Rings on the Direct Product of Two Cyclic Groups

by

Brett E. Leroux

A thesis submitted in partial fulfillment of the requirements
for graduation with Honors in Mathematics.

Whitman College

2014

Certificate of Approval

This is to certify that the accompanying thesis by Brett E. Leroux has been accepted in partial fulfillment of the requirements for graduation with Honors in Mathematics.

_____

Patrick W. Keef, Ph.D.

Whitman College

May 14, 2014

Abstract

The focus of this paper is a classification of rings whose additive group is the direct product of two cyclic groups. Such rings are represented by a quotient ring of the polynomials with integer coefficients. The paper begins with an overview of general ring theory including the Chinese Remainder theorem and the theory of local/irreducible rings. We then introduce Hensel's lemma which is later used as the main tool for classifying rings on the direct product of two cyclic groups. It is shown that two of these rings are isomorphic if and only if there is a solution to a particular quadratic equation in two variables mod n. We derive a new form of Hensel's lemma that applies directly to quadratic equations in two variables. It is used to systematically solve the quadratics in question and thus obtain a complete classification of rings on the direct product of two cyclic groups.

Contents

1 Introduction

Definition 1.1. *[3]*

A nonempty set R is a ring if it has two closed binary operations, addition and multiplication, satisfying the following conditions.

1. *$a + b = b + a$ for all $a, b \in R$.*

2. *$a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.*

3. *There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.*

4. *For every element $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.*

5. *$(ab)c = a(bc)$ for all $a, b, c \in R$.*

6. *$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.*

This can be summarized by saying that a ring is an additive abelian group with a second operation (multiplication) defined on it. The multiplicative operation must be associative and distribute over the addition. Therefore, every ring has an additive abelian group associated with it. If we ignore multiplication of the ring elements then the ring turns into its additive abelian group. This idea is the main motivation for this paper and will be our focus later. We will assume that a ring has a certain additive group associated with it and then ask how the structure of the additive group limits the possible ways that multiplication of the elements may be defined.

Before considering this problem, we will outline some basic finite commutative ring theory. The most important topics discussed are those that deal with the classification of rings. These include the Chinese Remainder theorem for rings, local/irreducible rings, and Wedderburn's little theorem. The Chinese remainder theorem allows one

to decompose a ring into the direct product of rings of prime power characteristic. In light of the Chinese Remainder theorem, when classifying rings it will be sufficient to consider rings of prime power characteristic. The theory of local/irreducible rings, which we will define later, allows one to decompose a ring into a direct product of local rings. This allows us to focus on local rings which have certain useful properties. Finally, Wedderburn's little theorem states that every finite division ring is a field. This extends our results in the section on finite fields to any finite division ring.

After stating these fundamental results, we will consider the problem of classifying rings with a given additive group. More specifically, we will assume that the additive group of a ring R is isomorphic to the direct product of two cyclic groups. Using R^+ to denote the additive group of R, we will be assuming that $R^+ \cong \mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ for some prime p and integers j and k. The question we are interested in is as follows: How many ways are there to define multiplication on the elements of $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ to form a commutative ring?

It is clear that if two rings are to be isomorphic then their additive groups must also be isomorphic. If we assume that we have two rings R and S such that $R^+ \cong S^+ \cong \mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$, another way of asking our question is the following: If we define multiplication in R a certain way and multiplication in S another way, when are R and S isomorphic as rings? That is, when are two seemingly different ways of defining multiplication actually the same?

To answer this question, we first establish that each ring of this type is associated with two integer parameters. One of these we call the *height* of the ring, the other is an element of $\mathbb{Z}_{p^j}$. It turns out that if two of these rings are isomorphic they must have the same height. For each possible height h, there are potentially p^j non isomorphic rings corresponding to the elements of $\mathbb{Z}_{p^j}$. We show from the basic properties of a ring

isomorphism that R and S are isomorphic if and only if there exists a root to a specific quadratic equation (determined by the parameters of the rings) in $\mathbb{Z}_{p^j}$.

Therefore, the problem of classifying rings on the direct product of two cyclic groups is reduced to the number theoretic problem of determining when certain quadratics have a root. The quadratic equations in question are messy and so we require an efficient method for determining when a solution exists. This method is provided to us by *Hensel's lemma*. We prove a variation on Hensel's lemma that allows us to determine when a given quadratic equation has a solution only by considering the *height* of the coefficients. Using Hensel's lemma we can very easily determine when quadratic equations have a solution and therefore when two given rings are isomorphic.

We conclude the paper by determining the isomorphism classes of rings with additive group $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$. We also count precisely how many rings there are. The reader who is familiar with finite commutative ring theory may wish to skip to section 5 where we begin the problem of classifying these rings.

2 Finite Commutative Ring Theory

Throughout the paper we assume that all rings have multiplicative identities, that is, there exists an element $1_R \in R$ such that $1_R a = a = a1_R$ for all $a \in R$. A ring is commutative if it satisfies $ab = ba$ for all $a, b \in R$. Some of the results in sections 1, 2, and 3 apply even to non-commutative rings. However, we are primarily interested in commutative rings.

Let R be a ring. Recall that a non-empty subset S of a ring is a subring of R if it is a ring with respect to the operations in R. The additive subgroup

$$S = \langle 1_R \rangle = \{n1 : n \in \mathbb{Z}\}$$

where 1_R is the multiplicative identity in R is a subring of R.

Definition 2.1. *[3] If the subring $S = \langle 1_R \rangle$ has infinite order, we say that the ring has characteristic 0. Otherwise, S is isomorphic to $\mathbb{Z}_n$, and we say that R has characteristic n.*

Another way of defining the characteristic of a ring is as the least positive integer n such that $na = 0$ for all $a \in R$. If no such integer exists, then the ring is said to have characteristic zero. The next proposition shows that this definition is the same as ours.

Proposition 2.1. *If R has characteristic n, then the order of every element under addition is a divisor of n. That is $na = 0$ for all $a \in R$.*

Proof. Let $x \in R$ and let k be the order of x. First note that $nx = (n1)x = 0x = 0$. This shows that $k \leq n$, so we can find q and r such that $n = kq + r$ and r is strictly less than k. Then,

$$0 = nx = (qk + r)x = qkx + rx = q(kx) + rx = 0 + rx = rx.$$

But $r < k$ so it must be that $r = 0$. So $n = kq$ and $k|n$. □

A special class of subrings is the set of ideals.

Definition 2.2. *[3] A non empty subset I of a ring R is an ideal of R if I is a subring of R and for all $r \in R$, $rI \subseteq I$ and $Ir \subseteq I$.*

Using ideals we can decompose a finite commutative ring into the direct product of rings of prime power characteristic. In the rest of this section we show how this can be done.

In a commutative ring, a *principal* ideal is one that is generated by a single element, i.e., I is principal if $I = (r) = \{rx : x \in R\}$ for some r in R. In fact every set of the form $(r) = \{rx : x \in R\}$ is an ideal of R. This happens even when R is not commutative. We have

Proposition 2.2. *Any subset of the form* $(r) = \{rx : x \in R\}$ *is an ideal of* R.

Proof. To see that (r) is a subring, note that

- The set (r) is not empty because $r \in R$.
- If $a, b \in (r)$, then $a = rx$ and $b = ry$ for some $x, y \in R$. Therefore, $ab = rxry = r(xry) \in (r)$ because $x, r, y \in R$.
- The element $a - b = rx - ry = r(x - y) \in (r)$ because $x - y \in R$.

Therefore (r) is a subring. To show that it is an ideal, take $rx \in (r)$ and $y \in R$. Then $rxy = r(xy) \in (r)$ because $xy \in R$. Similarly, $yrx = y(x + x + \cdots + x) = yx + yx + \cdots + yx = z + z + \cdots + z = rz \in (r)$ for some $z \in R$. This shows that (r) is an ideal. □

Ideals of a ring R can be used to form *quotient rings* R/I defined in the next proposition

Proposition 2.3. *Let* I *be an ideal of* R. *Then the quotient ring* R/I, *the set of additive cosets* $r + I$, *is a ring with operations defined by*

$$(r + I)(s + I) = rs + I$$

$$(r + I) + (s + I) = r + s + I$$

For a detailed discussion of quotient rings, the reader may consult [3].

Quotient rings provide us with the necessary tool to decompose any ring into the direct product of rings of prime power characteristic. This result is stated in the next theorem. It is a generalization of the Chinese Remainder Theorem.

Theorem 2.1 (Chinese Remainder Theorem)**.** *Suppose that R is a commutative ring of characteristic n where $n = rs$ and $(r, s) = 1$. Then the map*

$$f : R \to R/(r) \times R/(s)$$

given by $f(x) = (x + (r), x + (s))$ is a ring isomorphism.

Proof. It is easy to verify that this is a homomorphism of rings. So first we will show that f is surjective. To this end, note that since $(r, s) = 1$, there exists integers k and n such that $ns - kr = -1$. Therefore, $ns + 1 = kr$. Now, if we let $x = ns + 1 = kr$, then $f(x) = (kr + (r), ns + 1 + (s)) = ((r), 1 + (s)) = (0, 1)$ in the image. By precisely the same argument, we can define y so that $f(y) = (1, 0)$. Then given any $(a+(r), b+(s)) \in R/(r) \times R/(s)$, $f(ax + by) = (a + (r), b + (s))$. This shows that f is surjective.

Now, to show that this is a ring isomorphism, we need to show that the kernel of f is equal to $\{0\}$. But the additive identity in $R/(r) \times R/(s)$ is $((r), (s))$. So if $((r), (s)) = f(a) = (a + (r), a + (s))$ then a must be in both (r) and (s). It follows from this that the the order of a divides both r and s. Since $(r, s) = 1$, the order of a must be 1, and so a must be 0. □

To observe that the rings $R/(r)$ and $R/(s)$ have characteristic r and s respectively, first note that the multiplicative identity of $R/(r)$ is $1 + (r)$. Recall that the additive identity of R/I is (r). And it is clear that if x is less than r then $x + (r) \neq (r)$ and also that $r(1 + (r)) = (r)$. This shows that $R/(r)$ has characteristic r as desired.

To show that this allows us to decompose commutative rings into the direct product of rings of prime power characteristic, we can extend this result to an arbitrary number of quotient ring factors by induction. If R is a commutative ring of characteristic $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}$ then

$$R \cong R/({p_1}^{e_1}) \times R/({p_2}^{e_2}) \times \cdots \times R/({p_k}^{e_k}).$$

The characteristic of each $R/({p_i}^{e_i})$ is ${p_i}^{e_i}$.

In light of Theorem 2.1, when considering the problem of classifying commutative rings it will be sufficient to only consider rings that have prime power characteristic.

2.1 Finite Fields

In this section we obtain a complete classification for finite fields. The classification is as follows: Every field has prime power order. Furthermore, there is only one field of size p^k for each prime p and positive integer k. We state these results in theorems below after proving several preliminary results.

Theorem 2.2. *Let F be a field so that the nonzero elements of F, F^* form a group under multiplication. If G is a finite subgroup of F^* under multiplication then G is necessarily cyclic.*

Proof. Clearly G is abelian. By the Fundamental theorem of finite abelian groups,

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$$

for some $n_1, n_2, \cdots, n_k$ such that $n_k | n_{k-1} | \cdots | n_2 | n_1$. First, note that G certainly contains an element of order n_1. For any $(a_1, a_2, \cdots, a_k) \in Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$, all a_i satisfy $|a_i| \big| n_i \big| n_1$, which means that $({a_1}^{n_1}, {a_2}^{n_1}, \cdots, {a_k}^{n_1}) = 1$. Thus, all $x \in G$ satisfy

$x^{n_1} = 1$. But then every $x \in G$ is a root of the polynomial $x^{n_1} - 1$, of which there are at most n_1 in the field F. Therefore, $|G| \leq n_1$. Since we also know that $|G| \geq n_1$, it must be that $|G| = n_1$. Since G contains an element of order $n_1 = |G|$, G is cyclic. $\square$

Proposition 2.4. *Suppose that F is a field of characteristic p. Then the map ϕ defined by $\phi_F(x) = x^p$ is a ring homomorphism $F \to F$.*

Proof. To show that this is a ring homomorphism we compute

$$\phi_F(ab) = (ab)^p = a^p b^p = \phi_F(a)\phi_F(b).$$

$$\phi_F(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$

The only terms in this sum which do not have a factor of p are $\binom{p}{0}b^p$ and $\binom{p}{p}a^p$. Thus, it is equal to

$$a^p + b^p = \phi_F(a) + \phi_F(b).$$

This shows that $\phi_F(x)$ is a ring homomorphism. Furthermore, the map is one-to-one. To see this, note that if $\phi_F(a) = \phi_F(b)$, then $a^p = b^p$ so $0 = a^p - b^p = (a-b)^p$. This implies that $a - b = 0$ since there are no zero divisors in F, and hence $a = b$. Since F is finite, we have shown that ϕ is an isomorphism. $\square$

If $F = \mathbb{Z}_p$, then $\phi_F(1) = 1$, and $\phi_F(x) = \phi_F(1 + 1 + \cdots + 1) = 1 + 1 + \cdots + 1 = x$, so $\phi_F(x)$ is simply the identity mapping. Thus, for all $x \in \mathbb{Z}_p$, $x^p = x$, and so $x^p - x$ factors as

$$\prod_{i=0}^{p-1}(x - i).$$

Similarly as for $\phi_F(x)$, the map $\phi_F^k(x)$ defined by $\phi_F^k(x) = x^{p^k}$ is a ring homomorphism. Of course $(ab)^{p^k} = a^{p^k} b^{p^k}$ for all $a, b \in F$. To see that $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ for all k, we

will use induction. As our base case, we can use $(a+b)^p = a^p + b^p$, which was already shown. Now assume that $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ for some k. Then

$$(a+b)^{p^{k+1}} = ((a+b)^p)^{p^k} = (a^p + b^p)^{p^k} = ((a^p)^{p^k} + (b^p)^{p^k}) = a^{p^{k+1}} + b^{p^{k+1}}.$$

The map $\phi_F^k(x)$ is one to one since if $a^{p^k} = b^{p^k}$ then $0 = a^{p^k} - b^{p^k} = (a-b)^{p^k}$, and since F has no zero divisors, we know that $a = b$. So if F has p^k elements, then $\phi_F^k(x)$ is an isomorphism.

