| = p_j$ for every integer j with $1 \leq j \leq m$. Since $|G|$ is abelian, it can easily be shown that the element $\prod_{j=1}^{m} g_j$ has order $\prod_{j=1}^{m}$ and thus is a generator of G. It follows that G is cyclic. □

Any group of prime order is cyclic. The following is a condition on the order of a ring to guarantee that it is cyclic.

Lemma 7. *A finite ring with squarefree order is cyclic.*

Proof: Let R be a finite ring with squarefree order. Then R^+ is an abelian group with squarefree order. By the previous lemma, R^+ is a cyclic group. It follows that R is a cyclic ring. □

Some other definitions commonly used for a ring involve requiring the structure to have a multiplicative identity or not requiring that the multiplication be associative. Note that the only portion of the definition of a ring used to prove the previous lemma was that the structure is an abelian group under addition. Thus, no matter which of the mentioned definitions is used, the previous lemma holds.

7.2.2. *The Main Results.* The next two results are the main results of this work. In addition to their importance, these results, especially the first one, demonstrate a strong connection between ring theory and number theory. The next theorem is also proven in [4] and follows from a theorem proven in [1].

Theorem 19 (The Counting Theorem)**.** *Let n be a positive integer. Up to isomorphism, the number of cyclic rings of order n is exactly $\tau(n)$.*

Proof: By corollary 2, for every positive divisor k of n, up to isomorphism, $k\mathbb{Z}_{kn}$ is the only cyclic ring of order n with behavior k. Since the behavior of a cyclic ring must be a positive divisor of its order, then it is equivalent to count the positive divisors of n. Since there are $\tau(n)$ of these, it follows that, up to isomorphism, there are $\tau(n)$ cyclic rings of order n. □

The following corollary contains no mention of cyclic rings; however, its proof relies heavily on some of the facts that have been proven about these structures.

Corollary 10 (The Counting Corollary)**.** *Let n be a squarefree integer with m prime divisors. Up to isomorphism, the number of rings of order n is exactly 2^m.*

Proof: If $n = 1$, then $m = 0$ and $2^m = 2^0 = 1$. Up to isomorphism, there is only one ring of order one, and the statement is true in this case. Thus, for the remainder of the proof, it will be assumed that $n > 1$. Thus, $m > 0$.

By lemma 7, any ring of order n must be cyclic. Thus, by the counting theorem, up to isomorphism, there are $\tau(n)$ rings of order n.

Let $p_1, \ldots, p_m$ be distinct primes such that $n = \prod_{j=1}^{m} p_j$. Then

$$\tau(n) = \tau\left(\prod_{j=1}^{m} p_j\right) = \prod_{j=1}^{m} \tau(p_j) = \prod_{j=1}^{m} 2 = 2^m.$$

It follows that, up to isomorphism, there are 2^m rings of order n. □

Note that the counting theorem and the counting corollary hold even if the multiplication of a ring need not be associative. They do not hold, however, if a ring must have a multiplicative identity. Corollary 6 deals with this issue.

Acknowledgements

I would like to thank Dr. Leo Comerford for assisting me in clarifying proofs and finding relevant sources; the other thesis committee members: Dr. Duane Broline and Dr. Jonell Comerford; Dr. Patrick Coulton for encouraging me to create this thesis; and Dr. William Slough for showing me how to use TeX, which is the program with which this thesis was created.

Bibliography

[1] Kruse, Robert L. and Price, David T. *Nilpotent Rings.* New York: Gordon and Breach, 1969.

[2] Maurer, I. Gy. and Vincze, J. 'Despre Inele Ciclece.' *Studia Universitatis Babeş-Bolyai. Series Mathematica-Physica*, vol. 9 # 1. Cluj, Romania: Universitatea Babeş-Bolyai, 1964, pp. 25-27.

[3] Niven, Ivan; Zuckerman, Herbert S.; and Montgomery, Hugh L. *An Introduction to the Theory of Numbers.* New York: John Wiley and Sons, Inc., 1991.

[4] Peinado, Rolando E. 'On Finite Rings.' *Mathematics Magazine*, vol. 40 #2. Buffalo: The Mathematical Association of America, 1967, pp. 83-85.