We are now ready to show that any two fields of the same size are isomorphic.

Proposition 2.5. *If F is a field with p^k elements, F is the splitting field for $x^{p^k} - x$ over $\mathbf{Z}_p$.*

Proof. Since F has p^k elements, the order of F^* is $p^k - 1$. Therefore, for all $x \in F^*$, $x^{p^k-1} = 1$ and so $x^{p^k-1} - 1 = 0$. This shows that every element of F is a root of $x^{p^k} - x$. Since $x^{p^k} - x$ has at most p^k roots, F has to contain all of its roots, and so $x^{p^k} - x$ factors as

$$\prod_{i=0}^{p^k} (x - a_i)$$

for $a_i \in F$.

Since F is simply made up of the roots of $x^{p^k} - x$, it is the splitting field. □

Theorem 2.3. *Any two fields with p^k elements are isomorphic.*

Proof. If F and E have p^k elements, they are both the splitting field for $x^{p^k} - x$ over $\mathbf{Z}_p$. Since splitting fields are unique up to isomorphism (see [7]), $F \cong E$. □

Theorem 2.4. *There exists a field F of order p^k.*

Proof. Let S be the splitting field of $f(x) = x^{p^k} - x$ over $\mathbf{Z}_p$. Since $f'(x) = (p^k)x^{p^k-1} - 1 = -1$, the derivative $f'(x)$ shares no roots with $f(x)$ and so $f(x)$ has no multiple roots. To show that the roots of $f(x)$ form a field, note several things,

- 0 and 1 are of course roots of f.
- The sum and product of two roots is a root as well: If a and b are roots of f, then $(a+b)^{p^k} - (a+b) = a^{p^k} - a + b^{p^k} - b = 0$ and $(ab)^{p^k} - ab = a^{p^k} b^{p^k} - ab = ab - ab = 0$, so $a + b$ and ab are roots as well.
- The additive inverses of roots are roots, that is, if a is a root, then its additive inverse $-a$ is also a root.
- Multiplicative inverses are included as well since $(1/a)^{p^k} - (1/a) = (1/a^{p^k}) - (1/a) = (1/a) - (1/a) = 0$.

This shows that the roots of $f(x)$ are a subset of S that form a field. But this subfield must be all of S since $f(x)$ splits in it and S is the minimum such field. Therefore, the splitting field of $f(x)$ is a field of order p^k. □

This completes the proof that there exists a unique field of order p^k for each prime p and positive integer k. We now classify the subfields of finite fields and the Galois groups of finite fields over their subfields.

Definition 2.3. *Let F_{p^n} denote the field on p^n elements.*

Lemma 2.1. *$p^m - 1 | p^n - 1$ if and only if $m|n$*

Proof. Let $n = qm + r$ for some integers q and r such that $r < m$. Then

$$p^n - 1 = p^{qm+r} - 1 = p^{qm}p^r - 1 = (p^{qm} - 1)p^r + (p^r - 1) = p^r(p^m - 1)(p^{(q-1)m} + p^{(q-2)m} + \cdots + 1) + (p^r - 1)$$

From this we see that $p^m - 1 | p^n - 1$ if and only if $p^r - 1 = 0$, in which case $r = 0$ and thus $m|n$. □

Theorem 2.5. *Given integers n and m, F_{p^n} has a subfield isomorphic to F_{p^m} iff $m|n$. Identifying this subfield with F_{p^m}, Gal$(F_{p^n} : F_{p^m})$ is a cyclic group of order n/m and is generated by the automorphism $\gamma(x) = x^{p^m}$.*

Proof. First suppose that we have an embedding $F_{p^n} \subseteq F_{p^m}$. F_{p^m} has dimension m over F_p and F_{p^n} has dimension n over F_p. Thus,

$$[F_{p^n} : F_{p^m}] \cdot m = [F_{p^n} : F_{p^m}] \cdot [F_{p^m} : F_p] = [F_{p^n} : F_p] = n$$

and so $m|n$.

Now assume that $m|n$. By the lemma, $p^m - 1 | p^n - 1$. Therefore, if x is a root of $x^{p^m} - x$, then x is a root of $x^{p^n} - x$. Therefore, all the roots of $x^{p^m} - x$ are in F_{p^n} and thus F_{p^n} contains a splitting field for $x^{p^m} - x$ which must be a subfield isomorphic to F_{p^m}.

Now we will show that $\text{Gal}(F_{p^n} : F_{p^m}) = \langle\gamma\rangle$. That $\text{Gal}(F_{p^n}; F_{p^m})$ has order at most n/m follows from general Galois theory (see for example [7]) and the fact that the dimension of F_{p^n} over F_{p^m} is n/m. To show that $\langle\gamma\rangle$ is a subgroup of $\text{Gal}(F_{p^n} : F_{p^m})$ of order n/m first note that $\gamma \in \text{Gal}(F_{p^n} : F_{p^m})$ since $x^{p^m} = x$ for all $x \in F_{p^m}$ so γ fixes F_{p^m}. And $|\gamma|$ divides n/m because $\gamma^{n/m} = x^{p^n}$ is the identity automorphism on F_{p^n}. Furthermore, $|\gamma|$ is actually equal to n/m since for any $i < n$, $\gamma^{i/m} \neq \text{id}$ since $x^{p^i} - x$ has only p^i roots and so $\gamma^{i/m}$ cannot fix all of F_{p^n}. This combined with the fact that $\text{Gal}(F_{p^n} : F_{p^m})$ has order at most n/m shows that $\text{Gal}(F_{p^n} : F_{p^m}) = \langle\gamma\rangle$. □

2.2 Nilpotent Elements and the Nilradical

In this section we assume that R is commutative. Recall that an ideal P is prime if $P \neq R$ and if $ab \in P$ then $a \in P$ or $b \in P$. It turns out that the intersection of all the prime ideals of a finite commutative ring R is the collection of *nilpotent* elements in R. As a reference for the definitions in the rest of section 2 see [8].

Definition 2.4. *An element $x \in R$ is said to be nilpotent if for some positive integer n, $x^n = 0$. The set of nilpotent elements in R is called the nilradical.*

In this section we introduce nilpotent elements and concluded with a proof that, in a finite commutative ring, the set of nilpotent elements, the nilradical, is equal to the intersection of the prime ideals.

A nilpotent element is never a unit, because if n is an integer such that $x^n = 0$ and there exists an x^{-1} such that $xx^{-1} = 1$, then $0_R = x^n(x^{-1})^n = 1_R$, a contradiction. We begin with

Proposition 2.6. *If R is commutative, then the nilradical, denoted N, is an ideal.*

Proof. To see this, first we will show that N is an additive subgroup. Obviously, $0_R \in N$. Furthermore, if $a, b \in N$ and $a^n = b^m = 0$, then

$$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

If $k \geq n$, then $a^k = 0$ and if $k < n$, then $b^{n+m-k} = 0$. Therefore, all of the terms in the sum are zero. Thus, $(a+b)^{n+m} = 0$ and so $a + b \in N$. Also, $(-a)^n = (-1)^n a^n = 0$ so $-a \in N$. This shows that N is an additive subgroup of R. Finally, note that for any $r \in R$ and any nilpotent element x such that $x^n = 0$, $(rx)^n = r^n x^n = 0$ and $(xr)^n = x^n r^n = 0$. This shows that N is an ideal. □

We can show that this result fails for non-commutative rings. If we let R be the collection of 2×2 matrices and define A and B as

$$A = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$$

then A and B are nilpotent elements but their sum,

$$A + B = \begin{bmatrix} -2 & 0 \\ 0 & 2 \end{bmatrix}$$

is an invertible matrix, and hence a unit. This means that N is not an additive subgroup and so it cannot be an ideal. This was the reason for our assumption in this section that R is commutative. Thus Proposition 2.6 applies; the nilradical is an ideal. Recall that we will eventually be showing that N is the intersection of the prime ideals of R. Since the intersection of any collection of ideals is an ideal, it will follow that N is an ideal. However, proving that N is an ideal directly serves to highlight the difference between the commutative case and the non-commutative case. We continue with

Proposition 2.7. *If x is any nilpotent element in R and u is a unit then $u - x$ is a unit.*

Proof. First we will prove a simpler result: If x is a nilpotent element then $1 - x$ is a unit. To see that this is true, if we let $x^n = 0$, then

$$1 = 1 - x^n = (1 - x)(x^{n-1} + x^{n-2} + \cdots + 1)$$

so $(x^{n-1} + x^{n-2} + \cdots + 1)$ is an inverse for $1 - x$. Now let u be any unit and let v be the inverse for u. Then $(xv)^n = x^n v^n = 0$ so xv is nilpotent. By the first part, $1 - xv$

is a unit. Let w be the inverse for $1 - xv$. Then we have that

$$wv(u - x) = wv(u - (uv)x) = wvu(1 - xv) = w(1 - xv) = 1.$$

This shows that wv is an inverse for $u - x$. □

Now we state a series of results concluding with a proof that the set of nilpotent elements in R is equal to the intersection of the prime ideals.

Proposition 2.8. *If R is commutative, and P is a prime ideal of R, then $N \subseteq P$.*

Proof. Since P is a prime ideal, R/P is an integral domain. So if x is a nilpotent element not contained in P, then $x + P$ and $x^{n-1} + P$ are two non-identity elements in R/P such that $(x + P)(x^{n-1} + P) = x^n + P = P$, which means that they are zero divisors, a contradiction to the fact that R/P is an integral domain. Thus, every nilpotent element is contained in P. □

For the proof of the following theorem we need

Definition 2.5. *Suppose R is a commutative ring and let a be any element of R and P any subset of R. By (a, P) we mean the smallest ideal containing both a and P. The set (a, P) can be written formally as $\{r_0a + r_1p_1 + \cdots + r_np_n : n \in \mathbb{Z}^+, r_i \in R, p_i \in P\}$. We refer to (a, P) as the ideal generated by a and P.*

This can be used to prove

Proposition 2.9. *Suppose R is a commutative ring and $x \in R$ is not nilpotent. Let P be an ideal that is maximal with respect to the property that $P \cap \{x^k : k \in \mathbb{N}\} = \emptyset$. Then P is necessarily a prime ideal.*

Proof. let $ab \in P$. Assume for a contradiction that $a \notin P$ and $b \notin P$. Then the ideals generated by a, P and b, P, (a, P) and (b, P) respectively, properly contain P, and therefore since P was maximal with respect to the property $P \cap \{x^k : k \in \mathbb{N}\} = \emptyset$, then (a, P) and (b, P) must contain some power of x. Let $x^m \in (a, P)$ and $x^n \in (b, P)$. Then $x^{m+n} \in (ab, P)$, but since $ab \in P$, this means that $x^{m+n} \in P$, a contradiction. Therefore, one of a, b is in P. And this proves that P is prime. □

Theorem 2.6. *If R is any finite commutative ring then N is the intersection of the prime ideals of R.*

Proof. If x is nilpotent, then by Proposition 2.8, x is in any prime ideal of R, so x is in the intersection. Furthermore, if y is not nilpotent then by Proposition 2.9, there exists a prime ideal that does not contain y. This shows that N is precisely the intersection of the prime ideals of R. □

In fact, this result applies even when R is allowed to be infinite. In this case, we have to use *Zorn's Lemma* to construct the prime ideal mentioned in 2.9. In the case we proved, where R is finite, we are able to construct the ideal P that is maximal simply because any finite partially ordered set necessarily has maximal elements. See [8] for a discussion of Zorn's Lemma and partially ordered sets in relation to maximal ideals.

2.3 The Jacobson Radical

Similarly to how we define congruence of integers by some modulus, given an ideal in a commutative ring we can define congruence of elements in the ideal. If $I \subseteq R$ is an ideal and $x, y \in I$ then we can write $x \equiv y \pmod{I}$ if and only if $x - y \in I$, that is, $x + I = y + I \in R/I$.

Lemma 2.2. *Suppose that $M_1, M_2, \dots M_k$ are distinct maximal ideals of R. Then*

$$1_R = x_1 + x_2 + \cdots + x_k$$

such that for $i = 1, \dots k$, $x_i \equiv 1 \pmod{M_i}$ and for $i \neq j$, $x_i \equiv 0 \pmod{M_j}$.

Proof. First we will prove this for $i = 2$. So let $x_1 \equiv 1 \pmod{M_1}$, $x \equiv 0 \pmod{M_2}$, $x_2 \equiv 1 \pmod{M_2}$, and $x_2 \equiv 0 \pmod{M_1}$. Then $M_1 + M_2$ is also an ideal and $M_1 \subset M_1 + M_2 \subseteq R$. Since M_1 is maximal, we have that $M_1 + M_2 = R$ and so there exists $x_1 \in M_1$ and $x_2 \in M_2$ that satisfy the conditions and $x_1 + x_2 = 1_R$. Now assume that for some k, if $M_1, \dots, M_k$ are distinct maximal ideals of R then

$$1_R = x_1 + x_2 + \cdots + x_k$$

such that for $i = 1, \dots k$, $x_i \equiv 1 \pmod{M_i}$ and for $i \neq j$, $x_i \equiv 0 \pmod{M_j}$. Let $M_1, M_2, \dots M_{k+1}$ be distinct maximal ideals of R. Then the element $x_{k+1} = 1 - (x_1 + x_2 + \cdots + x_k)$ satisfies $x_1 + \cdots + x_{k+1} = 1_R$ and $x_{k+1} \equiv 0 \pmod{M_i}$ for all $1 \leq i \leq k$. Furthermore, since M_{k+1} is coprime to each M_i we have that $x_{k+1} \equiv 1_R \pmod{M_{k+1}}$. □

Proposition 2.10. *The map*

$$y \longmapsto (y + M_1, \cdots, y + M_k) : R \longmapsto (R/M_1) \times \cdots \times (R/M_k)$$

is a surjective ring homomorphism with kernel $M_1 \cap \cdots \cap M_k$.

Proof. It can be checked that the map is a ring homomorphism. To show that it is surjective, if $(y_1 + M_1, \cdots, y_k + M_k)$ is any element in $(R/M_1) \times \cdots \times (R/M_k)$, let

$y = x_1y_1 + \cdots + x_ky_k$ where the x_i are defined as above. Then y is mapped to

$$(x_1y_1 + M_1, \cdots, x_ky_k + M_k) = (y_1 + M_1, \cdots, y_k + M_k)$$

since $x_iy_i \equiv y_i$ for all i. This shows that the map is surjective. To find the kernel, assume that y is to map to the identity. Then y must be in each of the M_i, so the kernel of the map is $M_1 \cap \cdots \cap M_k$. □

Theorem 2.7. *If $I \subseteq R$ is an ideal, then R/I is isomorphic to the Cartesian product of a finite collection of fields if and only if I is the intersection of a finite collection of maximal ideals of R.*

Proof. $\Longleftarrow$ This follows by the previous result.

So assume that R/I is isomorphic to the Cartesian product of a finite collection of fields $F_1 \times \cdots \times F_k$. Let ϕ be the canonical homomorphism $\phi : R \mapsto F_1 \times \cdots \times F_k$ with kernel I. For each i let ϕ_i be a homomorphism $\phi_i : R \mapsto F_i$, and let $M_i = \ker(\phi_i)$. Then $\phi(x) = 0_R$ if and only if $\phi_i(x) = 0$ for all i. This means that $I = \ker(\phi_1) \cap \cdots \cap \ker(\phi_k) = M_1 \cap \cdots \cap M_k$. To see that the M_i are maximal ideals, note that since ϕ_i maps R to a field, F_i, the kernel of the map must be a maximal ideal of R. □

Let $\mathcal{M}$ be the collection of all maximal ideals of R and $\mathcal{P}$ be the collection of all prime ideals of R. It was previously shown that

$$N = \bigcap_{P \in \mathcal{P}} P,$$

the nilradical is the intersection of the prime ideals. We now define a new important ideal, the Jacobson radical.

Definition 2.6. *The Jacobson radical J of R is*

$$J = \bigcap_{M \in \mathcal{M}} M.$$

In the next few results we prove several nice relationships between the radicals and ideals of finite commutative rings with identity. Specifically we will show that $\mathcal{M} = \mathcal{P}$, i.e., an ideal is prime if and only if it is maximal, and that $J = N$, the Jacobson and nil radicals coincide. First it is required to prove

Theorem 2.8. *$R - (\bigcup_{M \in \mathcal{M}} M)$ is the multiplicative group of units of R.*

Proof. No unit is in any maximal ideal since if x is a unit in M then $x^{-1}x = 1$ is in M, which means M is R. If x is not a unit then then (x) is an ideal. And so there must be some maximal ideal containing (x) and thus containing x. This shows that $R - (\bigcup_{M \in \mathcal{M}} M)$ is precisely the units in R. It is of course a multiplicative group. □

To show that $N = J$, we can first note that $N \subseteq J$. Let $x \in N$ be any nilpotent element. Since N is the intersection of the prime ideals x is in every prime ideal. By a very well known theorem, any maximal ideal is prime, so x is also in every maximal ideal, which means that it is in the intersection of the maximal ideals, the Jacobson radical. To prove inclusion in the other direction we first need

Lemma 2.3. *If R is a finite integral domain, then R is a field.*

Proof. Let $b \in R$, $b \neq 0$. Define a map $\phi : R \mapsto R$ defined by $\phi(x) = bx$. First we show that ϕ is injective. If $\phi(x) = \phi(y)$ then $bx = by$ and so $b(x - y) = 0$. Because R is an integral domain, then either b or $x - y$ is zero. Since b is nonzero, $x - y = 0$ and so $x = y$. This shows that the map is injective. Since R is finite and the map goes from $R \mapsto R$, ϕ is a bijection. More importantly, it is surjective and so for $1_R \in R$, there

exists an $a \in R$ such that $1_R = \phi(a) = ba$, and so $a = b^{-1}$. We can use this method to show that any element in R has a multiplicative inverse, and so R is a field. $\square$

Theorem 2.9. *If R is a finite commutative ring, then $\mathcal{M} = \mathcal{P}$.*

Proof. We already know that every maximal ideal is prime. Now if I is a prime ideal in a finite commutative ring, then R/I is an integral domain, and by the lemma it is also a field. This implies that I is a maximal ideal. Thus, $\mathcal{M} = \mathcal{P}$. $\square$

This fails if R is allowed to be infinite. That the map in the lemma is surjective does not follow from injectivity if R is not finite. Thus every infinite integral domain is not necessarily a field, so there can be prime ideals that are not maximal.

The previous theorem states that in a finite commutative ring the nilradical and Jacobson radical coincide. This leads to the following theorem.

Theorem 2.10. *If R is a finite commutative ring with $N = J$, then R/N is isomorphic to a Cartesian product of fields $F_1 \times \cdots \times F_k$.*

Proof. Since $N = J$, N is equal to the intersection of a finite collection of maximal ideals of R. Therefore by Theorem 2.7,

$$R/N \cong F_1 \times \cdots \times F_k$$

$\square$

Theorem 2.11. *If R is a finite commutative ring, then $x \in R$ is unit in R iff $x + N$ is a unit in R/N.*

Proof. If x is a unit in R, then since $x \in (R - \bigcup_{M \in \mathcal{M}} M)$, $x \notin N$ because N is the intersection of the maximal ideals. And furthermore since x^{-1} is also a unit, by the

same reasoning, $x \notin N$. Thus, $x+N$ and $x^{-1}+N$ are non-identity elements in R/N, and so $(x+N)(x^{-1}+N) = (1+N)$ which means $(x+N)$ is a unit in R/N.
Now assume that $x+N$ is a unit in R/N. Since $R/N \cong (R/M_1) \times \cdots \times (R/M_k)$ where the M_i are maximal ideals of R, $x+N$ corresponds to $(x+M_1, \cdots, x+M_k)$ in $(R/M_1) \times \cdots \times (R/M_k)$. Therefore, if $x+N$ is a unit in R/N, then x cannot be in any of the M_i. Otherwise, some $x+M_i$ in $(x+M_1, \cdots, x+M_k)$ would be simply M_i and hence could not have a multiplicative inverse. Since, x is in none of the maximal ideals of R, $x \in (R - \bigcup_{M \in \mathcal{M}} M)$, and so x is a unit in R. □

2.4 Idempotents and Local Rings

Definition 2.7. *We say that $e \in R$ is an idempotent if $e^2 = e$.*

Definition 2.8. *A ring is local if it has a unique maximal ideal.*

In this section we discuss idempotents and local rings and show how the two are closely related. It is clear that $e = 0, 1$ are idempotents. By a *nontrivial* idempotent we mean one other than $0, 1$.
If e is idempotent, then so is $1-e$ because $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$. Idempotent elements are closely related to the idea of the reducibility of a ring.

Definition 2.9. *R is reducible if $R \cong S \times T$ where S and T are (non-zero) rings.*

In what follows, we demonstrate that R is irreducible if and only if it has no nontrivial idempotents. For the first direction, if $R \cong S \times T$ is reducible, then R has a nontrivial idempotent, the element of R that corresponds to $(0, 1)$.

Now assume that a ring R has a nontrivial idempotent e. First we will show that $Re = (e) = \{re : r \in R\}$ is a commutative ring under the operations it inherits from R. There is an additive identity since $0_R \in (e)$. Also, (e) is closed under addition

and multiplication since for any $re, se \in (e)$, $re + se = (r + s)e \in (e)$ and $rese = rse^2 = rse \in (e)$. Also (e) is commutative since $(re)(se) = (se)(re)$ simply because R is commutative. Because (e) inherits operations from R, all the other ring axioms are satisfied. Furthermore, e is the multiplicative unit since for any $re \in (e)$, $ere = re^2 = re$ and $ree = re^2 = re$.

Now let $S = (e)$ and $T = (1 - e) = (f)$. We will show that $\phi : R \to S \times T$ defined by $\phi(r) = (re, rf)$ is an isomorphism $R \cong S \times T$. It is a homomorphism since for any $r, s \in R$,

$$\phi(rs) = (rse, rsf) = (rese, rfsf) = (re, rf)(se, sf) = \phi(r)\phi(s).$$

and

$$\phi(r + s) = ((r + s)e, (r + s)f) = (re + se, rf + sf) = (re, rf) + (se, sf) = \phi(r) + \phi(s).$$

To show that the kernel is trivial, assume that $0 = \phi(r) = (re, r(1 - e))$. Then $re = 0$ and $r - re = 0$, so $r = 0$. To show that ϕ is onto, let (re, sf) be any element in $S \times T$. Note that $\phi(re) = (re^2, ref) = (re, re(1 - e)) = (re, re - re^2) = (re, 0)$ and $\phi(sf) = (sfe, sf^2) = (se(1 - e)) = (se - se^2, sf) = (0, sf)$. Therefore, $\phi(re + sf) = (re, sf)$ and so ϕ is onto. We have shown that ϕ is an isomorphism. What we have just shown is the following

Theorem 2.12. *A ring R is irreducible iff it has no nontrivial idempotents.*

We now prove a useful theorem for determining when a ring R is reducible. First we need

Lemma 2.4. *If $x \in R$, then for some $k \in \mathbb{N}$, x^k is an idempotent if and only if for some distinct $i, j \in \mathbb{N}$ we have $x^i = x^j$.*

Proof. First assume that for some $k \in \mathbb{N}$, x^k is idempotent. Then $x^{k^2} = x^k$ and $x^{2k} = x^k$. Now assume that for some distinct $i, j \in \mathbb{N}$, $x^i = x^j$. Assume that $i > j$ and let $k = i - j$. Then $x^j = x^i = x^j x^k = x^i x^k = x^j x^{2k} = x^i x^{2k} = x^j x^{3k} = \cdots$ and we can continue this process until we get $x^j = x^j x^{nk}$ for any $n \in \mathbf{N}$. Choose an n such that $nk > j$. Then $x^{nk} = x^j x^{nk-j} = x^j x^{nk} x^{nk-j} = x^{2nk} = (x^{nk})^2$. Therefore, x^{nk} is an idempotent. □

This allows us to prove

Proposition 2.11. *Suppose I is an ideal of R with a finite number of elements. If R/I is reducible, then so is R.*

Proof. Let $x + I \in R/I$ be a nontrivial idempotent of R/I. For every $n \in \mathbb{N}$ we have that $x^n \in x + I$. Since $x + I$ is a finite set, this implies that $x^i = x^j$ for some distinct i and j. By Lemma 2.4, for some k, x^k is idempotent, so R is reducible. □

We are now ready to discuss local rings. Recall that a ring is local if it has a unique maximal ideal.

Immediately we can say something interesting about local rings. Recall from Theorem 2.9 that $N = J$, the Jacobson radical consists of the nilpotent elements in the ring. If our ring R is local then since J is the intersection of the maximal ideals, $J = M$ where M is the unique maximal ideal. Recalling Theorem 2.8, we know that $R - M$ is all the units in R. Therefore we can conclude that every element in a local ring is either nilpotent or a unit.

One consequence of Zorn's lemma is that any ideal of a ring is contained in some maximal ideal. If R is a local ring, then it must also be irreducible. This follows by a contradiction. If a local ring R is reducible then it has a nontrivial idempotent, e. And $1-e$ is also an idempotent. Since $R-\bigcup_{m\in\mathcal{M}} M$ is the units of R, and the only invertible

idempotent is 1, we know that e and $1-e$ cannot be contained in $R - \bigcup_{m \in \mathcal{M}} M$. This means that they must be in some maximal ideal of R. Since R has a unique maximal ideal M, $(1-e)+e=1$ is in M and so $M = R$, a contradiction.

Note that any integral domain will be irreducible because if there is a nontrivial idempotent e, then $e(1-e) = e - e^2 = e - e = 0$ which cannot occur in an integral domain. However an integral domain such as $\mathbb{Z}$ will certainly not be local. To the contrary, we have the next result.

Theorem 2.13. *A finite commutative ring is local iff it is irreducible.*

Proof. We already showed that if R is local then it is irreducible. So assume that R is irreducible. Recall that in finite commutative rings, the nilradical N and Jacobson radical J coincide. Since R is irreducible, R/I must be irreducible for any I. By Theorem 2.10, $R/N \cong F_1 \times \cdots \times F_k$, a Cartesian product of fields. But since R/N is irreducible, this means that $R/N \cong F$, a single field. Therefore, N is a maximal ideal. But $N = J = \bigcap_{M \in \mathcal{M}} M$. This implies that R can have only one maximal ideal since if the intersection of several maximal ideals was maximal, then we would have a maximal ideal properly contained in another maximal ideal, a contradiction. Since we have showed that R has one maximal ideal, it is local. □

This result implies that any finite commutative ring is isomorphic to a Cartesian product of local rings. To see this, let R be any finite commutative ring. If it has no nontrivial idempotents then it is local. If it does have nontrivial idempotents then it is reducible and can be written as $R \cong S \times T$. Then if S and T have nontrivial idempotents we can further decompose them. We can continue this process until we are left with a Cartesian product of rings that have no nontrivial idempotents and are local.

Furthermore, this decomposition into local rings is unique. To see this, suppose that

$$R \cong S_1 \times S_2 \times \cdots \times S_k \cong T_1 \times T_2 \times \cdots \times T_\ell$$

where the S_i and T_j are local rings. Let $1_R = e_1 + e_2 + \cdots + e_k$ be the idempotents implied by the first decomposition and $1_R = f_1 + f_2 + \cdots + f_\ell$ be the idempotents implied by the second decomposition.

For each $i \in \{1, \cdots, k\}$, $e_i = e_i f_1 + e_i f_2 + \ldots + e_i f_\ell$. There must be at least one $j \in \{1, \ldots, \ell\}$ such that $e_i f_j$ is not zero because e_i is nonzero. If $e_i f_j$ is nonzero, then it must equal e_i since it is an idempotent in S_i. This implies that the other products are all 0. This shows that exactly one of the products is nonzero and so there is a unique $j \in \{1, \ldots, \ell\}$ such that $e_i = e_i f_j$ and $e_i f_m = 0$ when $m \neq j$. By parallel reasoning, for every $j \in \{1, \ldots \ell\}$ we can find a unique $i \in \{1, \ldots k\}$ such that $f_j = e_i f_j$. This means that associating $i \leftrightarrow j$ where $e_i = e_i f_j = f_j$ gives a one-to-one correspondence between the e_i and f_j. Therefore, $S_i = Re_i = Rf_j = T_j$ and so $k = \ell$ and we can reorder the indices so that $S_1 = T_1, S_2 = T_2, \ldots, S_k = T_k$.

We can use these properties of local/irreducible rings to describe finite Boolean rings.

Definition 2.10. *A ring is Boolean if every one of its elements is idempotent.*

Proposition 2.12. *If B is a finite Boolean local ring, then $B \cong \mathbb{Z}_2$.*

Proof. The ring B is Boolean so all of its elements are idempotent. And since B is local it contains only the trivial idempotents. Thus, $B = \{0, 1\}$ and so $B \cong \mathbb{Z}_2$. □

Proposition 2.13. *If B is a finite Boolean ring, then $B \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$.*

Proof. First note that Boolean rings are commutative. (For a proof see [9]). Since B is a finite commutative ring, B is isomorphic to a Cartesian product of local rings, $B \cong B_1 \times \cdots \times B_k$. Let b be any element in any B_i in the decomposition. We know that $(0, 0, \ldots b, 0 \ldots 0)$ is an element in B, and so $((0, 0, \ldots b^2, 0 \ldots 0)) = ((0, 0, \ldots b, 0 \ldots 0))^2 = (0, 0, \ldots b, 0 \ldots 0)$, which means that $b^2 = b$ and so b is idempotent. Since b and B_i were arbitrary, every B_i contains only idempotents. Thus, each B_i is boolean. Since the B_i are also local, they are all isomorphic to $\mathbb{Z}_2$ and so $B \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. □

3 Wedderburn's Little Theorem

Definition 3.1. *A division ring is a ring in which every nonzero element has a multiplicative inverse.*

Division rings are also known as *skew fields*. Every field is a division ring. The only difference between the two is that a field must be commutative while a division ring may not be commutative. There are infinite division rings which are not commutative and hence not fields. But in 1905, Wedderburn proved that every *finite* division ring is commutative and hence a field. This result is know as *Wedderburn's little theorem*. In proving this theorem we follow Herstein in [2] and [6], filling in many of the details with help from [4].

Lemma 3.1. *Let D be a division ring of characteristic p. For any $a \in D$ we define a mapping $\delta : D \longmapsto D$ by $\delta(x) = xa - ax$ for every $x \in D$. Then for any positive integer k, δ satisfies $\delta^{p^k}(x) = xa^{p^k} - a^{p^k}x$.*

Proof. First we show that for any positive integer m, δ satisfies

$$\delta^m(x) = \sum_{i=0}^{m} (-1)^i \binom{m}{i} a^i x a^{m-i}.$$

We prove this by induction. If $m = 1$ then of course the result is satisfied. Suppose that the result holds for some positive integer m. Then we have that

$$\begin{aligned}
\delta^{m+1}(x) = \delta(\delta^m)(x) &= \delta\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}a^i x a^{m-i}\right) \\
&= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}a^i x a^{m-i}\right)a - a\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}a^i x a^{m-i}\right) \\
&= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}a^i x a^{m-i+1}\right) + \left(\sum_{i=1}^{m}(-1)^{i+1}\binom{m}{i-1}a^i x a^{m-i+1}\right) \\
&= \sum_{i=1}^{m}\left((-1)^i\left(\binom{m}{i} + \binom{m}{i-1}\right)a^i x a^{m-i+1}\right) + xa^{m+1} + (-1)^{m+1}a^{m+1}x \\
&= \sum_{i=0}^{m+1}(-1)^i\binom{m+1}{i}a^i x a^{(m+1)-i}.
\end{aligned}$$

This shows that the result holds for all m. Using this we can prove the lemma.
Using the first result and that fact that p divides $\binom{p}{i}$ except when i is 0 or p, we see that

$$\delta^p(x) = xa^p - a^p x.$$

Now assume that $\delta^{p^k}(x) = xa^{p^k} - a^{p^k}x$ for some k. Then

$$\delta^{p^{k+1}}(x) = (\delta^p)^{p^k}(x) = x(a^p)^{p^k} - (a^p)^{p^k}x = xa^{p^{k+1}} - a^{p^{k+1}}x,$$

which proves the lemma. □

For the rest of the proof of Wedderburn's Little Theorem we need to make the following

Definition 3.2. *The center of a ring R is the subset $\{x \in R : xr = rx\ \forall r \in R\}$, i.e., it is the set of all elements of r that commute with all other elements. We will denote*

the center $\mathcal{Z}$.

Lemma 3.2. *Let D be a division ring of characteristic $p \neq 0$ and let $\mathcal{Z}$ be the center of D. Suppose that $a \in D, a \notin \mathcal{Z}$ is such that $a^{p^n} = a$ for some $n \geq 1$; then there exists an $x \in D$ such that $xax^{-1} = a^i \neq a$ for some integer i.*

Proof. Let the mapping δ be defined as above. Let $P = \{0, 1, \ldots p-1\}$ denote the prime field of $\mathcal{Z}$; since we have assumed that $a^{p^n} - a = 0$, we know that a is a algebraic over P. This means that $P(a)$ must be a finite field with p^m elements for some m. Hence $a^{p^m} = a$ and so $\delta^{p^m}(x) = xa^{p^m} - a^{p^m}x = xa - ax = \delta(x)$ for each x so $\delta^{p^m} = \delta$.

If $\lambda \in P(a)$, then a must commute with λ. And so for every x in D,

$$\delta(\lambda x) = (\lambda x)a - a(\lambda x) = \lambda(xa - ax) = \lambda\delta(x).$$

If λI denotes the map of D into D taking x into λx, what we have shown is that the maps δ and λI commutes for $\lambda \in P(a)$. Now since $P(a)$ is a field with p^m elements, the polynomial $t^{p^m} - t$ factors in $P(a)$ as

$$t^{p^m} - t = \prod_{\lambda \in P(a)} (t - \lambda).$$

Since δ and λI commute for each λ, we can substitute the function δ for t in the above equation to get

$$0 = \delta^{p^m} - \delta = \prod_{\lambda \in P(a)} (\delta - \lambda I).$$

Since $a \notin \mathcal{Z}$, $\delta \neq 0$ because $\delta = 0$ would imply that $xa - ax = 0$ for all x. Let $\delta(\delta - \lambda_1 I) \cdots (\delta - \lambda_k I)$ be the shortest product with the $\lambda_i \in P(a)$ which is 0. By what was said above, such a product exists and since $\delta \neq 0$, $k \geq 1$. Therefore, for some $r \neq 0$ in D, $\delta(r)(\delta - \lambda_1)(r) \cdots (\delta - \lambda_{k-1})(r) = w \neq 0$ and yet $(\delta - \lambda_k)(w) = 0$.

Hence $wa - aw = \lambda_k w$ ($\lambda_k \neq 0$) in $P(a)$. Since $w \neq 0$ and D is a division ring, we can multiply by w^{-1} to get $waw^{-1} = \lambda_k + a$ in $P(a)$. Since $\lambda_k \neq 0$, we have that $waw^{-1} = \lambda_k + a \neq a$. Now $P(a)$ is a finite field so the only elements in it whose order is that of a must be appropriate powers of a. We can verify this as follows; assume that $a \in P(a)$ has order n. Then since the polynomial $y^n - 1$ has all the roots $1, a, a^2, \ldots, a^{n-1}$ in the field and these roots are distinct, any other element with the same order must be a root of the polynomial and so must be one of these a^i. Then since $(waw^{-1})^n = wa^n w^{-1} = ww^{-1} = 1$, we can conclude that $waw^{-1} = a^i \neq a$ for some i. This is the lemma. □

Theorem 3.1 (Wedderburn's little theorem)**.** *A finite division ring is a field.*

Proof. Let D be a division ring and $\mathcal{Z}$ its center; D is of characteristic p and has $q = p^n$ elements. We proceed by induction on q, assuming that all division rings with fewer than q elements are commutative.

Suppose that $a, b \in D$ such that $ab \neq ba$ but $b^t a = ab^t$ for some t. Then $b^t \in \mathcal{Z}$. (We refer to this as result (1)). We can see this by considering the centralizer $N(b^t) = \{x \in D : xb^t = b^t x\}$. Recall that $N(b^t)$ is a sub-division ring of D. If $N(b^t) \neq D$ then by the induction hypothesis, $N(b^t)$ must be commutative. But this cannot be since $a, b \in N(b^t)$ and $ab \neq ba$. Hence, it must be that $N(b^t) = D$ and so $b^t \in \mathcal{Z}$.

If $u \in D$, let $m(u)$ be the least positive integer power such that $u^{m(u)} \in \mathcal{Z}$. Pick $a \in D$, $a \notin \mathcal{Z}$ such that $r = m(u)$ is minimal over all such elements. Then r is prime, for if r were composite then $r = st$, with $s, t < r$. Let $a_1 = a^s \in D$. Because r is minimal, a_1 cannot be in $\mathcal{Z}$. However, $a_1^t = a^r = 1$. This contradicts r being minimal so it must be that r is prime. By the lemma, there is an $x \in D$ such that $xax^{-1} = a^i \neq a$. We

can compute

$$x^2ax^{-2} = x(xax^{-1})x^{-1} = x(a^i)x^{-1} = (xax^{-1})^i = a^{i^2}.$$

This can be repeated to show that $x^kax^{-k} = a^{i^k}$ for any k. More importantly, $x^{r-1}ax^{-(r-1)} = a^{i^{r-1}}$. Now we claim that $r \nmid i$. For if it did, $i = sr$ for some s and since $xax^{-1} = a^i$, we have that $xa = (a^r)^s x$. Since $a^r \in \mathcal{Z}$, because $\mathcal{Z}$ is a subring, $(a^r)^s \in \mathcal{Z}$. Therefore, $xa = (a^r)^s x = x(a^r)^s$. And so $a = (a^r)^s$, which means that $a \in \mathcal{Z}$, a contradiction, and so $r \nmid i$.

Now since r is prime and $r \nmid i$, by Fermat's Little Theorem, $i^{r-1} \equiv 1 \pmod{p}$. Therefore, $i^{r-1} = 1 + fr$ for some integer f. If we let $\lambda = a^{fr} = (a^r)^f \in \mathcal{Z}$, then

$$a^{i^{r-1}} = a^{1+fr} = aa^{fr} = a\lambda = \lambda a.$$

Since $x^{r-1}ax^{-(r-1)} = a^{i^{r-1}}$, we have that $x^{r-1}ax^{-(r-1)} = \lambda a$. Because r is minimal with respect to the property that $u^{m(u)} \in \mathcal{Z}$ we can conclude that $x^{r-1} \notin \mathcal{Z}$. If it was the case that $\lambda = 1$ then $x^{r-1}a = ax^{r-1}$. Recalling that $xa \neq ax$, by result (1) we conclude that $x^{r-1} \in \mathcal{Z}$, a contradiction, so $\lambda \neq 1$. Let $b = x^{r-1}$; we have that $bab^{-1} = \lambda a$. Since $\lambda \in \mathcal{Z}$ and $a^r \in \mathcal{Z}$,

$$\lambda^r a^r = (\lambda a)^r = (bab^{-1})^r = ba^r b^{-1} = a^r bb^{-1} = a^r.$$

This shows that $\lambda^r = 1$. Therefore, using the fact that $ba = \lambda ab$ and so $a^{-1}ba = \lambda b$,

$$b^r = \lambda^r b^r = (\lambda b)^r = (a^{-1}ba)^r = a^{-1}b^r a$$

and so $ab^r = b^r a$. Recalling that $ab \neq ba$, by result (1), we get that $b^r \in \mathcal{Z}$.

Recall from Theorem 2.2 that every multiplicative subgroup of a finite field is cyclic. Therefore $\mathcal{Z}$ is cyclic. Suppose that $\mathcal{Z}$ is generated by γ and so there exist integers m and n such that $a^r = \gamma^n$, $b^r = \gamma^m$. If $n = kr$ for some integer k then $(a/\gamma^k)^r = 1$. There are at most r distinct roots to the polynomial $u^r - 1$ (with r prime) in $\mathcal{Z}(a/\gamma^k)$ and we know that $\lambda^r = 1$. Thus, $(a/\gamma^k)^r = 1$ implies that $a/\gamma^k = \lambda^i$ for some $0 \leq i < r$ which would make $a = \lambda^i\gamma^k \in \mathcal{Z}$, a contradiction. Thus $r \nmid n$; similarly $r \nmid m$. Let $a_1 = a^m$, $b_1 = b^n$. From $ba = \lambda ab$ we have $bab^{-1} = \lambda a$. Since $\lambda \in \mathcal{Z}$,

$$ba_1b^{-1} = ba^mb^{-1} = (bab^{-1})^m = (\lambda a)^m = \lambda^m a^m = \lambda^m a_1$$

and rearranging this we get that $\lambda^{-m}b = a_1ba_1^{-1}$. Since $\lambda \in \mathcal{Z}$, we have

$$a_1b_1a_1^{-1} = a_1b^na_1^{-1} = (a_1ba_1^{-1})^n = (\lambda^{-m}b)^n = \lambda^{-mn}b^n = \lambda^{-mn}b_1.$$

If we let $\mu = \lambda^{-mn}$ we have shown that $a_1b_1 = \mu b_1a_1$. Since r does not divide m or n, it follows that $\mu = \lambda^{-mn} \neq 1$ but $\mu^r = 1$. Also note that $a_1^r = a^{mr} = \gamma^{mn} = b^{nr} = b_1^r$.

We now claim that $(a_1^{-1}b_1)^r = \mu^{r(r-1)/2}$. In fact, we will show using induction that $(a_1^{-1}b_1)^t = \mu^{t(t-1)/2}a_1^{-t}b_1^t$ when t is any positive integer t. When $t = 1$ it clearly holds. So suppose that the formula holds for some positive integer t. Using $a_1b_1 = \mu b_1a_1$,

$$\begin{aligned}
(a_1^{-1}b_1)^{t+1} &= a_1^{-1}(b_1a_1^{-1})^tb_1 = a_1^{-1}(\mu a_1^{-1}b_1)^tb_1 \\
&= a_1^{-1}\mu^t(a_1^{-1}b_1)^tb_1 = a_1^{-1}\mu^t\mu^{t(t-1)/2}a_1^{-t}b_1^tb_1 \\
&= \mu^{t+(t-1)+(t-2)+\cdots+2+1}a_1^{-(t+1)}b_1^{t+1} \\
&= \mu^{t(t+1)/2}a_1^{-(t+1)}b_1^{t+1}
\end{aligned}$$

which proves that it holds for all t. When $t = r$, we get that $(a_1^{-1}b_1)^r = \mu^{r(r-1)/2}$ since

$a_1^r = b_1^r$ and so $a_1^{-r} b_1^r = 1$.

At this point we must consider separately the cases when r is an odd prime and when $r = 2$.

First, if r is odd then $\frac{r-1}{2}$ is an integer, so $\mu^r = 1$ implies that $(a_1^{-1} b_1)^r = \mu^{r(r-1)/2} = 1$. Using this we may make a similar argument as we did above to show that $a_1^{-1} b_1 = \lambda^i$ for some i. This implies that $b_1 = a_1 \lambda^i = \lambda^i a_1$ and so $b_1 a_1 = a_1 a_1 \lambda^i = a_1 b_1 = \mu b_1 a_1$. Therefore $\mu = 1$, a contradiction, proving the theorem when r is odd.

If $r = 2$ then since $\mu^2 = 1$ and $\mu \neq 1$ we have $\mu = -1$ and so $a_1 b_1 = -b_1 a_1 \neq b_1 a_1$. Furthermore, $\alpha = a_1^2 = b_1^2 \in \mathcal{Z}$. It can be verified that there are elements ϵ, ν such that $1 + \epsilon^2 - \alpha\nu^2 = 0$. Then $(a_1 + \epsilon b_1 + \nu a_1 b_1)^2 = \alpha(1 + \epsilon^2 - \alpha\nu^2) = 0$. Since we are in a division ring, $a_1 + \epsilon b_1 + \nu a_1 b_1 = 0$. We now have the contradiction

$$0 \neq 2a_1^2 = a_1(a_1 + \epsilon b_1 + \nu a_1 b_1) + (a_1 + \epsilon b_1 + \nu a_1 b_1) a_1 = 0.$$

which finishes the proof. □

4 Hensel's Lemma

Hensel's Lemma has many forms. One form of Hensel's lemma states that if a polynomial has a non-repeated root modulo a prime p then the same polynomial also has a root modulo p^k for any integer k. It is sometimes called Hensel's lifting lemma since it allows us to lift solutions from a lower prime power modulus to a higher one. We first state a general version of Hensel's lemma that deals with the factorization of polynomials with integer coefficients. We then state a more specific version that deals explicitly with lifting roots of polynomials to a higher prime power modulus. However, both of these versions of Hensel's lemma require that the polynomials be monic. Thus we conclude

this section with a version of Hensel's lemma that does not require the polynomial to be monic.

Lemma 4.1 (Hensel's Lemma, for a proof see [1]). *Assume that $u(x)$, $f(x)$, $g(x)$ are monic polynomials in $\mathbb{Z}[x]$ such that $f(x)$ and $g(x)$ are relatively prime modulo p and*

$$u(x) \equiv f(x)g(x) \pmod{p^k}.$$

Then there exists two relatively prime monic polynomials $f_1(x), g_1(x) \in \mathbb{Z}_{p^{k+1}}[x]$ that satisfy the relations

(i) $f(x) \equiv f_1(x) \pmod{p^k}$,

(ii) $g(x) \equiv g_1(x) \pmod{p^k}$,

(iii) $u(x) \equiv f_1(x)g_1(x) \pmod{p^{k+1}}$.

Another version of Hensel's lemma is the following

Lemma 4.2 (Hensel's lemma, simplified). *Assume that $u(x)$ is a monic polynomial in $\mathbb{Z}[x]$. Let p be any prime and $n \in \mathbb{Z}^+$. Assume that a is a non-repeated root of $u(x)$ modulo p^n, that is, a satisfies $u(x) \equiv 0 \pmod{p^n}$. Then the solution a may be lifted to a solution of the congruence $u(x) \equiv 0 \pmod{p^{n+1}}$.*

This version of Hensel's lemma can be proved by the more general one above by letting $f(x)$ or $g(x)$ be a linear factor. It shows how Hensel's lemma can be used to determine when a root of a polynomial exists. However, it still requires that the polynomials are monic. Later we will want to use Hensel's lemma to solve quadratic polynomials that are not monic. Thus, we state and prove another version of Hensel's lemma that does have the assumption of monicity.

Lemma 4.3. *[from [5]] Let $f(x)$ be a polynomial with integer coefficients, and let n, k be positive integers such that $n \leq k$. If r is an integer such that*

$$f(r) \equiv 0 \pmod{p^k} \text{ and } f'(r) \not\equiv 0 \pmod{p}$$

then there exists an integer s such that

$$f(s) \equiv 0 \pmod{p^{k+n}} \text{ and } r \equiv s \pmod{p^k}.$$

Furthermore, this s is unique modulo p^{k+n}, and can be computed explicitly as

$$s = r + tp^k \text{ where } t = -\frac{f(r)}{p^k}(f'(r)^{-1}).$$

Proof. Consider the Taylor expansion of f around r. Since $r \equiv s \pmod{p^k}$, s has to be of the form $s = r + tp^k$ for some integer t. Expanding $f(r + tp^k)$ gives

$$f(r + tp^k) = f(r) + tp^k \cdot f'(r) + \mathcal{O}(p^{2k})$$

where $\mathcal{O}(p^{2k})$ is some polynomial with terms divisible by p^{2k}. Reducing both sides modulo p^{k+m}, we see that for $f(s) \equiv 0 \pmod{p^{k+m}}$ to hold, we need

$$0 \equiv f(r + tp^k) \equiv f(r) + tp^k \cdot f'(r) \pmod{p^{k+m}}$$

where the $\mathcal{O}(p^{2k})$ terms cancel because $k + m \leq 2k$. Then we note that since r is a root of $f \bmod p^k$, $f(r) = zp^k$ for some integer z, so

$$0 \equiv (z + tf'(r))p^k \pmod{p^{k+m}},$$

and so

$$0 \equiv z + tf'(r) \pmod{p^m}.$$

Then we can substitute back $f(r)/p^k$ for z and solve for t in $\mathbb{Z}_{p^m}$ to get the formula

$$t = -\frac{f(r)}{p^k}(f'(r)^{-1}),$$

noting that our assumption that $f'(r) \not\equiv 0 \pmod{p}$ ensures that $f'(r)$ has an inverse mod p^m. Therefore a solution for t and thus s exists. Since the inverse for $f'(r)$ is unique, the solution for t is unique modulo p^m and so s exists uniquely modulo p^{k+m}. □

5 Rings with additive group $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$

All rings discussed are commutative and have a multiplicative identity. Furthermore, all rings will have prime power order. Recall that a ring is an abelian group under addition with a second binary operation (often called multiplication) that distributes over addition and is associative. Given information about the additive structure of a ring we will attempt to make conclusions about the multiplicative structure. In particular, we will assume that the additive group of a ring R is the Cartesian product of two cyclic groups. Then we will make conclusions about its multiplicative structure.

First, we introduce some notation. Suppose A is an abelian group and $a \in A$.

Definition 5.1. *If $a = 0$, we let $|a|_p = \infty$. Otherwise, let j be the smallest non-negative integer such that $a = p^h x$ has a solution. We call $|a|_p$ the height of a in A.*

One simple consequence of this definition is that $|a + b|_p \geq \min\{|a|_p, |b|_p\}$.

Let R be a ring whose additive group is the direct product of cyclic group. In light of the Chinese remainder theorem, we can assume that the order of R is a prime power. Therefore, using R^+ to denote the additive group of R, let $R^+ \cong \mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ where j and k are any integers.

We will now make an observation about the representation of the additive group of R that will make the notation and computations easier. The following discussion will apply to rings on the direct product of any number of cyclic groups although we are mainly interested in the case where R^+ is the direct product of two cyclic groups. Recall that we are only considering rings of prime power order. So let R be any ring of prime power order. Since the additive structure of a finite ring is a finite abelian group, it is isomorphic to a direct product of cyclic groups of prime power order. Let $A = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$ be the additive group of R.

For each i, let $f_i = (0, \ldots, 1, \ldots 0)$. Let $x = (y_1, \ldots, y_k)$ be an element in A of maximum order, meaning we let the order of x be $\max\{p^{e_1}, \ldots, p^{e_k}\}$. Choose j so that the order of f_j is equal to the order of x. Continuing with the above notation, we are ready to state

Proposition 5.1. *Define a map* $\phi : (\langle f_1 \rangle \times \cdots \times \langle f_{j-1} \rangle \times \langle x \rangle \times \langle f_{j+1} \rangle \times \cdots \times \langle f_k \rangle) \longrightarrow A$ *by*

$$\phi(f_1, \ldots, x, \ldots, f_k) = f_1 + \cdots + f_{j-1} + x + f_{j+1} + \cdots + f_k.$$

We claim that the map ϕ *is an isomorphism.*

Proof. It is clearly a homomorphism. To show that the map is onto, note that for any $a = (a_1, \ldots, a_k) \in A$, $\phi(a_1 f_1, \ldots, a_j x, \ldots, a_k f_k) = a$. To show that the kernel is trivial, suppose that $\phi(a_1 f_1, \ldots, a_j x, \ldots, a_k f_k) = 0$ which means that $a_1 f_1 + \cdots + a_j x, \cdots a_k f_k = 0$. Thus, $(a_1 + a_j y_1, a_2 + a_j y_2, \cdots, a_j y_j, \cdots, a_k + a_j y_k) = 0$. This means that $a_j y_j = 0$.

From this we can conclude that $a_j y_i = 0$ for all other i because y_j corrseponds to the f_j of maximum order, and so since the order of x is maximum, the order of y_j must also be maximum and hence it must be greater than the order of any other y_i. Since $a_j y_i = 0$ for all i, this shows that $a_i = 0$ for all i. This shows that the kernel is trivial. Therefore, ϕ is an isomorphism. □

Since 1_R has the greatest order in any ring, we can use this result to say that if the additive structure of R is isomorphic to $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$, then the additive structure of R is also isomorphic to $\langle 1_R \rangle \times \mathbb{Z}_{p^j}$.

Thus we may assume that 1_R is the element $(1, 0)$. If we let κ equal the element $(0, 1)$, then for rings of this type we can write $R = Z \times K$ where $Z = \langle 1_R \rangle$ and $K = \langle \kappa \rangle$. Note that 1_R has order p^{j+k} and κ has order p^j. And so we have that every $x \in R$ can be uniquely expressed as $a + b\kappa$ where $a \in \mathbb{Z}_{p^{j+k}}$ and $b \in \mathbb{Z}_{p^j}$.

Since every element in the ring can be written as $a + b\kappa$, the multiplication of R is completely determined by the value of k^2. To see this, let $\kappa^2 = a + b\kappa$ for some a and b. For any elements $c + d\kappa$ and $e + f\kappa$ in the ring, we have that $(c + d\kappa)(e + f\kappa) = ec + (ed + fc)\kappa + df\kappa^2$. Furthermore, since $p^j \kappa = 0$, we must have $p^j \kappa^2 = (p^j \kappa)\kappa = 0$, and so if $\kappa^2 = a + b\kappa$, it must be the case that $p^j a = 0$. In other words, it must be that $|a|_p \geq k$. For the number b in the expression for κ^2, we either have that $|b|_p < j$, or else $b = 0$ and $|b|_p = \infty$. However, as we will see next, the height of b is not as immediately consequential as that of a.

We have already seen that $|a|_p \geq k$ is a necessary condition for the value of κ^2 to define a commutative ring over the additive group. The next proposition shows that this is also a *sufficient* condition.

Proposition 5.2. *$|a|_p \geq k$ is a sufficient condition for $k^2 = a + bk$ to determine a multiplicative operation on $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ that defines a commutative ring.*

Proof. Consider the ring $\mathbb{Z}_{p^{j+k}}[x]/(x^2 - bx - a, p^k x)$. The additive group of this ring will be isomorphic to $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$. To see this, let $\phi : \mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j} \longrightarrow \mathbb{Z}_{p^{j+k}}[x]/(x^2 - bx - a, p^k x)$ be the additive group homomorphism defined by $\phi((a, b)) = a + bx$. It is natural to show that this map is an isomorphism of groups.

To show that the ring $\mathbb{Z}_{p^{j+k}}[x]/(x^2 - bx - a, p^k x)$ has the desired multiplication, observe that the element $x + (x^2 - bx - a, p^k x)$ in the polynomial ring corresponds to the element κ in $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$. This is because $\phi(\kappa) = \phi((0, 1)) = x + (x^2 - bx - a, p^k x)$. Now we compute $(x + (x^2 - bx - a, p^k x))^2 = x^2 + (x^2 - bx - a, p^k x) = bx + a + (x^2 - bx - a, p^k x)$. This shows that multiplication works as desired, that is, $\kappa^2 = a + b\kappa$. □

This proposition states that every ring whose additive group is the direct product of two cyclic groups is isomorphic to some ring of the form

$$\mathbb{Z}_{p^{j+k}}[x]/(x^2 - bx - a, p^k x)$$

where j and k simply correspond to the size of the ring and a and b are integers that can vary to produce rings with non-isomorphic multiplicative operations. We would like to determine precisely when two rings of this form are isomorphic. In the next section we discuss some preliminary cases; we outline all rings whose additive group is cyclic or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

5.1 Preliminary Cases

As a first case, consider a ring R whose additive group is cyclic.

Proposition 5.3. *If $R^+ \cong \mathbb{Z}_n$ for some n then R is also isomorphic to $\mathbb{Z}_n$ as a ring.*

Proof. Let k be the additive order of 1_R. We know that the additive order of every element in R divides k. From this we can conclude that $k = n$ since otherwise we

would not have any element with order n, a contradiction to $\mathbb{Z}_n$ being a cyclic group. Therefore, 1_R generates the ring. It follows from this that there is an additive group isomorphism $\phi : R \to \mathbb{Z}_n$ that is completely determined by specifying that 1_R maps to 1. Now we can verify that ϕ is also a ring isomorphism. It suffices to show that $\phi(ab) = \phi(a)\phi(b)$ for all a and b in R. But

$$\begin{aligned}
\phi(ab) &= \phi((1_R + \cdots + 1_R)(1_R + \cdots + 1_R)) \\
&= \phi((1_R + \cdots + 1_R) + \cdots + (1_R + \cdots + 1_R)) \\
&= \phi(a + \cdots + a) \\
&= \phi(a) + \cdots + \phi(a) \\
&= \phi(a)\phi(b)
\end{aligned}$$

This shows that ϕ is an isomorphism of rings and so the conclusion follows. □

Now consider a ring with additive group isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Then R consists of elements $a + b\kappa$ where $a, b \in \mathbb{Z}_p$. If we let $\kappa^2 = a + b\kappa$ then $x^2 - bx - a$ is the minimum polynomial for κ over $\mathbb{Z}_p$ and so the ring is isomorphic to $\mathbb{Z}_p[x]/(x^2 - bx - a)$.

From here there are three options for the multiplicative structure depending on the nature of the polynomial $x^2 - bx - a$. If the polynomial is irreducible over $\mathbb{Z}_p$, then we know by a familiar theorem (see [3]) that R is the field F_{p^2}. If it is reducible with two distinct roots then $R \cong \mathbb{Z}_p[x]/((x - \alpha)(x - \beta))$ for some $\alpha, \beta \in \mathbb{Z}_p$. This ring is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ by the map $\phi : \mathbb{Z}_p[x]/((x - \alpha)(x - \beta)) \to \mathbb{Z}_p \times \mathbb{Z}_p$ defined by $\phi(f(x)) = (f(\alpha), f(\beta))$.
Finally, if the polynomial is reducible with one repeated root then $R \cong \mathbb{Z}_p[x]/((x-\alpha)^2)$ which is the same as $\mathbb{Z}_p[x]/(x^2)$. What we have proven is the following

Proposition 5.4. *If $R^+ \cong \mathbb{Z}_p \times \mathbb{Z}_p$ then R is isomorphic to one of $F_{p^2}, \mathbb{Z}_p[x]/(x^2), \mathbb{Z}_p \times$*

$\mathbb{Z}_p$.

5.2 General Considerations

In this section we consider the problem of classifying rings with additive group $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ for any j and k. We will classify rings for both odd and even p. However it should be noted that the case when $p = 2$ is significantly different from the odd prime case. Assume first that p is odd. We will then show how our argument can be modified to deal with the $p = 2$ case as well.

Recall that we can express rings of this type as $R = Z \times K$ where $Z = \langle 1_R \rangle$ and $K = \langle \kappa \rangle$ Suppose $S = Z \times K$ is a second ring of this type where $\langle \lambda \rangle = L \cong \mathbb{Z}_{p^j}$. (So the element λ in S corresponds to the element κ in R.) Let multiplication in S be determined by $\lambda^2 = e + f\lambda$. If $\phi : R \longrightarrow S$ is a ring isomorphism, then it is characterized by $\phi(\kappa) = m + n\lambda$ for some integers m and n. Since ϕ is a **group** isomorphism, we must have that n is a unit in $\mathbb{Z}_{p^j}$, i.e., $|n|_p = 0$. Also note that $p^j\kappa = 0$ implies that $p^j m = 0$. Therefore, we must have that $|m|_p \geq k$. Since ϕ is a **ring** isomorphism, it must preserve the operation and so we have that

$$\begin{aligned}
(a + mb) + nb\lambda &= a + b(m + n\lambda) \\
&= \phi(a + b\kappa) \\
&= \phi(\kappa^2) \\
&= \phi(\kappa)^2 \\
&= (m + n\lambda)^2 \\
&= m^2 + 2mn\lambda + n^2\lambda^2 \\
&= (m^2 + n^2 e) + (2mn + n^2 f)\lambda.
\end{aligned}$$

So we must have

$$a + mb = m^2 + n^2 e \in \mathbb{Z}_{p^{j+k}} \tag{1}$$

and

$$b = 2m + nf \in \mathbb{Z}_{p^j} \tag{2}$$

The existence of values of m and n (with $|m|_p \geq k$, $|n|_p = 0$) for which (1) and (2) hold will be necessary and sufficient for R and S to be isomorphic.

Theorem 5.1. *We have $|b| \geq k$ if and only if there is a ring isomorphism $R \cong S$ with $S = Z \times L$, $L = \langle \lambda \rangle$ and $\lambda^2 = e$. (So $f = 0$).*

Proof. Suppose first that S and an isomorphism ϕ are given. Since $f = 0$, by (2) we have $b = 2m \in \mathbb{Z}_{p^j}$. Since $|m|_p \geq k$, we can conclude that $|b|_p \geq k$ as required.

Conversely, suppose that $|b|_p \geq k$. Consider $b/2 \in \mathbb{Z}_{p^{j+k}}$; it is worth noting that since $p \neq 2$, 2 will be a unit in $\mathbb{Z}_{p^{j+k}}$, and so division by 2 is valid. Since $|b|_p, |a|_p \geq k$, we can define S by setting $\lambda^2 = e = a + b^2/4$ ($f = 0$) and we will satisfy the requirement that $|e|_p \geq k$. Now, define $\phi : R \longrightarrow S$ by the equation $\phi(\kappa) = b/2 + \lambda$ (i.e., $m = b/2$ and $n = 1$). And since $|b|_p \geq k$ we have satisfied $|m|_p \geq k$, and so ϕ is an additive isomorphism. To show that this is a multiplicative isomorphism, equation (1) reads $a + (b/2)b = b^2/4 + (a + b^2/4)$ and (2) reads $b = 2(b/2)$. So ϕ is a ring isomorphism as required. □

As we will see shortly, rings that satisfy Theorem 5.1 can be easily classified. As such we give these rings a name,

Definition 5.2. *We say a ring R is a square-root-ring if it satisfies the last result, that is, if $R \cong Z \times K$ where $K = \langle \kappa \rangle$, $\kappa^2 = a + b\kappa$, and $|b|_p \geq k$*

Observe that if $k = 0$, so the additive group of R is $\mathbb{Z}_{p^j} \times \mathbb{Z}_{p^j}$ then by Theorem 5.1, R is necessarily a square root. To classify the square root rings, define an equivalence relation on $\mathbb{Z}_{p^{j+k}}$ by $a \sim a'$ iff $a = n^2 a'$ for some unit $n \in \mathbb{Z}_{p^{j+k}}$. We can see that $\{0\}$ must be one equivalence class. Furthermore, since n is a unit, if $a \sim a'$ then $|a|_p = |a'|_p$. For each possible height of a, a' there are two equivalence classes, one consisting of all the quadratic residues mod p^{j+k} and the other consisting of all the non-residues. Since $|a|_p \geq k$, we can determine exactly how many square-root-rings there are

Theorem 5.2. *For a fixed j and k, the square-root-rings are in a one-to-one correspondence with the equivalence classes on $\mathbb{Z}_{p^{j+k}}$ containing elements of height at least k. Therefore, there are $2j + 1$ such equivalence classes, and so there are $2j + 1$ square root rings.*

Proof. Assume $R = Z \times K$ and $S = Z \times L$ are square-root-rings where $\kappa^2 = a \in \mathbb{Z}_{p^{j+k}}$ and $\lambda^2 = e \in \mathbb{Z}_{p^{j+k}}$, so $b = f = 0$. We claim that $R \cong S$ iff $a \sim e$.

Suppose first that $a \sim e$ and let n be such that $a = n^2 e$. Define $\phi : R \longrightarrow S$ by setting $m = 0$. Then 1 says $a = n^2 e$ and 2 says $0 = 0$.

Conversely, suppose that we have a ring isomorphism ϕ, where $\phi(\kappa) = m + n\lambda$. Equation 2 says that $m = 0 \in \mathbb{Z}_{p^j}$, in other words, $|m|_p \geq j$. Since we also know that $|m|_p \geq k$, we can conclude that $|m|_p \geq j + k$ so that in $\mathbb{Z}_{p^{j+k}}$, $m^2 = 0$. Therefore, equation 1 says $a = n^2 e$, as required. □

Now we consider the rings that are **not** square-root-rings. This means that $|b|_p < k$. We shall use the abbreviation NSR rings for rings that are not square-root-rings. Observe that if $b = 0 \in \mathbb{Z}_{p^j}$ then R is a square-root-ring. So if R is a NSR ring we must have that $|b|_p < j$, and so $|b|_p < \min\{j, k\}$.

Proposition 5.5. *Suppose R and S are isomorphic NSR rings. Then $|b|_p = |f|_p$.*

Proof. Since $|m|_p \geq k$, this follows from equation 2. □

If R is one of the rings we are considering which is not a square-root-ring, we will call $|b|_p$ the height of the ring. So the question of classifying rings with additive group $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ has been reduced to the following: If $h < \min\{j, k\}$, how many NSR rings are there, up to isomorphism, of height h?

We can prove one easy case:

Proposition 5.6. *All NSR rings of height* 0 *are isomorphic.*

Proof. Let R be any NSR ring of height 0. Consider the quotient ring R/pR. We have that $|a|_p > 0$ and $|b|_p = 0$, so R/pR will be isomorphic to $\mathbb{Z}_p[x]/(x^2 - bx)$. Since over $\mathbb{Z}_p$ we can factor $x^2 - bx = x(x - b)$, and since 0 and b are relatively prime, R/pR will be isomorphic as a ring to $\mathbb{Z}_p[x]/(x - b) \times \mathbb{Z}_p[x]/(x) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Therefore, since R/pR is reducible, by Proposition 2.11, R is reducible, and will have to split into a direct product of rings which must be isomorphic to $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$. □

In the next proposition, we show that all NSR rings of a given height h can be put into a more "standard form".

Proposition 5.7. *Suppose R is a NSR ring of height h where $h < \min\{j, k\}$. Then $R \cong S$ where in S, $f = p^h$, i.e., $\lambda^2 = e + p^h\lambda$.*

Proof. Suppose $b = np^h$, where $|n|_p = 0$, and let $e = a/n^2$, $f = p^h$ and $m = 0$. Then $|e|_p = |a|_p \geq k$, so S is a ring. Equation 1 then says $a = n^2(a/n^2)$ and equation 2 says $b = np^h$. □

Definition 5.3. *We say that a NSR ring R is normalized if $k^2 = a + p^h\kappa$ where h is the height of R.*

Proposition 5.2 states that every NSR ring can be normalized. From now on we will assume that all NSR rings have been normalized, since it makes things easier. So assume that R and S are normalized NSR rings with $\kappa^2 = a + p^h\kappa$ in R and $\lambda^2 = e + p^h\lambda$ in S. Then our equations 1 and 2 become

$$a + mp^h = m^2 + n^2 e \in \mathbb{Z}_{p^{j+k}} \tag{3}$$

and

$$p^h = 2m + np^h \in \mathbb{Z}_{p^j}. \tag{4}$$

We can rewrite these equations to make them in the same modulus. Observe that $|a|_p, |e|_p, |m|_p \geq k$. Replacing a by $x = a/p^k$, e by $y = e/p^k$, and m by $r = m/p^k$ gives

$$x + rp^h = r^2 p^k + n^2 y \in \mathbb{Z}_{p^j} \tag{5}$$

and

$$p^h = 2rp^k + np^h \in \mathbb{Z}_{p^j}. \tag{6}$$

Now we can define an equivalence relation $\bowtie_h$ on $\mathbb{Z}_{p^j}$ by $x \bowtie_h y$ iff there are $r, n \in \mathbb{Z}_{p^j}$ with $|n|_p = 0$ such that 5 and 6 hold. So the question of classifying NSR rings can be stated as such:

For each h $0 < h < \min\{l, k\}$, what are the $\bowtie_h$ equivalence classes in $\mathbb{Z}_{p^j}$?

It is not obvious from its definition that $\bowtie_h$ is an equivalence relation. However, because we are considering isomorphism classes of rings, it must be that $\bowtie_h$ really does satisfy the properties of an equivalence relation. This is because the isomorphism relation is an equivalence relation.

What we have shown is that the isomorphism classes of rings of height h correspond

to the $\bowtie_h$ equivalence classes in $\mathbb{Z}_{p^j}$. All that is left to do is to determine how the $\bowtie_h$ equivalence relation partitions $\mathbb{Z}_{p^j}$.

We will now determine how to explicitly generate $\bowtie_h$ equivalence classes for a given x. Given any $r, n, y \in \mathbb{Z}_{p^j}$ with $|n|_p = 0$, then equation 5 gives x in terms of y, r, n by $x = r^2p^k - rp^h + n^2y$. In this equation, y can be any element of $\mathbb{Z}_{p^j}$, while the relation between r and n is determined by 6.

Given an arbitrary $r \in \mathbb{Z}_{p^j}$, equation 6 tells us that $np^h = p^h - 2m \in \mathbb{Z}_{p^j}$, and so

$$n = 1 - 2rp^{k-h} \pmod{p^{j-h}}.$$

Therefore, in $\mathbb{Z}_{p^j}$, the possible values for n are

$$n = 1 - 2rp^{k-h} + s$$

where s ranges over the values $p^{j-h}\mathbb{Z}_{p^j}$. (We may note that since $j, k > h$, we know that in this equation $|n|_p = 0$.) Therefore, as r varies over $\mathbb{Z}_{p^j}$ and t varies over $p^{j-h}\mathbb{Z}_{p^j}$, the equivalence class of y is the collection of all

$$x = r^2p^k - rp^h + (1 - 2rp^{k-h} + s)^2y \in \mathbb{Z}_{p^j}. \tag{7}$$

We can use this to help continue our investigations.

The following lemma is of no interest other than its use in proving the next theorem.

Lemma 5.1. *For $x \in \mathbb{Z}_{p^j}$ and for any integer i, p^i divides exactly one of the quantities $1 + \sqrt{1 + 4xp^i}$, $1 - \sqrt{1 + 4xp^i}$.*

Proof. First since $1 + \sqrt{1 + 4xp^i} + 1 - \sqrt{1 + 4xp^i} = 2$, p cannot divide both of the quantities. If it did, this would lead to the contradiction $p|2$. Now assume that p^i divides

neither of the two quantities. Since p cannot divide both, his implies that p^i does not divide their product. But their product is $(1+\sqrt{1+4xp^i})(1-\sqrt{1+4xp^i}) = -4xp^i$. This is a contradiction, so the conclusion of the lemma follows. □

Theorem 5.3. *The $\bowtie_h$ equivalence class of $\{0\}$ is all the elements in $\mathbb{Z}_{p^j}$ that are congruent to 0 mod p^h. Another way of saying this is the following; if R is a normalized NSR ring with $\kappa^2 = p^h a + p^h\kappa$ ($p^k|a$), then R is isomorphic to S where $\lambda^2 = p^h\lambda$. ($e = 0$)*

Proof. Equation (1) says that $p^h a + mp^h = m^2$. Equation (2) says $p^h = 2m + np^h$. Solving the first equation for m, we get that

$$m = \frac{p^h \pm \sqrt{p^{2h} + 4p^h a}}{2} = \frac{p^h \pm p^h\sqrt{1+4xp^{k-h}}}{2} = p^h\frac{1 \pm \sqrt{1+4xp^{k-h}}}{2}$$

where we have substituted $x = a/p^k$. To show that these really are solutions for m we need to verify that $1 + 4xp^{k-h}$ is a quadratic residue mod p^{j+k}. To that end, let $a = 1 - 4xp^{k-h}$ and let $f(y) = y^2 - a$. Note that $y = 1$ is a solution to the congruence $f(y) \equiv 0 \pmod{p}$. And $f'(y) \not\equiv 0 \pmod{p}$. By Hensel's lemma 4.3, we can lift this solution to a solution of the congruence $f(y) \equiv 0 \pmod{p^{j+k}}$. This shows that $y^2 - (1 - 4xp^{k-h})$ has a solution mod p^{j+k} and so $1 - 4xp^{k-h}$ is a quadratic residue mod p^{k-h}, as desired.

Now, substituting this value for m into equation (2), we get $p^h = p^h \pm p^h\sqrt{1+4xp^{k-h}} + np^h$ or $1 = 1 \pm \sqrt{1+4xp^{k-h}} + n$, and so we get that $n = \pm\sqrt{1+4xp^{k-h}}$. These values for n clearly satisfies the requirement that $|n|_p = 0$. It remains to verify that $|m|_p \geq k$. It will suffice to show that $p^{k-h}|(1 \pm \sqrt{1+4xp^{k-h}})$. By the Lemma 5.1, p^{k-h} divides one of $1 + \sqrt{1+4xp^{k-h}}$, $1 - \sqrt{1+4xp^{k-h}}$. We can simply pick the one that it does (this also determines our value for n). This ensures that $|m|_p \geq k$ □

We could continue to solve these equations in this manner; using the quadratic

formula and then using Hensel's lemma and divisibility arguments to show that what the quadratic formula gives us really is a solution. However, a much more systematic approach is possible.

If we multiply out equation (7) and collect terms we get the quadratic

$$0 = (p^k + 4yp^{2k-2h})r^2 - (p^h + 4yp^{k-h})r + 4yp^{j+k-2h}rs + yp^{2j-2h}s^2 + 2yp^{j-h}s + (y - x).$$

It follows that $x \bowtie_h$ iff this quadratic has a solution $r, s, \in \mathbb{Z}_{p^j}$.

Now recall that so far we have only been considering the case of odd primes. We can convert equations (5) and (6) to apply them to the case when $p = 2$. Letting $p = 2$, the equations become

$$x + r2^h = r^2 2^k + n^2 y \in \mathbb{Z}_{2^j}$$

and

$$2^h = rp^{k+1} + np^h \in \mathbb{Z}_{p^j}.$$

Note that the only major change is to the term that included a factor of 2 in equation (6). Following the same process as in the odd prime case, we can show that when $p = 2$, $x \bowtie_h y$ iff there is a solution $r, s \in \mathbb{Z}_{2^j}$ to the quadratic

$$0 = (2^k + y2^{2k-2h+2})r^2 - (2^h + y2^{k-h+2})r + y2^{j+k-2h+2}rs + y2^{2j-2h}s^2 + y2^{j-h+1}s + (y - x).$$

6 Applying a Variation on Hensel's Lemma

In discussing heights, we want $|p^m y|_p = |y|_p + m$ for all $y \in \mathbb{Z}_{p^j}$ and $m \geq 0$; so we adopt the conventions that

$$|0|_p = \infty = j, j+1, j+2, \ldots \text{ and } \infty > \infty.$$

Recall Hensel's lemma from section 4. The version of Hensel's lemma that will be useful now is Lemma 4.3. We will use this result to derive two versions of Hensel's lemma that apply specifically to quadratics. The first deals with normal quadratic equations and the second extends this result to quadratic equations in two variables.

Lemma 6.1. *Suppose $\alpha, \beta, \sigma \in \mathbb{Z}_{p^j}$ and we consider an equation in $\mathbb{Z}_{p^j}$ of the form*

$$\alpha r^2 + \beta r + \sigma = 0. \qquad (*)$$

(a) Suppose p is any prime. If $|\alpha|_p > |\beta|_p$, then (*) has a solution $r \in \mathbb{Z}_{p^j}$ iff $|\sigma|_p \geq |\beta|_p$.

(b) If $p = 2$, $|\alpha|_2 \geq |\beta|_2$ and

$$u = \begin{cases} 0, & \text{if } |\alpha|_2 > |\beta|_2 \\ 1, & \text{if } |\alpha|_2 = |\beta|_2, \end{cases}$$

then (*) has a solution $r \in \mathbb{Z}_{p^j}$ iff $|\sigma|_2 \geq |\beta|_2 + u$.

Proof. We deal with case (a) first. Suppose that we have a solution r. It follows that

$$\sigma = -\alpha r^2 - \beta r$$

which clearly implies that $|\sigma|_p \geq |\beta|_p$.

Conversely, suppose that $|\sigma|_2 \geq |\beta|_2$. Let $t = |\beta|_2$. If $t = \infty$ then out equation is $f(z) = 0$ and any r is a solution. We may therefore assume that $t < j$. Letting $\alpha_1 = \alpha/p^t, \beta_1 = \beta/p^t, \sigma_1 = \sigma/p^t$, it follows that $f(z) = 0$ has a solution in $\mathbb{Z}_{p^j}$ iff

$$f_1(z) = \alpha_1 z^2 + \beta_1 z + \sigma_1 = 0$$

has a solution in $\mathbb{Z}_{p^{j-t}}$. So replacing j, α, β, and σ by $j - t, \alpha_1, \beta_1, \sigma_1$, there is no loss of generality in assuming that β is a unit. (and $|\alpha|_p > 0$). Note that modulo p we have

$$f(\beta^{-1}\sigma) \equiv 0$$

and

$$f'(\beta^{-1}\sigma) \equiv \beta \neq 0.$$

Therefore by Lemma 4.3, there is a solution r to $f(z) = 0$ in $\mathbb{Z}_{p^j}$.

Now consider (b). Suppose that we have a solution r. It follows that

$$\sigma = -\alpha r^2 - \beta r.$$

This clearly implies that $|\sigma|_2 \geq |\beta|_2$. Furthermore, if $|\alpha|_2 = |\beta|_2 = a$, let $\beta_2 = \beta/2^a$, $\alpha_2 = \alpha/2^a$. Then

$$\sigma = -2^a \alpha_2 r(r + \alpha_2^{-1}\beta_2).$$

Since $\alpha_2^{-1}\beta_2$ is a unit, 2 divides either r or $r + \alpha_2^{-1}\beta_2$. This implies that $|\sigma|_2 \geq |\beta_2| + 1 = |\beta|_2 + u$ as required.

Conversely, suppose that $|\sigma|_2 \geq |\beta|_2 + u$. As we did above, we may in this case assume that β is a unit and $|\alpha|_2 > 0$. Note that modulo 2 we have

$$f(0) = \sigma \equiv 0$$

and

$$f'(0) = \beta \not\equiv 0.$$

Therefore by Lemma 4.3 there is a solution r to $f(z) = 0$ in $\mathbb{Z}_{p^j}$. □

We now consider quadratic equations in two variables.

Lemma 6.2. *Suppose $\alpha, \beta, \gamma, \delta, \epsilon, \sigma \in \mathbb{Z}_{p^j}$ and $|\gamma|_p > |\beta|_p$. Consider an equation in $\mathbb{Z}_{p^j}$ of the form*

$$\alpha r^2 + \beta r + \gamma rs + \delta s^2 + \epsilon s + \sigma = 0. \qquad (\dagger)$$

(a) If $|\alpha|_p > |\beta|_p$ and $|\delta|_p > |\epsilon|_p$, then $(\dagger)$ has a solution $r, s \in \mathbb{Z}_{p^j}$ iff

$$|\sigma|_p \geq \min\{|\beta|_p, |\epsilon|_p\}.$$

(b) If $p = 2$, $|\alpha|_2 \geq |\beta|_2$, $|\delta|_2 \geq |\epsilon|_2$ and

$$u = \begin{cases} 0, & \text{if } |\alpha|_2 > |\beta|_2 \\ 1, & \text{if } |\alpha|_2 = |\beta|_2, \end{cases} \qquad v = \begin{cases} 0, & \text{if } |\delta|_2 > |\epsilon|_2 \\ 1, & \text{if } |\delta|_2 = |\epsilon|_2, \end{cases}$$

then $(\dagger)$ has a solution $r, s \in \mathbb{Z}_{p^j}$ iff

$$|\sigma|_2 \geq \min\{|\beta|_2 + u, |\epsilon|_2 + v\}.$$

Proof. Suppose first that (†) has a solution r, s. In (a) it follows that

$$|\sigma|_p = |\alpha r^2 + \beta r + \gamma rs + \delta s^2 + \epsilon s|_p \geq \min\{|\beta|_p, |\epsilon|_p\}.$$

In (b) we have

$$|\sigma|_2 \geq \min\{|\alpha r^2 + \beta r|_2, |\gamma rs|_2, |\delta s^2 + \epsilon s|_2\} \geq \min\{|\beta|_2 + u, |\epsilon|_2 + v\}.$$

We now consider the converse. Suppose we are in case (a) and

$$|\sigma|_p \geq \min\{|\beta|_p, |\epsilon|_p\} \stackrel{\text{def}}{=} \kappa.$$

If $\kappa = |\beta|_p$, then in (†) we first let $s = 0$. The equation then reduces to

$$\alpha r^2 + \beta r + \sigma = 0,$$

and by Lemma 6.1(a), this has a solution $r \in \mathbb{Z}_{p^j}$.

Similarly, if $\kappa = |\epsilon|_p$, then in (†) we first let $r = 0$. The equation then reduces to

$$\delta s^2 + \epsilon s + \sigma = 0,$$

and by Lemma 6.1(a), this has a solution $s \in \mathbb{Z}_{p^j}$.

Next, suppose we are in case (b) and

$$|\sigma|_2 \geq \min\{|\beta|_2 + u, |\epsilon|_2 + v\} \stackrel{\text{def}}{=} \lambda.$$

If $\lambda = |\beta|_p + u$, then in (†) we first let $s = 0$. The equation then reduces to

$$\alpha r^2 + \beta r + \sigma = 0,$$

and by Lemma 6.1(b), this has a solution $r \in \mathbb{Z}_{p^j}$.

Similarly, if $\lambda = |\epsilon|_p + v$, then in (†) we first let $r = 0$. The equation then reduces to

$$\delta s^2 + \epsilon s + \sigma = 0,$$

and by Lemma 6.1(b), this has a solution $s \in \mathbb{Z}_{p^j}$. □

We need one more lemma before we can determine the $\bowtie_h$ equivalence classes.

Lemma 6.3.

(a) For any prime p, $|4yp^{j+k-2h}|_p > |p^h + 4yp^{k-h}|_p$.

(b) We have that $|y2^{j+k-2h+2}|_2 > |2^h + y2^{k-h+2}|_2$.

Proof. First consider (a). If $|y|_p \geq 2h-k$ then $|4yp^{j+k-2h}|_p = \infty$ and so the result holds. If $|y|_p < 2h - k$ then $|p^h + 4yp^{k-h}|_p = |y|_p + k - h < |y|_p + k - h + j - h = |4yp^{j+k-2h}|_p$ as desired.

Now consider (b). If $|y|_2 \geq 2h - k - 2$ then $|y2^{j+k-2h+2}|_2 = \infty$ and so the result holds. If $|y|_2 < 2h - k - 2$ then $|2^h + y2^{k-h+2}|_2 = |y|_2 + k - h + 2 < |y|_2 + k - h + 2 + j - h = |y2^{j+k-2h+2}|_2$ as desired. □

We now look at the case of odd primes.

Theorem 6.1. *Suppose p is odd. Then* $x \bowtie_h y$ *iff*

$$x \equiv y \pmod{p^w}$$

where

$$w = \min\{|p^h + 4yp^{k-h}|_p, |y|_p + j - h\}.$$

Proof. We consider the equation

$$0 = (p^k + 4yp^{2k-2h})r^2 - (p^h + 4yp^{k-h})r + 4yp^{j+k-2h}rs + yp^{2j-2h}s^2 + 2yp^{j-h}s + (y - x)$$

So let

$$\begin{aligned}
\alpha &\stackrel{\text{def}}{=} p^k + 4yp^{2k-2h} \\
\beta &\stackrel{\text{def}}{=} -(p^h + 4yp^{k-h}) = -\alpha p^{h-k} \\
\gamma &\stackrel{\text{def}}{=} 4yp^{j+k-2h} \\
\delta &\stackrel{\text{def}}{=} yp^{2j-2h} \\
\epsilon &\stackrel{\text{def}}{=} 2yp^{j-h} = \delta 2p^{h-j} \\
\sigma &\stackrel{\text{def}}{=} y - x.
\end{aligned}$$

If follows that $|\alpha|_p > |\beta|_p$ and $|\delta|_p > |\epsilon|_p = |y|_p + j - h$. The fact that $|\gamma|_p > |\beta|_p$ was proven in Lemma 6.3. The result therefore follows immediately from Lemma 6.2(a). □

We now look at the $p = 2$ case.

Theorem 6.2. *Suppose* $p = 2$ *and*

$$u = \begin{cases} 0, & \text{if } k > h \\ 1, & \text{if } k = h, \end{cases} \qquad v = \begin{cases} 0, & \text{if } j - 1 > h \\ 1, & \text{if } j - 1 = h, \end{cases}$$

Then $x \bowtie_h y$ *iff*

$$x \equiv y \pmod{2^z}$$

where

$$z = \min\{|2^h + y2^{k-h+2}|_2 + u, |y|_2 + j - h + 1 + v\}.$$

Proof. We look at the equation:

$$0 = (2^k + y2^{2k-2h+2})r^2 - (2^h + y2^{k-h+2})r + y2^{j+k-2h+2}rs + y2^{2j-2h}s^2 + y2^{j-h+1}s + (y-x)$$

Once again, we let

$$\begin{aligned}
\alpha &\stackrel{\text{def}}{=} 2^k + y2^{2k-2h+2} \\
\beta &\stackrel{\text{def}}{=} -(2^h + y2^{k-h+2}) = -\alpha 2^{h-k} \\
\gamma &\stackrel{\text{def}}{=} y2^{j+k-2h+2} \\
\delta &\stackrel{\text{def}}{=} y2^{2j-2h} \\
\epsilon &\stackrel{\text{def}}{=} y2^{j-h+1} = \delta 2^{h-j+1} \\
\sigma &\stackrel{\text{def}}{=} y - x.
\end{aligned}$$

It follows that $|\alpha|_2 \geq |\beta|_2$ and $|\alpha|_2 = |\beta|_2$ iff $h = k$, and similarly $|\delta|_2 \geq |\epsilon|_2 = |y|_2 + j - h + 1$ and $|\delta|_2 = |\epsilon|_2$ iff $j - 1 = h$. The fact that $|\gamma|_2 > |\beta|_2$ was proven in Lemma 6.3. The result therefore follows immediately from Lemma 6.2(b). □

Using these Theorems we can count the number of NSR rings of a given height and given j and k values.

Theorem 6.3. *Let p be odd. For a given j, k, and h there are*

$$p^{\ell-h-1}\Big(\big(2h-2\ell+j\big)\big(p-1\big)+p\Big)$$

rings of height h with additive group $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ if $2h \geq \ell$. If $2h < \ell$ then there are p^{j-h} rings.

Proof. First assume that $2h < \ell$. Then $x \bowtie_h y$ iff $x \equiv y \pmod{p^h}$. It follows that there are p^{j-h} $\bowtie_h$ equivalence classes.

Now assume that $2h \geq \ell$.

First consider the elements of height less than $2h-\ell$. For each height of y, $|y|_p = 0, 1, 2, \ldots, 2h-\ell-1$, $x \bowtie_h y$ iff $x \equiv y \pmod{p^{|y|_p+\ell-h}}$ and so the number of equivalence classes for each of these heights is the number of units in $\mathbb{Z}_{p^{\ell-h}}$. In total then there are $(2h-\ell)(p^{\ell-h}-p^{\ell-h-1})$.

Now if $|y|_p > 2h-\ell$, then $x \bowtie_h y$ iff $x \equiv y \pmod{p^h}$ and so for each height of y from $2h-\ell+1$ to $h-1$, the number of equivalence classes is the number of units in $\mathbb{Z}_{p^{h-|y|_p}}$. And so the total number of equivalence classes for elements of height greater than $2h-\ell$ is

$$\big(p^{h-((2h-\ell)+1)}-p^{h-((2h-\ell)+1)-1}\big)+\big(p^{h-((2h-\ell)+2)}-p^{h-((2h-\ell)+2)-1}\big)+\cdots+(p-1)$$

which telescopes to $p^{\ell-h-1}-1$. Then accounting for the equivalence class of 0 which is all elements with height greater than h, there are $p^{\ell-h-1}$ equivalence classes for y such that $|y|_p > 2h-\ell$.

Finally, consider y with height $2h-\ell$. If $j \leq k$ then $\ell = j$ and so $w = h$. So the interesting case is when $j > k$ which means that $w = \min\{h+|4\frac{y}{p^{|y|_p}}+1|_p, h+j-k\}$. We will consider elements separately depending on the height of $4\frac{y}{p^{|y|_p}}+1$.

There are $p-2$ units in $\mathbb{Z}_p$ such that $|4\frac{y}{p^{|y|_p}}+1|_p = 0$. Therefore, for y such that $|4\frac{y}{p^{|y|_p}}+1|_p = 0$ there are $\frac{(p-2)}{p}\frac{p^h}{p^{|y|_p}} = (p-2)p^{\ell-h-1}$ equivalence classes.
Now for each $i \in \{1, 2, \ldots, j-k-1\}$, for elements with $|4\frac{y}{p^{|y|_p}}+1|_p = i$, there are $\frac{1}{p^i}\big(p^{h-|y|_p+i} - p^{h-|y|_p+i-1}\big) = p^{\ell-h} - p^{\ell-h-1}$ equivalence classes. When $|4\frac{y}{p^{|y|_p}}+1|_p = j-k$, there are simply $p^{\ell-h}$. And so the total number of equivalence classes for y such that $|y|_p = 2h-\ell$ is $(p-2)p^{\ell-h-1} + (j-k-1)\big(p^{\ell-h} - p^{\ell-h-1}\big) + p^{\ell-h} = (p-2)p^{\ell-h-1} + (j-k)\big(p^{\ell-h} - p^{\ell-h-1}\big) + p^{\ell-h-1}$.

Adding all these together and simplifying, we get the desired formula. □

We now present an example of the $\bowtie_h$ equivalence classes for a specific j and k and the corresponding non-isomorphic rings.

Example 6.1. *Let $j = 4$, $k = 3$, and $p = 3$. So we are considering rings with additive group $\mathbb{Z}_{3^7} \times \mathbb{Z}_{3^4} = \mathbb{Z}_{2187} \times \mathbb{Z}_{81}$. Then the height of R can either be $0, 1$, or 2. Since all rings of height zero are isomorphic, we will only outline the equivalence classes when the height of R is 1 or 2. The $\bowtie_h$ equivalence classes for rings of height 1 and 2 are as follows;*

$\underline{h=1:}$

$\{0, 3, 6, 9, \ldots\ldots\ldots, 78\}$

$\{1, 4, 7, 10 \ldots\ldots\ldots, 79\}$

$\{2, 5, 8, 11, \ldots\ldots\ldots, 80\}$

$\underline{h=2:}$

$\{0, 9, 18, \ldots, 72\}$

$\{1, 4, 7, 10, \ldots\ldots\ldots, 79\}$

$\{2, 5, 8, 11, \ldots\ldots\ldots, 80\}$

$\{3, 12, 21, \ldots, 75\}$

$\{6, 33, 60\}$

$\{15, 42, 69\}$

$\{24, 51, 58\}$

Recalling that $x = a/p^k$, the the non-isomorhpic rings corresponding to these equiv-

alence classes are

$$\begin{array}{ccc}
\mathbb{Z}_{2187}[x]/(x^2-x,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-162,27x) \\
\mathbb{Z}_{2187}[x]/(x^2-3x,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-27,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-405,27x) \\
\mathbb{Z}_{2187}[x]/(x^2-3x-27,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-54,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-648,27x) \\
\mathbb{Z}_{2187}[x]/(x^2-3x-54,27x) & \mathbb{Z}_{2187}[x]/(x^2-9x-81,27x) &
\end{array}$$

Referring to Theorem 5.2, the square-root-rings are as follows;

$$\begin{array}{ccc}
\mathbb{Z}_{2187}[x]/(x^2,27x) & \mathbb{Z}_{2187}[x]/(x^2-27,27x) & \mathbb{Z}_{2187}[x]/(x^2-81,27x) \\
\mathbb{Z}_{2187}[x]/(x^2-243,27x) & \mathbb{Z}_{2187}[x]/(x^2-729,27x) & \mathbb{Z}_{2187}[x]/(x^2-56,27x) \\
\mathbb{Z}_{2187}[x]/(x^2-162,27x) & \mathbb{Z}_{2187}[x]/(x^2-486,27x) & \mathbb{Z}_{2187}[x]/(x^2-1458,27x)
\end{array}$$

These are all of the rings with additive group $\mathbb{Z}_{3^7} \times \mathbb{Z}_{3^4}$.

This example shows how Theorems 6.1 and 6.2 allow us to easily list off the $\bowtie_h$ equivalence classes and the corresponding non-isomorphic rings. We can then use Theorem 5.2 to list the square-root-rings to obtain a complete list of the non-isomorphic rings whose additive group is isomorphic to $\mathbb{Z}_{p^{j+k}} \times \mathbb{Z}_{p^j}$ where p is any prime and j, k are any integers.

References

[1] Gilberto Bini, Flaminio Flamini, *Finite Commutative Rings and their Applications*, Klewer (2002).

[2] I.N. Herstein, *Non-commutative Rings*, Mathematical Association of America (1968).

[3] Judson, *Abstract Algebra* (1997).

[4] Shamil Asgarli, *Wedderburn's Little Theorem*, http://www.math.ubc.ca/ reichst/423-project-wedderburn.pdf.

[5] Wikipedia, *Hensel's Lemma*.

[6] Herstein, I. N., *"Wedderburn's theorem and a theorem of Jacobson."*, American Mathematical Monthly **68** (1961) 249-251.

[7] Stewart, Ian., *Galois Theory*, Chapman and Hall, (2004).

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

[9] Stone, M. H., *The Theory of Representations for Boolean Algebras*, Amer. Math Soc., (1936).